Г.Хассе

ЛЕКЦИИ ПО ТЕОРИИ ЧИСЕЛ

«Лекции по теории чисел» Г. Хассе занимают положение, промежуточное между элементарным руководством по теории чисел и монографией по какому-либо из ее специальных разделов. Первая и вторая главы содержат материал, исторически давно сложившийся. Вторая половина книги вводит читателя в основные области современной теории чисел — теорию алгебраических чисел, теорию алгебраических функций с конечным полем констант и (в меньшей степени) в аналитическую теорию чисел. Эти области не рассматриваются в книге систематически, но характерные для них постановки вопросов, некоторые основные результаты и связи с элементарной теорией чисел выясняются на важнейших частных случаях. Книга может, таким образом, служить для первоначального ознакомления с теорией чисел, но представляет также интерес и для лиц, с теорией чисел уже знакомых.

Для чтения книги необходима сравнительно небольшая предварительная математическая подготовка. Автор широко пользуется алгебраической терминологией, однако для понимания книги не требуется глубокого владения алгеброй, а достаточно лишь знакомства с основными алгебраическими понятиями—кольцо, поле, группа, идеал и т. д. Из курса анализа достаточно знать основы дифференциального и интегрального исчисления. Только в нескольких местах, понимание которых не является необходимым для дальнейшего чтения книги, автор пользуется основами теории функций комплексного переменного и основной теоремой теории Галуа.

ОГЛАВЛЕНИЕ

УКАЗАТЕЛЬ

ИЗ ПРЕДИСЛОВИЯ АВТОРА

Настоящая книга представляет собой несколько расширенный годовой курс лекций. На опыте прошлых лет я убедился, что строго систематический аксиоматико-алгебраический метод построения арифметики полей алгебраических чисел и полей алгебраических функций представляет слишком большие трудности для читателя, приступающего к изучению теории чисел впервые. Чтобы иметь возможность полностью понять и оценить этот метод, в значительной степени пронизанный абстрактными понятиями и являющийся результатом длительного исторического развития, необходимо, конечно, известное знакомство с конкретным материалом, лежащим в основе теории. В том, чтобы дать такое знакомство и тем самым содействовать приобретению достаточного опыта для понимания абстрактных понятий и внутренних связей теории чисел, и состоит цель настоящих «Лекций».

Исходя из этого я избрал в основном индуктивный способ изложения. В каждой из четырех глав книги я подвожу к современной точке зрения и к трудно доступным проблемам, исходя из простейших понятий и следуя, в основном, историческому развитию вопроса. При этом требования, предъявляемые к читателю, к концу главы каждый раз возрастают. При такой форме изложения нельзя избежать того, что уже затронутые ранее вопросы возникают еще раз в более глубоком аспекте и связываются с новыми понятиями. Такие обобщения не всегда проводятся во всех подробностях. Подход к современным исследованиям порой заканчивается указанием на современную журнальную литературу.

Что касается приводимого в книге материала, то я обращал особое внимание на то, чтобы поставить на первое место предмет собственно теории чисел, именно, свойства натуральных чисел, а теоретические обобщения представить как вытекающие из них. Это соответствует моему глубокому убеждению, что достижения теории чисел имеют тем большее значение, чем больше они обогащают наши знания о свойствах натуральных чисел. Исходя из этой точки зрения, я изложил ряд вопросов более или менее выходящих за рамки систематического изложения; так, например, в гл. I рассматриваются вопросы о совершенных числах, о простых числах Мерсенна и Ферма, о гипотезе Артина относительно перво-

образных корней; в гл. II рассматриваются вопросы о распределении квадратичных вычетов; в гл. IV рассматриваются вопросы о вычислении единиц с помощью непрерывных дробей, о чисто арифметических формулах для числа классов и о гипотезе Куммера относительно кубических характеров. Я смею надеяться, что это будет содействовать оживлению интереса к этим чисто теоретико-числовым вопросам, которыми до сих пор в учебной литературе до некоторой степени пренебрегали.

Между четырьмя главами книги существует тесная внутренняя связь, что видно из многочисленных ссылок в тексте на предыдущее и из указаний на последующее. Особенно тесная связь существует между гл. II и на первый взгляд совершенно отличной от нее гл. III; благодаря Дирихле эта связь его теоремы о простых числах с теорией квадратичных вычетов стала уже классической. Эта связь еще глубже проявляется в гл. III и IV; относительно этого мне хотелось бы отметить следующее. Понятие дивизора, столь важное для теории чисел, впервые вводится мной в п. 5 § 15 в связи с аналитическим представлением для произведения L-рядов Дирихле; это, конечно, не соответствует ни историческому развитию, ни систематическому обоснованию теории дивизоров. Однако это имеет то преимущество, что вновь вводимое понятие дивизоров сразу становится ясным, по крайней мере, с формальной точки зрения. Кроме того, становятся понятными корни установленной Дирихле связи между анализом и теорией чисел.

Арифметика полей алгебраических чисел для общего случая дана лишь в наброске, без доказательств. Исчерпывающим образом разбираются только квадратичные поля в гл. IV. При этом я пользуюсь несправедливо забытым методом Куммера, который лучше всего соответствует требованию предельной близости содержательного определения дивизоров к натуральным числам.

Глава I

ОСНОВЫ ТЕОРИИ

§ 1. РАЗЛОЖЕНИЕ НА ПРОСТЫЕ МНОЖИТЕЛИ

1. Натуральные целые и рациональные числа. Прежде всего мы скажем о том, что предполагается известным заранее. Мы считаем, что читателю известно: 1) определения и законы *действий* с натуральными числами в пределах трех первых элементарных операций (сложения, вычитания, умножения), а также и четвертой (деления), когда она выполнима в области натуральных чисел; 2) определения и законы *упорядочения* натуральных чисел по их величине; 3) законы, касающиеся связи между действиями и упорядочением (например, что большее, сложенное или перемноженное с бо́льшим дает большее).

Далее, мы предполагаем известным также расширение области натуральных чисел до замкнутой по отношению к трем первым элементарным операциям *области целостности* Γ *целых чисел*:

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

и расширение этой последней до замкнутого по отношению к четырем элементарным операциям *поля* P *рациональных чисел*:

$$0;\ \pm 1;\ \pm 2,\ \pm\frac{1}{2};\ \pm 3,\ \pm\frac{1}{3};\ \pm 4,\ \pm\frac{3}{2},\ \pm\frac{2}{3},\ \pm\frac{1}{4};\ \ldots,$$

а также и перенос на эти расширения упорядочения вместе с его законами (включая понятие абсолютной величины).

Обозначения Γ, P, введенные для области целых, соответственно рациональных чисел, мы будем применять в дальнейшем все время, не объясняя снова их значений.

В основе всех доказательств существования в теории чисел лежат следующие два принципа, которые мы также считаем известными:

Принцип существования. *В каждом непустом множестве натуральных чисел существует наименьшее натуральное число.*

Этот принцип будет непосредственно очевиден, если прибегнуть к известному изображению целых чисел в виде неограниченной

в обе стороны последовательности точек на прямой, находящихся на равных расстояниях друг от друга (или, кратко, *представлению на числовой прямой*), которое мы и в дальнейшем будем иногда использовать. Также очевидно, а, впрочем, является и формальным следствием из сказанного выше, что в каждом ограниченном непустом множестве натуральных чисел существует наибольшее натуральное число.

Принцип полной индукции. *Если некоторое высказывание, в котором фигурирует неопределенное натуральное число n, верно для $n=1$ и из его правильности для всех натуральных чисел n' с $1 \leqslant n' \leqslant n$ (или также только для n) следует его правильность для $n+1$, то это высказывание верно для каждого натурального числа n.*

При применении этого принципа в основу часто кладется вместо области натуральных чисел n расширенная посредством присоединения числа 0 область целых чисел $n \geqslant 0$, и индукция начинается поэтому с $n=0$. Это лишь формальное видоизменение принципа, получающееся посредством подстановки $n \to n-1$. Также часто бывает, что высказывание, о котором идет речь, оказывается для исходного значения $n=1$, соответственно $n=0$, тривиально верным потому, что оно для этого значения бессодержательно. Такие индуктивные доказательства, при которых, таким образом, даже не надо проверять выполнение утверждения для начального значения, выглядят особенно изящными.

2. Элементарная теория делимости. Сначала мы рассмотрим только область целостности Γ. При этом все употребляемые буквы будут обозначать числа из Γ.

В основе элементарной теории чисел лежит следующее *определение делимости*:

b называется *делителем* a, если $a=gb$.

При этом ударение делается на том, что число g, входящее в последнее соотношение, принадлежит к Γ (т. е. является целым); ведь с числом g из P, а именно с $g=a/b$, это соотношение выполняется всегда, если только $b \neq 0$. Однако, ввиду принятого ранее условия об обозначениях, мы могли это дополнительное требование, что g должно быть целым, не упоминать.

Для того чтобы указать, что b есть делитель числа a, применяется следующее краткое *обозначение*:

$b \mid a$ (читается: b *делит* a); в противном случае $b \nmid a$ (читается: b *не делит* a).

Существуют и другие способы для выражения того, что $b \mid a$:

b *содержится* в a, b *входит* в a,

a *делится* на b, a *содержит* b, a есть *кратное* числа b.

Фигурирующее в определении число g называется *дополнительным* к b *делителем* a.

Относительно соотношения делимости имеют место следующие факты, доказательства которых, непосредственно следующие из определения и свойств Γ, мы проводить не будем.

$$\left.\begin{array}{l} a \mid a \text{ для каждого } a, \\ \left\{\begin{array}{l} b \mid 0 \text{ для каждого } b,\ \pm 1 \mid a \text{ для каждого } a \\ 0 \mid a \text{ только для } a = 0,\ b \mid \pm 1 \text{ только для } b = \pm 1 \end{array}\right\}, \\ \text{из } c \mid b,\ b \mid a \text{ следует } c \mid a, \\ \left\{\begin{array}{l} \text{из } b \mid a \text{ следует } cb \mid ca \text{ для каждого } c \\ \text{из } cb \mid ca, \text{ где } c \neq 0, \text{ следует } b \mid a \end{array}\right\}, \\ \text{из } b_1 \mid a_1,\ b_2 \mid a_2 \text{ следует } b_1 b_2 \mid a_1 a_2, \\ \left\{\begin{array}{l} \text{из } b \mid a_1,\ b \mid a_2 \text{ следует } b \mid a_1 \pm a_2 \\ \text{из } b \mid a \text{ следует } b \mid ca \text{ для каждого } c \\ \text{из } b \mid a_1,\ b \mid a_2 \text{ следует } b \mid c_1 a_1 + c_2 a_2 \text{ для любых } c_1,\ c_2 \\ \text{(и аналогично для линейных комбинаций с большим числом членов)} \end{array}\right\}, \\ \text{из } b \mid a \text{ и } a \mid b \text{ следует } b = \pm a \text{ (и обратно).} \end{array}\right.$$

Каждое a имеет *тривиальные делители* ± 1, $\pm a$. Оба первые, $+1$ и -1, характеризуются также тем, что они являются единственными делителями числа 1; они называются *единицами* области целостности Γ. Оба последние, $+a$ и $-a$, получаются из a посредством умножения его на единицы; они называются *ассоциированными с* a (ассоциированность обозначается знаком $\cong$). Если делитель b числа $a \neq 0$ не ассоциирован с a, то говорят о *собственном делителе* b числа a, обозначается это $b \| a$. Это имеет место (при сделанных предположениях $b \mid a$, $a \neq 0$) тогда и только тогда, когда $|b| < |a|$, или, что одно и то же, когда дополнительный к b делитель g числа a обладает свойством $|g| > 1$.

С точки зрения только что очерченной теории делимости в Γ, натуральные числа a можно рассматривать как такую мультипликативно-замкнутую подобласть, что в ней каждая пара ассоциированных (т. е. в смысле делимости равноправных) целых чисел $\pm a \neq 0$ имеет точно одного представителя. Ввиду этого мы при дальнейшем развитии теории делимости ограничимся сначала подобластью натуральных чисел, которая, собственно говоря, и является предметом элементарной теории чисел, и только позднее сделаем те дополнения, которые потребуются при переходе ко всей области целостности Γ.

3. Простые числа. В дальнейшем развитии теории делимости и вообще во всей теории чисел основное значение имеет следующее определение, которое дает нам объекты, играющие роль строительного материала при мультипликативном построении натуральных чисел.

Определение. *Натуральное число p называется простым, если $p \neq 1$ и не имеет нетривиальных делителей.*

Из натуральных делителей должны существовать, таким образом, только два тривиальных: 1 и p. То, что число 1 не причисляется к простым, является соглашением, которое оказывается целесообразным при формулировке почти всех теоретико-числовых закономерностей.

Простые числа существуют, в чем можно тотчас же убедиться непосредственной проверкой; их последовательность начинается с $p = 2, 3, 5, 7, \ldots$ Без всяких проб существование простых чисел получается из следующего предложения, которое мы еще используем в дальнейшем.

Лемма. *Каждое натуральное число $a > 1$ обладает по меньшей мере одним простым делителем p (т. е. простым числом p с $p \mid a$), и, в частности, наименьший натуральный делитель $p > 1$ числа a является простым.*

Доказательство. Рассмотрим множество $\mathfrak{M}$ всех натуральных делителей > 1 числа a. Это множество $\mathfrak{M}$ не пусто, так как $a > 1$ и a есть делитель a, т. е. содержится в $\mathfrak{M}$. Поэтому, согласно принципу существования в п. 1, в $\mathfrak{M}$ существует наименьшее натуральное число p, которое, таким образом, характеризуется тем, что оно есть наименьший, за исключением 1, натуральный делитель числа a. Если бы p не было простым, то оно имело бы нетривиальный делитель q. Ввиду транзитивности в $q \mid p \mid a$, q делило бы также и a; а так как $q > 1$, то оно принадлежало бы тогда к $\mathfrak{M}$. Однако $q < p$, что противоречит минимальности p в $\mathfrak{M}$.

Совсем другой характер, чем только что доказанная лемма, носит следующая теорема существования, которая — так же как и первая часть леммы — имеется уже в компендиуме классической греческой математики — «Началах» Евклида (книга IX, теорема 20), с приводимым ниже доказательством.

Теорема Евклида[1]). *Последовательность простых чисел не обрывается, т. е. простых чисел существует бесконечно много.*

Доказательство. Будет показано — и так именно и гласит формулировка Евклида, — что для каждого данного конечного множества простых чисел $p_1, \ldots, p_n$ существует простое число p_{n+1}, отличное от всех чисел этого множества. Для этого образуем натуральное число

$$a = p_1 \ldots p_n + 1.$$

Так как $a > 1$, то по доказанной перед этим лемме a обладает хотя бы одним простым делителем p_{n+1}. Он отличен от $p_1, \ldots, p_n$, так как в противном случае мы имели бы $p_{n+1} \mid p_1 \ldots p_n$, что вместе с $p_{n+1} \mid a$ давало бы $p_{n+1} \mid 1$, а это невозможно.

[1]) Это название, ставшее общепринятым, не означает, что эта теорема была впервые доказана Евклидом; кто первый доказал теорему — неизвестно.

Замечание. Интересно отметить, что этот вывод может начинаться уже с $n=0$, т. е. нам вообще не нужно заранее знать ни одного простого числа. Надо только формально условиться, что произведению n множителей $p_1 \dots p_n$ в специальном случае $n=0$ приписывается значение 1 (подобно тому, как под суммой n слагаемых $a_1+\dots+a_n$ в случае $n=0$ мы понимаем число 0). Тогда в нашем доказательстве при $n=0$ получится $a=1+1=2$, и, согласно лемме, это даст нам наименьшее простое число $p_1=2$. Продолжая таким способом, мы на втором шагу получим из $a=2+1=3$ второе по порядку простое число $p_2=3$, однако уже на третьем шагу из $a=2\cdot 3+1=7$ мы получим не третье по порядку простое число 5, а $p_3=7$, на четвертом шагу из $a=2\cdot 3\cdot 7+1=43$ — уже $p_4=43$ и т. д. Продолжая этот процесс далее, мы получим последовательность простых чисел p_n, которая, впрочем, не обязательно будет расти монотонно, так как получающиеся числа a не всегда будут сами простыми, как это имело место на первых шагах.

Мы используем теорему Евклида, чтобы получить, правда очень грубую, оценку сверху для n-го простого числа p_n (теперь имеется в виду последовательность всех простых чисел). Именно, из доказательства следует, что если первые n простых чисел $p_1, \dots, p_n$ известны, то $(n+1)$-е простое число p_{n+1} не превосходит наименьшего простого делителя числа $p_1 \dots p_n+1$. Отсюда посредством полной индукции по n получается оценка:

$$p_n \leqslant 2^{2^{n-1}} \text{ для каждого } n \geqslant 1.$$

Мы упомянем здесь также еще один, на первый взгляд, неожиданный факт, а именно, что в последовательности $p_1, p_2, \dots$ всех простых чисел встречаются промежутки сколь угодно большой длины $n \geqslant 1$. Действительно, среди n следующих друг за другом натуральных чисел

$$(n+1)!+2, \dots, (n+1)!+(n+1)$$

ни одно не является простым, так как $(n+1)!+k$ при $k>1$ имеет k своим собственным делителем.

4. Основная теорема элементарной теории чисел. Теперь мы докажем основную теорему элементарной теории чисел, которая показывает, что простые числа действительно играют роль строительного материала для мультипликативного построения натуральных чисел, как это было сказано при определении простых чисел.

Теорема об однозначном разложении на простые множители. *Каждое натуральное число a обладает*

представлением

$$a = p_1 \dots p_n$$

в виде произведения некоторого количества $n \geqslant 0$ *простых чисел* $p_1, \dots, p_n$ (*не обязательно различных*), *и с точностью до порядка сомножителей такое представление единственно.*

При этом допускается также число $n = 0$, чтобы включить случай $a = 1$ в смысле сделанного в п. 3 соглашения.

Однозначное представление $a = p_1 \dots p_n$ называется *разложением числа* a *на простые множители.*

Доказательство. Мы докажем оба утверждения теоремы, а именно, а) *существование* и б) *однозначность* разложения, посредством полной индукции по a, следуя идее, выдвинутой в недавнее время Цермело.

Для $a = 1$ существует разложение с $n = 0$, а однозначность тривиальна, потому что каждое произведение простых чисел $p_1 \dots p_n$ с $n \geqslant 1$ заведомо > 1.

Пусть $a > 1$, и предположим, что оба утверждения выполняются для всех натуральных $a' < a$. Покажем, что тогда они выполняются также и для a.

а) *Существование.* Согласно лемме из п. 3 a обладает, по крайней мере, одним простым делителем p. Тогда имеет место разложение

$$a = pb$$

с натуральным b, и при этом $1 \leqslant b < a$. Поэтому, по предположению индукции, b имеет разложение на простые множители

$$b = p_1 \dots p_r \qquad (r \geqslant 0).$$

Тем самым получается разложение на простые множители и для a:

$$a = pp_1 \dots p_r.$$

б) *Однозначность.* По предположению индукции, разложение на простые множители для b однозначно. Поэтому a во всяком случае не обладает другим разложением на простые множители, в которое входило бы p; в каждое другое, быть может, возможное, разложение числа a могут, таким образом, входить лишь простые множители, отличные от p.

Предположим, что мы имеем такое разложение на простые множители

$$a = qq_1 \dots q_s,$$

которое мы также запишем в виде

$$a = qc,$$

чтобы выделить один из простых множителей (q). Как уже было сказано, $q \neq p$, и можно даже считать, что $q > p$; последнее будет выполняться само собой, если перед этим p было выбрано как однозначно определенный, согласно доказательству леммы в п. 3, наименьший собственный натуральный делитель числа a. Далее, также и $q_1, \ldots, q_s \neq p$.

Сбразуем теперь целое число

$$a' = a - pc = \left\{ \begin{array}{l} p(b-c) \\ (q-p)\,c \end{array} \right\}.$$

Так как $q > p$, то a' является натуральным, а из $a' = a - pc$ следует $a' < a$. Делители $b-c$, $q-p$, c числа a также являются натуральными числами и $< a$. Поэтому, по предположению индукции, a', $b-c$, $q-p$, c все обладают однозначным разложением на простые множители. Равенство $a' = p(b-c)$ показывает тогда, что в разложение числа a' входит простой множитель p. Из равенства $a' = (q-p)\,c$ следует поэтому, что p входит также в разложение, по крайней мере, одного из чисел $q-p$ и c. Однако в разложение на простые множители числа $c = q_1 \ldots q_s$ p входить не может, так как уже установлено, что $q_1, \ldots, q_s \neq p$. Следовательно, p должно встретиться в разложении числа $q-p$ и, таким образом, $p \mid q-p$. Вместе с $p \mid p$ это дает, ввиду соотношения $(q-p)+p=q$, что $p \mid q$, а так как $p < q$, то даже $p \parallel q$. Но это противоречит тому, что q простое.

Поэтому сделанное предположение о существовании другого разложения числа a на простые множители неверно, т. е. разложение числа a однозначно. Тем самым оба утверждения теоремы доказаны посредством полной индукции.

5. Видоизменения основной теоремы. Теперь мы приведем три более или менее формальных видоизменения основной теоремы элементарной теории чисел. Первое получается посредством соединения одинаковых простых множителей, входящих в разложение, в степень; второе включает случай отрицательных целых чисел, и третье — также и дробные рациональные числа.

I. Соединение в степени. *Каждое натуральное число a обладает одним и с точностью до порядка сомножителей только одним представлением*

$$a = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$$

в виде произведения степеней некоторого количества $r \geqslant 0$ различных простых чисел с натуральными показателями $\alpha_1, \ldots, \alpha_r$.

Эта формулировка основной теоремы немедленно получится из приведенной в п. 4, если равные между собой простые множители p_i соединить в степени $p_i^{\alpha_i}$ с натуральными показателя-

ми α_i. Эти показатели α_i, равные кратностям, с которыми различные простые p_i входят в разложение числа a на простые множители, определены однозначно. Можно также сделать однозначным и порядок следования степеней простых чисел посредством некоторого нормирующего условия, а именно, посредством условия

$$p_1 < \ldots < p_r$$

(т. е. расположения простых множителей в порядке возрастания), и в этом смысле говорят иногда о *каноническом разложении* числа a.

Для наших целей — и вообще для всей теории чисел, включая ее высшие разделы, которые в настоящей книге не затрагиваются — большую важность имеет, однако, несколько иное формальное видоизменение формулировки I. Оно исходит из следующего соображения. При заданном натуральном a множество $\mathfrak{P}$ всех простых чисел распадается, согласно основной теореме, на два подмножества, дополнительных друг к другу, а именно, на множество $\mathfrak{P}_a$ простых чисел, входящих в a, и множество $\mathfrak{Q}_a$ простых чисел, не входящих в a. Подмножество $\mathfrak{P}_a$, согласно основной теореме, конечно, подмножество же $\mathfrak{Q}_a$, согласно теореме Евклида, бесконечно. Далее, число a определяет, согласно I, однозначно для каждого p_i из $\mathfrak{P}_a$ натуральный показатель α_i, а именно, кратность, с которой p_i входит в разложение числа a на простые множители. Это положение можно распространить и на бесконечное множество простых чисел q из $\mathfrak{Q}_a$: все они входят в разложение числа a на простые множители с кратностью 0. Таким образом, число a однозначно определяет для каждого простого p из всего множества $\mathfrak{P}$ целое число $\alpha_p \geqslant 0$, равное кратности, с которой p входит в разложение числа a на простые множители. Мы будем понимать совокупность этих значений α_p как неотрицательную функцию, определенную числом a на множестве $\mathfrak{P}$ всех простых чисел p. Она обладает особым свойством, что лишь для конечного множества значений аргумента p значение функции $\alpha_p > 0$.

Разложение числа a на простые множители можно тогда записать в виде формально бесконечного произведения

$$a = \prod_{p \in \mathfrak{P}} p^{\alpha_p}$$

по всем простым числам p из $\mathfrak{P}$. Действительно, согласно п. 1, уже конечное множество $p = p_i$ из $\mathfrak{P}_a$ дает произведение a, а формальное присоединение бесконечного множества $p = q$ из $\mathfrak{Q}_a$ ничего не меняет, так как каждое из них вносит в произведение множитель $p^{\alpha_p} = q^0 = 1$. В дальнейшем мы будем кратко обозначать произведение, распространенное на множество $\mathfrak{P}$

всех простых чисел через $\prod_p$. Таким образом, мы можем теперь вместо I дать основной теореме следующую формулировку:

I′. *Каждое натуральное число a обладает представлением*

$$a = \prod_p p^{\alpha_p}$$

с однозначно определенной числом a системой целочисленных показателей α_p, соответствующих простым числам p, со следующими свойствами:

$\alpha_p \geqslant 0$ *для каждого* p,

$\alpha_p > 0$ *лишь для конечного множества простых* p.

Обратно, каждая целочисленная система показателей с этими свойствами однозначно определяет по формуле I′ натуральное число a. Поэтому формула I′ дает взаимно однозначное соответствие между натуральными числами a и целочисленными системами показателей α_p с указанными свойствами.

Выгода такого понимания и формального способа записи I′ основной теоремы по сравнению с I станет очевидной, когда мы рассмотрим умножение натуральных чисел. Если даны два натуральных числа

$$a = \prod_p p^{\alpha_p}, \qquad b = \prod_p p^{\beta_p}$$

в их однозначных разложениях на простые множители, то разложение на простые множители их произведения получается, очевидно, в виде

$$ab = \prod_p p^{\alpha_p + \beta_p},$$

т. е. нужно сложить почленно (как функции от p) системы показателей α_p, β_p, соответствующие множителям a, b.

II. Включение отрицательных целых чисел (область целостности Γ). *Каждое целое число $a \neq 0$ обладает одним и с точностью до порядка множителей только одним представлением*

$$a = \varepsilon p_1^{\alpha_1} \dots p_r^{\alpha_r}$$

в виде произведения единичного множителя $\varepsilon = \pm 1$ и некоторого количества $r \geqslant 0$ степеней различных простых чисел $p_1, \dots, p_r$ с натуральными показателями $\alpha_1, \dots, \alpha_r$.

Если принять во внимание, как отрицательные целые числа получаются из натуральных, то это обобщение утверждения I становится очевидным как в отношении существования, так и в отношении однозначности разложения. Аналогично I′ оно может быть сформулировано также и так:

II′. *Каждое целое число* $a \neq 0$ *обладает представлением*

$$a = \varepsilon \prod_p p^{\alpha_p}$$

с однозначно определенными числом a, *единичным множителем* $\varepsilon = \pm 1$ *и системой целочисленных показателей* α_p, *соответствующих простым числам* p, *со следующими свойствами*:

$\alpha_p \geqslant 0$ *для каждого* p,

$\alpha_p > 0$ *лишь для конечного множества простых* p.

Обратно, каждая целочисленная система показателей α_p с этими свойствами вместе с каждым единичным множителем ε однозначно определяет по формуле II′ целое число $a \neq 0$.

Если даны два целых числа

$$a = \varepsilon \prod_p p^{\alpha_p}, \qquad b = \eta \prod_p p^{\beta_p} \qquad (a, b \neq 0)$$

в этом однозначном представлении, то аналогичное представление для их произведения получается, очевидно, в виде

$$ab = \varepsilon\eta \prod_p p^{\alpha_p + \beta_p},$$

т. е. нужно перемножить соответствующие сомножителям a, b единичные множители ε, η, а системы показателей α_p, β_p почленно сложить.

III. Включение дробных рациональных чисел (поле P). *Каждое рациональное число* $a \neq 0$ *обладает одним и с точностью до порядка множителей в числителе и знаменателе только одним представлением вида*

$$a = \varepsilon \frac{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}{q_1^{\beta_1} \cdots q_s^{\beta_s}},$$

где $\varepsilon = \pm 1$, p_i, q_j — *различные простые числа в количествах* r, $s \geqslant 0$ *и* α_i, β_j — *натуральные показатели.*

Так как в этом месте нашего построения элементарной теории чисел мы еще не обладаем теоремой о существовании и однозначности представления каждого рационального числа $a \neq 0$ в виде несократимой дроби, которая будет доказана лишь в § 2 с помощью развитой здесь теории, то высказанное обобщение утверждения II не следует сразу из того, как рациональные числа получаются из целых, и нуждается в доказательстве.

Доказательство. На основании построения рациональных чисел из целых каждое рациональное число обладает, по крайней мере, одним представлением вида

$$a = \varepsilon \frac{A}{B}$$

с единичным множителем ε и натуральными числами A, B. Последние мы считаем взятыми в их однозначных разложениях на простые множители в виде I, а общие простые множители в числителе и знаменателе считаем сокращенными в соответствии с правилами действий с рациональными числами. Так мы получаем представление требуемого вида; запишем его кратко

$$a = \varepsilon \frac{P}{Q},$$

где, таким образом,

$$P = p_1^{\alpha_1} \dots p_r^{\alpha_r}, \qquad Q = q_1^{\beta_1} \dots q_s^{\beta_s}$$

представляют собой произведения степеней различных простых чисел p_i, q_j в количествах r, $s \geqslant 0$. Пусть теперь

$$a = \varepsilon' \frac{P'}{Q'}$$

— другое представление такого же вида. Тогда, согласно признаку равенства рациональных чисел, мы будем иметь

$$\varepsilon P Q' = \varepsilon' P' Q.$$

Ввиду однозначности разложения II целых чисел на простые множители отсюда следует, с одной стороны, что $\varepsilon = \varepsilon'$, и, с другой стороны, что простые множители числа P, будучи отличными от простых множителей числа Q, должны встречаться среди простых множителей числа P' (и по меньшей мере в той же кратности), и, обратно, простые множители числа P' должны встречаться среди простых множителей числа P, так что $P = P'$, а тогда также и $Q = Q'$. Тем самым существование и однозначность утверждаемого разложения доказаны.

Теперь, аналогично II′, сразу получается следующая формулировка:

III′. *Каждое рациональное число* $a \neq 0$ *обладает представлением*

$$a = \varepsilon \prod_p p^{\alpha_p}$$

с однозначно определенными для числа a *единичным множителем* $\varepsilon = \pm 1$ *и системой целочисленных показателей* α_p, *соответствующих простым числам* p, *со следующим свойством*:

$\alpha_p \neq 0$ *лишь для конечного множества простых* p.

Обратно, каждая целочисленная система показателей с этим свойством вместе с каждым единичным множителем ε однозначно определяет по формуле III′ рациональное число $a \neq 0$.

Если даны два рациональных числа

$$a = \varepsilon \prod_p p^{\alpha_p}, \qquad b = \eta \prod_p p^{\beta_p} \qquad (a,\ b \neq 0)$$

в этом однозначном представлении, то аналогичные представления для их произведения и частного получаются, очевидно, в виде

$$ab = \varepsilon\eta \prod_p p^{\alpha_p+\beta_p}, \qquad \frac{a}{b} = \frac{\varepsilon}{\eta} \prod_p p^{\alpha_p-\beta_p},$$

т. е. нужно перемножить, соответственно разделить единичные множители, соответствующие сомножителям a, b, а системы показателей α_p, β_p почленно сложить, соответственно вычесть.

Мы будем называть данное в II′ для $a \neq 0$ из Γ и в III′ для $a \neq 0$ из P однозначное представление $a = \varepsilon \prod_p p^{\alpha_p}$ *разложением целых* соответственно *рациональных чисел на простые множители*. Когда единичный множитель ε (т. е. знак числа a) нас интересовать не будет, мы будем писать короче $a \cong \prod_p p^{\alpha_p}$, употребляя введенный в п. 2 знак ассоциированности $\cong$.

Единственная разница между формулировками II′ для Γ и III′ для P формально состоит в том, что имеющееся в II′ свойство системы показателей «$\alpha_p \geqslant 0$ для каждого p» в III′ отсутствует. Таким образом, если рассматривать область целостности Γ как подобласть поля P, то среди всех чисел $a \neq 0$ из P числа из Γ характеризуются тем, что в их разложении на простые множители все показатели $\alpha_p \geqslant 0$: каждое число $a \neq 0$ из Γ обладает этим свойством, и каждое число $a \neq 0$ из P с этим свойством принадлежит к Γ. Этот характерный признак, выделяющий целые числа среди рациональных, мы, ввиду его особой важности, сформулируем в качестве отдельной теоремы:

Теорема целостности. *Рациональное число $a \neq 0$ является целым тогда и только тогда, когда в его разложении $a \cong \prod_p p^{\alpha_p}$ на простые множители все показатели $\alpha_p \geqslant 0$.*

6. Иррациональность n-х корней из целых чисел. В качестве применения разложения рациональных чисел на простые множители рассмотрим вопрос о том, когда рациональное и в частности целое число $a \neq 0$ является n-й степенью некоторого рационального числа $b \neq 0$, где n — данное натуральное число.

Если представить a и b в их разложении на простые множители, то, ввиду его однозначности, равенство $a = b^n$ равносильно выполнению соотношений

$$\varepsilon = \eta^n, \quad \alpha_p = n\beta_p \quad \text{одновременно для всех } p.$$

Для того чтобы эти соотношения при заданных ε, α_p со свойствами из III′ имели решение η, β_p с теми же свойствами, очевидно, необходимо и достаточно, чтобы выполнялись следующие условия

$$\varepsilon = 1 \text{ в случае четного } n; \quad n \mid \alpha_p \text{ для всех } p.$$

Последние условия нетривиальны только для конечного множества простых чисел p с $\alpha_p \neq 0$.

Если, в частности, a предполагается целым, так что все $\alpha_p \geqslant 0$, то для всех β_p будет также $\beta_p \geqslant 0$, т. е. тогда и b обязательно целое.

Этим доказано:

IV. *Для того чтобы рациональное число $a \neq 0$ было n-й степенью некоторого рационального числа $b \neq 0$, необходимо и достаточно, чтобы в случае четного n было $a > 0$ и чтобы все простые числа p входили в разложение числа a на простые множители с показателями степени, делящимися на n.*

Если a целое, то и b обязательно целое.

Самое важное в этом результате заключается в последнем высказывании. Из него следует, что целое число $a \neq 0$, не являющееся n-й степенью *целого* числа, не является также n-й степенью *рационального* числа, так что в этом случае числа $\sqrt[n]{a}$ (существующие в поле вещественных или комплексных чисел) *иррациональны*. В частности, мы получаем, что при $n > 1$ иррациональны $\sqrt[n]{\pm p}$ при любом простом p, а также и все $\sqrt[n]{\pm p_1 \dots p_r}$ с $r \geqslant 1$ различных простых $p_1, \dots, p_r$.

§ 2. ОБЩИЙ НАИБОЛЬШИЙ ДЕЛИТЕЛЬ

1. Критерии делимости и простого делителя. Дальнейшему построению теории делимости в области целостности Γ целых чисел мы предпошлем установление критерия делимости, который сразу следует из теоремы целостности в § 1, п. 5.

Критерий делимости. *Пусть даны два целых, $\neq 0$ числа*

$$a \cong \prod_p p^{\alpha_p}, \ \alpha_p \geqslant 0, \qquad \textit{лишь конечное множество } \alpha_p > 0,$$

$$b \cong \prod_p p^{\beta_p}, \ \beta_p \geqslant 0, \qquad \textit{лишь конечное множество } \beta_p > 0,$$

в разложении на простые множители. $b \mid a$ тогда и только тогда, когда $\beta_p \leqslant \alpha_p$ для всех p.

Действительно, согласно определению, $b \mid a$ равносильно тому, что

$$\frac{a}{b} \cong \prod_p p^{\alpha_p - \beta_p}$$

целое, а это, по теореме целостности, в свою очередь равносильно тому, что все $\alpha_p - \beta_p \geqslant 0$.

Чтобы добиться того, чтобы этот критерий делимости оставался в силе и тогда, когда $a = 0$ или $b = 0$, мы введем формально разложение на простые множители также и для числа 0. Это число обладает свойством $b \mid 0$ для всех целых b. Таким образом, если положить $0 \cong \prod_p p^{\nu_p}$, то для действительности критерия при $a = 0$ необходимо потребовать, чтобы система показателей ν_p имела свойство $\beta_p \leqslant \nu_p$ для каждой возможной системы показателей β_p целого числа. Это будет выполняться тогда и только тогда, когда все $\nu_p = \infty$. Поэтому мы формально определяем:

$$0 \cong \prod_p p^{\infty}.$$

При таком определении критерий делимости остается в силе для $a = 0$. Однако он будет верен и для $b = 0$; в самом деле, в соответствии с тем фактом, что $0 \mid a$ имеет место лишь при $a = 0$, соотношения для показателей $\infty \leqslant \alpha_p$ имеют только решение $\alpha_p = \infty$.

Введенное разложение числа 0, в котором все показатели равны ∞, мы сопоставим с разложением

$$\pm 1 \cong \prod_p p^0$$

единиц ± 1, *в котором все показатели равны* 0. В смысле теории делимости числа ± 1 играют роль наименьших, а число 0 — роль наибольшего числа среди всех целых чисел a, что видно из соотношений делимости $\pm 1 \mid a \mid 0$, имеющих место для любого целого a. Это свойство минимальности, соответственно максимальности отражается в том, что система целочисленных неотрицательных показателей α_p в разложении на простые множители имеет соответственно наименьшее или наибольшее возможное значение.

В качестве важного следствия из критерия делимости мы дадим

Критерий простого делителя. *Простыми делителями p целого числа a, т. е. простыми числами p, входящими в a, являются те и только те p, для которых соответствующие показатели α_p в разложении числа a на простые множители* > 0.

Действительно, согласно критерию делимости, $p \mid a$ при простом p равносильно тому, что для соответствующего этому показателя α_p в разложении a на простые множители имеет место $\alpha \geqslant 1$.

2. Определение общего наибольшего делителя. Теперь мы поставим себе задачу получить обзор всех общих делителей x двух целых чисел a, b.

Для этого мы предположим, что a, b имеют такие же разложения на простые множители, как в формулировке критерия делимости, а для неизвестного x разложение пусть будет

$$x \cong \prod_p p^{\xi_p}.$$

Согласно критерию делимости, $x \mid a$ и $x \mid b$ имеют место одновременно тогда и только тогда, когда одновременно $\xi_p \leqslant \alpha_p$, $\xi_p \leqslant \beta_p$ для всех p, или, другими словами, когда $\xi_p \leqslant \min(\alpha_p, \beta_p)$ для всех p. Если теперь хотя бы одно из a, b отлично от 0, то

$$\delta_p = \min(\alpha_p, \beta_p)$$

представляет собой целочисленную систему показателей, для которой выполняются оба свойства:

$$\delta_p \geqslant 0 \text{ для каждого } p,$$

$$\delta_p > 0 \text{ лишь для конечного множества } p,$$

и потому эта система определяет натуральное число

$$d = \prod_p p^{\delta_p}.$$

Это число по самому его построению обладает следующими двумя свойствами:

$$d \mid a, \quad d \mid b \tag{1}$$

$$\text{из } x \mid a, \ x \mid b \text{ следует } x \mid d \text{ (и обратно).} \tag{2}$$

Сверх того, этими двумя свойствами число d определяется однозначно. Действительно, если натуральное число d' также имеет эти свойства, то из (1) для d и из (2) для d' следует, что $d \mid d'$, и точно так же из (1) для d' и из (2) для d следует, что $d' \mid d$, а вместе это дает $d = d'$.

Теперь мы можем получить обзор всех общих делителей двух целых чисел:

I. *Для двух целых чисел a, b, из которых хотя бы одно не равно 0, существует одно и только одно натуральное число d со свойствами* (1), (2). *Оно называется общим наибольшим делителем чисел a, b и обозначается*

$$d = (a, b).$$

Совокупность общих делителей чисел a, b совпадает с совокупностью делителей числа d.

В специальном случае, когда $a=0$ и $b=0$, необходимо положить $d=0$, чтобы сохранить свойства (1), (2); таким образом,

$$0=(0, 0).$$

За исключением этого специального случая, d является «наибольшим» общим делителем чисел a и b не только в смысле делимости [свойство (2)], но и в смысле обычной величины (упорядочение на числовой прямой), а также и по абсолютной величине.

В то время как для построения d использовались разложения чисел a, b на простые множители, в формулировке I, включая и свойства (1), (2), эти разложения уже не фигурируют. На этом важном обстоятельстве мы в дальнейшем еще подробно остановимся.

3. Определение общего наименьшего кратного. Совершенно аналогично можно решить вопрос об обзоре всех общих кратных y двух целых чисел a, b.

Для этого мы снова предположим, что a, b имеют такие же, как раньше, разложения на простые множители, а для неизвестного y разложение пусть будет

$$y=\prod_p p^{\eta_p}.$$

Согласно критерию делимости, $a \mid y$ и $b \mid y$ имеют место одновременно тогда и только тогда, когда одновременно $\alpha_p \leqslant \eta_p$, $\beta_p \leqslant \eta_p$ для всех p, или, другими словами, когда $\max(\alpha_p, \beta_p) \leqslant \eta_p$ для всех p. Если теперь a, b оба отличны от 0, то

$$\varepsilon_p = \max(\alpha_p, \beta_p)$$

представляет собой целочисленную систему показателей, для которой снова выполняются оба свойства:

$$\varepsilon_p \geqslant 0 \text{ для каждого } p,$$

$$\varepsilon_p > 0 \text{ лишь для конечного множества } p,$$

и потому эта система определяет натуральное число

$$e=\prod_p p^{\varepsilon_p}.$$

Это число, согласно его построению, обладает следующими двумя свойствами:

$$a \mid e, \quad b \mid e \tag{3}$$

$$\text{из } a \mid y, \quad b \mid y \text{ следует } e \mid y \text{ (и обратно).} \tag{4}$$

Этими двумя свойствами число e опять-таки определяется однозначно. Действительно, если натуральное число e' также имеет

эти свойства, то из (3) для e и из (4) для e' следует, что $e' \mid e$, и точно так же из (3) для e' и из (4) для e следует, что $e \mid e'$, а вместе это дает $e = e'$.

Теперь мы можем получить обзор всех общих кратных двух целых чисел:

II. *Для двух целых чисел a, b, которые оба отличны от 0, существует одно и только одно натуральное число e со свойствами* (3), (4). *Оно называется общим наименьшим кратным чисел a, b и обозначается*

$$e = [a, b].$$

Совокупность общих кратных чисел a, b совпадает с совокупностью кратных числа e.

В специальном случае, когда или $a = 0$, или $b = 0$, необходимо положить $e = 0$, чтобы сохранить свойства (3), (4); таким образом,

$$0 = [0, a] = [b, 0].$$

Заметим, что формальная аналогия между общим наибольшим делителем и общим наименьшим кратным нарушается только в специальных случаях; в I такой случай характеризуется тем, что «*a, b не оба равны* 0», а в II тем, что «*a, b оба не равны* 0». Если оба эти условия выразить посредством основных логических отношений $\vee$ (или), $\wedge$ (и):

$$a \neq 0 \vee b \neq 0 \text{ соответственно } a \neq 0 \wedge b \neq 0,$$

то они будут соответствовать друг другу по известному принципу двойственности формальной логики.

4. Свойства общего наибольшего делителя и общего наименьшего кратного. Свойства, совершенно аналогичные тем, которые были получены нами в п. 2, 3 для двух целых чисел a, b, имеет место также для *конечного множества* целых чисел a, b, ... При этом мы можем быть кратки.

Из разложений на простые множители

$$a \cong \prod_p p^{\alpha_p}, \qquad b \cong \prod_p p^{\beta_p}$$

определяются два числа

$$d = (a, b, \ldots) = \prod_p p^{\min(\alpha_p, \beta_p, \ldots)},$$

$$e = [a, b, \ldots] = \prod_p p^{\max(\alpha_p, \beta_p, \ldots)},$$

называемые *общим наибольшим делителем* и *общим наименьшим кратным* чисел a, b, ... При этом d есть натуральное число, если a, b, ... не все равны 0, в противном случае $d = 0$, и e

есть натуральное число, если все a, b, ... не равны 0, в противном случае $e=0$. Эти числа d, e имеют свойства

$$\left\{\begin{array}{ll} d\,|\,a,\ d\,|\,b,\ \ldots & (1)\\ \text{из } x\,|\,a,\ x\,|\,b,\ \ldots \text{ следует } x\,|\,d \text{ (и обратно)} & (2)\end{array}\right\},$$

$$\left\{\begin{array}{ll} a\,|\,e,\ b\,|\,e,\ \ldots & (3)\\ \text{из } a\,|\,y,\ b\,|\,y,\ \ldots \text{ следует } e\,|\,y \text{ (и обратно)} & (4)\end{array}\right\},$$

и этими свойствами они определяются однозначно.

Из свойств min и max без труда получаются следующие правила для образования $(a, b, \ldots)$ и $[a, b, \ldots]$:

$(a, b, \ldots)$ и $[a, b, \ldots]$ не зависят от порядка следования $a, b, \ldots$,

$(a, b, c, \ldots)=(a, (b, c, \ldots))$, $[a, b, c, \ldots]=[a, [b, c, \ldots]]$,

$(ta, tb, \ldots)\cong t\,(a, b, \ldots)$, $[ta, tb, \ldots]\cong t[a, b, \ldots]$ для каждого целого t,

$(0, a, b, \ldots)=(a, b, \ldots)$, $[1, a, b, \ldots]=[a, b, \ldots]$,

$(1, a, b, \ldots)=1$, $[0, a, b, \ldots]=0$.

Второе из этих правил позволяет рекуррентно свести определение общего наибольшего делителя и общего наименьшего кратного конечного множества целых чисел к последовательному определению общего наибольшего делителя, соответственно общего наименьшего кратного двух целых чисел, а согласно четвертому и пятому правилам, и, принимая во внимание, что знаки чисел нам безразличны, мы можем всегда предполагать, что a, b, ... — натуральные числа, отличные от 0 и 1. Далее, можно еще свести определение общего наименьшего кратного к определению общего наибольшего делителя. Для этого предположим, без ограничения общности, что a, b, ... все отличны от 0, и пусть A, B, ... — те целые числа, которые получаются при делении произведения ab ... на a, b, ...:

$$aA=bB=\ldots=ab\ldots.$$

Тогда имеет место

$$[a, b, \ldots]\cong\frac{ab\ldots}{(A, B, \ldots)}.$$

В самом деле, если α_p, β_p, ..., A_p, B_p, ... — системы показателей из разложений чисел a, b, ..., A, B, ... на простые множители, так что

$$\sigma_p=\alpha_p+\mathsf{A}_p=\beta_p+\mathsf{B}_p=\ldots$$

есть система показателей из разложения на простые множители произведения $ab \ldots$, то мы имеем

$$\max(\alpha_p, \beta_p, \ldots) = \max(\sigma_p - \mathsf{A}_p, \sigma_p - \mathsf{B}_p, \ldots) = \\ = \sigma_p - \min(\mathsf{A}_p, \mathsf{B}_p, \ldots);$$

отсюда следует наше утверждение. В частности, для двух целых чисел a, b, которые оба отличны от 0, это правило дает просто

$$[a, b] \cong \frac{ab}{(a, b)}.$$

Заметим еще, что при образовании общего наибольшего делителя можно даже допустить, что a, b, ... есть бесконечное множество целых чисел, однако в случае общего наименьшего кратного этого допускать нельзя.

5. Взаимная простота и попарная взаимная простота. Целые числа a, b, ... называются *взаимно простыми*, если их общий наибольший делитель $(a, b, \ldots) = 1$; они называются *попарно взаимно простыми*, если это имеет место для каждой выбранной из них пары.

Из данного в п. 4 разложения общего наибольшего делителя $d = (a, b, \ldots)$ на простые множители мы немедленно получаем в качестве необходимого и достаточного условия для $d = 1$, что для каждого p по меньшей мере один из показателей α_p, β_p, $\ldots = 0$. Согласно критерию простого делителя из п. 1, это означает, что для каждого p выполняется хотя бы одно из отношений $p + a$, $p + b$, ... Таким образом, получается

Критерий взаимной простоты. *Целые числа взаимно просты тогда и только тогда, когда они не имеют общего простого делителя.*

Отсюда следует.

Критерий попарной взаимной простоты. *Целые числа a, b, ... попарно взаимно просты тогда и только тогда, когда простые делители числа a, простые делители числа b, ... все различны между собой.*

Другой, не опирающийся на разложение в произведение простых множителей критерий попарной взаимной простоты конечного множества целых чисел a, b, ..., которые все не равны 0, гласит:

$$[a, b, \ldots] \cong ab \ldots.$$

Действительно, в обозначениях из п. 4 последнее соотношение равносильно выполнению соотношений

$$\max(\alpha_p, \beta_p, \ldots) = \alpha_p + \beta_p + \ldots$$

для всех p; а эти соотношения, очевидно, выполняются тогда и только тогда, когда среди показателей α_p, β_p, ..., которые все $\geqslant 0$, для каждого p самое большее один из них > 0, а это означает, согласно критерию простого делителя из п. 1, что простые делители чисел a, b, ... все различны между собой.

Используя доказанное в п. 4 соотношение

$$[a, b, \ldots] \cong \frac{ab \ldots}{(A, B, \ldots)},$$

мы получим отсюда часто применяемую теорему:

III. *Если a, b, ... — конечное множество целых чисел, которые все не равны* 0, *и A, B, ... получаются при делении произведения ab ... на a, b, ..., то a, b, ... попарно взаимно просты тогда и только тогда, когда A, B, ... взаимно просты.*

Следующая, важная для дальнейшего теорема гласит:

IV. *Если для целых a, b, g имеет место $b \mid ga$ и при этом g взаимно просто с b, то $b \mid a$.*

Доказательство. Пусть α_p, β_p, γ_p — показатели из разложений a, b, g на простые множители. Для тех p, для которых $\gamma_p > 0$, и, следовательно, $p \mid g$, мы по предположению имеем $p \nmid b$, и, следовательно, $\beta_p = 0$, а потому заведомо $\beta_p \leqslant \alpha_p$. Для p с $\gamma_p = 0$ предположение $\beta_p \leqslant \alpha_p + \gamma_p$ равносильно утверждению $\beta_p \leqslant \alpha_p$.

Наконец, из правила в п. 4 относительно вынесения общего множителя немедленно получается:

V. *Если a, b, ... — целые числа, которые все не равны* 0, *и*

$$(a, b, \ldots) = d,$$

то имеет место

$$a = da_0, \qquad b = db_0 \ldots$$

с

$$(a_0, b_0, \ldots) = 1,$$

т. е. с взаимно простыми целыми числами a_0, b_0, ...

6. Представление несократимой дробью, представление с общим наименьшим знаменателем. Используя теорию общего наибольшего делителя целых чисел, можно рассмотреть вопрос о *представлении* рациональных чисел *несократимыми дробями.*

Теорема о представлении несократимой дробью. *Каждое рациональное число $a \neq 0$ обладает представлением дробью*

$$a = \frac{m}{n}$$

с однозначно определенными целыми взаимно простыми числами m, n, *причем* $n > 0$.

Каждое другое представление дробью

$$a = \frac{M}{N}$$

с целыми M, N *и* $N > 0$ *получается из него посредством умножения числителя и знаменателя на некоторое натуральное число* t, *а именно, на* $t = (M, N)$:

$$M = tm, \qquad N = tn.$$

Доказательство. Если $a = M/N$ — какое-нибудь представление числа a дробью с $t = (M, N)$ и

$$M = tm, \qquad N = tn,$$

то после сокращения на t получится, согласно V п. 5, представление $a = m/n$ требуемого вида. Если имеется другое такое представление $a = m'/n'$, то

$$mn' = m'n,$$

и потому $n \mid mn'$ и $n' \mid m'n$. Ввиду того что $(m, n) = 1$ и $(m', n') = 1$, отсюда следует далее, по IV п. 5, что $n \mid n'$ и $n' \mid n$. Так как должно быть $n > 0$, $n' > 0$, то $n = n'$, а потому и $m = m'$.

Числа m и n, фигурирующие в представлении несократимой дробью $a = m/n$, коротко называются *числителем* и *знаменателем* числа a. Для $a \neq 0$ они, очевидно, получаются из разложения на простые множители

$$a = \varepsilon \prod_p p^{\alpha_p}$$

в виде

$$m = \varepsilon \prod_{\alpha_p > 0} p^{\alpha_p}, \qquad n = \prod_{\alpha_p < 0} p^{-\alpha_p}.$$

Для $a = 0$ имеем $m = 0$, $n = 1$.

Представление одного рационального числа a несократимой дробью обобщается для конечного множества рациональных чисел *представлением с общим наименьшим знаменателем*. Пусть n — общее наименьшее кратное знаменателей чисел $a_1, \ldots, a_r$, или так называемый общий наименьший знаменатель чисел $a_1, \ldots, a_r$. Тогда $a_1, \ldots, a_r$ можно записать в виде дробей с общим знаменателем n, т. е. существует система представлений

$$a_1 = \frac{m_1}{n}, \quad \ldots, \quad a_r = \frac{m_r}{n}$$

с целыми $m_1, \ldots, m_r$. Если теперь имеется какая-нибудь другая система представлений

$$a_1 = \frac{M_1}{N}, \ \ldots, \ a_r = \frac{M_r}{N}$$

с натуральным N и целыми $M_1, \ldots, M_r$, то N есть общее кратное знаменателей чисел $a_1, \ldots, a_r$ и потому делится на n. Поэтому дроби второй системы представлений получаются из дробей первой системы посредством умножения числителей и знаменателя на натуральное число t:

$$M_1 = tm_1, \ \ldots, \ M_r = tm_r, \ N = tn.$$

Отсюда следует, что $m_1, \ldots, m_r, n$ взаимно просты; в противном случае, согласно V п. 5, существовала бы система представлений рассматриваемого вида с общим знаменателем $n' \parallel n$, в то время как, по только что доказанному, для каждого такого представления имеет место $n \mid n'$. Поэтому первоначально взятая система представлений с общим наименьшим знаменателем n отличается от всех других взаимной простотой $m_1, \ldots, m_r, n$. Действительно, для каждой другой, по доказанному, имеет место

$$(M_1, \ \ldots, \ M_r, \ N) = t.$$

Если высказать установленное нами положение вещей несколько по-иному, то мы сможем сформулировать эти результаты в следующей форме, аналогичной случаю *одного* рационального числа a.

Теорема о представлении с общим наименьшим знаменателем. *Для данного конечного множества рациональных чисел $a_1, \ldots, a_r$ существует такое однозначно определенное натуральное число n, что*

$$a_1 = \frac{m_1}{n}, \ \ldots, \ a_r = \frac{m_r}{n}$$

с целыми $m_1, \ldots, m_r$ и $(m_1, \ \ldots, \ m_r, \ n) = 1$. Каждая другая система представлений дробями

$$a_1 = \frac{M_1}{N}, \ \ldots, \ a_r = \frac{M_r}{N}$$

с натуральным N и целыми $M_1, \ \ldots, \ M_r$ получается из нее посредством умножения числителей и знаменателя на некоторое натуральное число t, а именно, на $t = (M_1, \ \ldots, \ M_r, \ N)$:

$$M_1 = tm_1, \ \ldots, \ M_r = tm_r, \ N = tn.$$

Натуральное число n есть общий наименьший знаменатель чисел $a_1, \ \ldots, \ a_r$, т. е. общее наименьшее кратное знаменателей чисел $a_1, \ \ldots, \ a_r$.

7. Основная теорема об общем наибольшем делителе. Изложенное нами построение теории делимости в отношении материала соответствует программе элементарного математического обучения, только этот материал рассматривался здесь с теоретической точки зрения и был снабжен строгими математическими доказательствами. Последнее относится в особенности к составляющей основу всей теории теореме об однозначном разложении на простые множители, которая при элементарном изложении обычно молчаливо предполагается справедливой, поскольку на этой ступени вообще еще не может быть речи о строгих доказательствах. К сожалению, как показывает опыт, при первоначальном изучении теории чисел у многих вследствие этого складывается совершенно неправильное впечатление, будто эта теорема непосредственно очевидна и не нуждается ни в каком обосновании, впечатление, сохраняющееся у некоторых навсегда.

Что касается формы изложения, то данное нами построение теории делимости чисто мультипликативно, что вполне естественно при опирающемся лишь на умножение определении делимости. Тот факт, что при этом все же появляются сложение и вычитание для систем показателей разложений на простые множители, не играет роли; над собственными объектами исследования, целыми числами, производится только умножение. Сложение и вычитание самих этих объектов используется только в одном единственном, хотя и очень важном месте, а именно, при доказательстве однозначности разложения на простые множители в § 1, п. 4, где фигурируют разности $a-pc$, $b-c$, $q-p$ и применяется аддитивное правило «из $b \mid a_1$, $b \mid a_2$ следует $b \mid a_1 + a_2$» (кроме этого, сложение используется еще при образовании $p_1 \dots p_n+1$ в доказательстве Евклида в § 1, п. 3, которое, однако, для теории делимости не играет существенной роли). Непосредственно же в теории общего наибольшего делителя не остается уже никаких следов сложения и вычитания.

Поэтому тем более неожиданно, что общий наибольший делитель допускает кроме мультипликативного также и аддитивное истолкование, а именно, имеет место

Основная теорема об общем наибольшем делителе. *Общий наибольший делитель* $d=(a_1, \dots, a_r)$ *конечного множества целых чисел* $a_1, \dots, a_r$, *которые не все равны* 0, *может быть представлен в форме*

$$d = x_1a_1 + \dots + x_ra_r$$

с целыми $x_1, \dots, x_r$, *причем* d *есть наименьшее натуральное число, представимое в этой форме.*

Все числа, представимые в этой форме, являются кратными числа d (*и обратно*).

Доказательство этой основной теоремы основывается на *делении с остатком*, которое также известно из элементарной арифметики.

Теорема о делении с остатком. *Если даны целое число a и натуральное число m, то существует одна и только одна пара целых чисел q, r, таких, что*

$$a = qm + r \quad c \quad 0 \leqslant r < m;$$

q называется частным, r — остатком от деления a на m.

Доказательство. Посредством исключения r можно доказываемые соотношения выразить в форме $qm \leqslant a < (q+1)m$ или $q \leqslant a/m < q+1$. Имеется одно и только одно целое число q, для которого выполняются эти соотношения, а именно, существующее, согласно принципу существования в § 1, п. 1, наибольшее целое число, $\leqslant a/m$.

Если представить себе числовую прямую разделенной целыми числами на интервалы длины 1 и при этом причислять к каждому интервалу его левый (соответствующий меньшему целому числу) конец, то q будет левым концом того интервала, в котором лежит рациональное число a/m. Так, определенное целое число q называется также *целой частью* рационального числа a/m и обозначается

$$q = \left[\frac{a}{m}\right].$$

В виде непосредственно получающегося дополнения к теореме о делении с остатком отметим еще следующий критерий делимости:

Дополнение. *$m \mid a$ тогда и только тогда, когда при делении с остатком числа a на m получается остаток $r = 0$.*

Так как из элементарной арифметики в нашем распоряжении имеется простой, основанный на цифровом представлении натуральных чисел, способ деления с остатком, то мы имеем тем самым систематический метод для решения в каждом конкретном случае вопроса о делимости.

8. Доказательство основной теоремы как основной теоремы об идеалах в области целостности Γ целых чисел. Чтобы получить доказательство основной теоремы об общем наибольшем делителе, рассмотрим вообще для заданного конечного множества целых чисел $a_1, \ldots, a_r$, которые не все равны 0, всевозможные выражения

$$x = x_1 a_1 + \ldots + x_r a_r$$

с целочисленными коэффициентами $x_1, \ldots, x_r$, или, коротко, *целочисленные линейные комбинации* чисел $a_1, \ldots, a_r$. Эти выра-

жения x образуют некоторое множество $\mathfrak{A}$ целых чисел со следующими тремя свойствами:

вместе с x и y к $\mathfrak{A}$ принадлежат также $x \pm y$, (1)

вместе с x к $\mathfrak{A}$ принадлежит также gx для каждого целого g, (2)

$\mathfrak{A}$ содержит по крайней мере одно число, отличное от 0. (3)

Именно, если

$$x = x_1 a_1 + \ldots + x_r a_r \text{ с целыми } x_1, \ \ldots, \ x_r,$$
$$y = y_1 a_1 + \ldots + y_r a_r \text{ с целыми } y_1, \ \ldots, \ y_r,$$

то

$$x \pm y = (x_1 \pm y_1)\, a_1 + \ldots + (x_r \pm y_r)\, a_r \text{ с целыми } x_1 \pm y_1, \ \ldots, \ x_r \pm y_r,$$
$$gx = (gx_1)\, a_1 + \ldots + (gx_r)\, a_r \text{ с целыми } gx_1, \ \ldots, \ gx_r,$$

и $\mathfrak{A}$ содержит, в частности, числа $a_1, \ \ldots, \ a_r$, из которых, по предположению, хотя бы одно отлично от 0. Из свойств (1), (2) следует, что вообще вместе с конечным множеством целых чисел $x^{(1)}, \ \ldots, \ x^{(s)}$ к $\mathfrak{A}$ принадлежит и каждая их целочисленная линейная комбинация

$$g_1 x^{(1)} + \ldots + g_s x^{(s)},$$

так что множество $\mathfrak{A}$ замкнуто относительно образования целочисленных линейных комбинаций.

Множество $\mathfrak{A}$ целых чисел, обладающее свойствами (1), (2), (3), другими словами, множество целых чисел, состоящее не только из 0, и замкнутое относительно образования целочисленных линейных комбинаций, называется *идеалом* в области целостности Γ. Мы сформулировали это важное определение в том виде, в каком оно дается при обобщении на другие области целостности вместо Γ; в частном же случае области целостности Γ можно, как легко видеть, требование (2) опустить, так как оно является формальным следствием из (1) (умножение в Γ можно свести к повторному сложению или вычитанию).

В частности, для каждого целого числа $a \neq 0$ множество всех кратных этого числа образует идеал в Γ (случай $r = 1$ в рассмотренном выше введении к понятию идеала). Такой идеал называется *главным идеалом, порожденным числом* a. Тот же самый главный идеал порождается также и ассоциированным числом $-a$; поэтому число a, порождающее главный идеал, можно всегда без ограничения общности предполагать натуральным. Идеал $\mathfrak{A}$, состоящий из целочисленных линейных комбинаций чисел $a_1, \ \ldots, \ a_r$, называется порожденным числами $a_1, \ \ldots, \ a_r$.

Основная теорема об общем наибольшем делителе будет доказана теперь как следствие из приводимой ниже основной теоремы об идеалах в Γ, которая утверждает, что в области целостности Γ общее понятие идеала совпадает по своему содержанию со специальным понятием главного идеала.

Основная теорема об идеалах в Γ. *Каждый идеал $\mathfrak{A}$ в Γ является главным и состоит, таким образом, в точности из кратных некоторого натурального числа d. Это число определяется идеалом $\mathfrak{A}$ однозначно, а именно, как наименьшее натуральное число d, содержащееся в $\mathfrak{A}$.*

Доказательство. Так как $\mathfrak{A}$, ввиду (3), состоит не только из 0 и, ввиду (2), вместе с каждым числом a содержит также и ассоциированное с ним число $-a$, то $\mathfrak{A}$ содержит, по крайней мере, одно натуральное число. Согласно принципу существования в § 1, п. 1, в $\mathfrak{A}$ существует, таким образом, наименьшее натуральное число d. Ввиду (2), $\mathfrak{A}$ содержит тогда все кратные числа d, т. е. порожденный числом d главный идеал. Остается показать, что и, обратно, каждое число a из $\mathfrak{A}$ является кратным числа d. Для этого разделим a на d с остатком:

$$a = qd + r, \qquad q,\ r - \text{целые},\ 0 \leqslant r < d.$$

Ввиду (1), (2), остаток $r = a - qd$ также лежит в $\mathfrak{A}$. Однако, вследствие минимального выбора числа d в $\mathfrak{A}$, это не приводит к противоречию лишь в том случае, если $r = 0$. Но тогда, действительно, $a = qd$, и, таким образом, a есть кратное числа d.

Если применить доказанную тем самым основную теорему об идеалах в Γ к идеалу $\mathfrak{A}$, порожденному числами $a_1, \ldots, a_r$, то мы получим, что наименьшая натуральная целочисленная линейная комбинация

$$d = x_1 a_1 + \ldots + x_r a_r$$

чисел $a_1, \ldots, a_r$ существует и обладает тем свойством, что каждая целочисленная линейная комбинация этих чисел делится на d (и, конечно, обратно, каждое целое число, делящееся на d, представляется в виде линейной комбинации чисел $a_1, \ldots, a_r$). В частности, сами числа $a_1, \ldots, a_r$ делятся на d, т. е. d есть общий делитель чисел $a_1, \ldots, a_r$. Вследствие того, что d представляется через $a_1, \ldots, a_r$ в виде целочисленной линейной комбинации, мы получаем, что и, наоборот, каждый общий делитель чисел $a_1, \ldots, a_r$ входит в d. Согласно I п. 2, d является поэтому общим наибольшим делителем чисел $a_1, \ldots, a_r$. Таким образом, доказательство основной теоремы об общем наибольшем делителе завершено.

Из этого доказательства получается еще следующая формулировка основной теоремы:

VI. *Идеал, порожденный числами* $a_1, \ldots, a_r$, *состоит в точности из кратных их общего наибольшего делителя* $d = (a_1, \ldots, a_r)$.

В частности, отсюда следует критерий взаимной простоты:

VII. *Целые числа* $a_1, \ldots, a_r$ *взаимно просты тогда и только тогда, когда существуют такие целые числа* $x_1, \ldots, x_r$ *что* $x_1a_1 + \ldots + x_ra_r = 1$.

То, что это условие достаточно, очевидно, так как если оно выполняется, то из $d \mid a_1, \ldots, d \mid a_r$ немедленно следует $d \mid 1$. Интерес заключается в том, что это условие необходимо, т. е. что из целых взаимно простых чисел всегда можно составить линейную комбинацию, равную 1, а это вытекает только из основной теоремы об общем наибольшем делителе.

9. Алгоритм Евклида. Задача о нахождении общего наибольшего делителя и общего наименьшего кратного конечного множества заданных целых чисел может быть сведена, как уже отмечалось в п. 4, к определению общего наибольшего делителя двух натуральных чисел a, b. Этот последний мы до сих пор умеем находить, лишь пользуясь его определением из разложений на простые множители

$$a \cong \prod_p p^{\alpha_p}, \quad b \cong \prod_p p^{\beta_p}$$

в виде

$$d = \prod_p p^{\min(\alpha_p, \beta_p)}.$$

Однако мы не имеем удобного алгоритма для нахождения разложения натурального числа на простые множители; делать же это посредством проб для сколько-нибудь больших чисел слишком долго и трудоемко. Поэтому возникает желание иметь простой алгоритм для определения $d = (a, b)$. Такой алгоритм, называемый *алгоритмом Евклида*, можно получить с помощью деления с остатком.

Положим для удобства $a = a_0$, $b = a_1$ и произведем следующую последовательность делений с остатком:

$$\begin{aligned}
a_0 &= q_1 a_1 + a_2 \quad \text{с} \quad 0 < a_2 < a_1 \\
a_1 &= q_2 a_2 + a_3 \quad \text{с} \quad 0 < a_3 < a_2 \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
a_{n-2} &= q_{n-1}a_{n-1} + a_n \quad \text{с} \quad 0 < a_n < a_{n-1},
\end{aligned}$$

где $q_1, q_2, \ldots$ — частные и $a_2, a_3, \ldots$ — остатки. Эта последовательность продолжается до тех пор, пока остатки еще > 0. Так как остатки убывают монотонно, то через конечное число шагов мы обязательно получим остаток 0. Пусть a_n — последний остаток, >0; тогда мы завершим нашу последовательность

равенством

$$a_{n-1} = q_n a_n + 0.$$

Конечно, может случиться, что уже на первом шагу получится остаток 0, и тогда $n = 1$ (именно, если $a_1 \mid a_0$, т. е. $b \mid a$). Для частных во всяком случае имеет место $q_2, q_3, \ldots, q_n > 0$, а если предположить еще, что $a_0 > a_1$, то и $q_1 > 0$ (иначе только $q_1 \geqslant 0$).

Если пройти последовательность этих равенств один раз снизу вверх и один раз сверху вниз, то можно убедиться в справедливости следующих фактов:

$$a_n \mid a_{n-1},\ a_n \mid a_{n-2},\ \ldots,\ a_n \mid a_1,\ a_n \mid a_0, \tag{1}$$

$$\text{из } x \mid a_0,\ x \mid a_1 \text{ следует } x \mid a_2,\ \ldots,\ x \mid a_n. \tag{2}$$

Поэтому, в соответствии с I п. 2,

$$a_n = (a_0,\ a_1),$$

т. е. искомый общий наибольший делитель $d = (a, b)$ равен последнему отличному от 0 остатку a_n.

Спускаясь по последовательности, мы получаем далее, что

$a_2, a_3, \ldots, a_n$ суть целочисленные линейные комбинации

$$\text{чисел } a_0,\ a_1, \tag{3}$$

что представляет собой новое доказательство представимости общего наибольшего делителя $d = (a, b)$ в форме

$$d = xa + yb$$

с целыми x, y, т. е. основной теоремы об общем наибольшем делителе в частном случае двух чисел, которое, в отличие от нашего доказательства в п. 8, одновременно дает эффективный метод для определения x и y. Для случая более чем двух чисел соответствующую задачу можно, как замечено в п. 4, решить многократным применением этого метода; так основная теорема получается и в общем случае.

Алгоритм Евклида для двух натуральных чисел a, b можно также записать в виде *разложения* положительного рационального числа $a/b = a_0/a_1$ *в непрерывную дробь*:

$$\frac{a_0}{a_1} = q_1 + \frac{a_2}{a_1} \quad \text{с} \quad 0 < \frac{a_2}{a_1} < 1, \text{ при этом } q_1 \geqslant 0 \text{ — целое},$$

$$\frac{a_1}{a_2} = q_2 + \frac{a_3}{a_2} \quad \text{с} \quad 0 < \frac{a_3}{a_2} < 1, \text{ при этом } q_2 > 0 \text{ — целое},$$

. . . . . .

$$\frac{a_{n-2}}{a_{n-1}} = q_{n-1} + \frac{a_n}{a_{n-1}} \text{ с } 0 < \frac{a_n}{a_{n-1}} < 1 \text{ при этом } q_{n-1} > 0 \text{ — целое},$$

$$\frac{a_{n-1}}{a_n} = q_n + 0 \qquad \text{при этом } q_n > 0 \text{ — целое},$$

или собирая все вместе:

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots}}$$

$$q_{n-1} = \frac{1}{q_n}.$$

Это разложение в непрерывную дробь, состоящее в последовательном выделении целой части и перевертывании остатка, очевидно, однозначно, причем даже для любого положительного вещественного числа $\alpha = \alpha_0$ вместо рационального $a/b = a_0/a_1$ соответственно с положительными вещественными остатками $\rho_i = 1/\alpha_i < 1$ вместо рациональных a_{i+1}/a_i $(i = 1, 2, \ldots)$. Мы можем поэтому установить следующий дополнительный результат:

Разложение каждого положительного рационального числа в непрерывную дробь обрывается.

Обратно, каждая конечная непрерывная дробь дает, очевидно, положительное рациональное число. Наш результат поэтому означает, что положительные рациональные числа характеризуются среди всех положительных вещественных чисел конечностью своего разложения в непрерывную дробь. К теории непрерывных дробей мы вернемся в § 16, п. 5.

10. Другое доказательство основной теоремы элементарной теории чисел. Алгоритм Евклида применяется в «Началах» (книга VII, теорема 2) к доказательству следующей теоремы, которая, если существование и однозначность разложения на простые множители предполагать известными, непосредственно очевидна (см. критерий простого делителя в п. 1):

VIII. *Если простое число p входит в произведение ab двух натуральных чисел, то p входит, по крайней мере, в один из сомножителей a, b:*

$$\text{из } p \mid ab \text{ следует } p \mid a \text{ или } p \mid b.$$

Доказательство (по Евклиду, без разложения на простые множители). Пусть $p \mid ab$, и предположим, например, что $p + a$, так что нужно доказать, что $p \mid b$. Будучи делителем простого числа p, общий наибольший делитель $(a, p) = 1$ или p. Однако так как он является делителем числа a, то, в силу предположения, $(a, p) \neq p$. Следовательно, $(a, p) = 1$. Согласно алгоритму Евклида, существуют поэтому целые x, y с

$$xa + yp = 1.$$

Отсюда умножением на b получается

$$x(ab) + (yb)p = b;$$

далее, на основании предположения $p \mid ab$, следует $p \mid b$, что и требовалось доказать.

Непосредственно за теоремой VIII Евклид помещает лемму из § 1, п. 3 о том, что каждое натуральное число $a > 1$ обладает хотя бы одним простым делителем p. В то время как из этой последней теоремы без труда следует существование разложения на простые множители (см. § 1, п. 4), из теоремы VIII легко получается новое доказательство его однозначности; действительно, если предположить существование равенства $p_1 \dots p_r = q_1 \dots q_s$ двух произведений простых чисел, то по теореме VIII можно последовательно сокращать по одному множителю слева и справа и доказать таким способом совпадение p_i с q_j (с точностью до порядка следования), а также и их количеств r, s. Это доказательство однозначности, опирающееся на деление с остатком и основную теорему об общем наибольшем делителе, давалось до сих пор почти во всех изложениях теории чисел. Наше доказательство однозначности, по Цермело, в § 1, п. 4 имеет то преимущество, что позволяет построить теорию делимости чисто мультипликативно и благодаря этому представить в правильном свете неожиданное с этой точки зрения аддитивное истолкование общего наибольшего делителя. Такой ход доказательства является поэтому более естественным, чем тот, который до сих пор обычно применялся. Тот факт, что при этом мы (как уже было отмечено в п. 7) не можем обойтись совсем без аддитивных образований, не должен нас удивлять; ведь в каком-нибудь месте мы должны использовать то, что объекты, с которыми мы оперируем, являются именно натуральными числами, а не просто элементами какой-нибудь абстрактной мультипликативно замкнутой области.

Весьма удивителен тот факт, что, хотя Евклид и имел в своем распоряжении все необходимое для доказательства существования и однозначности разложения на простые множители в виде непосредственно следующих друг за другом высказываний теоремы VIII и леммы из § 1, п. 3, однако основную теорему элементарной теории чисел он даже не формулировал. Надо полагать, что грекам эта теорема была известна. Поэтому непонятно, почему на нее делаются только намеки в виде обоих вышеупомянутых высказываний, а явно она не формулируется, несмотря на строго систематический, исчерпывающий характер изложения в сочинении Евклида.

§ 3. СОВЕРШЕННЫЕ ЧИСЛА, ПРОСТЫЕ ЧИСЛА МЕРСЕННА И ФЕРМА

1. Определение совершенных чисел. Мы прервем наше систематическое изложение, чтобы исследовать один вопрос элементарной теории чисел, лежащий в стороне от нашего основного пути.

В одной своей части этот вопрос может быть решен уже имеющимися в нашем распоряжении средствами, однако в другой части он приводит к таким глубоким проблемам, что решение их до сих пор не поддается усилиям математиков.

Обозначим сумму всех натуральных делителей d натурального числа n через $\sigma(n)$, что мы будем записывать так:

$$\sigma(n) = \sum_{d|n} d, \tag{1}$$

причем условимся вообще, что знак $\sum_{d|n}$ обозначает суммирование по всем натуральным делителям d числа n.

Натуральное число n называется *совершенным*, если

$$\sigma(n) = 2n.$$

Если $\sigma(n) < 2n$, то n называется *недостаточным*, а если $\sigma(n) > 2n$, то n называется *избыточным*; впрочем, оба эти последние понятия будут нас интересовать здесь в меньшей мере.

Определение совершенных чисел имеется уже в «Началах» Евклида (книга IX, теорема 36). Оно станет понятнее, если принять во внимание, что греки не причисляли само число n к его делителям и потому рассматривали сумму $\sigma_0(n) = \sum_{d||n} d$ только собственных делителей числа n. В этом случае совершенные числа характеризуются свойством $\sigma_0(n) = n$, причем $n = 1$ должно быть исключено, так как для $n = 1$ соотношение $\sigma(n) = \sigma_0(n) + n$ становится неверным. Совершенные числа упоминаются и Платоном (в «Государстве»). Греки видели в них, как и в правильных многогранниках, некую совершенную гармонию, так сказать, отражение гармонии вселенной, и вследствие их влияния этим числам на протяжении всей древности и раннего средневековья придавали мистический смысл.

Существование совершенных, недостаточных и избыточных чисел показывают следующие примеры:

$$n = 6,\ 8,\ 12$$

с

$$\sigma_0(n) = 6,\ 7,\ 16.$$

Как легко убедиться, 6 есть наименьшее совершенное число; следующее будет 28. Возникает вопрос о перечне всех совершенных чисел. К этому вопросу мы и переходим.

2. Мультипликативная формула для суммы делителей. Если $n = p^\nu$ есть степень простого числа, то

$$\sigma(n) = 1 + p + \ldots + p^{\nu-1} + p^\nu = \frac{p^\nu - 1}{p-1} + p^\nu < 2p^\nu.$$

Поэтому все степени простых чисел недостаточны. Каждое совершенное число должно содержать по меньшей мере два различных простых делителя.

Можно и в общем случае вывести для суммы делителей $\sigma(n)$ из ее аддитивного определения (1) мультипликативное представление, соответствующее разложению n на простые множители. Пусть

$$n = p_1^{\nu_1} \dots p_r^{\nu_r}$$

есть это разложение в смысле I § 1 (каноническое разложение). Тогда, согласно критерию делимости в § 2, п. 1, натуральные делители d числа n задаются разложениями

$$d = p_1^{\delta_1} \dots p_r^{\delta_r},$$

где $\delta_1, \dots, \delta_r$ пробегают все системы целых чисел, таких, что

$$0 \leqslant \delta_1 \leqslant \nu_1, \dots, 0 \leqslant \delta_r \leqslant \nu_r.$$

Элементарным подсчетом получаем

$$\sigma(n) = \sum_{\delta_1, \dots, \delta_r = 0}^{\nu_1, \dots, \nu_r} p_1^{\delta_1} \dots p_r^{\delta_r} = \sum_{\delta_1 = 0}^{\nu_1} p_1^{\delta_1} \dots \sum_{\delta_r = 0}^{\nu_r} p_r^{\delta_r} =$$

$$= \frac{p_1^{\nu_1+1} - 1}{p_1 - 1} \dots \frac{p_r^{\nu_r+1} - 1}{p_r - 1}.$$

Если использовать разложение числа n на простые множители в форме I′ § 1:

$$n = \prod_p p^{\nu_p},$$

то эта мультипликативная формула для $\sigma(n)$ запишется в виде:

$$\sigma(n) = \prod_p \frac{p^{\nu_p+1} - 1}{p - 1} = \prod_p \sigma(p^{\nu_p}), \tag{2}$$

причем, так же, как в самом разложении числа n на простые множители, только конечное множество простых p, таких, что $\nu_p > 0$, т. е. являющихся простыми делителями числа n, дают множители, отличные от 1.

Согласно критерию взаимной простоты в § 2, п. 5, из мультипликативной формулы (2) получается следующее общее правило:

$$\sigma(n_1 n_2) = \sigma(n_1)\,\sigma(n_2), \text{ если } (n_1, n_2) = 1. \tag{3}$$

3. Достаточное условие для четных совершенных чисел: теорема Евклида. У Евклида имеется следующий замечательный результат о четных совершенных числах:

Теорема Евклида. *Если n имеет вид*

$$n = 2^{\nu}(2^{\nu+1} - 1) = 2^{\nu}p$$

и при этом

$$p = 2^{\nu+1} - 1 - \text{простое},$$

то n совершенно.

Доказательство. Если n имеет такой вид, то действительно, согласно (2),

$$\sigma(n) = (2^{\nu+1} - 1)\ (p+1) = p \cdot 2^{\nu+1} = 2n.$$

Среди показателей $\nu \leqslant 6$ важнейшее условие этой теоремы, а именно, что $2^{\nu+1} - 1 = p$ есть простое число, выполняется для $\nu = 1, 2, 4, 6$ с $p = 3, 7, 31, 127$. Так получаются четыре четных совершенных числа

$$n = 6,\ 28,\ 496,\ 8128,$$

которые были известны уже грекам. Что касается бóльших значений ν, то об этом мы будем говорить позднее.

4. Необходимое условие для четных совершенных чисел: теорема Эйлера. В связи с теоремой Евклида ряд математиков на протяжении столетий занимался вопросом о совершенных числах, но хотя и было получено много отдельных результатов, однако большей частью они носили характер чисто численных примеров. Первый крупный успех общего характера, который до сих пор остается и единственным, был достигнут Эйлером лишь примерно через 2000 лет после Евклида.

Теорема Эйлера. *Числа, имеющие вид, данный в теореме Евклида, являются единственными четными совершенными числами.*

Доказательство. Пусть мы имеем какое-нибудь четное число

$$n = 2^{\nu}u,$$

однозначно разложенное на степень 2 с показателем $\nu \geqslant 1$ и нечетное число u. Тогда, согласно (3),

$$\sigma(n) = (2^{\nu+1} - 1)\,\sigma(u).$$

Предположим теперь, что n совершенно, т. е. $\sigma(n) = 2n$. Тогда имеет место равенство

$$2^{\nu+1}u = (2^{\nu+1} - 1)\,\sigma(u),$$

или при другой записи

$$\frac{u}{\sigma(u)} = \frac{2^{\nu+1} - 1}{2^{\nu+1}}.$$

Справа в последнем равенстве стоит несократимая дробь. Поэтому, по теореме о представлении несократимой дробью (см. § 2, п. 6), левая дробь получается из нее умножением числителя и знаменателя на некоторое натуральное число t, т. е. одновременно выполняются равенства

$$u = (2^{\nu+1} - 1)\, t, \tag{а}$$

$$\sigma(u) = 2^{\nu+1} t. \tag{б}$$

Так как u имеет вид (а), то в сумму делителей $\sigma(u) = \sum_{d|u} d$ заведомо входят в качестве слагаемых d два различных делителя: t и $(2^{\nu+1} - 1)\, t > t$. Но их сумма уже дает значение $2^{\nu+1} t$, равное, согласно (б), сумме $\sigma(u)$ всех делителей. Поэтому u не имеет никаких других натуральных делителей, кроме

$$t \text{ и } (2^{\nu+1} - 1)\, t = u.$$

Но только простые числа p, согласно определению в § 1, п. 3, имеют точно два различных натуральных делителя, именно,

$$1 \text{ и } p.$$

Следовательно, $u = p$ есть простое число, и одновременно

$$t = 1 \text{ и } 2^{\nu+1} - 1 = p.$$

Поэтому n действительно имеет евклидовский вид.

5. Простые числа Мерсенна. Благодаря теоремам Евклида и Эйлера, мы получили неявную характеристику совокупности всех четных совершенных чисел, однако, чтобы получить из этого явный перечень этих чисел, нужно еще ответить на следующий вопрос:

Для каких натуральных показателей ν *число* $p = 2^{\nu+1} - 1$ *будет простым*?

Условие, необходимое для этого, и тем самым ограничение для рассматриваемых показателей ν дать легко. Для этого целесообразно положить $\nu + 1 = \pi$.

Тогда имеет место:

Число $p = 2^{\pi} - 1$ *может быть простым только тогда, когда показатель* π *простой.*

Доказательство. Если $\pi = \alpha\beta$ есть разложение числа π на два натуральных множителя α, β и притом нетривиальное, т. е. $1 < \alpha < \pi$, то

$$2^{\pi} - 1 = (2^{\alpha} - 1)\ (1 + 2^{\alpha} + \ldots + 2^{\alpha(\beta-1)})$$

будет разложением на два натуральных множителя числа $2^\pi - 1$ и притом также нетривиальным, так как $1 < 2^\alpha - 1 < 2^\pi - 1$.

Согласно этому результату, евклидовская форма четных совершенных чисел приводится к виду:

$$n = 2^{\pi-1}p, \text{ где } \left\{\begin{matrix}\pi - \text{простое число} \\ p = 2^\pi - 1 - \text{простое число}\end{matrix}\right\},$$

и остается вопрос:

Для каких простых π *число* $p = 2^\pi - 1$ *будет простым*?

Простые числа p такого вида называются *простыми числами Мерсенна* по имени французского математика Мерсенна, который переписывался о них с Ферма. Для первых четырех простых чисел

$$\pi = 2,\ 3,\ 5,\ 7$$

получаются четыре уже названных в п. 3 простых числа

$$p = 3,\ 7,\ 31,\ 127,$$

которые приводят к указанным там четырем четным совершенным числам классической греческой математики. Однако неверно то, что каждое простое π приводит к простому $p = 2^\pi - 1$, как полагали многие математики, и среди них такие крупные, как Лейбниц. Уже следующее простое число $\pi = 11$ приводит к составному числу $2^{11} - 1 = 2047 = 23 \cdot 89$. Для $\pi = 13$ снова получается простое число

$$p = 2^{13} - 1 = 8191,$$

и тем самым пятое четное совершенное число

$$n = 33550336.$$

Обрывается ли последовательность простых чисел Мерсенна или их существует бесконечно много, неизвестно до сих пор. Известно только, что среди следующих простых чисел $\pi \leqslant 257$ числа

$$\pi = 17,\ 19,\ 31,\ 61,\ 89,\ 107,\ 127$$

приводят к простым p, а остальные — к составным, за исключением, быть может, числа $\pi = 193$, которое еще не исследовано.

6. Нечетные совершенные числа. В то время как вопрос о четных совершенных числах принципиально решен теоремами Евклида и Эйлера и остается только вопрос о простых числах Мерсенна, до сих пор не известно ни одного нечетного совершенного числа и не доказано, что их не существует. Прямое рас-

смотрение требования $\sigma(n) = 2n$ в мультипликативной форме

$$\prod_p \frac{p^{\nu_p+1}-1}{p-1} = 2\prod_p p^{\nu_p}$$

как уравнения относительно неизвестной целочисленной системы показателей $\nu_p \geqslant 0$ с условием, что лишь конечное множество $\nu_p > 0$ приводит в случае нечетного n (когда, следовательно, $\nu_2 = 0$) к такому сложному сплетению требований относительно делимости чисел и их величин, что до сих пор были получены только отдельные, носящие более или менее частный характер, необходимые условия того, чтобы нечетное число могло быть совершенным. Так, например, доказано, что нечетное совершенное число n должно было бы иметь по меньшей мере шесть различных простых делителей, что может существовать самое большее конечное множество нечетных совершенных чисел с заданным количеством r различных простых делителей, причем наименьший простой делитель должен быть $\leqslant r$, а наибольший — $\geqslant 2\max(\nu_p+1)$.

Мы не будем вдаваться в доказательства этих утверждений (см. Канольд [1, 2, 3]), которые большей частью очень сложны и не имеют отношения к задачам настоящей книги. Мы привели их здесь только для того, чтобы дать понятие о том, что известно сейчас о нечетных совершенных числах. Докажем только, что невозможен случай $r = 2$, или, точнее, что:

Каждое нечетное натуральное число точно с двумя различными простыми делителями недостаточно.

Доказательство. Если n имеет каноническое разложение

$$n = p_1^{\nu_1} p_2^{\nu_2} \text{ с } p_1 \geqslant 3,\ p_2 \geqslant 5,$$

то, согласно (2),

$$\sigma(n) = \frac{p_1^{\nu_1+1}-1}{p_1-1} \cdot \frac{p_2^{\nu_2+1}-1}{p_2-1} < \frac{p_1^{\nu_1+1}}{p_1-1} \cdot \frac{p_2^{\nu_2+1}}{p_2-1},$$

и потому, действительно,

$$\frac{\sigma(n)}{n} < \frac{p_1}{p_1-1} \cdot \frac{p_2}{p_2-1} \leqslant \frac{3}{2} \cdot \frac{5}{4} = \frac{15}{8} < 2.$$

Наконец, в противоположность этому установим:

Существуют такие натуральные числа n, что отношение $\sigma(n)/n$ принимает сколь угодно большие значения.

Доказательство. Если мы перейдем от делителей d числа n к дополнительным делителям $d' = n/d$ и потом эти последние снова будем обозначать через d, то получим

$$\frac{\sigma(n)}{n} = \sum_{d \mid n} \frac{d}{n} = \sum_{d \mid n} \frac{1}{d}.$$

Если теперь специально положить $n = N! = 1 \cdot 2 \ldots N$, то среди делителей будут все числа $d = 1, \ldots, N$. Тогда

$$\frac{\sigma(n)}{n} \geqslant 1 + \frac{1}{2} + \ldots + \frac{1}{N}.$$

Так как стоящая справа частичная сумма гармонического ряда может быть, вследствие его расходимости, при соответствующем выборе N сделана сколь угодно большой, то наше утверждение доказано.

7. Простые числа Ферма. В заключение рассмотрим один вопрос, который не имеет прямого отношения к совершенным числам, но благодаря своей формальной аналогии с вопросом о простых числах Мерсенна близок к этому.

Для каких натуральных показателей n число $p = 2^n + 1$ будет простым?

Снова легко дать условие, необходимое для этого:

Число $p = 2^n + 1$ может быть простым только тогда, когда $n = 2^\nu$, т. е. показатель n есть степень 2.

Доказательство. Если $n = ut$ — разложение (безразлично, тривиальное или нет) числа n с нечетным множителем $u > 1$, то

$$2^n + 1 = (2^m + 1)(1 - 2^m + 2^{2m} - \ldots + 2^{(u-1)m})$$

будет разложением числа $2^n + 1$ на два натуральных множителя и притом нетривиальным, так как $1 < 2^m + 1 < 2^n + 1$.

Этот результат сводит наш вопрос к следующему:

Для каких целочисленных показателей $\nu \geqslant 0$ число $p = 2^{2^\nu} + 1$ будет простым?

Простые числа такого вида называются простыми числами Ферма. Они играют роль в теории деления круга. Как доказал Гаусс, правильный p-угольник для простого $p > 2$ можно построить циркулем и линейкой тогда и только тогда, когда p есть простое число Ферма. Ферма предполагал, подобно тому, как Лейбниц о простых числах Мерсенна, что для каждого целого $\nu \geqslant 0$ действительно получается простое p. Однако в то время как для

$$\nu = 0, 1, 2, 3, 4$$

получаются простые числа

$$p = 3, 5, 17, 257, 65537,$$

уже для $\nu = 5$ число $2^{2^5} + 1 = 2^{32} + 1$ делится на 641, как мы покажем в § 4, п. 2 в виде упражнения в действиях над сравнениями.

Относительно простых чисел Ферма тоже не известно, обрывается ли их последовательность, или их существует бесконечно

много. Во всяком случае, больше ни одного простого числа Ферма не найдено и проверено, что показатели

$$\nu = 6,\ 7,\ 8,\ 9,\ 11,\ 12,\ 18,\ 23,\ 36,\ 38,\ 73$$

приводят к составным числам.

8. Перечень вопросов, остающихся нерешенными. Перечислим еще раз вопросы, до сих пор остающиеся нерешенными:

I. *Существуют ли нечетные совершенные числа?*

II. *Существует ли бесконечно много простых чисел Мерсенна* $p = 2^n - 1$?

III. *Существует ли бесконечно много простых чисел Ферма* $p = 2^{2^\nu} + 1$?

Для теории чисел вообще характерно, и в этом заключается своеобразная прелесть этой математической дисциплины, что в ней существует ряд проблем, которые, подобно этим трем, хотя и формулируются простейшими средствами, вследствие чего могут быть сделаны понятными и даже заманчивыми и для нематематика, однако решение их до сих пор сопротивляется всем усилиям математиков. Во многих случаях, однако, эти усилия не были напрасными, так как благодаря ним возникли большие красивые и плодотворные теории, которые, хотя также не дают возможности решить исходный вопрос, но тем не менее часто обогащают науку результатами большого значения.

Так, из вопроса о простых числах Ферма возникла так называемая *малая теорема Ферма*, с которой мы познакомимся в § 4, п. 5, а из знаменитой, до сих пор не доказанной *великой теоремы Ферма*, а именно, что уравнение

$$x^n + y^n + z^n = 0$$

ни при каком натуральном $n > 1$ не имеет решения в целых, отличных от 0 числах x, y, z, возникла арифметическая теория алгебраических чисел, основами которой мы займемся в четвертой главе.

Что касается изложенного в этом параграфе вопроса о совершенных числах, то он не привел к подобным важным результатам, а занимал всегда в теории чисел скромное, изолированное от наиболее важных проблем место.

§ 4. СРАВНИМОСТЬ, КЛАССЫ ВЫЧЕТОВ

1. Определение сравнимости и классов вычетов. Пусть m — заданное натуральное число. Рассмотрим все целые числа a в их отношении к m, для чего разделим их на m с остатком:

$$a = qm + r; \quad q, r \text{ — целые}, \quad 0 \leqslant r < m.$$

Остаток r ограничен при этом m значениями $0, 1, \ldots, m-1$, каждое из которых действительно встречается (например, для $a = 0, 1, \ldots, m-1$). Естественно считать числа a, b, дающие при делении на m один и тот же остаток r, более родственными между собой в отношении к m, чем такие, для которых остатки получаются различные.

В математике введение удачного, четкого обозначения или удобного для применения исчисления часто имеет не только чисто формальное значение, но и решающим образом способствует или даже впервые делает возможным дальнейшее развитие по существу; это относится, например, к введенному Лейбницем обозначению для детерминанта или к его дифференциальному и интегральному исчислениям. Подобно этому, в теории чисел чрезвычайно счастливым и многозначащим оказалось то обстоятельство, что для равенства остатков от деления на заданное число m Гаусс ввел обозначение, подобное обычному знаку равенства, и стал изучать употребление получающегося при этом исчисления. Определение Гаусса гласит:

Определение. *Два целых числа a, b называются сравнимыми по* $\bmod m$ (*читается: по модулю m*), *если при делении на m они дают одинаковые остатки. Это обозначается так:*

$$a \equiv b \bmod m.$$

Натуральное число m называется модулем сравнения.

Определенная таким образом сравнимость, как и положенное в основу ее равенство (остатков), обладает свойствами

рефлексивности ($a \equiv a \bmod m$),

симметричности (из $a \equiv b \bmod m$ следует $b \equiv a \bmod m$),

транзитивности (из $a \equiv b$, $b \equiv c \bmod m$ следует $a \equiv c \bmod m$)

и является, таким образом, так называемым отношением эквивалентности. Поэтому оно приводит к разбиению всех целых чисел на классы чисел, сравнимых между собой по $\bmod m$. Эти классы называются *классами вычетов по* $\bmod m$. В соответствии с m возможными остатками существует m классов вычетов по $\bmod m$. Класс вычетов, соответствующий остатку r, состоит из всех чисел вида $a = qm + r$, где r постоянно, а q пробегает все целые числа. На числовой прямой эти числа образуют неограниченную в обе стороны последовательность точек, находящихся одна от другой на одном и том же расстоянии m. Красивой иллюстрацией классов вычетов по mod 12 является клавиатура (неограниченная в обе стороны); классы вычетов соответствуют при этом отличающимся друг от друга лишь на целые октавы тонам одинакового названия.

При практическом решении вопроса о сравнимости чисел чаще всего применяется следующий критерий, который также может быть положен в основу в качестве определения (при этом только симметричность и транзитивность потребуют несложной проверки):

I. $a \equiv b \bmod m$ *тогда и только тогда, когда* $m \mid a-b$.

Доказательство. Пусть при делении с остатком чисел a, b на m получается:

$$a = qm + r; \qquad q - \text{целое}, \quad 0 \leqslant r < m,$$
$$b = q'm + r'; \quad q' - \text{целое}, \quad 0 \leqslant r' < m,$$

и пусть для определенности $r \geqslant r'$. Тогда после вычитания получается как раз деление с остатком числа $a-b$ на m:

$$a - b = (q - q')\, m + (r - r'); \quad q - q' - \text{целое}; \quad 0 \leqslant r - r' < m.$$

Теперь, с одной стороны, согласно определению, $a \equiv b \bmod m$ равносильно с $r = r'$. С другой стороны, согласно дополнению в § 2, п. 7, также и $m \mid a-b$ равносильно с $r - r' = 0$. Вместе это и дает наше утверждение.

Согласно I, каждый класс вычетов по $\bmod m$ может быть описан не только соответствующим остатком r, но также и любым принадлежащим ему числом a_0; он состоит в точности из всех чисел вида $a = qm + a_0$, где q пробегает все целые числа. Класс вычетов по $\bmod m$, порожденный числом a_0, т. е. совокупность чисел $a \equiv a_0 \bmod m$, удобно обозначать просто через $a_0 \bmod m$ (без знака сравнимости $\equiv$).

Система из m целых чисел, содержащая по одному представителю из каждого класса вычетов по $\bmod m$, называется *полной системой вычетов* по $\bmod m$. При этом система всех возможных остатков от деления чисел на m

$$r = 0, 1, \ldots, m-1$$

называется *наименьшей системой вычетов по* $\bmod m$ (точнее, *наименьшей неотрицательной системой вычетов по* $\bmod m$), а система

$$S = \begin{cases} 0, \pm 1, \ldots, \pm \dfrac{m-1}{2} & \text{при нечетном } m \\ 0, \pm 1, \ldots, \pm \left(\dfrac{m}{2} - 1\right), \dfrac{m}{2} & \text{при четном } m \end{cases}$$

называется *абсолютно наименьшей системой вычетов по* $\bmod m$. Последняя действительно является полной системой вычетов по $\bmod m$, так как состоит из m следующих друг за другом чисел; она характеризуется неравенством $|s| \leqslant m/2$ для абсолютной величины и дополнительным условием, что в случае четного m из двух сравнимых между собой по $\bmod m$ чисел $\pm m/2$ берется положительное.

2. Кольцо классов вычетов. Удобство записи $a \equiv b \bmod m$ для отношения делимости $m \mid a-b$ состоит в том, что с такими

сравнениями можно оперировать совершенно так же, как с обычными равенствами, во всяком случае в пределах первых трех элементарных операций. Именно, имеют место следующие правила:

Из

$$a \equiv a' \bmod m,$$
$$b \equiv b' \bmod m$$

следует

$$a \pm b \equiv a' \pm b' \bmod m,$$
$$ab \equiv a'b' \bmod m.$$

Действительно, если

$$a = a' + gm,$$
$$b = b' + hm,$$

то

$$a \pm b = (a' \pm b') + (g \pm h)\, m,$$
$$ab = a'b' + (gb' + ha' + ghm)\, m,$$

и при этом вместе с a, b, a', b' и g, h будут целыми также и множители при m.

Эти правила можно высказать и так. Если из двух классов вычетов $a \bmod m$ и $b \bmod m$ произвольным образом выбирать по одному числу и их между собой складывать, соответственно вычитать или перемножать, то каждый раз будут получаться числа из одного и того же класса, а именно, из $a+b \bmod m$, соответственно $a-b \bmod m$ или $ab \bmod m$. Таким образом, каждым двум классам $a \bmod m$ и $b \bmod m$, независимо от выбора в них представителей a, b, можно сопоставить классы, являющиеся их суммой, разностью и произведением, т. е. в области классов вычетов по $\bmod m$ однозначным образом определяются первые три элементарные операции. Так как определение этих операций сводится к соответствующим операциям над числами из классов вычетов, то при этом сохраняются законы этих операций, именно коммутативность и ассоциативность сложения:

$$a+b=b+a, \quad (a+b)+c=a+(b+c),$$

возможность и однозначность вычитания:

$a+x=b$ всегда и однозначно разрешимо относительно x,

коммутативность и ассоциативность умножения:

$$ab=ba, \quad (ab)\,c=a\,(bc),$$

дистрибутивность умножения по отношению к сложению:

$$(a+b)\,c=ac+bc.$$

Абстрактная область, в которой определены операции сложения и умножения и имеют место перечисленные законы, называется кольцом. Мы можем теперь сказать:

II. *Относительно определенных выше операций классы вычетов по* $\bmod m$ *образуют кольцо, которое так и называется кольцом классов вычетов по* $\bmod m$.

Кольцо классов вычетов есть абстрактная область с определенными в ней операциями, состоящая лишь из конечного множества, а именно, точно из m элементов. Его нулевым элементом является класс вычетов $0 \bmod m$, а в качестве единичного элемента оно обладает классом вычетов $1 \bmod m$. Существование единичного элемента является условием, которое должно выполняться для всякого кольца, для того чтобы оно было даже областью целостности. Однако второе свойство области целостности, а именно, что произведение двух отличных от нуля элементов снова должно быть отлично от нуля, для кольца классов вычетов выполняется не всегда. Именно, если существует нетривиальное разложение $m = m_1 m_2$, то хотя оба класса вычетов $m_1 \bmod m$ и $m_2 \bmod m$, ввиду того что $m_1 \not\equiv 0 \bmod m$ и $m_2 \not\equiv 0 \bmod m$, отличны от нулевого класса, однако их произведение, вследствие того что $m_1 m_2 \equiv 0 \bmod m$, дает нулевой класс. Поэтому кольцо классов вычетов не всегда является областью целостности.

Численный пример. В качестве небольшого примера на применение сравнений дадим обещанное в § 3, п. 7 доказательство того, что число

$$2^{2^5} + 1 = 2^{32} + 1 \text{ делится на } 641.$$

Для этого мы рассмотрим два аддитивных разложения

$$641 = 640 + 1 = 5 \cdot 2^7 + 1,$$
$$641 = 625 + 16 = 5^4 + 2^4.$$

Из первого разложения мы имеем

$$5 \cdot 2^7 \equiv -1 \bmod 641.$$

Возводя в четвертую степень, получаем отсюда

$$5^4 \cdot 2^{28} \equiv 1 \bmod 641.$$

Согласно второму разложению, при этом имеет место

$$5^4 \equiv -2^4 \bmod 641.$$

Тем самым мы получаем

$$-2^{32} \equiv 1 \bmod 641$$

и, таким образом, действительно,

$$2^{32} + 1 \equiv 0 \bmod 641.$$

Подобным же образом, хотя и не так просто, доказывается существование собственных делителей и в других случаях, указанных в § 3, п. 5, 7. В случае простых чисел Ферма наибольшее исследованное число $2^{2^{73}}+1$ имеет свыше 10^{21} цифр. При ширине цифр в 1 *мм* оно будет более чем в $6\cdot 10^9$ раз длиннее экватора и потребует для своего написания около $2\cdot 10^{14}$ лет, если на написание каждой цифры тратить полсекунды. Эта поистине невообразимая величина не является, однако, непреодолимым препятствием для метода сравнений. Морхеду [1, 2] удалось доказать, что это число делится на $5\cdot 2^{75}+1$.

3. Деление в кольце классов вычетов. Теперь мы выясним оставленный до этого в стороне вопрос о делении в кольце классов вычетов по $\bmod m$, т. е. о разрешимости сравнения

$$ax \equiv b \bmod m$$

с заданными классами вычетов a, $b \bmod m$ посредством класса вычетов $x \bmod m$ и о совокупности его решений, если они существуют. Эти решения всегда являются, конечно, целыми классами вычетов по $\bmod m$, так как, согласно правилам из п. 2, вместе с числом x решением является и каждое число $x \equiv x_0 \bmod m$.

Для подготовки этого исследования мы прежде всего установим:

III. *Все числа a из одного класса вычетов по* $\bmod m$ *имеют с m один и тот же общий наибольший делитель* $d=(a, m)$.

Доказательство. Пусть $a \equiv a' \bmod m$, т. е. $a=a'+gm$ с целым g, и пусть $d=(a, m)$, $d'=(a', m)$. Из определения общего наибольшего делителя в I п. 2 § 2 наше утверждение вытекает тогда следующим образом:

ввиду $d \mid a$, $d \mid m$ имеет место также $d \mid a'$, $d \mid m$ и потому $d \mid d'$,

ввиду $d' \mid a'$, $d' \mid m$ имеет место также $d' \mid a$, $d' \mid m$ и потому $d' \mid d$.

Вместе это дает $d=d'$, что и требовалось доказать.

Таким образом, общий наибольший делитель $d=(a, m)$ зависит только от класса вычетов $a \bmod m$, а не от выбора представителя a в этом классе. Если, в частности, $(a, m)=1$, то класс $a \bmod m$ называется классом вычетов, взаимно простым с модулем, потому что он сплошь состоит из чисел, взаимно простых с m.

Теперь мы докажем первый факт относительно деления в кольце классов вычетов по $\bmod m$:

IV. *Деление на класс вычетов $a \bmod m$, взаимно простой с модулем, всегда возможно и однозначно, т. е. сравнение*

$$ax \equiv b \bmod m \text{ с } (a, m)=1$$

для каждого целого b имеет в качестве решения один и только один класс вычетов $x \bmod m$.

Доказательство. а) Если $(a, m) = 1$, то по основной теореме об общем наибольшем делителе (см. § 2, п. 7) уравнение

$$ax + my = b$$

при любом целом b разрешимо в целых x, y. Согласно I, это означает разрешимость сравнения $ax \equiv b \bmod m$ для каждого целого b.

б) Если решением этого сравнения наряду с $x \bmod m$ является также $x' \bmod m$, то из правил действий со сравнениями следует $a(x - x') \equiv 0 \bmod m$, и, таким образом, $m \mid a(x - x')$. Так как $(a, m) = 1$, то отсюда, согласно IV, п. 5, § 2, следует далее $m \mid x - x'$, т. е. $x \equiv x' \bmod m$. Таким образом, оба решения совпадают.

После того как мы доказали, что деление на класс вычетов, взаимно простой с модулем, всегда возможно и однозначно, покажем далее, что деление на класс вычетов, не взаимно простой с модулем, не всегда возможно, а если возможно, то не однозначно. При этом мы по образцу теории систем линейных уравнений исследуем, каково в общем случае необходимое и достаточное условие разрешимости сравнения $ax \equiv b \bmod m$ и как получить совокупность всех решений.

Если сравнение

$$ax \equiv b \bmod m, \text{ где } (a, m) = d$$

имеет решение, то, согласно III, необходимо должно иметь место $d \mid b$; таким образом, в случае $d \neq 1$ сравнение действительно разрешимо не для всех целых b.

Пусть теперь необходимое условие разрешимости $d \mid b$ выполнено. Тогда, согласно V п. 5 § 2, мы имеем

$$a = da_0, \quad b = db_0, \quad m = dm_0$$

с целыми a_0, b_0, натуральным m_0 и $(a_0, m_0) = 1$. Если мы, в соответствии с I, напишем исследуемое сравнение в виде $ax = b + gm$ с целым g, то увидим, что оно тогда равносильно с $a_0 x = b_0 + gm_0$, т. е. со сравнением

$$a_0 x \equiv b_0 \bmod m_0, \text{ где } (a_0, m_0) = 1.$$

Согласно IV, это последнее сравнение имеет своим решением точно один класс вычетов $x \equiv x_0 \bmod m_0$. Из представления на числовой прямой сразу видно, что каждый класс вычетов $x_0 \bmod m_0$ распадается точно на d классов вычетов по $\bmod m$, а именно, на классы

$$x \equiv x_0, \quad x_0 + m_0, \quad \ldots, \quad x_0 + (d-1)\, m_0 \bmod m.$$

Они и образуют совокупность решений исследуемого сравнения; таким образом, в случае $d \neq 1$ это сравнение, действительно, если разрешимо, то не однозначно.

Резюмируем то, что мы доказали:

V. *Для того, чтобы сравнение*

$$ax \equiv b \bmod m$$

было разрешимо, необходимо и достаточно, чтобы $d = (a, m)$ входило *также и в* b, *т. е. чтобы имело место*

$$b \equiv 0 \bmod d.$$

Если это выполнено, то сравнение имеет своими решениями точно d *классов вычетов* $x \bmod m$, *которые составляют один класс вычетов* $x \bmod m/d$.

Если применить это к специальному случаю $b \equiv 0 \bmod m$, когда заведомо выполнено необходимое условие разрешимости и существует решение $x \equiv 0 \bmod m$, то мы получим часто применяемое дополнение:

V′. *Сравнение* $ax \equiv 0 \bmod m$ *равносильно сравнению*

$$x \equiv 0 \bmod m/(a, m).$$

4. Группа классов вычетов, взаимно простых с модулем. Предыдущие теоремы показывают, какое значение для деления в кольце классов вычетов по $\bmod m$ имеют классы вычетов, взаимно простые с модулем. Поэтому мы рассмотрим их еще подробнее.

Сначала докажем:

VI. *Произведение и частное классов вычетов по* $\bmod m$, *взаимно простых с модулем, снова являются классами вычетов, взаимно простыми с модулем.*

Доказательство. Если $(a, m) = 1$, $(b, m) = 1$ и $ax \equiv b \bmod m$, то, с одной стороны, согласно критерию взаимной простоты в § 2, п. 5, также $(ab, m) = 1$, а с другой стороны, согласно III, $(ax, m) = 1$ и потому также $(x, m) = 1$.

Поэтому классы вычетов по $\bmod m$, взаимно простые с модулем, образуют совокупность, для всех элементов которой определена коммутативная, ассоциативная и однозначно обратимая операция умножения, т. е. мультипликативную *абелеву группу*, называемую *группой классов вычетов по* $\bmod m$, *взаимно простых с модулем.*

Если, в частности, $m = p$ есть *простое число*, то фигурирующее в IV условие $(a, p) = 1$ равносильно с $p \nmid a$, или, другими словами, с $a \not\equiv 0 \bmod p$; тогда при делении в кольце классов вычетов по $\bmod p$ нужно исключить из числа делителей только нулевой класс. Таким образом, при простом p в кольце классов

вычетов по $\bmod p$ выполняются оба дополнительных условия, названных выше после II, необходимых для того, чтобы оно было областью целостности. Так как, кроме того, деление на элементы, отличные от нуля, не только всегда однозначно, но и всегда возможно, то мы имеем даже область, замкнутую по отношению ко всем четырем элементарным операциям (за исключением деления на нуль), т. е. имеем *поле*. Если, однако, m *не является простым*, то либо $m = 1$, и тогда существует один-единственный класс вычетов (одновременно являющийся нулевым и единичным), либо m обладает нетривиальным разложением $m = m_1 m_2$, и тогда, как было показано в п. 2 в дополнение к II, кольцо классов вычетов по $\bmod m$ не является даже областью целостности, а подавно и полем.

Итак, мы установили:

VII. *Кольцо классов вычетов по* $\bmod m$ *тогда и только тогда является областью целостности, когда* $m = p$ *есть простое число; в последнем случае оно является даже полем.*

5. Малая теорема Ферма. Так как мы установили, что классы вычетов по $\bmod m$, взаимно простые с модулем, образуют мультипликативную абелеву группу, и притом состоящую из конечного множества элементов, то к ней можно применять известные из алгебры общие теоремы о конечных абелевых группах и получать из них теоретико-числовые результаты.

Если $\mathfrak{A}$ — мультипликативная абелева группа из n элементов (n называется тогда *порядком* $\mathfrak{A}$), то для каждого элемента A из $\mathfrak{A}$ выполняется соотношение

$$A^n = E, \tag{1}$$

где E — единичный элемент группы $\mathfrak{A}$.

В самом деле, если $X_1, \ldots, X_n$ — n различных элементов из $\mathfrak{A}$, то, вследствие однозначности деления в $\mathfrak{A}$, n произведений $AX_1, \ldots, AX_n$ все различны между собой, и потому они снова представляют собой n различных элементов $X_1, \ldots, X_n$ группы $\mathfrak{A}$, только, вообще говоря, в другом порядке.

Поэтому для их произведения мы имеем

$$A^n X_1 \ldots X_n = X_1 \ldots X_n,$$

а отсюда, ввиду однозначности деления в $\mathfrak{A}$, вытекает доказываемое соотношение (1).

Порядок группы классов вычетов по $\bmod m$, взаимно простых с модулем, обозначается через $\varphi(m)$. Это есть функция, определенная в области натуральных чисел m, или так называемая *теоретико-числовая функция*, у которой значение $\varphi(m)$ само есть натуральное число, а именно, количество классов вычетов

по $\bmod m$, взаимно простых с модулем. Она называется *функцией Эйлера*.

Если мы применим общее теоретико-групповое соотношение (1) к группе классов вычетов по $\bmod m$, взаимно простых с модулем, то получим теоретико-числовой результат:

Малая теорема Ферма. *Для каждого класса вычетов $a \bmod m$ взаимного простого с модулем, выполняется сравнение*

$$a^{\varphi(m)} \equiv 1 \bmod m.$$

Пусть снова $\mathfrak{A}$ есть некоторая мультипликативная абелева группа порядка n и A есть элемент из $\mathfrak{A}$.

Рассмотрим степени A^x с показателями x из области целостности Γ целых чисел. Так как $\mathfrak{A}$ конечна, то среди этого формально бесконечного множества степеней в действительности будет лишь конечное множество различных. Чтобы точнее выяснить положение вещей, рассмотрим специально те показатели y, для которых $A^y = E$. Эти y образуют идеал в Γ; действительно, три свойства (1), (2), (3) из § 2, п. 8 для них выполнены:

вместе с $A^{y_1} = E$, $A^{y_2} = E$ также и $A^{y_1+y_2} = A^{y_1} \cdot A^{y_2} = E$,

вместе с $A^y = E$ также и $A^{xy} = (A^y)^x = E$ для каждого целого x, в частности, $A^n = E$, согласно (1).

Поэтому, согласно основной теореме об идеалах в Γ (см. § 2, п. 8), все показатели y, о которых идет речь, являются кратными наименьшего положительного показателя k, для которого $A^k = E$; *другими словами*, имеет место:

$$A^y = E \text{ тогда и только тогда, когда } y \equiv 0 \bmod k. \qquad (2)$$

Отсюда сразу же следует более общее утверждение:

$$A^x = A^{x'} \text{ тогда и только тогда, когда } x \equiv x' \bmod k. \qquad (3).$$

Эти высказывания дают исчерпывающий ответ на вопрос о равенствах между степенями A^x. Согласно (3), различным степеням A^x взаимно однозначно соответствуют различные классы вычетов $x \bmod k$. Их представителями являются, например, k степеней

$$A^0 = E, \quad A^1 = A, \ \ldots, \ A^{k-1}. \qquad (4)$$

При этом k однозначно определено как такое наименьшее натуральное число, для которого

$$A^k = E. \qquad (5)$$

Это число k называется *порядком* элемента A. Из (1) следует еще, согласно (2), что этот порядок k элемента A является делителем порядка n группы $\mathfrak{A}$.

Степени A^x с целыми показателями x сами по себе образуют мультипликативную абелеву группу порядка k, которая содержится в группе $\mathfrak{A}$ в качестве подгруппы. Так как последовательность (4) ее различных элементов в силу соотношения (5) циклически повторяется, то такая группа называется *циклической*, и говорят, что она порождается элементом A. Ее элементы взаимно однозначно соответствуют по (3) классам вычетов по $\bmod k$. При этом умножению в $\mathfrak{A}$ соответствует сложение в кольце классов вычетов по $\bmod k$. Последние образуют аддитивную абелеву группу порядка k. Установленное нами положение вещей выражают еще и так: циклическая группа, порожденная элементом A, в силу взаимно однозначного соответствия $A^x \longleftrightarrow x \bmod k$ *изоморфна* аддитивной группе классов вычетов по $\bmod k$.

Если предыдущие общие теоретико-групповые факты применить к группе классов вычетов по $\bmod m$, взаимно простых с модулем, то получится теоретико-числовой результат:

VIII. *Для каждого класса вычетов* $a \bmod m$, *взаимно простого с модулем, существует наименьший натуральный показатель* k, *такой, что*

$$a^k \equiv 1 \bmod m.$$

Для неотрицательных x, x' *имеет место*:

$$a^x \equiv a^{x'} \bmod m \text{ тогда и только тогда, когда } x \equiv x' \bmod k,$$

и $k \mid \varphi(m)$.

Также называют k *показателем, к которому принадлежит класс вычетов* $a \bmod m$; это обозначение относится к тому времени, когда теоретико-групповые понятия еще не были известны. На языке последних k есть *порядок класса вычетов* $a \bmod m$ в группе классов вычетов по $\bmod m$, взаимно простых с модулем.

Относительно формулировки VIII заметим еще следующее. В то время как в общем теоретико-групповом высказывании (3) показатели x, x' могут быть любыми целыми, т. е. также и отрицательными числами, причем понятие степени для отрицательных показателей определяется обычным образом, в соответствующем высказывании VIII мы должны пока ограничиться только неотрицательными показателями x, x', так как понятие сравнения определено нами пока только для целых чисел. Потом мы устраним это ограничение посредством целесообразного расширения понятия сравнимости на дробные числа (со знаменателем, взаимно простым с модулем). Пока, в случае когда не выполнено условие $x, x' \geqslant 0$, мы будем считать, что сравнение, о котором идет речь, означает, согласно его теоретико-групповому происхождению, равенство классов вычетов $(a \bmod m)^x = (a \bmod m)^{x'}$.

Заметим, наконец, что в силу сравнения, фигурирующего в формулировке малой теоремы Ферма или также соответствующего сравнения в VIII, решение $x \bmod m$ линейного сравнения

$$ax \equiv b \bmod m \quad \text{с} \quad (a, m) = 1,$$

которое, согласно IV, существует и определено однозначно, может быть выражено в виде формулы, а именно, в виде

$$x \equiv a^{\varphi(m)-1} b \bmod m \text{ или также } x \equiv a^{k-1} b \bmod m.$$

Так как $k \mid \varphi(m)$ и, как мы увидим далее, вообще говоря, даже $k \| \varphi(m)$, то вторая формула в общем случае требует при ее применении меньшего количества вычислений, чем первая. Впрочем, для вычисления степеней $a^n \bmod m$, конечно, не нужно вычислять сами степени a^n, а посредством последовательного умножения на a и приведения каждый раз к наименьшему (или даже абсолютно наименьшему) вычету по $\bmod m$ ограничиться действиями с числами, не превосходящими $m \mid a \mid$ (или даже $m \mid a \mid /2$).

Пример. Степени класса вычетов $7 \bmod 11$ получаются по схеме:

$$\begin{array}{l|l} 7^1 \equiv -4 & 7^6 \equiv (-1)\cdot(-4) \equiv 4 \\ 7^2 \equiv (-4)\cdot(-4) \equiv 16 \equiv 5 & 7^7 \equiv (-1)\cdot 5 \equiv -5 \\ 7^3 \equiv 5\cdot(-4) \equiv -20 \equiv 2 & 7^8 \equiv (-1)\cdot 2 \equiv -2 \\ 7^4 \equiv 2\cdot(-4) \equiv -8 \equiv 3 & 7^9 \equiv (-1)\cdot 3 \equiv -3 \\ 7^5 \equiv 3\cdot(-4) \equiv -12 \equiv -1 & 7^{10} \equiv (-1)(-1) \equiv 1 \end{array}$$

Таким образом, $k = 10$, и линейное сравнение

$$7x \equiv b \bmod 11$$

для каждого целого b имеет решение

$$x \equiv 7^9 b \equiv -3b \bmod 11.$$

Сравним этот способ со следующим методом решения, который вытекает из нашего доказательства существования в п. 3 (доказательство утверждения IV). С помощью алгоритма Евклида определяют для a, m целочисленное решение x_0, y_0 уравнения $ax_0 + my_0 = 1$ (см. § 2, п. 9) и тем самым решение специального сравнения $ax_0 \equiv 1 \bmod m$ и отсюда получают $x \equiv x_0 b \bmod m$ в качестве решения общего сравнения $ax \equiv b \bmod m$.

Пример. Слева от черты дается алгоритм Евклида для 7, 11, причем для отличия остатков от частных остатки подчеркнуты снизу:

$$\begin{array}{r|l} \underline{11} = 1\cdot\underline{7} + \underline{4} & \underline{4} = (-1)\cdot\underline{7} + 1\cdot\underline{11} \\ \underline{7} = 1\cdot\underline{4} + \underline{3} & \underline{3} = (-1)\cdot\underline{4} + 1\cdot\underline{7} = 2\cdot\underline{7} + (-1)\cdot\underline{11} \\ \underline{4} = 1\cdot\underline{3} + \underline{1} & \underline{1} = (-1)\cdot\underline{3} + 1\cdot\underline{4} = -3\cdot\underline{7} + 2\cdot\underline{11}. \\ 3 = 3\cdot\underline{1} + 0 & \end{array}$$

Справа от черты вычислены получающиеся при спуске по последовательности равенств слева представления всех остатков в виде целочисленных линейных комбинаций от двух первых. Согласно последнему представлению, $x_0 = -3$ и потому $x \equiv -3b \bmod 11$ есть искомое решение.

6. Формула сложения для функции Эйлера. Возникает задача *определить количество* $\varphi(m)$ *классов вычетов по* $\bmod m$, *взаимно простых с модулем.*

Для этого представим себе все классы вычетов по $\bmod m$, имеющие с m один и тот же общий наибольший делитель d, объединенными в комплекс $\mathfrak{K}_d$ (d пробегает все натуральные делители числа m) и выразим количество m всех классов вычетов по $\bmod m$ как сумму количеств классов в отдельных комплексах $\mathfrak{K}_d$. Классы вычетов из $\mathfrak{K}_d$, т. е. классы вычетов $a \bmod m$ с $(a, m) = d$ однозначно соответствуют, в силу редукции $a = da_0$, $m = dm_0$, классам вычетов $a_0 \bmod m_0$ с $(a_0, m_0) = 1$, т. е. классам вычетов по $\bmod m_0$, взаимно простым с модулем; этот вывод нам уже известен из доказательства V, п. 3. Поэтому комплекс $\mathfrak{K}_d$ состоит точно из $\varphi(m_0) = \varphi(m/d)$ классов вычетов. Так получается формула

$$\sum_{d \mid m} \varphi(m/d) = m \quad \text{или также} \quad \sum_{d \mid m} \varphi(d) = m$$

(последнее посредством перехода к суммированию по дополнительным делителям). Вопрос теперь сводится к тому, чтобы из этого функционального уравнения для функции Эйлера определить эту функцию. Это можно сделать с помощью одного формального соотношения общего характера, которым мы сначала и займемся.

7. Формула обращения Мёбиуса. Мы определим теоретико-числовую функцию $\mu(m)$ со значениями $0, \pm 1$ следующим образом. Если каноническое разложение числа m есть

$$m = p_1^{\mu_1} \dots p_r^{\mu_r} \qquad (\mu_i \geqslant 1 \text{ для } i = 1, \dots r),$$

то пусть

$$\mu(m) = \begin{cases} (-1)^r, & \text{если все показатели } \mu_i = 1, \\ 0, & \text{если по крайней мере один показатель } \mu_i > 1. \end{cases}$$

Для $m = 1$, т. е. $r = 0$, целесообразно при этом считать

$$\mu(1) = 1.$$

Так определенная функция $\mu(m)$ называется *функцией Мёбиуса.*

Числа m, у которых все показатели $\mu_i = 1$, называются также *свободными от квадратов*, потому что они не делятся на квадрат

никакого натурального числа, отличного от 1. Тогда определение функции Мёбиуса может быть высказано также и так:

$$\mu(m)=\left\{\begin{array}{l}(-1)^r, \text{ если } m \text{ свободно от квадратов и имеет} \\ \qquad \text{точно } r \text{ различных простых делителей,} \\ 0, \text{ если } m \text{ не свободно от квадратов.}\end{array}\right\}$$

Аналогично установленному в § 3, п. 2 свойству (3) суммы делителей $\sigma(n)$, имеет место

$$\mu(m_1 m_2)=\mu(m_1)\,\mu(m_2), \text{ если } (m_1,\ m_2)=1. \tag{1}$$

Мы введем далее еще тривиальную теоретико-числовую функцию

$$\varepsilon(m)=\left\{\begin{array}{l}1 \text{ для } m=1 \\ 0 \text{ для } m\neq 1\end{array}\right\}$$

и докажем равенство:

$$\sum_{d\mid m}\mu(d)=\varepsilon(m). \tag{2}$$

Доказательство. Для $m=1$ утверждение выполняется. Пусть $m\neq 1$, так что в написанном выше каноническом разложении $r\geqslant 1$. Как и в § 3, п. 2, натуральные делители d числа m задаются в каноническом разложении в виде

$$d=p_1^{\delta_1}\ \ldots\ p_r^{\delta_r},$$

где $\delta_1,\ \ldots,\ \delta_r$ пробегают все системы целых чисел, таких, что

$$0\leqslant\delta_1\leqslant\mu_1,\ \ \ldots,\ 0\leqslant\delta_r\leqslant\mu_r,$$

и при этом, согласно (1),

$$\mu(d)=\mu(p_1^{\delta_1})\ \ldots\ \mu(p_r^{\delta_r}).$$

Аналогично тому, как в § 3, п. 2, отсюда получается

$$\sum_{d\mid m}\mu(d)=\sum_{\delta_1,\ \ldots,\ \delta_r=0}^{\mu_1,\ \ldots,\ \mu_r}\mu(p_1^{\delta_1})\ \ldots\ \mu(p_r^{\delta_r})=\sum_{\delta_1=0}^{\mu_1}\mu(p_1^{\delta_1})\ \ldots\ \sum_{\delta_r=0}^{\mu_r}\mu(p_r^{\delta_r})=$$

$$=[1+\mu(p_1)+\ \ldots\ +\mu(p_1^{\mu_1})]\ \ldots\ [1+\mu(p_r)+\ \ldots\ +\mu(p_r^{\mu_r})]=$$

$$=(1-1)\ \ldots\ (1-1)=0,$$

и таким образом утверждение верно и для $m\neq 1$.

С помощью доказанного тем самым равенства (2) мы выведем теперь следующее формальное соотношение, являющееся основным применением функции Мёбиуса:

Формула обращения Мёбиуса. *Если две теоретико-числовые функции $f(m)$ и $g(m)$ связаны одним из двух функциональных уравнений*

$$\sum_{d|m} f(d) = g(m), \tag{А}$$

$$\sum_{d|m} \mu\left(\frac{m}{d}\right) g(d) = f(m), \tag{Б}$$

то они связаны и вторым из этих соотношений.

Доказательство. а) Предположим, что выполнено соотношение (А). Рассмотрим тогда левую часть равенства (Б), заменив в ней $g(d)$ их выражениями из (А):

$$\sum_{d|m} \mu\left(\frac{m}{d}\right) g(d) = \sum_{d|m} \mu\left(\frac{m}{d}\right) \sum_{t|d} f(t) = \sum_{t|d|m} \mu\left(\frac{m}{d}\right) f(t).$$

Эта двойная сумма, в которой первое суммирование производится по d, может быть записана и так, что первое суммирование будет производиться по t, где t должно пробегать все натуральные делители числа m, а d каждый раз те натуральные делители числа m, для которых $t|d$. А это последнее условие равносильно (согласно определению!) обратному условию $m/d|m/t$ для дополнительных делителей. Поэтому посредством перехода при суммировании по d к дополнительным делителям $d' = m/d$ мы получаем далее:

$$\sum_{t|d|m} \mu\left(\frac{m}{d}\right) f(t) = \sum_{t|m} f(t) \sum_{d' \left| \frac{m}{t} \right.} \mu(d') = \sum_{t|m} f(t)\, \varepsilon\left(\frac{m}{t}\right) = f(m),$$

т. е. вместе с предыдущим получается соотношение (Б).

б) Предположим, что существует соотношение (Б). Рассмотрим тогда левую часть равенства (А), заменив в ней $f(d)$ их выражениями из (Б):

$$\sum_{d|m} f(d) \sum_{d|m} \sum_{t|d} \mu\left(\frac{d}{t}\right) g(t) = \sum_{t|d|m} \mu\left(\frac{d}{t}\right) g(t).$$

Посредством преобразований, аналогичных тем, которые производились выше, мы получаем далее:

$$\sum_{t|d|m} \mu\left(\frac{d}{t}\right) g(t) = \sum_{t|m} g(t) \sum_{d' \left| \frac{m}{t} \right.} \mu\left(\frac{m}{d't}\right) = \sum_{t|m} g(t) \sum_{d'' \left| \frac{m}{t} \right.} \mu(d'') =$$

$$= \sum_{t|m} g(t)\, \varepsilon\left(\frac{m}{t}\right) = g(m),$$

т. е. выполняется также и соотношение (А).

8. Формула умножения для функции Эйлера. Из выведенной в п. 6 формулы

$$\sum_{d \mid m} \varphi\left(\frac{m}{d}\right) = m \text{ или также } \sum_{d \mid m} \varphi(d) = m$$

следует с помощью формулы обращения Мёбиуса

$$\sum_{d \mid m} \mu\left(\frac{m}{d}\right) d = \varphi(m) \text{ или также } \sum_{d \mid m} \mu(d) \frac{m}{d} = \varphi(m).$$

Тем самым принципиально получено явное выражение для функции Эйлера $\varphi(m)$.

Полученную формулу можно еще преобразовать так, что в ней не будет больше фигурировать функция Мёбиуса. А именно, как и в п. 7 при доказательстве равенства (2), мы имеем (в тех же обозначениях):

$$\frac{\varphi(m)}{m} = \sum_{d \mid m} \frac{\mu(d)}{d} = \sum_{\delta_1, \ldots, \delta_r = 0}^{\mu_1, \ldots, \mu_r} \frac{\mu(p_1^{\delta_1})}{p_1^{\delta_1}} \cdots \frac{\mu(p_r^{\delta_r})}{p_r^{\delta_r}} =$$

$$= \sum_{\delta_1=0}^{\mu_1} \frac{\mu(p_1^{\delta_1})}{p_1^{\delta_1}} \cdots \sum_{\delta_r=1}^{\mu_r} \frac{\mu(p_r^{\delta_r})}{p_r^{\delta_r}} = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Если применить обычное краткое обозначение $\prod_{p \mid m}$ для произведения, распространенного на различные простые делители p числа m, то этот результат можно коротко записать в виде:

$$\frac{\varphi(m)}{m} = \prod_{p \mid m} \left(1 - \frac{1}{p}\right). \tag{1}$$

Отсюда для специального случая степени простого числа p^μ с $\mu \geqslant 1$ следует

$$\frac{\varphi(p^\mu)}{p^\mu} = 1 - \frac{1}{p}$$

или также

$$\varphi(p^\mu) = p^\mu - p^{\mu-1} = p^{\mu-1}(p-1),$$

и, в частности, для простых чисел p

$$\frac{\varphi(p)}{p} = 1 - \frac{1}{p}$$

или также

$$\varphi(p) = p - 1.$$

Таким образом, из общей формулы (1) следуют функциональные равенства:

$$\varphi(m) = \prod_p \varphi(p^{\mu_p}), \text{ если } m = \prod_p p^{\mu_p}, \tag{2}$$

$$\frac{\varphi(m)}{m} = \prod_{p \mid m} \frac{\varphi(p)}{p}. \tag{3}$$

Функциональное равенство (2) формально аналогично полученному в § 3, п. 2 функциональному равенству (2) для суммы делителей $\sigma(n)$. Подобно тому, как там из него следует (3), так и здесь получается общее функциональное равенство:

$$\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2), \text{ если } (m_1, m_2) = 1. \tag{4}$$

То, что $\varphi(p) = p - 1$, ясно и непосредственно; действительно, если p — простое число, то условие взаимной простоты $(a, p) = 1$ равносильно с $p \nmid a$, т. е. с $a \not\equiv 0 \bmod p$, а это условие выполняется точно для $p - 1$ классов из p классов вычетов $a \bmod p$. Точно так же можно непосредственно убедиться и в правильности формулы $\varphi(p^\mu) = p^\mu - p^{\mu-1}$; в самом деле, $(a, p^\mu) = 1$ снова равносильно с $a \not\equiv 0 \bmod p$, и так как имеется точно $p^{\mu-1}$ классов вычетов $a \bmod p^\mu$ с $a \equiv 0 \bmod p$ (представителями которых являются $p, 2p, \ldots, p^{\mu-1}\cdot p$), то условие $a \not\equiv 0 \bmod p$ выполняется точно для $p^\mu - p^{\mu-1}$ классов из всех p^μ классов вычетов $a \bmod p^\mu$.

Посредством обобщения этих рассуждений можно вывести также полученную выше с помощью функции Мёбиуса общую формулу

$$\varphi(m) = \sum_{d \mid m} \mu(d) \frac{m}{d} = m - \sum_{p \mid m} \frac{m}{p} + \sum_{\substack{p \mid m,\ p' \mid m \\ p \neq p'}} \frac{m}{pp'} - \ldots$$

Из m чисел $a = 1, 2, \ldots, m$ мы в первую очередь вычеркнем те, которые делятся на простой делитель p числа m; проделаем это для каждого p, причем каждый раз таких чисел будет точно m/p. При этом, однако, числа a, делящиеся на два различных простых делителя p, p', будут вычеркнуты дважды, и потому на втором шагу мы должны их снова добавить; для каждой пары p, p' их будет точно m/pp'. Потом, на третьем шагу, мы должны снова отбросить числа a, делящиеся на три различных простых делителя p, p', p''; таких чисел для каждой тройки p, p', p'' будет $m/pp'p''$; и т. д. То, что при этом каждое a, взаимно простое с m, в общем оказывается сосчитанным точно один раз, а каждое a, не взаимно простое с m, — ни разу и потому получается искомое количество $\varphi(m)$, доказывается следующим образом. Если $(a, m) = 1$, то a учитывается только в нулевом слагаемом m нашей формулы; т. е. только один раз. А если $(a, m) \neq 1$

и a делится точно на $\rho \geqslant 1$ простых делителей $p, p', \ldots, p^{(\rho-1)}$, то a учитывается в нулевом, первом, втором, ..., ρ-м слагаемых нашей формулы и притом с кратностями, равными числам сочетаний $1, \binom{\rho}{1}, \binom{\rho}{2}, \ldots, \binom{\rho}{\rho}$, и с чередующимися знаками, и, таким образом, с общей кратностью

$$1-\binom{\rho}{1}+\binom{\rho}{2}-\ldots+(-1)^{\rho}\binom{\rho}{\rho}=(1-1)^{\rho}=0.$$

В связи с этими вычислениями мы дадим в заключение *теоретико-вероятностное истолкование* функционального равенства (3). Для этого мы рассмотрим в множестве натуральных чисел $a=1, \ldots, m$, или, более обще, $a=1, \ldots, hm$ со сколь угодно большим натуральным h, следующие события:

E_m: a взаимно просто с m,
E_p: a взаимно просто с p,
$\overline{E}_p$: a не взаимно просто с p, или, что то же самое, a делится на p.

Вероятности этих событий, определяемые каждый раз как отношение числа «благоприятных» к числу всех возможных случаев, суть

$$w(E_m)=\frac{\varphi(m)}{m},\quad w(E_p)=\frac{\varphi(p)}{p}=\frac{p-1}{p},\quad w(\overline{E}_p)=\frac{1}{p}.$$

Таким образом, функциональное равенство (3) означает, что имеет место формула умножения

$$w(E_m)=\prod_{p\mid m} w(E_p)=\prod_{p\mid m}(1-w(\overline{E}_p)). \tag{3'}$$

Но событие E_m заключается как раз в одновременном наступлении событий E_p для всех простых делителей p числа m, или, другими словами, в одновременном ненаступлении противоположных событий $\overline{E}_p$. Таким образом, функциональное равенство (3) в истолковании (3') соответствует закону умножения вероятностей при одновременном наступлении событий. В теории вероятностей этот закон умножения связан с предположением, что рассматриваемые события *независимы* друг от друга. При этом точное определение понятия независимости является задачей, создающей значительные трудности в обосновании теории вероятностей. В данном случае мы можем во всяком случае утверждать, наоборот, что теоретико-числовые события E_p для каждого конечного множества различных простых чисел p независимы друг от друга, потому что для их одновременного наступления выполняется формула умножения (3'). Также незави-

симы друг от друга и противоположные события $\overline{E}_p$, что видно из соответствующего истолкования формулы $1/m = \prod_{p \mid m} 1/p$ для свободного от квадратов числа m.

9. Системы сравнений, разложение кольца классов вычетов в прямую сумму. Далее встает вопрос о том, возможно ли дать прямое, свободное от формального понятия функции Мёбиуса доказательство также и для функционального равенства (4) для функции Эйлера $\varphi(m)$. Тогда мы могли бы, применяя (4) в специальном виде (2) и используя для определения $\varphi(p^\mu)$ уже произведенные в п. 8 простые вычисления, получить новое доказательство явной формулы (1).

Этот путь действительно возможен и основывается он на очень важном методе — который, и помимо этой цели, имеет большое значение для теории чисел — а именно, на теории систем сравнений.

Рассмотрим какое-нибудь совершенно произвольно выбранное разложение

$$m = m_1 \dots m_r$$

заданного натурального числа m в произведение некоторого количества $r \geqslant 1$ попарно взаимно простых натуральных чисел $m_1, \dots, m_r$. В частности, за них могут быть взяты составляющие m степени $p_1^{\mu_1}, \dots, p_r^{\mu_r}$ различных простых чисел $p_1, \dots, p_r$. Поставим себе задачу ответить на вопрос, разрешима ли система сравнений вида

$$x \equiv a_1 \bmod m_1, \dots, x \equiv a_r \bmod m_r$$

с какими-нибудь заданными целыми $a_1, \dots, a_r$, и если разрешима, то какова совокупность ее решений.

Вместе с числом x решением этой системы сравнений является также каждое число $x' \equiv x \bmod m$. Обратно, если x, x' — два решения, то $x' - x$ делится на $m_1, \dots, m_r$; так как, однако, $m_1, \dots, m_r$ предполагаются попарно взаимно простыми, и потому, согласно § 2, п. 5, $[m_1, \dots, m_r] = m_1 \dots m_r = m$, то $x' - x$ делится тогда и на m, т. е. $x' \equiv x \bmod m$. Таким образом, если решения x нашей системы вообще существуют, то они образуют точно один класс вычетов по $\bmod m$.

Покажем теперь, что при любых $a_1, \dots, a_r$ действительно существует решение $x \bmod m$. Для этого рассмотрим дополнительные делители

$$M_1 = \frac{m}{m_1}, \dots, M_r = \frac{m}{m_r}.$$

Согласно III, п. 5, § 2, они взаимно просты. Таким образом, согласно VII, п. 8, § 2, существуют такие целые $g_1, \dots, g_r$, что

выполняется соотношение

$$g_1M_1+\ldots+g_rM_r=1,$$

которое может быть записано и без $M_1, \ldots, M_r$ в виде

$$\frac{g_1}{m_1}+\ldots+\frac{g_r}{m_r}=1.$$

Положим

$$e_1=g_1M_1, \ldots, e_r=g_rM_r.$$

Тогда

$$e_1+\ldots+e_r=1$$

и

$$e_1\equiv 0 \bmod M_1, \ldots, e_r\equiv 0 \bmod M_r.$$

Заменяя в этих сравнениях каждое $M_1, \ldots, M_r$ через входящие в них множители $m_1, \ldots, m_r$, причем в каждое M_i не входит только множитель m_i с тем же индексом, а по отношению к этим последним применяя предыдущее равенство, мы получим систему сравнений

$$\begin{aligned}
&e_1\equiv 1 \bmod m_1,\ e_1\equiv 0 \bmod m_2, \ldots, e_1\equiv 0 \bmod m_r,\\
&e_2\equiv 0 \bmod m_1,\ e_2\equiv 1 \bmod m_2, \ldots, e_2\equiv 0 \bmod m_r,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&e_r\equiv 0 \bmod m_1,\ e_r\equiv 0 \bmod m_2, \ldots, e_r\equiv 1 \bmod m_r,
\end{aligned}$$

у которых в правых частях по главной диагонали стоят 1, а всюду вне главной диагонали 0. Умножая строки этой системы сравнений соответственно на $a_1, \ldots, a_r$ и складывая, мы получим, что число

$$a=a_1e_1+\ldots+a_re_r$$

обладает свойствами

$$a\equiv a_1 \bmod m_1, \ldots, a\equiv a_r \bmod m_r,$$

так что класс вычетов $x\equiv a \bmod m$ является, таким образом, решением исходной системы сравнений.

Тем самым нами доказана

Основная теорема о системах сравнений. *Если $m=m_1\ldots m_r$ с попарно взаимно простыми $m_1, \ldots, m_r$, то система сравнений*

$$x\equiv a_1 \bmod m_1, \ldots, x\equiv a_r \bmod m_r$$

при любых заданных целых $a_1, \ldots, a_r$ имеет своим решением точно один класс вычетов $x\equiv a \bmod m$.

Сверх того, наше доказательство дает также способ для определения этого решения $a \bmod m$. Для этого нужно только

определить числа $e_1, \ldots, e_r$, не зависящие от $a_1, \ldots, a_r$ и потому пригодные для любых $a_1, \ldots, a_r$. Эти числа получаются из чисел $g_1, \ldots, g_r$, которые, в свою очередь, согласно § 2, п. 9, принципиально могут быть определены посредством повторного применения алгоритма Евклида. То, что числа $g_1, \ldots, g_r$ и $e_1, \ldots, e_r$ определяются при этом не однозначно, несущественно. По основной теореме, *классы вычетов* $e_1 \bmod m, \ldots, e_r \bmod m$, являясь решениями рассматриваемой системы сравнений для r специальных систем значений $(a_1, \ldots, a_r) = (1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)$, во всяком случае определяются однозначно, а нам важны только они. *Решение* $a \bmod m$ *определяется* тогда сравнением

$$a \equiv a_1 e_1 + \ldots + a_r e_r \bmod m.$$

При этом оно опять-таки зависит не от *чисел* $a_1, \ldots, a_r$, а только от входящих в систему сравнений *классов вычетов* $a_1 \bmod m_1, \ldots, a_r \bmod m_r$.

Однозначно определенный таким образом класс вычетов $a \bmod m$ называется *составленным* из классов вычетов $a_1 \bmod m_1, \ldots, a_r \bmod m_r$. При этом *компоненты* $a_1 \bmod m_1, \ldots, a_r \bmod m_r$ в свою очередь однозначно определяются заданием $a \bmod m$, потому что

$$a \equiv a_1 \bmod m_1, \ \ldots, \ a \equiv a_r \bmod m_r.$$

Если компоненты будут пробегать все $m_1 \ldots m_r$ систем классов вычетов $a_1 \bmod m_1, \ldots, a_r \bmod m_r$, то в качестве составного класса встретятся все m классов вычетов $a \bmod m$. Последнее можно заключить или исходя из системы компонент $a \bmod m_1, \ldots, a \bmod m_r$ (с равными между собой представителями $a_1 = \ldots = a_r = a$), или из доказанной перед этим однозначности в обе стороны в связи с равенством $m_1 \ldots m_r = m$. Тем самым мы получаем взаимно однозначное соответствие между всеми классами вычетов $a \bmod m$, с одной стороны, и всеми системами классов вычетов $a_1 \bmod m_1, \ldots, a_r \bmod m_r$, с другой. Кроме того, из определения

$$a \equiv a_1 \bmod m_1, \ \ldots, \ a \equiv a_r \bmod m_r$$

этого соответствия получается, что при этом выполнению первых трех элементарных операций над классами вычетов по $\bmod m$ соответствует выполнение этих операций над компонентами по

$$\bmod m_1, \ \ldots, \ \bmod m_r,$$

т. е. что классы вычетов $a \pm b$, $ab \bmod m$ имеют соответственно компоненты $a_i \pm b_i$, $a_i b_i \bmod m_i$ $(i = 1, \ldots, r)$. На языке алгебры такое положение вещей можно высказать так:

IX. *Кольцо классов вычетов по* $\bmod m$ *есть прямая сумма колец классов вычетов по* $\bmod m_1, \ldots, \bmod m_r$.

В соответствии с формулой

$$a \equiv a_1 e_1 + \ldots + a_r e_r \bmod m,$$

дающей выражение составного класса через компоненты, говорят, что это разложение в прямую сумму порождается *ортогональными идемпотентами* $e_1 \bmod m, \ldots, e_r \bmod m$. Это последнее название указывает на существование соотношений

$$e_i e_j \equiv \left\{ \begin{array}{ll} e_i \bmod m & \text{для } j = i \\ 0 \bmod m & \text{для } j \neq i \end{array} \right\}, \quad (i, j = 1, \ldots, r),$$

в силу которых каждый отдельный класс вычетов $e_i \bmod m$ равен своему квадрату (идемпотентен), а потому равен всем своим натуральным степеням, а два различных класса вычетов $e_i \bmod m$, $e_j \bmod m$ имеют своим произведением нулевой класс (ортогональны друг другу). Выполнение этих соотношений ортогональности проще всего проверить покомпонентно; ведь компоненты классов вычетов $e_1 \bmod m, \ldots, e_r \bmod m$ образуют строки единичной матрицы r-го порядка, а для этих строк соотношения ортогональности выполняются почленно.

Согласно IX, операции в кольце классов вычетов по $\bmod m$ сводятся к операциям в кольцах классов вычетов по $\bmod m_1, \ldots, \bmod m_r$. Посмотрим далее, как ведут себя при этом классы вычетов, взаимно простые с модулем. Из $a \equiv a_i \bmod m_i$ следует, в силу III, п. 3, что $(a, m_i) = (a_i, m_i)$ $(i = 1, \ldots, r)$. Если теперь $(a, m) = 1$, то и подавно все $(a, m_i) = 1$, а потому и все $(a_i, m_i) = 1$. Обратно, если все $(a_i, m_i) = 1$, то тогда, согласно критерию взаимной простоты (см. § 2, п. 5), также и $(a, m) = 1$. Таким образом:

X. *Класс вычетов* $a \bmod m$ *взаимно прост с модулем тогда и только тогда, когда все его компоненты* $a_1 \bmod m_1, \ldots, a_r \bmod m_r$ *взаимно просты с модулями.*

Вследствие этого, при разложении IX в прямую сумму операции в группе классов вычетов по $\bmod m$, взаимно простых с модулем, сводятся к операциям в группах классов вычетов по $\bmod m_1, \ldots, \bmod m_r$, взаимно простых с модулями. Так как это касается только операции умножения, то на языке алгебры это может быть высказано следующим образом:

XI. *Группа классов вычетов по* $\bmod m$, *взаимно простых с модулем, есть прямое произведение групп классов вычетов по* $\bmod m_1, \ldots, \bmod m_r$, *взаимно простых с модулями.*

Если при установленном ранее взаимно однозначном соответствии между классами вычетов $a \bmod m$, взаимно простыми с модулем, с одной стороны, и системами классов вычетов $a_1 \bmod m_1, \ldots, a_r \bmod m_r$, взаимно простыми с модулями, с другой, обратить внимание только на их количества, то мы получим формулу

$$\varphi(m) = \varphi(m_1) \ldots \varphi(m_r)$$

для каждого разложения числа m на попарно взаимно простые множители $m_1, \ldots, m_r$, т. е. функциональное равенство (4), обобщенное на любое количество r сомножителей. Тем самым мы решили в утвердительном смысле вопрос, в связи с которым мы рассматривали теорию систем сравнений.

10. Сравнимость для дробных чисел. В связи с формулировкой VIII, п. 5 нашего результата о порядке класса вычетов $a \bmod m$, взаимно простого с модулем, мы заметили, что было бы желательно обобщить понятие сравнимости на дробные рациональные числа со знаменателями, взаимно простыми с m. Теперь это будет сделано.

Рациональные числа со знаменателями (в смысле § 2, п. 6), взаимно простыми с m, образуют область целостности Γ_m, которая содержит область целостности Γ целых чисел; их называют также *m-целыми числами*. Для того чтобы установить, что Γ_m есть область целостности, и вообще для дальнейшего, заметим, что рациональное число α заведомо будет m-целым, если только оно *вообще* обладает дробным представлением $\alpha = b/a$ с a, взаимно простым с m; действительно, представление *несократимой* дробью $\alpha = b_0/a_0$, получающееся посредством освобождения от делителя $d = (a, b)$, тоже будет тогда иметь знаменатель a_0, взаимно простой с m.

Для чисел a, a' из Γ сравнимость $a \equiv a' \bmod m$ равносильна, согласно I, п. 1, тому, что в Γ имеет место отношение делимости $m \mid a - a'$, т. е. что $a - a' = gm$ с некоторым числом g из Γ. Соответственно этому, мы аналогично определим формально для чисел α, α' из Γ_m сравнимость $\alpha \equiv \alpha \bmod m$ как выполнение отношения делимости $m \mid \alpha - \alpha'$ в Γ_m, т. е. существование равенства $\alpha - \alpha' = \gamma m$ с некоторым числом γ из Γ_m. Мы здесь только вскользь упомянем о том, что набросанная в § 1, п. 2 элементарная теория делимости в Γ формально переносится на область целостности Γ_m и вообще на каждую область целостности, если только, вместо специальных единиц ± 1 в Γ понимать вообще под единицами делители числа 1, т. е. в случае Γ_m рациональные числа со знаменателем и числителем, взаимно простыми с m. Наше обобщение определения сравнимости может быть высказано и без этого следующим образом:

Определение. *Два m-целых числа α, α' называются сравнимыми по* $\bmod m$, *если число $\alpha - \alpha'/m$ является m-целым, т. е. если их разность имеет числитель, делящийся на m.*

Для этих обобщенных сравнений снова имеют место обычные правила действий в пределах трех первых элементарных операций. Это получается точно так же, как выше в п. 2, просто из того факта, что Γ_m как и Γ является областью целостности.

Выраженное в каком-нибудь представлении дробью

$$\alpha = \frac{b}{a}, \quad \alpha' = \frac{b'}{a'}$$

со знаменателями, взаимно простыми с m, обобщенное сравнение

$$\alpha \equiv \alpha' \bmod m$$

равносильно обычному сравнению

$$a'b \equiv ab' \bmod m.$$

В самом деле, тогда

$$\alpha - \alpha' = \frac{a'b - ab'}{aa'}$$

есть дробь со знаменателем, взаимно простым с m, и, таким образом, сравнимость $\alpha \equiv \alpha' \bmod m$, согласно определению, равносильна с делимостью $m \mid a'b - ab'$. Заметим при этом еще раз, что делимость числителя на m не зависит, согласно VI, п. 5, § 2, от того, взята ли у нас первоначально несократимая дробь или какая-нибудь дробь со знаменателем, взаимно простым с m.

Если, в частности, рациональные числа α, α' являются не только m-целыми, но и целыми в обычном смысле, то выше мы можем выбрать $a = 1$, $a' = 1$ и, таким образом, $\alpha = b$, $\alpha' = b'$. Поэтому обобщенное сравнение $\alpha = \alpha' \bmod m$ равносильно тогда обычному сравнению $b \equiv b' \bmod m$, или, другими словами, сравнению $\alpha \equiv \alpha' \bmod m$, понимаемому в обычном смысле, что и должно требоваться от всякого имеющего смысл расширения понятия.

Аналогично тому, как ранее в п. 2, наша обобщенная сравнимость приводит к разбиению области целостности Γ_m на классы вычетов по $\bmod m$. Согласно сказанному выше, для подобласти Γ получается при этом известное нам разбиение на m обычных классов вычетов по $\bmod m$. Может показаться, что в полной области Γ_m появятся еще и другие классы вычетов, так как разбивается ведь большее количество чисел. Однако это не так. Напротив, имеет место:

XII. *Каждое m-целое число α сравнимо по $\bmod m$ с некоторым целым в обычном смысле числом. Это последнее будет взаимно просто с m тогда и только тогда, когда числитель y α также взаимно прост с m.*

Доказательство. Пусть $\alpha = b/a$ — какое-нибудь дробное представление рассматриваемого m-целого числа α со знаменателем a, взаимно простым m. Тогда доказываемое сравнение $\alpha \equiv x \bmod m$, где $x = x/1$ — искомое целое число, равносильно, согласно только что сказанному, обычному сравнению $ax \equiv b \bmod m$. А это сравнение, в силу IV, п. 3, действительно разрешимо посредством некоторого целого числа x, так как $(a, m) = 1$, и при этом $(x, m) = 1$ тогда и только тогда, когда $(b, m) = 1$.

Из этого доказательства следует, что, наоборот, существующее и однозначно определенное, согласно IV п. 3, решение $x \bmod m$ сравнения

$$ax \equiv b \bmod m \text{ с } (a, m) = 1$$

посредством применения нашего обобщенного понятия сравнения может быть записано в виде

$$x \equiv \frac{b}{a} \bmod m,$$

т. е. получается, как и для аналогичного уравнения, просто формальным делением на множитель a. При этом, однако, необходимо иметь в виду, что таким способом задача о разрешении сравнения $ax \equiv b \bmod m$ исчерпывается только с формальной точки зрения. Действительно, при постановке этой задачи требуется найти явное *целочисленное* решение x, в то время как мы получаем таким способом только общее *дробное* решение b/a. Нахождение же сравнимого с ним по $\bmod m$ целого числа x равносильно, согласно доказательству XII, первоначальной задаче.

В то время как с практической точки зрения мы посредством нашего обобщения понятия сравнимости не получили никакого нового способа для решения общего линейного сравнения $ax \equiv b \bmod m$, с теоретической точки зрения возможность записи $x \equiv b/a \bmod m$ значительно облегчает нам запись наших рассуждений. Так, например, полученный нами в VIII, п. 5 результат $a^x \equiv a^{x'} \bmod m$ тогда и только тогда, когда $x \equiv x' \bmod k$, где k есть порядок класса вычетов $a \bmod m$, взаимно простого с модулем, теперь сразу приобретает смысл также и для отрицательных показателей x, x'. Действительно, класс вычетов, обратный к классу $a \bmod m$, который до сих пор мог быть выражен лишь в неудобной форме $(a \bmod m)^{-1}$ как решение $a' \bmod m$ сравнения $aa' \equiv 1 \bmod m$, теперь просто может записываться в виде $1/a \bmod m$ или $a^{-1} \bmod m$, а тогда и каждая степень с целым показателем x — в виде $a^x \bmod m$.

В более гибкой записи состоит основное значение нашего обобщения понятия сравнимости. В остальном результат XII показывает, что в отношении разбиения на классы вычетов наше обобщение не вносит ничего нового, кроме пополнения каждого отдельного класса вычетов присоединенными теперь дробными (лишь m-целыми) числами. Кольцо классов вычетов по $\bmod m$ в Γ_m состоит попросту из m пополненных таким образом классов кольца классов вычетов по $\bmod m$ в Γ, связанных теми же правилами операций, которые уже существуют в Γ. То же самое имеет место для мультипликативной группы классов вычетов по $\bmod m$, взаимно простых с модулем.

Между прочим, классы вычетов по $\bmod m$, взаимно простые с модулем, пополняются при переходе от Γ к Γ_m теми и только теми рациональными числами α, у которых не только знаменатель, но и числитель взаимно прост с m. Они являются как раз вышеупомянутыми единицами в Γ_m. Их называют также *взаимно простыми с m рациональными числами*. В их разложении на простые множители $\alpha \cong \prod_p p^{\alpha_p}$ они. характеризуются тем, что $\alpha_p = 0$ для всех $p|m$.

11. Поле классов вычетов по простому модулю. Как мы установили в VII, п. 4, в специальном случае простого числа $m = p$ кольцо классов вычетов по $\bmod p$ является полем. Рассмотрим теперь это *поле классов вычетов* по $\bmod p$ подробнее. Оно является конечным полем из p элементов. В алгебре показывается, что этим условием оно определяется однозначно; его называют *простым полем*, принадлежащим к p, и обозначают через Π. Далее в алгебраическую структуру этого поля Π мы здесь входить не будем.

Доказанная в п. 5 малая теорема Ферма в данном специальном случае гласит:

$$a^{p-1} \equiv 1 \bmod p \text{ для всех } a \not\equiv 0 \bmod p,$$

так как для функции Эйлера, как было показано в п. 8, имеет место $\varphi(p) = p - 1$. Включая также класс вычетов $\alpha \equiv 0 \bmod p$, можно обобщить эту теорему в виде высказывания

$$a^p \equiv a \bmod p \text{ для всех целых } a.$$

В силу этого, каждый элемент A поля Π имеет свойство $A^p = A$. Таким образом, если $A_0, A_1, \ldots, A_{p-1}$ обозначают p различных элементов поля Π и притом A_i обозначает класс вычетов $i \bmod p$, то многочлен p-й степени $t^p - t$, рассматриваемый как многочлен от t с коэффициентами из Π, имеет p различных корней $A_0, A_1, \ldots, A_{p-1}$. Отсюда по известной теореме из алгебры о корнях многочлена над некоторым полем следует существование тождества

$$t^p - t = (t - A_0)(t - A_1) \ldots (t - A_{p-1}),$$

или после сокращения на линейный множитель $t = t - A_0$

$$t^{p-1} - E = (t - A_1) \ldots (t - A_{p-1}),$$

где $E = A_1$ означает единичный элемент поля Π. Из этого тождества относительно t посредством сравнения коэффициентов получаются следующие формулы (называемые в алгебре в общем

случае формулами Виета):

$$A_1 + A_2 + \ldots + A_{p-1} = 0,$$
$$A_1A_2 + A_1A_3 + \ldots + A_{p-2}A_{p-1} = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$A_1A_2 \ldots A_{p-1} = (-1)^p E.$$

Так как A_i есть класс вычетов $i \bmod p$, то эти формулы означают сравнения:

$$1 + 2 + \ldots + (p-1) \equiv 0 \bmod p,$$
$$1 \cdot 2 + 1 \cdot 3 + \ldots + (p-2)(p-1) \equiv 0 \bmod p,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$1 \cdot 2 \ldots (p-1) \equiv (-1)^p \bmod p.$$

Последнее из них известно под названием *теоремы Вильсона*; так как всегда $(-1)^p \equiv -1 \bmod p$ (для $p \neq 2$ даже не $\equiv \bmod p$, а $=$), то она может быть высказана в форме

$$(p-1)! \equiv -1 \bmod p.$$

Как интересное и важное следствие из этой теоремы Вильсона отметим уже здесь один факт, относящийся, собственно говоря, к теории квадратичных вычетов (см. § 7):

XIII. *Для каждого простого числа* $p \equiv 1 \bmod 4$ *сравнение* $x^2 \equiv -1 \bmod p$ *разрешимо, т. е. класс вычетов* $-1 \bmod p$ *является квадратом в* Π.

Доказательство. Если $p = 4n+1$ с натуральным n, то

$$(p-1)! = [1 \cdot 2 \ldots (2n)]\,[(p-1)(p-2)\ldots(p-2n)] \equiv$$
$$\equiv [(2n)!]\,[(-1)^{2n}(2n)!] \equiv [(2n)!]^2 \bmod p.$$

Таким образом, согласно теореме Вильсона, $x \equiv (2n)! \bmod p$ является решением сравнения $x^2 \equiv -1 \bmod p$.

Что касается остальных сравнений, выведенных выше из сравнения коэффициентов, то они не представляют особого интереса. Первое из них даже тривиально, так как $1 + 2 + \ldots + (p-1) = p(p-1)/2$; для $p \neq 2$ значение $p(p-1)/2$ этой суммы есть кратное от p; для $p = 2$ первое сравнение вообще не встречается среди формул Виета, так как они сводятся в этом случае только к одной последней формуле.

Другой важный факт, играющий также большую роль в алгебраической теории простого поля Π, состоит в следующем:

XIV. *Для каждого простого числа* p *средние биномиальные коэффициенты*

$$\binom{p}{\nu} \equiv 0 \bmod p \qquad (\nu = 1, \ldots, p-1).$$

Доказательство. Как известно,

$$\binom{p}{\nu} = \frac{p(p-1)\dots(p-(\nu-1))}{1\cdot 2\dots\nu}.$$

У стоящей справа дроби числитель делится на p, а знаменатель для $\nu = 1, \dots, p-1$ взаимно прост с p. Поэтому, согласно IV, п. 5, § 2, также и частное $\binom{p}{\nu}$ (являющееся целым числом!) делится на p.

Согласно XIV и теореме о разложении бинома, для неизвестных x, y имеет место сравнение

$$(x+y)^p \equiv x^p + y^p \bmod p$$

в том смысле, что коэффициенты при произведениях одинаковых степеней справа и слева сравнимы между собой по $\bmod p$. Если вместо x, y подставить целые числа a, b, то получающееся высказывание

$$(a+b)^p \equiv a^p + b^p \bmod p$$

тривиально, так как по малой теореме Ферма обе стороны $\equiv a + b \bmod p$. Однако таким способом можно, наоборот, получить новое доказательство малой теоремы Ферма, если положить $b = 1$ и применить полную индукцию по a.

12. Аддитивное представление классов вычетов по степеням простого числа. Если конкретное натуральное число a хотят разбить на части, то обычно его представляют не в его первоначальной, натуральной форме в виде суммы a единиц $1+1+\dots+1$, а в десятичном представлении

$$a = a_0 + a_1 10 + \dots + a_{h-1} 10^{h-1},$$

причем $h \geqslant 1$ цифр $a_0, a_1, \dots, a_{h-1}$ принадлежат к наименьшей системе вычетов $0, 1, \dots, 9 \bmod 10$. Числа a, состоящие не более чем из h цифр, образуют тогда, если присоединить еще $a = 0$, наименьшую систему вычетов $0, 1, \dots, 10^h - 1 \bmod 10^h$.

То, что при таком способе записи за основание берется число 10, объясняется чисто практическим удобством этого числа при вычислениях. С теоретической же точки зрения совершенно равноправными являются и соответствующие представления с другими основаниями m, причем в качестве основания может быть выбрано каждое натуральное число $m \neq 1$. Системой цифр является тогда наименьшая система вычетов $0, 1, \dots, m-1 \bmod m$, а числа, состоящие не более чем из h цифр, снова образуют наименьшую систему вычетов $0, 1, \dots, m^h - 1 \bmod m$.

Специально для случая простого числа $m=p$ получается следующее часто применяемое аддитивное представление классов вычетов по $\bmod p^h$:

XV. *Для каждого данного показателя* $h \geqslant 1$ *классы вычетов* $a \bmod p^h$ *однозначно представляются в виде*

$$a \equiv a_0 + a_1 p + \ldots + a_{h-1} p^{h-1} \bmod p^h$$

с коэффициентами $a_0, a_1, \ldots, a_{h-1}$ *из наименьшей системы вычетов*

$$0,\ 1,\ \ldots,\ p-1 \bmod p.$$

Такое представление называется *p-адическим представлением* класса вычетов $a \bmod p^h$. Доказательство этого факта (существования такого представления и несравнимость по $\bmod p^h$ стоящих справа выражений) мы можем не давать ввиду отмеченной уже аналогии с 10-адическим представлением. Однако необходимо отчетливо указать следующее. Хотя это представление и однозначно, однако система цифр для суммы не получается почленным сложением систем цифр слагаемых; напротив, при сложении происходит перенос цифр, совершенно аналогично тому, как при обычных операциях с числами. Таким образом, это однозначное представление отличается от того, что в теории конечных абелевых групп (в данном случае аддитивной группы классов вычетов по $\bmod p^h$) называется представлением через базис.

Из представления для $a \bmod p^h$ в XV соответствующее представление для $a \bmod p^k$ с каким-нибудь показателем $k < h$ получается просто отбрасыванием членов, начиная с $a_k p^k$. В частности, таким образом, $a \equiv a_0 \bmod p$ есть такое (тривиальное) представление для $k=1$. Так как классы вычетов $a \bmod p^h$, взаимно простые с модулем, характеризуются свойством $a \not\equiv 0 \bmod p$, то отсюда получается следующее дополнение:

XV′. *В однозначном представлении* XV *классы вычетов* $a \bmod p^h$, *взаимно простые с модулем, характеризуются свойством* $a_0 \neq 0$.

Подсчет количества систем цифр $a_0, a_1, \ldots, a_{h-1}$ для классов вычетов, взаимно простых с модулем, приводит к уже известной нам из п. 8 формуле $\varphi(p^h) = (p-1)\,p^{h-1}$, получающейся формально другим способом, чем там.

Используем p-адическое представление натурального числа n

$$n = a_0 + a_1 p + \ldots + a_{h-1} p^{h-1}$$

для определения точного показателя, с каким простое число p входит в разложение $n!$ на простые множители, или, короче, входит в $n!$, и, кроме того, установим, с чем сравним по $\bmod p$

остающийся после деления $n!$ на эту степень числа p (точнее, числа $-p$) дополнительный множитель. Мы докажем следующее:

XVI. *Если n есть натуральное число, а p — простое число, то p входит в $n!$ с показателем $(n-s_n)/(p-1)$ и имеет место*

$$\frac{n!}{(-p)^{\frac{n-s_n}{p-1}}} \equiv t_n \bmod p,$$

где

$$s_n = a_0 + a_1 + \ldots + a_{h-1}$$

обозначает сумму цифр p-адического представления числа n, а

$$t_n = a_0!\, a_1! \ldots a_{h-1}!$$

— произведение факториалов этих цифр.

Доказательство. Применим полную индукцию по n, опираясь на функциональное уравнение

$$n! = (n-1)!\, n$$

для факториала. Для $n=1$ оба утверждения очевидны ($s_1 = 1$, $t_1 = 1$). Пусть $n > 1$ и p входит в n с показателем ν. Тогда в p-адическом представлении числа n первой цифрой, отличной от 0, будет a_ν, или, записывая подробно,

$$n = 0 + 0 \cdot p + \ldots + 0 \cdot p^{\nu-1} + a_\nu p^\nu + a_{\nu+1} p^{\nu+1} + \ldots + a_{h-1} p^{h-1}$$

с

$$a_\nu \geqslant 1$$

и

$$\frac{n}{p^\nu} \equiv a_\nu \bmod p.$$

Вычитая 1, мы получаем отсюда (принимая во внимание перенос цифр) p-адическое представление для $n-1$:

$$n-1 = (p-1) + (p-1)\,p + \ldots + (p-1)\,p^{\nu-1} + (a_\nu - 1)\,p^\nu + a_{\nu+1} p^{\nu+1} + \ldots + a_{h-1} p^{h-1}.$$

Поэтому, во-первых,

$$s_n = s_{n-1} + 1 - \nu(p-1)$$

и, таким образом,

$$\frac{n-s_n}{p-1} = \frac{(n-1)-s_{n-1}}{p-1} + \nu,$$

и, в силу этого соотношения, правильность первого утверждения для n следует из его правильности для $n-1$. Во-вторых, при-

нимая во внимание теорему Вильсона,

$$t_n = t_{n-1}\frac{a_\nu}{[(p-1)!]^\nu} \equiv t_{n-1}\frac{a_\nu}{(-1)^\nu} \equiv t_{n-1}\frac{n}{(-p)^\nu} \bmod p,$$

и, в силу этого соотношения, правильность второго утверждения для n также следует из его правильности для $n-1$.

Заметим, что при доказательстве по индукции первого утверждения была одновременно доказана также целочисленность показателей $(n-s_n)/(p-1)$. Однако она может быть получена также как прямое следствие p-адического разложения числа n в форме сравнения

$$n \equiv s_n \bmod p-1,$$

так как $p \equiv 1 \bmod p-1$. Последнее сравнение, рассматриваемое как критерий делимости n на $p-1$ или вообще как критерий для определения остатка от деления n на $p-1$, есть обобщение обычного признака делимости на 9 в 10-адичном представлении.

Пример. Для $n=100$, $p=7$ имеем

$$100 = 2+0\cdot 7+2\cdot 7^2$$

и, таким образом,

$$s_n = 2+0+2=4,\quad \frac{n-s_n}{p-1}=\frac{96}{6}=16,\quad t_n = 2!\cdot 0!\cdot 2! = 4,$$

и потому

$$100! \equiv 0 \bmod 7^{16}$$

и

$$\frac{100!}{(-7)^{16}} \equiv 4 \bmod 7.$$

13. Периодичность разложения рациональных чисел в m-ичную дробь. Как известно, каждое положительное вещественное число a обладает бесконечным *разложением в десятичную дробь*

$$a = \sum_{\nu \gg -\infty} \frac{a_\nu}{10^\nu}$$

с цифрами a_ν из наименьшей системы вычетов по mod 10, которое формально распространено на все целые индексы, однако в левую сторону (при $\nu \to -\infty$), начиная с некоторого места, все $a_\nu = 0$, на что указывает обозначение $\nu \gg -\infty$ под знаком суммы. Далее, известно также, что это разложение однозначно, если исключить разложения, обрывающиеся в правую сторону (при $\nu \to \infty$)

$$a = \ldots + \frac{a_n}{10^n} + \frac{0}{10^{n+1}} + \frac{0}{10^{n+2}} + \ldots$$

(a_n последнее, отличное от 0), записывая их в форме

$$a = \ldots + \frac{a_n - 1}{10^n} + \frac{9}{10^{n+1}} + \frac{9}{10^{n+2}} + \ldots .$$

Для такого разложения тоже можно взять в качестве основания любое натуральное число $m \neq 1$ вместо 10. Таким образом, каждое положительное вещественное число a обладает однозначно определенным, не обрывающимся вправо разложением в m-ичную дробь

$$a = \sum_{\nu \gg -\infty} \frac{a_\nu}{m^\nu}$$

с цифрами a_ν из наименьшей системы вычетов по $\bmod m$. Обратно, каждое такое разложение дает вещественное положительное число a.

Мы не будем давать здесь относящегося к анализу простого доказательства этого факта для любого *вещественного* $a > 0$, а займемся специальным случаем *рационального* $a > 0$. Из элементарного курса арифметики можно вспомнить, что разложения рациональных чисел $a > 0$ в десятичную дробь периодичны, и, обратно, каждая периодическая десятичная дробь дает рациональное число $a > 0$. Мы докажем здесь этот факт теоретико-числовыми средствами для любого основания m вместо 10 и дадим, кроме того, теоретико-числовую характеристику для способа определения разложения по заданному числу a.

Прежде всего мы должны придать этому способу определения единообразный вид. Для этого мы представим самое общее *разложение в периодическую m-ичную дробь* в следующей форме:

$$a = m^h \Big(b_1 m^{l-1} + \ldots + b_l + \frac{a_1}{m} + \ldots + \frac{a_k}{m^k} + \\ + \frac{a_1}{m^{k+1}} + \ldots + \frac{a_k}{m^{2k}} + \ldots ,$$

или коротко

$$a = m^h (b_1 \ldots b_l \cdot \overline{a_1 \ldots a_k}).$$

При этом мы считаем, что число h, *предпериод* $b_1 \ldots b_l$ и *период* $a_1 \ldots a_k$ установлены так, что выполнены следующие условия.

а) Период $a_1 \ldots a_k$ имеет наименьшую возможную длину ($k \geqslant 1$); в этом смысле говорят также о *простейшем* периоде.

б) Предпериод $b_1 \ldots b_l$ тоже имеет наименьшую возможную длину l ($\geqslant 0$). Таким образом, если он действительно имеется ($l \geqslant 1$), то $b_1 \neq 0$, $b_l \neq a_k$, а если его нет, то мы будем представлять себе, что он заменен числом 0, и понимать последнее требование в том смысле, что $a_k \neq 0$. Для ясности заметим, что тем самым в последнем случае, если к тому же $a_1 = 0$, преобра-

зование $m^h(\overline{0.0a_2\ldots a_k}) = m^{h-1}(\overline{0.a_2\ldots a_k0})$ недопустимо, так что нельзя достигнуть того, чтобы при $l=0$, $k>1$ всегда было также $a_1 \neq 0$.

Кроме того, в силу сделанного уже ранее условия, не может быть, чтобы период был одночленным с числом 0.

Все эти нормирования могут быть, очевидно, получены тривиальным преобразованием заданного периодического разложения. Тем самым определение разложения сводится к однозначному нахождению ряда чисел $a_1, \ldots, a_k, b_1, \ldots, b_l, h$ (последнее число — целое, $\gtreqless 0$). В этом смысле мы говорим о *нормированном* разложении в периодическую m-ичную дробь.

Сначала мы рассмотрим в качестве основного предмета нашего исследования характеризующийся уровнями $h=0$, $l=0$ специальный случай нормированного разложения в *чисто периодическую* m-ичную дробь:

$$a = 0.\overline{a_1\ldots a_k}.$$

Нормирующие условия сводятся здесь к двум требованиям, чтобы k было наименьшим возможным и $a_k \neq 0$. Обозначим через

$$A = a_1 m^{k-1} + \ldots + a_k$$

соответствующее периоду натуральное число, имеющее m-адическое представление с теми же самыми цифрами. Оно имеет свойства

$$0 < A \leqslant m^k - 1, \quad m \nmid A.$$

Тогда по формуле суммы бесконечной геометрической прогрессии a получается как рациональное число

$$a = \frac{A}{m^k} + \frac{A}{m^{2k}} + \ldots = \frac{A}{m^k - 1} = \frac{z}{n},$$

где последнее есть представление несократимой дробью, со свойствами

$$0 < z \leqslant n, \quad m \nmid z, \quad (m, n) = 1. \tag{1}$$

При этом

$$m^k \equiv 1 \mod n, \tag{2}$$

и потому, согласно VIII, п. 5, k делится на порядок k_0 класса вычетов $m \bmod n$, взаимно простого с модулем. В этой последовательности выводов из двух нормирующих условий было использовано только второе ($a_k \neq 0$; в силу его, $m \nmid A$, и потому $m \nmid z$), а первое (минимальность k) еще не использовано.

Пусть теперь, наоборот, дано рациональное число, представленное несократимой дробью $a = z/n$ со свойствами (1). Если

выбрать тогда какое-нибудь натуральное k, делящееся на порядок k_0 класса $m \bmod n$, так что будет выполняться и (2), то, согласно предыдущим формулам, представление числа a в виде дроби $a=A/(m^k-1)$ даст нам чисто периодическое разложение в m-ичную дробь $a=0.\overline{a_1 \ldots a_k}$ с периодом, определенным рядом цифр в m-адическом представлении числа A; при этом, в силу IV, п. 5, § 2, второе нормирующее требование ($a_k \neq 0$) будет выполнено, а первое (минимальность k) еще не обязательно. Но из хода наших рассуждений видно, что во всяком случае существует разложение числа a в периодическую m-ичную дробь с длиной периода k_0, так что минимальная длина периода должна быть $\leqslant k_0$, в то время как из предшествующих рассуждений следует, что она делится на k_0 и потому $\geqslant k_0$. Из этих условий вместе получается $k=k_0$.

Тем самым доказано:

XVII. *Нормированные разложения в чисто периодическую m-ичную дробь $a=0.\overline{a_1 \ldots a_k}$ имеют те и только те рациональные числа a, у которых представление несократимой дробью $a=z/n$ имеет свойства* (1), *т. е. является правильной дробью с числителем, не делящимся на m, и знаменателем, взаимно простым с m.*

При этом длина k простейшего периода равна порядку класса вычетов $m \bmod n$, взаимно простого с модулем, а последовательность $a_1 \ldots a_k$ совпадает с последовательностью цифр в m-адическом представлении числителя в соответствующем дробном представлении $a=A/(m^k-1)$.

Заметим еще, что, согласно доказательству, отказ от нормирующего требования $a_k \neq 0$ соответствует отмене условия $m \nmid z$. В дальнейшем мы будем применять высказывание XVII в этой, несколько модифицированной форме.

Общий случай любого нормированного разложения в периодическую m-ичную дробь

$$a=m^h\,(b_1 \ldots b_l.\overline{a_1 \ldots a_k})$$

теперь может быть легко разобран посредством сведения к чисто периодическому случаю. Обозначим через

$$B=b_1 m^{l-1}+\ldots+b_l$$

соответствующее предпериоду неотрицательное целое число и положим в прежних обозначениях

$$a^*=0.\overline{a_1 \ldots a_k}=\frac{A}{m^k-1}=\frac{z}{n}.$$

Тогда a есть рациональное число

$$a=m^h\,(B+a^*)=m^h\,\frac{B\,(m^k-1)+A}{m^k-1}=m^k\,\frac{Bn+z}{n}, \qquad (3)$$

где последний множитель при m^h представлен несократимой дробью. При этом, в силу нашего нормирования, прежде всего

$$B(m^k-1)+A\equiv -b_l+a_k\not\equiv 0 \bmod m. \qquad (4)$$

Отсюда следует:

XVIIIа. *Число h однозначно характеризуется числом a как такое наибольшее целое число ($\geqq 0$), что a/m^h имеет еще взаимно простой с m знаменатель — и притом не делящийся на m числитель.*

Далее, $0<a^*\leqslant 1$. Отсюда следует:

XVIIIб. *Соответствующее предпериоду число B однозначно характеризуется числом a как такое целое число ($\geqslant 0$), что a/m^h лежит в интервале $B<a/m^h\leqslant B+1$. В частности, поэтому длина предпериода l однозначно характеризуется числом a как такое наименьшее целое число ($\geqslant 0$), для которого еще $a/m^h\leqslant m^l$.*

Наконец, число a/m^h имеет тот же самый взаимно простой с m знаменатель n, что и a. Отсюда, согласно XVII, следует:

XVIIIв. *Длина периода k однозначно характеризуется числом a как порядок класса вычетов $m \bmod n$, где n есть знаменатель числа a/m^h. Соответствующее периоду число A получается как числитель правильной положительной дроби a/m^h-B, приведенной к знаменателю m^k-1.*

Если, наоборот, задано положительное рациональное число a, и мы определили для него h, l, B, k, A указанными в XVIIIа, б, в способами, то из разложения (3) получается разложение числа a в периодическую m-ичную дробь, если для a^* использовать чисто периодическое разложение по XVII, а для B взять его m-адическое разложение; ввиду (4) это разложение будет нормированным.

В итоге доказана следующая теорема, которая была уже упомянута в начале как известная из элементарной арифметики:

Основная теорема о разложении в m-ичную дробь. *Положительные рациональные числа характеризуются среди всех положительных вещественных чисел тем, что их разложения в m-ичные дроби при любом натуральном основании $m\neq 1$ периодичны.*

Кроме того, в высказываниях XVIIIа, б, в даются однозначные характеристики для определения этих периодических m-ичных разложений в нормированной форме по тому числу, которое должно быть в таком виде представлено.

§ 5. СТРУКТУРА ГРУППЫ КЛАССОВ ВЫЧЕТОВ, ВЗАИМНО ПРОСТЫХ С МОДУЛЕМ

1. Сведение к степеням простых чисел. Группа классов вычетов по $\bmod m$, взаимно простых с модулем, для натурального числа m есть конечная абелева группа порядка $\varphi(m)$, опре-

деленного в § 4, п. 8. Согласно XI, п. 9, § 4, она является прямым произведением групп классов вычетов по $\bmod p^\mu$, взаимно простых с модулем, для входящих в m степеней простых чисел p^μ. Тем самым вопрос о структуре группы классов вычетов по $\bmod m$, взаимно простых с модулем, сводится к вопросу о структуре групп классов вычетов по $\bmod p^\mu$, взаимно простых с модулем. Действия с классами вычетов $a \bmod m$, взаимно простыми с модулем, сводятся к почленным действиям с их компонентами — классами вычетов $a \bmod p^\mu$, взаимно простыми с модулем. Формальный аппарат этого разложения по компонентам подробно изложен в § 4, п. 9.

Нам достаточно поэтому заняться в дальнейшем структурой группы классов вычетов по $\bmod p^\mu$, взаимно простых с модулем, только для степени простого числа $p^\mu (\mu \geqslant 1)$. Эту конечную абелеву группу мы будем обозначать через $\mathfrak{P}_\mu$; согласно § 4, п. 8 или § 4, п. 12, она имеет порядок $\varphi(p^\mu) = (p-1)\, p^{\mu-1}$.

2. Случай простого числа. Мы начнем с исследования структуры группы классов вычетов по $\bmod p$, взаимно простых с модулем, для простого числа p, т. е. группы $\mathfrak{P}_1 = \mathfrak{P}$ порядка $\varphi(p) = p-1$. Она может быть описана так же, как мультипликативная группа поля классов вычетов по $\bmod p$ (простого поля Π) (см. § 4, п. 11). Это последнее описание мы будем существенно использовать в дальнейшем исследовании.

Порядок каждого элемента A из $\mathfrak{P}$ равен некоторому натуральному делителю d порядка группы $p-1$ (см. § 4, п. 11).

Теперь установим, обратно, как велико количество $\psi(d)$ элементов A из $\mathfrak{P}$ с порядком, равным данному натуральному делителю d числа $p-1$. A priori может случиться, что для данного $d \mid p-1$ в $\mathfrak{P}$ вообще нет ни одного элемента A порядка d, так что $\psi(d) = 0$. Если, однако, хотя бы один такой элемент A существует, т. е. $\psi(d) \neq 0$, то мы можем заключить следующее. Порожденная элементом A циклическая группа $\mathfrak{A}$, согласно § 4, п. 5, состоит точно из d различных элементов, соответствующих d различным классам вычетов $\delta \bmod d$. Все эти элементы являются корнями многочлена $t^d - E$ степени d, где через E обозначен единичный элемент поля Π. Аналогично тому, как в § 4, п. 11, отсюда следует выполнение тождества

$$t^d - E = \prod_{\delta \bmod d} (t - A^\delta).$$

При этом запись $\prod_{\delta \bmod d}$ означает, что умножение производится по какой-нибудь полной системе вычетов $\delta \bmod d$; этот инвариантный способ записи мы будем употреблять вместо не инва-

риантного $\prod_{\delta=0}^{d-1}$ всегда, когда значение произведения не зависит от выбора системы представителей в классах вычетов $\delta \bmod d$ (то же самое и для суммы).

Из полученного тождества следует далее, что каждый элемент B порядка d из $\mathfrak{P}$, будучи корнем многочлена $t^d - E$, равен одному из корней A^δ. Поэтому из предположения, что в $\mathfrak{P}$ существует элемент A порядка d, вытекает, что *все* элементы порядка d из $\mathfrak{P}$ представляются в виде $B = A^\delta$. Их количество $\psi(d)$ совпадает, таким образом, с количеством тех классов вычетов $\delta \bmod d$, для которых A^δ тоже имеет порядок d.

Но равенство $(A^\delta)^x = A^{\delta x} = E$ имеет место тогда и только тогда, когда $\delta x \equiv 0 \bmod d$, а это, в свою очередь, выполняется тогда и только тогда, когда $x \equiv 0 \bmod d/(\delta, d)$ (см. V′, п. 3, § 4). Поэтому A^δ имеет порядок $d/(\delta, d)$. В частности, A^δ само имеет порядок d в точности тогда, когда $(\delta, d) = 1$. Элементы $B = A^\delta$ порядка d точно соответствуют, таким образом, классам вычетов $\delta \bmod d$, взаимно простым с модулем, и количество их равно поэтому $\varphi(d)$.

Мы показали, что для каждого натурального делителя d числа $p-1$ выполняется одно из двух соотношений

$$\psi(d) = 0 \quad \text{или} \quad \psi(d) = \varphi(d).$$

Но, с другой стороны, имеют место соотношения

$$\sum_{d|p-1} \psi(d) = p-1 \quad \text{и} \quad \sum_{d|p-1} \varphi(d) = p-1,$$

первое из которых получается в результате подсчета всех $p-1$ элементов группы $\mathfrak{P}$, расположенных по их порядкам, а второе согласно § 4, п. 6 (где оно получается соответствующим подсчетом всех $p-1$ классов вычетов по $\bmod p-1$, расположенных по их общим наибольшим делителям с модулем). Отсюда следует, что соотношение $\psi(d) = 0$ в действительности никогда не имеет места, а, наоборот, всегда выполняется

$$\psi(d) = \varphi(d).$$

Тем самым мы доказали:

I. *Для каждого натурального делителя d числа $p-1$ существует точно $\varphi(d)$ классов вычетов по* $\bmod p$, *взаимно простых с модулем, имеющих порядок d. Если $a \bmod p$ — один из них, то все остальные получаются в виде $a^\delta \bmod p$ с δ, взаимно простым с d.*

Применим теперь этот результат к наибольшему делителю $d = p-1$, т. е. к самому порядку группы $\mathfrak{P}$. Тогда этот результат означает существование такого класса вычетов $w \bmod p$,

взаимно простого с модулем, что порожденная им циклическая группа $w^\alpha \bmod p$ ($\alpha \bmod p-1$) состоит точно из $p-1$ элементов и потому совпадает со всей группой $\mathfrak{P}$. Таким образом, в качестве *основного результата* нашего исследования мы получаем:

II. *Группа классов вычетов по* $\bmod p$, *взаимно простых с модулем, циклична.*

Порождающий ее класс вычетов $w \bmod p$ (а также и число w) называется *первообразным корнем* по $\bmod p$. Их имеется точно $\varphi(p-1)$; они получаются из одного из них в виде $w^\alpha \bmod p$ с α, взаимно простым с $p-1$. Все классы вычетов $a \bmod p$, взаимно простые с модулем, однозначно представляются через первообразный корень $w \bmod p$ в виде

$$a \equiv w^\alpha \bmod p \qquad (a \bmod p-1).$$

В смысле теории конечных абелевых групп это есть *представление* группы $\mathfrak{P}$ *через базис*. Умножению (соответственно делению) классов вычетов $a \bmod p$, взаимно простых с модулем, соответствует при этом сложение (соответственно вычитание) показателей $\alpha \bmod p-1$. Поэтому в старой теории чисел показатель α (нормированный как наименьший вычет по $\bmod p-1$) называли, по аналогии с логарифмами, *индексом* числа a (тоже нормированного как наименьший вычет по $\bmod p$) по отношению к определенному первообразному корню $w \bmod p$ и обозначали через $\alpha = \operatorname{ind}_w a$.

3. К определению первообразных корней, гипотеза Артина. Никакого алгоритма для определения одного из первообразных корней по $\bmod p$, например, наименьшего из них, неизвестно. Поэтому их приходится находить посредством проб. Так, последовательно вычисляя степени

$$2^0 \equiv 1,\ 2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 3,\ 2^4 \equiv 1 \bmod 5,$$
$$2^0 \equiv 1,\ 2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 1 \qquad \bmod 7,$$

мы находим, что 2 есть первообразный корень по $\bmod 5$, и, напротив, $2 \bmod 7$ имеет лишь порядок 3 (вместо 6), в то время как из

$$3^0 \equiv 1,\ 3^1 \equiv 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1 \bmod 7$$

следует, что 3 является первообразным корнем по $\bmod 7$.

Более интересен обратный вопрос:

Для каких простых чисел p *данное целое число* w *является первообразным корнем по* $\bmod p$?

Для $w=1$ речь может идти, конечно, только о $p=2$, и для $w=-1$ только о $p=2, 3$. Вообще, для квадратного числа $w=w_0^2$ нужно рассматривать только $p=2$; в самом деле, если $p \neq 2$, то для него, если только о нем вообще идет речь, т. е. если

$p \nmid w$, в силу малой теоремы Ферма $w^{p-1/2} = w_0^{p-1} \equiv 1 \bmod p$, и потому порядок $w \bmod p$ является делителем числа $(p-1)/2$ и не равен $p-1$, как требуется. Некоторые соображения теоретико-вероятностного характера привели Артина к следующей гипотезе:

Гипотеза Артина. *Для каждого целого числа $w \neq \pm 1$, не являющегося квадратом, существует бесконечно много таких простых чисел p (не входящих в w), что w является первообразным корнем по* $\bmod p$.

Если k есть наибольшее (обязательно нечетное) натуральное число, такое, что $w = w_0^k$ является k-й степенью, то отношение количества $\pi_w(n)$ этих простых чисел, не превосходящих n, к количеству $\pi(n)$ всех простых чисел, не превосходящих n, стремится при $n \to \infty$ к зависящему только от k пределу

$$\omega_k = \lim_{n\to\infty} \frac{\pi_w(n)}{\pi(n)} = \prod_{q \mid k} \left(1 - \frac{1}{q-1}\right) \cdot \prod_{q \nmid k} \left(1 - \frac{1}{(q-1)\,q}\right).$$

При этом произведение распространено на все простые числа q, отдельно для конечного множества делителей числа k и бесконечного множества простых чисел, не являющихся таковыми. Оно абсолютно сходится, так как ряд $\sum_q \frac{1}{(q-1)\,q}$ имеет, очевидно, сходящуюся мажоранту

$$\sum_{n=2}^{\infty} \frac{1}{(n-1)\,n} = \sum_{n=2}^{\infty} \left(\frac{1}{n-1} - \frac{1}{n}\right) = \left(1 - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \ldots = 1$$

и потому имеет (если k нечетно) вещественное положительное значение ω_k. Оно будет наибольшим для $k = 1$, когда w, таким образом, не является степенью с показателем, > 1, и лежит тогда между $1/3$ и $5/12$. В этом последнем специальном случае, т. е., например, при $w = 2$, 3 и вообще любому простому числу, можно поэтому ожидать, что w окажется первообразным корнем по $\bmod p$ более, чем для каждого третьего простого числа p при достаточно большом их количестве.

Гипотеза Артина до сих пор не доказана. В то же время аналогичную гипотезу, относящуюся не к полю P рациональных чисел, а к полю $\Omega(t)$ рациональных функций от одной переменной t над некоторым конечным полем Ω, Бильгарцу [1] удалось свести к так называемой гипотезе Римана о полях алгебраических функций, а эта последняя гипотеза была недавно доказана А. Вейлем [1].

4. Циклический сдвиг периода в разложении в m-ичную дробь. Сделаем еще небольшое замечание о первообразных

корнях в связи с теорией разложения в m-ичную дробь из § 4, п. 13, а именно, приведем следующий факт. Если p есть простое число, не входящее в основание m, то, согласно XVII, п. 13, § 4, $p-1$ правильных дробей a/p с $1 \leqslant a \leqslant p-1$ имеют чисто периодические разложения в m-ичную дробь

$$\frac{a}{p} = 0 \cdot \overline{a_1 \ldots a_k},$$

у которых длина периода k все время равна порядку класса вычетов $m \bmod p$. При этом вместе с периодом $a_1 \ldots a_k$ встречаются также и все периоды, получающиеся из него циклическим сдвигом цифр. А именно, циклический сдвиг на одно место влево дает, очевидно, дробь

$$\frac{a'}{p} = 0.\overline{a_2 \ldots a_k a_1} = \frac{ma}{p} - a_1,$$

где a' определяется через a как наименьший вычет числа ma по $\bmod p$, т. е.

$$ma \equiv a' \bmod p \text{ с } 1 \leqslant a' \leqslant p-1.$$

Поэтому при циклических сдвигах в качестве совокупности новых числителей получается циклически замкнутая система наименьших вычетов $a^{(\varkappa)}$ из

$$m^{\varkappa} a \equiv a^{(\varkappa)} \bmod p \text{ с } 1 \leqslant a^{(\varkappa)} \leqslant p-1 \ (\varkappa \bmod k-1).$$

На языке теории групп это будет определяемый элементом a смежный класс к порожденной элементом m циклической подгруппе порядка k группы $\mathfrak{P}$. В частности, получается — и в этом состоит наше замечание:

В том и только том случае, когда m является первообразным корнем по $\bmod p$, *т. е. $k = p-1$, дроби a/p, получающиеся циклическим сдвигом периода в m-ичном разложении одной из них, например, $1/p$, исчерпывают все $p-1$ правильных дробей a/p со знаменателем p.*

Это есть обобщение того факта (следующего из элементарных подсчетов), что шесть разложений в десятичную дробь

$$\frac{1}{7} = 0.\overline{142857}$$
$$\frac{3}{7} = 0.\overline{428571}$$
$$\frac{2}{7} = 0.\overline{285714}$$
$$\frac{6}{7} = 0.\overline{857142}$$
$$\frac{4}{7} = 0.\overline{571428}$$
$$\frac{5}{7} = 0.\overline{714285}$$

правильных дробей со знаменателем 7 получаются друг из друга циклическим сдвигом цифр. Действительно, как показано в п. 3, $10 \equiv 3 \bmod 7$ является первообразным корнем, и циклические сдвиги соответствующей последовательности 1, 3, 2, 6, 4, 5 наименьших вычетов по mod 7 будут в точности те же, которые получались выше посредством приведения к наименьшему вычету элементов циклической группы $3^0, 3^1, 3^2, 3^3, 3^4, 3^5 \bmod 7$.

5. Леммы о сравнениях по степени простого числа. Мы переходим теперь к исследованию структуры группы классов вычетов по $\bmod p^\mu$, взаимно простых с модулем, для степени простого числа p^μ, т. е. группы $\mathfrak{P}_\mu$ для показателя $\mu > 1$. В соответствии с разложением порядка группы $\varphi(p^\mu) = (p-1)\,p^{\mu-1}$ мы выведем разложение группы $\mathfrak{P}_\mu$ в прямое произведение двух циклических групп $\mathfrak{P}'_\mu$, $\mathfrak{P}''_\mu$ порядков $p-1$, $p^{\mu-1}$ и тем самым найдем представление элементов из $\mathfrak{P}_\mu$ через базис. Для $p=2$ разложение $\varphi(2^\mu) = 1 \cdot 2^{\mu-1}$ является тривиальным, так что получилось бы $\mathfrak{P}'_\mu = 1$, $\mathfrak{P}''_\mu = \mathfrak{P}_\mu$, в этом случае мы выведем разложение группы $\mathfrak{P}_\mu$ в прямое произведение двух циклических групп $\mathfrak{P}'_\mu$, $\mathfrak{P}''_\mu$ порядков 2, $2^{\mu-2}$, соответствующее разложению $\varphi(2^\mu) = 2 \cdot 2^{\mu-2}$; это последнее будет тривиальным только для наименьшего из рассматриваемых показателей $\mu = 2$.

Конструкция этих разложений групп $\mathfrak{P}_\mu$ в прямые произведения основывается на следующих трех леммах о сравнениях по модулю, равному степени простого числа, в которых p обозначает простое число, а a, b, c и g—целые или также только p-целые в смысле § 4 п. 10, числа:

Лемма 1. *Для каждого* $n \geqslant 1$

$$\text{из } a \equiv b \bmod p^n \text{ следует } a^p \equiv b^p \bmod p^{n+1}.$$

Доказательство. Предположение $a \equiv b \bmod p^n$ означает

$$a = b + gp^n \text{ с целым (соответственно } p\text{-целым) } g.$$

Тогда по правилу разложения бинома

$$a^p = b^p + \binom{p}{1} b^{p-1} g p^n + \ldots + \binom{p}{p-1} b g^{p-1} p^{(p-1)n} + g^p p^{pn}.$$

Вследствие делимости средних биномиальных коэффициентов на p (см. XIV, п. 11, § 4) и принимая во внимание, что при $n \geqslant 1$ $pn \geqslant n+1$, мы получаем отсюда наше утверждение $a^p \equiv b^p \bmod p^{n+1}$.

Из леммы 1 посредством повторного ее применения (полной индукцией) немедленно получается:

Лемма 2. *Для каждого* $\nu \geqslant 1$

$$\text{из } c \equiv 1 \bmod p^\nu \text{ следует } c^{p^{\mu-\nu}} \equiv 1 \bmod p^\mu \text{ для всех } \mu \geqslant \nu.$$

Мы будем применять лемму 2 только в следующем специальном случае:

$$\nu = 1 \text{ для } p \neq 2, \qquad \nu = 2 \text{ для } p = 2.$$

В этом специальном случае она будет видоизменена посредством уточнения предположения и соответствующего уточнения утверждения следующим образом.

Лемма 3. *Для* $p \neq 2$

$$\text{из } c \equiv 1 + gp \bmod p^2 \text{ следует } c^{p^{\mu-1}} \equiv 1 + gp^{\mu} \bmod p^{\mu+1}$$

$$\text{для всех } \mu \geqslant 1.$$

Для $p = 2$

$$\text{из } c \equiv 1 + g2^2 \bmod 2^3 \text{ следует } c^{2^{\mu-2}} \equiv 2 + g2^{\mu} \bmod 2^{\mu+1}$$

$$\text{для всех } \mu \geqslant 2.$$

Заметим, что в этом высказывании нам не важно само g, а важен только класс вычетов $g \bmod p$.

Доказательство. Мы применим полную индукцию по μ. Для $\mu = 1$, соответственно $\mu = 2$, утверждения тривиальны. Если предположить их верными для $\mu \geqslant 1$, соответственно $\mu \geqslant 2$, то прежде всего из имеющих, по предположению, место сравнений по лемме 1 следует

$$\text{для } p \neq 2: \quad c^{p^{\mu}} \equiv (1 + gp^{\mu})^p \bmod p^{\mu+2},$$

$$\text{для } p = 2: \quad c^{2^{\mu-1}} \equiv (1 + g2^{\mu})^2 \bmod 2^{\mu+2}.$$

Но теперь, аналогично доказательству леммы 1,

$$\text{для } p \neq 2: \quad (1 + gp^{\mu})^p = 1 + \binom{p}{1} gp^{\mu} + \ldots + \binom{p}{p-1} g^{p-1} p^{(p-1)\mu} + g^p p^{p\mu} \equiv 1 + gp^{\mu+1} \bmod p^{\mu+2},$$

так как тогда $p\mu \geqslant 3\mu \geqslant \mu + 2$ для $\mu \geqslant 1$;

$$\text{для } p = 2: \quad (2 + g2^{\mu})^2 = 1 + 2g\,2^{\mu} + g^2 2^{2\mu} \equiv 1 + g2^{\mu+1} \bmod 2^{\mu+2},$$

так как $2\mu \geqslant \mu + 2$ для $\mu \geqslant 2$.

Вместе получаются, таким образом, доказываемые сравнения для $\mu + 1$. Тем самым правильность утверждений доказана полной индукцией.

Заметим, что в нашем заключении относительно последнего члена биномиального разложения в случае $p \neq 2$ это предположение существенно используется в форме $p \geqslant 3$; для $p = 2$ это заключение неверно при $\mu = 1$. Поэтому необходимо различать в формулировке леммы 3 оба случая $p \neq 2$ и $p = 2$.

6. Случай степени нечетного простого числа. Теперь мы сконструируем, сначала для $p \neq 2$, уже упомянутое выше раз-

ложение группы $\mathfrak{P}_\mu$ порядка $\varphi(p^\mu) = (p-1)\,p^{\mu-1}$ в прямое произведение двух циклических групп $\mathfrak{P}'_\mu$, $\mathfrak{P}''_\mu$ порядков $p-1$, $p^{\mu-1}$. Для этого мы определим для каждого класса вычетов $a \bmod p^\mu$, взаимно простого с модулем, разложение на произведение

$$a \equiv bc \bmod p^\mu \tag{1}$$

двух компонент b, $c \bmod p^\mu$ посредством формул

$$b \equiv a^{p^{\mu-1}}, \qquad c \equiv a^{1-p^{\mu-1}} \bmod p^\mu, \tag{2}$$

и докажем следующий ряд фактов:

а) *Если $a \bmod p^\mu$ пробегает группу $\mathfrak{P}_\mu$, то b, $c \bmod p^\mu$ пробегают некоторые подгруппы $\mathfrak{P}'_\mu$, $\mathfrak{P}''_\mu$.*

Доказательство. Согласно (2), умножению и делению классов вычетов $a \bmod p^\mu$ соответствует, очевидно, умножение и деление компонент b, $c \bmod p^\mu$. Таким образом, пробегаемые ими подмножества $\mathfrak{P}'_\mu$, $\mathfrak{P}''_\mu$ группы $\mathfrak{P}_\mu$ замкнуты относительно умножения и деления и потому действительно являются подгруппами.

б) *Подгруппы $\mathfrak{P}'_\mu$, $\mathfrak{P}''_\mu$ характеризуются также свойствами*

$$b^{p-1} \equiv 1 \bmod p^\mu, \qquad c \equiv 1 \bmod p, \tag{3}$$

т. е. состоят из совокупностей всех b, $c \bmod p^\mu$ с этими свойствами.

Доказательство. То, что свойства (3) следуют из формул (2), легко увидеть на основании малой теоремы Ферма:

из $b \equiv a^{p^{\mu-1}} \bmod p^\mu$ следует $b^{p-1} \equiv a^{(p-1)\,p^{\mu-1}} \equiv a^{\varphi(p^\mu)} \equiv 1 \bmod p^\mu$,

из $c \equiv a^{1-p^{\mu-1}} \bmod p^\mu$ следует $c \equiv 1 \bmod p$,

последнее ввиду того, что $a^p \equiv a \bmod p$, а потому имеет место также $a^{p^{\mu-1}} \equiv a \bmod p$.

То, что, обратно, из свойств (3) следует существование формул (2) с подходящим образом подобранным классом вычетов $a \bmod p^\mu$, а именно, просто $a \equiv b$, соответственно $c \bmod p^\mu$, можно увидеть так:

из $b^{p-1} \equiv 1 \bmod p^\mu$ следует $b \equiv b^p \bmod p^\mu$

и потому также $b \equiv b^{p^{\mu-1}} \bmod p^\mu$.

из $c \equiv 1 \bmod p$ следует $c^{p^{\mu-1}} \equiv 1 \bmod p^\mu$ (см. лемму 2)

и, таким образом $c \equiv c^{1-p^{\mu-1}} \bmod p^\mu$.

в) *Подгруппы $\mathfrak{P}'_\mu$, $\mathfrak{P}''_\mu$ имеют порядки $p-1$, $p^{\mu-1}$.*

Доказательство. Для группы $\mathfrak{P}''_\mu$ это видно из того, что на основании характеристического свойства (3) ее элементы задаются, по XV, п. 12, § 4, в однозначном представлении в виде

$c \equiv 1 + c_1 p + \ldots + c_{\mu-1} p^{\mu-1} \bmod p^\mu$ с $c_1, \ldots, c_{\mu-1}$ из наименьшей системы вычетов по $\bmod p$, и потому, действительно, их количество равно $p^{\mu-1}$.

Для группы $\mathfrak{P}'_\mu$ это следует из ее получения в (2). Именно, если $a \bmod p^\mu$ будет пробегать там группу $\mathfrak{P}_\mu$, то во-первых, получающиеся классы вычетов $b \bmod p^\mu$ зависят, по лемме 2, только от класса вычетов $a \bmod p$ и, во-вторых, согласно (3), $b \equiv a \bmod p$. Так как для $a \bmod p$ имеется точно $p-1$ различных возможностей, то различных возможностей для $b \bmod p^\mu$, в силу первого факта, будет самое большее $p-1$, а в силу второго факта—самое меньшее $p-1$, так что количество различных $b \bmod p^\mu$ в самом деле равно точно $p-1$.

г) *Разложение* (1), *определяемое формулами* (2), *может быть также однозначно охарактеризовано как разложение элементов из* $\mathfrak{P}_\mu$ *на две компоненты из* $\mathfrak{P}'_\mu$, $\mathfrak{P}''_\mu$, *т. е. группа* $\mathfrak{P}_\mu$ *есть прямое произведение обеих подгрупп* $\mathfrak{P}'_\mu$, $\mathfrak{P}''_\mu$.

Доказательство. Теперь это получается просто посредством подсчета. Согласно «в», имеется $(p-1)\,p^{\mu-1}$ произведений некоторого элемента из $\mathfrak{P}'_\mu$ на некоторый элемент из $\mathfrak{P}''_\mu$. В силу «а», каждый из $\varphi(p^\mu)$ элементов группы $\mathfrak{P}_\mu$ встречается среди этих произведений хотя бы один раз. Поэтому, вследствие равенства $(p-1)\,p^{\mu-1} = \varphi(p^\mu)$, произведения элементов из $\mathfrak{P}'_\mu$ на элементы из $\mathfrak{P}''_\mu$ дают каждый элемент группы $\mathfrak{P}_\mu$ точно один раз, т. е. не существует никаких других разложений элемента из $\mathfrak{P}_\mu$ на компоненты из $\mathfrak{P}'_\mu$, $\mathfrak{P}''_\mu$, кроме построенного в (1), (2).

д) *Компонента* $b \bmod p^\mu$ *из* $\mathfrak{P}'_\mu$ *класса вычетов* $a \bmod p^\mu$ *из* $\mathfrak{P}_\mu$, *т. е. класс вычетов* $b \equiv a^{p^{\mu-1}} \bmod p^\mu$, *может быть также однозначно охарактеризована свойствами*

$$b \equiv a \bmod p, \qquad b^{p-1} \equiv 1 \bmod p^\mu.$$

Доказательство. То, что компонента обладает обоими этими свойствами, уже было установлено. То, что этими свойствами она характеризуется однозначно, можно увидеть так. Из второго свойства следует, как в доказательстве «б», что $b \equiv b^{p^{\mu-1}} \bmod p^\mu$, а тогда, далее, из первого свойства вытекает по лемме 2, что $b \equiv a^{p^{\mu-1}} \bmod p^\mu$.

а) *Подгруппы* $\mathfrak{P}'_\mu$, $\mathfrak{P}''_\mu$ *цикличны, и притом они порождаются:* $\mathfrak{P}'_\mu$—*посредством образованного из какого-нибудь первообразного корня* $w_0 \bmod p$ *класса вычетов* $w \equiv w_0^{p^{\mu-1}} \bmod p^\mu$, *однозначно характеризуемого также свойствами*

$$w \equiv w_0 \bmod p, \qquad w^{p-1} \equiv 1 \bmod p^\mu,$$

$\mathfrak{P}''_\mu$—*посредством какого-нибудь класса вычетов вида* $1 + gp \bmod p^\mu$ *с* $g \not\equiv 0 \bmod p$, *например, посредством* $1 + p \bmod p^\mu$.

Доказательство. Классы вычетов, относительно которых утверждается, что они порождают подгруппы $\mathfrak{P}'_\mu$, $\mathfrak{P}''_\mu$, в силу (2), соответственно (3), принадлежат этим подгруппам. Тогда, согласно «в», достаточно еще только показать, что их порядки не являются собственными делителями чисел $p-1$, соответственно $p^{\mu-1}$.

Для $\mathfrak{P}''_\mu$ это есть следствие из леммы 3; действительно, согласно этой лемме, для наибольшего собственного делителя $p^{\mu-2}$ числа $p^{\mu-1}$ будет $(1+gp)^{p^{\mu-2}} \equiv 1+gp^{\mu-1} \not\equiv 1 \bmod p^\mu$ (заметим, что здесь предполагается $\mu \geqslant 2$).

Для $\mathfrak{P}'_\mu$, вследствие того, что $w \equiv w_0 \bmod p$, мы для каждого собственного делителя d числа $p-1$ заведомо будем иметь $w^d \equiv w_0^d \not\equiv 1 \bmod p$, а потому и подавно $w^d \not\equiv 1 \bmod p^\mu$.

Ввиду всего этого мы можем установить:

III. *Классы вычетов* $a \bmod p^\mu$, *взаимно простые с модулем*, ($p \neq 2$, $\mu > 1$) *однозначно представляются через базисные классы в виде*

$$a \equiv w^{\alpha'}(1+p)^{\alpha''} \bmod p^\mu \left\{ \begin{array}{l} \alpha' \bmod p-1 \\ \alpha'' \bmod p^{\mu-1} \end{array} \right\},$$

где w *есть первообразный корень по* $\bmod p$, *нормированный так, что* $w^{p-1} \equiv 1 \bmod p^\mu$.

Так нормированный первообразный корень по $\bmod p$ *можно получить исходя из какого-нибудь первообразного корня* $w_0 \bmod p$ *в виде* $w \equiv w_0^{p^{\mu-1}} \bmod p^\mu$.

При таком представлении через базис мультипликативным операциям с классами вычетов $a \bmod p^\mu$, взаимно простыми с модулем, соответствуют почленные аддитивные операции с показателями $\alpha' \bmod p-1$, $\alpha'' \bmod p^{\mu-1}$.

Отметим еще следующий важный для приложений факт. Базис w, $1+p$ группы $\mathfrak{P}_\mu$ является одновременно базисом всех групп $\mathfrak{P}_\nu$ с $1 < \nu \leqslant \mu$; действительно, если нормирующее условие выполняется для w по $\bmod p^\mu$, то оно и подавно выполняется для w по $\bmod p^\nu$. Переход от представления через базис для $a \bmod p^\mu$ к представлению через базис для $a \bmod p^\nu$ осуществляется попросту тем, что классы вычетов $\alpha'' \bmod p^{\mu-1}$ заменяются классами вычетов $\alpha'' \bmod p^{\nu-1}$, т. е. выбрасываются из рассмотрения последние $\mu-\nu$ цифр в p-адическом представлении $\alpha'' \equiv \alpha_0 + \alpha_1 p + \ldots + \alpha_{\mu-2} p^{\mu-2} \bmod p^{\mu-1}$. Изложенный в п. 2 случай $\mu = 1$ может рассматриваться как частный случай, так как тогда базисный элемент $1+p$ будет $\equiv 1 \bmod p$, а его показатель сведется к $\alpha'' \equiv 0 \bmod 1$. Мы отметим еще следующий часто используемый факт:

IV. *Группы* $\mathfrak{P}_\mu$ ($p \neq 2$) *сами являются циклическими, а именно, они порождаются первообразным корнем* $\bar{w} \bmod p$ *с нормированием* $\bar{w}^{p-1} \not\equiv 1 \bmod p^2$.

В самом общем виде такой первообразный корень получается из нормированного по III *первообразного корня* $w \bmod p$ *в форме*

$$\bar{w} \equiv w(1+p)^{\omega} \equiv w(1+\omega p) \bmod p^2 \text{ с } \omega \not\equiv 0 \bmod p$$

(*или, что то же самое, в форме* $w \equiv \bar{w} + gp \bmod p^2$ с $g \not\equiv 0 \bmod p$).

Классы вычетов $a \bmod p^{\mu}$, *взаимно простые с модулем, однозначно представляются тогда через базисный класс в виде*

$$a \equiv \bar{w}^{\alpha} \bmod p^{\mu} \quad (\alpha \bmod (p-1)\,p^{\mu-1}).$$

Доказательство. Если $\bar{w}$ построено указанным образом, то

$$\bar{w}^{p-1} \equiv w^{p-1}(1+p)^{(p-1)\omega} \equiv 1 + (p-1)\omega p \equiv 1 - \omega p \bmod p^2$$

(последнее получается разложением бинома). Тогда для $\omega \not\equiv 0 \bmod p$, и только в этом случае, нормирующее условие $\bar{w}^{p-1} \not\equiv 1 \bmod p^2$ действительно будет выполняться.

Нам нужно показать теперь, что для каждого $\mu > 1$ класс вычетов $\bar{w} \bmod p^{\mu}$ имеет порядок $\varphi(p^{\mu}) = (p-1)\,p^{\mu-1}$, т. е. порождает всю группу $\mathfrak{P}_{\mu}$. Представление класса $\bar{w} \bmod p^{\mu}$ через базис, согласно замеченному перед этим, имеет вид

$$\bar{w} \equiv w(1+p)^{\omega_{\mu}} \bmod p^{\mu}$$

с некоторым классом вычетов $\omega_{\mu} \bmod p^{\mu-1}$, для которого имеет место $\omega_{\mu} \equiv \omega \not\equiv 0 \bmod p$. Для любой степени с целым показателем x отсюда получается следующее представление через базис:

$$\bar{w}^{x} \equiv w^{x}(1+p)^{x\omega_{\mu}} \bmod p^{\mu}.$$

Ввиду однозначности представления через базис, $\bar{w}^{x} \equiv 1 \bmod p^{\mu}$ будет иметь место тогда и только тогда, когда одновременно $x \equiv 0 \bmod p-1$, $x\omega_{\mu} \equiv 0 \bmod p^{\mu-1}$. Однако, вследствие того что $\omega_{\mu} \not\equiv 0 \bmod p-1$ и $p-1$ взаимно просто с $p^{\mu-1}$, это будет тогда и только тогда, когда $x \equiv 0 \bmod (p-1)\,p^{\mu-1}$. Таким образом, согласно VIII, п., 5, § 4, $\bar{w} \bmod p^{\mu}$ действительно имеет порядок $(p-1)\,p^{\mu-1}$.

В основе того факта, что $\mathfrak{P}_{\mu}$ сама циклична, лежит, впрочем, общая теоретико-групповая теорема, согласно которой прямое произведение конечного множества циклических групп с попарно взаимно простыми порядками $m_1, \ldots, m_r$ само циклично. Эта теорема является непосредственным следствием из рассмотренного в § 4, п. 9, разложения кольца классов вычетов по $\bmod m_1 \ldots m_r$ в прямую сумму, если мы, сообразно с § 4, п. 5, заменим циклические группы изоморфными им аддитивными группами классов вычетов по $\bmod m_1, \ldots, \bmod m_r$.

Примеры. Для $p=3$ нормирующее условие из III при каждом показателе μ выполняется, очевидно, для $w=-1$. Представление через базис из III имеет тогда вид

$$a \equiv (-1)^{\alpha'} 4^{\alpha''} \bmod 3^{\mu} \left\{ \begin{matrix} \alpha' \bmod 2 \\ \alpha'' \bmod 3^{\mu-1} \end{matrix} \right\}.$$

Так, для $\mu=2$ получается таблица

$a \bmod 3^2$	$\alpha' \bmod 2$	$\alpha'' \bmod 3$
1	0	0
4	0	1
7	0	2
$-1 \equiv 8$	1	0
$-4 \equiv 5$	1	1
$-7 \equiv 2$	1	2

Нормирующее условие из IV выполняется, очевидно, для $w=2$. Соответствующая таблица для $\mu=2$ будет такова:

$a \equiv 2^{\alpha} \bmod 3^2$	$\alpha \bmod 6$
1	0
2	1
4	2
8	3
7	4
5	5

Для $p=5$, $\mu=2$, исходя из первообразного корня $2 \bmod 5$, мы получим, что нормирующее условие из III выполняется для $w \equiv 2^5 \equiv 7 \bmod 5^2$, а нормирующее условие из IV, напротив, для каждого из четырех других нормирований $w \equiv 2,\ 12,\ 17,\ 22 \bmod 5^2$.

7. Случай степени простого числа 2. Теперь мы сконструируем, наконец, для $p=2$ уже упомянутое разложение группы $\mathfrak{P}_\mu$ порядка $\varphi(2^\mu)=2^{\mu-1}$ в прямое произведение двух циклических групп $\mathfrak{P}'_\mu$, $\mathfrak{P}''_\mu$ порядков 2, $2^{\mu-2}$. При этом мы можем быть

значительно более краткими, так как здесь имеет место такое же положение вещей, которое уже встретилось нам выше в примере $p=3$, а именно, сомножитель $\mathfrak{P}'_\mu$, который в общем случае для $p\neq 2$ и создавал нам как раз наибольшие трудности, теперь при *любом показателе* μ *порождается одним и тем же числом* -1.

Для $\mu=2$ группа $\mathfrak{P}_2$—циклическая порядка $\varphi(2^2)=2$ и состоит из обоих классов вычетов $a\equiv\pm 1 \bmod 2^2$, взаимно простых с модулем. Они однозначно представляются через базисный класс в виде

$$a\equiv(-1)^{\alpha'} \bmod 2^2 \qquad (\alpha' \bmod 2).$$

Отсюда следует, что каждое взаимно простое с 2 число a [целое или также только рациональное (см. § 4, п. 10)] обладает однозначным разложением вида

$$a=(-1)^{\alpha'}a^* \quad \text{с} \quad a^*\equiv 1 \bmod 2^2,$$

которое формально аналогично существующему для каждого рационального числа однозначному разложению

$$a=(-1)^{\alpha}|a| \quad \text{с} \quad |a|>0$$

на множитель, определяющий знак, и абсолютную величину, только здесь вместо нормирования $|a|>0$, связанного с понятием величины, фигурирует нормирование $a^*\equiv 1 \bmod 2^2$, связанное с понятием сравнимости. В дальнейшем мы в нашем изложении все время будем придерживаться введенного здесь обозначения a^* и будем применять его обычно также и в численных примерах, как, например, $3^*=-3$, $5^*=5$, $(-1)^*=1$.

Точно так же получается, что каждый класс вычетов $a \bmod 2^\mu$, взаимно простой с модулем, обладает однозначным разложением

$$a\equiv(-1)^{\alpha'}a^* \bmod 2^\mu \qquad (\alpha' \bmod 2),$$

где первый множитель принадлежит порожденной классом вычетов $-1 \bmod 2^\mu$ циклической подгруппе $\mathfrak{P}'_\mu$ порядка 2 группы $\mathfrak{P}_\mu$, а второй множитель — подгруппе $\mathfrak{P}''_\mu$ порядка $2^{\mu-2}$, которая состоит из всех классов вычетов по $\bmod 2^\mu$, лежащих в классе вычетов $1 \bmod 2^2$, т. е. из всех классов вычетов вида $1+0\cdot 2+a_2 2^2+\ldots+a_{\mu-1}2^{\mu-1} \bmod 2^\mu$ с $a_2, \ldots, a_{\mu-1}$ из наименьшей системы вычетов $0, 1 \bmod 2$.

Тем самым мы имеем аналогию с рассмотренным в п. 6 разложением (1), (2) и доказанными там относительно него высказываниями «а», «б», «в» — только здесь отпадает первое из соотношений (3), относящееся к $\mathfrak{P}^\mu$, ввиду отклоняющегося от (2) установления разложения (1) — и аналогично «г» мы можем вывести, что группа $\mathfrak{P}_\mu$ является прямым произведением обеих

подгрупп $\mathfrak{P}'_\mu$, $\mathfrak{P}''_\mu$; при этом для $\mu = 2$ речь идет о тривиальном разложении с $\mathfrak{P}'_2 = \mathfrak{P}_2$, $\mathfrak{P}''_2 = 1$.

Об эквивалентности первого из соотношений (3) и связанного с ним высказывания «д» мы будем говорить позднее. Аналогично «е» и здесь получается, что наряду с циклической подгруппой $\mathfrak{P}'_\mu$ порядка 2 подгруппа $\mathfrak{P}''_\mu$ порядка $2^{\mu-2}$ тоже циклична и притом порождается каким-нибудь классом вычетов вида $1 + g\,2^2 \bmod 2^\mu$ с $g \not\equiv 0 \bmod 2$, в частности, например, классом вычетов $1 + 2^2 \equiv 5 \bmod 2^\mu$; действительно, если $\mu \geqslant 3$ (для $\mu = 2$ нечего и доказывать), то, согласно лемме 3, для наибольшего собственного делителя $2^{\mu-3}$ числа $2^{\mu-2}$ заведомо будет $(1+g\,2^2)^{2^{\mu-3}} \equiv$ $\equiv 1 + g\,2^{\mu-1} \not\equiv 1 \bmod 2^\mu$.

Тем самым доказан факт, в значительной степени, но не полностью аналогичный III, п. 6:

V. *Классы вычетов* $a \bmod 2^\mu$, *взаимно простые с модулем*, $(\mu > 2)$ *однозначно представляются через базисные классы в виде*

$$a \equiv (-1)^{\alpha'} 5^{\alpha''} \bmod 2^\mu \left\{ \begin{matrix} \alpha' \bmod 2 \\ \alpha'' \bmod 2^{\mu-2} \end{matrix} \right\}.$$

Мультипликативным операциям с классами вычетов $a \bmod 2^\mu$, взаимно простыми с модулем, соответствуют при этом аддитивные операции с показателями $\alpha' \bmod 2$, $\alpha'' \bmod 2^{\mu-2}$. Из представления через базис для $a \bmod 2^\mu$ представление через базис для $a \bmod 2^\nu$ с $2 < \nu \leqslant \mu$ получается просто посредством замены класса вычетов $\alpha'' \bmod 2^{\mu-2}$ классом вычетов $\alpha'' \bmod 2^{\mu-2}$, т. е. выбрасыванием из рассмотрения последних $\mu - \nu$ цифр в 2-адическом представлении $\alpha'' \equiv \alpha_0 + \alpha_1 2 + \ldots + \alpha_{\mu-3} 2^{\mu-3} \bmod 2^{\mu-2}$. В случае $\mu = 2$ базисный элемент 5 будет $\equiv 1 \bmod 2^2$, а его показатель сведется к $\alpha'' \equiv 0 \bmod 1$. В случае $\mu = 1$ также и базисный элемент -1 будет $\equiv 1 \bmod 2$; здесь получается группа $\mathfrak{P}_1 = \mathfrak{P} = 1$.

Высказывание IV, п. 6 для $p = 2$ перестает быть верным; действительно, если $\mu > 2$, то, согласно V, для каждого класса вычетов $a \bmod 2^\mu$, взаимно простого с модулем, имеет место сравнение $a^{2^{\mu-2}} \equiv 1 \bmod 2^\mu$, так что в $\mathfrak{P}_\mu$ нет ни одного элемента порядка $\varphi(2^\mu) = 2^{\mu-1}$. Таким образом, для $p = 2$ среди групп $\mathfrak{P}_\mu$ циклической является только $\mathfrak{P}_2$ (и тривиальным образом также и $\mathfrak{P}_i = 1$).

Рассмотрим, наконец, вопрос об эквивалентности данных в (3) и «д» п. 6 характеристик первой компоненты разложения, которая в нашем случае представления V через базис равна $(-1)^{\alpha'}$. По определению разложения $a = (-1)^{\alpha'} a^*$, $\alpha' \equiv 0$ или

$1 \bmod 2$, в зависимости от того, $a \equiv 1$ или $-1 \bmod 2^2$, или также $\frac{a-1}{2} \equiv 0$ или $1 \bmod 2$. Поэтому класс вычетов $\alpha' \bmod 2$ однозначно получается из класса вычетов $a \bmod 2^2$ посредством формулы

$$\alpha' \equiv \frac{a-1}{2} \bmod 2. \tag{1}$$

Поэтому мы можем данное выше определение числа a^* записать также в форме

$$a = (-1)^{\frac{a-1}{2}} a^*$$

аналогично способу записи

$$a = \operatorname{sgn} a \cdot |a|$$

для определения абсолютной величины $|a|$.

Аналогичная (1) формула может быть получена также и для значения по $\bmod 2$ показателя α'' второй компоненты $a^* \equiv 5^{\alpha''} \bmod 2^\mu$ нашего представления V через базис. Согласно сделанному после V замечанию, это значение однозначно определяется уже классом вычетов $a \bmod 2^3$, или также $a^* \bmod 2^3$, и при этом $\alpha'' = 0$ или $1 \bmod 2$, в зависимости от того, $a^* \equiv 1$ или $5 \bmod 2^3$, или также $\frac{a^*-1}{4} \equiv 0$ или $1 \bmod 2$. Поэтому класс вычетов $\alpha'' \bmod 2$ однозначно получается из класса вычетов $a \bmod 2^3$, посредством формулы

$$\alpha'' \equiv \frac{a^*-1}{4} \equiv \frac{(-1)^{\frac{a-1}{2}} a - 1}{4} \bmod 2. \tag{2}$$

При применениях высказывания V большей частью используется только специальный случай $\mu = 3$ группы классов вычетов по $\bmod 8$, взаимно простых с модулем. В этом случае классы вычетов $a \bmod 8$, взаимно простые с модулем, в свою очередь полностью описываются выраженной в (1), (2) в виде формул парой классов вычетов $\alpha', \alpha'' \bmod 2$ (в то время как для $\mu > 3$ необходимо знать более точное значение $\alpha'' \bmod 2^{\mu-2}$). Поэтому само представление через базис может задаваться в форме

$$a \equiv (-1)^{\frac{a-1}{2}\frac{a^*-1}{4}} 5^{\frac{a^*-1}{4}} \bmod 8.$$

Обе эти функции $\frac{a-1}{2}$, $\frac{a^*-1}{4} \bmod 2$ класса вычетов $a \bmod 8$, взаимно простого с модулем, будут играть важную роль в следующей главе. Последняя из них может быть также представлена в форме

$$\frac{a^*-1}{4} \equiv \frac{a^2-1}{8} \bmod 2,$$

в которой она все время давалась в прежней литературе по теории чисел. В самом деле, для квадрата каждого взаимно простого с 2 числа $a = 1 + 2g$ имеет место

$$a^2 = 1 + 4g(g+1) \equiv 1 \bmod 8$$

[что ясно также из представления V через базис (см. приведенное выше общее сравнение $a^{2^{\mu-2}} \equiv 1 \bmod 2^\mu$)], и если положить $a^* = 1 + 4g'$, то получается более точно

$$a^2 = a^{*2} = 1 + 8g' + 16g'^2 \equiv 1 + 8g' \bmod 16$$

и потому

$$\frac{a^2-1}{8} \equiv g' \equiv \frac{a^*-1}{4} \bmod 2.$$

Глава II

КВАДРАТИЧНЫЕ ВЫЧЕТЫ

§ 6. ОПРЕДЕЛЕНИЕ, РЕДУКЦИЯ К ПРОСТЕЙШИМ СЛУЧАЯМ, КРИТЕРИИ

1. Определение квадратичных вычетов. Одной из наиболее красивых глав элементарной теории чисел, давшей к тому же существенный толчок к развитию высшей теории чисел, является теория квадратичных вычетов. Она берет свое начало в вопросе о том, для каких классов вычетов $a \bmod m$, взаимно простых с модулем ($m \neq 1$ — данное натуральное число), квадратное сравнение

$$x^2 \equiv a \bmod m$$

разрешимо посредством некоторого класса вычетов $x \bmod m$ (который тогда тоже взаимно прост с модулем), или, другими словами, какие элементы $a \bmod m$ из группы классов вычетов по $\bmod m$, взаимно простых с модулем, являются квадратами в этой группе. В зависимости от того, имеет это место или нет, a называется *квадратичным вычетом или квадратичным невычетом по* $\bmod m$.

Как мы увидим, с помощью результатов § 5 этот вопрос можно свести к случаям, когда или $m = p \neq 2$ (простое нечетное), или $m = 8$, и в последнем случае решить его непосредственно, а в первом случае дать для его решения простые критерии. Однако еще не в этом заключается интерес и значение самой теории. Они состоят в возможности обратить постановку нашего вопроса, подобно тому, как мы это делали в § 5, п. 3 для вопроса о первообразных корнях $w \bmod p$. Именно, мы зададимся вопросом о том, для каких простых p заданное целое число $a \neq 0$ является квадратичным вычетом по $\bmod p$. В то время как для первообразных корней такой обратный вопрос приводит к недоказанной до сих пор гипотезе Артина, для квадратичных вычетов он допускает полное и замечательное по своей своеобразной форме решение, составляющее собственно содержание этой теории.

Вместе с основным рассматриваемым вопросом о разрешимости сравнения $x^2 \equiv a \bmod m$ нас будут интересовать и сами решения $x \bmod m$, в частности, их количество, последнее, впрочем, в дальнейшем развитии теории отступает на задний план. Количество

решений сравнения $x^2 \equiv a \bmod m$ мы будем обозначать через $N_a(m)$. Если речь будет идти о квадратичных вычетах или невычетах $a \bmod m$ или о количестве решений $N_a(m)$, мы все время будем предполагать, что a взаимно просто с m, не оговаривая этого каждый раз.

2. Редукция к модулям, являющимся степенями простых чисел. Пусть

$$m = \prod_{i=1}^{r} p_i^{\mu_i} \qquad (r > 0,\ \mu_i > 0)$$

есть разложение данного натурального числа $m \neq 1$ на простые множители. На основании установленного в § 5, п. 1 разложения группы классов вычетов по $\bmod m$, взаимно простых с модулем, в прямое произведение групп классов вычетов по $\bmod p_i^{\mu_i}$, взаимно простых с модулем, класс вычетов $a \bmod m$, взаимно простой с модулем, является квадратом тогда и только тогда, когда являются квадратами его компоненты $a \bmod p_i^{\mu_i}$. Согласно изложенному в § 4, п. 9 аппарату этого разложения, решения $x \bmod m$ сравнения $x^2 \equiv a \bmod m$ взаимно однозначно соответствуют при этом системам решений $x_i \bmod p_i^{\mu_i}$ сравнений $x_i^2 \equiv a \bmod p_i^{\mu_i}$, в силу имеющей место системы сравнений $x \equiv x_i \bmod p_i^{\mu_i}$. Поэтому мы имеем:

I. *Число a является квадратичным вычетом по $\bmod m$ тогда и только тогда, когда a есть квадратичный вычет по $\bmod p_i^{\mu_i}$ для каждой степени простого числа $p_i^{\mu_i}$, входящей в m.*

При этом для количества решений имеет место мультипликативная формула

$$N_a(m) = \prod_{i=1}^{r} N_a(p_i^{\mu_i}).$$

3. Редукция к нечетным простым модулям. Пусть теперь $m = p^{\mu}$ есть степень простого числа p. Мы будем основываться на выведенном в § 5, п. 6, 7 представлении группы классов вычетов по $\bmod p^{\mu}$, взаимно простых с модулем, через базис, и потому должны различать случаи $p \neq 2$ и $p = 2$.

а) $p \neq 2$

В этом случае наше представление через базис имеет вид (см. III, п. 6, § 5):

$$a \equiv w^{\alpha'} (1+p)^{\alpha''} \bmod p^{\mu} \left\{ \begin{array}{l} \alpha' \bmod p - 1 \\ \alpha'' \bmod p^{\mu-1} \end{array} \right\},$$

где w — первообразный корень по $\bmod p$ с нормированием $w^{p-1} \equiv 1 \bmod p^\mu$. Если соответственно положить

$$x \equiv w^{\xi'} (1+p)^{\xi''} \bmod p^\mu \left\{ \begin{array}{c} \xi' \bmod p-1 \\ \xi'' \bmod p^{\mu-1} \end{array} \right\},$$

то, ввиду однозначности представления через базис, выполнение рассматриваемого сравнения $x^2 \equiv a \bmod p^\mu$ будет равносильно выполнению двух сравнений для показателей

$$2\xi' \equiv \alpha' \bmod p-1, \quad 2\xi'' \equiv \alpha'' \bmod p^{\mu-1}.$$

Условия, необходимые для разрешимости этих сравнений, согласно V п. 3 § 3, гласят:

$$\alpha' \equiv 0 \bmod (2,\ p-1) \qquad \alpha'' \equiv 0 \bmod (2,\ p^{\mu-1}).$$

В нашем случае, так как

$$(2,\ p-1) = 2, \quad (2,\ p^{\mu-1}) = 1,$$

эти условия сводятся к одному

$$\alpha' \equiv 0 \bmod 2.$$

Если это последнее условие выполняется, то, согласно V п. 3 § 4, существуют два решения ξ', $\xi' + (p-1)/2 \bmod p-1$ и одно решение $\xi'' \bmod p^{\mu-1}$. Им соответствуют тогда два решения вида $\pm x \bmod p^\mu$ рассматриваемого сравнения.

Очевидно, что если это сравнение вообще обладает решением $x \bmod p^\mu$, то решением является и противоположный класс вычетов $-x \bmod p^\mu$. Оба эти решения действительно различны, так как $1 \not\equiv -1 \bmod p^\mu$ для $p^\mu \neq 2$. Существование такой пары решений получается также и при данном выше формальном способе вывода, если заметить, что нормированный по $\bmod p^\mu$ первообразный корень $w \bmod p$ имеет свойство

$$w^{\frac{p-1}{2}} \equiv -1 \bmod p^\mu.$$

Это немедленно получается из разложения

$$0 \equiv w^{p-1} - 1 \equiv (w^{\frac{p-1}{2}} - 1)(w^{\frac{p-1}{2}} + 1) \bmod p^\mu,$$

в котором, ввиду первообразности $w \bmod p$, первый множитель

$$w^{\frac{p-1}{2}} - 1 \not\equiv 0 \bmod p,$$

т. е. взаимно прост с p^μ. Поэтому паре решений

$$\xi',\ \xi' + (p-1)/2 \bmod p-1$$

(вместе с $\xi'' \bmod p^{\mu-1}$) действительно соответствует пара решений вида $\pm x \bmod p^\mu$.

Согласно замечанию к III п. 6 § 5, выполнение сравнения $a' \equiv 0 \bmod 2$ является также условием разрешимости для каждого из сравнений $x^2 \equiv a \bmod p^\nu$ с $1 \leqslant \nu \leqslant \mu$, в частности также для $\nu = 1$. Таким образом, мы имеем следующий общий результат.

IIa. *В случае* $p \neq 2$ *число* a *является квадратичным вычетом по* $\bmod p^\mu$ $(\mu \geqslant 1)$ *тогда и только тогда, когда* a *есть квадратичный вычет по* $\bmod p$.

Если это имеет место, то

$$N_a(p^\mu) = N_a(p) = 2,$$

т. е. сравнение $x^2 \equiv a \bmod p^\mu$ *имеет два решения; они имеют вид* $\pm x \bmod p^\mu$.

б) $p = 2$

Мы можем оставить в стороне тривиальный случай $\mu = 1$, когда единственный класс вычетов $a \equiv 1 \bmod 2$, взаимно простой с модулем, является квадратичным вычетом, число решений $N_a(2) = 1$ и единственное решение есть $x \equiv 1 \bmod 2$.

Итак, мы предполагаем $\mu \geqslant 2$. Тогда представление через базис гласит (см. V п. 7 § 5):

$$a \equiv (-1)^{\alpha'} 5^{\alpha''} \bmod 2^\mu \left\{ \begin{array}{l} \alpha' \bmod 2 \\ \alpha'' \bmod 2^{\mu-2} \end{array} \right\}.$$

Если положить соответственно

$$x \equiv (-1)^{\xi'} 5^{\xi''} \bmod 2^\mu \left\{ \begin{array}{l} \xi' \bmod 2 \\ \xi'' \bmod 2^{\mu-2} \end{array} \right\},$$

то, аналогично предыдущему, выполнение сравнения $x^2 \equiv a \bmod 2^\mu$ равносильно выполнению сравнений

$$2\xi' \equiv \alpha' \bmod 2, \qquad 2\xi'' \equiv \alpha'' \bmod 2^{\mu-2}.$$

Условия, необходимые для разрешимости этих сравнений, согласно V п. 3 § 4, гласят:

$$\alpha' \equiv 0 \bmod 2, \quad \left\{ \begin{array}{ll} \alpha'' \equiv 0 \bmod 1, & \text{в случае } \mu = 2 \\ \alpha'' \equiv 0 \bmod 2, & \text{в случае } \mu > 2 \end{array} \right\}.$$

Если они выполняются, то, согласно V п. 3 § 4, существуют два решения $\xi' \equiv 0,\ 1 \bmod 2$,

$$\left\{ \begin{array}{ll} \text{одно решение } \xi'' \equiv 0 \bmod 1, & \text{в случае } \mu = 2 \\ \text{два решения } \xi'',\ \xi'' + 2^{\mu-3} \bmod 2^{\mu-2}, & \text{в случае } \mu > 2 \end{array} \right\}.$$

Им соответствуют тогда два решения вида $\pm x \bmod 2^2$, соответственно четыре решения вида

$$\pm x, \quad \pm x(1 + 2^{\mu-1}) \equiv \pm (x + 2^{\mu-1}) \bmod 2^\mu$$

рассматриваемого сравнения (см. об этом § 5, п. 5, лемма 3).

В случае $\mu = 2$, когда представление через базис сводится к $a \equiv (-1)^{\alpha'} \bmod 2^2$, из двух классов вычетов $a \equiv \pm 1 \bmod 2^2$, взаимно простых с модулем, квадратом является только $a \equiv 1 \bmod 2^2$, соответствующее ему количество решений есть $N_a(2^2) = 2$, и оба решения имеют вид $x \equiv \pm 1 \bmod 2^2$. Все это ясно, конечно, и заранее.

В случае $\mu \geqslant 3$ пара сравнений $\alpha' \equiv 0$, $\alpha'' = 0 \bmod 2$ является, согласно замечанию к V п. 7 § 5 также и условием разрешимости для каждого из сравнений $x^2 \equiv a \bmod 2^\nu$ с $3 \leqslant \nu \leqslant \mu$, в частности, и для $\nu = 3$, а это означает просто, что должно быть $a \equiv 1 \bmod 2^3$. Необходимость этого последнего условия для разрешимости сравнения $x^2 \equiv a \bmod 2^\mu$ ($\mu \geqslant 3$) также ясна непосредственно, ввиду заключительного замечания в § 5, п. 7, согласно которому каждое x, взаимно простое с 2, имеет свойство $x^2 \equiv 1 \bmod 2^3$.

Подытожим наши результаты:

IIб. *В случае $p = 2$ для $\mu = 2$, 3 число a является квадратичным вычетом по* $\bmod 2^\mu$ *тогда и только тогда, когда $a \equiv 1 \bmod 2^\mu$. Если это имеет место, то*

$$N_a(2^2) = 2, \qquad N_a(2^3) = 4,$$

т. е. сравнение $x^2 \equiv a \bmod 2^\mu$ имеет при $\mu = 2$ два решения, а именно оба класса вычетов $x \equiv \pm 1 \bmod 2^2$, взаимно простых с модулем, а при $\mu = 3$ — четыре решения, а именно все классы вычетов $x \equiv \pm 1$, $\pm 5 \bmod 2^3$, взаимно простые с модулем.

Для $\mu \geqslant 3$ число a является квадратичным вычетом по $\bmod 2^\mu$ *тогда и только тогда, когда a есть квадратичный вычет по* $\bmod 2^3$ (*т. е. $a \equiv 1 \bmod 2^3$*). *Если это имеет место, то*

$$N_a(2^\mu) = N_a(2^3) = 4,$$

т. е. сравнение $x^2 \equiv a \bmod 2^\mu$ имеет четыре решения; они имеют вид $\pm x$, $\pm (x + 2^{\mu-1}) \bmod 2^\mu$ т. е. редуцируются к паре противоположных классов вычетов $\pm x \bmod 2^{\mu-1}$.

То, что решения сравнения $x^2 \equiv a \bmod 2^\mu$, если они вообще существуют, образуют пары классов вычетов $\pm x \bmod 2^{\mu-1}$, опять таки ясно сразу из леммы 1 из § 5, п. 5, согласно которой из $x' \equiv \pm x \bmod 2^{\mu-1}$ следует $x'^2 \equiv x^2 \bmod 2^\mu$; и также непосредственно видно, что для $\mu = 2$ оба класса вычетов из такой пары совпадают, а для $\mu \geqslant 3$ не совпадают.

Из результатов IIа, б (и из сказанного о тривиальном случае $p = 2$, $\mu = 1$) для общего случая, согласно I п. 2, следует:

III. *Число a является квадратичным вычетом по* $\bmod m$ *тогда и только тогда, когда a является квадратичным вычетом по*

$\bmod p$ *для каждого* нечетного простого делителя $p \mid m$, и кроме того $a \equiv 1 \bmod 4$, *соответственно* $\bmod 8$, *в том случае, если* $4 \mid m$ *или, соответственно даже* $8 \mid m$.

Если эти условия выполнены, то количество решений $N_a(m)$ *сравнения* $x^2 \equiv a \bmod m$ *дается формулой*

$$N_a(m) = 2^{s+z},$$

где s *обозначает количество нечетных простых делителей* $p \mid m$, *и* $z = 0, 1, 2$ *в зависимости от того, имеет ли место* $4 \nmid m$, $4 \mid m$, *но* $8 \nmid m$, $8 \mid m$.

В силу результата III, решение нашего основного вопроса, а именно, когда a является квадратичным вычетом по $\bmod m$, сводится к случаю, когда модуль $m = p \neq 2$ есть нечетное простое число. К этому случаю мы теперь и обратимся. При этом под p все время будет пониматься нечетное простое число.

4. Первый критерий: символ Лежандра. Первый критерий того, является ли a квадратичным вычетом по $\bmod p$, мы получили уже при выводе нашего общего результата IIa, п. 3.

Первый критерий для квадратичного характера по $\bmod p$. *Число* a *является квадратичным вычетом по* $\bmod p$ *тогда и только тогда, когда в представлении*

$$a \equiv w^\alpha \bmod p \qquad (\alpha \bmod p - 1)$$

через первообразный корень $w \bmod p$ *показатель степени* $\alpha \equiv 0 \bmod 2$.

Заметим при этом, что, как вытекает из вывода, класс вычетов $\alpha \bmod 2$ однозначно определяется классом вычетов $\alpha \bmod p - 1$, так как $p - 1 \equiv 0 \bmod 2$.

Поэтому существует $(p-1)/2$ квадратичных вычетов по $\bmod p$, представляющихся степенями

$$1, \quad w^2, \quad \ldots, \quad w^{p-3},$$

и $(p-1)/2$ квадратичных невычетов по $\bmod p$, представляющихся степенями

$$w, \quad w^3, \quad \ldots, \quad w^{p-2}$$

какого-нибудь первообразного корня $w \bmod p$.

Свойства быть квадратичным вычетом или квадратичным невычетом подчиняются относительно умножения следующей схеме:

$$\begin{aligned} \text{вычет} \times \text{вычет} &= \text{вычет}, \\ \text{вычет} \times \text{невычет} &= \text{невычет}, \\ \text{невычет} \times \text{невычет} &= \text{вычет}, \end{aligned}$$

которая аналогична схеме сложения для «четного» и «нечетного».

На языке теории групп это положение вещей может быть выражено (а также и обосновано) следующим образом. В цикли-

ческой группе $\mathfrak{P}$ классов вычетов по $\bmod p$, взаимно простых с модулем, вследствие того что ее порядок $\varphi(p) = p - 1$ является четным, квадраты образуют подгруппу $\mathfrak{Q}$ порядка

$$\varphi(p) / 2 = (p-1) / 2,$$

т. е. индекса 2 (являющуюся единственной подгруппой такого индекса), состоящую из элементов $A = W^{\alpha}$ с четным показателем α при представлении элемента A через образующий элемент W группы $\mathfrak{P}$. Единственный смежный класс $W\mathfrak{Q}$ состоит из элементов с нечетными показателями α. Схема умножения для «вычетов» и «невычетов» есть поэтому схема умножения фактор-группы $\mathfrak{P} / \mathfrak{Q}$, состоящей из $\mathfrak{Q}$ и $W\mathfrak{Q}$.

Первый критерий наводит на мысль ввести некоторый специальный символ со значениями $(-1)^{\alpha}$, чтобы различать квадратичные вычеты и невычеты $a \bmod p$. Такой символ был введен Лежандром, в то время как Гаусс, от которого исходит понятие квадратичного вычета и невычета, пользовался лишь словесным описанием, как это делали до сих пор и мы.

Определение символа Лежандра. *Для a, взаимно простого с p, положим*

$$\left(\frac{a}{p}\right) = (-1)^{\alpha}$$

(читается: символ a по p) или подробнее

$$\left(\frac{a}{p}\right) = \left\{ \begin{array}{l} 1, \text{ если } a \text{ есть квадратичный вычет по } \bmod p \\ -1, \text{ если } a \text{ есть квадратичный невычет по } \bmod p \end{array} \right\}.$$

В изложение теории квадратичных вычетов символ Лежандра вносит значительные упрощения по сравнению с громоздким описательным способом Гаусса. Кроме того, этот символ имеет глубокое принципиальное значение в высшей теории чисел, как мы увидим это в четвертой главе.

Приведенная выше схема умножения для «вычетов» и «невычетов» представляется с помощью символа Лежандра в простой форме *правила умножения*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

для a, b, взаимно простых с p.

Будем вообще называть всюду отличную от нуля теоретико-числовую функцию $\chi(a)$, удовлетворяющую функциональному уравнению

$$\chi(ab) = \chi(a)\chi(b), \tag{1}$$

мультипликативной функцией. При этом областью определения не обязательно должна служить полная совокупность Γ всех

целых чисел a. Мультипликативная функция $\chi_m(a)$, определенная в области всех целых чисел a, взаимно простых с данным натуральным числом m, для которой, кроме того,

$$\chi_m(a') = \chi_m(a) \quad \text{если} \quad a' \equiv a \bmod m, \tag{2}$$

т. е. которая зависит только от класса вычетов $a \bmod m$ своего аргумента, называется *характером по* $\bmod m$. Согласно § 4, п. 10, такая функция, очевидно, может быть однозначно продолжена с сохранением свойств (1), (2) на область всех взаимно простых с m рациональных чисел. Так как эта область значений аргумента замкнута также и по отношению к делению (является мультипликативной группой), функция удовлетворяет в ней в силу (1) требованию

$$\chi_m(a) = 1, \quad \text{если} \quad a \equiv 1 \bmod m, \tag{2'}$$

из которого (2) вытекает тогда посредством рассмотрения аргумента a'/a. Символ Лежандра подчиняется этому общему понятию и потому является характером по $\bmod p$. Из всех характеров по $\bmod p$ он однозначно выделяется тем, что обладает еще и свойством

$$\chi_p(a)^2 = 1, \quad \text{т. е.} \quad \chi_p(a) = \pm 1. \tag{3}$$

для всех a, взаимно простых с p, но не равен 1 тождественно. В самом деле, если некоторый характер $\chi_p(a)$ обладает этим дополнительным свойством (3), то для первообразного корня $w \bmod p$ необходимо будет $\chi_p(w) = -1$, а потому вообще

$$\chi_p(a) = \chi_p(w^\alpha) = \chi_p(w)^\alpha = (-1)^\alpha = \left(\frac{a}{p}\right).$$

Поэтому символ Лежандра называют также *квадратичным характером по* $\bmod p$, причем это одно и то же, ибо никаких квадратичных характеров, отличных от символа Лежандра, не существует.

5. Второй критерий: критерий Эйлера. Первый критерий для квадратичного характера $a \bmod p$ неудобен в том отношении, что в нем фигурирует первообразный корень $w \bmod p$, который сам по себе не имеет отношения к поставленному вопросу и который для каждого p определяется не однозначно, а, согласно § 5, п. 2, может быть выбран $\varphi(p-1)$ различными способами. Однако можно исключить первообразный корень $w \bmod p$ и вместе с ним относящийся к нему показатель $\alpha \bmod p-1$ и таким образом получить второй критерий, который содержит только фигурирующие в постановке вопроса простое число p и класс вычетов $a \bmod p$.

Это достигается на основании уже упомянутого выше, при выводе IIa, п. 3, выполняющегося для каждого первообразного корня $w \bmod p$ сравнения

$$w^{\frac{p-1}{2}} \equiv -1 \bmod p.$$

Из него для $a \equiv w^{\alpha} \bmod p$ мы имеем соотношения

$$\left(\frac{a}{p}\right) = (-1)^{\alpha} \equiv w^{\alpha \cdot \frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \bmod p.$$

Если выкинуть промежуточные члены, то и получится нужное нам исключение w и α. Посредством остающегося сравнения между крайними членами символ Лежандра $\left(\frac{a}{p}\right)$ действительно определяется однозначно. А именно, согласно малой теореме Ферма, мы, подобно тому, как выше в п. 3, имеем

$$0 \equiv a^{p-1} - 1 \equiv \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \bmod p$$

и потому обязательно верно одно из двух сравнений

$$a^{(p-1)/2} \equiv \pm 1 \bmod p,$$

и притом только одно, так как $1 \not\equiv -1 \bmod p$. В зависимости от того, которое из них верно, из полученного выше сравнения получается значение символа Лежандра $\left(\frac{a}{p}\right) = \pm 1$. Итак, мы имеем

Второй критерий для квадратичного характера по $\bmod p$: критерий Эйлера.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p,$$

т. е. $\left(\frac{a}{p}\right) = 1$ *или* -1, *в зависимости от того,* $a^{\frac{p-1}{2}} \equiv 1$ *или* $-1 \bmod p$.

6. Третий критерий: лемма Гаусса. Выведем, наконец, из критерия Эйлера третий, особенно интересный и важный критерий. Для этого введем следующее

Определение. *Система* $r_1, \ldots, r_{(p-1)/2}$ *из* $(p-1)/2$ *целых (или только p-целых) чисел называется полусистемой по* $\bmod p$, *если* $p-1$ *число* $\pm r_1, \ldots, \pm r_{(p-1)/2}$ *образуют полную систему вычетов по* $\bmod p$, *взаимно простых с модулем.*

Примерами таких полусистем являются, например, положительные абсолютно наименьшие вычеты $1, 2, \ldots, (p-1)/2$

или также первые $(p-1)/2$ степеней $1, w, \ldots, w^{(p-3)/2}$ первообразного корня $w \bmod p$; последнее тотчас же следует из того, что $w^{(p-1)/2} \equiv -1 \bmod p$ и потому вообще $w^{(p-1)/2+\alpha} \equiv -w^{\alpha} \bmod p$. С точки зрения теории групп, полусистема по $\bmod p$ является системой представителей из $(p-1)/2$ смежных классов по состоящей из двух классов вычетов $\pm 1 \bmod p$ подгруппе порядка 2 группы классов вычетов по $\bmod p$, взаимно простых с модулем.

Пусть теперь $r_1, \ldots, r_{(p-1)/2}$ — какая-нибудь полусистема по $\bmod p$. Если рассмотреть, аналогично тому как при доказательстве малой теоремы Ферма в § 4, п. 5, произведения $ar_1, \ldots, ar_{(p-1)/2}$, то так как $\pm r_1, \ldots, \pm r_{(p-1)/2}$ образуют полную систему вычетов по $\bmod p$, взаимно простых с модулем мы получим систему сравнений вида

$$ar_i \equiv (-1)^{\alpha_i} r_{i'} \bmod p \quad \left(i = 1, \ldots, \frac{p-1}{2}\right) \tag{1}$$

с показателями $\alpha_i \bmod 2$ и индексами i' из ряда $1, \ldots, (p-1)/2$, которые однозначно определяются классом вычетов $a \bmod p$. Все эти индексы i' различны между собой и образуют, таким образом, перестановку индексов $i = 1, \ldots, (p-1)/2$. Действительно, если бы было $j' = i'$, то отсюда следовало бы $ar_j \equiv \pm ar_i \bmod p$, т. е. $r_j \equiv \pm r_i \bmod p$, а это, согласно определению полусистемы, имеет место лишь при $j = i$. Перемножая $(p-1)/2$ сравнений (1) и сокращая на взаимно простой с p множитель $r_1 \ldots r_{(p-1)/2}$, мы получаем отсюда, подобно тому, как при доказательстве малой теоремы Ферма, сравнение

$$a^{\frac{p-1}{2}} \equiv (-1)^{\sum_i \alpha_i} \bmod p.$$

Оно уточняет, какой знак должен стоять в получающемся из малой теоремы Ферма сравнении $a_{(p-1)/2} \equiv \pm 1 \bmod p$. Согласно критерию Эйлера, оно вместе с тем определяет значение символа Лежандра:

$$\left(\frac{a}{p}\right) = (-1)^{\sum_i \alpha_i}. \tag{2}$$

Класс вычетов по $\bmod 2$ показателя $\sum_i \alpha_i$ в формуле (2) можно понимать также как количество по $\bmod 2$ отрицательных сомножителей $(-1)^{\alpha_i} = -1$ в сравнениях (1).

Итак, мы получаем

Третий критерий для квадратичного характера по $\bmod p$: лемма Гаусса (общая форма).

$$\left(\frac{a}{p}\right) = (-1)^n,$$

где n есть количество отрицательных знаков, получающихся в (1) *при выражении* $(p-1)/2$ *произведений* ar_i *для полусистемы* $r_i \bmod p$ *через полную систему* $\pm r_i \bmod p$ *классов вычетов, взаимно простых с модулем.*

Сам Гаусс доказал эту лемму только для специальной полусистемы $1, 2, \ldots, (p-1)/2$. Тогда она звучит несколько короче

Лемма Гаусса (специальная форма):

$$\left(\frac{a}{p}\right) = (-1)^n,$$

где n есть количество отрицательных вычетов среди абсолютно наименьших вычетов по $\bmod p$ *для кратных* $a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)/2$.

Пример. Вычислим символ Лежандра $\left(\frac{7}{13}\right)$ с помощью каждого из трех критериев.

Первый критерий:

$\alpha \bmod 12$	0	1	2	3	4	5	6	7	8	9	10	11
$2^\alpha \bmod 13$	1	2	4	8	3	6	−1	−2	−4	−8	−3	−6

$$7 \equiv -6 \equiv 2^{11} \bmod 13, \quad \left(\frac{7}{13}\right) = (-1)^{11} = -1.$$

Второй критерий:

$\nu \bmod 12$	0	1	2	3	4	5	6
$7^\nu \bmod 13$	1	−6	−3	5	−4	−2	−1

$$7^6 \equiv -1 \bmod 13, \quad \left(\frac{7}{13}\right) = -1$$

Третий критерий:

r	1	2	3	4	5	6
$7^r \bmod 13$	−6	1	−5	2	−4	3

$$n = 3, \quad \left(\frac{7}{13}\right) = (-1)^3 = -1.$$

§ 7. КВАДРАТИЧНЫЙ ЗАКОН ВЗАИМНОСТИ: ЭЛЕМЕНТАРНОЕ ДОКАЗАТЕЛЬСТВО

1. Основной вопрос, сведение к простым числам. Тремя критериями из § 6, п. 4, 5, 6 мы дали исчерпывающий ответ на вопрос

Какие рациональные числа $a \neq 0$ являются квадратичными вычетами по заданному нечетному простому числу p?

Как уже было сказано в § 6, п. 1, основной интерес в теории квадратичных вычетов представляет обратный вопрос:

По каким нечетным простым числам p заданное рациональное число $a \neq 0$ является квадратичным вычетом?

Первый вопрос означает изучение символа Лежандра $\left(\frac{a}{p}\right) = \chi_p(a)$ при постоянном p как функции от a. Второй вопрос, к рассмотрению которого мы теперь перейдем, означает изучение символа Лежандра $\left(\frac{a}{p}\right) = \psi_a(p)$ при постоянном a как функции от p. В то время как в первой постановке вопроса значения аргумента a являются рациональными числами, взаимно простыми с p, во второй постановке значения аргумента p ограничиваются нечетными простыми числами, не входящими в a; таким образом, остаются без рассмотрения $p = 2$ и конечное множество простых делителей p числителя и знаменателя числа a.

Но данное рациональное число $a \neq 0$ является произведением $-1, 2$ и нечетных простых чисел q, и при этом символ Лежандра $\left(\frac{a}{p}\right)$, ввиду его мультипликативности (см. § 6, п. 4, правило умножения), равен соответствующему произведению символов $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, $\left(\frac{q}{p}\right)$. Таким образом, если мы будем знать эти последние специальные символы как функции от p, мы будем владеть по существу и общим символом Лежандра как функцией от p. Степень сложности высказывания относительно $\left(\frac{a}{p}\right)$ будет зависеть, конечно, от того, какого вида результаты получатся относительно $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, $\left(\frac{q}{p}\right)$. Мы увидим, что получение результата относительно $\left(\frac{a}{p}\right)$ в законченной форме потребует еще дополнительного рассмотрения, которое мы сделаем лишь позднее в § 9. Здесь же мы рассмотрим сначала только специальные символы Лежандра $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, $\left(\frac{q}{p}\right)$.

Ответ на вопрос о том, как ведут себя эти специальные символы как функции от p, дает доказанный Гауссом знаменитый квадратичный закон взаимности вместе с двумя дополнениями к нему, причем *дополнения* относятся к символам $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, в то время как высказывание относительно символов вида $\left(\frac{q}{p}\right)$ называется *общей формой закона взаимности*. Гаусс с полным

правом назвал этот закон *основной теоремой теории квадратичных вычетов*. В течение прошедших с тех пор 150 лет она заняла место центральной теоремы современной теории чисел, благодаря своим многочисленным приложениям и идейным связям со всевозможными теоретико-числовыми вопросами и теориями, а также благодаря ее обобщениям в теории алгебраических чисел.

2. Два дополнения к закону взаимности. Мы начнем с вывода обоих дополнений к закону взаимности.

а) Квадратичный характер $\left(\frac{-1}{p}\right)$ легко можно определить с помощью каждого из трех наших критериев из § 6, п. 4, 5, 6:

1. $-1 \equiv w^{\frac{p-1}{2}} \bmod p$ и потому $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
2. $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p$ и потому $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
3. Абсолютно наименьшие вычеты $(p-1)/2$ кратных

$$-1 \cdot 1, \quad -1 \cdot 2, \quad \ldots, \quad -1 \cdot \frac{p-1}{2}$$

совпадают с этими кратными и, таким образом, все отрицательны, и потому $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Тем самым доказано

Первое дополнение к квадратичному закону взаимности.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

для каждого нечетного простого числа p; словами:

-1 есть квадратичный вычет по всем простым числам $p \equiv 1 \bmod 4$,

-1 есть квадратичный невычет по всем простым числам $p \equiv -1 \bmod 4$.

Первое утверждение было доказано нами уже в XIII п. 11 § 4 в связи с теоремой Вильсона, когда мы для $p = 4n+1$ указали явное решение сравнения $x^2 \equiv -1 \bmod p$, а именно, $x \equiv (2n)! \bmod p$.

Из второго утверждения мы выведем одно интересное следствие. Разрешимость квадратного сравнения $x^2 \equiv -1 \bmod p$, очевидно, равносильна разрешимости соответствующего однородного квадратного сравнения

$$x^2 + y^2 \equiv 0 \bmod p \quad \text{с} \quad x, y \not\equiv 0 \bmod p.$$

Таким образом, имеет место

Следствие. *Сумма x^2+y^2 двух целочисленных квадратов может делиться, если не считать общих делителей x и y, только на простые числа $p \equiv 1 \bmod 4$ или на $p=2$.*

Поэтому, в частности, никакое простое $p \equiv -1 \bmod 4$ не может быть представлено в виде суммы двух целочисленных квадратов.

Для простого числа $p=2$ такое представление существует: $2=1^2+1^2$. То, что для всех простых $p \equiv 1 \bmod 4$ тоже существуют такие представления $p=x^2+y^2$, является глубоким фактом, который мы впервые получим в § 10, п. 8 в качестве побочного результата и притом способом, аналогичным тому, которым мы доказали в XIII п. 11 § 4 разрешимость сравнения $x^2 \equiv -1 \bmod p$, а именно, посредством явной конструкции.

б) Определение квадратичного характера $\left(\frac{2}{p}\right)$ уже несколько труднее. Здесь нельзя (по крайней мере непосредственно) достигнуть цели с помощью первого и второго критериев, но можно это сделать с помощью третьего критерия, в чем проявляется его преимущество.

Рассмотрим $(p-1)/2$ кратных

$$2 \cdot 1,\ 2 \cdot 2,\ \ldots,\ 2 \cdot \frac{p-1}{2},$$

т. е. четные числа

$$2,\ 4,\ \ldots,\ p-1.$$

Из них отрицательные абсолютно наименьшие вычеты получаются у тех и только тех, которые лежат между $p/2$ и p. Их количество n может быть определено также (посредством деления на 2) как количество целых чисел между $p/4$ и $p/2$. Первое из таких чисел есть $(p+3)/4$ или $(p+1)/4$, в зависимости от того, $p \equiv 1 \bmod 4$ или $p \equiv -1 \bmod 4$, в то время как последнее в обоих случаях есть $(p-1)/2$. Таким образом,

$$n = \frac{p-1}{2} - \frac{p+3}{2} + 1 = \frac{p-1}{4} \equiv \frac{p-1}{4} \bmod 2 \quad \text{для } p \equiv 1 \bmod 4,$$

$$n = \frac{p-1}{2} - \frac{p+1}{4} + 1 = \frac{p+1}{4} \equiv \frac{-p-1}{4} \bmod 2 \text{ для } p \equiv -1 \bmod 4.$$

На основании определения p^* в § 5, п. 7 обе эти формулы можно объединить в одну:

$$n \equiv \frac{p^*-1}{4} \bmod 2.$$

Тем самым доказано

Второе дополнение к квадратичному закону взаимности.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^*-1}{4}}$$

для каждого нечетного простого числа p; *словами*:

2 *есть квадратичный вычет по всем простым числам* $p \equiv \pm 1 \bmod 8$,

2 *есть квадратичный невычет по всем простым числам* $p \equiv \pm 5 \bmod 8$.

Как пример применения идей п. 1 мы вычислим символ $\left(\frac{-2}{p}\right)$, воспользовавшись при этом результатами обоих дополнений к закону взаимности о символах $\left(\frac{-1}{p}\right)$ и $\left(\frac{2}{p}\right)$. Формально получается

$$\left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{2}+\frac{p^*-1}{4}}$$

для каждого нечетного простого числа p. При этом фигурирующий в показателе класс вычетов $(p-1)/2+(p^*-1)/4 \bmod 2$ зависит только от класса вычетов $p \bmod 8$. Посредством проверки четырех возможных случаев $p \equiv \pm 1, \pm 5 \bmod 8$ можно убедиться в справедливости следующей словесной формулировки:

-2 *является квадратичным вычетом по всем простым числам* $p \equiv 1, -5 \bmod 8$,

-2 *является квадратичным невычетом по всем простым числам* $p \equiv -1, 5 \bmod 8$.

Интересно отметить, что в формулы дополнений к закону взаимности входят как раз показатели из представления класса вычетов $p \bmod 8$ через базис из V п. 7 § 5; это представление согласно замечанию, сделанному в конце § 5, п. 7, может быть записано в виде

$$p \equiv (-1)^{\frac{p-1}{2}} 5^{\frac{p^*-1}{4}} \bmod 8.$$

3. Общая форма закона взаимности. Теперь мы приступим к исследованию символа типа $\left(\frac{q}{p}\right)$, где q — какое-нибудь нечетное простое число, а p — отличное от q нечетное простое число. Этот символ мы не определим в виде элементарной функции от p, подобно рассмотренным до этого символам $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, а сможем лишь вывести некоторое соотношение, связывающее его с *обратным* символом $\left(\frac{p}{q}\right)$; отсюда и название «*закон взаимности*». Для нашей постановки вопроса эта своеобразная

и неожиданная форма ответа играет ту же роль, что и явное определение. Действительно, если в соответствии с постановкой вопроса рассматривать q как постоянное, а p как переменное, то этот ответ сводит *неизвестное* нам положение вещей, а именно, как зависит функция $\left(\frac{q}{p}\right)=\psi_q(p)$ от p, к зависимости квадратичного характера $\left(\frac{p}{q}\right)=\chi_q(p)$ от p, а эта зависимость нам уже *известна*. Мы еще рассмотрим этот вопрос подробнее, после того как выведем закон взаимности.

Гаусс дал для своей *основной теоремы* семь различных доказательств, а с тех пор количество их привысило 50, хотя, конечно, большей частью они заключаются лишь в незначительных видоизменениях ранее известных доказательств. Мы дадим здесь один очень простой и наглядный вариант одного из доказательств Гаусса, который принадлежит Фробениусу.

По лемме Гаусса

$$\left(\frac{q}{p}\right)=(-1)^n,$$

где n есть количество тех кратных qx с $x=1, \ldots, (p-1)/2$, у которых абсолютно наименьшие вычеты по $\bmod p$ отрицательны, т. е. для которых неравенство

$$-\frac{p}{2}<qx-py<0$$

имеет целочисленное решение y. Если это имеет место для некоторого x, то решение y определяется, очевидно, однозначно, и для него выполняются неравенства

$$y>0, \text{ так как } py>qx>0,$$

$$y<\frac{q+1}{2}, \text{ так как } py<qx+\frac{p}{2}<q\frac{p}{2}+\frac{p}{2}=p\frac{q+1}{2}.$$

Из этих двух неравенств и целочисленности следует, что решение, если оно существует, принадлежит к системе $y=1, \ldots, (q-1)/2$. Поэтому можно сказать также, что n есть количество пар

$$\left\{\begin{array}{l} x=1, \ldots, \frac{p-1}{2} \\ y=1, \ldots, \frac{q-1}{2} \end{array}\right\}$$

с $-p/2<qx-py<0$.

Точно так же мы можем получить, что

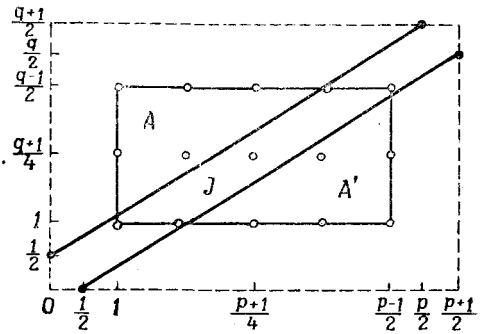
$$\left(\frac{p}{q}\right)=(-1)^{n'},$$

где n' есть количество пар

$$\left\{\begin{array}{l} x=1,\ \ldots,\ \dfrac{p-1}{2} \\ y=1,\ \ldots,\ \dfrac{q-1}{2} \end{array}\right\}$$

с $-q/2 < py - qx < 0$.

Последнее неравенство может быть также записано в виде $0 < qx - py < q/2$, т. е. с тем же самым выражением в середине, что и в первом неравенстве. Так как равенство $qx - py = 0$ при наших значениях x, y невозможно, потому что несократимая дробь p/q не допускает представления x/y с меньшими числителем и знаменателем, то при сложении количеств n и n' из обоих неравенств составляется одно, границами которого являются крайние члены прежних неравенств. Таким образом, получается



Фиг. 1.

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{n+n'},$$

где $n+n'$ есть количество пар

$$\left\{\begin{array}{l} x=1,\ \ldots,\ \dfrac{p-1}{2} \\ y=1,\ \ldots,\ \dfrac{q-1}{2} \end{array}\right\}$$

с $-\frac{p}{2} < qx - py < \frac{q}{2}$.

С точки зрения аналитической геометрии, последнее неравенство представляет в плоскости вещественных переменных x, y внутреннюю часть полосы, ограниченной двумя параллельными прямыми

$$qx - py = -\frac{p}{2}, \qquad qx - py = \frac{q}{2}.$$

Если точки с целочисленными координатами x, y называть *точками решетки*, то $n+n'$ равно количеству точек решетки, лежащих внутри этой полосы и одновременно в прямоугольнике (фиг. 1).

Полоса расположена симметрично относительно центра прямоугольника

$$(x_0,\ y_0) = \left(\frac{p+1}{4},\ \frac{q+1}{2}\right)$$

(который сам не обязательно принадлежит решетке). В этом можно убедиться или рассматривая, как это указано на чертеже, точки пересечения прямых, ограничивающих полосу, со сторонами увеличенного во всех направлениях на 1 прямоугольника

$$0 \leqslant x \leqslant \frac{p+1}{2},\quad 0 \leqslant y \leqslant \frac{q+1}{2},$$

или исходя из того, что средняя линия

$$qx - py = \frac{1}{2}\left(-\frac{p}{2} + \frac{q}{2}\right) = \frac{q-p}{4}$$

этой полосы проходит через центр прямоугольника

$$(x_0,\ y_0) = \left(\frac{p+1}{4},\ \frac{q+1}{4}\right).$$

Поэтому полоса разбивает прямоугольник на внутреннюю часть J и две внешние части A, A', симметрично расположенные относительно центра.

Согласно сказанному, $n+n'$ равно количеству точек решетки в J. В силу симметрии, A и A' содержат одно и то же количество m точек решетки. Но все эти точки вместе составляют точно $[(p-1)/2]\cdot[(q-1)/2]$ точек решетки во всем прямоугольнике. Таким образом,

$$n + n' + 2m = \frac{p-1}{2}\cdot\frac{q-1}{2}.$$

Отсюда следует

$$n + n' \equiv \frac{p-1}{2}\cdot\frac{q-1}{2} \bmod 2$$

и, таким образом, получается формула закона взаимности:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Чтобы в целях чистоты метода избегнуть геометрического вывода, который привел нас к доказательству этой формулы, то отражение от центра

$$(x_0,\ y_0) = \left(\frac{p+1}{4},\ \frac{q+1}{4}\right)$$

надо выразить в алгебраической форме подстановкой

$$(x,\ y) = \left(\frac{p+1}{2} - x',\ \frac{q+1}{2} - y'\right)$$

и продолжать следующим образом. Посредством этой подстановки совокупность $[(p-1)/2]\,[(q-1)/2]$ пар (x, y) с

$$\left\{\begin{array}{l} x=1,\ \ldots,\ \frac{p-1}{2} \\ y=1,\ \ldots,\ \frac{q-1}{2} \end{array}\right\}$$

взаимно однозначно отображается на себя. При этом пары (x, y), для которых выполняется неравенство

$$qx-py \leqslant -\frac{p}{2}\ \text{(A)},\ \text{соответственно}\ \frac{q}{2} \leqslant qx-py \qquad \text{(A')}$$

переходят, как легко вычислить, в совокупность пар (x', y'), для которых выполняется другое из этих неравенств

$$\frac{q}{2} \leqslant qx'-py' \qquad \text{(A')},\ \text{соответственно}\ qx'-py' \leqslant -\frac{p}{2}. \qquad \text{(A)}$$

Поэтому пары обоих этих типов имеются в одном и том же количестве m. Присоединяя сюда $n+n'$ пар (x, y) с неравенством

$$-\frac{p}{2} < qx-py < \frac{q}{2}, \qquad \text{(I)}$$

мы снова получим соотношение для количеств пар

$$n+n'+2m=\frac{p-1}{2}\frac{q-1}{2}$$

и тем самым формулу закона взаимности.

Итак, нами доказана

Общая форма квадратичного закона взаимности.

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

для каждой пары различных нечетных простых чисел p, q; словами:

Если хотя бы одно из простых чисел p или $q \equiv 1 \bmod 4$, то квадратичные характеры p по q и q по p совпадают.

Если оба простых числа p и $q \equiv -1 \bmod 4$, то квадратичные характеры p по q и q по p противоположны.

В нашем доказательстве эти два случая различаются тем, что во втором из них центр $((p+1)/4,\ (q+1)/4)$ является точкой решетки, а в первом не является. Можно провести это доказательство и так: рассмотреть только внутреннюю часть I и установить, что лежащие в ней точки решетки (количество которых равно $n+n'$) можно, за исключением только центра, если он принадлежит решетке, соединить в отличные друг от друга пары посредством отражений от центра.

Квадратичный закон взаимности получен нами в форме, симметричной относительно обоих простых чисел p, q, на чем, кстати, основывалось и данное нами доказательство. Для ответа на наш первоначальный вопрос о представлении символа $\left(\frac{q}{p}\right)$ как функции своего «знаменателя» p — так говорят для краткости, хотя никакой дроби здесь нет — удобнее другая форма, которая получается посредством применения первого дополнения к закону взаимности и правила умножения следующим образом:

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) =$$

$$= \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = \left(\frac{p^*}{q}\right).$$

Таким образом, имеет место простая *формула обращения*

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$$

для *каждой* пары различных нечетных простых чисел p, q. Эта изящная форма закона взаимности, в которой отсутствует множитель $(-1)^{[(p-1)/2]\cdot[(q-1)/2]}$, указывающий знак; особенно удобна для применений. Она также лучше всего соответствует глубокому значению этого закона в теории алгебраических чисел, как это выявится при доказательстве уже в следующем § 8 и позднее в § 19.

4. Символ Лежандра как функция своего знаменателя. Согласно общей форме закона взаимности и двум дополнениям к нему, специальные символы Лежандра

$$\left(\frac{-1}{q}\right), \left(\frac{2}{p}\right), \left(\frac{q}{p}\right) \quad (p \text{ и } q \text{ — различные простые числа})$$

выражаются в виде явных функций

$$(-1)^{\frac{p-1}{2}}, \quad (-1)^{\frac{p^*-1}{4}}, \quad \left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\left(\frac{p}{q}\right).$$

Неожиданное в этом ответе на наш основной вопрос заключается в природе этих функций, а именно в том, что они зависят только от классов вычетов

$$p \bmod 4, \; p \bmod 8, \; \left\{\begin{array}{l} p \bmod q, \text{ в случае } q \equiv 1 \bmod 4 \\ p \bmod 4q, \text{ в случае } q \equiv -1 \bmod 4 \end{array}\right\};$$

в последнем случае это получается из того, что непосредственно входящая в формулу пара классов вычетов $p \bmod 4$, $p \bmod q$,

согласно § 4, п. 9, однозначно определяется классом вычетов $p \bmod 4q$. Такого ответа совсем нельзя было ожидать заранее, особенно для символа третьего типа, который по своему определению есть характер $\left(\frac{q}{p}\right) = \chi_p(q)$ класса вычетов $q \bmod p$, взаимно простого с модулем, и как таковой, казалось бы, не имеет отношения к обратному классу вычетов $p \bmod q$.

Рассмотрим теперь общий символ $\left(\frac{a}{p}\right)$ с каким-нибудь заданным рациональным числом $a \neq 0$ как функцию своего знаменателя p, который тогда может меняться в области всех не входящих в a простых чисел. Для этого представим a в разложении на простые множители

$$a = (-1)^{\alpha} \prod_q q^{\alpha_q} = (-1)^{\alpha} 2^{\alpha_2} \prod_{q \neq 2} q^{\alpha_q}$$

($\alpha \bmod 2$, α_q — целые, лишь конечное множество $\alpha_q \neq 0$). Тогда, согласно правилу умножения и формулам закона взаимности, имеем

$$\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)^{\alpha} \cdot \left(\frac{2}{p}\right)^{\alpha_2} \prod_{q \neq 2} \left(\frac{q}{p}\right)^{\alpha_q} =$$

$$= (-1)^{\alpha \frac{p-1}{2}} \cdot (-1)^{\alpha_2 \frac{p^*-1}{4}} \cdot \prod_{q \neq 2} \left(\frac{p^*}{q}\right)^{\alpha_q} =$$

$$= (-1)^{\alpha \frac{p-1}{2}} \cdot (-1)^{\alpha_2 \frac{p^*-1}{4}} \cdot \prod_{q \neq 2} \left(\frac{-1}{q}\right)^{\alpha_q \frac{p-1}{2}} \left(\frac{p}{q}\right)^{\alpha_q}$$

для всех не входящих в a простых чисел p; при этом не определенный нами множитель с $q = p$, формально входящий в произведение, на самом деле отсутствует ввиду того, что $\alpha_p = 0$. Согласно этой формуле, символ $\left(\frac{a}{p}\right)$ зависит только от классов вычетов

$$p \bmod 4 \text{ в случае } \alpha \equiv 1 \bmod 2,$$

$$p \bmod 8 \text{ в случае } \alpha_2 \equiv 1 \bmod 2,$$

$$\left\{ \begin{array}{ll} p \bmod q & \text{для } q \equiv 1 \bmod 4 \\ p \bmod 4q & \text{для } q \equiv -1 \bmod 4 \end{array} \right\} \text{ с } \alpha_q \equiv 1 \bmod 2.$$

Поэтому $\left(\frac{a}{p}\right)$ заведомо зависит только от класса вычетов p по общему наименьшему кратному $m(a)$ всех этих отдельных модулей. Чтобы выразить $m(a)$, обозначим через

$$k(a) = (-1)^{\alpha} \prod_{\alpha_q \equiv 1 \bmod 2} q$$

произведение множителя $(-1)^{\alpha}$, определяющего знак, и различных простых чисел (включая 2), входящих в a с нечетными показателями α_q, т. е. так называемое *свободное от квадратов ядро* числа a. Тогда

$$m(a)=\left\{\begin{array}{ll} k(a), & \text{если } k(a)>0 \text{ и } k(a) \text{ содержит} \\ & \text{лишь простые числа } q\equiv 1 \bmod 4 \\ 4\,|\,k(a)\,|, & \text{в остальных случаях} \end{array}\right\}. \qquad (1)$$

Тогда для определенного таким образом модуля $m(a)$ имеет место

$$\left(\frac{a}{p}\right)=\left(\frac{a}{p'}\right), \quad \text{если } p\equiv p' \bmod m(a), \qquad (2)$$

для любых не входящих в a нечетных простых чисел p, p'.

Этим мы установили существование такого натурального числа $m(a)$, что символ $\left(\frac{a}{p}\right)$ имеет свойство (2) из § 6, п. 4 характера по $\bmod m(a)$. О выполнении свойства (1) из § 6, п. 4, а именно мультипликативности, здесь, конечно, не может идти речь, так как область значений аргумента состоит только из простых чисел p; мультипликативность мы получим в § 9, когда обобщим символ Лежандра на составные знаменатели.

В высказывании (2) модуль $m(a)$ из (1) можно еще в некоторых случаях заменить его собственным делителем. Мы покажем, что верно следующее усиление:

I. *Высказывание* (2) *остается справедливым, если заменить в нем модуль* $m(a)$ *из* (1) *на абсолютную величину числа*

$$f(a)=\left\{\begin{array}{ll} k(a), & \text{если } k(a)\equiv 1 \bmod 4 \\ 4k(a), & \text{если } k(a)\not\equiv 1 \bmod 4 \end{array}\right\}.$$

Доказательство. Нужно показать, что в $m(a)$ можно отбросить множитель 4 уже при предположении $k(a)\equiv 1 \bmod 4$, являющемся более слабым, чем фигурирующее в (1). Приведенное выше явное представление для $\left(\frac{a}{p}\right)$ как функции от p может быть записано в форме:

$$\left(\frac{a}{p}\right)=\left[(-1)^{\alpha}\prod_{q\neq 2}\left(\frac{-1}{q}\right)^{\alpha_q}\right]^{\frac{p-1}{2}}\cdot(-1)^{\alpha_2\frac{p^*-1}{4}}\cdot\prod_{q\neq 2}\left(\frac{p}{q}\right)^{\alpha_q}. \qquad (3)$$

Если $k(a)\equiv 1 \bmod 4$, то, с одной стороны, $\alpha_2\equiv 0 \bmod 2$, так что основание $((p^*-1)/4)$-й степени равно 1, а с другой стороны, и основание $((p-1)/2)$-й степени равно 1. Это последнее основание в случае $2\nmid k(a)$ попросту равно абсолютно наименьшему вычету ± 1 числа $k(a)$ по $\bmod 4$. Действительно, так как при

$q \neq 2$, согласно первому дополнению к закону взаимности, имеет место $\left(\frac{-1}{q}\right) \equiv q \bmod 4$, то

$$(-1)^{\alpha} \prod_{q \neq 2} \left(\frac{-1}{q}\right)^{\alpha_q} = (-1)^{\alpha} \prod_{\alpha_q \equiv 1 \bmod 2} \left(\frac{-1}{q}\right) \equiv$$

$$\equiv (-1)^{\alpha} \prod_{\alpha_q \equiv 1 \bmod 2} q \equiv k(a) \bmod 4.$$

Поэтому для $k(a) \equiv 1 \bmod 4$ равенство (3) принимает более простой вид

$$\left(\frac{a}{p}\right) = \prod_{q \neq 2} \left(\frac{p}{q}\right)^{\alpha_q}, \qquad (3')$$

так что в этом случае символ $\left(\frac{a}{p}\right)$ действительно не зависит от класса вычетов $p \bmod 4$, а только от класса вычетов $p \bmod |k(a)|$.

5. Ведущий модуль символа Лежандра как функции его знаменателя. Мы будем называть *определяющим модулем* символа Лежандра $\left(\frac{a}{p}\right)$ как функции его знаменателя p каждое натуральное число m, для которого выполняется утверждение (2) из п. 4, т. е. свойство

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p'}\right), \quad \text{если } p \equiv p' \bmod m,$$

в области всех простых чисел p, не входящих в a и m. Наименьший определяющий модуль f называется *ведущим модулем* символа $\left(\frac{a}{p}\right)$ как функции от p.

Теория ведущего модуля получит свое полное завершение лишь в § 9 после расширения области значений аргумента от простых чисел p на область всех составных чисел. Все же мы уже здесь рассмотрим ее в основных чертах в ограниченной области значений аргумента, так как она весьма поучительна и позволяет ясно понять значение данного в § 9 обобщения. Вследствие ограничения области значений аргумента простыми числами мы должны при этом опираться на одну глубокую теоретико-числовую теорему, доказательство которой будет изложено только в третьей главе, а именно, на знаменитую «*теорему о простых числах в арифметической прогрессии*» Дирихле:

В каждом классе вычетов, взаимно простом с модулем, имеется бесконечно много простых чисел.

Применяя эту теорему, мы докажем сначала следующий общий факт:

II. *Вместе с двумя натуральными числами* m_1, m_2 *также и их общий наибольший делитель* (m_1, m_2) *является определяющим модулем символа Лежандра* $\left(\frac{a}{p}\right)$ *и притом в области простых чисел* p, *не входящих в* a *и в общее наименьшее кратное* $[m_1, m_2]$.

Доказательство. Пусть m_1, m_2 — два определяющих модуля символа $\left(\frac{a}{p}\right)$ и пусть p_1, p_2 — два нечетных простых числа, не входящих в a, m_1, m_2 со свойством

$$p_1 \equiv p_2 \bmod (m_1, m_2).$$

Тогда оба класса вычетов $p_1 \bmod m_1$ и $p_2 \bmod m_2$, взаимно простых с модулями, можно объединить в однозначно определенный класс вычетов $r \bmod [m_1, m_2]$, взаимно простой с модулем, т. е. существует такое взаимно простое с $[m_1, m_2]$ число r, что

$$r \equiv p_1 \bmod m_1, \quad r \equiv p_2 \bmod m_2.$$

Ясно, что класс вычетов $r \bmod [m_1, m_2]$ определяется этими требованиями однозначно. Его существование доказывается так. Представим себе, что классы вычетов $p_1 \bmod m_1$ и $p_2 \bmod m_2$, взаимно простые с модулями, разложены в соответствии с § 4, п. 9 на компоненты по степеням q^{μ_1}, q^{μ_2} отдельных простых чисел q, с которыми они входят в разложения чисел m_1, m_2 на простые множители. Выберем тогда компоненты, соответствующие бо́льшим степеням $q^{\max(\mu_1, \mu_2)}$; в силу предположения

$$p_1 \equiv p_2 \bmod (m_1, m_2),$$

они содержатся в компонентах, соответствующих меньшим степеням $q^{\min(\mu_1, \mu_2)}$. Теперь, в соответствии с § 4, п. 9, объединим выбранные компоненты по $\bmod q^{\max(\mu_1, \mu_2)}$ в класс вычетов $r \bmod [m_1, m_2]$, взаимно простой с модулем. Тогда, в силу только что сказанного, требования $r \equiv p_1 \bmod q^{\mu_1}$, $r \equiv p_2 \bmod q^{\mu_2}$ выполняются для всех q, и потому действительно имеет место $r \equiv p_1 \bmod m_1$, $r \equiv p_2 \bmod m_2$.

Но по теореме Дирихле существует не входящее в a нечетное простое число p, такое, что $p \equiv r \bmod [m_1, m_2]$, т. е.

$$p \equiv p_1 \bmod m_1, \quad p \equiv p_2 \bmod m_2.$$

Другими словами, в силу этой теоремы, сделанное выше объединение можно выполнить даже и так, что вместо r получится не входящее в a *простое число* p. По предположению, для так определенного простого p имеет место

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p_1}\right), \quad \left(\frac{a}{p}\right) = \left(\frac{a}{p_2}\right).$$

А отсюда тогда следует

$$\left(\frac{a}{p_1}\right)=\left(\frac{a}{p_2}\right),$$

что и требовалось доказать.

Из II мы заключаем:

III. *Ведущий модуль* f *символа* $\left(\frac{a}{p}\right)$ *как функции от* p *является делителем каждого определяющего модуля* m *этого символа, и, в частности, таким образом модуля* $|f(a)|$ *из* I *п.* 4.

Доказательство. Из II, вследствие свойства минимальности ведущего модуля f, следует, что $(f, m)\geqslant f$, в то время как с другой стороны $(f, m)\leqslant f$, так как (f, m) делит f. Поэтому $(f, m)=f$, и тем самым $f\mid m$, что и утверждается.

Используя теорему Дирихле несколько по-иному, мы можем доказать и больше, а именно:

IV. *Ведущий модуль символа Лежандра* $\left(\frac{a}{p}\right)$ *как функции от* p *совпадает с модулем* $|f(a)|$ *из* I *п.* 4.

Доказательство. Согласно III, достаточно проверить только, что собственные делители модуля

$$|f(a)|=\left\{\begin{array}{l}|k(a)|, \text{ если } k(a)\equiv 1 \bmod 4\\ 4|k(a)|, \text{ если } k(a)\not\equiv 1 \bmod 4\end{array}\right\}$$

не являются определяющими модулями символа $\left(\frac{a}{p}\right)$. Далее, очевидно, можно ограничиться рассмотрением делителей вида $|f(a)|/q$, где q пробегает простые делители числа $|f(a)|$. Таким образом, нужно доказать, что для каждого простого делителя q числа $|f(a)|$ существует пара не входящих в a нечетных простых чисел p, p', для которых $p\equiv p' \bmod |f(a)|/q$, но $\left(\frac{a}{p}\right)\neq\left(\frac{a}{p'}\right)$, так что, например, $\left(\frac{a}{p}\right)=1$, $\left(\frac{a}{p'}\right)=-1$.

Для $q\neq 2$ мы выберем

$$p\equiv 1 \bmod |f(a)|/q, \quad p\equiv 1 \bmod q,$$
$$p'\equiv 1 \bmod |f(a)|/q, \quad p'\equiv w \bmod q,$$

где w есть первообразный корень по $\bmod q$ или даже только квадратичный невычет по $\bmod q$. Так как оба модуля взаимно просты друг с другом, то эти требования сводятся к выбору p, p' в двух классах вычетов по $\bmod |f(a)|$, взаимно простых с модулем, и потому, согласно теореме Дирихле, могут быть удовлетворены, причем p, p' не будут входить в a. Тогда в содержащемся в доказательстве утверждения I п. 4 явном представлении (3) для символа Лежандра соответствующие рассматриваемому

простому делителю q множители $\left(\frac{p}{q}\right)$, $\left(\frac{p'}{q}\right)$ для символов $\left(\frac{a}{p}\right)$, $\left(\frac{a}{p'}\right)$ будут равны соответственно 1 и -1, а все остальные множители будут равны 1. Таким образом, $\left(\frac{a}{p}\right)=1$, $\left(\frac{a}{p'}\right)=-1$, в то время как по нашей конструкции $p\equiv p' \bmod |f(a)|/q$.

Для $q=2$ мы поступим точно так же. Согласно I п. 4, в этом случае $k(a)\not\equiv 1 \bmod 4$ и $|f(a)|=4|k(a)|$. Выберем тогда

$$\left\{\begin{array}{l} p\equiv 1 \bmod |k(a)|, \quad p\equiv 1 \bmod 4 \\ p'\equiv 1 \bmod |k(a)|, \; p'\equiv -1 \bmod 4 \end{array}\right\}, \text{ если } k(a)\equiv -1 \bmod 4,$$

$$\left\{\begin{array}{l} p\equiv 1 \bmod \frac{|k(a)|}{2}, \quad p\equiv 1 \bmod 8 \\ p'\equiv 1 \bmod \frac{|k(a)|}{2}, \quad p'\equiv 5 \bmod 8 \end{array}\right\}, \text{ если } 2|k(a).$$

Тогда для $\left(\frac{a}{p}\right)$, $\left(\frac{a}{p'}\right)$ в формуле (3) из доказательства утверждения I п. 4 мы будем иметь, что в случае $k(a)\equiv -1 \bmod 4$ $((p-1)/2)$-я и $((p'-1)/2)$-я степени будут равны соответственно 1 и -1, а все остальные множители равны 1. в случае же $2|k(a)$ $((p^*-1)/4)$-я и $((p'^*-1)/2)$-я степени будут равны соответственно 1 и -1, а все остальные множители снова равны 1. Таким образом, опять-таки $\left(\frac{a}{p}\right)=1$, $\left(\frac{a}{p'}\right)=-1$, в то время как по конструкции

$$p\equiv p' \bmod 2|k(a)|, \text{ соответственно } \bmod 4\,\frac{|k(a)|}{2},$$

и потому в каждом случае $p\equiv p' \bmod |f(a)|/2$.

Примеры. $a=3$, $f(a)=4\cdot 3=12$.

$\left(\frac{3}{p}\right)=\left(\frac{p^*}{3}\right)=\pm 1$, в зависимости от $p^*\equiv \pm 1 \bmod 3$,

$p \bmod 12$	1	5	$7\equiv -5$	$11\equiv -1$
$\left(\frac{3}{p}\right)$	1	-1	-1	1

$a=-3$, $f(a)=-3$.

$\left(\frac{-3}{p}\right)=\left(\frac{p}{3}\right)=\pm 1$, в зависимости от $p\equiv \pm 1 \bmod 3$.

$p \bmod 3$	1	$2\equiv -1$
$\left(\frac{-3}{p}\right)$	1	-1

$a=5$, $f(a)=5$.

$\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right)=1$ или -1, в зависимости от того, $p\equiv\pm1$ или $\pm2 \bmod 5$.

$p \bmod 5$	1	2	$3\equiv-2$	$4\equiv-1$
$\left(\frac{5}{p}\right)$	1	-1	-1	1

$a=7$, $f(a)=4\cdot7=28$.

$\left(\frac{7}{p}\right)=\left(\frac{p^*}{7}\right)=\pm1$, в зависимости от $p^*\equiv\pm(1, 2, 4) \bmod 7$.

$p \bmod 28$	1	3	5	9	11	13	$15\equiv-13$	$17\equiv-11$	$19\equiv-9$	$23\equiv-5$	$25\equiv-3$	$27\equiv-1$
$\left(\frac{7}{p}\right)$	1	1	-1	1	-1	-1	-1	-1	1	-1	1	1

$a=-6=-2\cdot3$, $f(a)=-4\cdot6=-24$.

$\left(\frac{-6}{p}\right)=(-1)^{\frac{p^*-1}{4}}\left(\frac{-3}{p}\right)$, где $\left(\frac{-3}{p}\right)$ определенно выше.

$p \bmod 24$	1	5	7	11	$13\equiv-11$	$17\equiv-7$	$19\equiv-5$	$23\equiv-1$
$\left(\frac{-6}{p}\right)$	1	1	1	1	-1	-1	-1	-1

$a=21=3\cdot7$, $f(a)=21$.

$\left(\frac{21}{p}\right)=\left(\frac{3}{p}\right)\left(\frac{7}{p}\right)$, где $\left(\frac{3}{p}\right)$, $\left(\frac{7}{p}\right)$ определены выше.

$p \bmod 21$	1	2	4	5	8	10	$11\equiv-10$	$13\equiv-8$	$16\equiv-5$	$17\equiv-4$	$19\equiv-2$	$20\equiv-1$
$\left(\frac{21}{p}\right)$	1	-1	1	1	-1	-1	-1	-1	1	1	-1	1

Хотя в высказывании IV для нас важна только абсолютная величина $|f(a)|$, мы для дальнейшего сформулировали определение $f(a)$ в I п. 4 с учетом знака, который совпадает со знаком числа a. В предыдущих примерах распределение значений ±1 символа Лежандра в наименьшей системе вычетов по $\bmod|f(a)|$, взаимно простых с модулем, для $f(a)>0$ симметрично, а для $f(a)<0$ кососимметрично (симметричные члены противоположны

по знаку!) относительно среднего значения $|f(a)|/2$. В § 9, п. 5 мы покажем связь знака числа $f(a)$ с характеристическим свойством ведущего модуля и получим при этом правильность этого закона симметричности в общем случае.

§ 8. КВАДРАТИЧНЫЙ ЗАКОН ВЗАИМНОСТИ: ДОКАЗАТЕЛЬСТВО С ПОМОЩЬЮ ГАУССОВЫХ СУММ

1. Корни простой степени из 1. Ввиду большого значения квадратичного закона взаимности, мы приведем здесь еще одно его доказательство, базирующееся на совершенно других основах. В то время как наше первое доказательство, данное в § 7, п. 2, 3, основывалось, главным образом, на лемме Гаусса, т. е. на элементарной теоретико-числовой формуле для символа Лежандра, второе доказательство впервые даст представление о том, что этот закон имеет глубокие корни в теории алгебраических чисел. Хотя для характеристики символа Лежандра это доказательство использует элементарный теоретико-числовой критерий Эйлера, однако оно требует расширения области целостности Γ целых рациональных чисел и основ теории сравнений для этой расширенной области. Речь идет об области целостности $\Gamma[\zeta]$ всех многочленов с коэффициентами из Γ от корня ζ простой степени p из 1. Предварительно мы должны ознакомиться с простейшими фактами о p-х корнях из 1.

Сначала пусть n — какое-нибудь натуральное число. Под *n-ми корнями из* 1 мы понимаем n корней многочлена $x^n - 1$. Так как производная nx^{n-1} этого многочлена ни для одного из этих корней не обращается в 0, то эти n корней различны между собой. Далее, так как произведение и частное n-х корней из 1 снова являются таковыми, то n-ые корни из 1 образуют мультипликативную абелеву группу порядка n. Из основ анализа известно, что эта группа циклична, а именно, n-ые корни из 1 выражаются в полярных координатах в виде

$$\zeta^\nu = e^{\frac{2\pi i\nu}{n}} \qquad (\nu \bmod n),$$

т. е. являются степенями одного из них ($\zeta = e^{2\pi i/n}$). Вообще, n-й корень из 1, который, как в данном случае $\zeta = e^{2\pi i/n}$, имеет порядок, в точности равный n, и поэтому порождает всю группу, называется *первообразным n-м корнем из* 1. Существует $\varphi(n)$ первообразных корней, а именно, степени ζ^ν одного из них с ν, взаимно простым с n. Вместо того, чтобы опираться на относящееся к анализу понятие полярных координат, можно также доказать существование первообразного n-го корня ζ из 1 чисто алгебраически, а именно, точно следуя схеме доказательства существования первообразного корня $w \bmod p$ в § 5, п. 2; там

ведь речь идет просто о специальном случае $n = p - 1$, причем, конечно, основным полем (единичным элементом которого являются коэффициенты многочлена $x^n - 1$) является там не поле рациональных чисел P, как здесь, а простое поле Π из p элементов. Мы ограничимся здесь этим указанием, так как это касается фактов, относящихся к алгебре, а не к теории чисел.

Пусть теперь $n = p$ — простое число. Так как тогда группа p-х корней из 1 имеет порядок p, то существование первообразного p-го корня ζ из 1 непосредственно очевидно из чисто алгебраических соображений. Каждый отличный от 1 корень многочлена $x^p - 1$, другими словами, каждый корень многочлена

$$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \ldots + x + 1$$

имеет тогда порядок, равный отличному от 1 делителю числа p, т. е. необходимо равный самому p.

Для дальнейшего важен следующий факт:

I. *Многочлен* $f(x) = x^{p-1} + \ldots + x + 1$ *неприводим над полем рациональных чисел* P.

Доказательство. Неприводимость многочлена $f(x)$ равносильна неприводимости получающегося из него подстановкой $x = y + 1$ многочлена

$$g(y) = \frac{(y+1)^p - 1}{y} = y^{p-1} + \binom{p}{1} y^{p-2} + \ldots + \binom{p}{p-1}.$$

Наряду с этим последним мы рассмотрим также и получающийся из него подстановкой $y = 1/z$ и умножением на z^{p-1} многочлен

$$h(z) = \binom{p}{p-1} z^{p-1} + \ldots + \binom{p}{1} z + 1.$$

Согласно XIV п. 11 § 4, коэффициенты этих многочленов, за исключением первого коэффициента первого многочлена и последнего коэффициента второго многочлена, делятся на p.

Собственное разложение многочлена $g(y)$ над полем рациональных чисел P после умножения на общие знаменатели коэффициентов обоих сомножителей можно считать имеющим вид

$$ab \cdot g(y) = (a_r y^r + \ldots + a_0)\ (b_s y^s + \ldots + b_0), \tag{1}$$

где r, s — натуральные числа, $r + s = p - 1$ и $a_r, \ldots, a_0, a$, так же как $b_s, \ldots, b_0, b$ — две системы взаимно простых целых чисел; тогда наряду с этим имеет место также

$$ab \cdot h(z) = (a_0 z^r + \ldots + a_r)\ (b_0 z^s + \ldots + b_s). \tag{2}$$

Если в (1) a_ρ, b_σ — первые, считая слева, коэффициенты соответствующих многочленов, которые $\not\equiv 0 \bmod p$, то в произведении наивысшим членом, коэффициент которого $\not\equiv 0 \bmod p$, будет $a_\rho b_\sigma y^{\rho+\sigma}$.

Сравнивая с коэффициентами многочлена $ab\cdot g(y)$, получаем, что необходимо $\rho+\sigma=p-1$, и, таким образом, $\rho=r$, $\sigma=s$, а также $ab\equiv a_r b_s \not\equiv 0 \bmod p$.

Если в (2) a_μ, b_ν — первые, считая слева, коэффициенты соответствующих многочленов, которые $\not\equiv 0 \bmod p$, то в произведении наивысшим членом с коэффициентом, $\not\equiv 0 \bmod p$, будет $a_\mu b_\nu z^{(p-1)-(\mu+\nu)}$. Сравнивая это с коэффициентами многочлена $abh(z)$, видим, что необходимо $\mu+\nu=p-1$, т. е. $\mu=r$, $\nu=s$, и потому $a_0, \ldots, a_{r-1}$; $b_0, \ldots, b_{s-1} \equiv 0 \bmod p$.

Но $a_0 b_0 = \binom{p}{p-1} ab = pab$. Как следует из (1), в это число входит только p^1, а как следует из (2) — по меньшей мере p^2. Таким образом, предположение о существовании собственного разложения многочлена $f(x)$ над полем P приводит к противоречию.

2. Гауссовы суммы. Пусть p — нечетное простое число и ζ — раз навсегда выбранный первообразный p-й корень из 1. Мы сопоставим каждому первообразному p-му корню ζ^a ($a \not\equiv 0 \bmod p$) из 1 *принадлежащую квадратичному характеру* $\left(\frac{x}{p}\right)$ *гауссову сумму*

$$\tau_a = \sum_{x \not\equiv 0 \bmod p} \left(\frac{x}{p}\right) \zeta^{ax}.$$

Все эти $p-1$ гауссовых сумм могут быть выражены через

$$\tau = \sum_{x \not\equiv 0 \bmod p} \left(\frac{x}{p}\right) \zeta^{x},$$

т. е. через сумму $\tau_1 = \tau$, соответствующую $\zeta^1 = \zeta$. Именно, имеет место формула

$$\tau_a = \left(\frac{a}{p}\right) \tau. \tag{1}$$

Доказательство. Произведя в определении τ_a замену переменной суммирования $ax \equiv y \bmod p$, допускающую однозначное обращение $x \equiv a^{-1} y \bmod p$ (понимаемое в смысле § 4, п. 10), мы получим

$$\tau_a = \sum_{y \not\equiv 0 \bmod p} \left(\frac{a^{-1}y}{p}\right) \zeta^y = \left(\frac{a^{-1}}{p}\right) \sum_{y \not\equiv 0 \bmod p} \left(\frac{y}{p}\right) \zeta^y = \left(\frac{a}{p}\right) \tau,$$

причем мы использовали, что $\left(\frac{a^{-1}}{p}\right) = \left(\frac{a}{p}\right)^{-1} = \left(\frac{a}{p}\right)$.

Теперь мы перейдем к лежащей в основе всего нашего доказательства, а, помимо того, важной и вообще формуле

$$\tau^2 = p^*, \text{ или } \tau = \pm\sqrt{p^*}, \tag{2}$$

которая с точностью до знака определяет значение τ.

Доказательство. Из формулы, определяющей τ, мы формальным перемножением получаем представление в виде двойной суммы

$$\tau^2 = \sum_{x,\, y \not\equiv 0 \bmod p} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\zeta^x\zeta^y = \sum_{x,\, y \not\equiv 0 \bmod p} \left(\frac{xy}{p}\right)\zeta^{x+y}.$$

Если для каждого фиксированного значения $x \bmod p$ произвести замену переменной суммирования $y \equiv xt \bmod p$, допускающую однозначное обращение $t \equiv x^{-1}y \bmod p$, то получится

$$\tau^2 = \sum_{x,\, t \not\equiv 0 \bmod p} \left(\frac{x^2t}{p}\right)\zeta^{x+xt} = \sum_{x,\, t \not\equiv 0 \bmod p} \left(\frac{x}{p}\right)^2\left(\frac{t}{p}\right)\zeta^{x(1+t)} =$$

$$= \sum_{t \not\equiv 0 \bmod p} \left(\frac{t}{p}\right) \sum_{x \not\equiv 0 \bmod p} \zeta^{x(1+t)}.$$

Но вообще

$$\sum_{x \not\equiv 0 \bmod p} \zeta^{ax} = \begin{Bmatrix} p-1 & \text{для} & a \equiv 0 \bmod p \\ -1 & \text{для} & a \not\equiv 0 \bmod p \end{Bmatrix},$$

причем последнее следует из того, что ζ^{ax} пробегает в точности $p-1$ первообразных p-х корней из 1, другими словами, все корни многочлена $f(x) = x^{p-1} + \ldots + x + 1$. Поэтому далее следует

$$\tau^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{t \not\equiv 0, -1 \bmod p} \left(\frac{t}{p}\right) = \left(\frac{-1}{p}\right)p - \sum_{t \not\equiv 0 \bmod p} \left(\frac{t}{p}\right) =$$

$$= (-1)^{\frac{p-1}{2}} p - 0 = p^*,$$

причем мы использовали то, что $\sum_{t \not\equiv 0 \bmod p} \left(\frac{t}{p}\right) = 0$, так как существует одинаковое количество квадратичных вычетов и невычетов $t \bmod p$.

Заметим еще, что определение знака гауссовой суммы τ в (2) требует весьма глубоких методов. В то время как формула (2) не зависит от выбора первообразного p-го корня ζ из 1, знак τ зависит от этого нормирования, как показывает (1). При определении знака обычно используют аналитическое нормирование $\zeta = e^{2\pi i/p}$; в этом случае имеет место

$$\tau = \sqrt{p} \quad \text{для} \quad p \equiv 1 \bmod 4,$$

$$\tau = i\sqrt{p} \quad \text{для} \quad p \equiv -1 \bmod 4$$

с положительным значением квадратного корня. Мы еще вернемся к этому в четвертой главе (см. § 20, п. 5).

3. Доказательство закона взаимности. Пусть теперь дано еще одно нечетное простое число $q \neq p$. Как показано в § 4, п. 11, для неизвестных x, y выполняется сравнение $(x+y)^q \equiv x^q + y^q \bmod q$, в том смысле что коэффициенты при одинаковых степенях x, y слева и справа сравнимы между собой по $\bmod q$, что обозначено здесь знаком $\equiv$. Соответствующее правило, очевидно, имеет место и для сумм с бо́льшим количеством членов, что немедленно получается посредством полной индукции. Если применить это правило к формуле, определяющей гауссову сумму τ, и заметить, что $\left(\frac{x}{p}\right)^q = \left(\frac{x}{p}\right)$, то получится сравнение

$$\left(\sum_{x \not\equiv 0 \bmod p} \left(\frac{x}{p}\right) \zeta^x\right)^q \equiv \sum_{x \not\equiv 0 \bmod p} \left(\frac{x}{p}\right) \zeta^{qx} \bmod q$$

или, другими словами,

$$\tau^q \equiv \tau_q \bmod q, \tag{3}$$

теперь в том смысле, что сравнимы между собой коэффициенты при одинаковых степенях ζ слева и справа. Но теперь ζ не неизвестное, а число, удовлетворяющее алгебраическому уравнению $f(\zeta) = 0$. Поэтому между различными степенями ζ существуют линейные зависимости и заранее не ясно, будут ли сравнения такого рода оставаться справедливыми, если мы будем преобразовывать стоящие в них выражения, используя эти зависимости. Далее, не ясно также, можно ли оперировать с такими сравнениями по правилам, имеющим место для обычных сравнений.

Мы закончим сначала формальную часть доказательства и предположим для этого, что и то и другое действительно верно. Потом мы дадим исчерпывающее обоснование.

Из нашего исходного сравнения (3), согласно (1), получается сравнение

$$\tau^q \equiv \left(\frac{q}{p}\right) \tau \bmod q. \tag{4}$$

Чтобы не загружать наше дальнейшее обоснование доказательством возможности деления обеих сторон сравнения на τ, умножим это сравнение на τ и применим к обеим его сторонам (2); тогда

$$(p^*)^{\frac{q+1}{2}} \equiv \left(\frac{q}{p}\right) p^* \bmod q. \tag{5}$$

Но здесь с обеих сторон стоят уже целые рациональные числа. Если, таким образом, наши новые сравнения являются имеющим смысл обобщением обычных сравнений, то далее следует

$$(p^*)^{\frac{q+1}{2}} \equiv \left(\frac{q}{p}\right) p^* \bmod q \tag{6}$$

также и в обычном смысле. Тогда мы можем сократить взаимно простой с q множитель p^* и окончательно получим

$$(p^*)^{\frac{q-1}{2}} \equiv \left(\frac{q}{p}\right) \bmod q.$$

Сравнение этой формулы, полученной с помощью гауссовых сумм, с критерием Эйлера

$$(p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \bmod q$$

дает общую формулу закона взаимности

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right),$$

и притом сразу в изящной форме формулы обращения из § 7, п. 3.

Путь, приводящий от нашего исходного сравнения к формуле закона взаимности, очень краток и свободен от выкладок в собственном смысле этого слова; однако в доказательствах используемых формул (1), (2) для гауссовой суммы τ некоторые выкладки все же проделываются. Но в теории алгебраических чисел и эта подготовительная часть доказательства принципиально может быть проведена так, что формула (1) и формула закона взаимности получатся как высказывания о структурных соотношениях между полем p-х корней из 1 и содержащимся в нем, согласно (2), квадратичным подполем $\mathsf{P}(\sqrt{p^*})$ (см. § 9, п. 3).

4. Обоснование доказательства посредством теории сравнений в области корней из 1. Гауссова сумма τ является числом поля $\mathsf{P}(\zeta)$ p-х корней из 1, получающегося присоединением ζ к P и состоящего из всех рациональных функций с коэффициентами из P от первообразного p-го корня ζ из 1; при этом τ принадлежит даже к содержащейся в $\mathsf{P}(\zeta)$ области целостности $\Gamma[\zeta]$ всех целых рациональных функций от ζ с коэффициентами из Γ. Нам достаточно рассматривать здесь только эту область целостности $\Gamma[\zeta]$.

Каждую целую рациональную функцию от ζ можно, используя равенства

$$\zeta^p = 1 \text{ и более тонкое } \zeta^{p-1} + \zeta^{p-2} + \ldots + \zeta + 1 = 0,$$

преобразовать следующим образом:

$$\sum_{\nu=0}^{n} c_\nu \zeta^\nu = \sum_{\rho=0}^{p-1} b_\rho \zeta^\rho = \sum_{\rho=0}^{p-2} a_\rho \zeta^\rho,$$

где

$$b_\rho = \sum_{\substack{\nu=0 \\ \nu \equiv \rho \bmod p}}^{n} c_\nu, \quad a_\rho = b_\rho - b_{p-1}.$$

Если первоначальные коэффициенты c_ν были целыми рациональными числами, то получающиеся при этом коэффициенты b_ρ и a_ρ тоже будут целыми рациональными числами. Поэтому каждое число α из $\Gamma[\zeta]$ может быть представлено в виде многочлена от ζ с коэффициентами a_ρ из Γ, имеющего степень, $< p-1$. Это представление однозначно. Действительно, если бы было два различных представления для α такого вида, то посредством вычитания мы получили бы алгебраическое уравнение $g(\zeta) = 0$ с коэффициентами из Γ, которые не все равны 0, причем степень этого уравнения $< p-1$. Это, однако, противоречит установленной в § 1, п. 1 неприводимости над полем P многочлена $f(x)$ степени $p-1$, из которой следует, что $f(\zeta) = 0$ является уравнением наинизшей степени с коэффициентами из P, которому может удовлетворять ζ. Таким образом, мы показали:

II. *Числа α из $\Gamma[\zeta]$ однозначно представляются через базис в виде*

$$\alpha = \sum_{\rho=0}^{p-2} a_\rho \zeta^\rho \quad \text{с } a_\rho \text{ из } \Gamma.$$

Для чисел α из $\Gamma[\zeta]$ можно теперь построить, поскольку речь идет здесь об области целостности, элементарную теорию делимости, аналогичную теории § 1, п. 2 для чисел a из Γ, причем, однако, вместо фигурирующих там двух единиц ± 1 теперь в качестве единиц будут фигурировать все существующие в $\Gamma[\zeta]$ делители числа 1. Этими единицами, изучение которых требует особой теории, нам здесь заниматься нет необходимости. Для нас важно только то, что на основе элементарной теории делимости в $\Gamma[\zeta]$ можно построить аналогично § 4, п. 1, 2, элементарную теорию сравнений, если сравнимость $\alpha \equiv \beta \bmod \mu$ определить через делимость $\mu \mid \alpha - \beta$. Так как $\Gamma[\zeta]$ есть область целостности, то для определенного таким образом понятия сравнимости снова имеют место формальные правила действий в пределах первых трех элементарных операций, т. е. классы вычетов по $\bmod \mu$ образуют кольцо. В связи с этим см. также § 4, п. 10, где говорилось о распространении понятия сравнимости на область целостности Γ_m.

Нам нужно рассмотреть здесь только специальный случай, когда модуль $\mu = m$ является целым рациональным числом (не обязательно натуральным). В этом случае на основании представления II легко можно указать явный критерий для сравнимости по $\bmod m$ в $\Gamma[\zeta]$, а также получить тотчас же обзор эле-

ментов кольца классов вычетов по $\bmod m$ в $\Gamma[\zeta]$ в виде полной системы вычетов. Именно, имеет место

III. *Если m — натуральное число, то для двух чисел*

$$\alpha = \sum_{\rho=0}^{p-2} a_\rho \zeta^\rho, \quad \beta = \sum_{\rho=0}^{p-2} b_\rho \zeta^\rho \quad (a_\rho,\ b_\rho \text{ в } \Gamma),$$

заданных в представлении через базис, сравнение

$$\alpha \equiv \beta \bmod m$$

выполняется тогда и только тогда, когда выполняются сравнения

$$a_\rho \equiv b_\rho \bmod m \qquad (\rho = 0,\ \ldots,\ p-2)$$

для коэффициентов из Γ.

Поэтому m^{p-1} чисел α, у которых $p-1$ коэффициентов a_ρ выбраны всеми возможными способами из полной системы вычетов по $\bmod m$ в Γ, образуют полную систему вычетов по $\bmod m$ в $\Gamma[\zeta]$.

Доказательство. Согласно определению, сравнение $\alpha \equiv \beta \bmod m$ в $\Gamma[\zeta]$ равносильно выполнению равенства $\alpha = \beta + \gamma m$ с некоторым числом γ из $\Gamma[\zeta]$. Выражая также и это число в представлении через базис

$$\gamma = \sum_{\rho=0}^{p-2} g_\rho \zeta^\rho \qquad (g_\rho \text{ в } \Gamma),$$

мы получим равенство вида

$$\sum_{\rho=0}^{p-2} a_\rho \zeta^\rho = \sum_{\rho=0}^{p-2} (b_\rho + g_\rho m)\zeta^\rho,$$

а оно, в силу однозначности представления через базис, сводится к существованию равенств

$$a_\rho = b_\rho + g_\rho m \qquad (\rho = 0,\ \ldots,\ p-2)$$

для коэффициентов, т. е. к выполнению в Γ сравнений

$$a_\rho \equiv b_\rho \bmod m.$$

На основании критерия III мы теперь можем установить, так же как в § 4, п. 10 для сделанного там обобщения понятия сравнимости на Γ_m, что при обобщении понятия сравнимости по $\bmod m$ на область целостности $\Gamma[\zeta]$ имеет место следующий факт:

IV. *Если m — натуральное число, то для чисел a, b из Γ существование сравнения $a \equiv b \bmod m$ в смысле сравнимости в $\Gamma[\zeta]$ равносильно существованию этого сравнения в смысле сравнимости в Γ.*

Доказательство. Для чисел a из Γ однозначное представление II через базис, очевидно, имеет вид

$$a = a + 0 \cdot \zeta + \ldots + 0 \cdot \zeta^{p-2}.$$

Таким образом, среди чисел α из $\Gamma[\zeta]$ они характеризуются тем, что $a_1, \ldots, a_{p-2} = 0$, в то время как $a_0 = a$. Поэтому для двух чисел a, b из Γ критерий III для сравнимости $a \equiv b \bmod m$ в $\Gamma[\zeta]$ действительно сводится к выполнению сравнения $a \equiv b \bmod m$ в Γ.

В дальнейшее развитие теории сравнений в $\Gamma[\zeta]$ мы здесь вдаваться не будем, так как приведенные выше рассуждения уже дают нам в руки все необходимое для того, чтобы полностью обосновать наше доказательство в п. 3. Исходное сравнение (3) есть сравнение по $\bmod q$ в $\Gamma[\zeta]$ (употребляемый там знак $\equiv$ соответствует добавлению «в $\Gamma[\zeta]$» к знаку $=$ в предшествующих рассуждениях); действительно, согласно определению, оно означает, что $\tau^q - \tau_q$ есть целая рациональная функция от ζ с целыми рациональными коэффициентами, делящимися на q, т. е. произведение числа q на некоторое число из $\Gamma[\zeta]$. Законность перехода от (3) к (4) теперь очевидна; в самом деле, при этом только τ_q из $\Gamma[\zeta]$ заменяется в правой части сравнения другим *представлением* $\left(\frac{q}{p}\right)\tau$ в виде многочлена от ζ, а теперь, когда установлено, что понятие сравнимости инвариантно (не зависит от представления через ζ), это не имеет значения. Умножение на τ, приводящее от (4) к (5), согласно элементарным правилам действий над сравнениями, и переход от сравнения (5) в $\Gamma[\zeta]$ к такому же сравнению (6) в Γ законны в силу доказанной выше теоремы IV.

5. Доказательство второго дополнения к закону взаимности. Данное только что доказательство общей формы закона взаимности опирается на критерий Эйлера в отличие от данного в § 7, п. 3 элементарного доказательства, опирающегося на лемму Гаусса. В то время как первое дополнение к закону взаимности получалось в § 7, п. 2 в качестве непосредственного следствия из критерия Эйлера, для доказательства второго дополнения там тоже оказалось необходимым привлечь лемму Гаусса. Мы покажем, что для второго дополнения к закону взаимности тоже можно дать доказательство, опирающееся на критерий Эйлера, если привлечь для этой цели некоторую специальную гауссову сумму и теорию сравнений в соответствующей области корней из 1.

Для этого нам нужно рассмотреть область целостности $\Gamma[\zeta]$, где ζ есть первообразный корень из 1 степени $n = 8$, т. е. корень многочлена

$$f(x) = \frac{x^8 - 1}{x^4 - 1} = x^4 + 1,$$

который как раз имеет корнями $\varphi(8)=4$ первообразных 8-ых корня из 1: ζ, ζ^3, ζ^5, ζ^7, т. е. такие 8-е корни из 1, которые не являются в то же время 4-ми корнями из 1. Если ввести еще первообразный 4-й корень $\zeta^2=i$ из 1, являющийся корнем многочлена $x^2+1=(x-i)(x+i)$, то все 8-е корни из 1 можно представить в следующей форме:

$\nu \bmod 8$	0	1	2	3	4	5	6	7
ζ^ν	1	ζ	i	$i\zeta$	-1	$-\zeta$	$-i$	$-i\zeta$

Многочлен $f(x)=x^4+1$ неприводим над P, так как, с одной стороны, он, согласно IV п. 6 § 1, не имеет корней в P и потому не может быть разложен на два множителя первой и третьей степени, а с другой стороны, как мы сейчас покажем, он не обладает также разложением и на два множителя второй степени. Последнее доказывается следующим образом. Такое разложение обязательно должно иметь вид

$$x^4+1=(x^2+ax+b)\left(x^2-ax+\frac{1}{b}\right)$$

с

$$a^2=b+\frac{1}{b},\quad a\left(b-\frac{1}{b}\right)=0.$$

При этом обязательно или $a=0$ и тогда $b^2=-1$, или $b-\frac{1}{b}=0$, откуда $b=\pm 1$, и тогда $a^2=\pm 2$. Согласно IV п. 6 § 1, ни то ни другое, однако, невозможно ни для каких a, b из P.

Как и в п. 4, из неприводимости $f(x)$ следует, что числа α из $\Gamma[\zeta]$ обладают однозначным представлением через базис

$$\alpha=a_0+a_1\zeta+a_2\zeta^2+a_3\zeta^3=(a_0+a_2i)+(a_1+a_3i)\zeta$$

с a_0, a_1, a_2, a_3 из Γ,

и при этом числа a из Γ характеризуются тем, что a_1, a_2, $a_3=0$, $a=a_0$. Поэтому развитая в п. 4 теория сравнений по $\bmod m$ переносится на рассматриваемую здесь область целостности $\Gamma[\zeta]$.

После этих предварительных замечаний доказательство второго дополнения к закону взаимности может быть проведено аналогично доказательству общей формы этого закона, а именно, следующим образом.

Рассмотрим *принадлежащие квадратичному характеру* $(-1)^{(x^*-1)/4}$ *гауссовы суммы*

$$\tau_a = \sum_{\substack{x \bmod 8 \\ x \not\equiv 0 \bmod 2}} (-1)^{\frac{x^*-1}{4}} \zeta^{ax},$$

образованные с помощью четырех первообразных 8-ых корней ζ^a $(a \not\equiv 0 \bmod 2)$ из 1. Они могут быть выражены через одну из них, а именно, через

$$\tau = \sum_{\substack{x \bmod 8 \\ x \not\equiv 0 \bmod 2}} (-1)^{\frac{x^*-1}{4}} \zeta^{x}$$

в виде

$$\tau_a = (-1)^{\frac{a^*-1}{4}} \tau. \tag{1}$$

Это доказывается, точно так же, как соответствующий факт (1) в п. 2 на основании того, что $(-1)^{(x^*-1)/4} = \chi_8(x)$ является квадратичным характером по mod 8 в смысле § 6, п. 4 (это видно из того, что, согласно § 5, п. 7, $(x^*-1)/4 \bmod 2$ фигурирует в представлении через базис для $x \bmod 8$ в качестве показателя степени при 5). Вместо доказательства факта (2) из п. 2 здесь можно легко вычислить явное значение τ:

$$\tau = \zeta^1 - \zeta^3 - \zeta^5 + \zeta^7 = \zeta\,(1 - \zeta^2 - \zeta^4 + \zeta^6) = \zeta\,(1 - i + 1 - i) = 2\zeta\,(1 - i).$$

Отсюда следует, принимая во внимание, что $(1-i)^2 = -2i$,

$$\tau^2 = 8. \tag{2}$$

Пусть теперь дано нечетное простое число q. Возводя формулу для τ в степень q, мы получим, как и в п. 3, сравнение в $\Gamma[\zeta]$:

$$\tau^q \equiv \tau_q \bmod 8.$$

Согласно (1), из него следует

$$\tau^q \equiv (-1)^{\frac{q^*-1}{4}} \tau \bmod q.$$

Отсюда умножением на τ и применением (2) мы получаем

$$8^{\frac{q+1}{2}} \equiv (-1)^{\frac{q^*-1}{4}} 8 \bmod q,$$

т. е. сравнение по mod q между числами из Γ, которое поэтому можно понимать как сравнение в Γ. Сокращение на взаимно простой с q множитель 8 дает

$$8^{\frac{q-1}{2}} \equiv (-1)^{\frac{q^*-1}{4}} \bmod q,$$

в то время как, согласно критерию Эйлера,

$$8^{\frac{q-1}{2}} \equiv \left(\frac{8}{q}\right) \equiv \left(\frac{2}{q}\right) \bmod q.$$

Сравнение двух последних формул дает второе дополнение к закону взаимности:

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^*-1}{4}}.$$

§ 9. ОБОБЩЕНИЕ СИМВОЛА ЛЕЖАНДРА: СИМВОЛ ЯКОБИ

1. Определение символа Якоби. При исследовании символа Лежандра $\left(\frac{a}{p}\right)$ как функции его знаменателя p в § 7, п. 4, 5 была выяснена целесообразность расширения определения этого символа на составные знаменатели. Это расширение будет теперь сделано по методу Якоби.

По сказанному в § 7, п. 4 мы уже знаем, как нужно ввести это более широкое определение. Из закона взаимности там следовало, что $\left(\frac{a}{p}\right) = \chi_{|f(a)|}(p)$ имеет в области нечетных простых чисел p, не входящих в a, свойство *характера* [(2) из § 6, п. 4] *по* определяемому числом a в соответствии с I п. 4 § 7 *модулю* $|f(a)|$ (ведущему модулю), и притом *квадратичного* характера, так как выполняется также и свойство (3) из § 6, п. 4. Поэтому расширение определения должно быть сделано так, чтобы выполнялось еще и свойство (1) из § 6, п. 4, а именно, *мультипликативность*, о которой не могла идти речь в рассматривавшейся до сих пор области значений аргумента, состоявшей только из простых чисел p.

В соответствии со сказанным введем

Определение символа Якоби. *Для двух рациональных чисел a, $b \neq 0$ со свойствами:*

b взаимно просто с 2, a взаимно просто с b, положим, в соответствии с разложением

$$b = \prod_p p^{\beta_p}$$

числа b на простые множители:

$$\left(\frac{a}{b}\right) = \prod_p \left(\frac{a}{p}\right)^{\beta_p}.$$

Так, определенный символ Якоби $\left(\frac{a}{b}\right)$ имеет в области его определения следующие свойства. Прежде всего, он, будучи

произведением символов Лежандра $\left(\frac{a}{p}\right)$, мультипликативен по a, т. е. имеет место правило

$$\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right). \tag{1}$$

Далее, этот символ, согласно его определению, опирающемуся на разложение на простые множители, мультипликативен также и по b, т. е. имеет место правило

$$\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right). \tag{2}$$

Символ принимает лишь значения, равные обеим единицам ± 1, так что $\left(\frac{a}{b}\right)^2 = 1$. Отсюда, согласно правилам (1), (2), следует, что

$$\left(\frac{ax^2}{b}\right) = \left(\frac{a}{b}\right), \quad \left(\frac{a}{by^2}\right) = \left(\frac{a}{b}\right) \tag{3}$$

для любых, допустимых в соответствии с определением, рациональных x, $y \neq 0$, т. е. что значение символа остается неизменным, если в числителе или знаменателе приписать квадратные множители, допустимые в соответствии с определением.

То, что в (3) на квадратные множители накладываются предписанные определением ограничения

x взаимно просто с b, y взаимно просто с 2 и a,

очевидно, не имеет существенного значения. Именно, если ввести еще и разложение

$$a = (-1)^{\alpha} \prod_q q^{\alpha_q}$$

числа a на простые множители, то формулу, определяющую символ Якоби, можно будет записать в виде

$$\left(\frac{a}{b}\right) = \prod_p \left(\frac{-1}{p}\right)^{\beta_p} \cdot \prod_{p,\,q} \left(\frac{q}{p}\right)^{\alpha_q \beta_p}. \tag{4}$$

При таком способе записи в произведения формально входят не определенные нами множители с $q = p$ или $p = 2$, однако в действительности они выпадают, так как, согласно предположению относительно a, b, показатели степени $\alpha_q \beta_p$, соответственно $\alpha\beta_p$ у этих множителей равны 0. Если теперь условиться, что формула (4) должна определять символ $\left(\frac{a}{b}\right)$ также и в том случае, когда имеются неопределенные множители с $q = p$ или $p = 2$ и для них выполнены только условия $\alpha_q \beta_p$, соответственно $\alpha\beta_p \equiv 0 \bmod 2$ (а не обязательно $= 0$), то мы, очевидно, достигнем того, что рациональные числа x, y в (3) должны будут подчиняться

только тривиальному ограничению $x, y \neq 0$. Это дальнейшее, чисто формальное обобщение, отличающееся от обобщения Якоби в обычном его смысле, часто оказывается целесообразным из соображений законченности и красоты. В силу мультипликативной структуры формулы (4), правила (1), (2) при этом сохраняются. Предположения, при которых тогда будет определен символ Якоби, кратко могут быть высказаны так же, как и в первоначальном определении, но с заменой чисел a, b их свободными от квадратов ядрами $k(a)$, $k(b)$ (см. § 7, п. 4):

$k(b)$ *взаимно просто с* 2, $k(a)$ *взаимно просто с* $k(b)$.

Мы, однако, не всегда будем класть в основу эту максимально возможную область определения символа Якоби, а будем сужать ее посредством введения более сильных ограничений, если этого будет требовать природа рассматриваемых вопросов.

Предварительно скажем коротко о смысле и целях наших дальнейших исследований символа Якоби. В § 7, п. 4, 5, в качестве следствия из квадратичного закона взаимности выяснилось, что символ Лежандра $\left(\frac{a}{p}\right)$ определяет разбиение всех нечетных простых чисел $p \nmid k(a)$ на два класса, а именно, на класс тех, для которых $\left(\frac{a}{p}\right) = 1$, и класс тех, для которых $\left(\frac{a}{p}\right) = -1$, причем это разбиение может быть описано значениями простых чисел p по $\mathrm{mod}\,|f(a)|$ (с определенным там значением $f(a)$). Это разбиение на классы будет иметь основное значение для арифметики квадратичного поля $\mathsf{P}(\sqrt{a})$, которую мы разовьем в четвертой главе, и поэтому важно полностью изучить его природу. Символ Якоби $\left(\frac{a}{b}\right)$ представляет собой удобное вспомогательное средство для этой цели. А именно, он позволяет целесообразным способом распространить это разбиение на классы, определенное первоначально лишь в области нечетных *простых* чисел $p \nmid k(a)$, на область *всех* чисел b, взаимно простых с 2 и $k(a)$ или также только с $f(a)$, и сделать тем самым это разбиение более ясным, доступным теоретико-групповому описанию. Чтобы получить это описание, соответствующее рассмотрению символа $\left(\frac{a}{b}\right)$ как функции его знаменателя b, мы изучим сначала, что гораздо легче, само разбиение на классы, которое, как и для символа Лежандра, выявляется при рассмотрении символа $\left(\frac{a}{b}\right)$ как функция его числителя a. Затем мы покажем, что формулы квадратичного закона взаимности для символа Лежандра из § 7, п. 2, 3 переносятся также и на символ Якоби. Тем самым мы получим возможность перейти от рассмотрения символа $\left(\frac{a}{b}\right)$ как функ-

ции его числителя к рассмотрению его как функции знаменателя и описать, наконец, формулами непосредственно интересующее нас распространение разбиения на классы из § 7, п. 4, 5.

2. Символ Якоби как функция своего числителя. При рассмотрении символа Якоби $\left(\frac{a}{b}\right)$ как функции его числителя a целесообразно сделать следующие предположения, которые, с одной стороны, слабее тех, которые фигурируют в первоначальном определении, но, с другой стороны, представляют собой некоторое усиление только что названных предположений:

$k(b)$ взаимно просто с 2, a взаимно просто с $k(b)$.

Так как в формулу, определяющую $\left(\frac{a}{b}\right)$, *по существу* (а не формально) входят лишь символы Лежандра $\left(\frac{a}{p}\right)$ с простыми делителями p числа $k(b)$, и так как каждый такой символ, рассматриваемый как функция от a, является квадратичным характером по $\bmod p$, то символ Якоби $\left(\frac{a}{b}\right)$ обладает свойством

$$\left(\frac{a}{b}\right)=1, \quad \text{если} \quad a\equiv \bmod |k(b)|, \tag{5}$$

т. е. свойством (2′) из § 6, п. 4 для модуля $|k(b)|$. Таким образом, как функция от a этот символ является квадратичным характером по $\bmod |k(b)|$. Мы покажем, что его ведущий модуль, определяемый аналогично § 7, п. 4, в точности равен $|k(b)|$.

Для этого заметим, что развитая в § 7, п. 5 для $\left(\frac{a}{p}\right)$ как функции от p теория ведущего модуля немедленно переносится на рассматриваемый здесь случай символа $\left(\frac{a}{b}\right)$ как функции от a, однако теперь для этого *не нужно* привлекать теорему Дирихле о простых числах, потому что область значений аргумента не ограничивается теперь простыми числами p, а представляет собой совокупность всех взаимно простых с $k(b)$ чисел a. Это относится как к переносу на случай символа Якоби доказательства общего факта II п. 5 § 7, а вместе с ним и III, согласно которому ведущий модуль во всяком случае является делителем числа $|k(b)|$, так и к переносу доказательства предложения IV п. 5 § 7, которое исключает собственные делители числа $|k(b)|$. При проведении этого последнего вывода нам достаточно имеющихся у нас данных. Достаточно исключить делители вида $|k(b)|/p$, где p пробегает все простые делители числа $k(b)$. Таким образом, нужно показать, что для каждого простого делителя p числа $k(b)$ существует такое взаимно простое с $k(b)$ число a, что

$a \equiv 1 \bmod |k(b)|\,/\,p$ и $\left(\frac{a}{b}\right) = -1$. Это, однако, имеет место для каждого числа a со свойствами

$$a \equiv 1 \bmod \frac{|k(b)|}{p}, \quad a \equiv w \bmod p,$$

где w есть первообразный корень по $\bmod p$ или даже просто какой-нибудь квадратичный невычет по $\bmod p$. Так как оба модуля взаимно просты, то, согласно § 4, п. 9, эти требования выполняются для некоторого класса вычетов $a \bmod |k(b)|$, взаимно простого с модулем. Тогда, в силу первого требования, $\left(\frac{a}{p'}\right) = 1$ для всех отличных от p простых делителей p' числа $k(b)$, а в силу второго требования, $\left(\frac{a}{p}\right) = -1$. Поэтому, согласно определению символа Якоби, действительно $\left(\frac{a}{b}\right) = -1$.

Итак, доказано:

I. *Символ Якоби* $\left(\frac{a}{b}\right)$ *как функция своего числителя* a *является квадратичным характером, ведущий модуль которого равен абсолютной величине свободного от квадратов ядра* $k(b)$ *числа* b.

Как мы заметили в § 6, п. 4, символ Лежандра $\left(\frac{a}{p}\right) = \chi_p(a)$ является *единственным* квадратичным характером по $\bmod p$, ведущий модуль которого в точности равен p; действительно, сделанное там в связи с (1), (2), (3) предположение, что $\chi_p(a)$ не должно тождественно равняться 1, как раз и сводится к тому, что ведущий модуль не равен единственному собственному делителю числа p — числу 1. В качестве обобщения этого факта мы установим в дополнение к I, что символ Якоби $\left(\frac{a}{b}\right) = \chi_{|k(b)|}(a)$ является *единственным* квадратичным характером с ведущим модулем $|k(b)|$, так что мы можем сказать:

II. *Символ Якоби* $\left(\frac{a}{b}\right)$ *как функция своего числителя* a, *однозначно характеризуется свойством* I.

Доказательство. По предположению, $|k(b)|$ есть произведение различных нечетных простых чисел. В соответствии с этим представим себе, что классы вычетов $a \bmod |k(b)|$, взаимно простые с модулем, разложены на компоненты:

$$a \equiv \prod_{p \mid k(b)} a_p \bmod |k(b)|$$

с

$$a_p \equiv a \bmod p, \quad a_p \equiv 1 \bmod \frac{|k(b)|}{p}.$$

Если теперь ψ есть квадратичный характер по $\bmod |k(b)|$, то отсюда получается соответствующее разложение

$$\psi(a) = \prod_{p \mid k(b)} \psi_p(a)$$

с

$$\psi_p(a) = \psi(a_p).$$

При этом каждая компонента $\psi_p(a)$ представляет собой зависящую только от класса вычетов $a \bmod p$ мультипликативную функцию от a, квадрат которой равен 1 и которая является поэтому квадратичным характером *по* $\bmod p$. Если, далее, ψ имеет ведущий модуль, в точности равный $|k(b)|$, то каждая компонента ψ_p имеет ведущий модуль, равный p; действительно, если бы некоторая компонента $\psi_p(a)$ была тождественно равна 1, то $\psi(a) = 1$ имело бы место уже для всех $a \equiv 1 \bmod |k(b)|/p$. Но тогда, согласно замеченному ранее, для всех p $\psi_p(a) = \left(\frac{a}{p}\right)$. Отсюда следует $\psi(a) = \left(\frac{a}{b}\right)$, что и утверждалось.

В связи с фактами I, II, мы установим еще следующее. На основании свойств, определяющих квадратичный характер в § 6, п. 4, требование $\left(\frac{a}{b}\right) = 1$ при заданном b, имеющем взаимно простое с 2 свободное от квадратов ядро, определяет в группе $\mathfrak{G}$ классов вычетов $a \bmod |k(b)|$, взаимно простых с модулем, подгруппу $\mathfrak{H}$, которая или совпадает с $\mathfrak{G}$, в том случае, если символ $\left(\frac{a}{b}\right)$ как функция от a тождественно равен 1, или, в противном случае, имеет в $\mathfrak{G}$ индекс 2. В последнем случае классы вычетов $a \bmod |k(b)|$, взаимно простые с модулем, для которых $\left(\frac{a}{b}\right) = -1$, образуют единственный смежный класс *по этой подгруппе* $\mathfrak{H}$. Но $\left(\frac{a}{b}\right)$ как функция от a, в силу того что $|k(b)|$ является его ведущим модулем, может тождественно равняться 1 только тогда, когда $|k(b)| = 1$; в самом деле, в противном случае 1 было бы собственным делителем числа $|k(b)|$ со свойством $\left(\frac{a}{b}\right) = 1$ для всех (взаимно простых с $k(b)$) чисел $a \equiv 1 \bmod 1$. Так как $|k(b)|$ есть произведение различных простых чисел, входящих в b с нечетными показателями, то $|k(b)| = 1$ только в том тривиальном случае, когда b с точностью до знака является квадратом. Тем самым доказано:

III. *При постоянном* b, *имеющем взаимно простое с* 2 *свободное от квадратов ядро, требование* $\left(\frac{a}{b}\right) = 1$ *определяет в груп-*

пе $\mathfrak{G}$ классов вычетов $a \bmod |k(b)|$, взаимно простых с модулем, подгруппу $\mathfrak{H}$, имеющую индекс

$$[\mathfrak{G}:\mathfrak{H}] = \begin{cases} 1, & \text{если одно из чисел } \pm b \text{ есть квадрат} \\ 2, & \text{если ни одно из чисел } \pm b \text{ не есть квадрат} \end{cases}.$$

Тот факт, что подгруппа $\mathfrak{H}$ состоит из тех классов вычетов $a \bmod |k(b)|$, для которых квадратичный характер $\left(\frac{a}{b}\right)$ с ведущим модулем $|k(b)|$ имеет значение 1, не дает нам права смешивать ее с подгруппой $\mathfrak{U}$ квадратичных вычетов $a \bmod |k(b)|$. В специальном случае одного простого числа $b = p$, согласно определению символа Лежандра, действительно имеет место $\mathfrak{U} = \mathfrak{H}$. Однако если $k(b)$ содержит несколько простых делителей $p, p', \ldots$, то, согласно I § 6, a будет квадратичным вычетом по $\bmod |k(b)|$ тогда и только тогда, когда одновременно имеет место

$$\left(\frac{a}{p}\right) = 1, \left(\frac{a}{p'}\right) = 1, \ldots,$$

в то время как $\left(\frac{a}{b}\right) = 1$ будет всегда выполняться уже тогда, когда только произведение

$$\left(\frac{a}{p}\right)\left(\frac{a}{p'}\right)\ldots = 1.$$

Таким образом, $\mathfrak{U}$ будет в этом случае собственной подгруппой в $\mathfrak{H}$, и притом, как легко видеть, $\mathfrak{U}$ имеет в $\mathfrak{H}$ индекс $[\mathfrak{G}:\mathfrak{U}] = 2^r$, где r есть количество простых делителей p ядра $k(b)$ числа b. Поэтому символ Якоби $\left(\frac{a}{b}\right)$ является только *формальным* обобщением символа Лежандра $\left(\frac{a}{p}\right)$. *Содержательное* значение символа Лежандра как критерия для ответа на первый основной вопрос о квадратичных вычетах, которое ведь и послужило непосредственным поводом для его определения, при обобщении на символ Якоби утрачивается.

3. Дополнения к закону взаимности и общая форма закона. Значение обобщения символа Лежандра посредством символа Якоби, которое было сделано нами чисто формально, состоит в том, что для символа Якоби имеют место формулы, аналогичные формулам квадратичного закона взаимности и обоих дополнений к нему.

Заметим предварительно, что функции

$$\chi_4(a) = (-1)^{\frac{a-1}{2}}, \quad \chi_8(a) = (-1)^{\frac{a^*-1}{4}}$$

являются в области чисел a, взаимно простых с 2, квадратичными характерами с ведущими модулями 4, 8. Это немедленно следует из того, что в представлениях через базис

$$a \equiv (-1)^{\alpha'} \bmod 4, \quad a \equiv (-1)^{\alpha'} 5^{\alpha''} \bmod 8$$

из § 5, п. 7 в качестве показателей фигурируют

$$\alpha' \equiv \frac{a-1}{2} \bmod 2, \quad \alpha'' \equiv \frac{a^*-1}{4} \bmod 2.$$

Кроме того, функция

$$\chi_\infty(a) = (-1)^{\frac{\operatorname{sgn} a - 1}{2}}$$

есть квадратичный характер (не являющийся характером по модулю) в области всех рациональных чисел $a \neq 0$, т. е. она мультипликативна, и ее квадрат равен 1. Это получается из того, что в представлении

$$a = (-1)^{\alpha} |a|$$

фигурирует показатель $\alpha \equiv (\operatorname{sgn} a - 1)/2 \bmod 2$. В самом деле, соотношение $(-1)^{\alpha} = \operatorname{sgn} a$ может быть указанным образом разрешено относительно класса вычетов по mod 2, к которому принадлежит показатель, в чем мы тотчас же убеждаемся посредством проверки каждой из двух возможностей

$$a \gtrless 0, \ \alpha \equiv 0, 1 \bmod 2.$$

Мультипликативность указанных трех функций $\chi_4(a)$, $\chi_8(a)$, $\chi_\infty(a)$ или, что то же самое, аддитивность их показателей при перемножении аргументов будет играть основную роль при выводе формул закона взаимности для символа Якоби, к которому мы теперь приступаем.

Первое дополнение к закону взаимности. *Если b взаимно просто с 2, то*

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2} + \frac{\operatorname{sng} b - 1}{2}}.$$

Таким образом, в случае, когда, кроме того $b > 0$,

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}.$$

Второе дополнение к закону взаимности. *Если b взаимно просто с 2, то*

$$\left(\frac{2}{b}\right) = (-1)^{\frac{b^*-1}{4}}.$$

Доказательства. Пусть разложением числа b на простые множители будет

$$b=(-1)^{\beta}\prod_{p}p^{\beta_p},$$

причем, согласно предположению, $\beta_2=0$. Тогда, в силу определения символа Якоби, обоих дополнений к закону взаимности для символа Лежандра и нашего предварительного замечания, мы имеем:

$$\left(\frac{-1}{b}\right)=\prod_{p}\left(\frac{-1}{p}\right)^{\beta_p}=\prod_{p\neq 2}\chi_4(p)^{\beta_p}=\chi_4(|b|)=\chi_4(b)\,\chi_4(\operatorname{sgn}b),$$

$$\left(\frac{2}{b}\right)=\prod_{p}\left(\frac{2}{p}\right)^{\beta_p}=\prod_{p\neq 2}\chi_8(p)^{\beta_p}=\chi_8(|b|)=\chi_8(b),$$

что нам и требовалось доказать.

Дополнение. *При более слабом предположении, что только свободное от квадратов ядро $k(b)$ числа b взаимно просто с 2, получаются такие же формулы с заменой в показателях $(b-1)/2$, $(b^*-1)/4$ числа b его ядром $k(b)$.*

Относительно показателя $(\operatorname{sgn}b-1)/2$ заметим, что, конечно, $\operatorname{sgn}k(b)=\operatorname{sgn}b$. Впрочем, для b, взаимно простого с 2, показатели $(b-1)/2$, $(b^*-1)/4$ также инвариантны относительно замены b на $k(b)$, так как каждый нечетный квадрат $\equiv 1 \bmod 8$.

Общая форма закона взаимности. *Если a, b взаимно просты с 2 и взаимно просты между собой, то*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}+\frac{\operatorname{sgn}a-1}{2}\cdot\frac{\operatorname{sgn}b-1}{2}}.$$

Таким образом, в случае, когда, кроме того, $a>0$ или $b>0$,

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$$

Доказательство. Пусть разложениями чисел a, b на простые множители будут

$$a=(-1)^{\alpha}\prod_{q}q^{\alpha_q},\quad b=(-1)^{\beta}\prod_{p}p^{\beta_p},$$

причем, согласно предположению, $\alpha_2=0$, $\beta_2=0$ и $\alpha_q\beta_p=0$ для $q=p$. Тогда, по определению символа Якоби,

$$\left(\frac{a}{b}\right)=\left(\frac{-1}{b}\right)^{\alpha}\prod_{p,q}\left(\frac{q}{p}\right)^{\alpha_p\beta_q},\quad\left(\frac{b}{a}\right)=\left(\frac{-1}{a}\right)^{\beta}\prod_{p,q}\left(\frac{p}{q}\right)^{q\beta_p}.$$

Перемножая, мы получаем отсюда, в силу доказанного выше первого дополнения к закону взаимности для символа Якоби,

общей формы закона взаимности для символа Лежандра и нашего предварительного замечания (которое теперь будет использовано в аддитивном способе записи для сохранения симметрии между a и b), что

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=(-1)^{\omega_0+\omega},$$

где

$$\omega_0\equiv\alpha\left(\frac{b-1}{2}+\frac{\operatorname{sgn} b-1}{2}\right)+\beta\left(\frac{a-1}{2}+\frac{\operatorname{sgn} a-1}{2}\right)\equiv$$
$$\equiv\frac{\operatorname{sgn} a-1}{2}\left(\frac{b-1}{2}+\frac{\operatorname{sgn} b-1}{2}\right)+\frac{\operatorname{sgn} b-1}{2}\left(\frac{a-1}{2}+\frac{\operatorname{sgn} a-1}{2}\right)\equiv$$
$$\equiv\frac{\operatorname{sgn} a-1}{2}\cdot\frac{b-1}{2}+\frac{a-1}{2}\cdot\frac{\operatorname{sgn} b-1}{2}\bmod 2,$$

$$\omega\equiv\sum_{p,q\neq 2}\alpha_q\beta_p\frac{q-1}{2}\frac{p-1}{2}\equiv\sum_{q\neq 2}\alpha_q\frac{q-1}{2}\cdot\sum_{p\neq 2}\beta_p\frac{p-1}{2}\equiv$$
$$\equiv\frac{|a|-1}{2}\frac{|b|-1}{2}\equiv\left(\frac{a-1}{2}+\frac{\operatorname{sgn} a-1}{2}\right)\left(\frac{b-1}{2}+\frac{\operatorname{sng} b-1}{2}\right)\equiv$$
$$\equiv\frac{a-1}{2}\frac{b-1}{2}+\frac{\operatorname{sgn} a-1}{2}\cdot\frac{\operatorname{sgn} b-1}{2}+\frac{a-1}{2}\frac{\operatorname{sgn} b-1}{2}+$$
$$+\frac{\operatorname{sgn} a-1}{2}\cdot\frac{b-1}{2}\bmod 2,$$

что и доказывает наше утверждение.

Дополнение. *При более слабом предположении, что только свободные от квадратов ядра $k(a)$, $k(b)$ чисел a, b взаимно просты с 2 и взаимно просты между собой, получается такая же формула с заменой в показателях $(a-1)/2$, $(b-1)/2$ чисел a, b их ядрами $k(a)$, $k(b)$.*

Заметим, что при полученном нами обобщении формул закона взаимности на символ Якоби первое дополнение к закону взаимности утрачивает свое самостоятельное значение; оно содержится теперь как частный случай $a=-1$ в общей форме закона взаимности.

4. Рекуррентный метод для вычисления символа Якоби. Уже закон взаимности для символа Лежандра $\left(\frac{a}{p}\right)$ принципиально может быть использован для вычисления значения символа в конечное число шагов без обращения к критериям из § 6, п. 4, 5, 6. Для этого нужно только разложить a на простые множители (включая -1), определить по дополнениям к закону взаимности получающиеся при этом символы $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, а символы типа $\left(\frac{q}{p}\right)$ свести в соответствии с общей

формой закона взаимности к $\left(\frac{p}{q}\right)$. Тогда в этих последних символах можно, не изменяя их значения, заменить p его наименьшими или даже абсолютно-наименьшими вычетами r по отдельным q и свести тем самым нашу задачу к вычислению конечного множества символов $\left(\frac{r}{q}\right)$, у которых числители r по абсолютной величине меньше, чем первоначальный числитель a. Через конечное число таких шагов мы придем к концу, потому что *после отщепления множителей* -1, 2 числитель обратится в 1. Однако, вследствие того, что разложение на простые множители требует много времени, этот метод неудобен и мало пригоден для изложения в общем виде.

Пример. Пусть нужно вычислить $\left(\frac{-874}{5231}\right)$. Имеем

$$-874=(-1)\cdot 2\cdot 19\cdot 23,$$

и, таким образом,

$$\left(\frac{-874}{5231}\right)=(-1)\cdot(+1)\cdot\left[-\left(\frac{5231}{19}\right)\right]\times$$
$$\times\left[-\left(\frac{5231}{23}\right)\right]=-\left(\frac{6}{19}\right)\left(\frac{10}{23}\right).$$

При этом

$$\left(\frac{6}{19}\right)=-\left(\frac{3}{19}\right)=\left(\frac{19}{3}\right)=\left(\frac{1}{3}\right)=1,$$
$$\left(\frac{10}{23}\right)=\left(\frac{5}{23}\right)=\left(\frac{23}{5}\right)=\left(\frac{-2}{5}\right)=-1.$$

В итоге получается

$$\left(\frac{-874}{5231}\right)=1.$$

Обобщение закона взаимности на символ Якоби позволяет дать простую, удобную для употребления схему для описанного метода и изложить ее в общем виде, так как благодаря этому обобщению становится ненужным разложение на простые множители (за исключением необходимого и здесь отщепления простого множителя 2).

Пусть нам нужно в общем виде вычислить символ Якоби $\left(\frac{a_0}{a_1}\right)$, где числа a_0 и a_1 без ограничения общности можно предполагать целыми и обладающими свойствами

$$a_1 \text{ взаимно просто с } 2, \quad a_0 \text{ взаимно просто с } a_1.$$

На первом шагу сделаем приведение по модулю и отщепление степени числа 2:

$$a_0 \equiv 2^{\alpha_1} a_2 \bmod |a_1|, \text{ где } a_2 \text{ взаимно просто с } 2 \text{ и } |a_2|<|a_1|/2,$$

причем (освобожденный от простого делителя 2) абсолютно наименьший вычет a_2 тоже получается взаимно простым с a_1. Согласно I п. 2 и формуле закона взаимности из п. 3 имеет место

$$\left(\frac{a_0}{a_1}\right)=\left(\frac{a_0}{|a_1|}\right)=\left(\frac{2}{|a_1|}\right)^{\alpha_1}\left(\frac{a_2}{|a_1|}\right)=(-1)^{\alpha_1\frac{a_1^*-1}{4}+\frac{|a_1|-1}{2}\cdot\frac{a_2-1}{2}}\left(\frac{|a_1|}{|a_2|}\right).$$

На втором шагу снова сделаем приведение по модулю и отщепление степени числа 2:

$|a_1|\equiv 2^{\alpha_2}a_3 \bmod |a_2|$, где a_3 взаимно просто с 2 и $|a_3|<|a_2|/2$,

причем опять-таки a_3 получается взаимно простым с a_2. При этом, соответственно, имеет место

$$\left(\frac{|a_1|}{|a_2|}\right)=\left(\frac{2}{|a_2|}\right)^{\alpha_2}\left(\frac{a_3}{|a_2|}\right)=(-1)^{\alpha_2\frac{a_2^*-1}{4}+\frac{|a_2|-1}{2}\cdot\frac{a_3-1}{2}}\left(\frac{|a_2|}{|a_3|}\right).$$

Так как последовательность a_1, a_2, a_3, ... по абсолютной величине монотонно убывает, то через конечное число таких шагов получится $|a_{r+1}|=1$, так, что

$$\left(\frac{|a_{r-1}|}{|a_r|}\right)=\left(\frac{2}{|a_r|}\right)^{\alpha_r}\left(\frac{a_{r+1}}{|a_r|}\right)=(-1)^{\alpha_r\frac{a_r^*-1}{4}+\frac{|a_r|-1}{2}\cdot\frac{a_{r+1}-1}{2}},$$

и мы через конечное же число шагов дойдем до конца. Из этой последовательности равенств определяемое нами значение символа получается в виде

$$\left(\frac{a_0}{a_1}\right)=(-1)^{\alpha},\quad \text{где } \alpha\equiv\sum_{i=1}^{r}\left(\alpha_i\frac{a_i^*-1}{4}+\frac{|a_i|-1}{2}\frac{a_{i+1}-1}{2}\right)\bmod 2.$$

При изложении этого метода, напоминающего алгоритм Евклида, мы сознательно отказались от использования правила (3) из п. 1, согласно которому можно отбрасывать квадратные множители, не изменяя при этом значения символа, а вместе с тем и от использования более слабых предположений:

$k(a_1)$ взаимно просто с 2, $k(a_0)$ взаимно просто с $k(a_1)$,

потому что для отбрасывания квадратных множителей мы в отличие от деления с остатком не имеем удобного способа и должны для этого знать разложение на простые множители, а этого-то как раз мы и хотели избежать, применяя символ Якоби. В конкретных числовых случаях, конечно, можно отбрасывать известные квадратные множители и тем самым сокращать количество шагов. Также само собой разумеется, что в числовых случаях можно тотчас же вычислять появляющиеся после каждого шага множи-

тели, равные степени числа (-1), определяя для этого вычеты $a_i \bmod 8$, $|a_i| \bmod 4$, $a_{i+1} \bmod 4$, или, что еще проще, используя легко применимые правила для символа $\left(\frac{2}{|a_i|}\right)$ и так называемых обратных множителей

$$\left(\frac{a_{i+1}}{|a_i|}\right), \quad \left(\frac{|a_i|}{|a_{i+1}|}\right),$$

и ставить каждый раз правильный знак перед рассматриваемым далее символом.

Примеры. 1. Пусть нужно вычислить $\left(\frac{-874}{5231}\right)$ (см. вышеприведенный пример).

$$-874 = 2\cdot(-437)$$

$$\begin{array}{r} 5231 \\ 12\cdot 437 = 5244 \\ \hline \text{остаток } -13 \end{array}$$

$$\begin{array}{r} 437 \\ 34\cdot 13 = 442 \\ \hline \text{остаток } -5 \end{array}$$

$$\begin{array}{r} 13 \\ 3\cdot 5 = 15 \\ \hline \text{остаток } -2 \end{array}$$

$$\left(\frac{-874}{5231}\right) = \left(\frac{-437}{5231}\right) = -\left(\frac{5231}{437}\right) =$$

$$= -\left(\frac{-13}{437}\right) = -\left(\frac{437}{13}\right) =$$

$$= -\left(\frac{-5}{13}\right) = -\left(\frac{13}{5}\right) =$$

$$= -\left(\frac{-2}{5}\right) = 1.$$

2. Пусть нужно вычислить $\left(\frac{49337}{129061}\right)$.

$$\begin{array}{r} 129061 \\ 3\cdot 49337 = 148011 \\ \hline \text{остаток } -18950 \end{array} = 2\cdot(-9475)$$

$$\begin{array}{r} 49337 \\ 5\cdot 9475 = 47375 \\ \hline \text{остаток } 1962 = 2\cdot 981 \end{array}$$

$$\begin{array}{r} 9475 \\ 10\cdot 981 = 9810 \\ \hline \text{остаток } -335 \end{array}$$

$$\begin{array}{r} 981 \\ 3\cdot 335 = 1005 \\ \hline \text{остаток } -24 = 2^3\cdot(-3) \end{array}$$

$$\begin{array}{r} 335 \\ 3\cdot 112 = 336 \\ \hline \text{остаток } -1 \end{array}$$

$$\left(\frac{49337}{129061}\right) = \left(\frac{129061}{49337}\right) =$$

$$= \left(\frac{-9475}{49337}\right) = \left(\frac{49337}{9475}\right) =$$

$$= -\left(\frac{981}{9475}\right) = -\left(\frac{9475}{981}\right) =$$

$$= -\left(\frac{-335}{981}\right) = -\left(\frac{981}{335}\right) =$$

$$= -\left(\frac{-3}{335}\right) = -\left(\frac{335}{3}\right) =$$

$$= -\left(\frac{-1}{3}\right) = 1.$$

В этом примере вычисление могло быть еще сокращено посредством отбрасывания квадратных множителей в $9475 = 5^2 \cdot 379$ и $981 = 3^2 \cdot 109$.

5. Символ Якоби как функция своего знаменателя. Теперь мы приступаем к описанию символа Якоби $\left(\frac{a}{b}\right)$ как функции его знаменателя b. При этом целесообразно положить в основу предположения, которые являются более сильными, чем предположения из п. 1; однако эти предположения отличаются и от тех, которые были сделаны в п. 2 при описании символа как функции его числителя a. В соответствии с нашей теперешней целью мы формулируем эти предположения так, чтобы явно задавалась область допустимых значений аргумента b (а не a, как было выше):

$$a \neq 0 \text{ — любое}, \qquad b \text{ взаимно просто с } 2 \text{ и с } k(a).$$

Для данного рационального числа $a \neq 0$ рассмотрим два следующих однозначных представления:

$$\left\{ \begin{array}{ll} a = 2^{\alpha_2} (-1)^{\alpha_2'} a^* & \text{с } a^* \equiv 1 \bmod 4 \\ a = (-1)^{\alpha} |a| & \text{с } |a| > 0 \end{array} \right\}, \tag{1}$$

из которых первое является естественным обобщением данного в § 5, п. 7 определения обозначения a^* на любые (также и не взаимно простые с 2) числа. При этом знак числа a^* может быть выражен через показатели α_2', $\alpha \bmod 2$ по формуле

$$\operatorname{sgn} a^* = (-1)^{\alpha_2'} \operatorname{sgn} a = (-1)^{\alpha_2' + \alpha},$$

которую можно разрешить и относительно показателей:

$$\frac{\operatorname{sgn} a^* - 1}{2} \equiv \alpha_2' + \alpha \bmod 2.$$

Согласно формуле закона взаимности из п. 3, исследуемый символ Якоби $\left(\frac{a}{b}\right)$ представляется тогда следующим образом в виде явной функции своего знаменателя b:

$$\left(\frac{a}{b}\right) = \left(\frac{2}{b}\right)^{\alpha_2} \left(\frac{-1}{b}\right)^{\alpha_2'} \left(\frac{a^*}{b}\right) =$$

$$= (-1)^{\alpha_2 \frac{b^*-1}{4}} (-1)^{\alpha_2' \left(\frac{b-1}{2} + \frac{\operatorname{sgn} b - 1}{2}\right)} (-1)^{\frac{\operatorname{sgn} a^* - 1}{2} \frac{\operatorname{sgn} b - 1}{2}} \left(\frac{b}{a^*}\right) =$$

$$= (-1)^{\alpha \frac{\operatorname{sgn} b - 1}{2}} (-1)^{\alpha_2 \frac{b^*-1}{4} + \alpha_2' \frac{b-1}{2}} \left(\frac{b}{a^*}\right).$$

Стоящие впереди множители могут быть выражены через введенные в п. 3 квадратичные характеры $\chi_4(b)$, $\chi_8(b)$, $\chi_\infty(b)$, в то время как последний множитель, согласно I, II п. 2, является квадратичным характером

$$\chi_{|k(a^*)|}(b) = \left(\frac{b}{a^*}\right)$$

с ведущим модулем $|k(a^*)|$. Мы будем записывать поэтому полученное нами явное представление также в виде

$$\left(\frac{a}{b}\right) = \chi_\infty(b)^{\alpha}\,\chi_8(b)^{\alpha_2}\,\chi_4(b)^{\alpha_2'}\,\chi_{|k(a^*)|}(b), \tag{2}$$

в котором ясно виден характер зависимости символа от b; при этом показатели α, α_2, $\alpha_2' \bmod 2$, так же как и a^*, определяются представлениями (1).

Символ $\left(\frac{a}{b}\right)$ как функция от b является характером по модулю в прежнем смысле лишь при $\alpha \equiv 0 \bmod 2$, т. е. $a > 0$ и тем самым также $k|a| > 0$, так как в этом случае обусловленная множителем $\chi_\infty(b)^{\alpha}$ дополнительная зависимость от знака числа b в действительности исчезает. Ведущий модуль $f(a)$ этого характера определяется тогда следующим образом.

Если имеет место также α_2, $\alpha_2' \equiv 0 \bmod 2$, т. е. $k(a) = k(a^*)$, то

$$f(a) = k(a^*) = k(a).$$

Если $\alpha_2 \equiv 0 \bmod 2$, но $\alpha_2' \equiv 1 \bmod 2$, т. е. $k(a) = -k(a^*)$, то в силу обусловленной множителем $\chi_4(b)^{\alpha_2'}$ действительно имеющей место зависимости от класса вычетов $b \bmod 4$, в ведущем модуле появляется еще множитель 4; таким образом, в этом случае

$$f(a) = 4\,|k(a^*)| = 4k(a).$$

Наконец, если $\alpha_2 \equiv 1 \bmod 2$ и $\alpha_2 \bmod 2$ — любое, т. е. $k(a) = \pm 2k(a^*)$, то в силу обусловленной множителем $\chi_8(b)\,\chi_4(b)^{\alpha_2'}$ действительно имеющей место зависимости от класса вычетов $b \bmod 8$, в ведущем модуле вместо множителя 4 появляется даже множитель 8; таким образом, в этом случае $f(a) = 8\,|k(a^*)| = 4k(a)$.

В каждом из этих случаев в качестве ведущего модуля $f(a)$ получается тот же модуль, что и в § 7, п. 5 для ограниченной простыми числами $b = p$ области аргумента, хотя теперь мы обошлись *без* теоремы Дирихле о простых числах и вообще без повторения прежнего вывода, а получили этот результат непосредственно из менее глубокого соответствующего факта I, п. 2 для символа Якоби как функции его числителя, основываясь на формулах закона взаимности.

Для $\alpha \equiv 1 \bmod 2$, т. е. $a < 0$ и тем самым также $k(a) < 0$, символ $\left(\frac{a}{b}\right)$ уже не является характером по модулю в прежнем смысле, в силу обусловленной множителем $\chi_\infty(b)$ действительно имеющей место зависимости от знака числа b. Однако абсолютная величина $|f(a)|$ вычисляемого в каждом отдельном случае уже указанным способом числа $f(a)$, которое теперь отрицательно, снова обладает свойствами ведущего модуля, если ограничить область значений аргумента или только числами $b > 0$, или только числами $b < 0$ с сохранением остальных предположений. При этом каждый класс вычетов по $\bmod |f(a)|$ разлагается на два *полукласса*, один из которых состоит из положительных, а другой из отрицательных чисел. Это разбиение классов вычетов тоже целесообразно выразить на языке теории сравнений.

Для этого нам нужно только рассматривать определяющий знак множитель -1 как некоторый модуль, который и производит это разбиение, а именно, условиться раз навсегда, что для отрицательного модуля $-m$ сравнение

$$a \equiv a' \bmod (-m)$$

равносильно с $a \equiv a' \bmod m$ и $\operatorname{sgn} a = \operatorname{sgn} a'$. На основании этого определения использованное выше представление $a = (-1)^\alpha |a|$ с $|a| > 0$ может быть записано в форме

$$a = (-1)^\alpha |a| \quad \text{с} \quad |a| \equiv 1 \bmod (-1),$$

аналогичной определению a^*, или, коротко, в виде представления

$$a \equiv (-1)^\alpha \bmod (-1) \qquad (\alpha \bmod 2)$$

через базис группы классов вычетов по $\bmod(-1)$ (имеющей порядок $\varphi(-1) = 2$).

В нашем случае оба полукласса по $\bmod |f(a)|$, отличающихся друг от друга знаком, будут тогда формально классами вычетов по $\bmod f(a)$. В этом смысле символ $\left(\frac{a}{b}\right)$ также и для $a < 0$ является характером по модулю с ведущим модулем $f(a)$.

В итоге мы можем считать установленным следующее обобщение утверждений I, IV § 7:

IV. *Если сравнимость по отрицательному модулю понимать как сравнимость по его абсолютной величине и равенство знаков, то символ Якоби* $\left(\frac{a}{b}\right)$, *рассматриваемый при постоянном числителе* $a \neq 0$ *как функция его знаменателя* b, *является квадратичным характером с ведущим модулем*

$$f(a) = \left\{ \begin{array}{ll} k(a), & \text{если } k(a) \equiv 1 \bmod 4 \\ 4k(a), & \text{если } k(a) \not\equiv 1 \bmod 4 \end{array} \right\},$$

где $k(a)$ есть свободное от квадратов ядро числа a, и это имеет место в области чисел b, взаимно простых с 2 и $k(a)$.

Сравнивая это высказывание со специальным случаем I, IV § 7, для $b=p$ замечаем, что так как простые числа $p>0$, то сравнение $p\equiv p' \bmod |f(a)|$ влечет за собой более сильное сравнение $p\equiv p' \bmod f(a)$ в нашем новом смысле.

Заметим далее, что положенное здесь в основу определение сравнения $a\equiv a' \bmod (-m)$ не пригодно для постоянного употребления. Ведь с элементарной точки зрения сравнение $a\equiv a' \bmod m$, определяемое через делимость $m\mid a-a'$, *инвариантно* относительно замены m на $-m$, так что, вообще говоря, сравнение $a\equiv a' \bmod (-m)$ надо понимать как равносильное сравнению $a\equiv a' \bmod m$. На этом основании, а также и из других соображений, изложение которых здесь завело бы нас слишком далеко, в высшей теории чисел употребляется другой способ записи для сравнимости, включая равенство знаков; при этом к модулю m вместо -1 добавляется в качестве множителя новый символ ∞. Тогда введенный в п. 3 квадратичный характер χ_∞ относится как раз к группе классов вычетов по $\bmod \infty$; отсюда и его обозначение. Однако если пользоваться этим символом ∞, то данные здесь в IV формулы для ведущего модуля $f(a)$ как функции от a получаются не в такой простой форме.

Если при выводе IV речь шла о зависимости символа $\left(\frac{a}{b}\right)$ от знака b, то это понималось там в том смысле, что при $a<0$ для равенства $\left(\frac{a}{b}\right)=\left(\frac{a}{b'}\right)$ значений символа недостаточно только сравнимости $b\equiv b' \bmod |f(a)|$, а необходимо еще и равенство знаков $\operatorname{sgn} b=\operatorname{sgn} b'$, т. е. должно иметь место сравнение $b\equiv b' \bmod f(a)$, понимаемое в новом смысле. Мы подчеркиваем это потому, что если символ $\left(\frac{a}{b}\right)$ рассматривать просто как *числовую функцию*, а не как характер по некоторому модулю, то, согласно определению, всегда имеет место

$$\left(\frac{a}{b}\right)=\left(\frac{a}{-b}\right),$$

т. е. эта числовая функция не зависит от знака числа b, или, как еще говорят, является *четной*. Подробнее, положение вещей таково. Если числа b, взаимно простые с 2 и с $k(a)$, представить на числовой прямой, то символ $\left(\frac{a}{b}\right)$ определяет распределение значений ± 1 по точкам, соответствующим числам b. Это распределение, во-первых, будет периодичным с периодом $|f(a)|$ отдельно в области $b>0$ и в области $b<0$, и во-вторых, симметричным относительно нулевой точки. Если $a>0$, то это распределение будет периодичным также и во всей области

$b \gtrless 0$, однако, если $a < 0$, то это уже не так. Внутри наименьшей системы вычетов по $\bmod |f(a)|$, взаимно простых с модулем, эти два случая будут отличаться друг от друга тем, что

$$\left(\frac{a}{b}\right) = \left(\frac{a}{|f(a)|-b}\right) \qquad \text{для } a > 0,$$
$$\left(\frac{a}{b}\right) = -\left(\frac{a}{|f(a)|-b}\right) \qquad \text{для } a < 0;$$

действительно, в первом случае $|f(a)| - b \equiv -b \bmod f(a)$, а во втором случае лишь $|f(a)| - b \equiv\equiv -b \bmod |f(a)|$, а не по $\bmod f(a)$. Поэтому для $a > 0$ описанное нами распределение значений символа в наименьшей системе вычетов по $\bmod |f(a)|$ будет *симметричным* относительно средней точки $|f(a)|/2$, а для $a < 0$ — только *кососимметричным* (симметрично расположенные значения противоположны по знаку); с этим мы познакомились уже в § 7, п. 5 в разобранных там примерах. В соответствии с этим символ $\left(\frac{a}{b}\right)$ как *характер* по $\bmod f(a)$ называется *четным* или *нечетным*, в то время как, рассматриваемый как числовая функция, он, как уже сказано, всегда будет четным.

Подобно тому, как из факта I, п. 2, касающегося символа Якоби как функции числителя, с помощью формул закона взаимности следует аналогичный факт IV относительно этого символа как функции знаменателя. Относительно символа Якоби как функции числителя можно получить аналогичные выводы об этом символе как функции знаменателя и из дальнейших рассуждений II, III, п. 2.

Что касается аналога теоретико-группового высказывания III, п. 2. то мы пока оставим его, так как он станет ясным только после видоизменения определения символа Якоби, которое будет дано в п. 6; таким образом, мы ограничимся здесь аналогом теоремы единственности II, п. 2.

Пусть, как до этого в (1),

$$a = 2^{\alpha_2}(-1)^{\alpha_2'} a^* \qquad \text{с } a^* \equiv 1 \bmod 4,$$
$$a = (-1)^{\alpha} |a| \qquad \text{с } |a| \equiv \bmod (-1).$$

Тогда, согласно IV,

$$f(a) = \left\{ \begin{array}{lll} (-1)^{\alpha} |k(a^*)| & \text{для } \alpha_2 \equiv 0,\ \alpha_2' \equiv 0 & \bmod 2 \\ (-1)^{\alpha} \cdot 4 \cdot |k(a^*)| & \text{для } \alpha_2 \equiv 0,\ \alpha_2' \equiv 1 & \bmod 2 \\ (-1)^{\alpha} \cdot 8 |k(a^*)| & \text{для } \alpha_2 \equiv 1,\ \alpha_2' \text{ любое} & \bmod 2 \end{array} \right\}$$

и, согласно (2),

$$\left(\frac{a}{b}\right) = \chi_{\infty}(b)^{\alpha} \chi_8(b)^{\alpha_2} \chi_4(b)^{\alpha_2'} \chi_{|k(a^*)|}(b).$$

Нам надо исследовать, является ли этот квадратичный характер единственным, имеющим ведущий модуль $f(a)$. Для этого рассмотрим модуль

$$m(a) = (-1) \cdot 8 \cdot |k(a^*)|,$$

который в каждом из трех случаев содержит $f(a)$, и в соответствии с его структурой разложим классы вычетов $b \bmod m(a)$, взаимно простые с модулем, на компоненты:

$$b \equiv b_\infty b_8 b_{|k(a^*)|} \bmod m(a),$$

где

$$b_\infty \equiv \left\{ \begin{matrix} b \bmod (-1) \\ 1 \bmod 8 \,|\, k(a^*)| \end{matrix} \right\}, \quad b_8 \equiv \left\{ \begin{matrix} b \bmod 8 \\ 1 \bmod (-|k(a^*)|) \end{matrix} \right\},$$

$$b_{|k(a^*)|} \equiv \left\{ \begin{matrix} b \bmod |k(a^*)| \\ 1 \bmod (-8) \end{matrix} \right\}.$$

То, что механизм разложения на компоненты переносится на рассматриваемый здесь случай отрицательного модуля $m(a)$, немедленно станет ясным, если сначала произвести разложение по компонентам только для $\bmod |m(a)|$, а затем посредством прибавления к компонентам достаточно большого кратного числа $|m(a)|$ позаботиться о том, чтобы для них выполнялись и дополнительные условия, касающиеся их знаков.

Если теперь ψ есть квадратичный характер по $\bmod f(a)$, а потому и подавно по $\bmod m(a)$, то, аналогично тому как в п. 2, при доказательстве утверждения II, существует соответствующее разложение на компоненты

$$\psi(b) = \psi_\infty(b)\, \psi_8(b)\, \psi_{|k(a^*)|}(b),$$

где

$$\psi_\infty(b) = \psi(b_\infty), \quad \psi_8(b) = \psi(b_8), \quad \psi_{|k(a^*)|}(b) = \psi(b_{|k(a^*)|}),$$

и эти компоненты являются квадратичными характерами по $\bmod(-1)$, $\bmod 8$, $\bmod |k(a^*)|$. Если, далее, ψ имеет ведущий модуль, в точности равный $f(a)$, то, как и в II п. 2, ведущими модулями компонент являются соответственно $(-1)^\alpha$, 1, $|k(a^*)|$ или $(-1)^\alpha$, 4, $|k(a^*)|$, или $(-1)^\alpha$, 8, $|k(a^*)|$, в зависимости от того, чему равно $f(a)$, так что их произведение каждый раз равно $f(a)$. Но единственными квадратичными характерами с ведущими модулями -1, 4, 8, в силу представления через базис для этих модулей, являются соответственно характеры χ_∞, χ_4, $\{\chi_8, \chi_8\chi_4\}$, и единственным квадратичным характером с ведущим модулем $|k(a^*)|$ является, согласно II п. 2, символ Якоби $\chi_{|k(a^*)|}(b) = \left(\frac{b}{a^*}\right)$. Поэтому для ψ разложение на компоненты

имеет вид

$$\psi = \chi_\infty^{\alpha} (\chi_8 \chi_4^{\delta})^{\alpha_2} \chi_4^{\alpha_4'} \chi_{|k(a^*)|},$$

где показатель $\delta \bmod 2$ точнее определить нельзя.

В случае $\alpha_2 \equiv 0 \bmod 2$, когда этот показатель δ не играет роли, мы имеем поэтому

$$\psi(b) = \left(\frac{a}{b}\right).$$

Таким образом, в этом случае $\left(\frac{a}{b}\right)$ как функция от b действительно является единственным квадратичным характером с ведущим модулем $f(a)$.

Однако в случае $\alpha_2 \equiv 1 \bmod 2$, в соответствии с двумя значениями $\delta \equiv 0, 1 \bmod 2$, получаются два квадратичных характера с ведущим модулем $f(a)$, а именно,

$$\psi(b) = \left(\frac{a}{b}\right) \quad \text{и} \quad \psi(b) = (-1)^{\frac{b-1}{2}} \left(\frac{a}{b}\right) = (-1)^{\frac{\operatorname{sgn} b - 1}{2}} \left(\frac{-a}{b}\right),$$

где последнее преобразование основано на первом дополнении к закону взаимности. Эти характеры отличаются друг от друга тем, что первый является четной числовой функцией, а второй — нечетной числовой функцией.

Тем самым мы доказали факт, аналогичный теореме единственности II, п. 2:

V. *Символ Якоби* $\left(\frac{a}{b}\right)$ *как функция своего знаменателя* b *однозначно характеризуется своим свойством* IV *и тем, что как числовая функция он является четным.*

Если свободное от квадратов ядро $k(a)$ *числа* a *взаимно просто с* 2, *то для однозначности достаточно одного свойства* IV; *если же* $k(a)$ *не взаимно просто с* 2, *то свойством* IV, *кроме четной числовой функции* $\left(\frac{a}{b}\right)$, *обладает еще нечетная числовая функция*

$$(-1)^{\frac{b-1}{2}} \left(\frac{a}{b}\right) = (-1)^{\frac{\operatorname{sgn} b - 1}{2}} \left(\frac{-a}{b}\right).$$

Высказывание IV вместе с V представляет собой вариант квадратичного закона взаимности, не содержащий формул и потому имеет принципиальный интерес. Оно устанавливает, что символ $\left(\frac{a}{b}\right)$, который по своему определению является квадратичным характером по $\bmod |k(b)|$ только как функция от a, но как функция от b не имеет отношения к тому, как ведет себя b по какому бы то ни было модулю, в действительности является квадратичным характером по модулю $f(a)$, определяе-

мому числом a, и притом вполне определенным характером, а именно, единственным, ведущий модуль которого равен $f(a)$ и который как числовая функция является четным. Явное выражение этого однозначно определенного характера в виде данной выше формулы (2) позволяет тогда перейти от этой формулировки к формулировке закона взаимности по существу, с помощью формул. Последнее замечание показывает, что, в отличие от того как делали мы, для доказательства квадратичного закона взаимности, можно было бы сначала вывести формулировку по существу. Это действительно можно сделать с помощью методов теории алгебраических чисел. Мы вернемся к этому в четвертой главе (см. § 19, п. 3).

6. Символ Кронекера. Развитая в п. 5 теория символа Якоби, как функции своего знаменателя, обладает еще одним недостатком с точки зрения формальной законченности. А именно, в то время как в случае $k(a) \not\equiv 1 \bmod 4$, когда $f(a) = 4k(a)$, область значений аргумента

$$b \text{ взаимно просто с } 2,\ b \text{ взаимно просто с } k(a)$$

представляет собой совокупность всех чисел, взаимно простых с модулем $f(a)$, в случае $k(a) \equiv 1 \bmod 4$, когда $f(a) = k(a)$, область значений аргумента есть только часть этой совокупности. В последнем случае ограничение, состоящее в том, что b должно быть взаимно просто с 2, не является органически необходимым, а появляется только вследствие того, что символ Лежандра определен лишь для простых $p \neq 2$.

Это обстоятельство побудило Кронекера еще несколько расширить определение символа Якоби в случае $k(a) \equiv 1 \bmod 4$. Естественно сделать это следующим образом. Данное в п. 5 явное представление (2) для $\left(\frac{a}{b}\right)$ как функция от b принимает в рассматриваемом случае вид

$$\left(\frac{a}{b}\right) = (-1)^{\frac{\operatorname{sgn} a-1}{2}\frac{\operatorname{sgn} b-1}{2}} \left(\frac{b}{a}\right) \quad \text{для} \quad k(a) \equiv 1 \bmod 4. \qquad (1)$$

Но стоящее справа выражение определено для *всех* b, взаимно простых (или также лишь имеющих взаимно простые свободные от квадратов ядра) с $k(a) = f(a)$, и потому дает определенное значение стоящему слева символу $\left(\frac{a}{b}\right)$ также и при b, не взаимно простых (имеющих не взаимно простые ядра) с 2. Полученное таким образом обобщение символа Якоби называется *символом Кронекера*, причем это название применяется также и в случае $k(a) \not\equiv 1 \bmod 4$, когда никакого расширения определения не делается. Согласно IV, п. 5, случаи $k(a) \equiv 1$, $k(a) \not\equiv 1 \bmod 4$

различаются также тем, что в первом из них $2 \nmid f(a)$, а во втором $2 \mid f(a)$.

Согласно определению символа Кронекера, он, как и символ Якоби, мультипликативен по a и по b. Относительно мультипликативности по a надо отметить, что из $k(a) \equiv 1$, $k(a') \equiv 1 \bmod 4$ следует также $k(aa') \equiv 1 \bmod 4$. Вследствие мультипликативности по b сделанное расширение области определения символа редуцируется к добавлению *одного* нового значения символа

$$\left(\frac{a}{2}\right) = \left(\frac{2}{a}\right) \quad \text{для } k(a) \equiv 1 \bmod 4, \tag{2}$$

или, по второму дополнению к закону взаимности, в явной форме

$$\left(\frac{a}{2}\right) = (-1)^{\frac{k(a)-1}{4}} \quad \text{для } k(a) \equiv 1 \bmod 4, \tag{3}$$

и к требованию мультипликативности по b.

Если для любого a, ядро которого взаимно просто с 2, положить $a = (-1)^{\frac{a'}{2}} a^*$ с $k(a^*) \equiv 1 \bmod 4$, то, очевидно, имеет место $\left(\frac{2}{a}\right) = \left(\frac{2}{a^*}\right)$; поэтому, согласно формуле (2), второе дополнение к закону взаимности в самой общей форме принимает вид формулы обращения $\left(\frac{2}{a}\right) = \left(\frac{a^*}{2}\right)$, правая сторона которой рассматривается как определяемая формулой (3) (с a^* вместо a).

Что же касается общей формулы (1), то, ввиду ее симметричности относительно a и b, безразлично, сделать ли дополнительное предположение $k(a) \equiv 1 \bmod 4$ ($f(a)$ взаимно просто с 2) или $k(b) \equiv 1 \bmod 4$ ($f(b)$ взаимно просто с 2). Поэтому мы имеем формулировку, в которой как предположение, так и утверждение симметричны относительно a и b.

Закон взаимности для символа Кронекера. *Если*

$f(a)$ или $f(b)$ взаимно просто с 2, $k(a)$ и $k(b)$ взаимно просты между собой,

то

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{\operatorname{sgn} a - 1}{2}\,\frac{\operatorname{sgn} b - 1}{2}}.$$

На основании IV, п. 5 мы могли бы объединить оба предположения в одно, а именно, что $f(a)$ и $f(b)$ должны быть взаимно просты друг с другом, однако мы не сделали этого, так как нам желательно здесь понимать взаимную простоту ведущих модулей, учитывая также и множители, определяющие знак (-1 или символ ∞). Если $f(a)$ и $f(b)$ взаимно просты между

собой в этом более сильном смысле (и только при этом предположении), то зависящий от знаков чисел a и b множитель в формуле закона взаимности равен 1. Поэтому мы имеем

Дополнение. *Если предполагать, что $f(a)$ и $f(b)$ взаимно просты между собой (учитывая и множитель, определяющий знак), то имеет место простая формула обращения*

$$\left(\frac{a}{b}\right)=\left(\frac{b}{a}\right).$$

Как уже было выведено в квадратичном законе взаимности, для символа Кронекера второе дополнение тоже может быть получено как частный случай общей формулы при $a=2$; первое же дополнение получалось как частный случай $a=-1$ уже в законе взаимности для символа Якоби. Поэтому закон взаимности для символа Кронекера следует рассматривать как самое общее формульное выражение закона взаимности для квадратичных вычетов. Но он удобен не только благодаря этой своей общности, но также и благодаря своей простоте и симметричности относительно a и b в предположении и в утверждении.

Правда, относительно общности нужно еще сказать следующее. Самые общие предположения, при которых теперь определен наш символ, гласят:

$k(a)$ и $k(b)$ взаимно просты между собой (в обычном смысле), если $2 \mid k(b)$, то $2 \nmid f(a)$.

В случае $2 \mid k(b)$ символ удовлетворяет предположениям закона взаимности для символа Кронекера, однако в случае $2 \nmid k(b)$ — не обязательно, так как все-таки может иметь место $2 \mid f(b)$ (а именно, если $k(b) \equiv -1 \bmod 4$), и одновременно может быть $2 \mid f(a)$. Однако если аналогично тому, как было сделано при выводе второго дополнения, положить $b=(-1)^{\beta} 2^{\alpha} b^{*}$ с $k(b^{*}) \equiv 1 \bmod 4$, то тривиальным образом будем иметь $\left(\frac{a}{b}\right)=\left(\frac{a}{b^{*}}\right)$ и для измененного символа $\left(\frac{a}{b^{*}}\right)$ предположения закона взаимности уже будут выполнены. Поэтому закон взаимности для символа Кронекера может применяться для *каждого* определенного символа $\left(\frac{a}{b}\right)$, если в случае необходимости предварительно изменять знак числа b.

В области чисел b, взаимно простых с $f(a)$, символ Кронекера $\left(\frac{a}{b}\right)$ как функция своего знаменателя b является квадратичным характером с ведущим модулем $f(a)$ и при этом единственным таким характером, если требовать еще, чтобы как числовая функция характер был четным; это было установлено еще высказыванием IV, п. 5 для символа Якоби. При переходе

к символу Кронекера обобщение состоит здесь только в расширении области определения символа до полной совокупности всех чисел b, взаимно простых с $f(a)$, что и послужило поводом для введения символа Кронекера. Теперь мы дадим еще аналог для символа как функции знаменателя теоретико-группового высказывания III и 2, касающегося символа как функции числителя:

VI. *При постоянном* $a \neq 0$ *требование* $\left(\frac{a}{b}\right) = 1$ *определяет в группе* $\mathfrak{G}$ *классов вычетов* $b \bmod f(a)$, *взаимно простых с модулем, подгруппу* $\mathfrak{H}$ *индекса*

$$[\mathfrak{G} : \mathfrak{H}] = \begin{cases} 1, \text{ если } 1 \text{ есть квадрат} \\ 2, \text{ если } 1 \text{ не есть квадрат.} \end{cases}$$

Доказательство. Из того, что $\left(\frac{a}{b}\right) = \chi_{f(a)}(b)$ является квадратичным характером по $\bmod f(a)$, следует, что классы вычетов $b \bmod f(a)$, взаимно простые с модулем, для которых $\left(\frac{a}{b}\right) = 1$, образуют подгруппу $\mathfrak{H}$, которая или совпадает с $\mathfrak{G}$, в том случае, если $\left(\frac{a}{b}\right)$ как функция от b тождественно равняется 1 или в противном случае имеет в $\mathfrak{G}$ индекс 2. Но в силу свойств ведущего модуля $f(a)$, $\left(\frac{a}{b}\right)$ как функция от b может тождественно равняться 1 только тогда, когда $f(a) = 1$; действительно, в противном случае 1 была бы собственным делителем числа $f(a)$ со свойством: $\left(\frac{a}{b}\right) = 1$ для всех (взаимно простых с $f(a)$), $b \equiv 1 \bmod 1$. Но, согласно IV п. 5, $f(a) = 1$ только в том тривиальном случае, когда a есть квадрат.

Фигурирующая в VI подгруппа $\mathfrak{H}$ группы $\mathfrak{G}$ классов вычетов по $\bmod f(a)$, взаимно простых с модулем, имеет (в отличие от менее важной подгруппы, фигурирующей в III п. 2) большое значение в теории алгебраических чисел. Она связана с арифметикой квадратичного поля $\mathsf{P}(\sqrt{a})$, определяемого числом a, как мы увидим это в четвертой главе (см. § 19,1). На это принципиальное истолкование символа Кронекера будет опираться основанное на арифметике поля $\mathsf{P}(\sqrt{a})$ доказательство квадратичного закона взаимности, о котором уже шла речь в п. 5 в связи с высказываниями IV, V.

§ 10. ВОПРОСЫ РАСПРЕДЕЛЕНИЯ КВАДРАТИЧНЫХ ВЫЧЕТОВ ПО ПРОСТОМУ МОДУЛЮ

1. Количество решений квадратных сравнений. Квадратичный закон взаимности, теорию которого мы подробно развили в § 7—9, дает исчерпывающий ответ на второй, более трудный

из двух поставленных в § 7, п. 1 основных вопросов, а именно, по каким нечетным простым числам p заданное число a является квадратичным вычетом. Теперь мы вернемся еще раз к первому, более простому из этих вопросов, а именно, какие числа a являются квадратичными вычетами по заданному нечетному простому числу p. Непосредственно на этот вопрос полностью дают ответ три критерия из § 6, с помощью которых можно тремя различными способами решить, является ли a квадратичным вычетом по $\bmod p$ или нет. Однако ни один из этих трех критериев не позволяет нам узнать, как распределены квадратичные вычеты и невычеты в наименьшей системе вычетов по $\bmod p$.

В этом отношении мы можем пока сделать только следующие слабые высказывания:

I. *Среди $p-1$ вычетов $a \bmod p$, взаимно простых с модулем, существует точно $(p-1)/2$ квадратичных вычетов и $(p-1)/2$ квадратичных невычетов.*

II. *Распределение квадратичных вычетов и невычетов $a \bmod p$ в наименьшей системе вычетов $0 < a < p$, взаимно простых с модулем, является симметричным или кососимметричным относительно $p/2$, в зависимости от того, $p \equiv 1$ или $-1 \bmod 4$.*

Доказательства. Первое было установлено уже в § 6, п. 4; второе следует из того, что квадратичный характер $\left(\frac{a}{p}\right) = \chi_p(a)$ является четным или нечетным (см. § 9, п. 5) в зависимости от того, имеет ли место $\left(\frac{-1}{p}\right) = \chi_p(-1) = 1$ или -1, а это по первому дополнению к закону взаимности определяется тем, что $p \equiv 1$ или $-1 \bmod 4$.

Желание получить более точные высказывания о распределении квадратичных вычетов в наименьшей системе вычетов по $\bmod p$ послужило в последнее время поводом для развития интересной теории, которая систематически рассматривает те общие вопросы распределения, к которым можно придти, исходя из теории квадратичных вычетов. Правда, для этого привлекаются глубокие вспомогательные средства арифметической теории полей алгебраических функций. Здесь мы сделаем обзор вопросов и результатов этой теории, а в тех случаях, когда необходимые вспомогательные средства будут для нас доступны, дадим также и элементарные доказательства.

В дальнейшем мы все время будем понимать под p простое нечетное число, которое сначала рассматривается как фиксированное.

Для рассматриваемого вопроса — а также и из других соображений — целесообразно распространить определение символа Лежандра $\left(\frac{a}{p}\right)$ на нулевой класс $a \equiv 0 \bmod p$, а именно,

положить

$$\left(\frac{a}{p}\right)=0 \qquad \text{для } a\equiv 0 \bmod p. \tag{1}$$

Это дополнительное определение дано так, что в расширенной области определения остаются в силе правило умножения

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

и критерий Эйлера

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \bmod p.$$

Однако необходимо отметить, что это расширение определения символа $\left(\frac{a}{p}\right)$ как *характера* по $\bmod p$ *не согласуется* со сделанным в § 9, п. 1 расширением этого определения на числа a, имеющие лишь взаимно простые с p свободные от квадратов ядра. То расширение было целесообразным для квадратичного закона взаимности; действительно, при этом, в отличие от (1), значение символа определялось так: $\left(\frac{a}{p}\right)=\left(\frac{a_0}{p}\right)$, если $a=p^{2\alpha}a_0$ с a_0, взаимно простым с p. Поэтому здесь мы должны отказаться от этого последнего расширения определения символа $\left(\frac{a}{p}\right)$ *как числовой функции*.

Факт I, а именно, что в каждой системе вычетов по $\bmod p$, взаимно простых с модулем, существует одинаковое количество квадратичных вычетов и невычетов, можно выразить с помощью символа Лежандра в виде формулы

$$\sum_{a \bmod p}\left(\frac{a}{p}\right)=0, \tag{2}$$

где a может теперь пробегать также и полную систему вычетов по $\bmod p$ (а не только вычеты, взаимно простые с модулем).

Непосредственное значение дополнительного определения (1) для нашей цели заключается в том факте, что теперь количество N решений сравнения $x^2\equiv a \bmod p$ для каждого $a \bmod p$ дается выражением

$$N[x^2\equiv a \bmod p]=1+\left(\frac{a}{p}\right). \tag{3}$$

В самом деле, для $a\not\equiv 0 \bmod p$ уже в IIа п. 3 § 6 было установлено, что $N=2$ или 0 в зависимости от того, является ли a квадратичным вычетом или невычетом по $\bmod p$, т. е. зависит от того, имеет ли место $\left(\frac{a}{p}\right)=1$ или -1; если же $a\equiv 0 \bmod p$,

т. е. нужно считать $\left(\frac{a}{p}\right)=0$, то мы имеем $N=1$, так как тогда решением сравнения является лишь $x\equiv 0 \bmod p$.

В дальнейшем мы будем использовать примененный в (3) способ обозначения для количества решений сравнения также и в более общих случаях

$$N[f(x)\equiv 0 \bmod p], \qquad N[f(x, y)\equiv 0 \bmod p],$$

где $f(x)$, $f(x, y)$ суть многочлены с целыми (или только p-целыми) коэффициентами. В последнем случае имеется в виду количество пар $x, y \bmod p$, являющихся решениями. Если же понадобится выразить только количество решений $y \bmod p$ при постоянном $x \bmod p$, то мы будем указывать это постоянное x в виде индекса при N. В этом смысле имеет место общая формула сложения

$$N[f(x, y)\equiv 0 \bmod p]=\sum_{x \bmod p} N_x[f(x, y)-0 \bmod p]. \tag{4}$$

Если записать (3) с помощью двух неизвестных x, y в виде

$$N_x[x\equiv y^2 \bmod p]=1+\left(\frac{x}{p}\right),$$

то, принимая во внимание (2), мы получим из (4) формулу

$$N[x\equiv y^2 \bmod p]=p. \tag{5}$$

Это — первый результат такого типа, который будет фигурировать в дальнейшем. Правда, этот результат совсем тривиален; в самом деле, он делается тотчас же очевидным, если решения x, y расположить не по отдельным x, как в приведенном выводе, а по отдельным y.

Таким же путем можно вообще из

$$N_x[f(x)\equiv y^2 \bmod p]=1+\left(\frac{f(x)}{p}\right)$$

получить формулу

$$N[f(x)\equiv y^2 \bmod p]=p+\sum_{x \bmod p}\left(\frac{f(x)}{p}\right)=p+\Phi_p(f) \tag{6}$$

для любого многочлена $f(x)$ с целыми (или только p-целыми) коэффициентами. Здесь, кроме основного члена p, появляется справа еще дополнительный член

$$\Phi_p(f)=\sum_{x \bmod p}\left(\frac{f(x)}{p}\right). \tag{7}$$

В специальном случае (5) с $f(x)=x$ этот дополнительный член $\sum\limits_{x \bmod p}\left(\frac{x}{p}\right)=0$, и, как уже было сказано в связи с (2),

этим выражается приведенное в начале слабое высказывание I о распределении квадратичных вычетов и невычетов по $\bmod p$. Аналогично и в более общем случае имеет место

$$N[f_1(x) \equiv y^2 \bmod p] = p, \qquad \Phi_p(f_1) = 0 \tag{8}$$

для каждого линейного по $\bmod p$ многочлена

$$f_1(x) = ax + b \qquad (a \not\equiv 0 \bmod p).$$

Действительно, при $a \not\equiv 0 \bmod p$ вместе с x также и $ax + b$ пробегает полную систему вычетов по $\bmod p$.

Если нам удастся вычислить дополнительный член $\Phi_p(f)$ для другого, нелинейного многочлена f, то тем самым мы будем иметь дальнейшее высказывание об этом распределении, правда, в неявной форме. Как мы увидим дальше, конкретные вопросы о распределении квадратичных вычетов по $\bmod p$ приводят к обратной задаче вычисления определенной в (7) суммы $\Phi_p(f)$ для определенного многочлена f. Для этой суммы, очевидно, имеют место следующих два формальных правила:

$$\Phi_p(f(ax + b)) = \Phi_p(f(x)) \qquad (a \not\equiv 0 \bmod p), \tag{9}$$

$$\Phi_p(af(x)) = \left(\frac{a}{p}\right) \Phi_p(f(x)), \tag{10}$$

в силу которых можно без ограничения общности подвергать исследуемый многочлен f целым, линейным по $\bmod p$ преобразованиям, и предполагать его старший коэффициент равным 1.

Прежде чем обратиться к упомянутым конкретным вопросам распределения, заметим еще, что с помощью символа Лежандра можно выразить количество решений не только для специального квадратного сравнения $x^2 - a \equiv 0 \bmod p$, но и для общего квадратного сравнения

$$f_2(x) = ax^2 + bx + c \equiv 0 \bmod p \qquad (a \not\equiv 0 \bmod p).$$

Так как $p \neq 2$ и $a \not\equiv 0 \bmod p$, то мы можем перейти к умноженному на $4a$ сравнению

$$4af_2(x) = (2ax + b)^2 - d \equiv 0 \bmod p,$$

где

$$d = b^2 - 4ac,$$

и определить для него количество решений в неизвестном $y \bmod p$, которое взаимно однозначно связано с $x \bmod p$ посредством формулы

$$y \equiv 2ax + b \bmod p.$$

Тем самым наша задача сводится к специальному случаю (3).

Таким образом, получается формула

$$N[f_2(x) \equiv 0 \bmod p] = 1 + \left(\frac{d}{p}\right), \tag{11}$$

где d — дискриминант квадратного многочлена f_2 по $\bmod p$.

2. Последовательности с заданными значениями характера. Для того чтобы полностью выяснить распределение квадратичных вычетов и невычетов по $\bmod p$, нужно было бы знать, следует ли за данным квадратичным вычетом, соответственно невычетом $a \bmod p$ квадратичный вычет или невычет $a+1 \bmod p$. Однако такое *исчерпывающее* описание распределения вряд ли возможно получить. Мы должны быть довольны, если нам удастся узнать, аналогично приведенному вначале слабому высказыванию I, п. 1, *количество* встречающихся в системе классов вычетов, взаимно простых с модулем, последовательностей каждого из четырех типов: ВВ, ВН, НВ, НН, где В, Н обозначают «квадратичный вычет», соответственно «невычет». Эта цель оказывается выполнимой.

Мы обобщим этот вопрос на последовательности какой угодно длины n с $1 \leqslant n \leqslant p-1$, т. е. поставим вопрос о количестве $N_0(\varepsilon_1, \ldots, \varepsilon_n \mid p)$ встречающихся в системе классов вычетов по $\bmod p$, взаимно простых с модулем, n-членных последовательностей $x+1, \ldots, x+n$ с заданными квадратичными характерами

$$\left(\frac{x+1}{p}\right) = \varepsilon_1, \quad \ldots, \quad \left(\frac{x+n}{p}\right) = \varepsilon_n, \tag{1}$$

где, таким образом, $\varepsilon_1, \ldots, \varepsilon_n$ суть заданные единицы ± 1. Если считать, что у нас взята наименьшая система вычетов по $\bmod p$, взаимно простых с модулем, то следует предполагать $0 \leqslant x < p-n$, для того чтобы последовательность $x+1, \ldots, x+n$ целиком принадлежала этой системе. Очевидно, что n требований (1) одновременно удовлетворяются тогда и только тогда, когда

$$\left(1+\varepsilon_1\left(\frac{x+1}{p}\right)\right) \ldots \left(1+\varepsilon_n\left(\frac{x+n}{p}\right)\right) = 2^n,$$

в то время как в каждом другом случае (при указанном ограничении относительно x) это произведение равно 0. Поэтому искомое количество дается аддитивной формулой

$$N_0(\varepsilon_1, \ldots, \varepsilon_n \mid p) = \frac{1}{2^n} \sum_{0 \leqslant x < p-n} \left(1+\varepsilon_1\left(\frac{x+1}{p}\right)\right) \ldots \left(1+\varepsilon_n\left(\frac{x+n}{p}\right)\right). \tag{2}$$

С теоретической точки зрения целесообразнее вместо этой суммы, ограниченной значениями $0 \leqslant x < p-n$, рассматривать сумму, распространенную на всю систему вычетов $0 \leqslant x < p$, в которой тогда вместо этой наименьшей системы вычетов по $\bmod p$ может фигурировать также и любая другая система:

$$N(\varepsilon_1, \ldots, \varepsilon_n \mid p) = \frac{1}{2^n} \sum_{x \bmod p} \left(1+\varepsilon_1\left(\frac{x+1}{p}\right)\right) \ldots \left(1+\varepsilon_n\left(\frac{x+n}{p}\right)\right). \tag{3}$$

Сумма добавляющихся при переходе от (2) к (3) n членов легко может быть определена. В каждом из этих членов среди $x+1, \ldots, x+n$ встречается $x+\nu_0 = p$, которому соответствует множитель $1+\varepsilon_{\nu_0}\left(\frac{x+\nu_0}{p}\right) = 1$. Произведение остальных $n-1$ множителей равно 2^{n-1}, если для остальных $x+\nu$ выполняются поставленные требования (1), в противном же случае произведение равно 0. Принимая во внимание множитель $1/2^n$ перед знаком суммы, мы получаем, что сумма этих n дополнительных членов равна половине количества тех x в интервале $p-n \leqslant x < p$, для которых выполняются $n-1$ требований (1) с $x+\nu \neq p$. Другими словами, в формуле для N, в отличие от N_0, система вычетов $x \bmod p$ рассматривается как циклически замкнутая, причем N равно количеству n-членных последовательностей, для которых выполняются требования (1), плюс половина количества n-членных последовательностей, для которых одно из этих требований $\left(\frac{x+\nu_0}{p}\right) = \varepsilon_{\nu_0}$ заменено на $\left(\frac{x+\nu_0}{p}\right) = 0$, а все остальные остаются те же. Поэтому для количеств N_0, N из (2), (3) во всяком случае имеет место неравенство

$$0 \leqslant N - N_0 \leqslant \frac{n}{2}. \tag{4}$$

В тривиальном частном случае $n = 1$ будет

$$N = p/2 = (p-1)/2 + 1/2.$$

Как мы сейчас покажем, количество N может быть вычислено, исходя из (3). Раскрывая скобки в общем члене справа и суммируя получающиеся при этом 2^n произведений, мы сначала получим главный член

$$\frac{1}{2^n} \sum_{x \bmod p} 1 = \frac{p}{2^n},$$

соответствующий произведению всех слагаемых, равных 1, и далее $2^n - 1$ дополнительных членов, соответствующих произведениям, в которые входит хотя бы одно из слагаемых вида $\varepsilon_\nu\left(\frac{x+\nu}{p}\right)$;

эти дополнительные члены имеют вид

$$\frac{1}{2^n}\varepsilon_{\nu_1}\ \dots\ \varepsilon_{\nu_r}\sum_{x \bmod p}\left(\frac{(x+\nu_1)\ \dots\ (x+\nu_r)}{p}\right)=\frac{1}{2^n}\varepsilon_{\nu_1}\ \dots\ \varepsilon_{\nu_r}\Phi_p\left(f_{\nu_1,\dots,\nu_r}\right),$$

где $\nu_1, \dots, \nu_r$ пробегают всевозможные комбинации из $1, \dots, n$ с количествами членов $r=1, \dots, n$. При этом в числителях символов Лежандра стоят многочлены r-й степени

$$f_{\nu_1,\dots,\nu_r}(x)=(x+\nu_1)\ \dots\ (x+\nu_r),$$

так что с точностью до множителя $(1/2^n)\varepsilon_{\nu_1}\ \dots\ \varepsilon_{\nu_r}$ получаются определенные в (7) п. 1 суммы $\Phi_p\left(f_{\nu_1,\dots,\nu_r}\right)$ для этих многочленов. В итоге мы получаем:

$$N(\varepsilon_1, \dots, \varepsilon_n \mid p)=\frac{p}{2^n}+\frac{1}{2^n}\sum_{r=1}^{n}\sum_{\{\nu_1,\dots,\nu_r\}}\varepsilon_{\nu_1}\ \dots\ \varepsilon_{\nu_r}\Phi_p\left(f_{\nu_1,\dots,\nu_r}\right), \tag{5}$$

где $\{\nu_1, \dots, \nu_r\}$ пробегает r-членные комбинации из $1, \dots, n$. Таким образом, наряду с главным членом $p/2^n$ фигурирует еще сумма 2^n-1 дополнительных членов, снабженная множителем $1/2^n$; эти дополнительные члены (с точностью до знаков, определяемых значениями $\varepsilon_1, \dots, \varepsilon_n$) имеют вид (7) п. 1 с многочленами степени $r=1, \dots, n$ и старшими коэффициентами, равными 1.

3. Теоретико-вероятностное истолкование. Обзор результатов. В связи с формулами (6) п. 1 и (5) п. 2 мы говорили о *главном члене* и *дополнительных членах*. Теперь мы поясним подробнее, почему мы употребляем такие названия. С наивной теоретико-вероятностной точки зрения следует ожидать, что сравнению $f(x)\equiv y^2 \bmod p$ будет удовлетворять приблизительно p-я часть всех p^2 пар классов вычетов $x, y \bmod p$ и что требованиям $\left(\frac{x+\nu}{p}\right)=\varepsilon_\nu$ $(\nu=1, \dots, n)$, наложенным на последовательность, будет удовлетворять приблизительно 2^n-я часть всех p классов вычетов $x \bmod p$. Действительно, в первом случае на пары классов вычетов $x, y \bmod p$ накладывается одно условие $f(x)\equiv y^2 \bmod p$, из которого при заданном $x \bmod p$, вообще говоря, определяется $y \bmod p$, а во втором случае на классы вычетов $x \bmod p$ накладывается система n условий $\left(\frac{x+\nu}{p}\right)=\varepsilon_\nu$ $(\nu=1, \dots, n)$, каждое из которых выполняется приблизительно для половины всех классов вычетов $x \bmod p$. В каждом из этих случаев главный член равен вероятности $1/p$, соответственно $1/2^n$ наступления рассматриваемого события, увеличенной в число раз, равное

количеству всех рассматриваемых пар классов вычетов, или, соответственно, просто классов вычетов, т. е. равное p^2, соответственно p. Впрочем, надо сказать, что в первом случае сравнение $f(x) \equiv y^2 \bmod p$ при заданном $x \bmod p$ определяет в действительности или ни одного, или одно, или два значения $y \bmod p$, так что приведенное выше наивное рассуждение в действительности не решает вопрос, существует ли в совокупности приблизительно p решений x, $y \bmod p$ (например, для $f(x) = x^2$, когда сравнение $x^2 \equiv y^2 \bmod p$ распадается на два сравнения: $x \equiv y$ или $x \equiv -y \bmod p$, существует $2p-1$ решений), а во втором случае не устанавливает, являются ли n условий $\left(\frac{x+\nu}{p}\right) = \varepsilon_\nu$ $(\nu = 1, \ldots, n)$ независимыми в теоретико-вероятностном смысле, т. е. действительно ли вероятность равна произведению $1/2^n$ отдельных вероятностей $1/2$. Далее, строго говоря, нельзя говорить о вероятности, пока простое число p рассматривается фиксированным, так как в этом случае мы имеем всего одно испытание, соответственно одну систему из n испытаний. Однако если распространить рассмотрение на совокупность всех нечетных простых чисел p, то, вследствие ее бесконечности, мы в действительности получаем предпосылку для применения теоретико-вероятностных методов.

При таком подходе к вопросу надо считать фиксированными целочисленный многочлен $f(x)$, соответственно натуральное число n и единицы $\varepsilon_1, \ldots, \varepsilon_n$ и рассматривать количество решений $N[f(x) \equiv y^2 \bmod p]$, соответственно количество последовательностей $N(\varepsilon_1, \ldots, \varepsilon_n | p)$ для всех нечетных простых чисел p (в последнем случае $p \geqslant n$). Тогда возникает вопрос, имеет ли отклонение этого количества N от главного члена p, соответственно $p/2^n$, рассматриваемое как функция от p, *меньший порядок возрастания*, чем главный член, т. е. стремится ли к нулю при $p \to \infty$ это отклонение, деленное на p, соответственно $p/2^n$. Если это имеет место, то можно говорить, что рассматриваемый вопрос распределения касается одного, соответственно n, *независимых событий*, и называть главный член *наиболее вероятным* или *средним значением*, а дополнительный член, соответственно сумму дополнительных членов — *ошибкой*. Если, более того, окажется, что ошибка имеет порядок возрастания, не только меньший чем p, но даже не превосходящий порядка $O(\sqrt{p})$, т. е. что абсолютная величина этой ошибки меньше, чем $C\sqrt{p}$, где C — некоторая, пусть и неопределенная, но во всяком случае не зависящая от p константа, то, как принято в так называемом законе больших чисел, мы будем говорить, что для рассматриваемого вопроса распределения выполняется *статистический закон рассеивания*. Наконец, если можно показать, что ошибка

точно имеет порядок $O(\sqrt{p})$ (т. е. порядок, не меньший чем у $\sqrt{p}$), то можно будет говорить о *случайном распределении*.

Так, например, рассмотренное в (8) п. 1 сравнение $f_1(x) \equiv y^2 \bmod p$ с линейным многочленом $f_1(x) = ax + b$ тривиальным образом удовлетворяет статистическому закону рассеивания, ибо за исключением конечного множества $p \mid a$ все время имеет место $N = p$; так как, однако, ошибка здесь равна нулю, то случайного распределения мы здесь не имеем. Для приведенного выше сравнения $x^2 \equiv y^2 \bmod p$, напротив, не имеет места статистическое рассеивание, потому что в этом случае все время $N = 2p - 1 = p + (p-1)$; это сравнение нельзя рассматривать как одно независимое событие, что находит себе выражение в том, что это сравнение распадается на два исключающих друг друга сравнения $x \equiv y$ или $x \equiv -y \bmod p$. Так же обстоит дело и в более общем случае для сравнений $f_1(x)^2 \equiv y^2 \bmod p$ с линейным многочленом f_1. В дальнейшем мы познакомимся с одним типом сравнений $f(x) \equiv y^2 \bmod p$, для которого выполняется закон рассеивания, и имеет место случайное распределение.

Для количества последовательностей $N(\varepsilon_1, \ldots, \varepsilon_n \mid p)$ наш вопрос о порядке возрастания дополнительных членов сводится посредством формулы (5) п. 2 и в соответствии с (6), (7) п. 1 к аналогичному вопросу для количеств решений $N[f(x) \equiv y^2 \bmod p]$ с некоторыми определенными многочленами $f = f_{\nu_1, \ldots, \nu_r}$ степеней $r = 1, \ldots, n$. Если можно будет показать, что для этих многочленов все время имеет место

$$\Phi(f_{\nu_1, \ldots, \nu_r}) = O(\sqrt{p}),$$

то, действительно, будет следовать

$$N(\varepsilon_1, \ldots, \varepsilon_n \mid p) = \frac{p}{2^n} + O(\sqrt{p}),$$

причем даже с одной и той же константой C в члене, дающем оценку ошибки. Тогда, согласно (4) п. 2, такая же формула, вообще говоря (с другими константами), имеет место и для исходного количества последовательностей $N_0(\varepsilon_1, \ldots, \varepsilon_n \mid p)$, когда не принимаются во внимание последовательности, не лежащие целиком в наименьшей системе вычетов.

Оказывается, что верна следующая совершенно общая оценка:

$$N[f(x, y) \equiv 0 \bmod p] = p + O(\sqrt{p}), \tag{1}$$

где $f(x, y)$ есть какой-нибудь целочисленный многочлен от двух неизвестных, который только должен быть абсолютно неприводимым (т. е. неприводимым в поле всех алгебраических чисел). Несколько лет назад А. Вейль сообщил о доказательстве этого факта, а в вышедшей недавно работе это доказательство

проводится полностью. Оно опирается на очень глубокие вспомогательные средства из арифметической теории полей алгебраических функций или алгебраической геометрии. С помощью этих средств мне удалось за несколько лет до этого доказать для интересующих нас здесь сравнений специального типа оценку

$$N[f(x)\equiv y^2 \bmod p] = p + O(\sqrt{p}), \text{ т. е. } \Phi(f) = O(\sqrt{p}) \qquad (2)$$

в случаях свободных от квадратов многочленов $f(x)$ третьей и четвертой степени. Впрочем, при таком доказательстве, опирающемся на теорию алгебраических функций, для ошибки получается точная оценка в виде

$$|N^* - (p+1)| \leqslant 2g\sqrt{p}, \qquad (3)$$

где N^* есть количество решений в несколько ином смысле, а именно, принимаются во внимание также и должным образом определенные бесконечные решения (тогда среднее значение получается уже равным $p+1$), а константа g есть определяемый в этой теории *род* алгебраического уравнения $f(x, y) = 0$; при этом исключается из рассмотрения конечное множество тех p, для которых при переходе к сравнению $f(x, y) \equiv 0 \bmod p$ утрачивается абсолютная неприводимость или понижается род.

Для сравнений типа (2), интересующих нас здесь в связи с вопросом о последовательностях, абсолютная неприводимость по $\bmod p$ будет иметь место, если $f(x)$, рассматриваемый как многочлен над полем классов вычетов по $\bmod p$, при условии что его старший коэффициент равен 1, не является квадратом. Если, без существенного ограничения общности, предположить, что $f(x) \bmod p$ даже свободен от квадратов (что равносильно тому, что его дискриминант $\not\equiv 0 \bmod p$), то многочлены степеней $2g+1$, $2g+2$ всегда будут иметь род g. Бесконечные решения определяются в этих случаях следующим образом. Пусть

$$f(x) \equiv a_0 x^{2g+2} + a_1 x^{2g+1} + \ldots + a_{2g+2} \bmod p$$

с $a_0 \equiv 0$, $a_1 \not\equiv 0$ или $a_0 \not\equiv 0 \bmod p$ в зависимости от того, имеет ли $f(x) \bmod p$ степень $2g+1$ или $2g+2$. Положим тогда $x = 1/\xi$, $y = \eta/\xi^{g+1}$. Сравнение $f(x) \equiv y^2 \bmod p$ перейдет при этом в

$$a_0 + a_1\xi + \ldots + a_{2g+2}\xi^{2g+2} \equiv \eta^2 \bmod p.$$

Бесконечными решениями сравнения $f(x) \equiv y^2 \bmod p$ будут называться те решения ξ, $\eta \bmod p$ последнего сравнения, для которых $\xi \equiv 0 \bmod p$ и, следовательно, $\eta^2 \equiv a_0 \bmod p$. Их количество, согласно (3) п. 1, равно $1 + \left(\frac{a_0}{p}\right)$. Поэтому для количества решений в новом смысле получается

$$N^* = N + 1 + \left(\frac{a_0}{p}\right),$$

и потому

$$N^* - (p+1) = \left\{ \begin{array}{ll} N-p & \text{для нечетной степени } 2g+1 \\ N+\left(\frac{a_0}{p}\right)-p & \text{для четной степени } 2g+2 \end{array} \right\},$$

где a_0 означает старший коэффициент многочлена $f(x) \bmod p$, если его формально записывать в виде многочлена степени $2g+2$. Поэтому в случаях $g=0$ и $g=1$, т. е. для многочленов первой — второй и третьей — четвертой степени, которыми мы будем заниматься в дальнейшем, высказывание (3) принимает вид:

$$\left\{ \begin{array}{ll} N=p & \text{для степени } 1 \\ N=p-1 & \text{для степени } 2 \end{array} \right\} \qquad (3_0)$$

$$\left\{ \begin{array}{ll} |N-p| & \leqslant 2\sqrt{p} \text{ для степени } 3 \\ |N+1-p| & \leqslant 2\sqrt{p} \text{ для степени } 4 \end{array} \right\}, \qquad (3_1)$$

Мы привели здесь без доказательства эти сведения из арифметической теории алгебраических функций, относящиеся к случаю $f(x) \equiv y^2 \bmod p$, чтобы сделать ясным, что специальные результаты, которые будут получены в дальнейшем, подчиняются приведенным перед этим общим фактам (1), (2), (3).

Как уже сказано, случай многочлена первой степени ($g=0$) является, в силу (8) п. 1, тривиальным. Случай многочленов второй степени ($g=0$), так же как и случай многочленов третьей степени ($g=1$) того специального вида, который фигурирует в формуле (5) п. 2 для количества последовательностей, был уже давно исследован Якобшталем элементарными методами. В дальнейшем мы и изложим подробно эти результаты Якобшталя и применим их к вопросу о последовательностях.

Предварительно заметим еще, что глубоким, исчерпывающим результатам (1), (2) предшествовали полученные более простыми средствами результаты Морделла и Давенпорта, относящиеся к специальному случаю сравнений вида $f(x) \equiv y^m \bmod p$ (не только для $m=2$). При этом, однако, для оценки ошибки были получены несколько менее точные порядки $O(p^\theta)$ с $1/2 < \theta < 1$.

4. Случай многочленов второй степени. Рассмотрим целочисленный свободный от квадратов многочлен $f_2(x)$, относительно которого мы, согласно (10) п. 1, можем без ограничения общности предположить, что его старший коэффициент равен 1:

$$f_2(x) = x^2 + bx + c.$$

Дискриминант многочлена f_2 равен

$$d = b^2 - 4c.$$

Мы хотим точно вычислить сумму

$$\Phi_p(f_2) = \sum_{x \bmod p} \left(\frac{f_2(x)}{p}\right).$$

Для этого мы, *во-первых*, сделаем оценку ее абсолютной величины, а *во-вторых* и *в-третьих*, определим ее значения по $\bmod 2$ и по $\bmod p$.

Оценка для абсолютной величины суммы $\Phi_p(f_2)$ получается сразу:

$$|\Phi_p(f_2)| \leqslant p. \tag{1}$$

Действительно, сумма $\Phi_p(f_2)$ состоит из p членов, каждый из которых имеет одно из значений ± 1, 0, т. е. по абсолютной величине $\leqslant 1$.

Для значения $\Phi_p(f_2)$ по $\bmod 2$ прежде всего следует

$$\Phi_p(f_2) \equiv (p-N)\cdot 1 + N\cdot 0 \equiv p - N \equiv 1 - N \equiv N - 1 \bmod 2,$$

где N есть количество решений сравнения $f_2(x) \equiv 0 \bmod p$. Но согласно (11) п. 1, $N = 1 + \left(\frac{d}{p}\right)$. Отсюда получается:

$$\Phi_p(f_2) \equiv \left(\frac{d}{p}\right) \equiv \left\{ \begin{array}{ll} 1 \bmod 2 & \text{для } d \not\equiv 0 \bmod p \\ 0 \bmod 2 & \text{для } d \equiv 0 \bmod p \end{array} \right\}. \tag{2}$$

Для определения значения $\Phi_p(f_2)$ по $\bmod p$ нам будут нужны значения по $\bmod p$ сумм

$$S_r \equiv \sum_{x \bmod p} x^r \equiv \sum_{x \not\equiv 0 \bmod p} x^r \bmod p$$

для натуральных показателей r. Если для $x \not\equiv 0 \bmod p$ ввести представление

$$x \equiv w^{\nu} \bmod p \quad (\nu \bmod p-1)$$

через первообразный корень $w \bmod p$, то эти нужные нам значения получаются такими:

$$S_r \equiv \sum_{\nu \bmod p-1} w^{\nu r} \equiv \left\{ \begin{array}{ll} p-1 \equiv -1 \bmod p & \text{для } r \equiv 0 \bmod p-1 \\ \frac{w^{(p-1)r}-1}{w^r-1} \equiv 0 \bmod p & \text{для } r \not\equiv 0 \bmod p-1 \end{array} \right\}.$$

С помощью этих формул искомое значение $\Phi_p(f_2)$ по $\bmod p$ получается следующим красивым приемом. Согласно критерию Эйлера,

$$\left(\frac{f_2(x)}{p}\right) \equiv f_2(x)^{\frac{p-1}{2}} \equiv (x^2+bx+c)^{\frac{p-1}{2}} \equiv$$

$$\equiv x^{p-1} + a_1 x^{p-2} + \ldots + a_{p-2}x + a_{p-1} \bmod p$$

с некоторыми целыми коэффициентами $a_1, \ldots, a_{p-1}$. Отсюда суммированием по $x \bmod p$ получается

$$\Phi_p(f_2) \equiv S_{p-1} + a_1 S_{p-2} + \ldots + a_{p-2} S_1 + p a_{p-1} \bmod p,$$

и потому, согласно полученным выше формулам,

$$\Phi_p(f_2) \equiv -1 \bmod p. \tag{3}$$

Теперь из высказываний (1), (2), (3) можно установить точное значение $\Phi_p(f_2)$. Прежде всего, (2) и (3) вместе дают

$$\Phi_p(f_2) \equiv \left\{ \begin{array}{ll} -1 \bmod 2p & \text{для } d \not\equiv 0 \bmod p \\ p-1 \bmod 2p & \text{для } d \equiv 0 \bmod p \end{array} \right\}.$$

Далее, согласно (1), $\Phi_p(f_2)$ равно одному из $2p+1$ чисел $-p, \ldots, p$. Среди этих чисел каждый класс вычетов $\not\equiv p \bmod 2p$ имеет только одного представителя, и потому $\Phi_p(f_2)$ должно совпадать с только что указанным, принадлежащим этой последовательности остатком -1, соответственно $p-1$ по $\bmod 2p$. Таким образом, мы имеем следующий результат:

III. *Если f_2 есть целочисленный квадратный многочлен со старшим коэффициентом 1 и дискриминантом d, то*

$$\Phi_p(f_2) = \left\{ \begin{array}{ll} -1 & \text{для } d \not\equiv 0 \bmod p \\ p-1 & \text{для } d \equiv 0 \bmod p \end{array} \right\}$$

и, таким образом,

$$N[f_2(x) \equiv y^2 \bmod p] = \left\{ \begin{array}{ll} p-1 & \text{для } d \not\equiv 0 \bmod p \\ 2p-1 & \text{для } d \equiv 0 \bmod p \end{array} \right\}.$$

С точки зрения общего изложения в п. 3, относительно этого результата нужно заметить следующее. В случае $d \equiv 0 \bmod p$

$$f_2(x) \equiv \left(x + \frac{1}{2} b\right)^2 \bmod p,$$

так что сравнение

$$f_2(x) - y^2 \equiv \left(x + \frac{1}{2} b\right)^2 - y^2 \bmod p$$

распадается на два сравнения

$$x + \frac{1}{2} b - y \equiv 0 \quad \text{или} \quad x + \frac{1}{2} b + y \equiv 0 \bmod p,$$

и, как уже было установлено в п. 3, имеет количество решений

$$N = 2p - 1 = p + (p-1).$$

Таким образом, в этом случае наш результат тривиален. В случае $d \not\equiv 0 \bmod p$ сравнение $f_2(x) - y^2 \equiv 0 \bmod p$ абсолютно неприводимо и имеет род $g = 0$. Наш результат подтверждает тогда второе высказывание из (3_0) п. 3.

5. Применение к двучленным последовательностям. В случае $n=2$ общая формула (5) п. 2 для количества последовательностей принимает вид

$$N(\varepsilon_1, \varepsilon_2 \mid p) = \frac{p}{4} + \frac{\varepsilon_1}{4}\Phi_p(x+1) + \frac{\varepsilon_2}{4}\Phi_p(x+2) + \frac{\varepsilon_1\varepsilon_2}{4}\Phi_p(x+1)(x+2).$$

Из трех дополнительных членов первые два с линейными многочленами $x+1$, $x+2$ имеют, согласно (8) п. 1, значение 0, в то время как последний с квадратным многочленом $(x+1)(x+2)$, в силу III, п. 4, имеет значение -1. Таким образом, мы получаем:

$$N(\varepsilon_1, \varepsilon_2 \mid p) = \frac{p}{4} - \frac{\varepsilon_1\varepsilon_2}{4}. \tag{1}$$

Поэтому для двучленных последовательностей выполняется статистический закон рассеивания. Однако случайное распределение не имеет места; напротив, ошибка все время имеет одно из значений $\pm 1/4$.

Вычислим также первоначальное количество последовательностей $N_0(\varepsilon_1, \varepsilon_2 \mid p)$, когда не принимаются в расчет граничные пары $(-1, 0)$ и $(0, 1) \bmod p$. В силу (2), (3) п. 2 и первого дополнения к закону взаимности, мы получаем

$$N(\varepsilon_1, \varepsilon_2 \mid p) - N_0(\varepsilon_1, \varepsilon_2 \mid p) =$$
$$= \frac{1}{4}\left(1+\varepsilon_1\left(\frac{-1}{p}\right)\right)\left(1+\varepsilon_2\left(\frac{0}{p}\right)\right) + \frac{1}{4}\left(1+\varepsilon_1\left(\frac{0}{p}\right)\right)\left(1+\varepsilon_2\left(\frac{1}{p}\right)\right) =$$
$$= \frac{1}{4}\left(1+\varepsilon_1(-1)^{\frac{p-1}{2}}\right) + \frac{1}{4}(1+\varepsilon_2).$$

Поэтому, согласно (1), для $p \equiv 1 \bmod 4$

$$N_0(\varepsilon_1, \varepsilon_2 \mid p) = \frac{p}{4} - \frac{\varepsilon_1\varepsilon_2 + (1+\varepsilon_1) + (1+\varepsilon_2)}{4} = \frac{p-1}{4} - \frac{(1+\varepsilon_1)(1+\varepsilon_2)}{4} \tag{2а}$$

и для $p \equiv -1 \bmod 4$

$$N_0(\varepsilon_1, \varepsilon_2 \mid p) = \frac{p}{4} - \frac{\varepsilon_1\varepsilon_2 + (1-\varepsilon_1) + (1+\varepsilon_2)}{4} = \frac{p-3}{4} + \frac{(1+\varepsilon_1)(1-\varepsilon_2)}{4}. \tag{2б}$$

Из этих формул получается следующая таблица для отдельных случаев:

ε_1 ε_2	$N_0(\varepsilon_1\varepsilon_2 \mid p \equiv 1 \bmod 4)$	$N_0(\varepsilon_1\varepsilon_2 \mid p \equiv -1 \bmod 4)$
$+1$ $+1$	$\frac{p-5}{4}$	$\frac{p-3}{4}$
$+1$ -1	$\frac{p-1}{4}$	$\frac{p+1}{4}$
-1 $+1$	$\frac{p-1}{4}$	$\frac{p-3}{4}$
-1 -1	$\frac{p-1}{4}$	$\frac{p-3}{4}$

6. Случай специального многочлена третьей степени. В случае $n=3$ в общей формуле (5) п. 2 для количества последовательностей, кроме многочленов первой и второй степени, фигурирует еще многочлен $(x+1)(x+2)(x+3)$ третьей степени. Мы хотим вычислить соответствующую ему сумму

$$\Phi_p = \Phi_p((x+1)(x+2)(x+3)) = \sum_{x \bmod p} \left(\frac{(x+1)(x+2)(x+3)}{p}\right).$$

При этом, согласно (9) п. 1, мы можем рассматривать получающийся посредством подстановки $x \to x-1$ многочлен $(x-1)x \times (x+1) = x(x^2-1)$:

$$\Phi_p = \Phi_p(x(x^2-1)) = \sum_{x \bmod p} \left(\frac{x}{p}\right)\left(\frac{x^2-1}{p}\right).$$

Согласно (6), (7) п. 1, эта сумма равна ошибке

$$\Phi_p = N[x(x^2-1) \equiv y^2 \bmod p] - p.$$

Мы перейдем посредством простого преобразования к аналогичному представлению для другого сравнения, в котором вместо многочлена третьей степени $x(x^2-1)$ будет стоять многочлен четвертой степени x^4-1, и определим количество решений этого нового сравнения.

Преобразование получается следующим образом. Согласно результату III, п. 4, для многочленов второй степени мы имеем

$$\sum_{x \bmod p} \left(\frac{x^2-1}{p}\right) = -1.$$

Отсюда

$$\Phi_p = \sum_{x \bmod p} \left(1+\left(\frac{x}{p}\right)\right)\left(\frac{x^2-1}{p}\right) + 1.$$

Согласно (3) п. 1, это можно также записать в виде

$$\Phi_p = \sum_{x \bmod p} N_x[x \equiv y^2 \bmod p]\left(\frac{x^2-1}{p}\right) + 1.$$

Если понимать здесь количества решений N_x как кратности, с которыми входят в сумму слагаемые $\left(\frac{x^2-1}{p}\right)$, и суммировать по решениям $y \bmod p$ вместо $x \bmod p$, то эти кратности пропадут и мы получим просто

$$\Phi_p = \sum_{y \bmod p} \left(\frac{y^4-1}{p}\right) + 1,$$

причем, конечно, вместо y можно снова писать x. Таким образом, получается представление:

$$\Phi_p = N[x^4-1 \equiv y^2 \bmod p] + 1 - p. \qquad (1)$$

Фигурирующее здесь сравнение $x^4-1\equiv y^2 \bmod p$ рассматривать легче, чем исходное сравнение $x(x^2-1)\equiv y^2 \bmod p$, несмотря на то, что степень повышается от 3 к 4, ибо новое сравнение имеет более простой вид.

Нам нужно будет рассматривать отдельно оба случая $p\equiv 1 \bmod 4$ и $p\equiv -1 \bmod 4$.

а) $p\equiv -1 \bmod 4$.

Мы рассматриваем этот случай первым, так как он совсем прост. Сравним количество решений сравнения

$$x^4\equiv a \bmod p$$

при фиксированном $a \bmod p$ с количеством решений сравнения

$$u^2\equiv a \bmod p.$$

Если $\left(\frac{a}{p}\right)=-1$, то оба сравнения не имеют решений. Если $\left(\frac{a}{p}\right)=0$, то оба сравнения имеют точно одно решение, а именно, $x\equiv 0$, соответственно $u\equiv 0 \bmod p$. Если $\left(\frac{a}{p}\right)=1$, то последнее сравнение имеет точно два решения $\pm u \bmod p$. При этом, вследствие того что $\left(\frac{-1}{p}\right)=-1$, одно из этих решений однозначно определяется требованием $\left(\frac{u}{p}\right)=1$. Тогда для него сравнение $u\equiv x^2 \bmod p$ имеет точно два решения $\pm x \bmod p$ и они являются решениями первого сравнения. Других решений первое сравнение иметь не может, так как, очевидно, каждая пара $\pm x \bmod p$ его решений в свою очередь дает, в силу $x^2\equiv u \bmod p$, решение $u \bmod p$ последнего сравнения с $\left(\frac{u}{p}\right)=1$. Таким образом, во всех случаях имеет место

$$N[x^4\equiv a \bmod p]=N[u^2\equiv a \bmod p].$$

Применяя это к $a\equiv 1+y^2 \bmod p$ для любого $y \bmod p$, мы получаем

$$N_y[x^4-1\equiv y^2 \bmod p]=N_y[u^2-1\equiv y^2 \bmod p]$$

и потому

$$N[x^4-1\equiv y^2 \bmod p]=N[u^2-1\equiv y^2 \bmod p].$$

Таким образом, в рассматриваемом случае $p\equiv -1 \bmod 4$ наше сравнение с биквадратным многочленом x^4-1 сводится к соответствующему сравнению с квадратным многочленом u^2-1. Причина этого сведения заключается в том, что в циклической группе классов вычетов по $\bmod p$, взаимно простых с модулем, квад-

раты совпадают с четвертыми степенями, если 2 входит в порядок $p-1$ только в первой степени.

Теперь, в силу результата III, п. 4 о квадратных многочленах, мы имеем:

$$N[u^2-1\equiv y^2 \bmod p]=p-1.$$

Поэтому в рассматриваемом случае $p\equiv -1 \bmod 4$ мы также имеем:

$$N[x^4-1\equiv y^2 \bmod p]=p-1. \tag{2а}$$

Тем самым, согласно (1), получается:

$$\Phi_p=0. \tag{3а}$$

Поэтому для исходного многочлена третьей степени имеет место:

$$N[x(x^2-1)\equiv y^2 \bmod p]=p. \tag{4а}$$

б) $p\equiv 1 \bmod 4$.

Этот случай труднее, но зато и интереснее. Подлежащее определению количество решений может быть выражено, аналогично тому как мы получили (1), в форме

$$N[x^4-1\equiv y^2 \bmod p]=\sum_{\substack{x,\,y \bmod p\\ x^4-1\equiv y^2 \bmod p}} 1=$$

$$=\sum_{\substack{u,\,v \bmod p\\ u-1\equiv v \bmod p}} N_u[x^4\equiv u \bmod p]\cdot N_v[y^2\equiv v \bmod p].$$

Здесь $N_v[y^2\equiv v \bmod p]=1+\left(\frac{v}{p}\right)$. Нам нужно еще соответствующее представление для $N_u[x^4\equiv u \bmod p]$. Для этого мы должны ввести по аналогии с квадратичным характером $\psi_p(a)=\left(\frac{a}{p}\right)$ биквадратичный характер $\chi_p(a)$. Это легко сделать по образцу § 6, п. 4. Не развивая систематической теории биквадратичных вычетов, мы ограничимся здесь только небольшим количеством необходимых для нашей цели фактов.

Представим классы вычетов $a \bmod p$, взаимно простые с модулем, с помощью первообразного корня $w \bmod p$ в форме

$$a\equiv w^\alpha \bmod p \quad (\alpha \bmod p-1)$$

и определим:

$$\chi_p(a)=i^\alpha,$$

где i есть первообразный четвертый корень из 1. В рассматриваемом случае $p\equiv 1 \bmod 4$ это определение однозначно, т. е. не зависит от выбора показателя α в его классе вычетов по $\bmod p-1$. Оно дает нам зависящую только от класса вычетов $a \bmod p$

мультипликативную функцию $\chi_p(a)$ со свойством $\chi_p(a)^4 = 1$, т. е. биквадратичный характер по $\bmod p$. Мы снова дополним наше определение, положив

$$\chi_p(a) = 0 \quad \text{для } a \equiv 0 \bmod p$$

с сохранением мультипликативности. Для того чтобы $a \not\equiv 0 \bmod p$ было биквадратичным вычетом по $\bmod p$, т. е. чтобы было разрешимо сравнение $x^4 \equiv a \bmod p$, необходимо и достаточно, вследствие того что мы можем записать

$$x \equiv w^{\xi} \bmod p \quad (\xi \bmod p - 1),$$

чтобы было разрешимо сравнение для показателей

$$4\xi \equiv \alpha \bmod p - 1.$$

Так как $p \equiv 1 \bmod 4$, то, согласно V, п. 3, § 4, это имеет место тогда и только тогда, когда $\alpha \equiv 0 \bmod 4$, т. е. когда $\chi_p(a) = 1$, и в этом случае существует точно четыре решения $\xi \bmod p - 1$, а потому и точно четыре решения $x \bmod p$. Отсюда вытекает формула

$$N[x^4 \equiv a \bmod p] = 1 + \chi_p(a) + \chi_p^2(a) + \chi_p^3(a).$$

В самом деле, для $a \not\equiv 0 \bmod p$ стоящая справа сумма равна 4 или 0 в зависимости от того, равен или не равен 1 четвертый корень из 1 $\chi_p(a)$, а для $a \equiv 0 \bmod p$ обе стороны равенства равны 1. Для биквадратичного характера $\chi_p(a)$ также имеет место формула сложения

$$\sum_{a \bmod p} \chi_p(a) = 0.$$

Действительно, четырем возможным значениям характера $\chi_p(a) = 1, i, i^2, i^3$ соответствует в системе классов вычетов $a \bmod p$ одно и то же количество, а именно, $(p-1)/4$ чисел, ибо четыре значения показателя $\alpha \equiv 0, 1, 2, 3 \bmod 4$ встречаются одинаково часто, и $1 + i + i^2 + i^3 = 0$. Заметим еще, что

$$\chi_p^2(a) \equiv \psi_p(a) = \left(\frac{a}{p}\right),$$

т. е. $\chi_p^2(a)$ есть квадратичный характер по $\bmod p$, и

$$\chi_p^3(a) = \chi_p^{-1}(a) = \overline{\chi}_p(a),$$

т. е. $\chi_p^3(a)$ комплексно сопряжено с $\chi_p(a)$; при этом запись $\chi_p^{-1}(a)$ можно, строго говоря, применять только для $a \not\equiv 0 \bmod p$.

Согласно всему сказанному, приведенную выше формулу для количества решений можно дальше преобразовать следующим

образом:

$$N[x^4-1\equiv y^2 \bmod p]=$$
$$=\sum_{\substack{u,v \bmod p\\ u-1\equiv v \bmod p}}(1+\chi_p(u)+\chi_p^2(u)+\chi_p^3(u))(1+\psi_p(v))=$$
$$=\sum_{u \bmod p}(1+\psi_p(u)+\chi_p(u)+\bar{\chi}_p(u))(1+\psi_p(u-1))=$$
$$=p+\sum_{u \bmod p}\psi_p(u(u-1))+$$
$$+\sum_{u \bmod p}\chi_p(u)\psi_p(u-1)+\sum_{u \bmod p}\bar{\chi}_p(u)\psi_p(u-1).$$

Из трех фигурирующих десь наряду с главным членом p дополнительных членов для первого, согласно III п. 4, получается

$$\sum_{u \bmod p}\psi_p(u(u-1))=-1,$$

в то время как два последних

$$\pi=\sum_{u \bmod p}\chi_p(u)\psi_p(u-1),\quad \bar{\pi}=\sum_{u \bmod p}\bar{\chi}_p(u)\psi_p(u-1)$$

комплексно сопряжены между собой. Если использовать эти сокращенные обозначения, то формула для количества решений принимает вид:

$$N[x^4-1\equiv y^2 \bmod p]=p-1+\pi+\bar{\pi}. \tag{2б}$$

Таким образом, согласно (1),

$$\Phi_p=\pi+\bar{\pi} \tag{3б}$$

и потому

$$N[x(x^2-1)\equiv y^2 \bmod p]=p+\pi+\bar{\pi}. \tag{4б}$$

В этом результате для рассматриваемого случая $p\equiv 1 \bmod 4$ в качестве ошибки Φ_p фигурирует, вместо 0 в соответствующем результате для $p\equiv -1 \bmod 4$, удвоенная вещественная часть комплексного числа

$$\pi=\sum_{u \bmod p}\chi_p(u)\psi_p(u-1), \tag{5}$$

которую нам и остается определить. В ее определении и заключается трудность нашего исследования, но также и его привлекательность. Мы покажем, что

$$|\pi|^2=\pi\bar{\pi}=p, \tag{6}$$

откуда следует тогда

$$|\Phi_p|\leqslant 2\sqrt{p}. \tag{7}$$

Доказательство утверждения (6) проводится по образцу доказательства соответствующего факта (2) из § 8, п. 2 для рассматриваемой там гауссовой суммы τ. Прежде всего, в сумме (5) суммирование может быть ограничено системой классов вычетов $u \not\equiv 0 \bmod p$, так как $\chi_p(u) = 0$ при $u \equiv 0 \bmod p$. Посредством формального перемножения обеих комплексно сопряженных сумм π, $\bar{\pi}$, для $|\pi|^2 = \pi\bar{\pi}$ получается представление в виде двойной суммы

$$|\pi|^2 = \sum_{u,\ t \not\equiv 0 \bmod p} \chi_p(u)\,\bar{\chi}_p(v)\,\psi_p(u-1)\,\psi_p(v-1).$$

Если для каждого $u \bmod p$ произвести замену $v \equiv ut \bmod p$ индекса суммирования, однозначно обратимую в виде $t \equiv u^{-1}v \bmod p$, то получится

$$|\pi|^2 = \sum_{u,\ t \not\equiv 0 \bmod p} \chi_p(u)\,\bar{\chi}_p(u)\,\bar{\chi}_p(t)\,\psi_p((u-1)(ut-1)).$$

Здесь $\chi_p(u)\,\bar{\chi}_p(u) = 1$. Если, далее, вынести из аргумента функции ψ_p за скобку множитель t и заметить, что

$$\bar{\chi}_p\psi_p = \chi_p^{-1}\chi_p^2 = \chi_p,$$

то будет следовать

$$\begin{aligned}|\pi|^2 &= \sum_{u,\ \not\equiv 0 \bmod p} \chi_p(t)\,\psi_p((u-1)(u-t^{-1})) = \\ &= \sum_{t \not\equiv 0 \bmod p} \chi_p(t)\left[\sum_{u \bmod p} \psi_p((u-1)(u-t^{-1})) - \psi_p(t^{-1})\right] = \\ &= \sum_{t \not\equiv 0 \bmod p} \chi_p(t) \sum_{u \bmod p} \psi_p((u-1)(u-t^{-1})),\end{aligned}$$

причем последнее преобразование сделано на основании того, что $\chi_p(t)\,\psi_p(t^{-1}) = \chi_p(t)\,\chi_p^{-2}(t) = \bar{\chi}_p(t)$ и $\sum_{t \not\equiv 0 \bmod p} \bar{\chi}_p(t) = 0$. Согласно результату III, п. 4 о квадратных многочленах,

$$\sum_{u \bmod p} \psi_p((u-1)(u-t^{-1})) = \left\{\begin{array}{ll} p-1 & \text{для } t \equiv 1 \bmod p \\ -1 & \text{для } t \not\equiv 1 \bmod p \end{array}\right\}.$$

Отсюда получается

$$\begin{aligned}|\pi|^2 &= \sum_{t \not\equiv 0,\ 1 \bmod p} \chi_p(t)\,(-1) + \chi_p(1)\,(p-1) = \\ &= -\sum_{t \not\equiv 0 \bmod p} \chi_p(t) + p = p,\end{aligned}$$

что и требовалось доказать.

Доказанная тем самым оценка (7) подтверждает, согласно (2б), (4б), общие высказывания из (3_1), п. 3 для обоих специальных многочленов $x(x^2-1)$ и x^4-1 третьей и четвертой степени также и в случае $p \equiv 1 \bmod 4$; в случае $p \equiv -1 \bmod 4$ это

тривиальным образом вытекало уже из (2а), (4а). В то время как для $p \equiv -1 \bmod 4$ ошибка, согласно (3а), равна 0, для $p \equiv 1 \bmod 4$, наоборот, в первый раз появляется ошибка, отличная, согласно (3б), (6), от 0. Потом мы еще займемся подробнее ее интересной арифметической структурой. При этом мы узнаем, в частности, правда без доказательства, что оценку (7) нельзя улучшить, так что для количеств решений (2б), (4б) имеет место случайное распределение в смысле сказанного в п. 3.

7. Применение к трехчленным последовательностям. В случае $n=3$ общая формула (5) п. 2 для количества последовательностей редуцируется, если принять во внимание высказывания (8) п. 1 и III, п. 4 о многочленах первой и второй степени, к виду

$$N(\varepsilon_1, \varepsilon_2, \varepsilon_3 \mid p) = \frac{p}{8} - \frac{\varepsilon_1\varepsilon_2 + \varepsilon_1\varepsilon_3 + \varepsilon_2\varepsilon_3}{8} + \frac{\varepsilon_1\varepsilon_2\varepsilon_3}{8}\Phi_p, \tag{1}$$

где Φ_p имеет значение из п. 6

а) $p \equiv -1 \bmod 4$.

Согласно (3а) п. 6, в этом случае $\Phi_p = 0$. Поэтому количество последовательностей выражается здесь аналогичной формуле (1) из п. 5 формулой

$$N(\varepsilon_1, \varepsilon_2, \varepsilon_3 \mid p) = \frac{p}{8} - \frac{\varepsilon_1\varepsilon_2 + \varepsilon_1\varepsilon_3 + \varepsilon_2\varepsilon_3}{8}. \tag{1а}$$

Мы снова хотим, аналогично (2) п. 5, определить также первоначальное количество последовательностей $N_0(\varepsilon_1, \varepsilon_2, \varepsilon_3 \mid p)$, когда не принимаются в расчет граничные тройки $(-2, -1, 0)$, $(-1, 0, 1)$, $(0, 1, 2)$. Согласно (2), (3) п. 2 и обоим дополнениям к закону взаимности, мы получаем

$$\begin{aligned}
&N(\varepsilon_1, \varepsilon_2, \varepsilon_3 \mid p) - N_0(\varepsilon_1, \varepsilon_2, \varepsilon_3 \mid p) = \\
&= \frac{1}{8}\left(1+\varepsilon_1\left(\frac{-2}{p}\right)\right)\left(1+\varepsilon_2\left(\frac{-1}{p}\right)\right) + \\
&\quad + \frac{1}{8}\left(1+\varepsilon_1\left(\frac{-1}{p}\right)\right)\left(1+\varepsilon_3\left(\frac{1}{p}\right)\right) + \\
&\quad + \frac{1}{8}\left(1+\varepsilon_2\left(\frac{1}{p}\right)\right)\left(1+\varepsilon_3\left(\frac{2}{p}\right)\right) = \\
&= \frac{1}{8}\left(1-\varepsilon_1(-1)^{\frac{p+1}{4}}\right)(1-\varepsilon_2) + \\
&\quad + \frac{1}{8}(1-\varepsilon_1)(1+\varepsilon_3) + \frac{1}{8}(1+\varepsilon_2)\left(1+\varepsilon\right)(-1)^{\frac{p+1}{4}}.
\end{aligned}$$

Поэтому, как можно установить легким вычислением, принимая во внимание (1а), для $p \equiv -1 \bmod 8$

$$N_0(\varepsilon_1, \varepsilon_2, \varepsilon_3 \mid p) = \frac{p+1}{8} - \frac{(1-\varepsilon_1)(1-\varepsilon_2) + (1+\varepsilon_2)(1+\varepsilon_3)}{4} \tag{2а$_1$}$$

и для $p \equiv -5 \bmod 8$

$$N_0(\varepsilon_1, \varepsilon_2, \varepsilon_3 \mid p) = \frac{p-3}{8} \quad \text{(независимо от } \varepsilon_1, \varepsilon_2, \varepsilon_3\text{)}. \qquad (2a_2)$$

Отсюда для отдельных значений получается следующая таблица:

ε_1	ε_2	ε_3	$N_0(\varepsilon_1, \varepsilon_2, \varepsilon_3 \mid p \equiv -1 \bmod 8)$	$N_0(\varepsilon_1, \varepsilon_2, \varepsilon_3 \mid p \equiv -5 \bmod 8)$
$+1$	$+1$	$+1$	$\frac{p-7}{8}$	$\frac{p-3}{8}$
$+1$	$+1$	-1	$\frac{p+1}{8}$	
$+1$	-1	$+1$	$\frac{p+1}{8}$	
$+1$	-1	-1	$\frac{p+1}{8}$	
-1	$+1$	$+1$	$\frac{p-7}{8}$	
-1	$+1$	-1	$\frac{p+1}{8}$	
-1	-1	$+1$	$\frac{p-7}{8}$	
-1	-1	-1	$\frac{p-7}{8}$	

б) $p \equiv 1 \bmod 4$.

В этом случае, согласно (3б) п. 6, $\Phi_p = \pi + \bar{\pi}$ с приведенным там значением π, которое мы еще поясним подробнее в п. 8. Поэтому для количества последовательностей $N(\varepsilon_1, \varepsilon_2, \varepsilon_3 \mid p)$ из (1) получается формула, содержащая $\pi + \bar{\pi}$, которая также может служить и, наоборот, для определения вещественной части числа π посредством подсчета последовательностей (например, с $\varepsilon_1 = 1$, $\varepsilon_2 = 1$, $\varepsilon_3 = 1$), что представляет интерес в связи с тем, что будет изложено в п. 8. Из установленной в (7) п. 6 оценки $|\Phi_p| \leqslant 2\sqrt{p}$ получается менее точная оценка

$$\left| N(\varepsilon_1, \varepsilon_2, \varepsilon_3 \mid p) - \frac{p}{8} \right| \leqslant \frac{3+2\sqrt{p}}{8} \left(< \frac{2+\sqrt{3}}{8}\sqrt{p} \right) \qquad (1б)$$

для количества последовательностей. Отсюда, согласно (4) п. 2, следует оценка

$$\left| N_0(\varepsilon_1, \varepsilon_2, \varepsilon_3 \mid p) - \frac{p}{8} \right| \leqslant \frac{15+2\sqrt{p}}{8} \left(< \frac{2+5\sqrt{3}}{8}\sqrt{p} \right) \qquad (2б)$$

для количества последовательностей в первоначальном смысле. Эту оценку можно несколько уточнить, если, аналогично (2a), рассматривать отдельные системы $\varepsilon_1, \varepsilon_2, \varepsilon_3$ и различать значения $p \equiv 1$ или $\equiv 5 \bmod 8$. Однако мы не будем вдаваться в это подробнее.

В смысле изложенного в п. 3 настоящие результаты означают, что для трехчленных последовательностей выполняется статистический закон рассеивания и при этом с ошибкой, которая в случае $p \equiv -1 \bmod 4$, как и для двучленных последовательностей, имеет порядок возрастания $O(1)$ (т. е. ограничена), а в случае $p \equiv 1 \bmod 4$ имеет порядок возрастания, не больший чем $O(\sqrt{p})$, а как мы увидим в п. 8, также и не меньший порядок. Поэтому в случае $p \equiv 1 \bmod 4$ для трехчленных последовательностей имеет место случайное распределение.

8. Разложение простых чисел $p \equiv 1 \bmod 4$ на сумму двух квадратов. В соответствии с результатами из п. 6, в случае $p \equiv 1 \bmod 4$ больший интерес представляют комплексно сопряженные числа

$$\pi = \sum_{u \bmod p} \chi_p(u)\,\psi_p(u-1), \quad \bar{\pi} = \sum_{u \bmod p} \bar{\chi}_p(u)\,\psi_p(u-1), \tag{1}$$

где ψ_p есть квадратичный, а χ_p, $\bar{\chi}_p$ — пара комплексно сопряженных биквадратичных характеров по $\bmod p$. Эти два числа принадлежат полю $\mathsf{P}(i)$ четвертых корней из 1 и притом, в силу представления (1), лежат в области целостности $\Gamma[i]$ так называемых *целых комплексных чисел*. Поэтому они обладают представлениями вида

$$\pi = a + bi, \qquad \bar{\pi} = a - bi$$

с целыми рациональными числами a, b. При этом

$$\Phi_p = \pi + \bar{\pi} = 2a \tag{2}$$

есть ошибка из п. 6, 7, и, согласно (6) п. 6, имеет место

$$p = \pi\bar{\pi} = a^2 + b^2. \tag{3}$$

Это последнее соотношение дает нам, безотносительно к рассматриваемым в этом параграфе вопросам распределения, следующий важный результат:

IV. *Каждое простое число $p \equiv 1 \bmod 4$ обладает представлением $p = a^2 + b^2$ в виде суммы двух квадратов.*

То, что такое представление возможно только для простых чисел вида $p \equiv 1 \bmod 4$, если не считать простого числа $p = 2 = 1^2 + 1^2$, ясно из первого дополнения к квадратичному закону взаимности, как это уже было отмечено в § 7, п. 2.

Способ, которым мы получили здесь высказывание IV, подобен тому способу, которым мы доказали в XIII, п. 11, § 4, не прибегая к теории квадратичных вычетов, разрешимость сравнения $x^2 \equiv -1 \bmod p$ для $p \equiv 1 \bmod 4$; именно, мы сконструировали там явное решение в виде $x \equiv ((p-1)/2)! \bmod p$. Здесь мы также конструируем основание одного из квадратов, а именно, согласно (2) и, принимая во внимание значение Φ_p из п. 6, в следующей форме:

$$a = \frac{1}{2}\Phi_p = \frac{1}{2}\sum_{x \bmod p}\left(\frac{x}{p}\right)\left(\frac{x^2-1}{p}\right). \tag{4}$$

По этой формуле — или, как уже сказано в п. 7, также и по имеющейся там формуле (1) для трехчленных последовательностей — можно при заданном простом числе $p \equiv 1 \bmod 4$ вычислить a.

Для того, чтобы углубить полученный только что факт, мы несколько забежим вперед и приведем некоторые результаты, доказываемые нами только в четвертой главе. Там мы подробно займемся арифметикой общих квадратичных полей. При этом для специального поля $\mathsf{P}(i)$ и содержащейся в нем области целостности $\Gamma[i]$ в § 16, п. 6, XIXA получится, что каждое целое комплексное число обладает разложением на единичные множители ± 1, $\pm i$ и некоторое количество *комплексных простых чисел* π (т. е. чисел из $\Gamma[i]$, имеющих только тривиальные разложения), причем с точностью до порядка следования простых сомножителей и их выбора среди ассоциированных $\pm\pi$, $\pm i\pi$ это разложение однозначно. Для простых чисел $p \equiv 1 \bmod 4$ из Γ, рассматриваемых как числа из $\Gamma[i]$, это разложение как раз окажется имеющим вид (3). Тем самым, оба множителя π, $\bar{\pi}$ из (3) определяются для данного p однозначно с точностью до подстановок $\pi \to \pm\pi$, $\pm i\pi$ и замены π на $\bar{\pi}$; в этом и заключается результат, который нам здесь понадобится. Поэтому для данного p оба основания квадратов a, b в (3) определяются однозначно с точностью до порядка следования и знаков, что мы видим из следующего рассмотрения всех возможных случаев:

$$\begin{aligned} \pi &= a + bi, & \bar{\pi} &= a - bi, \\ -\pi &= -a - bi, & -\bar{\pi} &= -a + bi, \\ i\pi &= -b + ai, & -i\bar{\pi} &= -b - ai, \\ -i\pi &= b - ai, & i\bar{\pi} &= b + ai. \end{aligned}$$

Так как из двух оснований квадратов a, b одно обязательно четно, а другое нечетно, то порядок расположения можно однозначно нормировать требованием, чтобы a было нечетным. Знак

числа a можно однозначно нормировать требованием $a > 0$, или также требованием $a \equiv 1 \bmod 4$, или, вообще, требованием вида

$$a \equiv \varepsilon_p \bmod 4 \tag{5}$$

с некоторой заданной как функция от p единицей $\varepsilon_p = \pm 1$. Наконец, посредством требования $b > 0$ можно однозначно нормировать и знак числа b, однако нам это здесь не нужно, так как мы будем иметь дело только с числом a.

Итак, посредством требования (5) разложение вида (3) при заданных $p \equiv 1 \bmod 4$ и $\varepsilon_p = \pm 1$ определяется однозначно с точностью до знака числа b (и в соответствии с этим с точностью до различия между π и $\bar{\pi}$). Тогда возникает вопрос, является ли разложение (3), получающееся из теории распределения сообразно с (4), как раз так нормированным разложением. Мы покажем, что при подходящем выборе нормирующей единицы ε_p это действительно так. Все сводится к тому, чтобы установить, что выражение $\Phi_p/2$, стоящее в правой части (4), нечетно, и к тому, чтобы определить его значение ε_p по $\bmod 4$ как функцию от p.

Для того, чтобы в выражении

$$\frac{1}{2}\Phi_p = \frac{1}{2} \sum_{x \bmod p} \left(\frac{x}{p}\right)\left(\frac{x^2-1}{p}\right)$$

освободиться от знаменателя 2, представляющего для нашего исследования неудобство, мы при суммировании отбросим класс вычетов $x \equiv 0 \bmod p$, который вносит в сумму слагаемое, равное 0, и объединим каждые два противоположных класса вычетов $\pm x \bmod p$, которые, вследствие $\left(\frac{-1}{p}\right) = 1$, вносят в сумму равные слагаемые. Тогда получится свободное от знаменателя представление

$$\frac{1}{2}\Phi_p = \sum_{\pm x \bmod p} \left(\frac{x}{p}\right)\left(\frac{x^2-1}{p}\right),$$

в котором суммирование распространено только на полусистему по $\bmod p$ (см. § 6, п. 6), на что указывает обозначение $\pm x \bmod p$ под знаком суммы. Но, согласно высказыванию II, п. 1, в случае $p \equiv 1 \bmod 4$ уже в каждой полусистеме по $\bmod p$ имеется одинаковое количество квадратичных вычетов и невычетов, и потому имеет место усиление утверждения (2) п. 1:

$$\sum_{\pm x \bmod p} \left(\frac{x}{p}\right) = 0.$$

Посредством вычитания этого соотношения получаем

$$\frac{1}{2}\Phi_p = \sum_{\pm x \bmod p} \left(\frac{x}{p}\right)\left[\left(\frac{x^2-1}{p}\right) - 1\right].$$

Так как при $\pm x \not\equiv 1 \bmod p$ вторые множители в этой сумме $\equiv 0 \bmod 2$, мы можем для определения значения этой суммы по $\bmod 4$ привести первые множители к наименьшим вычетам по $\bmod 2$, т. е. заменить их на 1; в члене с $\pm x \equiv 1 \bmod p$ первый множитель уже равен 1. Поэтому

$$\frac{1}{2}\Phi_p \equiv \sum_{x \bmod p} \left[\left(\frac{x^2-1}{p}\right) - 1\right] \bmod 4.$$

Теперь, согласно результату III, п. 4 для квадратных многочленов,

$$1 + 2 \sum_{\pm x \bmod p} \left(\frac{x^2-1}{p}\right) = \sum_{x \bmod p} \left(\frac{x^2-1}{p}\right) = -1,$$

и потому также

$$\sum_{\pm x \bmod p} \left(\frac{x^2-1}{p}\right) = -1.$$

Таким образом, мы получаем:

$$\frac{1}{2}\Phi_p \equiv -1 - \frac{p-1}{2} \equiv -\frac{p+1}{2} \equiv \left\{\begin{array}{ll} -1 \bmod 4 & \text{для } p \equiv 1 \bmod 8 \\ 1 \bmod 4 & \text{для } p \equiv 5 \bmod 8 \end{array}\right\},$$

что с помощью второго дополнения к закону взаимности можно выразить проще:

$$\frac{1}{2}\Phi_p \equiv -\left(\frac{2}{p}\right) \bmod 4.$$

Этим доказано, что построенное в (4) число $a = \Phi_p/2$ действительно нечетно и удовлетворяет нормирующему условию (5) с единицей $\varepsilon_p = -\left(\frac{2}{p}\right)$. Поэтому в дополнение к IV мы можем установить следующий результат:

V. *Для* $p \equiv 1 \bmod 4$ *сумма*

$$a = \frac{1}{2}\Phi_p = \frac{1}{2}\sum_{x \bmod p}\left(\frac{x}{p}\right)\left(\frac{x^2-1}{p}\right) = \sum_{\pm x \bmod p}\left(\frac{x}{p}\right)\left(\frac{x^2-1}{p}\right)$$

дает основание a *нечетного квадрата в разложении* $p = a^2 + b^2$ *с нормированием* $a \equiv -\left(\frac{2}{p}\right) \bmod 4$, *т. е.*

$$a \equiv \left\{\begin{array}{ll} -1 \bmod 4 & \textit{для } p \equiv 1 \bmod 8 \\ 1 \bmod 4 & \textit{для } p \equiv 5 \bmod 8 \end{array}\right\}.$$

В (29) п. 5, § 18 мы укажем в дополнение к этому способ определения еще не установленного знака у основания b четного квадрата.

Заметим, между прочим, что в случае $p \equiv -1 \bmod 4$, когда $\left(\frac{-x}{p}\right) = -\left(\frac{x}{p}\right)$, редукция к суммированию по полусистеме по $\bmod p$ в выражении для Φ_p немедленно дает факт $\Phi_p = 0$, который мы доказали в (3а) п. 6, по принятой там системе изложения, несколько более сложным путем.

Обратимся, наконец, к высказанному в конце п. 6 утверждению, что оценку $|\Phi_p| \leqslant 2\sqrt{p}$ нельзя улучшить. Методами аналитической теории чисел, о которой мы дадим представление в третьей главе (впрочем, недостаточное для разрешения стоящей здесь задачи), Гекке показал, что существует бесконечное множество таких простых чисел $p \equiv 1 \bmod 4$, что отношение b^2/a^2 квадратов их нормированных разложений $p = a^2 + b^2$ принадлежит любому наперед заданному положительному интервалу. Если, в частности, выбрать интервал вида $0 < b^2/a^2 < \varepsilon$, то все простые числа из этого бесконечного множества будут обладать свойством

$$p = a^2 + b^2 < (1 + \varepsilon)\, a^2,$$

т. е. для них будет иметь место соотношение

$$|\Phi_p| = 2|a| > \frac{1}{\sqrt{1+\varepsilon}}\, 2\sqrt{p}.$$

Так как при достаточно малом ε множитель при $2\sqrt{p}$ можно сделать сколь угодно близким к 1, то в силу этой теоремы Гекке оценку $|\Phi_p| \leqslant 2\sqrt{p}$ действительно нельзя улучшить, что относится как к порядку возрастания $O(\sqrt{p})$, так и к константе 2.

9. Разложение простых чисел $p \equiv 1 \bmod 3$ на сумму квадрата и утроенного квадрата. Кроме изложенного в п. 6 и 8 случая сравнения $x(x^2 - 1) \equiv y^2 \bmod p$, которое в нашей постановке вопроса после преобразования оказалось эквивалентным сравнению

$$x^4 - 1 \equiv y^2 \bmod p,$$

с помощью элементарных методов может быть изложен еще один случай, а именно, случай сравнения

$$x^3 - 1 \equiv y^2 \bmod p.$$

Мы выведем для этого последнего сравнения факты, совершенно аналогичные тем, что были доказаны в п. 6 и 8 для вышеназванного сравнения. Вследствие далеко идущей аналогии обоих случаев мы можем быть несколько более кратки.

Рассмотрим ошибку

$$\Phi_p = N[x^3 - 1 \equiv y^2 \bmod p] - p = \sum_{x \bmod p} \left(\frac{x^3-1}{d}\right).$$

Сначала мы рассмотрим случай

$$p \equiv -1 \bmod 3,$$

который здесь оказывается тривиальным. В этом случае порядок $p-1$ группы классов вычетов по $\bmod p$, взаимно простых с модулем, не делится на 3. Поэтому сравнение $x^3 \equiv a \bmod p$ для каждого $a \bmod p$ имеет точно одно решение. Вследствие этого здесь имеет место

$$N[x^3 - 1 \equiv y^2 \bmod p] = N[u - 1 \equiv y^2 \bmod p] =$$
$$= \sum_{y \bmod p} N_y[u - 1 \equiv y^2 \bmod p] = \sum_{y \bmod p} 1 = p$$

и, таким образом,

$$\Phi_p = 0.$$

Предположим теперь, что

$$p \equiv 1 \bmod 3.$$

Тогда порядок $p-1$ группы классов вычетов по $\bmod p$, взаимно простых с модулем, делится на 3. В соответствии с этим существует кубический характер по $\bmod p$, определяемый посредством

$$\chi_p(a) = \rho^\alpha \quad \text{для} \quad a \equiv w^\alpha \bmod p \quad (\alpha \bmod p - 1),$$

где w есть первообразный корень по $\bmod p$ и ρ — первообразный корень третьей степени из 1. Если положить еще

$$\chi_p(a) = 0 \quad \text{для} \quad a \equiv 0 \bmod p,$$

то снова имеет место

$$N[x^3 \equiv a \bmod p] = 1 + \chi_p(a) + \chi_p^2(a),$$

а также и

$$\sum_{a \bmod p} \chi_p(a) = 0,$$

причем здесь использовано то, что $1 + \rho + \rho^2 = 0$. Характер $\chi_p^2 = \chi_p^{-1} = \bar{\chi}_p$ является комплексно сопряженным с χ_p. Если через

$$\psi_p(a) = \left(\frac{a}{p}\right)$$

обозначить квадратичный характер по $\bmod p$, то

$$\chi_p(a)\,\psi_p(a) = (-\rho)^\alpha \quad \text{для} \quad a \equiv w^\alpha \bmod p \quad (\alpha \bmod p - 1);$$

таким образом, $\chi_p\psi_p$ есть бикубический характер по $\bmod p$, соответствующий первообразному шестому корню $-\rho$ из 1, а $\bar{\chi}_p\psi_p$ —

комплексно сопряженный с ним характер. Так как $1-\rho+\rho^2-\rho^3+\rho^4-\rho^5=0$, мы получаем, что имеет место также равенство

$$\sum_{a \bmod p} \chi_p(a)\,\psi_p(a)=0.$$

В силу всего сказанного мы имеем

$$N[x^3-1\equiv y^2 \bmod p]=$$

$$=\sum_{\substack{u,\,v \bmod p\\ u-1\equiv v \bmod p}} (1+\chi_p(u)+\chi_p^2(u))(1+\psi_p(v))=p+\pi+\bar{\pi},$$

т. е.

$$\Phi_p=\pi+\bar{\pi}$$

с

$$\pi=\sum_{u \bmod p}\chi_p(u)\,\psi_p(u-1),\quad \bar{\pi}=\sum_{u \bmod p}\bar{\chi}_p(u)\,\psi_p(u-1).$$

Как мы сейчас покажем, для определенных таким образом комплексно сопряженных чисел π, $\bar{\pi}$ снова имеет место равенство

$$|\pi|^2=\pi\bar{\pi}=p,$$

и, таким образом,

$$|\Phi_p|\leqslant 2\sqrt{p}.$$

Аналогично рассмотренному в п. 6 случаю мы получаем

$$|\pi|^2=\sum_{u,\,v\not\equiv 0 \bmod p}\chi_p(u)\,\bar{\chi}_p(v)\,\psi_p(u-1)\,\psi_p(v-1)=$$

$$=\sum_{u,\,t\not\equiv 0 \bmod p}\chi_p(u)\,\bar{\chi}_p(u)\,\bar{\chi}_p(t)\,\psi_p((u-1)(ut-1))=$$

$$=\sum_{u,\,t\not\equiv 0 \bmod p}\bar{\chi}_p(t)\,\psi_p(t)\,\psi_p((u-1)(u-t^{-1}))=$$

$$=\sum_{t\not\equiv 0 \bmod p}\bar{\chi}_p(t)\,\psi_p(t)\Big[\sum_{u \bmod p}\psi_p((u-1)(u-t^{-1}))-\psi_p(t^{-1})\Big]=$$

$$=\sum_{t\not\equiv 0 \bmod p}\bar{\chi}_p(t)\,\psi_p(t)\sum_{u \bmod p}\psi_p((u-1)(u-t^{-1}))=$$

$$=\sum_{t\not\equiv 0,\,1 \bmod p}\bar{\chi}_p(t)\,\psi_p(t)\,(-1)+\bar{\chi}_p(1)\,\psi_p(1)\,(p-1)=$$

$$=p-\sum_{t\not\equiv 0 \bmod p}\bar{\chi}_p(t)\,\psi_p(t)=p.$$

Оба комплексно сопряженных числа π, $\bar{\pi}$ принадлежат полю $\mathbf{P}(\rho)$ корней третьей степени из 1, и притом они лежат в области

целостности $\Gamma[\rho]$ и потому обладают представлениями

$$\pi = a + b\rho, \quad \bar{\pi} = a + b\rho^2$$

с целыми рациональными a, b. При этом

$$\Phi_p = \pi + \bar{\pi} = 2a - b$$

и

$$p = \pi\bar{\pi} = a^2 - ab + b^2.$$

Как будет следовать в XIXA, п. 6 § 16, из арифметики области целостности $\Gamma[\rho]$, разложение последнего вида определяется заданием p однозначно с точностью до замены π одним из шести ассоциированных с ним чисел $\pm\pi$, $\pm\rho\pi$, $\pm\rho^2\pi$ и до различия между π и $\bar{\pi}$. Из

$$\pi = a + b\rho$$
$$\rho\pi = -b + (a-b)\rho$$
$$\rho^2\pi = (b-a) - a\rho,$$

а также из того, что a и b не могут оба быть четными, мы усматриваем, что выбор $\pm\pi$ среди трех пар ассоциированных чисел, отличающихся друг от друга только знаком, может быть определен требованием

$$b \equiv 0 \bmod 2.$$

Для конструируемого здесь разложения это требование выполняется. Именно,

$$2a - b = \Phi_p = \sum_{x \bmod p} \left(\frac{x^3-1}{p}\right) = \sum_{\substack{x \bmod p \\ x^3 \not\equiv 1 \bmod p}} 1 \equiv p - 3 \equiv 0 \bmod 2,$$

так как сравнение $x^3 \equiv 1 \bmod p$ имеет точно три решения $(1, w^{(p-1)/3}, w^{2(p-1)/3} \bmod p)$. Если ввести представления

$$\rho = \frac{-1+\sqrt{-3}}{2}, \quad \rho^2 = \frac{-1-\sqrt{-3}}{2}$$

для первообразных корней третьей степени из 1, то написанные выше формулы примут вид:

$$\pi = A + B\sqrt{-3}, \quad \bar{\pi} = A - B\sqrt{-3},$$
$$\Phi_p = \pi + \bar{\pi} = 2A,$$
$$p = \pi\bar{\pi} = A^2 + 3B^2$$

с целыми рациональными A, B, для которых получается

$$A = a - \frac{1}{2}b, \quad B = \frac{1}{2}b.$$

При разложении такого вида, когда оба множителя π, $\bar{\pi}$ принадлежат к меньшей чем $\Gamma[\rho]$ области целостности $\Gamma[\sqrt{-3}]$, остаются тогда неопределенными только знаки чисел A, B, что соответствует тому, что вместо π можно выбрать $-\pi$ или $\bar{\pi}$. Так как A не делится на 3, то его знак можно однозначно нормировать посредством требования

$$A \equiv \varepsilon_p \bmod 3$$

с некоторой, заданной как функция от p, единицей $\varepsilon_p = \pm 1$, а знак числа B можно, например, нормировать условием $B > 0$, что нам, однако, не понадобится.

Чтобы определить нормирующую единицу ε_p для конструируемого здесь разложения, мы выясним значение Φ_p по $\bmod 3$. Для этого мы должны поступить несколько иначе, чем в п. 6, а именно, привлечь еще один факт из арифметики в $\Gamma[\rho]$. Число $1-\rho$ из $\Gamma[\rho]$ обладает тем свойством, что для комплексно сопряженного с ним числа $1-\rho^2$ имеет место

$$1-\rho^2 = -\rho^2(1-\rho) \cong 1-\rho,$$

т. е. $1-\rho^2$ ассоциировано с $1-\rho$. Поэтому

$$3 = (1-\rho)(1-\rho^2) \cong (1-\rho)^2.$$

Если мы теперь будем знать, что для двух целых рациональных чисел a, b выполняется сравнение $a \equiv b \bmod (1-\rho)$ в $\Gamma[\rho]$, то отсюда посредством вычитания и возведения в квадрат будет следовать $(a-b)^2 \equiv 0 \bmod 3$ и потому также $a-b \equiv 0 \bmod 3$, т. е. $a \equiv b \bmod 3$. Поэтому достаточно выяснить значение Φ_p по $\bmod (1-\rho)$. Мы имеем

$$\pi = \sum_{u \bmod p} \chi_p(u)\,\psi_p(u-1) \equiv \sum_{u \not\equiv 0 \bmod p} \psi_p(u-1) \bmod (1-\rho),$$

и при этом здесь

$$\sum_{u \not\equiv 0 \bmod p} \psi_p(u-1) = -\psi_p(-1) = -\left(\frac{-1}{p}\right).$$

Так как аналогичный факт имеет место для $\bar{\pi}$, то получается $\Phi_p = \pi + \bar{\pi} \equiv -2\left(\frac{-1}{p}\right) \bmod (1-\rho)$ и потому также сравнимо и по $\bmod 3$. Поэтому здесь

$$A = \frac{1}{2}\Phi_p \equiv -\left(\frac{-1}{p}\right) \bmod 3.$$

Мы получили нормирующую единицу $\varepsilon_p = -\left(\frac{-1}{p}\right)$.

Аналогично доказанным в п. 8 фактам IV, V мы доказали тем самым следующий результат:

VI. *Каждое простое число* $p \equiv 1 \bmod 3$ *обладает представлением* $p = A^2 + 3B^2$ *в виде суммы квадрата и утроенного квадрата.*

Основание A *первого из этих квадратов с нормированием*

$$A \equiv -\left(\frac{-1}{p}\right) \bmod 3, \text{ т. е. } A \equiv \left\{\begin{array}{l} -1 \bmod 3 \text{ для } p \equiv 1 \bmod 4 \\ 1 \bmod 3 \text{ для } p \equiv -1 \bmod 4 \end{array}\right\}$$

дается суммой

$$A = \frac{1}{2}\Phi_p = \frac{1}{2}\sum_{x \bmod p}\left(\frac{x^3 - 1}{p}\right).$$

Глава III

ТЕОРЕМА ДИРИХЛЕ О ПРОСТЫХ ЧИСЛАХ

§ 11. ЭЛЕМЕНТАРНЫЕ ЧАСТНЫЕ СЛУЧАИ

1. Следствия из теории квадратичных вычетов. В § 7, п. 5 мы уже упоминали известную теорему Дирихле о простых числах в арифметической прогрессии и использовали ее там для изучения символа Лежандра как функции его знаменателя. В формулировке Дирихле эта теорема утверждает, что в каждой арифметической прогрессии

$$r+km \quad (r\text{ — целое},\ m\text{ — натуральное},\ k=0,\ 1,\ 2,\ \ldots),$$

у которой первый член r взаимно прост с разностью m, содержится бесконечно много простых чисел. На языке современной теории чисел это означает, что

В каждом классе вычетов $r \bmod m$, взаимно простом с модулем, существует бесконечно много простых чисел.

Настоящая глава посвящена доказательству этой теоремы. Для этого мы используем аналитические методы, которые ввел в теорию чисел Дирихле.

Прежде чем приступить к общему доказательству, мы проведем в этом параграфе исследование некоторых частных случаев, которое может быть выполнено без привлечения аналитических методов. Это, во-первых, случаи конкретных (небольших) значений m и, во-вторых, случаи классов вычетов $r \equiv 1 \bmod m$ и $r \equiv -1 \bmod m$ при любом m. Во всех этих случаях метод доказательства является обобщением доказательства Евклида из § 1, п. 3 существования бесконечного множества простых чисел вообще (без дополнительных условий о сравнимости), которое, впрочем, можно рассматривать как частный случай $m=1$ или 2 с единственным взаимно простым с модулем классом вычетов $r \equiv 1 \bmod 1$ или $\bmod 2$.

В основе доказательств частных случаев первого типа лежит следующий факт, который получается из теории квадратичных вычетов:

I. *Для каждого числа a, не являющегося квадратом, существует бесконечно много простых чисел p с $\left(\frac{a}{p}\right)=-1$ и бесконечно много простых чисел p с $\left(\frac{a}{p}\right)=1$.*

Доказательство. Если a не является квадратом, то, согласно результату VI, п. 6, § 9, классы вычетов $b \bmod f(a)$, для которых $\left(\frac{a}{b}\right) = 1$, образуют подгруппу $\mathfrak{H}$ индекса 2 в группе $\mathfrak{G}$ всех классов вычетов по $\bmod f(a)$, взаимно простых с модулем. Тогда классы вычетов $b \bmod f(a)$, для которых $\left(\frac{a}{b}\right) = -1$, образуют единственный смежный класс по этой подгруппе, а именно, дополнение $\mathfrak{G} - \mathfrak{H}$. Надо показать, что в каждом из этих комплексов $\mathfrak{H}$ и $\mathfrak{G} - \mathfrak{H}$, состоящих из $\varphi(f(a)) / 2$ классов вычетов по $\bmod f(a)$, взаимно простых с модулем, имеется бесконечно много простых чисел. При этом $f(a)$ имеет значение из IV, п. 5, § 9; если без ограничения общности предположить a свободным от квадратов, то

$$f(a) = \left\{ \begin{array}{lll} a & \text{для} & a \equiv 1 \bmod 4 \\ 4a & \text{для} & a \not\equiv 1 \bmod 4 \end{array} \right\}.$$

а) Мы начнем с доказательства для дополнения $\mathfrak{G} - \mathfrak{H}$, которое можно получить особенно просто. Так как $\mathfrak{H}$ имеет индекс 2 и потому $\mathfrak{G} - \mathfrak{H}$ не пусто, в $\mathfrak{G} - \mathfrak{H}$ имеются целые числа b. Пусть b_0 — какое-нибудь из них. Так как -1 принадлежит к $\mathfrak{H}$, то $b_0 \neq \pm 1$, так что b_0 обладает простыми делителями. Если бы все эти простые делители лежали в $\mathfrak{H}$, то там же лежало бы и их произведение $\pm b_0$, а потому и само b_0. Следовательно, по крайней мере один простой делитель p_0 числа b_0 лежит в $\mathfrak{G} - \mathfrak{H}$.

Пусть теперь уже известно некоторое количество $r \geqslant 1$ простых чисел $p_0, \ldots, p_{r-1}$ из $\mathfrak{G} - \mathfrak{H}$. Определим тогда целое b_r со свойствами

$$b_r \equiv b_0 \bmod f(a), \tag{1}$$

$$b_r \text{ взаимно просто с } p_0 \ldots p_{r-1}. \tag{2}$$

Это всегда можно сделать; действительно, уточним требование (2), а именно, потребуем, чтобы b_r принадлежало к какому-нибудь определенному классу вычетов по $\bmod p_0 \ldots p_{r-1}$, взаимно простому с модулем, например,

$$b_r \equiv 1 \bmod p_0 \ldots p_{r-1} \tag{2'}$$

и применим основную теорему из § 4, п. 9 о системах сравнений с попарно взаимно простыми модулями; при этом еще нужно заметить, что содержащееся в случае $a < 0$ в требовании (1) условие $\operatorname{sgn} b_r = \operatorname{sgn} b_0$ также может быть выполнено (ср. в доказательстве V из § 9, п. 5). Так как, согласно (1), b_r принадлежит к $\mathfrak{G} - \mathfrak{H}$, то точно так же, как выше для b_0, мы получаем отсюда, что по крайней мере один простой делитель p_r числа b_r тоже принадлежит к $\mathfrak{G} - \mathfrak{H}$. Однако, согласно (2),

p_r отлично от $p_0, \ldots, p_{r-1}$. Таким образом, в $\mathfrak{G} - \mathfrak{H}$ найдено новое простое число p_r.

Сходство этого доказательства с доказательством Евклида из § 1, п. 3 бросается в глаза. Образование числа $p_0 p_1 \ldots p_{r-1} + 1$, простой делитель которого давал нам там новое простое число, заменяется здесь более общим образованием $g_r p_0 \ldots p_{r-1} + 1$ [если пользоваться требованием (2′)], где g_r есть некоторый добавочный множитель, появление которого обусловлено дополнительным требованием (1) и который подбирается поэтому из условия $g_r p_0 \ldots p_{r-1} \equiv b_0 - 1 \bmod f(a)$. Кроме наличия этого добавочного множителя g_r, имеется и еще одно различие, заключающееся в том, что в доказательстве Евклида нас удовлетворяет *каждый* простой делитель числа $p_0 \ldots p_{r-1} + 1$, в то время как здесь устанавливается только существование *хотя бы одного* нужного нам простого делителя числа $g_r p_0 \ldots p_{r-1} + 1$.

б) Несколько сложнее доказательство в случае подгруппы $\mathfrak{H}$, когда такой метод уже не пригоден. Теперь мы будем использовать следующий факт. Пусть, без ограничения общности, a свободно от квадратов, и пусть x — какое-нибудь целое число со свойствами:

$$x^2 - a \neq \pm 1, \tag{1}$$

$$\text{если } a \text{ нечетно, то } x \text{ четно}, \tag{2}$$

$$x \text{ взаимно просто с } a. \tag{3}$$

Вследствие (1) и того, что по сделанному относительно a предположению также $x^2 - a \neq 0$, $x^2 - a$ обладает простыми делителями, которые, в силу (2), (3), все нечетны и отличны от простых делителей числа a. Для каждого такого простого делителя p числа $x^2 - a$ имеет поэтому место $\left(\frac{a}{p}\right) = 1$, т. е. p лежит в $\mathfrak{H}$. Кроме того, в силу (3), p отлично от простых делителей числа x.

Выберем такое целое число g, чтобы условия (1), (2), (3) выполнялись не только для $x = g$, а и для каждого кратного $x = gh$ с нечетным h, взаимно простым с a. Как легко видеть, такое число подобрать можно, например,

$$g = a \pm 1, \text{ в зависимости от } a \gtrless 0.$$

Пусть теперь уже известно некоторое количество $r \geqslant 1$ простых чисел $p_0, \ldots, p_{r-1}$ из $\mathfrak{H}$. Они, конечно, взаимно просты с $f(a)$, а так как a свободно от квадратов, то и с самим a. Если тогда положить $x = g p_0 \ldots p_{r-1}$, то, в силу сказанного, каждый простой делитель p_r числа $x^2 - a$ принадлежит к $\mathfrak{H}$ и отличен от $p_0, \ldots, p_{r-1}$. Таким образом, найдено новое простое число p_r, принадлежащее $\mathfrak{H}$.

Также и для этого доказательства бросается в глаза сходство с доказательством Евклида. Обобщение имеет место в двух отношениях. Во-первых (как и в случае $\mathfrak{G}-\mathfrak{H}$), вместо произведения $p_0 \dots p_{r-1}$ рассматривается его кратное $gp_0 \dots p_{r-1}$ (причем теперь g не зависит от r). Во-вторых, из этого произведения составляется теперь не линейный многочлен $x+1$, как в доказательстве Евклида, а квадратный многочлен x^2-a, и тогда нас удовлетворяет снова каждый простой делитель (в отличие от случая $\mathfrak{G}-\mathfrak{H}$).

Высказывание I имеет непосредственное отношение к теореме Дирихле о простых числах, поскольку оно устанавливает существование бесконечного множества простых чисел в каждом из комплексов $\mathfrak{H}$ и $\mathfrak{G}-\mathfrak{H}$, имеющих по $\varphi(f(a))/2$ классов вычетов по $\bmod f(a)$, взаимно простых с модулем. При этом нужно отметить, что в случае $a<0$ сравнимость по модулю $f(a)<0$ понимается в смысле § 9, п. 5. Каждый из комплексов $\mathfrak{H}$ и $\mathfrak{G}-\mathfrak{H}$ состоит тогда из $\varphi(f(a))/4=\varphi(|f(a)|)/2$ пар противоположных полуклассов по $\bmod|f(a)|$, взаимно простых с модулем, из которых, однако, вопрос о существовании в них простых чисел имеет смысл только для положительных. Поэтому в каждом случае каждый из комплексов $\mathfrak{H}$ и $\mathfrak{G}-\mathfrak{H}$ содержит точно $\varphi(|f(a)|)/2$ положительных полуклассов по $\bmod f(a)$, взаимно простых с модулем. Таким образом, если, в частности, $\varphi(|f(a)|)/2=1$, то утверждение I доказывает правильность теоремы Дирихле о простых числах для модуля $m=|f(a)|$.

Так как, согласно § 4, п. 8, имеет место

$$\varphi(m)=\prod_{p|m}(p-1)\,p^{\mu-1} \quad \text{для} \quad m=\prod_{p|m}p^{\mu},$$

то равенство $\varphi(m)=2$ верно только для $m=3, 4, 6$. Два первых модуля действительно являются абсолютными величинами ведущих модулей, а именно, для $a=-3,\ -1$ будет, соответственно $|f(a)|=3, 4$. Таким образом, мы можем установить:

II. *Существует бесконечно много простых чисел каждого из следующих видов*:

$$p\equiv 1 \bmod 3, \qquad p\equiv -1 \bmod 3,$$
$$p\equiv 1 \bmod 4, \qquad p\equiv -1 \bmod 4.$$

Во всех остальных случаях высказывание I слабее, чем теорема Дирихле о простых числах для модуля $m=|f(a)|$, так как оно тогда относится не к отдельным классам вычетов, взаимно простым с модулем, а только к комплексам таких классов, содержащим их в количестве, большем чем один. Можно отметить еще случаи, когда получаются комплексы, содержащие только по два класса вычетов, взаимно простых с модулем (соответственно по два положительных полукласса, взаимно простых с

модулем), т. е. когда $\varphi(|f(a)|)/2 = 2$. Равенство $\varphi(m) = 4$ выполняется только для

$$m = 5,\ 8,\ 12,\ 10.$$

Из этих модулей только первые три являются абсолютными величинами ведущих модулей $m = |f(a)|$, а именно, для

$$a = 5,\ \pm 2,\ 3.$$

Поэтому в случае $m = 5$ из I получается следующее высказывание:

III. *Существует бесконечное множество простых чисел каждого из двух видов*

$$p \equiv 1,4 \bmod 5, \qquad p \equiv 2,3 \bmod 5.$$

В случаях $m = 8,12$ можно получить несколько более сильное высказывание. Прежде всего, из I следует, что существует бесконечное множество простых чисел каждого из видов

$$\left.\begin{array}{l} p \equiv 1,7 \bmod 8,\ p \equiv 3,5 \bmod 8, \\ p \equiv 1,3 \bmod 8,\ p \equiv 5,7 \bmod 8, \end{array}\right| \quad p \equiv 1,11 \bmod 12, \quad p \equiv 5,7 \bmod 12,$$

Далее, согласно II, существует также бесконечное множество простых чисел каждого из видов

$$p \equiv 1,5 \bmod 8,\ p \equiv 3,7 \bmod 8, \left|\begin{array}{l} p \equiv 1,7 \bmod 12,\ p \equiv 5,11 \bmod 12 \\ p \equiv 1,5 \bmod 12,\ p \equiv 7,11 \bmod 12. \end{array}\right.$$

Так как для каждого из модулей теперь фигурируют все возможные пары классов вычетов, взаимно простых с модулем, то получается следующее более сильное высказывание:

IV. *Из четырех классов вычетов по* $\bmod 8$, *взаимно простых с модулем, и из четырех классов вычетов по* $\bmod 12$, *взаимно простых с модулем, конечное множество простых чисел может содержать в каждом случае самое большее один класс.*

Причина того, что в случаях $m = 8,12$ оказалось возможным получить более сильное по сравнению с III высказывание IV, заключается в том, что в этих случаях группа $\mathfrak{G}$ классов вычетов, взаимно простых с модулем, есть прямое произведение двух циклических групп порядка 2 (так называемая четверная группа), и потому обладает тремя подгруппами $\mathfrak{H}_1, \mathfrak{H}_2, \mathfrak{H}_3$ индекса 2, в то время как для $m = 5$ получается циклическая группа порядка 4, обладающая всего одной подгруппой $\mathfrak{H}$ индекса 2.

2. Многочлен деления круга. Примененное в доказательстве I, п. 1 в случае $\left(\frac{a}{p}\right) = 1$, т. е. в случае подгруппы $\mathfrak{H}$, обобщение метода доказательства Евклида может быть далее обобщено

так, что оно позволит нам доказать теорему Дирихле о простых числах для единичного класса $r \equiv 1 \bmod m$ при любом m. Для этого вместо используемого там многочлена $x^2 - a$ нужно использовать такой многочлен $f_m(x)$, корнями которого являются первообразные m-е корни из 1. Сначала мы и займемся этим многочленом $f_m(x)$.

Напомним общие факты о корнях из 1, изложенные в начале § 8, п. 1. Согласно § 8 п. 1, m-е корни из 1 при любом натуральном m образуют циклическую группу порядка m. Образующие элементы этой группы называются первообразными m-ми корнями из 1. Их существует точно $\varphi(m)$, а именно, первообразными корнями будут все степени ζ^r любого одного из них с показателями r, взаимно простыми с m. Поэтому многочлен $f_m(x)$, корни которого являются первообразными m-ми корнями из 1, представляется в виде

$$f_m(x) = \prod_{\substack{r \bmod m \\ (r, m)=1}} (x - \zeta^r), \tag{1}$$

где ζ есть какой-нибудь первообразный m-й корень из 1. $f_m(x)$ называется m-м *многочленом деления круга*. Его степень равна $\varphi(m)$.

Каждый m-й корень ζ^a из 1 есть первообразный m/d-й корень из 1 с определенным натуральным делителем d числа m, а именно, равным (a, m). Если, наоборот, собрать все первообразные m/d-е корни из 1 для всех натуральных делителей d числа m, то мы получим как раз все m-е корни из 1, т. е. корни многочлена

$$x^m - 1 = \prod_{a \bmod m} (x - \zeta^a).$$

Поэтому имеет место равенство многочленов:

$$x^m - 1 = \prod_{d|m} f_{m/d}(x). \tag{2}$$

Мы вывели это тем же самым методом, какой был применен для вывода формулы сложения в § 4, п. 6

$$m = \sum_{d|m} \varphi\left(\frac{m}{d}\right).$$

Эта формула сложения оказывается здесь соотношением между степенями многочленов в равенстве (2).

Применим теперь к равенству (2) формулу обращения Мёбиуса из § 4, п. 7. Правда, она была выведена там только для сумм, однако ее доказательство автоматически переносится и на произведения, если заменить формально сложение значений функции их перемножением и в соответствии с этим писать

целочисленные множители $\mu\left(\frac{m}{d}\right)$ в виде показателей. Таким образом, для любых двух всюду отличных от 0 теоретико-числовых функций $f(m)$ и $g(m)$ одновременно с любым из двух мультипликативных функциональных равенств

$$\prod_{d|m} f(d) = g(m), \qquad \prod_{d|m} g(d)^{\mu\left(\frac{m}{d}\right)} = f(m)$$

выполняется также и второе. Если в этих формулах делители заменить дополнительными делителями и применить формулы к теоретико-числовым функциям $f(m) = f_m(x)$ и $g(m) = x^m - 1$ (которые, кроме m, зависят также от неизвестного x, играющего роль параметра), то из (2) следует равенство многочленов

$$f_m(x) = \prod_{d|m} (x^{\frac{m}{d}} - 1)^{\mu(d)}, \tag{3}$$

представляющее собой явное выражение для многочлена деления круга $f_m(x)$. Полученное таким же способом в § 4, п. 8 явное представление

$$\varphi(m) = \sum_{d|m} \mu(d) \frac{m}{d}$$

для функции Эйлера снова оказывается соотношением между степенями многочленов в равенстве (3).

Первоначальное представление (1) для многочлена деления круга позволяет заключить, что его коэффициенты принадлежат полю $\mathsf{P}(\zeta)$ m-х корней из 1 и даже принадлежат содержащейся в нем области целостности $\Gamma[\zeta]$. Равенство же (3) показывает, что в действительности эти коэффициенты принадлежат полю P и даже содержащейся в нем области целостности Γ.

V. *Коэффициенты многочлена деления круга $f_m(x)$ суть целые рациональные числа.*

Доказательство. Если в (3) объединить множители с $\mu(d) = 1$ и множители с $\mu(d) = -1$, то мы получим представление

$$f_m(x) = \frac{g_m(x)}{h_m(x)},$$

где $g_m(x)$ и $h_m(x)$ суть многочлены с целыми рациональными коэффициентами. Как известно, при делении многочленов с остатком коэффициенты частного и остатка, вообще говоря, выражаются рационально через коэффициенты делимого и делителя, причем в качестве знаменателя может фигурировать только коэффициент при старшем члене делителя. В настоящем случае, когда деление выполняется без остатка и коэффициент при старшем члене у делителя $h_m(x)$ [так же как и у делимого

$g_m(x)]$ равен 1, действительно получается поэтому, что коэффициенты частного $f_m(x)$ суть целые рациональные числа.

Прежде чем приступить к тем свойствам многочлена деления круга $f_m(x)$, которые будут нужны нам для нашей цели, мы докажем один факт, не являющийся для нашей цели необходимым, но вообще очень важный. В специальном случае простого числа $m = p$ мы познакомились с ним уже в I, п. 1, § 8. Именно:

VI. *Многочлен деления круга $f_m(x)$ неприводим над полем рациональных чисел* P.

Доказательство опирается на известную теорему из алгебры целочисленных многочленов, для которой мы дадим здесь короткое доказательство.

Теорема Гаусса. *При любом разложении*

$$f(x) = g(x)\,h(x)$$

целочисленного многочлена f со старшим коэффициентом 1 на два многочлена g, h с рациональными коэффициентами и старшими коэффициентами 1 коэффициенты сомножителей g, h тоже будут целыми числами.

Доказательство теоремы Гаусса. После умножения на общие наименьшие знаменатели b, c многочленов g, h получается разложение

$$af(x) = G(x)\,H(x) \quad \text{с} \quad a = bc,$$

в котором G, H суть многочлены с целыми взаимно простыми коэффициентами. Предположим, что $a \neq 1$. Тогда существует простое число $p \mid a$. Рассмотрим тогда последнее равенство как равенство многочленов над полем Π классов вычетов по $\bmod p$. Над этим полем левая часть равенства представляет собой нулевой многочлен, так как $p \mid a$, в то время как оба множителя справа, ввиду взаимной простоты их коэффициентов, отличны от нулевого многочлена. Это, однако, невозможно. Следовательно, предположение $a \neq 1$ неверно. Поэтому $a = 1$, а потому также $b = 1$, $c = 1$, так что действительно $g = G$ и $h = H$ суть целочисленные многочлены со старшими коэффициентами, равными 1.

Доказательство утверждения VI. Пусть ζ — некоторый определенный первообразный m-й корень из 1. Тогда, как доказывается в алгебре, существует такой однозначно определенный неприводимый многочлен $g_m(x)$ с рациональными коэффициентами и старшим коэффициентом 1, что $g_m(\zeta) = 0$ и $f_m(x)$ делится на $g_m(x)$. Неприводимость $f_m(x)$ будет доказана, если мы покажем, что каждый корень ζ^r многочлена $f_m(x)$ является также корнем $g_m(x)$; действительно, тогда $g_m(x)$ в свою очередь будет делиться на $f_m(x)$, и потому $f_m(x) = g_m(x)$.

Согласно V и теореме Гаусса, $g_m(x)$, будучи делителем многочлена $f_m(x)$, имеет целые коэффициенты. Поэтому, как уже было замечено в доказательстве утверждения V, при делении с остатком

$$h(x) = q(x)\, g_m(x) + r(x)$$

для каждого целочисленного многочлена $h(x)$ получается остаток $r(x)$ степени, меньшей чем степень $g_m(x)$, и имеющий целые коэффициенты. Полагая $x = \zeta$, мы получаем, что каждый элемент $h(\zeta)$ области целостности $\Gamma[\zeta]$ обладает представлением

$$h(\zeta) = c_0 + c_1\zeta + \ldots + c_{n-1}\zeta^{n-1}$$

с целыми рациональными коэффициентами $c_0, \ldots, c_{n-1}$, где n есть степень многочлена $g_m(x)$. Ввиду неприводимости $g_m(x)$, это представление однозначно.

Применим это к элементам $g_m(\zeta^r)$ из $\Gamma[\zeta]$, где r пробегает классы вычетов по $\bmod m$, взаимно простые с модулем, а потому ζ^r, согласно (1), пробегает корни многочлена $f_m(x)$. Нам нужно доказать, что эти элементы равны 0. В силу представления

$$g_m(\zeta^r) = c_0^{(r)} + c_1^{(r)}\zeta + \ldots + c_{n-1}^{(r)}\zeta^{n-1},$$

каждому классу вычетов $r \bmod m$, взаимно простому с модулем, однозначно соответствует система целочисленных коэффициентов $c_0^{(r)}, \ldots, c_{n-1}^{(r)}$. Пусть c есть максимум абсолютных величин этих $n\varphi(m)$ коэффициентов.

Рассмотрим теперь специально те классы вычетов $r \bmod m$, взаимно простые с модулем, в которых имеются простые числа p. Согласно § 4, п. 11, для каждого целочисленного многочлена g в поле классов вычетов по $\bmod p$ выполняется тождество $g(x)^p \equiv g(x^p) \bmod p$. Если применить это к $g = g_m$, то, так как $g_m(\zeta) = 0$, мы будем иметь соотношение вида $g_m(\zeta^p) = pG(\zeta)$, где G — некоторый целочисленный многочлен. Если $G(\zeta)$ тоже представить в данной выше форме, то мы получим, что коэффициенты $c_0^{(r)}, \ldots, c_{n-1}^{(r)}$, соответствующие $g_m(\zeta^r)$, все $\equiv 0 \bmod p$, если $r \equiv p \bmod m$, где p — простое число. Если, кроме того, $p > c$, то из того, что $|c_0^{(r)}|, \ldots, |c_{n-1}^{(r)}| \leqslant c$, следует, что все коэффициенты $c_0^{(r)}, \ldots, c_{n-1}^{(r)} = 0$. Таким образом, из $g_m(\zeta) = 0$ следует $g_m(\zeta^r) = 0$, если $r \equiv p \bmod m$ с $p > c$.

Если теорему Дирихле о простых числах предполагать известной, то доказательство тем самым завершено; действительно, тогда уже будет известно, что в *каждом* классе вычетов $r \bmod m$, взаимно простом с модулем, существует простое число $p > c$. Чтобы достигнуть цели также и без теоремы Дирихле, применим наше рассуждение несколько раз. Мы получим тогда, что из $g_m(\zeta) = 0$ следует $g_m(\zeta^r) = 0$ также и в том случае, когда для

каждого класса вычетов по $\bmod m$, взаимно простого с модулем, существует конечное множество таких (не обязательно различных) простых чисел $p_\varkappa > c$ ($\varkappa = 1, \ldots, k$), что $r \equiv p_1 \ldots p_k \bmod m$. Это, однако, действительно имеет место; в самом деле, если $Q = q_1 \ldots q_l$ есть произведение всех не входящих в m простых чисел $q_\lambda \leqslant c$, то, согласно § 4, п. 9, существует такое натуральное число P, что $P \equiv r \bmod m$, P взаимно просто с Q (например, $\equiv 1 \bmod Q$), а тогда $P = p_1 \ldots p_k$ имеет лишь простые делители $p_\varkappa > c$. Тем самым показано, что действительно каждый корень ζ^r многочлена $f_m(x)$ является также корнем многочлена $g_m(x)$, что, как уже было сказано, и доказывает наше утверждение $f_m(x) = g_m(x)$.

3. Случай единичного класса вычетов $r \equiv 1 \bmod m$. Чтобы получить доказательство теоремы Дирихле о простых числах для единичного класса при любом модуле m, т. е. доказать существование бесконечного множества простых чисел $p \equiv 1 \bmod m$, нам понадобятся два особых свойства m-го многочлена деления круга $f_m(x)$.

Первое из этих свойств аналогично использованному в п. 1 при доказательстве утверждения I (случай подгруппы $\mathfrak{H}$) факту, а именно, тому, что при целом x все не входящие в a нечетные простые делители p числа $x^2 - a$ лежат в подгруппе $\mathfrak{H}$, т. е. для них выполняется интересующее нас там соотношение $\left(\frac{a}{p}\right) = 1$. Здесь мы, соответственно, имеем:

VII. *При целом x все не входящие в m простые делители p числа $f_m(x)$ лежат в единичном классе вычетов по* $\bmod m$, *т. е. из* $p \mid f_m(x)$, $p \nmid m$ *следует* $p \equiv 1 \bmod m$.

Доказательство. Пусть сначала x — неизвестное. Из равенства (2) п. 2 немедленно можно заключить, что имеет место

$$x^m - 1 = f_m(x) F_m(x) \tag{1}$$

с некоторым целочисленным многочленом $F_m(x)$. Аналогично для каждого делителя $d \neq 1$ числа m имеет место

$$\frac{x^m - 1}{x^{\frac{m}{d}} - 1} = f_m(x) G_{m,d}(x) \tag{2}$$

с некоторым целочисленным многочленом $G_{m,d}(x)$; действительно,

$$x^{\frac{m}{d}} - 1 = \prod_{t \mid \frac{m}{d}} f_{\frac{m}{td}}(x)$$

есть часть произведения

$$x^m - 1 = \prod_{t \mid m} f_{\frac{m}{t}}(x),$$

которая при $d \neq 1$ не содержит множитель $f_m(x)$ (другими словами, m/d-е корни из 1 образуют подмножество m-х корней из 1, в котором при $d \neq 1$ не содержится первообразный m-й корень из 1).

Пусть теперь x — целое число и p — не входящий в m простой делитель числа $f_m(x)$. С одной стороны, из (1), вследствие предположения $p \mid f_m(x)$, заведомо следует, что

$$x^m \equiv 1 \bmod p. \tag{3}$$

С другой стороны, если использовать еще предположение $p \nmid m$, то из (2) получаем, что

$$x^{\frac{m}{d}} \not\equiv 1 \bmod p \text{ для всех } d \mid m,\ d \neq 1, \tag{4}$$

действительно, если бы было $x^{\frac{m}{d}} \equiv 1 \bmod p$, то прежде всего отсюда следовало бы

$$\frac{x^m - 1}{x^{\frac{m}{d}} - 1} = x^{\frac{m}{d}(d-1)} + \ldots + x^{\frac{m}{d}} + 1 \equiv d \bmod p,$$

поэтому, согласно (2), было бы $d \equiv 0 \bmod p$, и, таким образом, $p \mid d \mid m$, что противоречит тому, что $p \nmid m$.

Согласно (3) и (4), класс вычетов $x \bmod p$ имеет порядок m. Отсюда, согласно VIII, п. 5, § 4, следует $m \mid \varphi(p) = p - 1$, т. е. $p \equiv 1 \bmod m$, что и требовалось доказать.

Второе нужное нам свойство многочлена деления круга $f_m(x)$ состоит просто в том, что при $m \neq 1$ свободный член $f_m(x)$ равен 1:

$$f_m(0) = 1 \text{ при } m \neq 1. \tag{5}$$

Это получается из явного представления (3) п. 2, согласно которому имеет место

$$f_m(0) = \prod_{d \mid m} (-1)^{\mu(d)} = (-1)^{\sum_{d \mid m} \mu(d)} = (-1)^{\varepsilon(m)}$$

с $\varepsilon(m) = 1$ или 0 в зависимости от того, $m = 1$ или $\neq 1$ (ср. § 4, п. 7). В тривиальном случае $m = 1$, поэтому будет $f_m(0) = -1$, что ясно и непосредственно, так как $f_1(x) = x - 1$.

Теперь мы приступаем к доказательству самой теоремы Дирихле о простых числах для единичного класса вычетов:

VIII. *Для каждого натурального m существует бесконечно много простых чисел $p \equiv 1 \bmod m$.*

Доказательство. Без ограничения общности можно предположить $m \neq 1$. Пусть уже известно некоторое количество $r \geqslant 0$

простых чисел $p_0, \ldots, p_{r-1} \equiv 1 \bmod m$. Образуем тогда значение m-го многочлена деления круга $f_m(x)$ для натурального числа

$$x_r = gmp_0 \ldots p_{r-1},$$

причем натуральное число g выбрано так, что все, быть может, существующие в области натуральных чисел корни двух алгебраических уравнений $f_m(x) = \pm 1$, количество которых во всяком случае конечно, по величине меньше, чем gm. Тогда $f_m(x_r) \neq \pm 1$ и, конечно, также $f_m(x_r) \neq 0$, ибо при $m \neq 1$ ни одно натуральное число не является первообразным m-м корнем из 1. Следовательно, $f_m(x_r)$ обладает по крайней мере одним простым делителем p_r. Так как $x_r \equiv 0 \bmod m$, то из (5), кроме отличия от нуля, следует даже, что

$$f_m(x_r) \equiv 1 \bmod m$$

и потому p_r не входит в m. Поэтому, согласно VII, $p_r \equiv 1 \bmod m$. В силу того, что $x_r \equiv 0 \bmod p_0 \ldots p_{r-1}$, из (5) далее следует, что

$$f_m(x_r) \equiv 1 \bmod p_0 \ldots p_{r-1}$$

и потому p_r отлично от $p_0, \ldots, p_{r-1}$. Таким образом, найдено новое простое число $p_r \equiv 1 \bmod m$.

Сделаем еще несколько замечаний относительно этого доказательства.

1. В качестве дополнительного множителя можно взять $g = 1$ и оперировать просто с

$$x_r = mp_0 \ldots p_{r-1}.$$

А именно, если $m \neq 1$, то имеет место

$$|f_m(x)| > 1 \text{ для каждого натурального } x \neq 1.$$

Действительно, согласно (1) п. 2,

$$|f_m(x)| = \prod_{\substack{r \bmod m \\ (r, m)=1}} |x - \zeta^r|,$$

и здесь все сомножители $|x - \zeta^r| > 1$, как расстояния от точки $x \geqslant 2$ на вещественной оси до точек $\zeta^r \neq 1$ на единичном круге (фиг. 2).

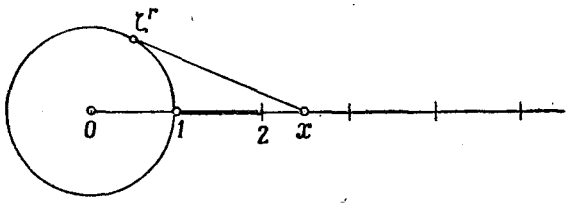
2. При этом упрощении наше доказательство в специальном случае $m = 2$, когда $f_m(x) = x + 1$, совпадает с доказательством Евклида из § 1, п. 3; действительно, входящий в $x_r = mp_0 \ldots p_{r-1}$ множитель $m = 2$ можно тогда рассматривать как первое простое число $p = 2$, а простые числа $p_0, \ldots, p_{r-1}$ в этом случае нечетны.

3. В специальном случае, когда $m = q^\mu$ есть степень простого числа q, последовательность заключений, приводящая к доказа-

тельству, принимает особенно простой вид. Начинаем с рассмотрения целочисленного многочлена

$$f_{q^\mu}(x) = \frac{x^{q^\mu}-1}{x^{q^{\mu-1}}-1} = x^{q^{\mu-1}(q-1)} + \ldots + x^{q^{\mu-1}} + 1 = f_q(x^{q^{\mu-1}})$$

(не используя того, что он есть q^μ-й многочлен деления круга) и показываем по схеме доказательства утверждения VII, что для целого x из $p \mid f_{q^\mu}(x)$, $p \neq q$ следует $x^{q^\mu} \equiv 1$, $x^{q^{\mu-1}} \not\equiv 1 \mod r$, и



Фиг. 2.

потому $q^\mu \mid \varphi(p) = p-1$, т. е. $p \equiv 1 \bmod q^\mu$. Так как здесь очевидно, что $f_{q^\mu}(0) = 1$ и

$$f_{q^\mu}(x) > 1 \text{ для каждого натурального } x,$$

то каждый простой делитель p_r числа $f_{q^\mu}(qp_0 \ldots p_{r-1})$ дает нам отличное от $p_0, \ldots, p_{r-1}$ простое число $p_r \equiv 1 \bmod q^\mu$. Можно это доказательство модифицировать и так, что дополнительный множитель q сделается излишним. Для этого заметим, что, за исключением тривиального частного случая $q^\mu = 2^1$, из представления $f_{q^\mu}(x)$ в виде отношения и из § 5, п. 5 (лемма 3) вытекает следующее дополнение к VII:

VII′. *При целом x простое число q или совсем не входит в $f_{q^\mu}(x)$, или входит с показателем 1, в зависимости от того, $x \not\equiv 1$ или $x \equiv 1 \bmod q$.*

Так как, очевидно,

$$f_{q^\mu}(x) > q \text{ для каждого натурального } x \neq 1,$$

то $f_{q^\mu}(p_0 \ldots p_{r-1})$ содержит простые делители $p_r \neq q$ и *каждый из них дает отличное от $p_0, \ldots, p_{r-1}$ простое число $p_r \equiv 1 \bmod q^\mu$.*

4. Случай класса вычетов $r \equiv -1 \bmod m$. С помощью в значительной степени аналогичного метода можно получить доказательство теоремы Дирихле о простых числах также и для класса вычетов $r \equiv -1 \bmod m$, т. е. показать существование бесконечного множества простых чисел $p \equiv -1 \bmod m$ при любом m. В связи с тем, что у нас уже есть образец доказательства

для единичного класса вычетов, мы можем теперь провести изложение несколько более сжато. Чтобы освободиться от неправильности наших формул в специальном случае $m = 1$, которая имела место уже и там, а здесь еще более значительна, мы в дальнейшем все время будем предполагать $m \neq 1$.

Представим себе использованные в п. 3 многочлены

$$g_m(x) = x^m - 1 = \prod_{a \bmod m} (x - \zeta^a),$$

$$f_m(x) = \prod_{d \mid m} g_{\frac{m}{d}}(x)^{\mu(d)} = \prod_{\substack{r \bmod m \\ (r, m)=1}} (x - \zeta^r)$$

от одного неизвестного x записанными в однородной форме

$$g_m(x, y) = x^m - y^m = \prod_{a \bmod m} (x - \zeta^a y),$$

$$f_m(x, y) = \prod_{d \mid m} g_{\frac{m}{d}}(x, y)^{\mu(d)} = \prod_{\substack{r \bmod m \\ (r, m)=1}} (x - \zeta^r y)$$

и заменим в них неизвестные x, y через $x + iy$, $x - iy$, точнее, образуем целочисленные многочлены

$$\left.\begin{aligned} V_m(x, y) = \frac{1}{2i} g_m(x + iy, x - iy) = \frac{1}{2i}[(x + iy)^m - (x - iy)^m] = \\ = J[(x + iy)^m] \end{aligned}\right\} \quad (1)$$

$$W_m(x, y) = f_m(x + iy, x - iy) = \prod_{d \mid m} V_{\frac{m}{d}}(x, y)^{\mu(d)}, \quad (2)$$

у которых коэффициенты при членах, содержащих наивысшую степень x, равны соответственно:

$$\frac{1}{y} V_m(x, y)\,|_{x=1,\, y=0} = m,$$

$$W_m(1, 0) = f_m(1, 1) = \prod_{d \mid m} \left(\frac{m}{d}\right)^{\mu(d)}.$$

Заметим, что вследствие нашего предположения $m \neq 1$, согласно (2) п. 7, § 4, имеет место $\sum_{d \mid m} \mu(d) = 0$.

Кроме того, нам понадобятся еще соответствующие мнимым частям V_m вещественные части U_m выражений $(x + iy)^m$; эти вещественные части определяются формулами, аналогичными (1). Однако эти формулы нам не понадобятся, а будут нужны лишь формулы

$$\left.\begin{aligned} (x + iy)^m = U_m(x, y) + iV_m(x, y) \\ (x^2 + y^2)^m = U_m(x, y)^2 + V_m(x, y)^2 \end{aligned}\right\}. \quad (3)$$

Для простоты записи мы будем в дальнейшем в большинстве случаев опускать аргументы x, y у U_m, V_m, W_m и у других встречающихся однородных многочленов.

Приводя формулы (1), (2) п. 3 к однородной форме и применяя указанную выше подстановку, мы тотчас же получаем

$$V_m = W_m H_m, \tag{4}$$

$$\frac{V_m}{V_{\frac{m}{d}}} = W_m K_{m,d} \text{ при } d \mid m \tag{5}$$

с целочисленными многочленами H_m, $K_{m,d}$. Далее, согласно (3), для любых натуральных чисел k, n, n_1, n_2 имеют место формулы

$$V_{kn} = V_n \left[\binom{k}{1} U_n^{k-1} - \binom{k}{3} U_n^{k-3} V_n^2 \pm \dots \right], \tag{6}$$

$$V_{n_1+n_2} = U_{n_1} V_{n_2} + U_{n_2} V_{n_1}. \tag{7}$$

Аналогично VII, п. 3 мы докажем теперь относительно многочлена W_m следующий факт, являющийся основным для нашей цели.

IX. *При целых взаимно простых x, y все не входящие в m простые делители вида $p \equiv -1 \bmod 4$ числа $W_m(x, y)$ лежат в классе вычетов $-1 \bmod m$, т. е.*

Из $p \mid W_m$, $p \nmid m$, $p \equiv -1 \bmod 4$ следует $p \equiv -1 \bmod m$.

Доказательство. С одной стороны, из $p \mid W_m$, согласно (4), следует

$$V_m \equiv 0 \bmod p. \tag{8}$$

С другой стороны, принимая во внимание $p \nmid m$, $p \equiv -1 \bmod 4$, мы, согласно (5), получаем, что

$$V_{\frac{m}{d}} \not\equiv 0 \bmod p \text{ для всех } d \mid m,\ d \neq 1. \tag{9}$$

Действительно, если бы было $V_{m/d} \equiv 0 \bmod p$, то отсюда прежде всего следовало бы, согласно (6) (с $n = m/d$, $k = d$),

$$\frac{V_m}{V_{\frac{m}{d}}} = \binom{d}{1} U_{\frac{m}{d}}^{d-1} - \binom{d}{3} U_{\frac{m}{d}}^{d-3} V_{\frac{m}{d}}^2 \pm \dots \equiv d U_{\frac{m}{d}}^{d-1} \bmod p,$$

и потому, согласно (5), было бы $dU_{m/d}^{d-1} \equiv 0 \bmod p$. Таким образом, имело бы место или $p \mid d \mid m$, что противоречит тому, что $p \nmid m$, или $U_{m/d} \equiv 0 \bmod p$; однако в последнем случае, согласно (3), было бы также $U_{m/d}^2 + V_{m/d}^2 \equiv 0 \bmod p$, а потому $(x^2+y^2)^{m/d} \equiv 0 \bmod p$, что вследствие $p \equiv -1 \bmod 4$ возможно только при $x, y \equiv 0 \bmod p$ (см. § 7, п. 2), в то время как по условию $(x, y) = 1$.

Наряду с $V_{m/d}$ мы рассмотрим V_{p+1}. Согласно (6) (с $n=1$, $k=p+1$),

$$V_{p+1}=y\left[\binom{p+1}{1}x^p-\binom{p+1}{3}x^{p-2}y^2\pm\ldots\right.$$
$$\left.\ldots+(-1)^{\frac{p-1}{2}}\binom{p+1}{p}xy^{p-1}\right].$$

Так как $p\equiv -1 \bmod 4$, то последний знак здесь отрицателен; далее, при $\nu=2, \ldots, p-1$ для биномиальных коэффициентов имеет место

$$\binom{p+1}{\nu}=\frac{(p+1)\,p\,(p-1)\,\ldots\,(p-(\nu-2))}{1\cdot 2\,\ldots\,\nu}\equiv 0 \bmod p.$$

Поэтому

$$V_{p+1}\equiv (p+1)\,(x^py-xy^p) \bmod p.$$

Отсюда, согласно малой теореме Ферма, следует

$$V_{p+1}\equiv 0 \bmod p. \tag{10}$$

Пусть теперь делитель d числа m определен формулой

$$\frac{m}{d}=(p+1,\ m).$$

По основной теореме об общем наибольшем делителе существуют такие целые числа h, k, что

$$\frac{m}{d}=h\,(p+1)-km, \text{ т. е. } h\,(p+1)=\frac{m}{d}+km;$$

числа h, k можно выбрать даже натуральными, так как они определяются только с точностью до кратной пары gm, $g\,(p+1)$ с целым g. Тогда, согласно (7),

$$V_{h\,(p+1)}=U_{\frac{m}{d}}V_{km}+U_{km}V_{\frac{m}{d}}.$$

Но, согласно (6), из (10) следует также $V_{h(p+1)}\equiv 0 \bmod p$ и, соответственно, из (8) — также $V_{km}\equiv 0 \bmod p$. Поэтому $U_{km}V_{\frac{m}{d}}\equiv$ $\equiv 0 \bmod p$. Но, как и раньше, вследствие того, что $p\equiv -1 \bmod 4$ и $(x, y)=1$, из $V_{km}\equiv 0 \bmod p$ следует, согласно (3), что обязательно $U_{km}\not\equiv 0 \bmod p$. Поэтому отсюда получается, что $V_{m/d}\equiv 0 \bmod p$.

Согласно (9), последнее возможно только тогда, когда $d=1$. Но это означает, что $(p+1, m)=m$, т. е. $m \mid p+1$ и, таким образом, $p\equiv -1 \bmod m$, что и требовалось доказать.

Кроме доказанного тем самым факта IX, нам нужен здесь, так как речь идет о классе вычетов $-1 \bmod m$, аналог утверждения (5) п. 3 с -1 вместо 1. Для этого мы используем сле-

дующих два свойства многочлена W_m. С одной стороны, для его старшего коэффициента имеет место

$$W_m(1, 0) = \prod_{d \mid m} \left(\frac{m}{d}\right)^{\mu(d)} > 0.$$

Поэтому значения $W_m(x, y)$ при достаточно больших положительных несократимых дробях x/y положительны. Но, с другой стороны, заведомо существует несократимая дробь a/b с отрицательным значением $W_m(a, b)$. Последнее легко следует из (2) и данного перед этим разложения на линейные множители:

$$W_m(x, y) = f_m(x + iy, x - iy) = \prod_{\substack{r \bmod m \\ (r, m) = 1}} [(x + iy) - \zeta^r (x - iy)] =$$
$$= \prod_{\substack{r \bmod m \\ (r, m) = 1}} [(1 - \zeta^r) x + i (1 + \zeta^r) y],$$

в силу которого все корни $\xi_r = i(\zeta^r + 1)/(\zeta^r - 1)$ соответствующего неоднородного многочлена $W_m(x, 1)$ вещественны; в самом деле, для комплексно-сопряженных с ними имеем

$$\bar{\xi}_r = -i \frac{\zeta^{-r} + 1}{\zeta^{-r} - 1} = -i \frac{\zeta^{-r}}{\zeta^{-r}} \cdot \frac{1 + \zeta^r}{1 - \zeta^r} = i \frac{\zeta^r + 1}{\zeta^r - 1} = \xi_r.$$

Так как эти корни ξ_r связаны с первообразными m-ми корнями из 1 посредством однозначно обратимой дробно-линейной подстановки, то все они различны между собой. Будучи многочленом с вещественными коэффициентами, имеющим только простые вещественные корни, $W_m(x, 1)$ при вещественных x принимает значения обоих знаков. Поэтому обязательно существует несократимая дробь a/b с $W_m(a/b, 1) < 0$, тогда также $W_m(a, b) = b^{\varphi(m)} \times$ $\times W_m(a/b, 1) < 0$, что нам и нужно.

Пусть теперь a, b определены указанным образом и пусть, для краткости, положено

$$-W_m(a, b) = w_m,$$

где w_m есть натуральное число. Образуем многочлен

$$Z_m(x) = \frac{1}{w_m} W_m(w_m b x + a, b).$$

Тогда мы действительно имеем в качестве аналога (5) п. 3, что

$$Z_m(0) = -1. \tag{11}$$

Остальные коэффициенты у Z_m, как и у W_m, суть целые числа, в чем тотчас же можно убедиться, располагая $Z_m(x)$ по степеням x. Старший коэффициент у Z_m, как и у W_m, положителен, так что для достаточно больших натуральных x значения $Z_m(x)$ тоже будут натуральными числами. При этом соответствующая пара

$w_m bx + a$, b значений аргументов многочлена W_m будет взаимно простой, так как взаимно просты a, b.

Теперь мы приступаем непосредственно к доказательству теоремы Дирихле для класса вычетов $r \equiv -1 \bmod m$:

X. *Для каждого натурального m существует бесконечно много простых чисел*

$$p \equiv -1 \bmod m.$$

Доказательство. Без ограничения общности можно предположить, что $m \neq 1$, так что имеют место все установленные перед этим факты. Пусть уже известно некоторое количество $r \geqslant 0$ простых чисел $p_0, \ldots, p_{r-1} \equiv -1 \bmod m$. Образуем тогда число

$$Z_m(x_r) = \frac{1}{w_m} W_m(w_m b x_r + a,\ b),$$

где

$$x_r = 4gmp_0 \ldots p_{r-1}.$$

При этом натуральное число g выберем столь большим, чтобы $Z_m(x_r)$ было положительным, а следовательно, натуральным числом. Тогда, согласно (11), это число имеет свойство

$$Z_m(x_r) \equiv -1 \bmod 4mp_0 \ldots p_{r-1}.$$

Так как $Z_m(x_r) \equiv -1 \bmod 4$, оно обладает по крайней мере одним простым делителем $p_r \equiv -1 \bmod 4$. Так как $Z_m(x_r) \equiv -1 \bmod m$, то p_r не входит в m. Таким образом, существует не входящий в m простой делитель $p_r \equiv -1 \bmod 4$ числа $W_m(w_m b x_r + a,\ b)$, причем значения аргументов суть целые взаимно простые числа. Поэтому, согласно IX, $p_r \equiv -1 \bmod m$. Так как $Z_m(x_r) \equiv -1 \bmod p_0 \ldots p_{r-1}$, то p_r отлично от $p_0, \ldots, p_{r-1}$. Таким образом, найдено новое простое число $p_r \equiv -1 \bmod m$.

§ 12. МЕТОД ДИРИХЛЕ

1. Эйлеровское доказательство бесконечности множества простых чисел. Как уже отмечалось, все приведенные в § 11 доказательства частных случаев теоремы Дирихле о простых числах представляют собой обобщения доказательства Евклида из § 1, п. 3 о существовании бесконечного множества простых чисел вообще. В отличие от этого метод доказательства Дирихле для общего случая связан с другим, основанным на совершенно иных соображениях, доказательством бесконечности множества простых чисел, которое было дано Эйлером. Это доказательство существенно опирается на известный из анализа факт, что так называемый *гармонический ряд*, представляющий собой распрост-

раненную на все натуральные числа n сумму $\sum_n 1/n$, расходится, так как для любого натурального ν сумма членов с $2^{\nu-1} \leqslant n < 2^{\nu}$ будет больше, чем $1/2$. Эйлер первым понял связь этого факта с бесконечностью множества всех простых чисел p, связь, которая стала потом играть важную роль в теории чисел благодаря исследованиям Дирихле.

В дальнейшем мы будем кратко обозначать распространенную на все натуральные числа n сумму через $\sum_n$, подобно тому как уже и раньше мы все время обозначали через $\prod_p$ произведение, распространенное на все простые числа p. Если будут накладываться дополнительные условия, например $(n, m) = 1$, $p \nmid m$, то мы будем писать $\sum_{(n,\,m)=1}$, $\prod_{p \nmid m}$.

Открытая Эйлером связь состоит в следующем. По формуле суммы бесконечной геометрической прогрессии мы имеем

$$\frac{1}{1-\frac{1}{p}} = \sum_{\nu=0}^{\infty} \frac{1}{p^{\nu}}.$$

Представим себе, что образовано произведение таких рядов для конечного множества различных простых чисел $p_1, \ldots, p_r$. Так как мы имеем здесь дело с рядами с положительными членами, то почленным перемножением можно получить:

$$\frac{1}{1-\frac{1}{p_1}} \cdots \frac{1}{1-\frac{1}{p_r}} = \sum_{\nu_1, \ldots, \nu_r=0}^{\infty} \frac{1}{p_1^{\nu_1} \cdots p_r^{\nu_r}} = \sum_n{}' \frac{1}{n}. \qquad (1)$$

При этом, в силу основной теоремы об однозначном разложении на простые множители, под знаком суммы получаются обратные величины всех тех натуральных чисел $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$, которые составляются из простых чисел $p_1, \ldots, p_r$ и каждая такая величина получается точно один раз. Пусть на это ограничение при суммировании по n указывает штрих при знаке суммы; согласно (1), эта сумма представляет собой сходящуюся часть гармонического ряда.

Если бы теперь существовало только конечное множество простых чисел $p_1, \ldots, p_r$, то в (1) справа получилась бы сумма обратных величин *всех* натуральных чисел n, т. е. полный гармонический ряд $\sum_n 1/n$. Но так как он расходится, то это противоречит конечности произведения в левой части (1). Следовательно, существует бесконечное множество простых чисел.

Основная идея этого эйлеровского доказательства состоит в том, что для построения бесконечного множества натуральных

чисел n требуется бесконечное же множество «отдельных кирпичей» — простых чисел p. Вообще говоря, подобных заключений делать нельзя, как показывает уже противоречащий пример бесконечного множества всех степеней p^ν одного-единственного простого числа p, или, более обще, аналогичное положение вещей для конечного множества простых чисел $p_1, \ldots, p_r$, с которым мы сталкиваемся в (1). Но это рассуждение делается корректным, если от грубого подсчета самих n перейти к более тонкому рассмотрению суммы их обратных величин, что и делается в доказательстве Эйлера.

Эйлеровское доказательство сразу показывает, что распространенное на все простые числа произведение

$$\prod_p \frac{1}{1-\frac{1}{p}} \text{ расходится.}$$

Заметим попутно, что отсюда следует также, что и распространенная на все простые числа p сумма

$$\sum_p \frac{1}{p} \text{ расходится.} \tag{2}$$

А именно, вообще бесконечное произведение $\prod_{\nu=1}^{\infty} 1/(1-x_\nu)$ с вещественными $x_\nu \geqslant 0$ сходится тогда и только тогда, когда сходится ряд $\sum_{\nu=1}^{\infty} x_\nu$, что следует из двусторонней оценки для логарифмического ряда

$$\ln \frac{1}{1-x} = \frac{x}{1} + \frac{x^2}{2} + \frac{x^3}{3} + \ldots$$

$$\left.\begin{array}{ll} \geqslant x & \text{при } x \geqslant 0 \\ \leqslant x + x^2 + x^3 + \ldots = \dfrac{x}{1-x} \leqslant 2x & \text{при } 0 \leqslant x \leqslant \dfrac{1}{2} \end{array}\right\},$$

а также известно и из основ анализа. Факт (2) можно рассматривать как положительное высказывание, представляющее собой усиление чисто отрицательного высказывания о том, что последовательность простых чисел не обрывается. Согласно (2), простые числа p расположены во множестве всех натуральных чисел n настолько густо, что сумма их обратных величин все еще расходится, как и сумма обратных величин всех натуральных чисел. В этом смысле простые числа расположены, например, гуще, чем квадраты n^2, для которых сумма обратных величин сходится:

$$\sum_n \frac{1}{n^2} = 1 + \sum_n \frac{1}{(n+1)^2} < 1 + \sum_n \frac{1}{n(n+1)} = 1 + \sum_n \left(\frac{1}{n} - \frac{1}{n+1}\right) = 2.$$

Вернемся еще раз к лежащему в основе доказательства Эйлера соотношению (1). Мы будем понимать его как некоторое соотношение между формально понимаемым расходящимся произведением $\prod_p 1/\left(1-1/p\right)$ и формально понимаемым расходящимся рядом $\sum_n 1/n$ и будем выражать это соотношение с помощью особого знака, а именно,

$$\prod_p \frac{1}{1-\frac{1}{p}} \cong \sum_n 1/n. \tag{3}$$

Таким образом, эта запись означает попросту формальное соединение соотношений (1) при всех возможных выборах конечного множества простых чисел $p_1, \ldots, p_r$. При каждом таком выборе часть произведения (конечно, сходящаяся), распространенная на эти простые числа, равна части суммы (также сходящейся), распространенной на все составленные из этих простых чисел натуральные числа $n = p_1^{\nu_1} \ldots p_r^{\nu_r}$. Соотношение (3) называется (*специальным*) *тождеством Эйлера*. Эйлер записывал его с обычным знаком равенства, однако вследствие расходимости обеих частей это равенство можно понимать, конечно, только в указанном выше формальном смысле.

Очевидно, что для вывода (1), а тем самым и (3), из формулы суммы геометрической прогрессии важно только то, что обратная величина $1/n$ есть мультипликативная функция натурального числа n, значения которой лежат в области сходимости $|x| < 1$ геометрической прогрессии при простых значениях аргумента (а потому также и значения для составных n). Поэтому точно таким же способом можно получить понимаемое в таком же смысле (*общее*) *тождество Эйлера*

$$\prod_p \frac{1}{1-f(p)} \cong \sum_n f(n) \tag{4}$$

для каждой мультипликативной теоретико-числовой функции $f(n)$ с вещественными или комплексными значениями, удовлетворяющими условию $|f(n)| < 1$.

Это чисто формальное тождество при известных условиях может иметь значение обычного равенства. А именно, имеет место следующий факт, лежащий в основе всей дальнейшей теории:

I. *Если в общем тождестве Эйлера* (4) *стоящий справа ряд абсолютно сходится, то абсолютно сходится и стоящее слева*

произведение, и обе стороны имеют одно и то же численное значение:

$$\prod_p \frac{1}{1-f(p)} = \sum_n f(n).$$

Доказательство. Пусть S означает сумму, стоящую справа, и пусть для каждого натурального N под P_N понимается частичное произведение из левой части, распространенное на все простые числа $p > N$. Согласно значению тождества (4),

$$|S - P_N| \leqslant \sum_{n'} |f(n')|,$$

где n' пробегает все те натуральные числа, в которые входит хотя бы один простой сомножитель $p > N$. Эти числа n' образуют подмножество всех натуральных чисел $n > N$. Поэтому подавно

$$|S - P_N| \leqslant \sum_{n>N} |f(n)|.$$

Так как, по предположению, стоящая справа сумма при достаточно большом N может быть сделана сколь угодно малой, то отсюда следует, что произведение слева сходится к значению S. Так как абсолютная сходимость бесконечного произведения $\prod_{\nu=1}^{\infty} 1/(1-x_\nu)$ определяется через абсолютную сходимость соответствующего ряда $\sum_{\nu=1}^{\infty} x_\nu$, то в нашем случае имеет место абсолютная сходимость произведения, ибо ряд $\sum_p f(p)$ абсолютно сходится по предположению.

2. Метод доказательства Дирихле для модулей 3 и 4. Дирихле так видоизменил только что изложенный аналитический метод доказательства Эйлера, что он стал применим к простым числам в классах вычетов по $\bmod m$, взаимно простых с модулем, для любого натурального m. Мы поясним сначала метод Дирихле на обоих частных случаях $m = 3, 4$, для которых нами уже были даны элементарные доказательства в § 11, п. 1.

Оба случая $m = 3, 4$ характеризуются тем, что количество рассматриваемых классов вычетов, взаимно простых с модулем, имеет наименьшее возможное нетривиальное значение $\varphi(m) = 2$. Это же имеет место и для $m = 6$; так как, однако, оба класса вычетов $\pm 1 \bmod 6$, взаимно простых с модулем, в области нечетных чисел совпадают с классами вычетов $\pm 1 \bmod 3$, взаимно простыми с модулем, и так как для теоремы Дирихле можно отвлечься от единственного четного простого числа $p = 2$, то для

теоремы Дирихле оба случая $m=3$ и $m=6$ эквивалентны между собой. Это же верно, впрочем, и вообще для каждых двух случаев $m=m_0$ и $m=2m_0$ с нечетным m_0, как мы это уже видели для тривиальных случаев $m=1$ и $m=2$ в § 11, п. 3.

Мы рассмотрим оба случая $m=3, 4$ совместно. Обозначим через

$$\chi(n)=\left\{\begin{array}{c} 1 \text{ при } n\equiv 1 \bmod m \\ -1 \text{ при } n\equiv -1 \bmod m \end{array}\right\}$$

квадратичный характер с ведущим модулем m. В то время как элементарные доказательства в § 11, п. 1, опирались на получающееся из квадратичного закона взаимности представление

$$\chi_n=\left(\frac{-m}{n}\right) \text{ при } n, \text{ взаимно простом с } m, \text{ и } n>0$$

для этого характера, мы обойдемся теперь без привлечения квадратичного закона взаимности, а будем исходить из указанного элементарного значения $\chi(n)$.

Если в общем тождестве Эйлера (4) п. 1 мы выберем в качестве мультипликативной теоретико-числовой функции $f(n)$ с $|f(n)|<1$ сначала функцию

$$f(n)=\frac{1}{n} \text{ при } (n, m)=1, \quad f(n)=0 \text{ в противном случае,}$$

а затем функцию

$$f(n)=\frac{\chi(n)}{n} \text{ при } (n, m)=1, \quad f(n)=0 \text{ в противном случае,}$$

то, подобно специальному тождеству Эйлера (3) п. 1, получим следующих два тождества:

$$\left\{\begin{array}{l} \prod\limits_{p\nmid m}\dfrac{1}{1-\dfrac{1}{p}}\cong\sum\limits_{(n, m)=1}\dfrac{1}{n} \\ \prod\limits_{p\nmid m}\dfrac{1}{1-\dfrac{\chi(p)}{p}}\cong\sum\limits_{(n, m)=1}\dfrac{\chi(n)}{n} \end{array}\right\}, \tag{1}$$

которые можно также записать в виде

$$\left\{\begin{array}{l} \prod\limits_{p\equiv 1 \bmod m}\dfrac{1}{1-\dfrac{1}{p}}\cdot\prod\limits_{p\equiv -1 \bmod m}\dfrac{1}{1-\dfrac{1}{p}}\cong\sum\limits_{(n, m)=1}\dfrac{1}{n} \\ \prod\limits_{p\equiv 1 \bmod m}\dfrac{1}{1-\dfrac{1}{p}}\cdot\prod\limits_{p\equiv -1 \bmod m}\dfrac{1}{1+\dfrac{1}{p}}\cong\sum\limits_{(n, m)=1}\dfrac{\chi(n)}{n} \end{array}\right\}.$$

Из них, умножая и деля их друг на друга, мы получаем

$$\left.\begin{aligned} &\prod_{p\equiv 1 \bmod m}\left(\frac{1}{1-\frac{1}{p}}\right)^2 \cdot \prod_{p\equiv -1 \bmod m}\frac{1}{1-\frac{1}{p^2}} \cong \sum_{(n,\,m)=1}\frac{1}{n}\cdot\sum_{(n,\,m)=1}\frac{\chi(n)}{n} \\ &\frac{\prod\limits_{p\equiv -1 \bmod m}\frac{1}{1-\frac{1}{p}}}{\prod\limits_{p\equiv -1 \bmod m}\frac{1}{1+\frac{1}{p}}} \cong \frac{\sum\limits_{(n,\,m)=1}\frac{1}{n}}{\sum\limits_{(n,\,m)=1}\frac{\chi(n)}{n}}. \end{aligned}\right\} \quad (2)$$

Эти соотношения, согласно их происхождению, означают следующее. Выберем какое-нибудь конечное множество $\mathfrak{P}$ простых чисел и распространим произведения слева на все простые числа обоих сортов $p \equiv \pm 1 \bmod m$ из $\mathfrak{P}$, а суммы справа—на все те взаимно простые с m натуральные числа n, в которые входят только простые числа из $\mathfrak{P}$. Тогда каждый раз выражения слева равны выражениям справа. Представим себе теперь, что в качестве $\mathfrak{P}$ выбрано множество $\mathfrak{P}_N$ всех простых чисел $p < N$ для какого-нибудь натурального N, и обозначим через $\mathfrak{M}_N$ множество всех натуральных чисел, в которые входят только простые числа из $\mathfrak{P}$. Так как в $\mathfrak{M}_N$ заведомо содержатся все $n \leqslant N$, то при достаточно большом N члены частичных сумм

$$\sum_{\substack{(n,\,m)=1\\ n\in\mathfrak{M}_N}}\frac{1}{n}, \qquad \sum_{\substack{(n,\,m)=1\\ n\in\mathfrak{M}_N}}\frac{\chi(n)}{n}, \quad (3)$$

стоящих в правых частях тождеств (2), сколь угодно далеко совпадают с членами рядов

$$\sum_{(n,\,m)=1}\frac{1}{n}, \qquad \sum_{(n,\,m)=1}\frac{\chi(n)}{n}, \quad (4)$$

распространенных на *все* взаимно простые с m натуральные n.

Ряд

$$\sum_{(n,\,m)=1}\frac{1}{n} = \left\{\begin{aligned} &\frac{1}{1}+\frac{1}{2}+\frac{1}{4}+\frac{1}{5}+\ldots && \text{при } m=3 \\ &\frac{1}{1}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\ldots && \text{при } m=4 \end{aligned}\right\} \text{ расходится; } (4_1)$$

действительно, при его почленном перемножении со сходящейся геометрической прогрессией

$$\frac{1}{1-\frac{1}{3}} = \sum_{\nu=0}^{\infty}\frac{1}{3^\nu}, \quad \text{соответственно} \quad \frac{1}{1-\frac{1}{2}} = \sum_{\nu=0}^{\infty}\frac{1}{2^\nu},$$

получается полный гармонический ряд $\sum_n 1/n$, так что из его сходимости следовала бы и сходимость гармонического ряда. Напротив, ряд

$$\sum_{(n,m)=1} \frac{\chi(n)}{n} = \begin{cases} \frac{1}{1} - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} \pm \dots & \text{при } m=3 \\ \frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \pm \dots & \text{при } m=4 \end{cases} \text{ сходится к сумме, } \neq 0, \quad (4_2)$$

как знакопеременный ряд с монотонно стремящимися к 0 членами. Вследствие расходимости ряда (4_1), ряд (4_2) сходится не абсолютно, а только условно, так что его сумма зависит от порядка следования его членов. Когда здесь говорится, что его сумма $\neq 0$, то, как и всегда в дальнейшем, имеется в виду натуральный порядок расположения его членов.

В силу установленного, приведенное выше сравнение частичных сумм (3) с полными рядами (4) показывает, с одной стороны, что

$$\lim_{N\to\infty} \sum_{\substack{(n,m)=1 \\ n\in\mathfrak{M}_N}} \frac{1}{n} = \infty \qquad (3_1)$$

и, с другой стороны, делает весьма вероятным, что соответственно $\lim_{N\to\infty} \sum_{\substack{(n,m)=1 \\ n\in\mathfrak{M}_N}} \frac{\chi(n)}{n}$ существует и $\neq 0$, а именно, $= \sum_{(n,m)=1} \frac{\chi(n)}{n}$, (3_2)

если рассматривать натуральный порядок расположения членов. В то время как соотношение (3_1), ввиду положительности членов, очевидно, соотношение (3_2) еще не доказано; действительно, здесь речь идет об условно сходящихся рядах, из которых выхватываются частичные суммы, которые хотя и исчерпывают при $N \to \infty$ все члены этих рядов, но не в их натуральной последовательности.

Предположим, что наряду с (3_1) верно также и (3_2). Тогда, выбирая множество простых чисел $\mathfrak{P} = \mathfrak{P}_N$ с достаточно большим N, можно сделать сколь угодно большими правые части обоих тождеств (2). Поэтому при сделанном предположении из второго тождества немедленно следует, что существует бесконечно много простых чисел $p \equiv -1 \bmod m$, а из первого тождества точно так же будет следовать, что существует бесконечно много простых чисел $p \equiv 1 \bmod m$, если только установить еще, что входящее дополнительно в правую часть этого тождества произведение $\prod_{p\equiv -1 \bmod m} 1/(1-1/p^2)$ сходится. Но, согласно тождеству Эйлера,

для полного произведения имеет место

$$\prod_p \frac{1}{1-\frac{1}{p^2}} \cong \sum_n \frac{1}{n^2},$$

и стоящий справа ряд сходится, как было показано выше в п. 1. Поэтому, согласно I, п. 1, сходится и стоящее слева произведение, а его часть, о которой идет речь,—и подавно.

Таким образом, аналитическое доказательство теоремы Дирихле о простых числах для модулей $m = 3, 4$ сводится к доказательству предельного соотношения (3_2). Как видно из рассуждений, с помощью которых мы получили это соотношение, оно может быть записано также в виде

$$\prod_{p \nmid m} \frac{1}{1-\frac{\chi(p)}{p}} = \sum_{(n,m)=1} \frac{\chi(n)}{n}, \tag{5}$$

причем с обеих сторон подразумевается натуральный порядок расположения членов. Это есть соответствующее второму из формальных тождеств (1) обычное равенство; оно означает, что стоящее слева бесконечное произведение (условно) сходится и что его значение совпадает с суммой (условно) сходящегося бесконечного ряда, стоящего справа.

Соотношение (5) действительно оказывается справедливым. Однако его доказательство нельзя получить теми простыми аналитическими средствами, которыми мы пользовались до сих пор. Эта трудность и побудила Дирихле развить новый аналитический метод, к которому мы теперь и переходим. При этом необходимость доказывать соотношение (5) отпадает. То, что оно действительно верно, вытекает из этого метода только впоследствии, окольным путем. Однако в рамках этой книги мы должны отказаться от этого доказательства, так как для него необходимо одно из нетривиальных утверждений закона распределения простых чисел (см. конец п. 5).

3. Подход Дирихле к доказательству общего случая теоремы. Изложенный в п. 2 подход к доказательству теоремы Дирихле о простых числах для частных случаев $m = 3, 4$, основную идею которого мы пояснили в п. 1 на примере эйлеровского доказательства в случае $m = 1$, был видоизменен Дирихле таким образом, что его стало возможным применить и к общему случаю, причем можно избежать указанной нами в конце п. 2 трудности. Это достигается с помощью двух существенно различных приемов, которые мы сначала обрисуем в общих чертах, не вдаваясь в их доказательства.

Первый из этих приемов носит *аналитический* характер. Благодаря нему можно обойти трудность, с которой мы столкнулись

в конце п. 2. Этот прием можно проиллюстрировать уже на примере эйлеровского доказательства из п. 1, т. е. для частного случая $m = 1$. Вместо того, чтобы оперировать с расходящимся гармоническим рядом $\sum_n 1/n$, мы будем рассматривать ряд $\sum_n 1/n^s$, сходящийся для всех вещественных $s > 1$. Вместо постепенного исчерпывания членов ряда $\sum_n 1/n$ посредством предельного перехода $N \to \infty$ для множества $\mathfrak{P}_N$ всех простых чисел $p \leqslant N$, здесь мы будем производить предельный переход $s \to 1 + 0$ для ряда $\sum_n 1/n^s$. Таким образом, мы будем исходить из тождества Эйлера

$$\prod_p \frac{1}{1 - \frac{1}{p^s}} \cong \sum_n \frac{1}{n^s}$$

с вещественным параметром s, в котором (если доказать сходимость стоящего справа ряда) можно, согласно I, п. 1, поставить при $s > 1$ обычный знак равенства, а затем с обеих сторон произведем предельный переход $s \to 1 + 0$. Это мы выполним в п. 4.

Второй прием носит *алгебраический* характер. Он состоит в выделении отдельных классов вычетов по $\bmod m$, взаимно простых с модулем, из множества всех натуральных чисел n, взаимно простых с m. В частных случаях $m = 3$, 4 для этого используются характеры

$$\varepsilon(n) = 1 \quad \text{для всех } n, \text{ взаимно простых с } m,$$
$$\chi(n) = \pm 1 \quad \text{в зависимости от } n \equiv \pm 1 \bmod m,$$

и с их помощью образуются тождества Эйлера (1) п. 2; тогда выделение, о котором идет речь, достигается с помощью перемножения и деления этих равенств в форме (2) п. 2. Так как группа классов вычетов по $\bmod m$, взаимно простых с модулем, имеет здесь порядок $\varphi(m) = 2$, то оба эти характера ε, χ составляют, очевидно, совокупность всех характеров по $\bmod m$. В общем случае используются все характеры χ группы классов вычетов по $\bmod m$, взаимно простых с модулем; их теория подробно изложена в § 13. Тогда мы придем к рассмотрению тождеств Эйлера

$$\prod_{p \nmid m} \frac{1}{1 - \frac{\chi(n)}{p^s}} \cong \sum_{(n, m) = 1} \frac{\chi(n)}{n^s},$$

в которых, согласно I, п. 1, снова можно поставить обычный знак равенства, если $s > 1$.

Доказательство теоремы Дирихле получается тогда, как мы увидим в § 14, с помощью по существу тех же основных идей,

которые использовались в п. 2 для частных случаев $m = 3, 4$. Появляющаяся там в конце трудность, а именно, доказательство того, что написанные выше тождества Эйлера (за исключением того, в котором фигурирует так называемый главный характер $\chi = \varepsilon$) также и для $s = 1$ имеют силу как обычные равенства (5) п. 2, обходится, как уже сказано, посредством сделанной Дирихле замены предельного перехода $N \to \infty$ предельным переходом $s \to 1 + 0$. А именно, это доказательство гораздо проще получается из того, что имеют место предельные соотношения

$$\lim_{s \to 1+0} \sum_{(n, m)=1} \frac{\chi(n)}{n^s} = \sum_{(n, m)=1} \frac{\chi(n)}{n} \qquad (\chi \neq \varepsilon).$$

Однако в общем случае при этом появляется новая трудность. Для специальных квадратичных характеров $\chi \neq \varepsilon$ из п. 2 непосредственно видно, что

$$\sum_{(n, m)=1} \frac{\chi(n)}{n} \neq 0,$$

и этот факт имеет решающее значение при проведении доказательства, опирающегося на изложенные нами основные идеи; но в общем случае необращение в нуль этих сумм отнюдь не является очевидным. Тогда уже не получаются знакопеременные ряды; напротив, значения характера $\chi(n)$ будут комплексными корнями из 1, которые или не все вещественны, или все равны ± 1, причем в последнем (самом трудном) случае оба значения $\chi(n) = \pm 1$, вообще говоря, уже не чередуются в области взаимно простых с m чисел n, а лишь периодически повторяются с периодом m. Для таких рядов уже нельзя доказать их необращение в нуль таким простым способом, как для специальных характеров $\chi \neq \varepsilon$ из п. 2.

Эту основную трудность в доказательстве можно преодолеть различными способами, однако при этом всегда потребуются или сложные вычисления и оценки элементарно-аналитического характера, или глубокие методы теории функций комплексного переменного или теории алгебраических чисел. Об этом мы будем говорить подробно в § 15.

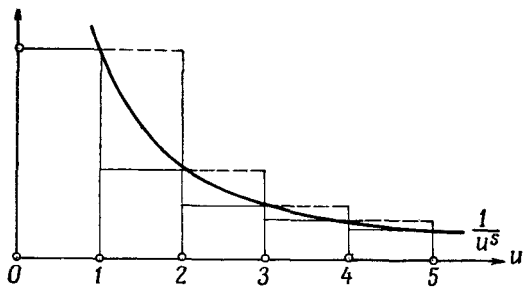
4. Дзета-ряд и видоизменение эйлеровского доказательства, сделанное Дирихле. В связи с первым из описанных в п. 3 аналитическим усовершенствованием эйлеровского доказательства нам надо рассмотреть ряд

$$\zeta(s) = \sum_n \frac{1}{n^s}.$$

В самом общем виде, как функция комплексного переменного s, этот ряд был введен в аналитическую теорию чисел Риманом; он

используется в далеко идущих исследованиях о распределении простых чисел. Он обозначается введенным Риманом знаком ζ и называется дзета-функцией Римана. Для наших целей достаточно (за исключением § 15, п. 4) ограничиться рассмотрением вещественных значений переменной s, как это делает Дирихле; кроме того, нам нужно делать упор не на свойства этого выражения как функции от s, как делал Риман, а на свойства его как бесконечного ряда; поэтому мы будем говорить здесь о дзета-ряде.

Вследствие расходимости гармонического ряда дзета-ряд расходится при $s=1$, а потому и подавно при $s<1$. Сейчас мы



Фиг. 3.

простым способом докажем, что для всех $s>1$ этот ряд сходится, и даже покажем несколько больше. Для этого мы рассмотрим члены $1/n^s$ как значения функции $1/u^s$ с вещественным $u>0$ для натуральных чисел $u=n$, а s — как параметр. Если $s>0$, то в области $u>0$ функция $1/u^s$ монотонно убывает. Поэтому имеют место неравенства

$$\int_n^{n+1}\frac{du}{u^s}<\frac{1}{n^s}<\int_{n-1}^{n}\frac{du}{u^s},$$

причем левое для $n\geqslant 1$, а правое для $n\geqslant 2$ (фиг. 3). Отсюда посредством суммирования следует

$$\int_1^{\infty}\frac{du}{u^s}<\zeta(s)<1+\int_1^{\infty}\frac{du}{u^s},$$

т. е. получается сходимость дзета-ряда и оценка с обеих сторон для его значения, если доказать, что сходится фигурирующий здесь несобственный интеграл. Для конечного верхнего предела $t>0$ мы имеем

$$\int_1^t\frac{du}{u^s}=\int_1^t u^{-s}\,du=\left\{\begin{array}{ll}\dfrac{u^{1-s}}{1-s}\Big|_1^t=\dfrac{t^{1-s}}{1-s}-\dfrac{1}{1-s} & \text{для } s\neq 1\\ \ln t & \text{для } s=1\end{array}\right\}.$$

Поэтому интеграл с бесконечным верхним пределом расходится при $s \leqslant 1$ и сходится к значению

$$\int_1^\infty \frac{du}{u^s} = \frac{1}{s-1} \qquad \text{при} \quad s > 1.$$

Первое дает нам новое доказательство расходимости гармонического ряда, второе — сходимость дзета-ряда при $s > 1$, и, кроме того, конкретную оценку

$$\frac{1}{s-1} < \zeta(s) < 1 + \frac{1}{s-1}. \tag{1}$$

Если записать эту оценку в виде

$$1 < (s-1)\zeta(s) < s,$$

то мы получим предельное соотношение

$$\lim_{s \to 1+0} (s-1)\zeta(s) = 1 \tag{1'}$$

при s, стремящемся к 1 справа.

Итак, мы установили:

II. *Дзета-ряд* $\zeta(s) = \sum_n 1/n^s$ *при вещественных* s *сходится в области* $s > 1$. *Если* s *стремится справа к* 1, *то* $\zeta(s)$ *стремится к* ∞ *и притом так, что имеют место неравенства* (1) *и вытекающее из них предельное соотношение* (1').

Таким образом, при предельном переходе $s \to 1+0$, $\zeta(s)$ является бесконечностью того же порядка, что и $1/(s-1)$, и притом это имеет место не только в грубом смысле (1'), означающем, что отношение $\zeta(s) : 1/(s-1)$ стремится к 1 (т. е. что имеет место так называемое асимптотическое равенство), но, согласно (1), и в более сильном смысле, а именно, остается ограниченной разность $\zeta(s) - 1/(s-1)$. Для выражения этого последнего обстоятельства мы введем сокращенное обозначение

$$\zeta(s) \approx \frac{1}{s-1}, \tag{2}$$

которое будем всегда применять при предельном переходе $s \to 1+0$ в указанном смысле. Тем самым мы избавляемся (аналогично тому, как при сокращенном способе записи для сравнимости в элементарной теории чисел) от необходимости подробно выписывать те выражения, которые для наших заключений не будут играть роли, и получаем возможность сосредоточить наше внимание на существенном. Предельное соотношение $\approx$ для вещественной переменной s является соотношением того типа, который соответствует при аналитическом усовершенствовании доказательства Эйлера предельному соотношению $\cong$ для натураль-

ной переменной N. В литературе вместо (2) часто употребляется запись $\zeta(s) - 1/(s-1) = O(1)$.

Вследствие мультипликативности теоретико-числовой функции $1/n^s$ для нее имеет место общее тождество Эйлера (4) п. 1 с $f(n) = 1/n^s$ $(s > 0)$. Так как дзета-ряд сходится (и притом, конечно, абсолютно) при $s > 1$, мы, в силу I, п. 1, получаем играющее в аналитической теории чисел основную роль представление дзета-ряда в виде (абсолютно) сходящегося бесконечного произведения:

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}} \qquad \text{для } s > 1, \tag{3}$$

в котором коренится значение дзета-ряда для теории простых чисел.

Для доказательства Дирихле удобнее пользоваться логарифмами рядов, потому что таким образом мы от произведений переходим к суммам, с которыми проще оперировать при предельном переходе. Согласно (3),

$$\ln \zeta(s) = \sum_p \ln \frac{1}{1 - \frac{1}{p^s}} = \sum_p \sum_{\nu=1}^{\infty} \frac{1}{\nu} \frac{1}{p^{\nu s}}.$$

В стоящих справа двойных суммах при предельном переходе $s \to 1 + 0$ можно пренебрегать в смысле $\approx$ членами с $\nu \geqslant 2$. В самом деле, для суммы этих членов имеет место

$$\sum_p \sum_{\nu=2}^{\infty} \frac{1}{\nu} \frac{1}{p^{\nu s}} < \frac{1}{2} \sum_p \sum_{\nu=2}^{\infty} \frac{1}{p^{\nu s}} = \frac{1}{2} \sum \frac{\frac{1}{p^{2s}}}{1 - \frac{1}{p^s}} <$$

$$< \frac{1}{2} \sum_p \frac{\frac{1}{p^{2s}}}{1 - \frac{1}{2^1}} = \sum_p \frac{1}{p^{2s}} < \zeta(2s) < \zeta(2),$$

т. е. она ограничена. Таким образом, мы имеем предельное соотношение

$$\ln \zeta(s) \approx \sum_p \frac{1}{p^s}. \tag{4}$$

В этом предельном соотношении и заключается видоизменение эйлеровского доказательства из п. 1, которое дает аналитический метод Дирихле. Посредством перехода к логарифму из (2) или даже из более грубого предельного соотношения (1′) следует

$$\ln \zeta(s) \approx \ln \frac{1}{s-1}.$$

Поэтому, согласно (4), имеет место также

$$\sum_p \frac{1}{p^s} \approx \ln \frac{1}{s-1}\,. \tag{5}$$

Так как правая часть при $s \to 1+0$ стремится к бесконечности, это же должно иметь место и для левой части. Поэтому должно существовать бесконечное множество простых чисел. Мы видим, как при этом видоизменении доказательства использование расходящегося гармонического ряда ($s=1$) и рассмотрение его частичных сумм заменяется рассмотрением дзета-ряда в его области сходимости $s>1$ и предельным переходом $s \to 1+0$.

5. Замечания относительно закона распределения простых чисел. Отметим, что предельное соотношение (4) служит также исходным пунктом для доказательства основной теоремы о распределении простых чисел, или так называемого закона распределения простых чисел:

$$\pi(N) \sim \frac{N}{\ln N}\,, \tag{6}$$

согласно которому количество $\pi(N)$ простых чисел $p \leqslant N$ асимптотически равно элементарной функции $N/\ln N$, т. е. выполняется предельное соотношение

$$\lim_{N\to\infty} \frac{\pi(N)}{N/\ln N} = 1.$$

Вывод (6) из (5) в принципе очень ясен, однако для подробного изложения довольно труден.

Рассмотрим ряды следующего общего типа:

$$f(s) = \sum_n \frac{a_n}{n^s}$$

с какими-нибудь коэффициентами a_n. Такие ряды называются рядами Дирихле. Дзета-ряд представляет собой простейший частный случай ряда Дирихле (все $a_n = 1$), подобно тому как геометрическая прогрессия $\sum_{\nu=0}^{\infty} x^\nu$ является простейшим частным случаем степенного ряда. Каждому ряду Дирихле сопоставляется частичная сумма его коэффициентов

$$S(N) = \sum_{n\leqslant N} a_n$$

как функция от N. Для специального ряда Дирихле $f(s) = \sum_p \frac{1}{p^s}$ из (5) (для которого $a_n = 1$ или 0 в зависимости от того, является

ли n простым числом или нет) мы для частичной суммы коэффициентов получаем как раз $S(N) = \pi(N)$.

Из предельного поведения частичной суммы коэффициентов $S(N)$ при $N \to \infty$ сравнительно просто сделать в самом общем виде заключение о предельном поведении $f(s)$ при $s \to 1+0$. Это достигается посредством переноса на ряды Дирихле высказываний типа известной теоремы Абеля о непрерывности для степенных рядов. При таком переносе (5) оказывается следствием из (6). Чтобы, наоборот, получить (6) как следствие из (5), надо обратить эту обобщенную теорему Абеля о непрерывности таким образом, чтобы из предельного поведения функции $f(s)$ при $s \to 1+0$ можно было сделать заключение о предельном поведении частичной суммы коэффициентов $S(N)$ при $N \to \infty$. Это возможно сделать уже не в самых общих предположениях, а лишь при некоторых дополнительных условиях относительно коэффициентов a_n, однако для того специального случая, который нужен для закона распределения простых чисел, это сделать можно. При этом нельзя обойтись только методами вещественного анализа, а необходимо привлечь интегральную теорему Коши или эквивалентную ей формулу для интеграла комплексного переменного

Мы ограничимся этими указаниями. Кроме закона распределения простых чисел аналитическая теория чисел исследует еще вопрос о точном порядке возрастания ошибки в (6). Основным подходом к решению этой задачи является идущее от Римана глубокое изучение $\zeta(s)$ как функции комплексного переменного s.

§ 13. ХАРАКТЕРЫ КОНЕЧНЫХ АБЕЛЕВЫХ ГРУПП. ХАРАКТЕРЫ ПО МОДУЛЮ

1. Определение характеров и доказательство их существования. Теперь мы переходим ко второму из описанных в § 12, п. 3, алгебраическому усовершенствованию эйлеровского доказательства, сделанному Дирихле. Сначала мы изложим общую теорию характеров конечных абелевых групп, а затем специально нужную для нашей цели теорию характеров групп классов вычетов, взаимно простых с модулем, причем в обоих случаях несколько подробнее, чем это необходимо непосредственно для доказательства теоремы Дирихле о простых числах.

Пусть $\mathfrak{A}$ – абелева группа конечного порядка n. Под характером χ группы $\mathfrak{A}$ понимается функция элементов A групп $\mathfrak{A}$, обладающая свойствами

$$\chi(AB) = \chi(A)\chi(B), \tag{1}$$

$$\chi(A) \neq 0, \tag{2}$$

т. е. мультипликативная функция элементов A группы $\mathfrak{A}$, значения которой все отличны от нуля; областью значений этой функции мы будем считать здесь поле комплексных чисел.

Вместо (2) достаточно требовать только существования одного элемента A из $\mathfrak{A}$, для которого $\chi(A) \neq 0$. Для единичного элемента E группы $\mathfrak{A}$ из мультипликативности (1) следует

$$\chi(A) = \chi(AE) = \chi(A)\chi(E)$$

для каждого A из $\mathfrak{A}$; так как $\chi(A) \neq 0$ (по крайней мере для одного A), то отсюда получается

$$\chi(E) = 1.$$

Так как, далее, для каждого элемента A из $\mathfrak{A}$ имеет место $A^n = E$, то, согласно (1), все значения χ удовлетворяют равенству

$$\chi(A)^n = 1,$$

т. е. являются n-ми корнями из 1 (и потому все отличны от 0).

Если характеры χ группы $\mathfrak{A}$ перемножать как функции, т. е. под $\chi\psi$ понимать функцию со значениями $\chi(A)\psi(A)$, то характеры сами образуют абелеву группу, называемую группой характеров группы $\mathfrak{A}$. Действительно, произведение $\chi\psi$, так же как и соответствующим образом определенное частное χ/ψ, снова является всюду отличной от нуля мультипликативной функцией элементов из $\mathfrak{A}$. Главным характером называется единичный элемент ε группы характеров $\mathfrak{X}$, имеющий значения

$$\varepsilon(A) = 1 \quad \text{для всех } A \text{ из } \mathfrak{A}.$$

До сих пор было установлено существование только этого главного характера ε. Теперь мы докажем

I. *Абелева группа $\mathfrak{A}$ порядка n имеет точно n различных характеров χ, т. е. ее группа характеров тоже имеет порядок n.*

Доказательство. Рассмотрим начинающуюся с единичной подгруппы $\mathfrak{E}$ и оканчивающуюся самой группой $\mathfrak{A}$ последовательность

$$\mathfrak{E} = \mathfrak{U}_0 < \mathfrak{U}_1 < \ldots < \mathfrak{U}_s = \mathfrak{A}$$

подгрупп группы $\mathfrak{A}$, выбранную таким образом, что факторгруппы $\mathfrak{U}_i/\mathfrak{U}_{i-1}$ $(i = 1, \ldots, s)$ цикличны. Чтобы получить такую последовательность подгрупп, нужно только, исходя из $R_0 = E$, выбрать такую последовательность элементов $R_1, \ldots, R_s$ из $\mathfrak{A}$, что R_i каждый раз не содержится в порожденной элементами $R_0, \ldots, R_{i-1}$ подгруппе $\mathfrak{U}_{i-1}$. Тогда доказательство I получается s-кратным применением следующего предложения:

Лемма. *Если $\mathfrak{U}$ есть подгруппа индекса k группы $\mathfrak{A}$ с циклической фактор-группой $\mathfrak{A}/\mathfrak{U}$, то каждый характер χ подгруппы $\mathfrak{U}$ может быть продолжен точно k различными способами до характера группы $\mathfrak{A}$.*

Доказательство. Пусть R есть представитель класса, порождающего фактор-группу $\mathfrak{A}/\mathfrak{U}$. Тогда каждый элемент A из $\mathfrak{A}$ можно однозначно представить в виде

$$A = R^{\varkappa}U \quad (\varkappa = 0,\ 1,\ \ldots,\ k-1,\ U \text{ из } \mathfrak{U}),$$

и при этом

$$R^k = C$$

является элементом из $\mathfrak{U}$. В силу этого соотношения операции над элементами A из $\mathfrak{A}$ полностью определяются операциями над элементами U из $\mathfrak{U}$ и соотношением $R^k = C$.

Очевидно, что каждый характер χ группы $\mathfrak{A}$ является продолжением некоторого характера подгруппы $\mathfrak{U}$ и при этом каждое значение характера $\chi(R)$ есть корень уравнения

$$\chi(R)^k = \chi(C).$$

Если, наоборот, задать характер χ подгруппы $\mathfrak{U}$ и выбрать какое-нибудь конкретное значение $\chi(R)$ из k корней этого уравнения, то посредством формулы

$$\chi(A) = \chi(R)^{\varkappa}\chi(U)$$

определяется продолжение характера χ до функции, определенной на всей группе $\mathfrak{A}$. При этом, в силу выбора $\chi(R)$ из каждого соотношения $A'A'' = A$ в $\mathfrak{A}$ вытекает соответствующее соотношение $\chi(A')\ \chi(A'') = \chi(A)$ для значений функции χ. Поэтому определенное нами продолжение является характером группы $\mathfrak{A}$. Мы получаем таким образом k различных продолжений, соответствующих k различным корням $\chi(R)$. Тем самым лемма доказана. Как уже было сказано, из нее вытекает правильность утверждения 1.

2. Соотношения между характерами. Пусть χ есть характер группы $\mathfrak{A}$. Рассмотрим сумму

$$S = \sum_A \chi(A),$$

распространенную на все элементы A из $\mathfrak{A}$. Если B — какой-нибудь элемент из $\mathfrak{A}$, то

$$S \cdot \chi(B) = \sum_A \chi(AB) = \sum_A \chi(A) = S,$$

так как при постоянном B вместе с A также и AB пробегает все элементы группы $\mathfrak{A}$, причем каждый точно один раз. Если $\chi \neq \varepsilon$, то B может быть выбрано так, что $\chi(B) \neq 1$; тогда получится $S = 0$. Если $\chi = \varepsilon$, то все время $\chi(A) = \varepsilon(A) = 1$ и, таким

образом, $S=n$. Мы получаем, следовательно, n соотношений

$$\sum_A \chi(A) = \begin{cases} n & \text{для } \chi=\varepsilon \\ 0 & \text{для } \chi\neq\varepsilon \end{cases}. \tag{1}$$

Чтобы получить из них дальнейшие соотношения между характерами, мы прежде всего заметим следующее. Вместе с каждым характером χ в группе $\mathfrak{X}$ встречается также комплексно сопряженный с ним характер $\bar{\chi}$. Так как для каждого корня из 1, ζ имеет место $\bar{\zeta}=\zeta^{-1}$ (вследствие того, что $|\zeta|^2=\zeta\bar{\zeta}=1$), то

$$\bar{\chi}=\chi^{-1}, \text{ откуда } \bar{\chi}(A)=\chi^{-1}(A)=\chi(A^{-1}),$$

т. е. комплексно сопряженный характер $\bar{\chi}$ равен χ^{-1}, и его значения получаются посредством замены аргументов A на обратные к ним A^{-1}.

Если соотношения (1) применить к частному двух характеров χ, ψ, то получится n^2 соотношений

$$\sum_A \chi(A)\bar{\psi}(A) = \begin{cases} n & \text{для } \chi=\psi \\ 0 & \text{для } \chi\neq\psi \end{cases}. \tag{2}$$

Запишем теперь n^2 значений $\chi(A)$ характеров χ из $\mathfrak{X}$ в виде n строк квадратной матрицы

$$\mathfrak{C}=(\chi(A)) \begin{cases} \text{индексами строк служат } \chi \text{ из } \mathfrak{X} \\ \text{индексами столбцов служат } A \text{ из } \mathfrak{A} \end{cases}$$

из n^2 элементов, у которой в каждом столбце стоят n значений различных характеров при постоянном A из $\mathfrak{A}$. Тогда соотношения (2) равносильны матричному равенству

$$\mathfrak{C}\bar{\mathfrak{C}}'=n\mathfrak{E}, \tag{3}$$

где $\bar{\mathfrak{C}}'$ обозначает транспонированную комплексно сопряженную матрицу и $\mathfrak{E}$ — n-строчную единичную матрицу. Поэтому матрица $\mathfrak{C}$ невырожденная, для квадрата абсолютной величины ее детерминанта получается

$$\|\mathfrak{C}\|^2=n^n,$$

и обратная справа матрица удовлетворяет соотношению

$$\left(\frac{1}{\sqrt{n}}\mathfrak{C}\right)^{-1}=\frac{1}{\sqrt{n}}\bar{\mathfrak{C}}', \tag{4}$$

т. е. матрица $(1/\sqrt{n})\,\mathfrak{C}$ унитарна.

Как известно из линейной алгебры, правая обратная некоторой невырожденной матрицы является одновременно и левой обратной. Поэтому из равенства (3) следует другое матричное равенство

$$\bar{\mathfrak{C}}'\mathfrak{C}=n\mathfrak{E}. \tag{3'}$$

Оно означает, что выполняются также n^2 соотношений

$$\sum_{\chi} \chi(A)\,\bar{\chi}(B) = \begin{cases} n & \text{для} \quad A = B \\ 0 & \text{для} \quad A \neq B \end{cases} \qquad (2')$$

для каждых двух элементов A, B из $\mathfrak{A}$, причем суммирование распространяется на все характеры χ из $\mathfrak{X}$. Из них специально для $B = E$ следуют n соотношений

$$\sum_{\chi} \chi(A) = \begin{cases} n & \text{для} \quad A = E \\ 0 & \text{для} \quad A \neq E \end{cases}. \qquad (1')$$

Соотношения (2), (2′) называются также соотношениями ортогональности для характеров, потому что они показывают, что каждые две различные строки или два различных столбца матрицы $\mathfrak{C}$ ортогональны между собой в смысле обычной ортогональности комплексных векторов. В большинстве случаев используются только специальные соотношения (1), (1′), из которых общие соотношения ортогональности тотчас же следуют, если χ, соответственно A заменить отношением χ/ψ, соответственно A/B.

Для наших применений к доказательству теоремы Дирихле о простых числах важен следующий факт, который немедленно получается из матричного равенства (4) или также обычным в линейной алгебре способом из соотношений ортогональности (2), (2′):

II. *Решения x_A системы линейных уравнений*

$$\sum_{A} \chi(A)\, x_A = y_\chi$$

при заданных y_χ однозначно определяются в виде системы линейных уравнений

$$x_A = \frac{1}{n} \sum_{\chi} \bar{\chi}(A)\, y_\chi,$$

и обратно.

3. Принцип двойственности. Мы докажем еще несколько фактов из теории характеров конечных абелевых групп, которые хотя и не нужны для доказательства теоремы Дирихле о простых числах, но образуют алгебраический фундамент других, частично уже встречавшихся теоретико-числовых приложений характеров.

Как следует из определения характеров и их умножения, $\chi(A)$ не только при постоянном χ и переменном A является характером группы $\mathfrak{A}$, но и, наоборот, при постоянном A и переменном χ является характером группы $\mathfrak{X}$. Поэтому рассматриваемая в п. 2 матрица $\mathfrak{C} = (\chi(A))$, составленная из значений характеров, не только имеет своими строками системы значе-

ний n различных характеров χ группы $\mathfrak{A}$, но также имеет своими столбцами системы значений n характеров группы $\mathfrak{X}$. Вследствие невырожденности $\mathfrak{Z}$ последние n характеров также различны и потому, согласно I, п. 1, образуют полную систему характеров группы $\mathfrak{X}$. Они взаимно однозначно сопоставляются элементам A из $\mathfrak{A}$, играющим здесь роль функций от аргумента χ, и умножение их как функций соответствует умножению элементов A из $\mathfrak{A}$. Таким образом, имеет место:

III. *Если $\mathfrak{X}$ есть группа характеров группы $\mathfrak{A}$, то $\mathfrak{A}$ в свою очередь можно понимать как группу характеров группы $\mathfrak{X}$, если в значениях характеров $\chi(A)$ поменять ролями элементы A из $\mathfrak{A}$ (аргументы) и χ из $\mathfrak{X}$ (функции).*

Отсюда вытекает

Принцип двойственности. *Каждое верное высказывание относительно элементов A и характеров χ конечной абелевой группы переходит в верное высказывание, если во всех выражениях $\chi(A)$ поменять ролями элементы A и характеры χ.*

В этом смысле пары соотношений (1), (1′) и (2), (2′) из п. 2 дают примеры двойственных друг другу высказываний. С другими примерами мы встретимся в п. 4.

К лежащему в основе принципа двойственности факту III имеется еще одно интересное дополнение. Оно получается, если перейти от данной в доказательстве I, п. 1 неявной конструкции n характеров χ группы $\mathfrak{A}$ к явному их представлению.

Для этого мы используем основную теорему о конечных абелевых группах. Она гласит, что каждая конечная абелева группа $\mathfrak{A}$ представляется как прямое произведение циклических групп. Вследствие этого элементы A группы $\mathfrak{A}$ однозначно представляются в виде

$$A = \prod_{i=1}^{r} W_i^{\alpha_i} \quad (\alpha_i \bmod n_i) \tag{1}$$

через некоторое количество r базисных элементов W_i, имеющих порядки n_i, причем $\prod_{i=1}^{r} n_i = n$. Умножению элементов A из $\mathfrak{A}$ соответствует при этом сложение систем показателей $\alpha_i \bmod n_i$.

Мы не будем воспроизводить здесь доказательство этой общей основной теоремы, относящееся к алгебре (теории групп). В частном случае, когда $\mathfrak{A} = \mathfrak{G}_m$ есть группа классов вычетов по $\bmod m$, взаимно простых с модулем, мы доказали существование такого однозначного представления через базис в § 5, где было показано, что $\mathfrak{G}_m$ есть прямое произведение $\mathfrak{G}_{p^\mu}$ для составляющих число m степеней p^μ простых чисел и что $\mathfrak{G}_{p^\mu}$ обладает одночленными или двучленными представлениями указанного вида (см. III, п. 6, § 5 и V, п. 7, § 5).

Для каждого характера χ группы $\mathfrak{A}$ значения $\chi(W_i) = x_i$ образуют, в силу $W_i^{n_i} = E$, систему n_i-х корней из 1. На основании представления (1) все значения χ определяются через эти специальные значения в форме

$$\chi(A) = \prod_{i=1}^{r} x_i^{\alpha_i} \quad (\alpha_i \bmod n_i). \tag{2}$$

Обратно, если задана любая система x_i n_i-х корней из 1, то посредством (2) однозначно, т. е. независимо от выбора показателей α_i в их классах вычетов по $\bmod n_i$, определяется мультипликативная и всюду отличная от нуля функция χ элементов группы $\mathfrak{A}$, являющаяся, таким образом, характером группы $\mathfrak{A}$. Следовательно, $\prod_{i=1}^{r} n_i = n$ различных систем n_i-х корней из 1 x_i дают нам точно n различных характеров χ группы $\mathfrak{A}$. При такой конструкции перемножение характеров χ сводится к почленному перемножению систем n_i-х корней из 1 x_i. Согласно § 8, п. 1, n_i-е корни из 1 образуют циклическую группу порядка n_i. Следовательно, группа характеров $\mathfrak{X}$ есть прямое произведение r циклических групп порядков n_i и потому изоморфна группе $\mathfrak{A}$. Тем самым, мы доказали в дополнение к III:

IV. *Группа характеров $\mathfrak{X}$ изоморфна группе $\mathfrak{A}$.*

Если системы x_i n_i-х корней из 1 представлять через раз навсегда выбранную систему w_i первообразных n_i-х корней из 1, то представление (2) для значений характеров принимает вид:

$$\chi(A) = \prod_{i=1}^{r} w_i^{\xi_i \alpha_i} \quad (\xi_i, \alpha_i \bmod n_i). \tag{3}$$

Если же ввести еще специальные характеры ω_i со значениями $\omega_i(A) = w_i^{\alpha_i}$ $(\alpha_i \bmod n_i)$, для которых в качестве n_j-х корней из 1 x_j каждый раз выбирается одно $x_i = \omega_i$, а остальные $x_j = 1$ $(j \neq i)$, то получается однозначное представление через базис

$$\chi = \prod_{i=1}^{r} \omega_i^{\xi_i} \quad (\xi_i \bmod n_i) \tag{4}$$

для элементов χ группы $\mathfrak{X}$. Сравнение (4) с (1) дает явное представление изоморфизма между $\mathfrak{X}$ и $\mathfrak{A}$, а симметричность формул (3) относительно систем показателей $\alpha_i \bmod n_i$ из (1) и $\xi_i \bmod n_i$ из (4) явным образом выражает лежащий в основе принципа двойственности факт III.

Если, наконец, выразить первообразные n_i-е корни w_i из 1 в виде степеней некоторого одного n-го первообразного корня w из 1, например, в самой простой возможной форме $w_i = w^{n/n_i}$,

то формулы (3) перейдут в

$$\chi(A) = \omega^{\sum_{i=1}^{r} \frac{n}{n_i} \xi_i \alpha_i} \qquad (\xi_i,\ \alpha_i \bmod n_i).$$

Тогда высказывание типа $\chi(A) = 1$ представляется в виде однородного линейного сравнения $\sum_{i=1}^{r} (n/n_i)\, \xi_i \alpha_i \equiv 0 \bmod n$. Тем самым достигается формальная аналогия между принципом двойственности для конечных абелевых групп и известным принципом двойственности в аналитической геометрии.

4. Характеры и подгруппы. Мы будем исходить из следующих очевидных высказываний:

$\chi(A) = 1$ для всех A из $\mathfrak{A}$ равносильно тому, что $\chi = \varepsilon$, (1)

и более обще

$\chi(A) = \psi(A)$ для всех A из $\mathfrak{A}$ равносильно тому, что $\chi = \psi$. (2)

Они представляют собой просто определение равенства характеров χ как функций элементов группы $\mathfrak{A}$. Двойственными им являются следующие, уже нетривиальные высказывания:

$\chi(A) = 1$ для всех χ из $\mathfrak{X}$ равносильно тому, что $A = E$, (1′)

и более обще

$\chi(A) = \chi(B)$ для всех χ из $\mathfrak{X}$ равносильно тому, что $A = B$. (2′)

Они означают, что элемент A из $\mathfrak{A}$ однозначно характеризуется заданием системы значений $\chi(A)$ характеров χ группы $\mathfrak{A}$. Отсюда и происходит название «характер».

Характеры χ группы $\mathfrak{A}$ можно использовать и для более общей цели — охарактеризовать подгруппы $\mathfrak{U}$ группы $\mathfrak{A}$. Это основывается на следующих двух двойственных друг другу высказываниях, верность которых немедленно следует из мультипликативности $\chi(A)$ по χ и по A.

Если $\mathfrak{U}$ есть подгруппа группы $\mathfrak{A}$, то характеры χ, (3)
для которых $\chi(A) = 1$ для всех A из $\mathfrak{U}$, образуют подгруппу $\mathfrak{R}$ группы $\mathfrak{X}$.

Если $\mathfrak{R}$ есть подгруппа группы $\mathfrak{X}$, то элементы A, (3′)
для которых $\chi(A) = 1$ для всех χ из $\mathfrak{R}$, образуют подгруппу $\mathfrak{U}$ группы $\mathfrak{A}$.

Тривиальным образом получается:

Подгруппе $\mathfrak{U} = \mathfrak{E}$ соответствует, в силу (3), подгруппа $\mathfrak{R} = \mathfrak{X}$.

Подгруппе $\mathfrak{R} = \mathfrak{E}$ соответствует, в силу (3′), подгруппа $\mathfrak{U} = \mathfrak{A}$.

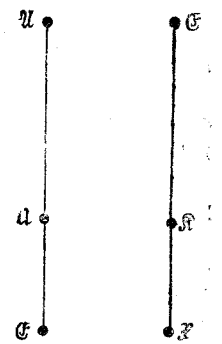
Согласно (1), (1′), имеет место и обратное:

Подгруппе $\mathfrak{U} = \mathfrak{A}$ *соответствует, в силу* (3), подгруппа $\mathfrak{K} = \mathfrak{E}$.
Подгруппе $\mathfrak{K} = \mathfrak{X}$ соответствует, в силу (3′), подгруппа $\mathfrak{U} = \mathfrak{E}$. Таким образом, в этих крайних случаях соответствия (3) и (3′) взаимно обусловливают друг друга.

Однако последнее верно также и в общем случае. Именно, имеет место следующий закон:

V. *Если, в силу* (3), *подгруппе* $\mathfrak{U}$ *соответствует подгруппа* $\mathfrak{K}$, *то, в силу* (3′), *подгруппе* $\mathfrak{K}$ *соответствует подгруппа* $\mathfrak{U}$, *и обратно.*

При этом $\mathfrak{K}$ *есть группа характеров для* $\mathfrak{A}/\mathfrak{U}$, *если понимать характеры* χ *из* $\mathfrak{K}$ *как функции классов* $A\mathfrak{U}$, *и* $\mathfrak{X}/\mathfrak{K}$ *есть группа характеров для* $\mathfrak{U}$, *если классы характеров* $\chi\mathfrak{K}$ *понимать как функции элементов* A из $\mathfrak{U}$.



Фиг. 4. $\mathfrak{K}$—группа характеров группы $\mathfrak{A}/\mathfrak{U}$; $\mathfrak{K} \cong \mathfrak{A}/\mathfrak{U}$. $\mathfrak{X}/\mathfrak{K}$—группа характеров группы $\mathfrak{U}$; $\mathfrak{X}/\mathfrak{K} \cong \mathfrak{A}$

Доказательство. Если в силу (3) подгруппе $\mathfrak{U}$ соответствует подгруппа $\mathfrak{K}$, то для χ из $\mathfrak{K}$ и любого A из $\mathfrak{A}$ значение характера $\chi(A)$ зависит только от класса $A\mathfrak{U}$, к которому принадлежит A в фактор-группе $\mathfrak{A}/\mathfrak{U}$. Следовательно, характеры χ из $\mathfrak{K}$ дают, если понимать их как функции классов $A\mathfrak{U}$, характеры фактор-группы $\mathfrak{A}/\mathfrak{U}$. Обратно, каждый характер χ факторгруппы $\mathfrak{A}/\mathfrak{U}$ превращается, если рассматривать его как функцию элементов A из классов $\mathfrak{A}/\mathfrak{U}$, в характер χ группы $\mathfrak{A}$ со свойством $\chi(U) = 1$ для всех U из $\mathfrak{U}$, т. е. в характер χ из подгруппы $\mathfrak{K}$, соответствующей подгруппе $\mathfrak{U}$, в силу (3). Согласно этим двум фактам, при заданной подгруппе $\mathfrak{U}$ группа характеров для $\mathfrak{A}/\mathfrak{U}$ есть как раз подгруппа $\mathfrak{K}$, соответствующая $\mathfrak{U}$ в силу (3). Если приведенное выше высказывание (1′) применить к $\mathfrak{A}/\mathfrak{U}$ вместо $\mathfrak{A}$ и $\mathfrak{K}$ вместо $\mathfrak{X}$, то получится, что подгруппа, соответствующая $\mathfrak{K}$ в силу (3′), есть $\mathfrak{U}$. Тем самым доказана первая половина утверждений из V. Вторая половина получается отсюда посредством применения принципа двойственности.

Закон V представляет собой замечательную аналогию основной теореме теории Галуа. А именно, из него немедленно получается:

V′. *Если, в силу* (3), (3′), *подгруппы* $\mathfrak{U}$, $\mathfrak{U}'$ *группы* $\mathfrak{A}$ *и подгруппы* $\mathfrak{K}$, $\mathfrak{K}'$ *группы* $\mathfrak{X}$ *соответствуют друг другу, то соотношения* $\mathfrak{U} \leqslant \mathfrak{U}'$ *и* $\mathfrak{K} \geqslant \mathfrak{K}'$ *взаимно обусловливают друг друга и при этом* $\mathfrak{K}/\mathfrak{K}'$ *есть группа характеров для* $\mathfrak{U}'/\mathfrak{U}$.

Среди всех частных случаев важнейшим для теоретико-числовых приложений является тот, когда

$\mathfrak{U}$ есть подгруппа, состоящая из всех k-х степеней элементов из $\mathfrak{A}$ для какого-нибудь данного натурального числа k, причем без

ограничения общности можно считать k делителем n. Действительно, если $(k, n) = d$, то k-е степени подавно являются d-ми степенями, и, наоборот, вследствие целочисленной разрешимости уравнения $kk' + nn' = d$ d-е степени являются также и k-ми степенями. Подгруппа $\mathfrak{K}$ группы $\mathfrak{X}$, соответствующая в силу (3) этой подгруппе $\mathfrak{U}$ группы $\mathfrak{A}$, характеризуется тем, что

$$\chi(A^k) = 1 \text{ или также } \chi^k(A) = 1 \text{ для всех } A \text{ из } \mathfrak{A}.$$

Но, согласно (1), это равносильно тому, что $\chi^k = \varepsilon$, т. е. $\mathfrak{K}$ есть подгруппа, состоящая из всех характеров показателя k из $\mathfrak{X}$. Она состоит поэтому из всех характеров, порядки которых равны или самому k, или некоторому делителю k. Из того факта, что подгруппе $\mathfrak{K}$ в силу (3′) снова соответствует $\mathfrak{U}$, получается следующий критерий:

VI. *Элемент A из $\mathfrak{A}$ является k-й степенью тогда и только тогда, когда для всех характеров χ показателя k имеет место* $\chi(A) = 1$.

Таким образом, если A лежит в подгруппе $\mathfrak{U}$, то решения X уравнения $X^k = A$ образуют смежный класс по подгруппе $\mathfrak{V}$, состоящей из решений V уравнения $V^k = E$ Согласно IV, п. 3, эта подгруппа $\mathfrak{V}$ группы $\mathfrak{A}$ изоморфна подгруппе $\mathfrak{K}$ группы $\mathfrak{X}$, так как речь идет о совокупностях элементов показателя k в двух изоморфных между собой группах. Таким образом, для A из $\mathfrak{U}$ количество $N_k(A)$ решений уравнения $X^k = A$ равно порядку N_k подгруппы $\mathfrak{K}$. Если A не лежит в $\mathfrak{U}$, то $N_k(A) = 0$. Поэтому во всех случаях $N_k(A)$ имеет то же самое значение, что и правые части соотношений (1′) п. 2 для фактор-группы $\mathfrak{A}/\mathfrak{U}$ с группой характеров $\mathfrak{K}$. Тем самым доказано

VII. *Для каждого натурального k (без ограничения, что k должно быть делителем n) и каждого A из $\mathfrak{A}$ количество $N_k(A)$ решений уравнения $X^k = A$ дается формулой*

$$N_k(A) = \sum_{\chi^k = \varepsilon} \chi(A) = \left\{ \begin{array}{l} N_k \text{ для } A, \text{ лежащего в } \mathfrak{U} \\ 0 \text{ для } A, \text{ не лежащего в } \mathfrak{U} \end{array} \right\},$$

где N_k есть количество характеров χ показателя k группы $\mathfrak{A}$.

Количество N_k при заданной группе $\mathfrak{A}$ легко может быть определено из представления через базис (4) п. 3 для группы характеров $\mathfrak{X}$; именно,

$$N_k = \prod_{i=1}^{r} (k, n_i).$$

Общие факты VI, VII представляют собой алгебраическую основу специальных результатов из § 6, п. 2, 3, 4 и § 10 п. 6, 9 о количестве решений сравнения $x^2 \equiv a \bmod p^\mu$, в частности $x^2 \equiv a \bmod p$, и сравнений $x^3 \equiv a \bmod p$ и $x^4 \equiv a \bmod p$.

5. Характеры по модулю. Теперь мы рассмотрим специально абелеву группу $\mathfrak{A} = \mathfrak{G}_m$ классов вычетов по $\bmod m$, взаимно простых с модулем, для некоторого натурального числа m. Ее порядок есть $n = \varphi(m)$. Характеры χ группы $\mathfrak{G}_m$ определяются сначала как функции элементов A из $\mathfrak{G}_m$, т. е. классов вычетов $a \bmod m$, взаимно простых с модулем. Мы сделаем их числовыми функциями, если положим

$$\chi(a) = \chi(A) \text{ для всех чисел } a \text{ из } A.$$

С теоретико-групповой точки зрения это сводится к следующему. Взаимно простые с m в смысле § 4, п. 10 рациональные числа a, т. е. те рациональные числа, у которых и числитель, и знаменатель взаимно просты с m, образуют мультипликативную абелеву группу $\mathfrak{M}$ бесконечного порядка. Числа $a \equiv 1 \bmod m$, т. е. те взаимно простые с m рациональные числа, у которых числитель и знаменатель сравнимы между собой по $\bmod m$, образуют в этой группе подгруппу $\mathfrak{U}$. Тогда группа классов вычетов по $\bmod m$, взаимно простых с модулем, получается как факторгруппа $\mathfrak{G}_m = \mathfrak{M}/\mathfrak{U}$. При этом, аналогично закону V, п. 4, характеры χ группы $\mathfrak{G}_m$ можно понимать как функции элементов из $\mathfrak{M}$ со свойством $\chi(a) = 1$ для всех a из $\mathfrak{U}$.

Определенные нами в области рациональных чисел, взаимно простых с m, $\varphi(m)$ функций $\chi(a)$ называются характерами по $\bmod m$. Как таковые, они характеризуются следующими свойствами:

$$\chi(ab) = \chi(a)\,\chi(b), \tag{1}$$

$$\chi(a) \neq 0, \tag{2}$$

$$\chi(a) = 1 \text{ для } a \equiv 1 \bmod m. \tag{3}$$

При этом, как показано в п. 1, вместо (2) достаточно потребовать только

$$\chi(a_0) \neq 0 \text{ по крайней мере для одного } a_0, \text{ взаимно простого с } m. \tag{2'}$$

Тогда, согласно (1), $\chi(1) = 1$, а отсюда вытекает общее свойство (2). Далее, из (3) на основании (1) следует

$$\chi(a) = \chi(a') \text{ для } a \equiv a' \bmod m. \tag{3'}$$

Если в качестве области значений аргумента брать только целые взаимно простые с m числа a, то требование (3) надо заменить общим требованием (3').

Со всем этим мы познакомились еще в § 6, п. 4 при определении символа Лежандра. Здесь мы еще раз собрали все это для того, чтобы подчеркнуть, что специальное понятие характера по модулю подчиняется общему понятию характера конечной

абелевой группы. Отсюда, в частности, мы получили доказательство существования точно $\varphi(m)$ характеров по $\bmod m$, которое раньше нами установлено не было.

Квадратичные характеры по $\bmod m$, подробно изученные нами во второй главе, характеризуются дополнительными свойствами $\chi^2 = \varepsilon$, $\chi \neq \varepsilon$; таким образом, это суть элементы порядка 2 из группы характеров $\mathfrak{X}$ группы $\mathfrak{M}$. В силу $\overline{\chi} = \chi^{-1}$, требование $\chi^2 = \varepsilon$ равносильно требованию $\overline{\chi} = \chi$. Поэтому квадратичные характеры по некоторому модулю можно определить также как различные, не равные главному характеру, вещественные характеры по этому модулю. Они будут играть особую важную роль в доказательстве Дирихле. Кроме особых свойств этих квадратичных характеров, в доказательстве Дирихле будет использовано только то, что существует $\varphi(m)$ характеров по $\bmod m$ и что для них имеет место выведенный в п. 2 из соотношений ортогональности факт II.

6. Ведущий модуль, собственные характеры. Мы хотим придать законченную форму изложенной выше общей теории характеров по $\bmod m$ посредством систематического изложения теории ведущего модуля, основные черты которой мы изложили уже во второй главе для рассматривавшихся там квадратичных характеров. Сейчас мы пока не будем пользоваться сделанным там обобщением понятия сравнимости на отрицательные модули посредством дополнительного требования равенства знаков (см. § 9, п. 5) и будем предполагать пока, как и в п. 5, что m — натуральное число.

Пусть χ есть характер по $\bmod m$. Если для некоторого другого натурального числа m' χ имеет аналогичное (3) п. 5 свойство

$$\chi(a) = 1 \quad \text{для } a \equiv 1 \bmod m', \tag{1}$$

причем, в соответствии с определением χ, a предполагается взаимно простым с m, то m' называется определяющим модулем характера χ. Основанием для такого названия служит утверждение

VIII. *Если χ есть характер по $\bmod m$ и m' — его определяющий модуль, то посредством однозначного расширения определения*

$$\chi(a') = \chi(a) \text{ для } a \equiv a' \bmod m' \text{ при } a, \text{ взаимно простом с } m, \tag{2}$$

на все a', взаимно простые с m', и выбрасывания значений, соответствующих числам a, взаимно простым с m, но не с m', характер χ превращается в характер по $\bmod m'$.

При этом говорят также, что χ *определяется* по $\bmod m'$.

Доказательство. Пусть дано взаимно простое с m' число a'. Тогда в классе вычетов $a' \bmod m'$, взаимно простом с модулем, существуют числа a, взаимно простые с m. Действи-

тельно, можно одновременно удовлетворить сравнения $a \equiv a' \bmod m'$ и, например, $a \equiv 1 \bmod m_0$, где m_0 есть произведение всех не входящих в m' простых делителей числа m. Поэтому расширенное определение (2) охватывает все взаимно простые с m' числа a'. Далее, если a_1, a_2 — два таких взаимно простых с m числа, что $a_1 \equiv a'$, $a_2 \equiv a' \bmod m'$, то $a_1/a_2 \equiv 1 \bmod m'$, и потому, согласно предположению (1), $\chi(a_1) = \chi(a_2)$. Следовательно, расширенное определение (2) не зависит от выбора взаимно простого с m вспомогательного числа a, т. е. однозначно. Очевидно, что при этом выполняются свойства (1), (2), (3) п. 5 с заменой m на m'. Таким образом, у нас действительно определяется χ как характер по $\bmod m'$.

Если в VIII поменять ролями m и m', то мы получим, что, обратно, определение по $\bmod m$ однозначным образом вытекает из определения по $\bmod m'$. Поэтому исходное определение по $\bmod m$ ничем не выделяется среди всех возможных определений по $\bmod m'$. Различные определения по $\bmod m$, $\bmod m'$, ... образуют систему функций, у которых областями значений аргумента каждый раз служат числа, взаимно простые с m, m', ..., и каждые две из этих функций совпадают в пересечении их областей значений аргумента (состоящем из чисел, взаимно простых и с m, и с m'). Таким образом, эти функции однозначно определяют функцию χ в объединении всех областей значений аргумента (состоящем из чисел, взаимно простых или с m, или с m', ...). Возникает вопрос о том, каково это объединение всех областей значений аргумента. Для ответа на него нам нужно получить обзор всех определяющих модулей характера χ.

Прежде всего, тривиальным образом выполняется

IX. *Вместе с m также и каждое его кратное m' является определяющим модулем характера χ.*

В этом случае при переходе от определения по $\bmod m$ к определению по $\bmod m'$ не появляется никаких новых аргументов, а только выбрасываются те из числа старых, которые взаимно просты с m, но не с m' (если таковые вообще существуют). При обратном переходе от определения по $\bmod m'$ к определению по $\bmod m$, которое при заданном m' возможно, конечно, только в том случае, если m снова есть определяющий модуль, положение будет как раз обратным: никакие аргументы не выбрасываются, а только присоединяются в качестве новых аргументов числа, взаимно простые с m, но не с m' (если такие вообще существуют).

Вообще, переход от одного определения по $\bmod m$ к другому определению по $\bmod m'$ может быть сведен к только что описанным двум типам перехода, если переходить сначала от m к общему наибольшему делителю (m, m'), а затем к его кратному m'. Действительно, далее имеет место

X. *Вместе с* m_1, m_2 *также и их общий наибольший делитель* (m_1, m_2) *является определяющим модулем характера* χ.

Доказательство. Согласно IX, вместе с m_1, m_2 определяющим модулем характера χ является также их общее наименьшее кратное $[m_1, m_2]$. На этом основании мы можем считать χ определенным как характер по mod $[m_1, m_2]$. Пусть a_1, a_2 — какие-нибудь два взаимно простых с $[m_1, m_2]$ числа, для которых $a_1 \equiv a_2 \bmod (m_1, m_2)$. Тогда, как было показано в доказательстве II, п. 5, § 7, существует такое взаимно простое с $[m_1, m_2]$ число a, что $a \equiv a_1 \bmod m_1$, $a \equiv a_2 \bmod m_2$. Отсюда следует, в силу того что m_1, m_2 являются определяющими модулями характера χ, что $\chi(a) = \chi(a_1)$, $\chi(a) = \chi(a_2)$, т. е. $\chi(a_1) = \chi(a_2)$. Таким образом, (m_1, m_2) действительно есть определяющий модуль характера χ.

Из фактов IX, X можно теперь получить следующий обзор всех определяющих модулей характера χ и всех соответствующих определений:

XI. *Совокупность определяющих модулей* m *характера* χ *есть совокупность всех кратных наименьшего из них. Этот наименьший определяющий модуль, который однозначно определяется характером* χ, *называется ведущим модулем характера* χ *и обозначается через* $f(\chi)$.

Из определения по mod $f(\chi)$, *которое имеет самую обширную из всех возможных область значений аргумента, состоящую из чисел, взаимно простых с* $f(\chi)$, *определения по* mod m *получаются каждый раз выбрасыванием чисел, взаимно простых с* $f(\chi)$, *но не с* m.

Доказательство. Если из какого-нибудь бесконечного множества $\mathfrak{M}$ натуральных чисел m выбирать шаг за шагом такую подпоследовательность $m_1, m_2, \ldots$, что каждый раз m_{i+1} не является кратным общего наибольшего делителя $d_i = (m_1, \ldots, m_i)$, то вследствие монотонного убывания последовательности делителей $d_1, d_2, \ldots$ мы уже через конечное число шагов получим такой делитель $d_r = (m_1, \ldots, m_r)$, что все числа m из $\mathfrak{M}$ будут его кратными, т. е. общий наибольший делитель всех m из $\mathfrak{M}$. Поэтому, применяя X конечное число раз, мы получим, что общий наибольший делитель $f(\chi)$ всех определяющих модулей m характера χ снова является определяющим модулем характера χ. Таким образом, каждый определяющий модуль m является кратным этого наименьшего определяющего модуля $f(\chi)$, и обратно, согласно IX, каждое кратное m числа $f(\chi)$, является определяющим модулем характера χ. Дальнейшее утверждение из XI получается тогда в силу ранее сказанного.

Характер χ, определенный в самой обширной из возможных областей значений аргумента, т. е. для всех чисел, взаимно простых с его ведущим модулем $f(\chi)$, называется собственным характером. Каждый характер по mod m однозначно определяет

принадлежащий ему собственный характор, если по схеме из VIII присоединить значения $\chi(a)$ для чисел a, взаимно простых с $f(\chi)$, но не с m. С этим расширением определения мы уже познакомились раньше в одном специальном случае, а именно, при переходе от символа Якоби $\left(\frac{a}{b}\right)$ к символу Кронекера в § 9, п. 6, где в случае $k(a) \equiv 1 \bmod 4$, т. е. $f(a) = k(a)$, область определения расширялась от чисел b, взаимно простых с 2 и с $k(a)$, до чисел b, взаимно простых только с $k(a) = f(a)$.

Чтобы получить обзор всех характеров с заданным ведущим модулем $f(\chi) = f$, мы сначала рассмотрим вообще поведение характеров по $\bmod m$ при разложении группы классов вычетов по $\bmod m$, взаимно простых с модулем, в прямое произведение. Пусть

$$m = m_1 \dots m_r$$

есть какое-нибудь разложение числа m на попарно взаимно простые множители m_i. Если для каждого класса вычетов $a \bmod m$ взаимно простого с модулем, однозначно определить его компоненты — классы $a_i \bmod m_i$ — посредством

$$a_i \equiv a \bmod m_i, \quad a_i \equiv 1 \bmod \frac{m}{m_i},$$

то разложение в прямое произведение представится в форме

$$a \equiv a_1 \dots a_r \bmod m.$$

Если, далее, определить независимо от выбора компонент a_i в их классах вычетов по $\bmod m$, функции χ_i посредством

$$\chi_i(a) = \chi(a_i),$$

то эти функции, очевидно, будут удовлетворять свойствам (1), (2), (3) п. 5 для модулей m_i, т. е. они являются характерами по $\bmod m_i$, и притом

$$\chi(a) = \chi(a_1) \dots \chi(a_r) = \chi_1(a) \dots \chi_r(a),$$

т. е.

$$\chi = \chi_1 \cdots \chi_r.$$

Это разложение χ на множители χ_i, являющиеся характерами по $\bmod m_i$, однозначно. Действительно, если

$$\chi = \chi_1' \cdots \chi_r'$$

есть другое такое разложение, то

$$\chi_i(a) = \chi(a_i) = \chi_1'(a_i) \dots \chi_r'(a_i) = \chi_i'(a_i) = \chi_i'(a),$$

т. е. $\chi_i = \chi_i'$. Если, наоборот, заданы любые характеры χ_i по $\bmod m_i$, то $\chi = \chi_1 \dots \chi_r$, очевидно, является характером по $\bmod m$. Таким образом, доказано

XII. *Если $m = m_1 \dots m_r$ есть разложение числа m на попарно взаимно простые множители m_i, то группа характеров группы классов вычетов по $\bmod m$, взаимно простых с модулем, есть прямое произведение групп характеров групп классов вычетов по $\bmod m_i$, взаимно простых с модулями; это разложение в прямое произведение представляется в форме*

$$\chi = \chi_1 \cdots \chi_r,$$

где компоненты χ_i определяются из χ соотношениями

$$\chi_i(a) = \chi(a_i) \quad \text{с} \quad a_i \equiv a \bmod m_i, \quad a_i \equiv 1 \bmod \frac{m}{m_i}.$$

Далее, если m' есть делитель числа m и

$$m' = m_1' \dots m_r'$$

есть его однозначное разложение в произведение чисел m_i', являющихся делителями m_i, $(m_i' = (m_i, m'))$, то выполнение для m' свойства (1) определяющего модуля для характера χ, т. е.

$$\chi(a) = 1 \qquad \text{для } a \equiv 1 \bmod m' \tag{а}$$

равносильно выполнению свойств

$$\chi_i(a) = 1 \qquad \text{для } a \equiv 1 \bmod m_i' \tag{б}$$

для всех компонент. Действительно, если $a \equiv 1 \bmod m_i'$, то $a_i \equiv 1 \bmod m_i'$, и так как всегда $a_i \equiv 1 \bmod m/m_i$, то заведомо $a_i \equiv 1 \bmod m'$; поэтому, вследствие $\chi_i(a) = \chi(a_i)$, из (а) следует (б). Обратно, если $a \equiv 1 \bmod m'$, то $a_i \equiv 1 \bmod m_i'$; поэтому вследствие $\chi = \chi_1 \dots \chi_r$ из (б) следует (а). Итак, m' тогда и только тогда является определяющим модулем для χ, когда все m_i' — определяющие модули для χ_i. Так как, согласно XI, для определения ведущих модулей характеров χ и χ_i можно ограничиться рассмотрением делителей m' числа m и делителей m_i' чисел m_i, то ведущий модуль $f(\chi)$ (наименьший определяющий модуль $m' \mid m$) является как раз произведением ведущих модулей $f(\chi_i)$ (наименьших определяющих модулей $m_i' \mid m_i$). Тем самым доказано

XIII. *При разложении на компоненты из* XII *для ведущих модулей имеет место*

$$f(\chi) = f(\chi_1) \dots f(\chi_r).$$

Наконец, из способа разложения на компоненты в XII немедленно получается

XIV. *Характеры χ определенного показателя k $(\chi^k = \varepsilon)$ составляются из компонент показателя k $(\chi_i^k = \varepsilon)$.*

Если в XII в качестве разложения на попарно взаимно простые множители взять разложение на простые множители, то задача определения всех характеров χ с заданным ведущим модулем $f(\chi)=f$ сведется к случаю степени простого числа $f=p^\nu$. Если

$$f=p_1^{\nu_1}\dots p_r^{\nu_r}\quad(\nu_i\geqslant 1)$$

есть разложение f на простые множители, то, согласно XII, XIII, для искомых характеров получается однозначное представление

$$\chi=\chi_1\dots\chi_r,$$

где каждый χ_i пробегает все характеры с ведущим модулем $f(\chi_i)=p_i^{\nu_i}$.

Пусть теперь дана степень простого числа $f=p^\nu$ ($\nu\geqslant 1$ для $p\neq 2$; $\nu\geqslant 2$ для $p=2$) и пусть

$$a\equiv w^{\alpha'}(1+p)^{\alpha''}\bmod p^\nu \text{ для } p\neq 2\ (\alpha'\bmod p-1,\ \alpha''\bmod p^{\nu-1}),$$

соответственно

$$a\equiv(-1)^{\alpha'}5^{\alpha''}\bmod 2^\nu \text{ для } p=2\ (\alpha'\bmod 2,\ \alpha''\bmod 2^{\nu-2})$$

есть представление из § 5, п. 6, 7 классов вычетов $a \bmod p^\nu$, взаимно простых с модулем, через базисные классы. Тривиальный случай $p=2$, $\nu=1$ мы можем оставить в стороне, так как группа классов вычетов по mod 2, взаимно простых с модулем, состоит только из единичного класса, и потому характеров с ведущим модулем 2^1 не имеет. Согласно (3), (4) п. 3, все характеры по mod p^ν получаются в однозначном представлении

$$\chi=\chi_p^{\varkappa'}\chi_{p^\nu}^{\varkappa''} \text{ для } p\neq 2\ (\varkappa'\bmod p-1,\ \varkappa''\bmod p^{\nu-1}),$$

соответственно

$$\chi=\chi_4^{\varkappa'}\chi_{2^\nu}^{\varkappa''} \text{ для } p=2\ (\varkappa'\bmod 2,\ \varkappa''\bmod 2^{\nu-2}),$$

где базисные характеры задаются схемой значений

	w	$1+p$
χ_p	ζ_{p-1}	1
χ_{p^ν} ($\nu>1$)	1	$\zeta_{p^{\nu-1}}$

соответственно

	-1	5
χ_4	-1	1
χ_{2^ν} ($\nu>2$)	1	$\zeta_{2^{\nu-2}}$

с фиксированными первообразными корнями ζ_{p-1}, $\zeta_{p^{\nu-1}}$, $\zeta_{2^{\nu-2}}$ из 1 порядков $p-1$, $p^{\nu-1}$, $2^{\nu-2}$. Эти базисные характеры имеют своими ведущими модулями стоящие в качестве индексов степени

простого числа p; это очевидно для χ_p и χ_4, а для χ_{p^ν} это видно из того, что $\chi_{p^\nu}(a)=1$ имеет место уже не для всех $a\equiv 1 \bmod p^{\nu-1}$ (именно, этого не будет для $a\equiv 1+p^{\nu-1}\equiv(1+p)^{p^{\nu-2}} \bmod p^\nu$, соответственно $a\equiv 1+2^{\nu-1}\equiv(1+2^2)^{2^{\nu-3}} \bmod 2^\nu$). Отсюда получается, что выраженный через базисные характеры характер χ имеет своим ведущим модулем точно $f(\chi)=p^\nu$, если

$$\varkappa' \not\equiv 0 \bmod p-1 \text{ для } \nu=1,\ \varkappa'' \not\equiv 0 \bmod p \text{ для } \nu>1,$$

соответственно

$$\varkappa' \not\equiv 0 \bmod 2 \text{ для } \nu=2,\ \varkappa'' \not\equiv 0 \bmod 2 \text{ для } \nu>2.$$

Тем самым получен полный обзор всех характеров χ с ведущим модулем $f(\chi)=f$.

Только что изложенная теория ведущего модуля и собственного характера, так же как и разложение на компоненты, немедленно переносится на случай, когда χ есть характер по отрицательному модулю m в смысле § 9, п. 5, т. е. характер группы $\mathfrak{G}_m$ полуклассов по $\bmod |m|$, взаимно простых с модулем, имеющей порядок $\varphi(m)=2\varphi(|m|)$. Для этого нужно только заменить входящий в m множитель -1 символом ∞, который в различных высказываниях о делимости, при образовании общего наибольшего делителя и общего наименьшего кратного, а также и при разложении на компоненты играет роль нового простого множителя. Однако мы хотим здесь, как и в § 9, п. 5, сохранить способ записи с множителем -1, что, как мы знаем, целесообразно для теории квадратичных характеров, а символ ∞ применять исключительно в качестве индекса. Тогда в качестве возможной компоненты для только что рассмотренных составных характеров χ_{p^ν} с $f(\chi)=p^\nu$ появляется еще один характер χ_∞ с $f(\chi_\infty)=-1$, определяемый формулой

$$\chi_\infty(a)=(-1)^\alpha \qquad \text{для } a\equiv(-1)^\alpha \bmod -1.$$

С этим характером, записанным в виде

$$\chi_\infty(a)=(-1)^{\frac{\operatorname{sgn} a-1}{2}}=\left\{\begin{array}{rl} 1 & \text{для } a>0 \\ -1 & \text{для } a<0 \end{array}\right\},$$

мы познакомились уже в § 9, п. 3. Согласно XII, XIII, он встречается в качестве компоненты для тех и только тех характеров χ, у которых в ведущий модуль $f(\chi)$ входит множитель -1. Таким образом, имеет место

XV. *Характер χ содержит компоненту χ_∞ тогда и только тогда, когда его ведущий модуль $f(\chi)<0$.*

. Если рассматривать, в частности, квадратичные характеры χ, важные для доказательства Дирихле, то, согласно XIV, XIII,

будут квадратичными характерами и их компоненты χ_{p^ν} с ведущими модулями, равными степеням простых чисел. Так как, однако, характеры χ_{p^ν} с $p \neq 2$, $\nu > 1$ и с $p = 2$, $\nu > 3$, очевидно, не являются квадратичными, то в ведущий модуль $f(\chi)$ квадратичного характера χ простые числа $p \neq 2$ могут входить только в первой степени, а простое число $p = 2$ — только во второй или в третьей степени. Следовательно, имеет место

XVI. *Ведущий модуль квадратичного характера равен или свободному от квадратов нечетному числу, или учетверенному свободному от квадратов (четному или нечетному) числу.*

Относительно определения собственного характера заметим, в заключение, следующее. Обычно область определения собственного характера χ с ведущим модулем $f(\chi)$ посредством определения

$$\chi(a) = 0 \text{ для } a, \text{ не взаимно простых с } f(\chi) \tag{3}$$

расширяют до области всех рациональных чисел a, являющихся $f(\chi)$-целыми. Мультипликативность при этом расширении сохраняется; действительно, произведение $f(\chi)$-целых чисел a, b не будет взаимно просто с $f(\chi)$ тогда и только тогда, когда по крайней мере один из сомножителей a, b не взаимно прост с $f(\chi)$, что согласуется со свойствами числа 0 при умножении. В частности, при этом расширенном определении имеет место

$$\chi(0) = \left\{ \begin{array}{lll} 1 & \text{для} & \chi = \varepsilon \\ 0 & \text{для} & \chi \neq \varepsilon \end{array} \right\}.$$

Действительно, для $\chi = \varepsilon$, $f(\chi) = 1$ и 0 взаимно прост с 1; для $\chi \neq \varepsilon$, напротив, $f(\chi) \neq 1$, и тогда 0 не взаимно прост с $f(\chi)$ (также и для $f(\chi) = -1$, где -1 рассматривается в связи с этим как нетривиальный общий делитель чисел 0 и $f(\chi)$).

7. Четные и нечетные характеры. Характер χ называется четным или нечетным как числовая функция, в зависимости от того, является ли распределение значений $\chi(a)$ на числовой прямой аргумента a симметричным или кососимметричным (т. е. с противоположными по знаку симметрично расположенными членами) относительно нулевой точки, и четным или нечетным как характер по $\bmod m$, в зависимости от того, симметрично или кососимметрично распределение значений в наименьшей системе вычетов по $\bmod |m|$ относительно среднего значения $|m|/2$. Для специального случая квадратичных характеров мы вводили эти понятия уже в § 9, п. 5. Вообще, каждый характер и как числовая функция, и как характер по $\bmod m$ будет или четным, или нечетным, причем четность или нечетность во втором смысле не зависит от выбора определяющего модуля m. Это доказывается следующим образом.

С одной стороны, в силу мультипликативности имеет место формула

$$\chi(-a)=\chi(-1)\chi(a) \quad \text{для всех } a, \tag{1}$$

включая также и введенные в рассмотрение расширенным определением (3) п. 6 не взаимно простые с $f(\chi)$ числа a. Из этой формулы следует

XVII. *Характер χ как числовая функция является четным или нечетным в зависимости от того, имеет ли место $\chi(-1)=1$ или -1.*

С другой стороны, мы сейчас докажем формулу

$$\chi(|m|-a)=\chi(-1)\operatorname{sgn} f(\chi)\cdot\chi(a) \quad \text{для } 0<a<|m| \tag{2}$$

при любом определяющем модуле m (т. е. любом кратном числа $f(\chi)$). Из этой формулы следует

XVIII. *Характер χ как характер по модулю является четным или нечетным в зависимости от того, имеет ли место $\chi(-1)\times\operatorname{sgn} f(\chi)=1$ или -1.*

Чтобы убедиться в правильности формулы (2), заметим, что для взаимно простого с $f(\chi)$ числа a с $0<a<|m|$ имеет место

$$\frac{|m|-a}{-a}\equiv -1 \bmod -1 \text{ и } \equiv 1 \bmod |f(\chi)|.$$

Таким образом, если $\chi=\chi_\infty^{\varkappa}\chi'$ есть разложение χ на две компоненты, из которых первая $-\chi_\infty^{\varkappa}$ ($\varkappa \bmod 2$) — соответствует характеру χ_∞ с ведущим модулем -1, а вторая — χ' — есть характер, для которого $f(\chi')>0$, то

$$\chi_\infty^{\varkappa}\left(\frac{|m|-a}{-a}\right)=\chi_\infty^{\varkappa}(-1)=(-1)^{\varkappa},\ \chi'\left(\frac{|m|-a}{-a}\right)=1,$$

и потому, согласно XV, п. 6,

$$\chi\left(\frac{|m|-a}{-a}\right)=(-1)^{\varkappa}=\operatorname{sgn} f(\chi).$$

Следовательно, имеет место

$$\chi(|m|-a)=\operatorname{sgn} f(\chi)\cdot\chi(-a),$$

причем как для a, взаимно простого с $f(\chi)$, так и для не взаимно простого, ибо в последнем случае обе стороны этого соотношения равны 0. Если принять во внимание (1), то отсюда следует доказываемая формула (2).

Для доказательства Дирихле нужны будут только значения характера $\chi(a)$ с $a>0$. Если иметь в виду только их, то χ можно нормировать посредством умножения на степень $\chi_\infty^{\varkappa}$ ($\varkappa \bmod 2$) характера χ_∞ с ведущим модулем -1, так как это может отразиться только на значениях $\chi(a)$ для $a<0$. При этом ведущий

модуль $f(\chi)$ может лишь изменить знак, а именно,

$$f(\chi_\infty^\varkappa \chi) = (-1)^\varkappa f(\chi),$$

что следует из XV, п. 6. Показатель $\varkappa \bmod 2$ при таком нормировании можно было определить требованием $\operatorname{sgn} f(\chi) = (-1)^\varkappa$, так что $\chi' = \chi_\infty^\varkappa \chi$ получил бы ведущий модуль $f(\chi') > 0$; это нормирование играло роль выше, в доказательстве формулы (2). Для нас важно сейчас другое нормирование такого вида, а именно,

$$\chi^* = \chi_\infty^\varkappa \chi \quad \text{с} \quad \chi(-1) = (-1)^\varkappa, \tag{3}$$

при котором $\varkappa \bmod 2$ в соответствии с XVII определяется так, что χ^* становится четным как числовая функция. Так нормированный характер χ^* имеет ведущий модуль

$$f(\chi^*) = \chi(-1) f(\chi), \tag{4}$$

и как характер по модулю является, согласно XVIII, четным или нечетным в зависимости от того, имеет ли место $f(\chi^*) > 0$ или < 0.

Мы уже установили в V, п. 5, § 9, что символ Якоби — или лучше символ Кронекера как собственный характер — как функция своего знаменателя является единственным четным как числовая функция квадратичным характером, ведущий модуль которого имеет вид из IV, п. 5, § 9, и доказали одно еще несколько более сильное высказывание такого рода. Но, согласно XVI, п. 6, ведущий модуль каждого квадратичного характера имеет с точностью до знака вид из IV, п. 5, § 9. Используя более сильное высказывание из V, п. 5, § 9 и принимая во внимание также знак ведущего модуля, мы докажем в заключение следующее уточнение указанных результатов из § 9, которое будет использоваться в доказательстве теоремы Дирихле о простых числах:

XIX. *Если χ есть какой-нибудь собственный квадратичный характер по модулю, то получающийся из него в соответствии с* (3) *нормированный характер χ^* с ведущим модулем* (4) *совпадает в области взаимно простых с $f(\chi^*)$ чисел a с символом Кронекера*

$$\chi^*(a) = \left(\frac{f(\chi^*)}{a}\right).$$

Для самого характера χ имеет место поэтому

$$\chi(a) = \left(\frac{\chi(-1) f(\chi)}{a}\right) \text{ для взаимно простых с } f(\chi) \text{ чисел } a > 0.$$

Доказательство. Мы будем различать следующих два случая, которые, согласно XVI, только и могут представиться.

а) Пусть $f(\chi)=k$ или $4k$ с нечетным свободным от квадратов k. Тогда мы однозначно определим — формально не так, как в (3) — множитель $(-1)^{\varkappa}$ посредством требования $(-1)^{\varkappa}k\equiv 1$, соответственно $-1 \bmod 4$. Тогда $(-1)^{\varkappa}f(\chi)$ имеет вид из IV, п. 5, § 9. Далее, $(-1)^{\varkappa}f(\chi)=f(\chi_\infty^{\varkappa}\chi)$. Согласно результату из V, п. 5, § 9, где в настоящем случае нет необходимости предполагать четность характера как числовой функции, мы тогда имеем

$$\chi_\infty^{\varkappa}(a)\chi(a)=\left(\frac{f(\chi_\infty^{\varkappa}\gamma)}{a}\right).$$

Так как символ Кронекера как числовая функция является четным, то и характер $\chi_\infty^{\varkappa}\chi$ будет как числовая функция четным. Поэтому наше нормирование совпадает с тем, которое определено в (3), т. е. $\chi_\infty^{\varkappa}\chi=\chi^*$, что и доказывает наше утверждение.

б) Пусть $f(\chi)=4k$ с четным свободным от квадратов k. Тогда $\pm f(\chi)$ оба имеют вид из IV, п. 5, § 9. Тогда, согласно результату из V, п. 5, § 9, где в этом случае характер как числовая функция предполагается четным, для нормированного по (3) характера χ^* следует наше утверждение.

Результат XIX может быть высказан еще и так. Каждый четный как числовая функция собственный квадратичный характер χ есть (в области взаимно простых с $f(\chi)$ чисел) символ Кронекера как функция его знаменателя с числителем $f(\chi)$. Каждый нечетный как числовая функция собственный квадратичный характер χ получается из символа Кронекера с числителем $-f(\chi)$ посредством умножения на квадратичный характер χ_∞ с ведущим модулем -1. Эти факты делают понятным значение символа Кронекера для теории квадратичных характеров.

§ 14. ДОКАЗАТЕЛЬСТВО ДИРИХЛЕ

1. L-ряды. Пусть m — натуральное число и χ пробегает $\varphi(m)$ характеров по $\bmod m$. Мы будем рассматривать соответствующие этим характерам ряды Дирихле

$$L_m(s\,|\,\chi)=\sum_{(n,\,m)=1}\frac{\chi(n)}{n^s},$$

где s — переменная, значения которой мы сначала ограничим вещественными числами. Эти ряды называются L-рядами для характеров χ. Черта между аргументом s и характером χ означает, что речь идет не о функции двух переменных, а о функции одной переменной s, причем эта функция, кроме того, зависит от теоретико-числовой функции χ.

Так как для вещественных $s > 1$ дзета-ряд является абсолютно сходящейся мажорантой для L-ряда (см. II, п. 4, § 12), мы имеем

I. *Для вещественных $s > 1$ L-ряды абсолютно сходятся.*

Точнее, дзета-ряд для $s = 1 + \delta$ с любым $\delta > 0$ есть абсолютно сходящаяся мажоранта для L-рядов для всех $s \geqslant 1 + \delta$. Поэтому в каждой области $s \geqslant 1 + \delta$ с $\delta > 0$ L-ряды сходятся равномерно. Так как, кроме того, при $s \to +\infty$ все их члены, кроме члена с $n = 1$, стремятся к 0, мы имеем

II. *Для вещественных $s > 1$ L-ряды являются непрерывными функциями от s и*

$$\lim_{s \to +\infty} L_m(s \mid \chi) = 1.$$

Согласно тождеству Эйлера (см. (4) и I, п. 1, § 12), из I и мультипликативности теоретико-числовой функции $f(n) = \chi(n) / n^s$ получается

III. *Для вещественных $s > 1$ L-ряды обладают представлениями в виде абсолютно сходящихся бесконечных произведений*

$$L_m(s \mid \chi) = \prod_{p \nmid m} \frac{1}{1 - \frac{\chi(p)}{p^s}}.$$

Для доказательства Дирихле было бы достаточно оперировать с только что определенными L-рядами, в которых характеры χ рассматриваются как характеры по заданному фиксированному модулю m. Однако, с алгебраической точки зрения, разумнее положить в основу соответствующие им собственные характеры (см. § 13, п. 6), т. е. характеры χ, рассматриваемые как характеры по их ведущим модулям $f(\chi)$, причем область их определения, в соответствии с (3) п. 6, § 13, посредством присоединения значения 0 для не взаимно простых с $f(\chi)$ значений аргумента, расширяется до совокупности всех целых чисел. Так определенные ряды Дирихле

$$L(s \mid \chi) = \sum_n \frac{\chi(n)}{n^s}, \tag{1}$$

когда суммирование распространено на все натуральные n, называются собственными L-рядами для характеров χ.

Для собственных L-рядов снова имеют место факты I, II, а также и III с представлением в виде бесконечного произведения

$$L(s \mid \chi) = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}}, \tag{2}$$

где произведение распространено теперь на все простые числа p. Это следует из того, что собственные характеры χ мультиплика-

тивны также и в области всех целых чисел. Собственные L-ряды связаны с определенными ранее несобственными L-рядами посредством формул

$$L(s|\chi) = \prod_{p|m} \frac{1}{1-\frac{\chi(p)}{p^s}} L_m(s|\chi), \tag{3}$$

т. е. собственный ряд получается из несобственного умножением на конечное число элементарных множителей с $p|m$, из которых отличны от 1 только множители с $p \nmid f(\chi)$.

Согласно (1), L-рядом, соответствующим главному характеру $\chi = \varepsilon$, является просто дзета-ряд:

$$L(s|\varepsilon) = \zeta(s).$$

Поэтому из (3) следует

$$L_m(s|\varepsilon) = \prod_{p|m} \left(1-\frac{1}{p^s}\right) \zeta(s).$$

Этот факт выявлялся у нас при рассмотрении случаев $m=3$, 4 в § 12, п. 2 при доказательстве расходимости рядов

$$L_m(1|\varepsilon) = \sum_{(n,\,m)=1} \frac{1}{n}.$$

Напротив, единственный фигурировавший там характер $\chi \neq \varepsilon$ имеет ведущий модуль $f(\chi) = m$, т. е. заранее является собственным, так что для него имеет место $L_m(s|\chi) = L(s|\chi)$.

В то время как для доказательства Дирихле, как уже сказано, нет необходимости переходить к собственным L-рядам, так как конечное число дополнительных множителей в (3) не играет здесь роли, в теории алгебраических чисел оказывается, что только собственные L-ряды приводят к простым формулам и закономерностям. Об этом мы еще будем говорить в конце § 15, п. 5.

2. Выделение множеств простых чисел, лежащих в отдельных классах вычетов. Классы вычетов $a \bmod m$, взаимно простые с модулем, рассматриваемые как элементы группы $\mathfrak{G}_m$, мы будем кратко обозначать через A.

В $\varphi(m)$ представлениях в виде произведения из III, п. 1 встречаются все простые числа $p \nmid m$. При этом простые числа p из одного и того же класса вычетов A характеризуются системой значений $\chi(p) = \chi(A)$ всех характеров χ; согласно (2′) п. 4, § 13, класс вычетов A характеризуется этой системой значений однозначно. Сообразно с этим мы распределим сомножители в $\varphi(m)$ представлениях из III, п. 1 по $\varphi(m)$ совокупностям, каждая из которых соответствует простым числам из одного и того же

класса вычетов A:

$$L_m(s|\chi) = \prod_A \prod_{p \text{ из } A} \frac{1}{1 - \frac{\chi(A)}{p^s}}.$$

Чтобы получить в изолированном виде фигурирующие здесь частичные произведения, распространенные на множества простых чисел из отдельных классов вычетов A, мы в специальных случаях $m = 3, 4$ в § 12, п. 2, когда вследствие $\varphi(m) = 2$ было только два класса вычетов E, A и два характера ε, χ, образовывали произведение и частное обоих бесконечных произведений для $L_m(s|\varepsilon)$ и $L_m(s|\chi)$. Теперь мы обобщим этот процесс на любое m.

Прежде всего, так же как и для дзета-ряда (случай $m = 1$) в § 12, п. 4, мы перейдем к логарифмам L-рядов. Так как здесь у нас будут логарифмы комплексного аргумента, мы должны указать, какую ветвь логарифма, являющегося в комплексной области многозначной функцией, мы будем брать. Значения функции на различных ветвях отличаются друг от друга на некоторую кратность $2\pi i$. Согласно II, п. 1, выбор ветви можно нормировать требованием

$$\lim_{s \to +\infty} \ln L_m(s|\chi) = 0,$$

причем, в силу III, п. 1, ветвь определяется этим однозначно. Для нее, согласно III, п. 1, для вещественных $s > 1$ имеет место аддитивная формула

$$\ln L_m(s|\chi) = \sum_{p \nmid m} \ln \frac{1}{1 - \frac{\chi(p)}{p^s}},$$

если логарифмы множителей в правой части подчинить таким же нормирующим условиям

$$\lim_{s \to +\infty} \ln \frac{1}{1 - \frac{\chi(p)}{p^s}} = 0.$$

Но эти последние нормирующие условия для вещественных $s > 1$ выполняются, очевидно, как раз для абсолютно сходящихся логарифмических рядов

$$\ln \frac{1}{1 - \frac{\chi(p)}{p^s}} = \sum_{\nu=1}^{\infty} \frac{1}{\nu} \frac{\chi(p^\nu)}{p^{\nu s}}.$$

Следовательно, при таком нормировании для логарифмов L-рядов для вещественных $s > 1$ получаются аддитивные представления

$$\ln L_m(s|\chi) = \sum_{p \nmid m} \sum_{\nu=1}^{\infty} \frac{1}{\nu} \frac{\chi(p^\nu)}{p^{\nu s}} \tag{1}$$

с абсолютно сходящимися рядами в правой части. Так как эти ряды мажорируются дзета-рядом, то, как и для дзета-ряда в § 12, п. 4, при предельном переходе $s \to 1+0$ сумма членов с $\nu \geqslant 2$ остается ограниченной. Поэтому из (1) получаются аналогичные (4) п. 4, § 12 предельные соотношения

$$\ln L_m(s \mid \chi) \approx \sum_{p \nmid m} \frac{\chi(p)}{p^s}. \tag{2}$$

Согласно (3) п. 1, в левой части этих соотношений можно несобственные ряды $L_m(s \mid \chi)$ заменить собственными рядами $L(s \mid \chi)$, так как произведение конечного количества дополнительных множителей имеет при $s \to 1$ конечный, отличный от нуля предел. Если далее сгруппировать слагаемые в правой части по отдельным классам вычетов A, то предельные соотношения (2) принимают вид

$$\sum_A \chi(A) \sum_{p \text{ из } A} \frac{1}{p^s} \approx \ln L(s \mid \chi). \tag{3}$$

Эти предельные соотношения можно подробно записать в виде системы уравнений

$$\sum_A \chi(A) \sum_{p \text{ из } A} \frac{1}{p^s} = \ln L(s \mid \chi) + E(s \mid \chi),$$

где дополнительные члены $E(s \mid \chi)$ при $s \to 1+0$ остаются ограниченными. Эта система уравнений имеет такой же вид, как и система из II, п. 2, § 13. Как было там установлено, ее можно разрешить в виде системы

$$\sum_{p \text{ из } A} \frac{1}{p^s} = \frac{1}{\varphi(m)} \sum_\chi \overline{\chi}(A) \ln L(s \mid \chi) + \frac{1}{\varphi(m)} \sum_\chi \overline{\chi}(A) E(s \mid \chi).$$

Так как вторая сумма в правой части остается ограниченной при $s \to 1+0$, мы получаем предельные соотношения

$$\sum_{p \text{ из } A} \frac{1}{p^s} \approx \frac{1}{\varphi(m)} \sum_\chi \overline{\chi}(A) \ln L(s \mid \chi). \tag{4}$$

В них множества простых чисел из отдельных классов вычетов фигурируют изолированно друг от друга.

Только в этой изоляции друг от друга простых чисел, лежащих в разных классах вычетов, и заключается значение характеров χ для доказательства Дирихле; это значение часто переоценивается неалгебраистами. Как мы выяснили, по сути дела все сводится к совершенно прозрачному методу рассужде-

ния из линейной алгебры. Суммы

$$x_A = \sum_{p \text{ из } A} \frac{1}{p^s},$$

которые интересуют нас в доказательстве Дирихле, посредством линейной подстановки с матрицей $\mathfrak{C} = (\chi(A))$ из значений характеров и обратной транспонированной к ней матрицей

$$\mathfrak{C}'^{-1} = \frac{1}{\varphi(m)}\,\overline{\mathfrak{C}} = \frac{1}{\varphi(m)}\,(\overline{\chi}(A))$$

(с точностью до членов, остающихся при $s \to 1+0$ ограниченными), связаны с логарифмами $y_\chi = \ln L(s|\chi)$ L-рядов, предельное поведение которых при $s \to 1+0$ изучить легче.

В частности, для $m = 3, 4$ эта матрица имеет вид $\mathfrak{C} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$; мы приходим, таким образом, к образованию суммы и разности логарифмов $L(s|\varepsilon)$ и $L(s|\chi)$, что для самих L-рядов означает образование произведения и отношения, что и делалось в § 12, п. 2. В общем же случае этот изолирующий процесс нельзя хорошо провести без перехода к логарифмам, потому что пришлось бы иметь дело с комплексными значениями характеров $\chi(A)$ в качестве показателей степеней.

3. Предельное поведение L-рядов. Доказанные перед этим предельные соотношения (4) п. 2 сводят доказательство теоремы Дирихле о простых числах к доказательству того, что линейные комбинации $\sum_\chi \overline{\chi}(A) \ln L(s|\chi)$ логарифмов L-рядов при $s \to 1+0$ не остаются ограниченными; действительно, это же тогда будет иметь место и для сумм

$$\sum_{p \text{ из } A} \frac{1}{p^s},$$

так что в отдельных взаимно простых с модулем классах вычетов A обязательно должно содержаться бесконечно много простых чисел p. В то время как изложенная до сих пор часть доказательства опиралась на представление (2) п. 1 для L-рядов в виде бесконечного произведения, посредством чего в нашу последовательность выводов вводились простые числа, остающаяся еще, существенно аналитическая часть доказательства использует взятое за определение представление (1) из п. 1 L-рядов в виде бесконечных рядов.

Как уже было установлено в п. 1, для главного характера $\chi = \varepsilon$ имеет место $L(s|\varepsilon) = \zeta(s)$ и, согласно (1′) п. 4, § 12, $\ln \zeta(s) \approx \approx \ln[1/(s-1)]$. Таким образом, в вышеупомянутых линейных комбинациях член $\ln L(s|\varepsilon)$, соответствующий характеру $\chi = \varepsilon$,

при $s \to 1+0$ не остается ограниченным. Поэтому для завершения доказательства достаточно показать, что все остальные члены остаются при $s \to 1+0$ ограниченными, т. е. что остается ограниченным $\ln L(s|\chi)$ при $s \to 1+0$ для каждого характера $\chi \neq \varepsilon$.

В связи с этим мы сначала докажем

IV. *Если* $\chi \neq \varepsilon$, *то* L*-ряд*

$$L(s|\chi) = \sum_n \frac{\chi(n)}{n^s}$$

при натуральном порядке следования членов сходится даже для всех вещественных $s > 0$ *и представляет собой непрерывную функцию от* s.

При этом для $0 < s \leqslant 1$ порядок следования членов действительно важен, так как для этих значений s сходимость будет не абсолютной, а только условной вследствие расходимости дзета-ряда.

Доказательство. Достаточно показать, что ряд $L(s|\chi)$ равномерно сходится в каждой области $s \geqslant \delta$ с $\delta > 0$. Мы применим критерий сходимости Коши, т. е. покажем, что кусок ряда $\sum_{\nu < n \leqslant N}$ при $\nu \to \infty$ стремится к нулю и притом равномерно для всех $N \geqslant \nu$ и всех $s \geqslant \delta$. Если $f = f(\chi)$ есть ведущий модуль характера χ, $\varkappa f$ и Kf — ближайшие к ν и N кратные f, то куски ряда, соответствующие ν и N, а также $\varkappa f$ и Kf отличаются друг от друга самое большее на f членов, которые при $\nu \to \infty$ равномерно стремятся к нулю для всех $N \geqslant \nu$ и всех $s \geqslant \delta$. Поэтому достаточно ограничиться рассмотрением кусков вида $\sum_{\varkappa f < n \leqslant Kf}$, которые удобны вследствие периодичности коэффициентов $\chi(n)$ с периодом f.

Вследствие этой периодичности

$$\sum_{\varkappa f < n \leqslant Kf} \frac{\chi(n)}{n^s} = \sum_{r=1}^{f} \chi(r) \sum_{\varkappa \leqslant k < K} \frac{1}{(r+kf)^s} = \frac{1}{f^s} \sum_{r=1}^{f} \chi(r) \sum_{\varkappa \leqslant k < K} \frac{1}{(k+\rho)^s},$$

где для краткости положено $\rho = r/f$. Вследствие того, что $0 < \rho \leqslant 1$, $1/(k+\rho)^s$ лежит для больших k близко от $1/(k+1)^s$. Так как $\chi \neq \varepsilon$, то, как показано в (1) п. 2, § 13, $\sum_{r=1}^{f} \chi(r) = 0$, и потому

$$0 = \frac{1}{f^s} \sum_{r=1}^{f} \chi(r) \sum_{\varkappa \leqslant k < K} \frac{1}{(k+1)^s}.$$

Вычитая это соотношение из написанного выше представления

для нашего куска ряда, мы получаем

$$\sum_{\varkappa f<n\leqslant Kf}\frac{\chi(n)}{n^s}=\frac{1}{f^s}\sum_{r=1}^{f}\chi(r)\sum_{\varkappa\leqslant k<K}\left[\frac{1}{(k+\rho)^s}-\frac{1}{(k+1)^s}\right].$$

Теперь, по теореме о среднем значении из дифференциального исчисления, мы имеем

$$\frac{1}{(k+\rho)^s}-\frac{1}{(k+1)^s}=\frac{(1-\rho)s}{(k+\rho')^{s+1}}\quad\text{с }\rho\leqslant\rho'\leqslant 1.$$

Так как s/x^{s+1} имеет как функция от s производную $(1-\ln x^s)/x^{s+1}\leqslant 0$ для $\ln x^s\geqslant 1$, т. е. с возрастанием s монотонно убывает, если только $x^s\geqslant e$, то отсюда получается оценка

$$0\leqslant\frac{1}{(k+\rho)^s}-\frac{1}{(k+1)^s}\leqslant\frac{(1-\rho)\delta}{(k+\rho')^{\delta+1}}\leqslant\frac{\delta}{k^{\delta+1}},$$

если только $k\geqslant e^{1/\delta}$. Последнее условие будет в нашем доказательстве соблюдаться, если мы заранее выберем $\varkappa\geqslant e^{1/\delta}$. Вследствие $|\chi(r)|\leqslant 1$, для нашего куска ряда получается тем самым оценка

$$\left|\sum_{\varkappa f<n\leqslant Kf}\frac{\chi(n)}{n^s}\right|\leqslant\frac{f\delta}{f^\delta}\sum_{\varkappa\leqslant k<K}\frac{1}{k^{\delta+1}}\quad\text{для }\varkappa\geqslant e^{1/\delta}.$$

Так как фигурирующий в правой части кусок дзета-ряда $\zeta(1+\delta)$ вследствие сходимости этого ряда при $\delta>0$ равномерно по K стремится к нулю при $\varkappa\to\infty$, то то же самое получается и для куска ряда, стоящего слева, и притом равномерно также для всех $s\geqslant\delta$, что и утверждалось.

Из доказанного тем самым факта IV следует, что для каждого характера $\chi\neq\varepsilon$ существует $\lim\limits_{s\to 1}L(s|\chi)$ (даже при приближении с любой стороны) и что он имеет конечное значение

$$L(1|\chi)=\sum_n\frac{\chi(n)}{n}$$

с натуральным порядком расположения членов. Теперь для завершения доказательства Дирихле остается только показать, что

$$L(1|\chi)\neq 0;$$

действительно, тогда $\lim\limits_{s\to 1}\ln L(s|\chi)$ также будет существовать и иметь конечное значение $\ln L(1|\chi)$, так что $\ln L(s|\chi)$ заведомо будет оставаться ограниченным при $s\to 1+0$.

Употребленное нами слово «только» является здесь, впрочем, необоснованным, так как в доказательстве этого последнего факта

и заключается главная трудность доказательства Дирихле, как это уже отмечалось в конце § 12, п. 3. Об этом мы будем подробно говорить в § 15.

4. Плотность Дирихле и натуральная плотность. Предположим на мгновение, что нами уже доказано, что $L(1|\chi) \neq 0$ для $\chi \neq \varepsilon$. Тогда, как уже сказано в п. 3, предельные соотношения (4) п. 2 принимают более простой вид

$$\sum_{p \text{ из } A} \frac{1}{p^s} \approx \frac{1}{\varphi(m)} \ln \zeta(s) \approx \frac{1}{\varphi(m)} \ln \frac{1}{s-1}. \tag{1}$$

Отсюда, как уже говорилось, вытекает теорема Дирихле о простых числах. Однако тот факт, что правая часть не зависит от класса вычетов A и содержит числовой множитель $1/\varphi(m)$, зависящий только от m, позволяет сделать и более точные заключения.

Используем для этого установленное уже в (5) п. 4, § 12 предельное соотношение

$$\sum_{p} \frac{1}{p^s} \approx \ln \frac{1}{s-1},$$

которое получается также как частный случай из (1) при $m = 1$. Тогда соотношения (1) примут вид

$$\sum_{p \text{ из } A} \frac{1}{p^s} \approx \frac{1}{\varphi(m)} \sum_{p} \frac{1}{p^s}. \tag{2}$$

Они означают теперь, что все стоящие слева суммы, соответствующие отдельным классам вычетов A, имеют при $s \to 1+0$ один и тот же порядок возрастания и что он точно в $\varphi(m)$ раз меньше порядка возрастания соответствующей суммы для всего множества простых чисел. Это находит себе выражение также и в несколько более слабых обычных предельных соотношениях, вытекающих из (2):

$$\lim_{s \to 1+0} \frac{\sum\limits_{p \text{ из } A} \frac{1}{p^s}}{\sum\limits_{p} \frac{1}{p^s}} = \frac{1}{\varphi(m)}. \tag{3}$$

Предельные соотношения (3) дают повод для следующего совершенно общего определения. Пусть $\mathfrak{P}$ есть множество всех простых чисел и $\mathfrak{M}$ — какое-нибудь его подмножество, которое, например, может быть задано, как в случае классов вычетов, взаимно простых с модулем, как пересечение $\mathfrak{P}$ с некоторым

множеством, определенным в области всех натуральных чисел. Тогда, если существует предел

$$\lim_{s\to 1+0}\frac{\sum\limits_{p\text{ из }\mathfrak{M}}\frac{1}{p^s}}{\sum\limits_{p\text{ из }\mathfrak{P}}\frac{1}{p^s}}=\delta(\mathfrak{M}),$$

который, очевидно, обязательно конечен и удовлетворяет неравенствам $0\leqslant\delta(\mathfrak{M})\leqslant 1$, то говорят, что множество простых чисел $\mathfrak{M}$ имеет (в множестве $\mathfrak{P}$ всех простых чисел) плотность Дирихле $\delta(\mathfrak{M})$. С помощью этого понятия мы можем высказать результат (3) следующим образом:

V. *Для каждого натурального m множества простых чисел, лежащих в $\varphi(m)$ классах вычетов по* $\bmod m$, *взаимно простых с модулем, все имеют одну и ту же плотность Дирихле, а именно,* $1/\varphi(m)$.

Понятие плотности Дирихле, очевидно, удовлетворяет тем требованиям, которые мы должны предъявить к понятию плотности. А именно, во-первых, как уже сказано, всегда $0\leqslant\delta(\mathfrak{M})\leqslant 1$. Во-вторых, *полное множество* $\mathfrak{P}$ *всех простых чисел имеет плотность* $\delta(\mathfrak{P})=1$, пустое множество $\mathfrak{O}$ имеет плотность $\delta(\mathfrak{O})=0$. Также и каждое конечное множество $\mathfrak{M}$ простых чисел имеет плотность $\delta(\mathfrak{M})=0$. В-третьих, если $\mathfrak{M}\leqslant\mathfrak{M}'$, то $\delta(\mathfrak{M})\leqslant\delta(\mathfrak{M}')$, и, в-четвертых, если $\mathfrak{M}$, $\mathfrak{M}'$ не имеют общих элементов, то $\delta(\mathfrak{M}+\mathfrak{M}')=\delta(\mathfrak{M})+\delta(\mathfrak{M}')$, причем в обоих случаях предполагается, что плотности $\delta(\mathfrak{M})$, $\delta(\mathfrak{M}')$ существуют.

С элементарной точки зрения, понятие плотности Дирихле представляется несколько искусственным: естественнее определить плотность множества $\mathfrak{M}$ простых чисел как предел

$$\lim_{N\to\infty}\frac{\pi_{\mathfrak{M}}(N)}{\pi_{\mathfrak{P}}(N)}=\omega(\mathfrak{M})$$

(если он существует), где

$$\pi_{\mathfrak{M}}(N)=\sum_{\substack{p\text{ из }\mathfrak{M}\\ p\leqslant N}}1,\qquad \pi_{\mathfrak{P}}(N)=\sum_{\substack{p\text{ из }\mathfrak{P}\\ p\leqslant N}}1$$

— количества простых чисел $p\leqslant N$ из $\mathfrak{M}$, $\mathfrak{P}$ (последнее обычно обозначается просто через $\pi(N)$). В этом последнем смысле говорят о натуральной плотности $\omega(\mathfrak{M})$ множества $\mathfrak{M}$ (в множестве $\mathfrak{P}$ всех простых чисел).

Предельное соотношение

$$\sum_{p\text{ из }\mathfrak{P}}\frac{1}{p_s}\approx\ln\frac{1}{s-1}\quad\text{при } s\to 1+0.$$

лежащее в основе определения плотности Дирихле, соответствует для натуральной плотности упомянутой в § 12, п. 5 теореме о простых числах

$$\pi_{\mathfrak{P}}(N) \sim \frac{N}{\ln N} \quad \text{при} \quad N \to \infty.$$

Там говорилось о том, посредством какого рода рассуждений эти предельные соотношения следуют одно из другого. Совершенно то же самое можно сказать и вообще о связи плотности Дирихле и натуральной плотности. Если существует одна из них, то существует и другая и обе имеют одно и то же значение $\delta(\mathfrak{M}) = \omega(\mathfrak{M})$. Переход от натуральной плотности к плотности Дирихле по существу прост (обобщение теоремы Абеля о непрерывности); обратный переход от плотности Дирихле к натуральной плотности существенно сложнее (обращение одного обобщения теоремы Абеля о непрерывности из теории функций комплексного переменного). Способом, который мы в рамках этой книги разбирать не можем, из V получается соответствующий ему факт:

VI. *Для каждого натурального m множества простых чисел, лежащих в $\varphi(m)$ классах вычетов по* $\bmod m$, *взаимно простых с модулем, все имеют одну и ту же натуральную плотность, а именно,* $1/\varphi(m)$.

Плотность Дирихле имеет то преимущество перед натуральной плотностью, что доказательство ее существования и определение значения требует существенно меньших аналитических средств (зато, правда, бóльших алгебраических и арифметических средств), что относится как к рассматриваемому здесь случаю простых чисел в классах вычетов, взаимно простых с модулем, так и к другим случаям, встречающимся в теории алгебраических чисел. Поэтому алгебраист или теоретико-числовик охотно пользуется несколько более искусственным определением плотности Дирихле и удовлетворяется результатом V, как выражающим суть дела, в то время как аналитик бывает удовлетворен только тогда, когда совершит сложный переход к VI.

§ 15. НЕОБРАЩЕНИЕ L-РЯДОВ В НУЛЬ

1. Произведения L-рядов. 1. Остающееся еще доказательство того, что для каждого характера $\chi \neq \varepsilon$ для собственного L-ряда имеет место

$$L(1|\chi) = \sum_n \frac{\chi(n)}{n} \neq 0,$$

может быть проведено многими способами. Например, можно оперировать только элементарными средствами вещественного анализа; тогда доказательство сводится к довольно сложным вычислениям и оценкам. Мы изложим сначала один такой эле-

ментарно-аналитический путь доказательства, исходящий от Мертенса, причем мы выберем из числа многих имеющихся вариантов самый прозрачный с алгебраической точки зрения. Можно привлечь и глубокие методы исследования или из теории функций комплексного переменного, или из теории полей алгебраических чисел; тогда доказательство будет совершенно прозрачно с аналитической, а также арифметической точки зрения. Мы дадим обзор этих методов доказательства после элементарно-аналитического доказательства. Для одного из этих методов, а именно, того, который применял сам Дирихле в его ставшей классической работе 1837 года [1], мы изложим необходимые сведения из теории квадратичных полей в четвертой главе. Существует и совершенно свободное от использования аналитических методов доказательство теоремы Дирихле о простых числах, принадлежащее Цасенхаузу [1]. Оно получается из классического доказательства Дирихле посредством замены фигурирующих там бесконечных рядов и произведений близкими им по значению конечными выражениями. Отметим еще следующий важный результат Ю. В. Линника [1]: существует такая абсолютная константа $k > 0$, что для каждого натурального m в каждом классе вычетов по $\bmod m$, взаимно простом с модулем, имеется простое число $p < m^k$.

2. В каждом известном до сих пор доказательстве необращения L-рядов в нуль так или иначе используется произведение

$$\zeta_m(s) = \prod_{\chi} L(s|\chi) = \zeta(s) \prod_{\chi \neq \varepsilon} L(s|\chi) \tag{1а}$$

собственных L-рядов для $\varphi(m)$ характеров χ группы классов вычетов по $\bmod m$, взаимно простых с модулем. Элементарно-аналитические доказательства, а также и элементарные варианты теоретико-функциональных и алгебраическо-теоретико-числовых доказательств, используют, кроме того, частичное произведение

$$\zeta(s|\chi) = L(s|\varepsilon)\, L(s|\chi) = \zeta(s)\, L(s|\chi) \tag{1б}$$

с некоторым фиксированным вещественным, т. е. квадратичным характером χ.

Действительную причину этих фактов, которая коренится в значении $\zeta_m(s)$ для арифметики поля P_m m-х корней из 1 и $\zeta(s|\chi)$ для арифметики квадратичного поля $\mathsf{P}(\sqrt{\chi(-1)f(\chi)})$, мы изложим позднее. Сначала мы хотим вывести некоторые основные факты относительно произведений $\zeta_m(s)$, $\zeta(s|\chi)$.

Это исследование станет прозрачнее и не потребует существенно бо́льших средств, если мы рассмотрим произведение

$$\zeta(s|\mathfrak{K}) = \prod_{\chi \text{ из } \mathfrak{K}} L(s|\chi) \tag{1}$$

собственных L-рядов для характеров χ из какой-нибудь группы $\mathfrak{K}$, состоящей из k характеров по $\bmod m$. Интересующие нас здесь случаи (1а) и (1б) соответствуют тогда группе $\mathfrak{X}$ всех $\varphi(m)$ характеров по $\bmod m$ и состоящей только из главного характера ε и квадратичного характера χ подгруппе порядка 2.

В соответствии с нашей элементарно-аналитической установкой мы все время будем ограничиваться вещественными $s > 1$, не оговаривая этого каждый раз. Как мы показали в I—III, п. 1, § 14, в этой области $L(s\,|\,\chi)$ являются непрерывными функциями от s, и как взятые за определение представления

$$L(s\,|\,\chi) = \sum_n \frac{\chi(n)}{n^s} \tag{Р}$$

в виде рядов Дирихле, так и получающиеся из тождества Эйлера представления

$$L(s\,|\,\chi) = \prod_p \frac{1}{1-\frac{\chi(p)}{p^s}} \tag{П}$$

в виде произведений Дирихле, абсолютно сходятся. Так как в группу $\mathfrak{K}$ вместе с каждым невещественным характером χ входит также и комплексно сопряженный характер $\overline{\chi} = \chi^{-1}$, то произведение $\zeta(s\,|\,\mathfrak{K})$ во всяком случае вещественно.

К дальнейшим высказываниям относительно $\zeta(s\,|\,\mathfrak{K})$ мы придем, если в произведении (1) заменим множители $L(s\,|\,\chi)$ один раз их представлениями (Р) в виде рядов, а другой раз — представлениями (П) в виде произведений и каждый раз их почленно перемножим, что допустимо вследствие абсолютной сходимости.

3. Сначала мы подставим представления (Р) в виде рядов, затем перемножим их. Если $\chi_1, \ldots, \chi_k$ обозначают k характеров из $\mathfrak{K}$, то мы будем иметь

$$\prod_{\chi \text{ из } \mathfrak{K}} L(s\,|\,\chi) = \sum_{n_1} \frac{\chi_1(n_1)}{n_1^s} \cdots \sum_{n_k} \frac{\chi_k(n_k)}{n_k^s} \sum_{n_1, \ldots, n_k} \frac{\chi_1(n_1) \ldots \chi_k(n_k)}{(n_1 \ldots n_k)^s},$$

где $n_1, \ldots, n_k$ пробегают все натуральные числа. Тем самым для произведения (1) получается представление

$$\zeta(s\,|\,\mathfrak{K}) = \sum_n \frac{\sigma(n\,|\,\mathfrak{K})}{n^s} \quad \text{с} \quad \sigma(n\,|\,\mathfrak{K}) = \sum_{n_1 \ldots n_k = n} \chi_1(n_1) \ldots \chi_k(n_k) \tag{2}$$

в виде ряда Дирихле, где в коэффициентах $\sigma(n\,|\,\mathfrak{K})$ суммирование производится по всем разложениям числа n на k натуральных множителей. Эти коэффициенты суть значения теоретико-числовой функции $\sigma(n\,|\,\mathfrak{K})$, определяемой группой $\mathfrak{K}$ и обладающей свойством

$$\sigma(nn'\,|\,\mathfrak{K}) = \sigma(n\,|\,\mathfrak{K})\,\sigma(n'\,|\,\mathfrak{K}) \text{ для } (n, n') = 1. \tag{3}$$

Действительно, каждой паре разложений

$$n = n_1 \dots n_k, \qquad n' = n'_1 \dots n'_k$$

на k натуральных множителей однозначно соответствует разложение

$$nn' = (n_1 n'_1) \dots (n_k n'_k)$$

на k натуральных множителей, и если n, n' взаимно просты, то и, обратно, каждое такое разложение числа nn' на k натуральных множителей получается таким способом из однозначно определенной пары разложений чисел n, n' на k натуральных множителей. Поэтому мы действительно имеем

$$\sigma(nn' \mid \mathfrak{K}) = \sum_{\substack{n_1 \dots n_k = n \\ n'_1 \dots n'_k = n'}} \chi_1(n_1 n'_1) \dots \chi_k(n_k n'_k) =$$

$$= \sum_{n_1 \dots n_k = n} \chi_1(n_1) \dots \chi_k(n_k) \sum_{n'_1 \dots n'_k = n'} \chi_1(n'_1) \dots \chi_k(n'_k) =$$

$$= \sigma(n \mid \mathfrak{K})\, \sigma(n' \mid \mathfrak{K}).$$

На основании свойства (3) теоретико-числовая функция $\sigma(n \mid \mathfrak{K})$ определяется уже своими значениями для степеней простых чисел $n = p^\nu$. Эти специальные значения, согласно (2), даются формулой

$$\sigma(p^\nu \mid \mathfrak{K}) = \sum_{\substack{\nu_1 + \dots + \nu_k = \nu \\ \nu_1, \dots, \nu_k \geqslant 0}} \chi_1(p^{\nu_1}) \dots \chi_k(p^{\nu_k}) \tag{4}$$

в которой суммирование производится по всем разложениям числа ν на k неотрицательных целых слагаемых $\nu_1, \dots, \nu_k$.

4. Теперь подставим представления (П) в виде произведений и перемножим их. После подстановки из (1) посредством перестановки сомножителей (перемены порядка умножения) прежде всего получается

$$\zeta(s \mid \mathfrak{K}) = \prod_p \left(\prod_{\chi \text{ из } \mathfrak{K}} \frac{1}{1 - \frac{\chi(p)}{p^s}} \right). \tag{5}$$

На основании теоретико-группового значения характеров χ можно преобразовать стоящее здесь внутреннее (конечное) произведение для каждого данного p следующим образом.

Для фиксированного простого числа p, только те характеры χ из заданной группы характеров $\mathfrak{K}$ порядка k вносят в произведение (5) множители, отличные от 1, для которых $\chi(p) \neq 0$, т. е. для которых p не входит в ведущий модуль $f(\chi)$. Так как для произведения характеров $\chi\psi$ число $f(\chi) f(\psi)$ заведомо является определяющим модулем и потому ведущий модуль $f(\chi\psi)$

является делителем произведения $f(\chi)\,f(\psi)$, то характеры χ с $p \nmid f(\chi)$ образуют подгруппу $\mathfrak{K}_p$ группы $\mathfrak{K}$. Пусть порядок этой подгруппы равен k_p, т. е.

K_p есть количество тех характеров χ из $\mathfrak{K}$, для которых $p \nmid f(\chi)$. Далее, характеры χ с $\chi(p) = 1$ образуют подгруппу $\mathfrak{U}_p$ группы $\mathfrak{K}_p$. Пусть порядок $\mathfrak{U}_p$ равен g_p, т. е.

g_p есть количество тех характеров χ из $\mathfrak{K}$, для которых $\chi(p) = 1$, а индекс $\mathfrak{U}_p$ в $\mathfrak{K}_p$ обозначим через f_p, так что

$$k_p = f_p g_p.$$

Фактор-группа $\mathfrak{K}_p / \mathfrak{U}_p$ порядка f_p изоморфна группе $\mathfrak{Z}$ значений $\chi(p) = \zeta$ для всех χ из $\mathfrak{K}_p$, так как отдельные классы из $\mathfrak{K}_p / \mathfrak{U}_p$ состоят из характеров χ с одним и тем же значением $\chi(p) = \zeta$ и умножение классов соответствует умножению этих значений. Поэтому каждое из f_p чисел ζ из $\mathfrak{Z}$ встречается в качестве значения $\chi(p) = \zeta$ точно для g_p характеров из $\mathfrak{K}_p$. Но значения $\chi(p) = \zeta$ из $\mathfrak{Z}$ во всяком случае являются k-ми корнями из 1. Как подгруппа циклической группы всех k-х корней из 1, группа $\mathfrak{Z}$ циклична и потому состоит из всех f_p-х корней из 1. В силу этого, имеет место

$$\prod_{\chi \text{ из } \mathfrak{K}} \left(1 - \frac{\chi(p)}{p^s}\right) = \prod_{\chi \text{ из } \mathfrak{K}_p} \left(1 - \frac{\chi(p)}{p^s}\right) = \prod_{\zeta^{f_p}=1} \left(1 - \frac{\zeta}{p^s}\right)^{g_p} = \left(1 - \frac{1}{p^{f_p s}}\right)^{g_p}.$$

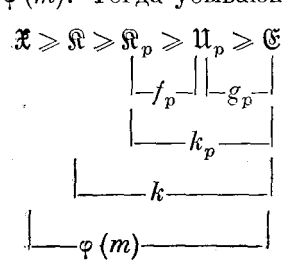
Тем самым из (5) получается представление в виде абсолютно сходящегося произведения

$$\zeta(s \mid \mathfrak{K}) = \prod_p \left(\frac{1}{1 - \frac{1}{p^{f_p s}}}\right)^{g_p}, \tag{6}$$

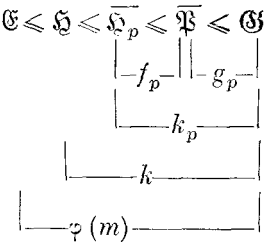
где натуральные числа f_p, g_p определяются для отдельных простых чисел p, как было указано выше.

5. Данное нами определение чисел f_p, g_p можно привести еще к другому, более удобному для применений виду, если воспользоваться изложенными в § 13, п. 4 фактами относительно характеров и подгрупп. Пусть $\mathfrak{G}$ — группа всех классов вычетов по $\bmod m$, взаимно простых с модулем, и $\mathfrak{X}$ — группа всех ее характеров, обе порядка $\varphi(m)$. Тогда убывающим цепочкам подгрупп

$$\mathfrak{X} \geqslant \mathfrak{K} \geqslant \mathfrak{K}_p \geqslant \mathfrak{U}_p \geqslant \mathfrak{E}$$



с указанными индексами (порядки понимаются здесь как индексы единичной подгруппы), согласно V, V′, п. 3, § 13, взаимно однозначно соответствуют возрастающие цепочки подгрупп



с теми же самыми индексами (на соответствующих местах), и при этом $\mathfrak{K}$, $\mathfrak{K}_p$, $\mathfrak{U}_p$ являются, соответственно, группами характеров для $\mathfrak{G}/\mathfrak{H}$, $\mathfrak{G}/\overline{\mathfrak{H}_p}$, $\mathfrak{G}/\overline{\mathfrak{P}}$.

Пусть теперь

$$m = p^{\mu_p} m_p \quad \text{с} \quad p \nmid m_p$$

есть разложение числа m на степень простого числа p и неделящееся на p натуральное число m_p. Далее, пусть $\mathfrak{G}_p$ есть группа всех классов вычетов по $\bmod m_p$, взаимно простых с модулем, и $\mathfrak{X}_p$ — группа всех ее характеров, обе порядка $\varphi(m_p)$. Согласно § 4, п. 9, группа $\mathfrak{G}_p$ изоморфна тому прямому сомножителю группы $\mathfrak{G}$, который соответствует множителю m_p числа m. Для преследуемой здесь цели предпочтительнее другой вывод $\mathfrak{G}_p$ из $\mathfrak{G}$. А именно, мы также получим $\mathfrak{G}_p$, если образуем композит группы $\mathfrak{G}$, рассматриваемой как числовая группа, и группы $\mathfrak{E}_p$ всех $a \equiv 1 \bmod m_p$ (т. е. единичного класса по $\bmod m_p$):

$$\mathfrak{G}_p = \mathfrak{G}\mathfrak{E}_p.$$

Действительно, при этом отдельные классы вычетов $a \bmod m$, взаимно простые с модулем, пополняются до классов вычетов $a \bmod m_p$, взаимно простых с модулем. Группа $\mathfrak{X}_p$ содержится в $\mathfrak{X}$ в качестве подгруппы, а именно, $\mathfrak{X}_p$ есть совокупность тех характеров χ из $\mathfrak{X}$, для которых уже m_p является определяющим модулем, т. е. для которых $p \nmid f(\chi)$. Подгруппа $\overline{\mathfrak{E}_p}$ группы $\mathfrak{G}$, соответствующая по § 13, п. 4 подгруппе $\mathfrak{X}_p$ группы $\mathfrak{X}$, характеризуется тем, что $\chi(a) = 1$ для всех χ из $\mathfrak{X}_p$, т. е. состоит из взаимно простых с m чисел $a \equiv 1 \bmod m_p$, или, другими словами, является пересечением

$$\overline{\mathfrak{E}_p} = \mathfrak{E}_p \cap \mathfrak{G}.$$

Схематически это представлено на фиг. 5.

В силу только что сказанного, интересующая нас здесь подгруппа $\mathfrak{K}_p$ группы $\mathfrak{K}$, состоящая из тех χ из $\mathfrak{K}$, для которых

$p \nmid f(\chi)$, является просто пересечением

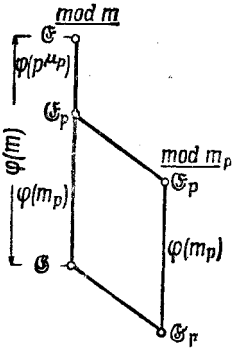
$$\mathfrak{K}_p = \mathfrak{K} \cap \mathfrak{X}_p.$$

Соответственно этому приведенная выше схема цепочки убывающих групп характеров изображена на фиг. 6а, где композит $\mathfrak{K}\mathfrak{X}_p$ в дальнейшем не будет представлять для нас интереса, а не встречавшийся ранее индекс e_p подгруппы $\mathfrak{K}_p$ в группе $\mathfrak{K}$, для которого, таким образом, имеет место

$$k = e_p f_p g_p$$

будет играть роль только в п. 5 и далее, в § 19, п. 2.

Если рассматривать $\mathfrak{K}_p$ как подгруппы $\mathfrak{X}_p$, то нужно основываться на расширении области определения характера χ (для которого $p \nmid f(\chi)$) от совокупности чисел, взаимно простых с m, до совокупности чисел, взаимно простых лишь с m_p. Это расширение содержится в полном расширении до собственного характера (см. VIII, п. 6, § 13). Подгруппы $\mathfrak{H}_p$, $\mathfrak{P}$ группы $\mathfrak{G}_p$, соответствующие по § 13, п. 4 подгруппам $\mathfrak{K}_p$, $\mathfrak{U}_p$, группы $\mathfrak{X}_p$, получаются, в силу данного там правила соответствия, посредством аналогичного расширения подгрупп $\overline{\mathfrak{H}}_p$, $\overline{\mathfrak{P}}$ группы $\mathfrak{G}$, соответствующих подгруппам $\mathfrak{K}_p$, $\mathfrak{U}_p$ группы $\mathfrak{X}$. Согласно сказанному выше, этот процесс расширения может быть описан посредством образования композитов с единичным классом $\mathfrak{E}_p$. Именно,



Фиг. 5.

$$\mathfrak{H}_p = \overline{\mathfrak{H}}_p \mathfrak{E}_p, \qquad \mathfrak{P} = \overline{\mathfrak{P}} \mathfrak{E}_p,$$

и, наоборот,

$$\overline{\mathfrak{H}}_p = \mathfrak{H}_p \cap \mathfrak{G}, \qquad \overline{\mathfrak{P}} = \mathfrak{P} \cap \mathfrak{G}.$$

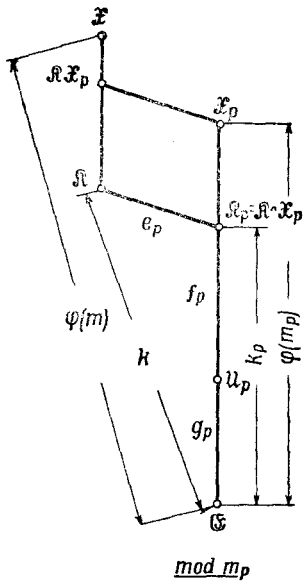
Индексы f_p, g_p, k_p для $\mathfrak{H}_p$, $\mathfrak{P}$ будут те же самые, что и для $\overline{\mathfrak{H}}_p$, $\overline{\mathfrak{P}}$, в силу сопоставления с одними и теми же группами характеров $\mathfrak{K}_p$, $\mathfrak{U}_p$. Это можно понимать так же как изоморфизм соответствующих факторгрупп, если выполнять переход от $\overline{\mathfrak{H}}_p$, $\overline{\mathfrak{P}}$ к $\mathfrak{H}_p$, $\mathfrak{P}$ на основании изоморфизма $\mathfrak{G}_p$ с некоторым прямым сомножителем группы $\mathfrak{G}$ (разложение характеров на компоненты из XII, п. 6, § 13!). Согласно всему сказанному, приведенная выше схема цепочки возрастающих групп классов вычетов изображается фиг. 6б.

Что касается подгруппы $\mathfrak{H}_p$, которая будет в дальнейшем интересовать нас в первую очередь, то, в силу правила соответствия из § 13, п. 4, она состоит из тех классов вычетов

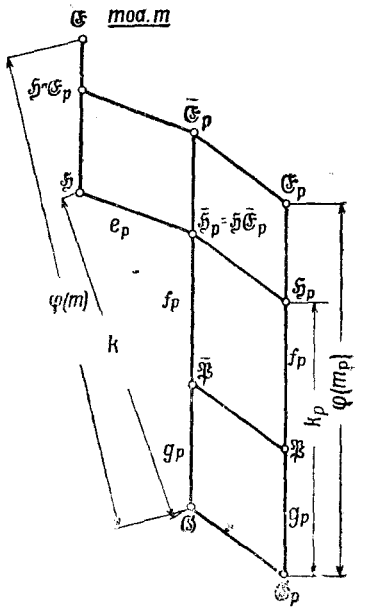
$a \bmod m_p$, взаимно простых с модулем, для которых

$$\chi(a) = 1 \text{ для всех } \chi \text{ из } \mathfrak{K}_p.$$

На основании изложенной перед этим теоретико-групповой схемы можно получить и другую, более удобную для наших целей характеристику подгруппы $\mathfrak{H}_p$, где упор будет сделан на соответствующую группе характеров $\mathfrak{K}$ группу классов вычетов $\mathfrak{H}$.



Фиг. 6а.



Фиг. 6б.

Прежде всего, в соответствии с представлением $\mathfrak{K}_p = \mathfrak{K} \cap \mathfrak{X}_p$ для пересечения, мы посредством образования композита $\mathfrak{H}$ и определенного по $\bmod m$ единичного класса $\overline{\mathfrak{E}}_p \bmod m_p$ получаем $\overline{\mathfrak{H}}_p = \mathfrak{H}\overline{\mathfrak{E}}_p$ и, далее, образуя композит $\overline{\mathfrak{H}}_p$ и определенного по $\bmod m_p$ единичного класса $\mathfrak{E}_p \bmod m_p$, имеем $\mathfrak{H}_p = \overline{\mathfrak{H}}_p\mathfrak{E}_p$. Так как $\overline{\mathfrak{E}}_p \leqslant \mathfrak{E}_p$, то вместе это дает попросту

$$\mathfrak{H}_p = \mathfrak{H}\mathfrak{E}_p.$$

Таким образом, $\mathfrak{H}_p$ есть группа тех классов вычетов по $\bmod m_p$, взаимно простых с модулем, в которых содержатся числа из классов вычетов по $\bmod m$ из $\mathfrak{H}$. Тогда число k_p, которое выше было определено исходя из группы характеров $\mathfrak{K}$, может

быть определено также и исходя из соответствующей группы классов вычетов $\mathfrak{H}$ как индекс расширенной группы $\mathfrak{H}_p$ в полной группе $\mathfrak{G}_p$ классов вычетов, взаимно простых с модулем, или так же как порядок фактор-группы $\mathfrak{G}_p/\mathfrak{H}_p$.

Наконец, чтобы охарактеризовать, как было обещано выше, на этой новой основе число f_p, а тем самым тогда также и g_p, как дополнительный к f_p делитель числа k_p, заметим, что порядок обозначенной выше через $\mathfrak{Z}$ циклической группы значений $\chi(p)=\zeta$ для χ из $\mathfrak{K}_p$ *является наименьшим натуральным показателем* со свойством

$$\chi(p)^{f_p}=\zeta^{f_p}=1 \text{ для всех } \chi \text{ из } \mathfrak{K}_p.$$

Замечая, что $\chi(p)^{f_p}=\chi(p^{f_p})$, и сравнивая эту характеристику для f_p с данной перед этим характеристикой для $\mathfrak{H}_p$, мы получаем, что f_p есть также наименьший натуральный показатель, для которого p^{f_p} лежит в $\mathfrak{H}_p$, т. е. получаем порядок класса вычетов $p \bmod m_p$, взаимно простого с модулем, в фактор-группе $\mathfrak{G}_p/\mathfrak{H}_p$.

Между прочим, на этой основе можно охарактеризовать также и подгруппу $\mathfrak{P}$ группы $\mathfrak{G}_p$, содержащую $\mathfrak{H}_p$ с индексом f_p; именно, $\mathfrak{P}$ характеризуется тем, что циклическая фактор-группа $\mathfrak{P}/\mathfrak{H}_p$ порядка f_p порождается классом вычетов $p \bmod m_p$. Для этого, в силу только что установленного, достаточно показать, что класс вычетов $p \bmod m_p$ лежит в $\mathfrak{P}$. Но по определению, $\mathfrak{P}$ состоит из взаимно простых с модулем классов вычетов $a \bmod m_p$, для которых

$$\chi(a)=1 \text{ при всех } \chi \text{ из } \mathfrak{U}_p,$$

и $\mathfrak{U}_p$ определяется через $\chi(p)=1$. Поэтому класс вычетов $p \bmod m_p$ действительно удовлетворяет требованию, определяющему группу $\mathfrak{P}$.

6. Итак, мы имеем следующий результат:

I. *Произведение*

$$\zeta(s\,|\,\mathfrak{K})=\prod_{\chi \text{ из } \mathfrak{K}} L(s\,|\,\chi)$$

собственных L-рядов для характеров χ из некоторой группы характеров по $\bmod m$ $\mathfrak{K}$ *порядка k обладает представлением*

$$\zeta(s\,|\,\mathfrak{K})=\prod_{p}\left(\frac{1}{1-\frac{1}{p^{f_p s}}}\right)^{g_p}$$

в виде произведения Дирихле, абсолютно сходящегося при $s>1$, с натуральными показателями f_p, g_p, которые определяются по следующей схеме:

Пусть

$\mathfrak{H}$ — *группа тех* $a \bmod m$, *для которых* $\chi(a)=1$ *при всех* χ *из* $\mathfrak{K}$.

Далее, пусть

$$m = p^{\mu_p} m_p \quad \text{с} \quad p \nmid m_p,$$

$\mathfrak{H}_p$ — *группа тех* $a \bmod m_p$, *для которых* $a \bmod m$ *лежит в* $\mathfrak{H}$,
k_p — *индекс группы* $\mathfrak{H}_p$ *в группе классов вычетов по* $\bmod m_p$, *взаимно простых с модулем.*

Тогда

f_p *есть порядок класса* $p \bmod m_p$ *по отношению к* $\mathfrak{H}_p$,
g_p *есть дополнительный к* f_p *делитель числа* k_p.

За исключением конечного множества простых делителей p числа m, дело обстоит проще: $m_p = m$, $\mathfrak{H}_p = \mathfrak{H}$, $k_p = k$, т. е. f_p есть порядок класса $p \bmod m$ по отношению к $\mathfrak{H}$ и $f_p g_p = k$.

В случае $\zeta_m(s)$, где $\mathfrak{K} = \mathfrak{X}$ есть группа всех $k = \varphi(m)$ характеров по $\bmod m$, $\mathfrak{K}_p = \mathfrak{X}_p$ будет группой всех $k_p = \varphi(m_p)$ характеров по $\bmod m_p$ и $\mathfrak{H}_p = \mathfrak{E}_p$ — единичным классом вычетов по $\bmod m_p$. Поэтому в этом случае просто f_p есть порядок класса $p \bmod m_p$, $f_p g_p = \varphi(m_p)$, где $m = p^{\mu_p} m_p$ с $p \nmid m_p$. Поэтому имеет место представление в виде произведения

$$\zeta_m(s) = \prod_p \left(\frac{1}{1 - \frac{1}{p^{f_p s}}} \right)^{g_p} \tag{6a}$$

с этими значениями чисел f_p, g_p.

В случае $\zeta(s \mid \chi)$, где $\mathfrak{K}$ есть порожденная квадратичным характером χ группа порядка $k = 2$, мы можем, в отличие от предыдущих рассуждений, когда предполагалось $m > 0$ и потому также $f(\chi) > 0$, заранее нормировать характер χ по схеме (3), (4) п. 7, § 13 как четную числовую функцию и, кроме того, заранее предположить $m = f(\chi)$ (теперь уже не обязательно $m > 0$); действительно, при рассмотрении L-ряда $L(s \mid \chi)$ важны только значения $\chi(n)$ с натуральными n, а их это нормирование не затрагивает. Тогда, согласно XIX, п. 7, § 13, χ есть символ Кронекера с числителем $f(\chi)$. Подгруппа $\mathfrak{H}$, соответствующая $\mathfrak{K}$, в силу V, п. 4, § 13, характеризуется тогда в группе $\mathfrak{G}$ всех классов вычетов $a \bmod f(\chi)$, взаимно простых с модулем, тем, что $\left(\frac{f(\chi)}{a}\right) = 1$, т. е. это есть как раз группа, определенная и подробно рассмотренная в VI, п. 6, § 9. Для всех $p \nmid f(\chi)$ будет $k_p = 2$ и $\mathfrak{H}_p = \mathfrak{H}$; для конечного множества $p \mid f(\chi)$ будет $k_p = 1$. Следовательно, в этом случае

$$\begin{aligned}
&f_p = 1,\ g_p = 2 \quad \text{для } p \nmid f(\chi),\ p \text{ из } \mathfrak{H},\\
&f_p = 2,\ g_p = 1 \quad \text{для } p \nmid f(\chi),\ p \text{ не из } \mathfrak{H},\\
&f_p = 1,\ g_p = 1 \quad \text{для } p \nmid f(\chi),
\end{aligned}$$

и подробно записанное представление (6) принимает вид

$$\zeta(s|\chi)=\prod_{\substack{p\nmid f(\chi)\\ p\text{ из }\mathfrak{H}}}\left(\frac{1}{1-\frac{1}{p^s}}\right)^2\cdot\prod_{\substack{p\nmid f(\chi)\\ p\text{ не из }\mathfrak{H}}}\frac{1}{1-\frac{1}{p^{2s}}}\cdot\prod_{p\mid f(\chi)}\frac{1}{1-\frac{1}{p^s}}. \qquad (6б)$$

При использовавшемся до этого нормировании $f(\chi)>0$ характера χ группа $\mathfrak{H}$ определяется с помощью символа Кронекера с числителем $\chi(-1)f(\chi)$.

7. В качестве первого непосредственного следствия из представления (6) отметим неравенство

$$\zeta(s|\mathfrak{K})>1, \qquad (7)$$

которое в случае $\zeta_m(s)$, $\zeta(s|\chi)$ будет играть основную роль в нашем элементарно-аналитическом доказательстве.

Чтобы получить еще и второе следствие, которое будет играть основную роль в теоретико-функциональном доказательстве, мы представим себе отдельные сомножители из (6) разложенными в абсолютно сходящиеся ряды

$$\left(\frac{1}{1-\frac{1}{p^{f_p s}}}\right)^{g_p}=\sum_{\nu=0}^{\infty}\binom{\nu+g_p-1}{\nu}\frac{1}{p^{\nu f_p s}}$$

(эта формула доказывается (g_p-1)-кратным дифференцированием геометрической прогрессии $1/(1-x)=\sum_{\nu=0}^{\infty}x^\nu$) и затем почленно перемноженными. Последнее можно осуществить по схеме, похожей на получение тождества Эйлера, однако здесь это несколько сложнее ввиду наличия дополнительных показателей f_p и числовых коэффициентов $\binom{\nu+g_p-1}{\nu}$. Но и не производя фактически этого перемножения, мы можем быть уверенными, что для произведения $\zeta(s|\mathfrak{K})$ получается абсолютно сходящийся ряд Дирихле, первый член которого равен 1, а остальные коэффициенты — целые неотрицательные числа. Для теоретико-функционального доказательства в случаях $\zeta_m(s)$, $\zeta(s|\chi)$ именно это последнее свойство является основным.

Полученное нами сейчас представление $\zeta(s|\mathfrak{K})$ в виде абсолютно сходящегося ряда Дирихле совпадает с полученным ранее другим способом представлением (2). В этом можно убедиться двумя способами — или аналитическим, или алгебраическим.

Аналитически это немедленно следует из того, что коэффициенты a_n абсолютно сходящегося при $s>1$ ряда Дирихле

$$f(s)=\sum_n\frac{a_n}{n^s}$$

однозначно определяются значениями ряда $f(s)$ (так называемая теорема единственности для рядов Дирихле). Это доказывается аналогично соответствующему утверждению для степенных рядов. Достаточно показать, что из $f(s)=0$ для всех $s>1$ следует $a_n=0$ для всех n. Если бы это было не так и в первый раз $a_\nu \neq 0$, то мы записали бы предположение $f(s)=0$ в форме

$$a_\nu + \sum_{n>\nu} a_n \left(\frac{\nu}{n}\right)^s = 0$$

и совершили бы предельный переход $s \to +\infty$. Так как из абсолютной сходимости при $s>1$ следует равномерная сходимость в каждой области $s \geqslant 1+\delta$ с $\delta > 0$, то этот предельный переход можно выполнить почленно. Получается $a_\nu + 0 = 0$, что противоречит сделанному предположению.

При алгебраическом доказательстве мы будем исходить из лежащей в основе (6) формулы

$$\prod_{\chi \text{ из } \mathfrak{K}} \left(1 - \frac{\chi(p)}{p^s}\right) = \left(1 - \frac{1}{p^{f_p s}}\right)^{g_p}$$

для сомножителей, соответствующих отдельным простым числам p. Согласно ее выводу, она справедлива даже, если вместо $1/p^s$ подставить неизвестное x, т. е. как тождество многочленов

$$\prod_{\chi \text{ из } \mathfrak{K}} (1 - \chi(p)\, x) = (1 - x^{f_p})^{g_p}.$$

Отсюда формально-алгебраически, т. е. и для неизвестного x, вытекает тождество рядов

$$\prod_{\chi \text{ из } \mathfrak{K}} \sum_{\nu=0}^{\infty} \chi(p)^\nu x^\nu = \sum_{\nu=0}^{\infty} \binom{\nu + g_p - 1}{\nu} x^{\nu f_p},$$

которое означает, что коэффициенты ряда слева, получающегося почленным перемножением отдельных степенных рядов, совпадают с коэффициентами ряда справа. Для доказательства мы используем формулу суммы геометрической прогрессии в виде последовательности сравнений для многочленов $(1-x)\sum_{\nu=0}^{N-1} x^\nu \equiv$ $\equiv 1 \bmod x^N$ при всех натуральных N. Если тогда $P_N(\chi)$, P_N и Q_N обозначают соответствующие частичные суммы сомножителей из левой части, произведения из левой части и ряда из правой части, то, с одной стороны,

$$\prod_{\chi \text{ из } \mathfrak{K}} P_N(\chi) \equiv P_N \bmod x^N,$$

а, с другой стороны,

$$(1-\chi(p)\,x)\,P_N(\chi)\equiv 1,\ (1-x^{f_p})^{g_p}Q_N\equiv 1 \bmod x^N$$

(последнее получается полной индукцией по g_p), откуда на основании тождества многочленов вытекает сравнение

$$(1-x^{f_p})^{g_p}(P_N-Q_N)\equiv 0 \bmod x^N.$$

Так как $(1-x^{f_p})^{g_p}$ не содержит сомножителем x, отсюда следует $P_N\equiv Q_N \bmod x^N$, т. е. $P_N=Q_N$ для всех натуральных N, что и утверждалось. Тогда посредством замены $x=1/p^s$ получается тождество

$$\prod_{\chi \text{ из } \mathfrak{K}}\sum_{\nu=0}^{\infty}\frac{\chi(p)^\nu}{p^{\nu s}}=\sum_{\nu=0}^{\infty}\binom{\nu+g_p-1}{\nu}\frac{1}{p^{\nu f_p s}}$$

в том смысле, что ряд Дирихле слева, получающийся посредством почленного перемножения отдельных рядов Дирихле, имеет те же коэффициенты, что и ряд Дирихле справа. Но тогда то же самое следует и для ряда Дирихле, получающегося почленным перемножением по всем p, что можно заключить по той же схеме, по какой доказывалось тождество Эйлера. Но при этом в качестве коэффициентов ряда слева получаются, согласно приведенным выше формулам (3), (4), как раз $\sigma(n\,|\,\mathfrak{K})$ из (2). Поэтому коэффициенты ряда (2) действительно совпадают с коэффициентами ряда, получающегося в (6) после перемножения.

8. Благодаря доказанной теореме единственности мы получаем теперь для коэффициентов $\sigma(n\,|\,\mathfrak{K})$ произведения $\zeta(s\,|\,\mathfrak{K})$ в представлении (2) в виде ряда как дополнение к мало удобным для употребления формулам (3), (4) также и явные выражения через биномиальные коэффициенты, которые делают очевидными уже отмеченные целостность и неотрицательность этих коэффициентов. Именно, если заметить, что уже выведенное тождество для сомножителей, соответствующих отдельным p, определяет специальные коэффициенты $\sigma(p^\nu\,|\,\mathfrak{K})$, то в итоге получается

II. *Произведение*

$$\zeta(s\,|\,\mathfrak{K})=\prod_{\chi \text{ из } \mathfrak{K}}L(s\,|\,\chi)$$

собственных L-рядов для характеров χ из некоторой группы $\mathfrak{K}$ характеров по mod m *обладает представлением*

$$\zeta(s\,|\,\mathfrak{K})=\sum_n\frac{\sigma(n\,|\,\mathfrak{K})}{n^s}$$

в виде абсолютно сходящегося при $s>1$ ряда Дирихле с целыми неотрицательными коэффициентами $\sigma(n\,|\,\mathfrak{K})$, причем эти коэффи-

циенты, в соответствии с разложением $n = \prod_p p^{\nu}$ числа n на простые множители, мультипликативно составляются из специальных коэффициентов

$$\sigma(p^{\nu} \mid \mathfrak{K}) = \begin{cases} \binom{\nu_0 + g_p - 1}{\nu_0} & \text{для } \nu = \nu_0 f_p \\ 0 & \text{для } f_p \nmid \nu \end{cases},$$

где f_p, g_p имеют значения, определенные в I.

В интересующих нас здесь случаях $\zeta_m(s)$, $\zeta(s \mid \chi)$ числа f_p, g_p имеют специальные значения, определенные непосредственно после формулировки I. Относительно $\zeta_m(s)$ больше говорить нечего. Для $\zeta(s \mid \chi)$ закон для коэффициентов гласит

$$\sigma(p^{\nu} \mid \chi) = \begin{cases} \nu + 1 & \text{для } p \nmid f(\chi),\ p \text{ лежит в } \mathfrak{H} \\ 1 \text{ или } 0, \text{ в зависимости от того, четно или нечетно } \nu, & \\ & \text{для } p \nmid f(\chi),\ p \text{ не лежит в } \mathfrak{H} \\ 1 & \text{для } p \nmid f(\chi) \end{cases};$$

для этого случая это можно также без труда получить из (4). Кроме того, мы будем использовать также исходный закон для коэффициентов из (2), который здесь может быть записан в простой форме

$$\sigma(n \mid \chi) = \sum_{d \mid n} \chi(d).$$

2. Элементарно-аналитическое доказательство для неквадратичных характеров. В IV, п. 3, § 14 мы установили, что L-ряды

$$L(s \mid \chi) = \sum_n \frac{\chi(n)}{n^s}$$

с $\chi \neq \varepsilon$ *при натуральном порядке расположения членов* даже при $s > 0$ сходятся и представляют непрерывные функции от s. Помимо этого, для нашего доказательства нам понадобится:

III. *Функции $L(s \mid \chi)$ с $\chi \neq \varepsilon$ при $s > 0$ являются непрерывно дифференцируемыми, и их производные равны*

$$L'(s \mid \chi) = -\sum_n \frac{\chi(n) \ln n}{n^s},$$

т. е. получаются почленным дифференцированием.

Доказательство. Достаточно показать, что почленно продифференцированные ряды равномерно сходятся в каждой области $s \geqslant \delta$ с $\delta > 0$; действительно, тогда эти ряды можно будет почленно проинтегрировать в пределах от s до $+\infty$, в результате чего как раз получатся исходные ряды. Это доказательство

можно с небольшими изменениями получить по образцу доказательства утверждения IV, п. 3, § 14.

Кроме того, нам понадобится оценка

$$\ln n = \int_1^n \frac{dx}{x} < \int_1^n x^\varepsilon \frac{dx}{x} = \frac{n^\varepsilon - 1}{\varepsilon} < \frac{n^\varepsilon}{\varepsilon} \quad \text{для каждого } \varepsilon > 0.$$

Из нее, при $\varepsilon = \delta/2$, вытекает оценка

$$\frac{\ln n}{n^s} \leqslant \frac{\ln n}{n^\delta} < \frac{2}{\delta} \cdot \frac{1}{n^{\delta/2}} \quad \text{для всех } s \geqslant \delta.$$

Поэтому общий член продифференцированного ряда при $n \to \infty$ стремится к нулю равномерно для всех $s \geqslant \delta$. Следовательно, снова достаточно ограничиться оценкой специальных кусков ряда с $\varkappa f < n \leqslant Kf$.

Аналогично доказательству непрерывности (см. § 14, 3, IV) мы представим здесь эти куски ряда в форме

$$\sum_{\varkappa f < n \leqslant Kf} \frac{\chi(n) \ln n}{n^s} = \frac{1}{f^s} \sum_{r=1}^{f} \chi(r) \sum_{\varkappa \leqslant k < K} \left[\frac{\ln f + \ln(k+\rho)}{(k+\rho)^s} - \frac{\ln f + \ln(k+1)}{(k+1)^s} \right] =$$

$$= \frac{\ln f}{f^s} \sum_{r=1}^{f} \chi(r) \sum_{\varkappa \leqslant k < K} \left[\frac{1}{(k+\rho)^s} - \frac{1}{(k+1)^s} \right] +$$

$$+ \frac{1}{f^s} \sum_{r=1}^{f} \chi(r) \sum_{\varkappa \leqslant k < K} \left[\frac{\ln(k+\rho)}{(k+\rho)^s} - \frac{\ln(k+1)}{(k+1)^s} \right] = A + B$$

где положено $f = f(\chi)$ и $\rho = r/f$. Для первой двойной суммы, согласно вышеупомянутому доказательству, получается оценка

$$|A| \leqslant \frac{f^\delta \ln f}{f^\delta} \sum_{\varkappa \leqslant k < K} \frac{1}{k^{\delta+1}} \quad \text{для всех } s \geqslant \delta,$$

если только заранее выбрать $\varkappa \geqslant e^{1/\delta}$. Для второй двойной суммы посредством применения теоремы о среднем значении из дифференциального исчисления сначала получается

$$\frac{\ln(k+\rho)}{(k+\rho)^s} - \frac{\ln(k+1)}{(k+1)^s} = \frac{(1-\rho)\,[s \ln(k+\rho^*) - 1]}{(k+\rho^*)^{s+1}} \quad \text{с } \rho \leqslant \rho^* \leqslant 1,$$

а отсюда, на основании предположения $\varkappa \geqslant e^{1/\delta}$, далее,

$$0 \leqslant \frac{\ln(k+\rho)}{(k+\rho)^s} - \frac{\ln(k+1)}{(k+1)^s} \leqslant \frac{\delta \ln(k+1)}{k^{\delta+1}} \quad \text{для всех } s \geqslant \delta.$$

Так как, согласно сказанному выше, $\ln(k+1) \leqslant \ln 2k < 2(2k)^{\delta/2}/\delta$

для второй двойной суммы получается оценка

$$|B| \leqslant \frac{2f \cdot 2^{\frac{1}{2}\delta}}{f^{\delta}} \sum_{x \leqslant k < K} \frac{1}{k^{\frac{1}{2}\delta+1}} \text{ для всех } s \geqslant \delta.$$

Теперь утверждение следует из сходимости дзета-рядов $\zeta(1+\delta)$ и $\zeta(1+\delta/2)$ так же, как в доказательстве непрерывности.

В силу доказанного высказывания III, для каждого характера $\chi \neq \varepsilon$

$$\lim_{s \to 1} \frac{L(s|\chi) - L(1|\chi)}{s-1} = L'(1|\chi)$$

существует и конечен. Если бы для некоторого характера $\chi_1 \neq \varepsilon$ имело бы место $L(1|\chi_1) = 0$, то также существовал и был бы конечным

$$\lim_{s \to 1} \frac{L(s|\chi_1)}{s-1} = L'(1|\chi_1).$$

Мы попытаемся получить отсюда в связи с доказанным в II, п. 4, § 12 предельным соотношением

$$\lim_{s \to 1+0} (s-1)\zeta(s) = 1$$

противоречие с поведением рассмотренного в п. 1 произведения

$$\zeta_m(s) = \zeta(s) \prod_{\chi \neq \varepsilon} L(s|\chi).$$

Для этого запишем это произведение в виде

$$\zeta_m(s) = (s-1)\zeta(s) \cdot \frac{L(s|\chi_1)}{s-1} \cdot \prod_{\chi \neq \varepsilon, \chi_1} L(s|\chi).$$

Если бы было $L(1|\chi_1) = 0$, то из указанных предельных соотношений для ζ_s, $L(s|\chi_1)$ и непрерывности остальных $L(s|\chi)$ получалось бы, что $\zeta_m(s)$ при $s \to 1+0$ стремится к конечному пределу. Однако это еще не составляет противоречия с тем, что мы пока знаем относительно $\zeta_m(s)$. В силу (7) п. 1, нам известно в этом отношении только, что во всяком случае $\zeta_m(s) > 1$ для всех $s > 1$. Однако этого факта уже достаточно, чтобы получить указанным образом противоречие с предположением, что для двух различных характеров χ_1, $\chi_2 \neq \varepsilon$ имеет место $L(1|\chi_1)$, $L(1|\chi_2) = 0$. Для этого запишем результат отношения в форме

$$\frac{\zeta_m(s)}{s-1} = (s-1)\zeta(s) \frac{L(s|\chi_1)}{s-1} \cdot \frac{L(s|\chi_2)}{s-1} \cdot \prod_{\chi \neq \varepsilon, \chi_1, \chi_2} L(s|\chi).$$

Из нашего предположения следует, что $\zeta_m(s)/(s-1)$ стремится к конечному пределу при $s \to 1+0$. Однако это противоречит тому, что $\zeta_m(s) > 1$ для всех $s > 1$.

Тем самым доказано, что среди $\varphi(m)-1$ характеров $\chi \neq \varepsilon$ группы классов вычетов по $\bmod m$, взаимно простых с модулем, самое большее для одного χ_1 может иметь место $L(1|\chi_1)=0$. Этот характер χ_1 должен быть тогда обязательно вещественным, т. е. квадратичным; действительно, в противном случае он был бы отличен от сопряженного с ним характера $\overline{\chi_1}$, а для этого последнего тоже имело бы место $L(1|\overline{\chi_1})=0$. Поэтому мы можем считать установленным

IV. *Для каждого неквадратичного характера* $\chi \neq \varepsilon$ $L(1|\chi) \neq 0$. *Среди квадратичных характеров по* $\bmod m$ *самое большее для одного* χ_1 *имеет место* $L(1|\chi_1)=0$.

В результате сказанного мы можем установить

V. *Если* $\lim\limits_{s\to 1+0} \zeta_m(s)=\infty$, *то* $L(1|\chi)\neq 0$ *для всех* $\chi \neq \varepsilon$.

Относительно результата IV заметим еще следующее. Модуль m играет здесь лишь вспомогательную роль. Действительно, характер χ с ведущим модулем $f(\chi)$ встречается среди характеров по $\bmod m$ для каждого кратного m числа $f(\chi)$. Поэтому два различных характера χ, ψ встречаются вместе среди характеров по $\bmod m$ для какого-нибудь общего кратного m их ведущих модулей $f(\chi)$, $f(\psi)$. Следовательно, мы можем сказать точнее, чем в IV:

IV′. *Среди всех квадратичных характеров вообще самое большее для одного* χ_1 *может иметь место* $L(1|\chi_1)=0$.

Впрочем, этот последний результат, несмотря на свой почти исчерпывающий характер, не дает никакого облегчения для остающейся части доказательства, так как он ничего не устанавливает относительно, быть может, существующего исключительного квадратичного характера χ_1.

3. Элементарно-аналитическое доказательство для квадратичных характеров. Докажем теперь последний факт, необходимый для завершения доказательства теоремы Дирихле:

VI. *Для каждого квадратичного характера* χ $L(1|\chi)\neq 0$.

Доказательство. В то время как в изложенном в п. 2 доказательстве для неквадратичных характеров $\chi \neq \varepsilon$ мы основывались на свойствах рассмотренного в п. 1 произведения $\zeta_m(s)=\zeta(s)\prod\limits_{\chi\neq\varepsilon} L(1|\chi)$ всех L-рядов по $\bmod m$, теперь мы будем использовать свойства также рассмотренного там частичного произведения

$$\zeta(s|\chi)=\zeta(s)L(s|\chi)=\sum_n \frac{\sigma(n|\chi)}{n^s}. \tag{1}$$

Однако, если в п. 2 мы довольствовались слабым высказыванием $\zeta_m(s)>1$ для $s>1$, которое может быть получено просто

из разложения в произведение, без знания коэффициентов $\sigma_m(n)$ для рядов, то здесь нам понадобится более сильное высказывание относительно $\zeta(s|\chi)$, для которого существенны арифметические свойства коэффициентов $\sigma(n|\chi)$. Как мы установили в II, п. 1, эти коэффициенты $\sigma(n|\chi)$ являются целыми неотрицательными числами. Далее, согласно формулам в конце п. 1, $\sigma(n|\chi)=0$ тогда и только тогда, когда в n входит с нечетным показателем степени простое число p, не входящее в $f(\chi)$ и не лежащее в группе $\mathfrak{H}$. Но это условие заведомо не может выполняться для чисел $n=n_0^2$, являющихся квадратами. Поэтому

$$\sigma(n|\chi)\geqslant 0 \quad \text{для всех } n,$$
$$\sigma(n|\chi)\geqslant 1 \quad \text{для } n=n_0^2.$$

Отсюда следует, что ряд

$$\zeta\left(\frac{1}{2}\middle|\chi\right)=\sum_n \frac{\sigma(n|\chi)}{\sqrt{n}} \text{ расходится.} \tag{2}$$

Действительно, его члены неотрицательны, а частичный ряд из членов с $n=n_0^2$ имеет в качестве миноранты расходящийся гармонический ряд $\sum_{n_0}\frac{1}{n_0}$.

На этом факте (2) и будет основываться наше доказательство. Именно, мы покажем, что из $L(1|\chi)=0$ следовала бы сходимость ряда $\zeta\left(\frac{1}{2}\middle|\chi\right)$.

Для краткости обозначим

$$L(s)=L(s|\chi), \quad Z(s)=\zeta(s|\chi), \quad \sigma(n)=\sigma(n|\chi).$$

Далее, для ряда Дирихле

$$f(s)=\sum_n \frac{a_n}{n^s}$$

будем вообще обозначать через

$$f_x(s)=\sum_{n\leqslant x}\frac{a_n}{n^s}, \quad f^x(s)=\sum_{n>x}\frac{a_n}{n^s}$$

его частичные суммы и остатки, и при этом из формальных соображений мы не будем предполагать расщепляющее число x обязательно целым, а будем допускать для него любые положительные вещественные значения. В действительности, конечно, будет подразумеваться целая часть $N=[x]$ числа x, определяемая посредством $N\leqslant x<N+1$.

Как было установлено в конце п. 1, для коэффициентов $\sigma(n)$ из формулы (1), которая теперь запишется в виде

$$Z(s) = \zeta(s) L(s) = \sum_n \frac{\sigma(n)}{n^s},$$

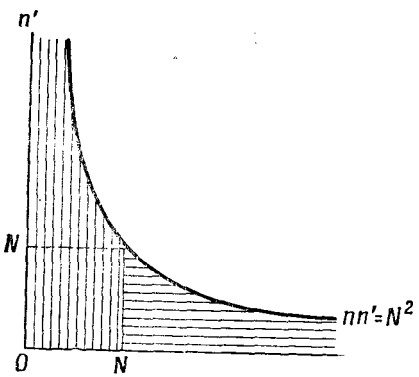
выполняются формулы

$$\sigma(n) = \sum_{d \mid n} \chi(d).$$

Рассмотрим теперь специальную частичную сумму

$$Z_{N^2}\left(\frac{1}{2}\right) = \sum_{n \leqslant N^2} \frac{\sigma(n)}{\sqrt{n}}$$

ряда $Z(1/2)$, который, согласно (2), расходится с пределом суммирования N^2, являющимся квадратом. С помощью формул для коэффициентов мы выведем для нее аналогичное формуле для $Z(s)$ соотношение, в котором будут фигурировать частичные суммы $\zeta_x(1/2)$ и остатки $L^x(1/2)$. При этом $L^x(1/2)$ можно будет оценить, а $\zeta_x(1/2)$ выразить в элементарной форме с точностью до не имеющих значения членов. Как и следовало ожидать, будет фигурировать частичная сумма $L_N(1/2)$, но кроме нее неожиданно появится и частичная сумма $L_N(1)$. Тогда получающееся таким образом соотношение между $Z_{N^2}(1/2)$ и $L_N(1/2)$, $L_N(1)$ позволит с помощью предельного перехода при $N \to \infty$ сделать заключение, что из $L(1) = 0$ следовала бы сходимость ряда $Z(1/2)$.



Фиг. 7.

Приступим к проведению доказательства по этой схеме. Прежде всего, в силу имеющихся у нас формул для коэффициентов, получается

$$Z_{N^2}\left(\frac{1}{2}\right) = \sum_{n \leqslant N^2} \sum_{d \mid n} \frac{\chi(d)}{\sqrt{n}}.$$

Если положить $n = dn'$ и ввести n' вместо n в качестве независимого индекса суммирования наряду с d, то эта двойная сумма будет распространена на все пары натуральных чисел d, n' с $dn' \leqslant N^2$. Если вместо d снова писать n, то мы будем

поэтому иметь

$$Z_{N^2}\left(\frac{1}{2}\right)=\sum_{nn'\leqslant N^2}\frac{1}{\sqrt{n'}}\frac{\chi(n)}{\sqrt{n}}.$$

Если сумму разбить на две суммы, как показано штриховкой на фиг. 7, то

$$Z_{N^2}\left(\frac{1}{2}\right)=\sum_{n\leqslant N}\frac{\chi(n)}{\sqrt{n}}\sum_{n'\leqslant\frac{N^2}{n}}\frac{1}{\sqrt{n'}}+\sum_{n'<N}\frac{1}{\sqrt{n'}}\sum_{N<n\leqslant\frac{N^2}{n'}}\frac{\chi(n)}{\sqrt{n}},$$

или также

$$Z_{N^2}\left(\frac{1}{2}\right)=\sum_{n\leqslant N}\frac{\chi(n)}{\sqrt{n}}\zeta_{\frac{N^2}{n}}\left(\frac{1}{2}\right)+\sum_{n<N}\frac{1}{\sqrt{n}}\left[L^N\left(\frac{1}{2}\right)-L^{\frac{N^2}{n}}\left(\frac{1}{2}\right)\right]. \quad (3)$$

Теперь нам нужно получить явное значение для частичных сумм $\zeta_x(1/2)$ и оценку для остатков $L^x(1/2)$.

а) Определение частичных сумм $\zeta_x(1/2)$. Как и в § 12, п. 4,

$$\int_{n\ (n\geqslant 1)}^{n+1}\frac{du}{\sqrt{u}}<\frac{1}{\sqrt{n}}<\int_{n-1\ (n>1)}^{n}\frac{du}{\sqrt{u}},$$

и потому

$$\int_1^x\frac{du}{\sqrt{u}}<\int_1^{[x]+1}\frac{du}{\sqrt{u}}<\zeta\left(\frac{1}{2}\right)<1+\int_1^{[x]}\frac{du}{\sqrt{u}}<1+\int_1^x\frac{du}{\sqrt{u}},$$

т. е.

$$2\sqrt{x}-2<\zeta_x\left(\frac{1}{2}\right)<2\sqrt{x}-1.$$

Однако для нашей цели эта двусторонняя оценка для $\zeta_x(1/2)$ не является достаточной; напротив, мы должны определить $\zeta_x(1/2)$ с точностью до члена с порядком возрастания $O(1/\sqrt{x})$. Это достигается следующим образом посредством более тонкого сравнения с интегралом $\int_1^x\frac{du}{\sqrt{u}}$. Мы имеем

$$\zeta_x\left(\frac{1}{2}\right)-(2\sqrt{x}-2)=\sum_{n\leqslant x}\frac{1}{\sqrt{n}}-\int_1^x\frac{du}{\sqrt{u}}=$$

$$=\sum_{n\leqslant x}\int_n^{n+1}\left(\frac{1}{\sqrt{n}}-\frac{1}{\sqrt{u}}\right)du+\int_x^{[x]+1}\frac{du}{\sqrt{u}}.$$

Здесь в правой части второе слагаемое $< 1/\sqrt{x}$. Первое слагаемое есть соответствующая x частичная сумма сходящегося ряда с положительными членами

$$a = \sum_n \int_n^{n+1} \left(\frac{1}{\sqrt{n}} - \frac{1}{\sqrt{u}}\right) du < \sum_n \left(\frac{1}{\sqrt{n}} - \frac{1}{\sqrt{n+1}}\right) = 1$$

со следующей оценкой для остатка:

$$\sum_{n>x} \int_n^{n+1} \left(\frac{1}{\sqrt{n}} - \frac{1}{\sqrt{u}}\right) du < \sum_{n>x} \left(\frac{1}{\sqrt{n}} - \frac{1}{\sqrt{n+1}}\right) < \frac{1}{\sqrt{x}}.$$

Таким образом, если частичную сумму $\sum_{n\leqq x}$ заменить полной суммой $a = \sum_n$, то справа нужно будет еще добавить отрицательный остаток, абсолютная величина которого $\leqq 1/\sqrt{x}$. В итоге тем самым получается

$$\zeta_x\left(\frac{1}{2}\right) = 2\sqrt{x} - 2 + a + \frac{\theta_x}{\sqrt{x}} \quad \text{с } |\theta_x| < 1.$$

Точное значение постоянной a, входящей в это соотношение, не играет роли. Во всяком случае для нее, в соответствии с нашим выводом, справедливы неравенства $0 < a < 1$.

После того как мы определили частичные суммы $\zeta_x(1/2)$ первый член в (3) определяется с точностью до не имеющей значения ошибки следующим образом:

$$\sum_{n\leqq N} \frac{\chi(n)}{\sqrt{n}} \zeta_{N^2/n}\left(\frac{1}{2}\right) = \sum_{n\leqq N} \frac{\chi(n)}{\sqrt{n}} \left(2\frac{N}{\sqrt{n}} - 2 + a\right) + \sum_{n\leqq N} \frac{\chi(n)}{\sqrt{n}} \frac{\theta_{N^2/n}\sqrt{n}}{N} =$$

$$= 2L_N(1)\,N - (2-a)\,L_N\left(\frac{1}{2}\right) + \frac{1}{N}\sum_{n\leqq N} \chi(n)\,\theta_{N^2/n} =$$

$$= 2L_N(1)\,N - (2-a)\,L_N\left(\frac{1}{2}\right) + \theta_N \quad \text{с } |\theta_N| < 1.$$

Фигурирующая здесь частичная сумма $L_N(1/2)$ ограничена при $N \to \infty$, ибо ряд $L(1/2)$, согласно IV, п. 3, § 14, сходится. Поэтому для первого члена в (3) получается выражение

$$\sum_{n\leqq N} \frac{\chi(n)}{\sqrt{n}} \zeta_{N^2/n}\left(\frac{1}{2}\right) = 2L_N(1)\,N + O(1) \tag{4a}$$

с точностью до ошибки порядка $O(1)$ (т. е. ограниченной при $N \to \infty$).

б) Оценка остатков $L^x(1/2)$. Мы оценим остатки $L^x(s)$ для любого $s > 0$, так как в конце нам понадобится оценка и для

$L^x(1)$. Введем в рассмотрение частичные суммы коэффициентов

$$L_x(0) = \sum_{n \leqslant x} \chi(n)$$

ряда

$$L(s) = \sum_n \frac{\chi(n)}{n^s}.$$

Тогда коэффициенты $\chi(n)$ можно представить в виде разностей

$$\chi(n) = L_n(0) - L_{n-1}(0).$$

Если эти выражения подставить в ряд $L(s)$, то посредством так называемого частичного суммирования мы получим

$$L^x(s) = \sum_{n>x} \frac{L_n(0) - L_{n-1}(0)}{n^s} = \sum_{n>x} \frac{L_n(0)}{n^s} - \sum_{n>x} \frac{L_n(0)}{(n+1)^s} - \frac{L_{[x]}(0)}{([x]+1)^s} =$$

$$= \sum_{n>x} L_n(0)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) - \frac{L_{[x]}(0)}{([x]+1)^s}.$$

Так как $\sum_{n \bmod f} \chi(n) = 0$ для каждой полной системы вычетов $n \bmod f$, где $f = f(\chi)$ есть ведущий модуль характера χ, то, очевидно,

$$|L_x(0)| = \left|\sum_{n \leqslant x} \chi(n)\right| \leqslant \frac{1}{2} f \text{ для каждого } x.$$

Отсюда для остатка $L^x(s)$ получается оценка

$$|L^x(s)| < \frac{1}{2} f \frac{1}{([x]+1)^s} + \frac{1}{2} f \frac{1}{([x]+1)^s} < \frac{f}{x^s}.$$

В частности $|L^x(1/2)| < f/\sqrt{x}$. Тогда для второго члена в (3) получается оценка

$$\left|\sum_{n<N} \frac{1}{\sqrt{n}}\left[L^N\left(\frac{1}{2}\right) - L^{\frac{N^2}{n}}\left(\frac{1}{2}\right)\right]\right| < f \sum_{n \leqslant N} \frac{1}{\sqrt{n}}\left(\frac{1}{\sqrt{N}} + \frac{\sqrt{n}}{N}\right) =$$

$$= \frac{f}{\sqrt{N}} \zeta_N\left(\frac{1}{2}\right) + f.$$

Но, как доказано выше, заведомо $\zeta_N(1/2) < 2\sqrt{N}$. Поэтому оценка для второго члена из (3) принимает вид

$$\left|\sum_{n<N} \frac{1}{\sqrt{n}}\left[L^N\left(\frac{1}{2}\right) - L^{\frac{N^2}{n}}\left(\frac{1}{2}\right)\right]\right| < 3f, \tag{4б}$$

откуда следует, что этот член имеет порядок возрастания $O(1)$.

Согласно (3), из (4а) и (4б) следует соотношение

$$\mathsf{Z}_{N^2}\left(\frac{1}{2}\right) = 2L_N(1)\,N + 0(1)$$

или также

$$\mathsf{Z}_{N^2}\left(\frac{1}{2}\right) = 2L(1)\,N - 2L^N(1)\,N + O(1).$$

Как доказано только что, $|L^N(1)| < f/N$, т. е. и второй член справа имеет порядок $O(1)$, а потому

$$\mathsf{Z}_{N^2}(1/2) = 2L(1)\,N + O(1).$$

Если бы теперь было $L(1) = 0$, то из последнего соотношения следовало бы, что $\mathsf{Z}_{N^2}(1/2)$ ограничено при $N \to \infty$. Но это противоречит установленной в (2) расходимости ряда $\mathsf{Z}(1/2)$, из которой, в силу неотрицательности членов, вытекает неограниченность также и специальных частичных сумм $\mathsf{Z}_{N^2}(1/2)$. Поэтому необходимо имеет место $L(1) \neq 0$, что и требовалось доказать.

Тем самым наше элементарно-аналитическое доказательство теоремы Дирихле о простых числах завершено.

4. Теоретико-функциональный метод доказательства. Если предполагать известными элементы теории функций комплексного переменного, то не только делается более ясным данное только что элементарно-аналитическое доказательство необращения L-рядов в нуль, но и появляется возможность понять с аналитической точки зрения глубокие основания этого факта, в результате чего можно будет различными способами получить новые, краткие и четкие доказательства.

1. Мы должны предпослать некоторые общие факты относительно рядов Дирихле

$$f(s) = \sum_n \frac{a_n}{n^s},$$

причем теперь s рассматривается как комплексная переменная и под n^s понимается $n^s = e^{s \ln n}$ с вещественным $\ln n$. При этом — а также и при окончательных применениях к дзета-функции и L-рядам — мы ограничимся лишь беглым обзором, так как теоретико-функциональная сторона вещей, естественно, не стоит в центре внимания этой книги, посвященной теории чисел.

Мы представим комплексную переменную в обычной форме $s = \sigma + it$ с вещественными σ, t. Подобно тому как для степенных рядов комплексной переменной x область сходимости зависит только от абсолютной величины $|x|$, в случае рядов Дирихле область сходимости зависит только от вещественной части σ. Как там область сходимости задается неравенством $|x| < r$ (т. е.

кру́гом), так здесь область сходимости задается неравенством $\sigma > \alpha$ (т. е. правой полуплоскостью), причем и здесь, как и там, вопрос о сходимости на границе может решаться по-разному. Мы будем называть α (вещественное число или $\pm\infty$) абсциссой сходимости. Описанное выше положение со сходимостью правдоподобно потому, что абсолютная величина общего члена $|a_n/n^s| = |a_n|/n^\sigma$ зависит только от вещественной части.

Для доказательства нужно показать, что из сходимости $f(s)$ для $s_0 = \sigma_0 + it_0$ следует сходимость для всех комплексных чисел s с $\sigma > \sigma_0$. Одновременно мы проведем и доказательство того, что сходимость является тогда равномерной в каждой области $\sigma \geqslant \sigma_0 + \delta$, $|t - t_0| \leqslant T$ с $\delta > 0$, $T > 0$, т. е. что функция $f(s)$ является регулярной аналитической функцией в области $\sigma > \sigma_0$. При этом вместо сходимости $f(s_0)$ нам достаточно будет предполагать только, что частичные суммы $f_n(s_0)$ ограничены. Мы имеем

$$f(s) = \sum_n \frac{a_n}{n^{s_0}} \frac{1}{n^{s-s_0}} = \sum_n \frac{f_n(s_0) - f_{n-1}(s_0)}{n^{s-s_0}}.$$

Отсюда, подобно тому как в п. 3 при оценке остатка, для общего куска ряда с $\nu < n \leqslant N$ частичным суммированием получается представление

$$f_N(s) - f_\nu(s) = \sum_{\nu < n \leqslant N} f_n(s_0) \left(\frac{1}{n^{s-s_0}} - \frac{1}{(n+1)^{s-s_0}} \right) - \\ - \frac{f_\nu(s_0)}{(\nu+1)^{s-s_0}} + \frac{f_N(s_0)}{(N+1)^{s-s_0}}.$$

Но здесь

$$\frac{1}{n^{s-s_0}} - \frac{1}{(n+1)^{s-s_0}} = (s - s_0) \int_n^{n+1} \frac{du}{u^{s-s_0+1}},$$

откуда

$$\left| \frac{1}{n^{s-s_0}} - \frac{1}{(n+1)^{s-s_0}} \right| \leqslant \frac{(\sigma - \sigma_0) + |t - t_0|}{n^{\sigma-\sigma_0+1}},$$

и потому, как в доказательстве утверждения IV, п. 3, § 14,

$$\left| \frac{1}{n^{s-s_0}} - \frac{1}{(n+1)^{s-s_0}} \right| \leqslant \frac{\delta + T}{n^{\delta+1}},$$

если только заранее взято $\nu \geqslant e^{1/\delta}$. Отсюда и из предполагаемой ограниченности $|f_n(s_0)| \leqslant C$ в области $\sigma \geqslant \sigma_0 + \delta$, $|t - t_0| \leqslant T$ получается равномерная оценка

$$|f_N(s) - f_\nu(s)| \leqslant C(\delta + T)[\zeta_N(1+\delta) - \zeta_\nu(1+\delta)] + \frac{2C}{\nu^\delta},$$

и потому вследствие сходимости $\zeta(1+\delta)$ — равномерная сходи-

мость $f(s)$ в этой области. Нижняя грань всех этих σ_0 и дает абсциссу сходимости α.

Если вместо ограниченности $f_n(s_0) = O(1)$ сделать более общее предположение $f_n(s_0) = O(n^\gamma)$ с вещественным $\gamma \geqslant 0$, то таким же способом мы получим сходимость для $\sigma > \sigma_0 + \gamma$. Таким образом, если мы будем, в частности, знать, что для частичных сумм коэффициентов имеет место $f_n(0) = O(n^\gamma)$, то для абсциссы сходимости мы получим $\alpha \leqslant \gamma$.

Наряду с абсциссой сходимости α для ряда Дирихле можно определить также абсциссу сходимости β для ряда абсолютных величин. С одной стороны, очевидно, $\alpha \leqslant \beta$. С другой стороны, $\beta \leqslant \alpha + 1$; действительно, из сходимости $f(s_0)$ следует $|a_n / n^{s_0}| \leqslant C$, т. е. мажорирование $|a_n / n^s| \leqslant C / n^{\sigma - \sigma_0}$ посредством членов дзета-ряда $C\zeta(\sigma - \sigma_0)$, сходящегося для $\sigma - \sigma_0 > 1$, т. е. следует абсолютная сходимость $f(s)$ для $\sigma > \sigma_0 + 1$. В отличие от степенных рядов, для рядов Дирихле может быть $\alpha < \beta$; тогда между абсциссами α и β лежит полоса условной сходимости, ширина которой не превосходит 1.

2. Для дзета-ряда, согласно II, п. 4, § 12, абсцисса сходимости $\alpha = 1$, а также и абсцисса абсолютной сходимости $\beta = 1$. Поэтому в полуплоскости $\sigma > 1$ $\zeta(s)$ есть регулярная аналитическая функция. Для остальных L-рядов, согласно IV, п. 3, § 14, абсцисса сходимости $\alpha = 0$ — очевидно с расходимостью при $\sigma = 0$, — напротив, абсцисса абсолютной сходимости $\beta = 1$. Поэтому $L(s|\chi)$ с $\chi \neq \varepsilon$ являются регулярными аналитическими функциями в полуплоскости $\sigma > 0$.

Аналогично тому, как для степенных рядов геометрическая прогрессия (все коэффициенты равны 1) может быть аналитически продолжена из ее круга сходимости $|x| < 1$ на всю плоскость, так и для рядов Дирихле дзета-ряд (все коэффициенты равны 1) может быть аналитически продолжен из его полуплоскости сходимости $\sigma > 1$ на всю плоскость; для геометрической прогрессии при этом аналитическом продолжении получается один-единственный полюс при $x = 1$ с вычетом -1, и, аналогично, при аналитическом продолжении для дзета-ряда получается один-единственный полюс при $s = 1$ с вычетом 1; однако для дзета-ряда эти факты доказываются не так просто, как для геометрической прогрессии. Мы удовлетворимся здесь доказательством аналитической продолжаемости на полуплоскость $\sigma > 0$ и высказывания о полюсе; последнее для нас особенно важно. И то, и другое получается из тождества

$$\left(1 - \frac{2}{2^s}\right)\zeta(s) = \left(1 - \frac{2}{2^s}\right)\sum_n \frac{1}{n^s} = \sum_n \frac{1}{n^s} - 2\sum_k \frac{1}{(2n)^s} =$$

$$= \frac{1}{1^s} - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \ldots.$$

Фигурирующий здесь ряд Дирихле имеет ограниченные частичные суммы коэффициентов. Поэтому его абсцисса сходимости $\alpha \leqslant 0$. Следовательно, он представляет для $\sigma > 0$ регулярную аналитическую функцию. Деление этой функции на $1-2/2^s$ дает аналитическое представление для $\zeta(s)$ при $\sigma > 0$. В качестве полюсов $\zeta(s)$ на этой полуплоскости могут получиться только нули выражения $1-2/2^s$; это суть точки $s = 1 + 2g\pi i/\ln 2$ для всех целых g. Среди них $s=1$ заведомо является полюсом, потому что $1 - 1/2 + 1/3 - 1/4 + \ldots = \ln 2 \neq 0$; в силу $\lim\limits_{s\to 1} \frac{1-2/2^s}{s-1} = \ln 2$, в качестве вычета получается

$$\lim_{s\to 1} (s-1)\,\zeta(s) = 1.$$

Частично мы познакомились с этим предельным соотношением уже в § 12, п. 4 (при приближении к 1 по вещественным $s > 1$). Остальные точки $s = 1 + 2g\pi i/\ln 2$ с $g \neq 0$ не являются полюсами функции $\zeta(s)$. В этом можно убедиться на основании единственности аналитического продолжения, если провести такие же рассуждения с множителем $1 - k/k^s$ для какого-нибудь натурального $k \geqslant 2$. Получающийся тогда ряд Дирихле

$$\left(1-\frac{k}{k^s}\right)\zeta(s) = \left(1-\frac{k}{k^s}\right)\sum_n \frac{1}{n^s} = \sum_n \frac{1}{n^s} - k\sum_n \frac{1}{(kn)^s} =$$

$$= \left(\frac{1}{1^s} + \ldots + \frac{1}{(k-1)^s} - \frac{(k-1)}{k^s}\right) +$$

$$+ \left(\frac{1}{(k+1)^s} + \ldots + \frac{1}{(2k-1)^s} - \frac{k-1}{(2k)^s}\right) + \ldots,$$

очевидно, также имеет ограниченные частичные суммы коэффициентов и потому регулярно аналитичен для $\sigma > 0$. Если, в частности, в качестве k взять каких-нибудь два различных простых числа p, q, то совокупности нулей $1 + 2g\pi i/\ln p$, $1 + 2h\pi i/\ln q$ (g, h — целые) будут иметь только одно общее число 1, так как уравнение $p^h = q^g$ имеет лишь одно решение $g = 0$, $h = 0$.

В итоге мы получаем

VII. *Дзета-ряд $\zeta(s)$ можно аналитически продолжить из его полуплоскости сходимости $\sigma > 1$ на полуплоскость $\sigma > 0$, где он будет регулярной аналитической функцией, за исключением полюса первого порядка при $s = 1$ с вычетом равным 1.*

Остальные L-ряды $L(s|\chi)$ ($\chi \neq \varepsilon$) являются повсюду в их полуплоскости сходимости $\sigma > 0$ регулярными аналитическими функциями.

3. На основании этой более глубокой теоретико-функциональной точки зрения становится, прежде всего, совершенно прозрачным

наше элементарно-аналитическое доказательство из п. 2 для необращения в нуль всех $L(1|\chi)$ за исключением, быть может, одного $L(1|\chi_1)$ с квадратичным характером χ_1. Именно, согласно VII, произведение

$$\zeta_m(s) = \zeta(s) \prod_{\chi \neq \varepsilon} L(s|\chi)$$

также является для $\sigma > 0$ регулярной аналитической функцией, за исключением, быть может, полюса первого порядка при $s = 1$. Относительно ν—степени первого, отличного от нуля, члена ряда Лорана $\zeta_m(s)$ в точке $s = 1$, имеются тогда следующие три возможности:

(а) $\nu = -1$; тогда все $L(1|\chi) \neq 0$ и $\zeta_m(s)$ имеет при $s = 1$ полюс первого порядка с вычетом

$$\lim_{s \to 1} (s-1)\zeta_m(s) = \prod_{\chi \neq \varepsilon} L(1|\chi).$$

(б) $\nu = 0$; тогда точно для одного χ_1 $L(1|\chi_1) = 0$, причем нуль первого порядка, и $\zeta_m(s)$ при $s = 1$ регулярна и $\neq 0$.

(в) $\nu \geqslant 1$; тогда или $L(1|\chi_1) = 0$ с нулем порядка выше первого, или по меньшей мере для двух χ_1, χ_2 имеет место $L(1|\chi_1)$, $L(1|\chi_2) = 0$ и $\zeta_m(s)$ тогда имеет нуль при $s = 1$.

Поэтому:

VIII. *Утверждение, что все* $L(1|\chi) \neq 0$, *равносильно утверждению, что* $\zeta_m(s)$ *имеет при* $s = 1$ *полюс.*

Согласно нашему элементарно-аналитическому доказательству в п. 3, оба этих эквивалентных друг другу утверждения действительно имеют силу, т. е. имеет место обстоятельство (а). Чтобы доказать это прозрачным способом с помощью дальнейшего использования теоретико-функциональных средств, мы исключим возможности (б) и (в).

Возможность (в), очевидно, исключается в силу грубого свойства $\zeta_m(s) > 1$, получающегося в (7) п. 1 из представления(6). В случае (б) характер χ_1 должен тогда, как показано в п. 2, обязательно быть вещественным, т. е. квадратичным; для исключения этой возможности достаточно тогда показать наличие особенности при $s = 1$ не для полного произведения $\zeta_m(s)$, а лишь для каждого частичного произведения

$$\zeta(s|\chi) = \zeta(s) L(s|\chi)$$

с квадратичным χ, или доказать одно из предельных соотношений

$$\lim_{s \to 1+0} \zeta_m(s) = +\infty, \qquad \lim_{s \to 1+0} \zeta(s|\chi) = +\infty$$

для вещественных $s > 1$, или, наконец, только установить неограниченность $\zeta_m(s)$ или $\zeta(s|\chi)$ для вещественных $s > 1$ (из которой,

впрочем, тотчас же будут следовать вышеупомянутые предельные соотношения в силу неотрицательности коэффициентов у рядов Дирихле).

4. Первое из указанных утверждений (наличие особенности при $s=1$), носящее чисто теоретико-функциональный характер, может быть получено из одной *общей теоремы о рядах Дирихле*

$$f(s)=\sum_n \frac{a_n}{n^s}$$

с вещественными неотрицательными коэффициентами a_n, *согласно которой представляемая этим рядом функция, в том случае если абсцисса сходимости* α *конечна, имеет особенность при* $s=\alpha$. Доказательство настолько просто, что мы его здесь приведем. Предположим, что получающаяся из этого ряда посредством аналитического продолжения функция $f(s)$ при $s=\alpha$ регулярна. Тогда разложение $f(s)$ в степенной ряд в окрестности точки $s=\alpha+\delta$ с некоторым $\delta>0$ сходится в круге радиуса, большего, чем δ, с центром в этой точке, т. е. заведомо сходится для лежащего достаточно близко от α вещественного $s<\alpha$. Это разложение в степенной ряд имеет вид

$$f(s)=\sum_{\nu=0}^{\infty}\frac{1}{\nu!}f^{(\nu)}(\alpha+\delta)\,[s-(\alpha+\delta)]^{\nu}.$$

Так как ряд Дирихле $f(s)$ равномерно сходится, скажем, при $|s-(\alpha+\delta)|\leqslant(\delta/2)^{\delta}$, и так как равномерно сходящийся ряд регулярных аналитических функций можно дифференцировать почленно сколько угодно раз, мы имеем

$$\frac{1}{\nu!}f^{(\nu)}(\alpha+\delta)=(-1)^{\nu}\sum_n \frac{a_n}{n^{\alpha+\delta}}\frac{(\ln n)^{\nu}}{\nu!},$$

откуда

$$f(s)=\sum_{\nu=0}^{\infty}\sum_n \frac{a_n}{n^{\alpha+\delta}}\frac{([(\alpha+\delta)-s]\ln n)^{\nu}}{\nu!}.$$

В силу предположения относительно a_n, члены этой двойной суммы при вещественном $s<\alpha$ суть неотрицательные вещественные числа, и так как для s, достаточно близкого к α, ряд сходится, мы можем изменить порядок суммирования. Но тогда получится как раз исходный ряд Дирихле $f(s)$. Он сходился бы таким образом для достаточно близкого к α вещественного числа $s<\alpha$, что противоречит тому, что α есть абсцисса сходимости.

Эта общая теорема применима к рядам Дирихле $\zeta_m(s)$, $\zeta(s\,|\,\chi)$. Действительно, во-первых, как было установлено в II, п. 1, их коэффициенты $\sigma_m(n)$, $\sigma(n\,|\,\chi)$ неотрицательны, и, во-вторых, их абсциссы сходимости α_m, $\alpha(\chi)$ конечны.

Последнее будет доказано, если мы дадим двустороннюю оценку для этих абсцисс сходимости α_m, $\alpha(\chi)$; оценку снизу мы будем тогда существенно использовать. С одной стороны, из II, п. 1 мы немедленно имеем оценку сверху α_m, $\alpha(\chi) \leqslant 1$. С другой стороны, из доказанной в (2) п. 3 расходимости ряда

$$\zeta\left(\frac{1}{2}\,\middle|\,\chi\right) = \sum_n \frac{\sigma(n\,|\,\chi)}{n^{1/2}}$$

следует оценка снизу $\alpha(\chi) \geqslant 1/2$. Совершенно так же получается оценка снизу $\alpha_m \geqslant 1/\varphi(m)$, если установить расходимость ряда

$$\zeta_m\left(\frac{1}{\varphi(m)}\right) = \sum_n \frac{\sigma_m(n)}{n^{1/\varphi(m)}}.$$

Из арифметического закона для коэффициентов $\sigma_m(n)$ из II, п. 1 следует, в силу того что все фигурирующие там f_p являются здесь делителями числа $\varphi(m)$, что для $\varphi(m)$-х степеней $n = n_0^{\varphi(m)}$ имеет место $\sigma_m(n) \geqslant 1$, так что ряд $\zeta_m(1/\varphi(m))$ минорируется расходящимся гармоническим рядом $\sum_{n_0} 1/n_0$.

Следовательно, доказанная выше общая теорема действительно применима к $\zeta_m(s)$, $\zeta(s\,|\,\chi)$. Таким образом, эти функции имеют на своих абсциссах сходимости α_m, $\alpha(\chi)$ особые точки. Но так как мы установили неравенства

$$\frac{1}{\varphi(m)} \leqslant \alpha_m \leqslant 1, \quad \frac{1}{2} \leqslant \alpha(\chi) \leqslant 1$$

с положительными нижними границами, то мы можем утверждать, что особые точки α_m, $\alpha(\chi)$ заведомо лежат в полуплоскости $\sigma > 0$. Однако, согласно VII, в этой полуплоскости в качестве особой точки может быть только полюс первого порядка при $s = 1$. Отсюда следует, что абсциссы сходимости α_m, $\alpha(\chi) = 1$ и что $\zeta_m(s)$, $\zeta(s\,|\,\chi)$ при $s = 1$ действительно имеют полюс первого порядка, что нам и оставалось еще показать.

В дополнение к нашим результатам I, II, п. 1 о произведениях L-рядов $\zeta_m(s)$, $\zeta(s\,|\,\chi)$ мы можем поэтому установить, принимая во внимание VII:

IX. *Функции* $\zeta_m(s)$, $\zeta(s\,|\,\chi)$ *регулярны в полуплоскости* $\sigma > 0$, *за исключением* $s = 1$, *где они имеют полюсы первого порядка с вычетами*

$$\lim_{s\to 1}(s-1)\,\zeta_m(s) = \prod_{\chi\neq\varepsilon} L(1\,|\,\chi), \quad \lim_{s\to 1}(s-1)\,\zeta(s\,|\,\chi) = L(1\,|\,\chi).$$

В этом факте, согласно VII, и заключается глубокая, теоретико-функциональная причина необращения $L(1\,|\,\chi)$ в нуль для $\chi \neq \varepsilon$.

5. Если не использовать доказанной выше общей теоремы о рядах Дирихле с неотрицательными коэффициентами — ведь эта теорема все-таки требует знакомства с понятиями регулярной аналитической функции и аналитического продолжения, — то завершить доказательство необращения L-рядов в нуль можно также и следующим, более элементарным теоретико-функциональным способом. Вместо того, чтобы доказывать, что $s=1$ является особой точкой $\zeta(s|\chi)$ для каждого квадратичного характера χ, что мы делали только что, достаточно, как в п. 3, из предположения $L(1|\chi)=0$ вывести сходимость $\zeta(s|\chi)$ для $\sigma>1/2$ и получить отсюда противоречие с доказанной в (2) п. 3 расходимостью ряда $\zeta(1/2|\chi)$, которая использовалась также и в предыдущем выводе. Это достигается на основании той же самой идеи, что и при элементарно-аналитическом доказательстве в п. 3, однако значительно проще.

В сокращенных обозначениях из п. 3 мы имеем

$$Z(s)=\zeta(s)L(s)=\sum_n \frac{\sigma(n)}{n^s}\cdot \text{ с } \sigma_n=\sum_{d\mid n}\chi(d).$$

Вместо частичных сумм $Z_{N^2}(1/2)$ мы рассмотрим здесь частичные суммы коэффициентов

$$Z_N(0)=\sum_{n\leqslant N}\sigma(n),$$

причем еще фигурировавшее там число N^2 заменяется здесь любым натуральным числом N. Аналогично (3) п. 3 получается формула

$$Z_N(0)=\sum_{n\leqslant\sqrt{N}}\chi(n)\,\zeta_{\frac{N}{n}}(0)+\sum_{n<\sqrt{N}}(L^{\sqrt{N}}(0)-L^{\frac{N}{n}}(0)).$$

Вследствие того что

$$\zeta_{\frac{N}{n}}(0)=\sum_{n'\leqslant\frac{N}{n}}1=\left[\frac{N}{n}\right]=\frac{N}{n}-\theta_n^N \text{ с } 0\leqslant\theta_n^N<1,$$

она может быть представлена также в виде

$$Z_N(0)=L_{\sqrt{N}}(1)\,N-\sum_{n\leqslant\sqrt{N}}\chi(n)\,\theta_n^N+\sum_{n<\sqrt{N}}(L^{\sqrt{N}}(0)-L^{\frac{N}{n}}(0)),$$

или

$$Z_N(0)-L(1)\,N=-L^{\sqrt{N}}(1)\,N-\sum_{n\leqslant\sqrt{N}}\chi(n)\,\theta_n^N+$$
$$+\sum_{n<\sqrt{N}}(L^{\sqrt{N}}(0)-L^{\frac{N}{n}}(0)).$$

Вместо сложных вычислений и оценок в части «а» доказательства из п. 3 здесь мы имеем просто

$$\Big|\sum_{n\leqslant\sqrt{N}}\chi(n)\,\theta_{N/n}\Big|<\sqrt{N},$$

$$|L^{\sqrt{N}}(0)-L^{\frac{N}{n}}(0)|=\Big|\sum_{\sqrt{N}<n'\leqslant\frac{N}{n}}\chi(n')\Big|<\tfrac{1}{2}f,$$

и, на основании простой оценки остатка в части «б» доказательства из п. 3,

$$|L^{\sqrt{N}}(1)|<\frac{f}{\sqrt{N}}.$$

Тем самым мы получаем оценку

$$|\mathsf{Z}_N(0)-L(1)\,N|<\Big(f+1+\tfrac{1}{2}f\Big)\sqrt{N}<2f\sqrt{N},$$

и потому во всяком случае

$$\mathsf{Z}_N(0)-L(1)\,N=0\,(\sqrt{N})$$

Если бы теперь было $L(1)=0$, то для частичной суммы коэффициентов получилось бы отсюда $\mathsf{Z}_N(0)=0\,(\sqrt{N})$. Тогда, на основании предпосланной нами общей теории сходимости рядов Дирихле, следовало бы, что ряд $\mathsf{Z}(s)$ имеет абсциссу сходимости $\alpha\leqslant 1/2$, т. е. сходится для $\sigma>1/2$. Так как, согласно VII, $\mathsf{Z}(s)=\zeta(s)\,L(s)$ для $\sigma>0$ регулярна (за исключением, быть может, полюса при $s=1$), то значение функции $\mathsf{Z}(1/2)$ можно было бы вычислить из этого сходящегося ряда как $\lim\limits_{s\to 1/2+0}\mathsf{Z}(s)$, т. е. этот предел существовал бы и был конечным. Но, согласно приводящим к доказательству формулы (2) п. 3 неравенствам для коэффициентов, для всех $s>1/2$ все время имеет место $\mathsf{Z}(s)\geqslant\zeta(2s)$, и потому $\lim\limits_{s\to 1/2+0}\mathsf{Z}(s)=+\infty$. Мы получили противоречие.

При таком теоретико-функциональном подходе становится ясной также и основная идея нашего элементарно-аналитического доказательства из п. 3. Все дело заключается в доказательстве сходимости ряда Дирихле

$$\mathsf{Z}(s)-L(1)\,\zeta(s)=\zeta(s)\,(L(s)-L(1))$$

для $\sigma>1/2$, откуда будет следовать, что полюс $s=1$ функции $\zeta(s)$ уничтожается нулем $s=1$ выражения $L(s)-L(1)$, т. е. этот ряд в каждом случае является регулярной функцией для $\sigma>0$. При теоретико-функциональном подходе это получается ссылкой на общую теорию сходимости для рядов Дирихле с помощью

несложного определения порядка возрастания частичных сумм коэффициентов

$$\mathsf{Z}_N(0) - L(1)\,\zeta_N(0) = \mathsf{Z}_N(0) - L(1)\,N,$$

при элементарно-аналитическом подходе приходится производить значительно более сложное вычисление частичных сумм

$$\mathsf{Z}_{N^2}\left(\frac{1}{2}\right) - L(1)\,\zeta_{N^2}\left(\frac{1}{2}\right) \sim \mathsf{Z}_{N^2}\left(\frac{1}{2}\right) - 2L(1)\,N$$

в самой исследуемой точке $s = 1/2$.

5. Алгебраически-теоретико-числовой метод доказательства. 1. Дирихле в своем классическом доказательстве следующим образом показывал необращение в нуль L-рядов $L(1\,|\,\chi)$ с квадратичными характерами χ. Он выводит явное выражение для предельного значения

$$\lim_{s\to 1+0} (s-1)\,\zeta(s\,|\,\chi) = L(1\,|\,\chi)$$

(или, на языке теории функций, для вычета функции $\zeta(s\,|\,\chi)$ при $s=1$). Это выражение оказывается мультипликативно составленным из некоторых величин, которые у Дирихле рассматриваются как инварианты целочисленных бинарных квадратичных форм с дискриминантом $\chi(-1)\,f(\chi)$, а с современной точки зрения являются инвариантами, характеризующими арифметику квадратичного поля $\mathsf{P}(\sqrt{\chi(-1)\,f(\chi)})$. Тогда необращение $L(1\,|\,\chi)$ в нуль получается из того, что эти инварианты, важнейшим из которых является так называемое число классов $h(\chi)$ поля $\mathsf{P}(\sqrt{\chi(-1)\,f(\chi)})$, по самой своей природе отличны от нуля.

Далее, Дирихле также находит сумму бесконечного ряда

$$L(1\,|\,\chi) = \sum_n \frac{\chi(n)}{n}.$$

Это легко можно сделать элементарно-аналитическими средствами, обобщая вывод известной формулы $1 - 1/3 + 1/5 - 1/7 \pm \pm \ldots = \pi/4$, которая соответствует частному случаю квадратичного характера χ с ведущим модулем $f(\chi) = 4$. Правда, из получающегося при этом конечного выражения для суммы ряда не видно, как в указанном частном случае, что эта сумма отлична от нуля, иначе наши усилия доказать этот факт были бы излишними. Посредством сравнения этого выражения для суммы с вышеупомянутым выражением для вычета Дирихле получает, кроме доказательства необращения $L(1\,|\,\chi)$ в нуль, а вместе с тем и доказательства своей теоремы о простых числах, также и явное представление в виде конечной суммы для числа классов $h(\chi)$.

Метод доказательства Дирихле проходит не только для отдельного L-ряда $L(1|\chi)$ с квадратичным характером χ, но также и для произведения $\prod_{\chi \neq \varepsilon} L(1|\chi)$ всех L-рядов по $\bmod m$ с отличными от главного характерами χ, благодаря чему становится ненужным элементарно-аналитическое сведение к случаю одного квадратичного характера χ (см. п. 2). Для предельного значения

$$\lim_{s \to 1+0} (s-1)\,\zeta_m(s) = \prod_{\chi \neq \varepsilon} L(1|\chi)$$

получается явное выражение, которое мультипликативно составлено из инвариантов арифметики поля P_m m-х корней из 1, инварианты отличны от нуля по самой своей природе. Тогда для важнейшего из этих инвариантов числа классов h_m поля P_m получается представление в виде произведения конечных сумм, если вычислить в конечном виде сумму бесконечного ряда

$$L(1|\chi) = \sum_n \frac{\chi(n)}{n}\,.$$

Этот алгебраически-теоретико-числовой метод доказательства мы, в связи с общими рассуждениями в п. 1 о произведениях L-рядов, изложим здесь только в общих чертах, так как у нас нет в распоряжении необходимых сведений из арифметики полей $\mathsf{P}(\sqrt{\chi(-1)f(\chi)})$, P_m. Заполнение пробелов в нашем изложении мы сделаем в четвертой главе, когда будут развиты основы арифметики квадратичных полей $\mathsf{P}(\sqrt{\chi(-1)f(\chi)})$, и, в частности, в § 18, п. 1 мы приведем классическое доказательство Дирихле и связанное с ним определение числа классов $h(\chi)$.

2. Как и в п. 1, мы будем рассматривать более общее произведение

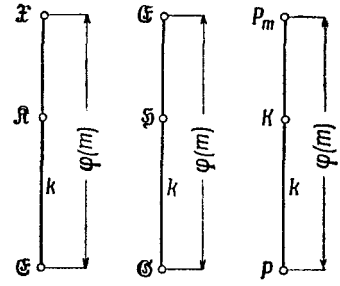
$$\zeta(s|\mathfrak{K}) = \prod_{\chi \text{ из } \mathfrak{K}} L(s|\chi) = \zeta(s) \prod_{\substack{\chi \text{ из } \mathfrak{K} \\ \chi \neq \varepsilon}} L(s|\chi)$$

собственных L-рядов для характеров из какой-нибудь подгруппы $\mathfrak{K}$ порядка k группы $\mathfrak{X}$ всех характеров по $\bmod m$, где m есть натуральное число. Пусть как и там $\mathfrak{H}$ есть соответствующая $\mathfrak{K}$ подгруппа индекса k группы $\mathfrak{G}$ всех классов вычетов $a \bmod m$, взаимно простых с модулем; $\mathfrak{H}$ характеризуется свойством

$$\chi(a) = 1 \text{ для всех } \chi \text{ из } \mathfrak{K}.$$

Помимо изложенного в п. 1, мы покажем, что этой подгруппе $\mathfrak{H}$ группы $\mathfrak{G}$ соответствует поле алгебраических чисел K степени k, содержащееся в поле P_m m-х корней из 1 (фиг. 8; см. также в связи с этим фиг. 6б в п. 1); это подполе K поля P_m определяется следующим образом. $\mathsf{P}_m = \mathsf{P}(\zeta)$, где ζ есть первообразный

m-й корень из 1. Все первообразные m-е корни из 1, имеющие вид ζ^a, где a пробегает классы вычетов по $\bmod m$, взаимно простые с модулем, являются корнями m-го многочлена деления круга $f_m(x)$. Согласно V и VI, п. 2, § 11, этот многочлен имеет (целые) рациональные коэффициенты и неприводим над P. Поэтому P_m есть нормальное расширение поля P и группа Галуа этого расширения представляется $\varphi(m)$ подстановками $\zeta \to \zeta^a$ с a, взаимно простыми с m. Так как перемножению этих подстановок соответствует перемножение классов вычетов $a \bmod m$, взаимно простых с модулем, то мультипликативную группу $\mathfrak{G}$ можно рассматривать как изоморфное представление группы Галуа поля P_m. Тогда подгруппе $\mathfrak{H}$ индекса k группы $\mathfrak{G}$ по основной теореме теории Галуа соответствует в качестве инвариантного поля подполе K поля P_m. Поле K имеет степень k и порождается основными симметрическими функциями от ξ_a с $a \bmod m$ из $\mathfrak{H}$. Обратно, каждое подполе K поля P_m соответствует в этом смысле некоторой подгруппе $\mathfrak{H}$ группы $\mathfrak{G}$, а вместе с тем и некоторой подгруппе $\mathfrak{K}$ группы $\mathfrak{X}$.



Фиг. 8.

Если, в частности, $\mathfrak{K} = \mathfrak{X}$ есть группа всех $\varphi(m)$ характеров по $\bmod m$, то $\mathfrak{H} = \mathfrak{E}$ состоит только из единичного класса $1 \bmod m$, и $\mathsf{K} = \mathsf{P}_m$ будет полным m-м полем деления круга. Если же $\mathfrak{K}$ есть порожденная квадратичным характером χ подгруппа порядка 2, причем без ограничения общности можно считать, что $m = f(\chi)$, то, как мы установили в п. 1 в связи с (6б), подгруппа $\mathfrak{H}$ индекса 2 состоит из $a \bmod f(\chi)$ с $\left(\frac{\chi(-1) f(\chi)}{a}\right) = 1$; ей соответствует квадратичное поле $\mathsf{K} = \mathsf{P}(\sqrt{\chi(-1) f(\chi)})$.

3. Последнее вытекает из следующей важной для теории квадратичных полей теоремы:

X. *Если χ есть квадратичный характер с (натуральным) ведущим модулем f, то с помощью принадлежащей χ гауссовой суммы* $\tau(\chi) = \sum_{m \bmod f} \chi(x) \zeta^x$ (ζ *первообразный m-й корень из* 1) *квадратичное поле*

$$\mathsf{K} = \mathsf{P}(\sqrt{\chi(-1) f})$$

вкладывается в f-е поле деления круга $\mathsf{P}_f = \mathsf{P}(\zeta)$; *именно*

$$\tau(\chi)^2 = \chi(-1) f. \qquad (1)$$

При автоморфизмах $\zeta \to \zeta^a$ *(с взаимно простыми с модулем* $a \bmod f$*) поля* P_f *в подполе* K *индуцируются автоморфизмы*

$$\tau(\chi) \to \chi(a)\,\tau(\chi); \tag{2}$$

поэтому K *инвариантно в точности относительно определенной условием* $\chi(a) = 1$ *подгруппы* $\mathfrak{H}$ *группы Галуа* $\mathfrak{G}$ *поля* P_f.

Доказательство. Нужно доказать формулы (1), (2) для гауссовой суммы $\tau(\chi)$, аналогичные формулам (1), (2) п. 2, § 8 того специального случая, когда ведущий модуль $f = p$ равен простому числу. Мы докажем более общие формулы, имеющие силу для любого характера χ с ведущим модулем f, именно

$$\tau(\chi)\,\overline{\tau(\chi)} = f, \tag{1*}$$

$$\tau(\chi) \to \overline{\chi}(a)\,\tau(\chi) \quad \text{при} \quad \zeta \to \zeta^a; \tag{2*}$$

эти общие формулы понадобятся нам позднее. Для квадратичного характера χ имеет место $\overline{\chi} = \chi$, и потому (2*) равносильно в этом случае (2); $\overline{\tau(\chi)}$ получается из $\tau(\chi)$ посредством подстановки $\zeta \to \zeta^{-1}$, и потому, согласно (2*), $\overline{\tau(\chi)} = \chi(-1)\,\tau(\chi)$, так что (1*) переходит в (1).

Для доказательства теоремы надо заметить, что вследствие соотношения $\chi(x) = 0$ для $(x, f) \neq 1$ в определении $\tau(\chi)$ можно вводить или, наоборот, отбрасывать ограничение $(x, f) = 1$.

Что касается (2*), то мы имеем, аналогично § 8, п. 2, что при $\zeta \to \zeta^a$

$$\tau(\chi) \to \sum_{\substack{x \bmod f \\ (x,\,f)=1}} \chi(x)\,\zeta^{ax} = \sum_{\substack{y \bmod f \\ (y,\,f)=1}} \chi(a^{-1}y)\,\zeta^{y} =$$

$$= \chi(a)^{-1} \sum_{\substack{y \bmod f \\ (y,\,f)=1}} \chi(y)\,\zeta^{y} = \overline{\chi}(a)\,\tau(\chi).$$

Что же касается (1*), то, принимая во внимание наше замечание, мы прежде всего имеем, аналогично § 8, п. 2,

$$\overline{\tau(\chi)}\,\tau(\chi) = \sum_{\substack{x \bmod f \\ (x,\,f)=1}} \sum_{y \bmod f} \overline{\chi}(x)\,\chi(y)\,\zeta^{-x}\zeta^{y} = \sum_{\substack{x \bmod f \\ (x,\,f)=1}} \sum_{y \bmod f} \chi(x^{-1}y)\,\zeta^{y-x} =$$

$$= \sum_{\substack{x \bmod f \\ (x,\,f)=1}} \sum_{t \bmod f} \chi(t)\,\zeta^{x(t-1)} = \sum_{t \bmod f} \chi(t) \sum_{\substack{x \bmod f \\ (x,\,f)=1}} \zeta^{x(t-1)}.$$

Для внутренней суммы

$$S_f(t) = \sum_{\substack{x \bmod f \\ (x,\,f)=1}} \zeta^{x(t-1)} = \sum_{\substack{x \bmod f \\ (x,\,f)=1}} \zeta_f^{x(t-1)},$$

рассматриваемой как функция натурального числа f, мы получаем, аналогично тому как в § 4, п. 6, функциональное равенство

$$\sum_{d\mid f} S_d(t) = \sum_{x \bmod f} \zeta^{x(t-1)} = \sum_{x \bmod f} \zeta_f^{x(t-1)} = \begin{cases} f & \text{для } t \equiv 1 \bmod f \\ 0 & \text{для } t \not\equiv 1 \bmod f \end{cases}.$$

Отсюда, в силу формул обращения Мёбиуса (см. § 4, п. 7), получаем явное представление

$$S_f(t) = \sum_{\substack{d\mid f \\ d\mid t-1}} \mu\left(\frac{f}{d}\right) d.$$

Поэтому

$$\tau(\chi)\,\overline{\tau(\chi)} = \sum_{t \bmod f} \chi(t) \sum_{\substack{d\mid f \\ d\mid t-1}} \mu\left(\frac{f}{d}\right) d = \sum_{d\mid f} \mu\left(\frac{f}{d}\right) d \sum_{\substack{t \bmod f \\ t\equiv 1 \bmod d}} \chi(t).$$

Но здесь для внутренней суммы имеет место

$$X_d = \sum_{\substack{t \bmod f \\ t\equiv 1 \bmod d}} \chi(t) = \begin{cases} 1 & \text{для } d = f \\ 0 & \text{для } d\mid f,\ d < f \end{cases}.$$

Это очевидно для $d = f$. Для $d\mid f$, $d < f$, в силу того, что f есть ведущий модуль характера χ, существует взаимно простой с f класс вычетов $c \equiv 1 \bmod d$ с $\chi(c) \neq 1$, и тогда

$$\chi(c)\, X_d = \sum_{\substack{t \bmod f \\ t\equiv 1 \bmod d}} \chi(ct) = \sum_{\substack{u \bmod f \\ u\equiv 1 \bmod d}} \chi(u) = X_d,$$

потому что $u \equiv ct \bmod f$ пробегает те же самые классы вычетов, что и $t \bmod f$; таким образом, в этом случае действительно $X_d = 0$. Тем самым мы получаем наше утверждение

$$\tau(\chi)\,\overline{\tau(\chi)} = \sum_{d\mid f} \mu\left(\frac{f}{d}\right) d X_d = f.$$

4. Доказав эту теорему, мы представим, сначала чисто формально, соответствующее подгруппе $\mathfrak{R}$ произведение L-рядов $\zeta(s\,\mathfrak{R})$ в новой форме, подсказанной формулами из п. 1; при этом будет видно, что эта новая форма имеет значение для арифметики соответствующего квадратичного поля K. Мы будем исходить из представления произведения L-рядов в виде произведения Дирихле

$$\zeta(s\,|\,\mathfrak{R}) = \prod_p \left(\frac{1}{1 - \frac{1}{p^{f_p s}}}\right)^{g_p} \qquad (\mathrm{I}_0)$$

с определенными в I, п. 1 значениями показателей f_p, g_p. Наша новая форма представления получится, если посредством введения соответствующего нового понятия мы освободимся в представлении (I_0) от показателей f_p, g_p.

Для этого мы каждому простому числу p формально сопоставим g_p новых символов $\mathfrak{p}_i$ $(i = 1, \ldots, g_p)$, которые мы будем также писать и без индекса i, подобно тому как ранее это делалось для простых чисел p; таким образом, мы будем кратко говорить о g_p символах $\mathfrak{p}$, сопоставленных простому числу p. Пока в эти символы не вложено никакого содержания, кроме чисто формального определения; в частности, их ни в коем случае нельзя понимать как числа. Однако они должны находиться в некотором отношении к числам. Именно, мы свяжем их с числами, определив для них функцию $\mathfrak{N}$ со значениями

$$\mathfrak{N}(\mathfrak{p}) = p^{f_p};$$

таким образом, эта функция имеет одно и то же значение p^{f_p} для всех символов $\mathfrak{p}$, сопоставленных одному и тому же простому числу p. На основании этих определений произведение Дирихле (I_0) принимает новый вид

$$\zeta(s \mid \mathfrak{K}) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{p})^s}}, \tag{I}$$

где умножение распространено на совокупность введенных нами символов $\mathfrak{p}$ (для всех простых чисел p). Тем самым формально исчезают фигурирующие в (I_0) показатели f_p, g_p.

Далее, мы будем рассматривать символы $\mathfrak{p}$ как образующие свободной мультипликативной абелевой группы $\mathfrak{D}$, элементы которой $\mathfrak{a}$ однозначно представляются, таким образом, через базис в виде

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha_\mathfrak{p}} \left\{ \begin{array}{l} \alpha_\mathfrak{p} \text{ целые рациональные,} \\ \alpha_\mathfrak{p} \neq 0 \text{ только для конечного множества } \mathfrak{p} \end{array} \right\}.$$

И наконец, мы определим также и для этих элементов $\mathfrak{a}$ функцию $\mathfrak{N}$ посредством формулы

$$\mathfrak{N}(\mathfrak{a}) = \prod_{\mathfrak{p}} \mathfrak{N}(\mathfrak{p})^{\alpha_\mathfrak{p}},$$

т. е. таким образом, что она будет мультипликативной функцией от элементов группы $\mathfrak{D}$ с рациональными значениями функции. Элементы

$$\mathfrak{n} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}} \left\{ \begin{array}{l} \nu_\mathfrak{p} \geqslant 0 \text{ целые рациональные} \\ \nu_\mathfrak{p} > 0 \text{ только для конечного множества } \mathfrak{p} \end{array} \right\}$$

мы будем называть целыми элементами группы $\mathfrak{D}$; для них

$$\mathfrak{N}(\mathfrak{n}) = \prod_{\mathfrak{p}} \mathfrak{N}(\mathfrak{p})^{\nu_{\mathfrak{p}}}$$

есть целое рациональное число. Тогда для $\zeta(s \mid \mathfrak{K})$ мы получаем, по схеме доказательства тождества Эйлера, примененной к функции $\mathfrak{N}$ символа $\mathfrak{p}$, а не к простым числам p, представление в виде ряда Дирихле

$$\zeta(s \mid \mathfrak{K}) = \sum_{\mathfrak{n}} \frac{1}{\mathfrak{N}(\mathfrak{n})^s}, \tag{II}$$

где суммирование распространено на все целые элементы $\mathfrak{n}$ из $\mathfrak{D}$. Сравнение этого представления с представлением II, п. 1 в виде ряда Дирихле

$$\zeta(s \mid \mathfrak{K}) = \sum_{n} \frac{\sigma(n \mid \mathfrak{K})}{n^s} \tag{II_0}$$

показывает, что коэффициенты $\sigma(n \mid \mathfrak{K})$ с помощью введенных нами понятий могут быть определены как количества целых $\mathfrak{n}$ из $\mathfrak{D}$ с $\mathfrak{N}(\mathfrak{n}) = n$:

$$\sigma(n \mid \mathfrak{K}) = \sum_{\mathfrak{N}(\mathfrak{n}) = n} 1.$$

Другими словами, в нашей новой записи пропадают также и фигурирующие в (II_0) коэффициенты $\sigma(n \mid \mathfrak{K})$.

Полученные нами формулы (I), (II) для произведения L-рядов $\zeta(s \mid \mathfrak{K})$ отличаются от соответствующих формул

$$\zeta(s) = \prod_{p} \frac{1}{1 - \frac{1}{p^s}}$$

$$\zeta(s) = \sum_{n} \frac{1}{n^s}$$

для дзета-функции Римана $\zeta(s)$ формально только тем, что вместо простых чисел p теперь стоят значения функции $\mathfrak{N}$ от вновь введенных символов $\mathfrak{p}$, а вместо натуральных чисел n — значения функции $\mathfrak{N}$ от целых элементов $\mathfrak{n}$ группы $\mathfrak{D}$, имеющей своими образующими символы $\mathfrak{p}$. В определение этих формальных понятий по существу входят только показатели f_p, g_p, которые в соответствии с I, п. 1 определяются заданием группы характеров $\mathfrak{K}$.

5. Согласно вышеизложенному, мы можем вместо группы характеров $\mathfrak{K}$ исходить также и из соответствующего ей поля K через посредство соответствующей группы классов вычетов $\mathfrak{H}$ и при этом рассматривать числа f_p, g_p и функцию $\zeta(s \mid \mathfrak{K})$ как определяемые полем K. Переход к такому пониманию мы уже

подготовили в п. 1 тем, что перешли от первоначального определения чисел f_p, g_p через $\mathfrak{R}$ к характеристике их через $\mathfrak{H}$, что было подчеркнуто в формулировке результата I; отсюда остается один шаг до характеристики этих чисел через K. На первый взгляд это новое понимание, при котором упор делается на поле K, может показаться искусственным. Однако оказывается, что при этом группа $\mathfrak{D}$ с образующими элементами $\mathfrak{p}$, целыми элементами $\mathfrak{n}$ и мультипликативной числовой функцией $\mathfrak{N}$ получает определенное содержание, благодаря чему становится полностью понятной формальная аналогия между $\zeta(s\,|\,\mathfrak{R})$ и $\zeta(s)$. Именно, оказывается, что эти формальные понятия играют роль строительного материала для арифметики поля алгебраических чисел K, которая в значительной степени аналогична изложенной в первой главе арифметике поля рациональных чисел P.

6. Ниже мы дадим в общих чертах обзор основ арифметики поля K алгебраических чисел. От подробного и систематического построения этой теории в рамках этой книги мы вынуждены отказаться. Мы лишь изложим основные точки зрения и новые понятия, которые играют главную роль при построении арифметики полей алгебраических чисел, и при этом, во-первых, выясним роль, которую играет произведение L-рядов $\zeta(s\,|\,\mathfrak{R})$ в арифметике определенных выше специальных полей K, и, во-вторых, укажем путь, по которому достигается доказательство необращения $L(1\,|\,\chi)$ в нуль. Для последней цели мы рассмотрим, в частности, входящие в формулу для вычета функции $\zeta(s\,|\,\mathfrak{R})$ арифметические инварианты поля K.

Как уже говорилось, построение арифметики, которое сейчас будет лишь набросано, мы проведем во всех подробностях для квадратичных полей в четвертой главе (см. § 16, 17). При этом нам будет полезно полученное здесь предварительное знакомство с предметом, подобно тому, как путешественнику, желающему познакомиться с чужой страной, бывает полезно сначала бросить взгляд на карту этой страны.

А. *Аддитивная арифметика.* Если мы хотим обобщить на поле алгебраических чисел K степени k основы арифметики, изложенные нами в первой главе для поля рациональных чисел P, то прежде всего нужно по аналогии с областью целостности Γ целых чисел из P определить область целостности $\mathfrak{l}$ целых чисел из K. Число α из K называется *целым*, если образованный с помощью сопряженных с ним чисел *главный многочлен*

$$g(x) = (x-\alpha)(x-\alpha')\ldots(x-\alpha^{(k-1)})$$

с рациональными коэффициентами и со старшим коэффициентом 1 имеет целые рациональные коэффициенты. Согласно теореме Гаусса (см. § 11, п. 2), дело сведется к одному и тому же, если это требование предъявить к соответствующему α неприводимому

многочлену с рациональными коэффициентами и со старшим коэффициентом, равным 1; $g(x)$ равен этому многочлену, возведенному в некоторую степень. Поэтому понятие *целого алгебраического числа* α не зависит от поля K, в котором оно рассматривается. Имеет место утверждение:

Целые числа из K *образуют область целостности* I.

Вследствие независимости понятия целостности числа от поля, далее, имеет место:

Рациональное число тогда и только тогда является целым алгебраическим, когда оно целое рациональное; поэтому пересечение $\mathsf{I} \cap \mathsf{P} = \Gamma$.

Далее доказывается:

Существует такой базис $\omega_1, \ldots, \omega_k$ *поля* K, *что числа* α *из* I *(и только они) обладают однозначным представлением*

$$\alpha = a_1\omega_1 + \ldots + a_k\omega_k \quad (a_1, \ldots, a_k \text{ из } \Gamma).$$

Такой базис $\omega_1, \ldots, \omega_k$ называется *целочисленным базисом* поля K. Он определен только с точностью до линейного преобразования с целыми рациональными коэффициентами и определителем, равным ± 1. Остающийся при этом инвариантным квадрат определителя

$$d = d(\omega_1, \ldots, \omega_k) = \begin{vmatrix} \omega_1 & \omega_1' & \ldots & \omega_1^{(k-1)} \\ \cdot & \cdot & \ldots & \cdot \\ \omega_k & \omega_k' & \ldots & \omega_k^{(k-1)} \end{vmatrix}^2,$$

столбцами которого служат элементы базиса и сопряженные с ними числа, есть целое рациональное число, $\neq 0$. Этот арифметический инвариант d поля K называется *дискриминантом* поля K. Он является — наряду с являющейся алгебраическим инвариантом *степенью* k поля K — мерилом того, насколько сильно отличается аддитивная арифметика в K — от аддитивной арифметики в P.

Б. *Мультипликативная арифметика.* С помощью области целостности I в поле K определяется элементарная теория делимости в смысле § 1, п. 2. Вследствие того, что $\mathsf{I} \cap \mathsf{P} = \Gamma$, понятия *делимости, единиц, ассоциированности* этой теории делимости при применении к рациональным числам совпадают с этими же понятиями из § 1, п. 2, т. е. можно говорить о продолжении теории делимости в P, определенной с помощью области целостности Γ. При дальнейшем построении мультипликативной арифметики в K, опирающемся на элементарную теорию делимости, мы отметим два коренных отличия от мультипликативной арифметики в P из § 1, п. 3—5, одно из которых касается *единиц*, а другое — *разложения на простые множители*.

а) *Единицы.* В I, кроме тривиальных, содержащихся уже в Γ единиц ± 1 — вещественных корней из 1 — и, быть может, также

других, комплексных корней из 1, которые тоже, очевидно, являются единицами, существуют, вообще говоря, также и *нетривиальные единицы* ε. Вместе с тривиальными единицами они образуют мультипликативную группу E. Прежде всего доказывается:

Число ε из I является единицей тогда и только тогда, когда его норма $N(\varepsilon) = \pm 1$ есть единица из Γ.

При этом *норма* $N(\alpha) = \alpha\alpha' \ldots \alpha^{(k-1)}$ числа α из K определяется вообще как произведение сопряженных с α чисел; она есть мультипликативная функция в K, обращающаяся в 0 лишь для $\alpha = 0$.

Основная теорема о единицах гласит:

Теорема Дирихле о единицах. *Если среди k полей, сопряженных с K, имеется r_1 вещественных и $2r_2$ попарно комплексно сопряженных, то группа единиц E поля K обладает однозначным $r_1 + r_2 = r$-членным представлением вида*

$$\varepsilon = \zeta^{\nu}\varepsilon_1^{n_1} \ldots \varepsilon_{r-1}^{n_{r-1}} \left\{ \begin{array}{c} \nu \bmod w \\ n_1, \ \ldots, \ n_{r-1} \text{ целые рациональные} \end{array} \right\}.$$

При этом ζ есть корень из 1 максимального встречающегося в K порядка, а $\varepsilon_1, \ldots, \varepsilon_{r-1}$ суть $r-1$ независимых друг от друга и от корней из 1 нетривиальных единиц из K. Если, в частности, как в нашем применении, K нормально, то сопряженные с K поля или все вещественны, или все попарно комплексно сопряжены и в соответствии с этим $r = k$ или $k/2$.

В качестве не зависящих от выбора основных единиц $\varepsilon_1, \ldots, \varepsilon_{r-1}$ инвариантов, группе единиц E поля K сопоставляются два числа, во-первых, порядок w корня из $1\,\zeta$, который характеризуется также как *количество корней из* 1 в K, и, во-вторых, абсолютная величина определителя

$$R = \left\| \begin{array}{cccc} e \ln|\varepsilon_1| & e' \ln|\varepsilon_1'| & \ldots & e^{(r-1)} \ln|\varepsilon^{(r-1)}| \\ \cdots & \cdots & \cdots & \cdots \\ e \ln|\varepsilon_{r-1}| & e' \ln|\varepsilon_{r-1}'| & \ldots & e^{(r-1)} \ln|\varepsilon_{r-1}^{(r-1)}| \\ \frac{1}{r} & \frac{1}{r} & \ldots & \frac{1}{r} \end{array} \right\|$$

из логарифмов абсолютных величин нетривиальных основных единиц $\varepsilon_1, \ldots, \varepsilon_{r-1}$ и сопряженных с ними чисел; при этом из каждой пары $\mathsf{K}^{(x)}$, $\overline{\mathsf{K}}^{(x)}$ комплексно сопряженных (с одинаковыми абсолютными величинами) нужно принимать во внимание лишь одного представителя $\mathsf{K}^{(x)}$ и ставить дополнительный множитель $e^{(x)} = 2$ (т. е. берется квадрат абсолютной величины), в то время как для вещественных сопряженных $\mathsf{K}^{(x)}$ дополнительный множитель $e^{(x)} = 1$. Благодаря этим добавочным множителям сумма элементов в каждой из первых $r-1$ строк равна 0, в то время

как сумма элементов последней строки равна 1; поэтому R можно определить также как абсолютную величину миноров, составленных из первых $r-1$ строк, которая будет одна и та же при любом выборе $r-1$ столбцов. Оказывается, что абсолютная величина R нашего детерминанта действительно инвариантна относительно всех возможных преобразований базиса и, кроме того, $\neq 0$, т. е. является положительным вещественным числом. R называется *регулятором* поля K. Оба арифметических инварианта w и R служат, так сказать, мерилом того, насколько сильно отличается мультипликативная арифметика поля K от мультипликативной арифметики поля P в отношении единиц.

б) *Разложение на простые множители.* Оказывается, что в I, вообще говоря, уже не верна основная теорема об однозначном разложении на простые множители. Этот основной факт мы проиллюстрируем в § 16, п. 6 на примерах неоднозначных разложений. Несмотря на это, мультипликативное построение отличных от 0 чисел из K все же возможно получить; впервые это показал Куммер для подполей K поля деления круга P_m, а затем Дедекинд, Кронекер и Гензель различными способами сделали это и в общем случае. Мы удовлетворимся здесь описанием рассмотренного Куммером случая подполя K поля P_m, который ведь только и важен в отношении интересующих нас здесь вопросов.

Опираясь на элементарную теорию сравнений в I, которую можно развить из элементарной теории делимости (ср. § 8, п. 4), Куммер ввел для этой цели новые объекты, которые он назвал *идеальными числами*; мы будем здесь называть их *дивизорами*, как это стало принято после Кронекера и Гензеля. Было бы слишком жалко лишь мельком обрисовать эти оригинальные и далеко идущие идеи Куммера в узких рамках настоящего обзора. В связи с этим мы отсылаем читателя к исчерпывающему изложению в § 17, п. 2. Формально мы уже знакомы с введенными Куммером дивизорами поля K. Именно, это элементы $\mathfrak{a}$ группы $\mathfrak{D}$, которые мы ввели выше при формальном видоизменении (I), (II) представлений (I_0), (II_0) для $\zeta(s|\mathfrak{K})$ в виде произведения и ряда.

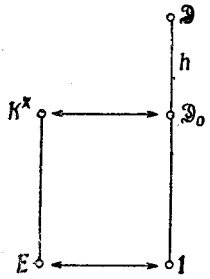
Теперь мы изложим, как с помощью этих формальных образований можно описать мультипликативное построение чисел $\alpha \neq 0$ из K. При этом мы будем считать эти числа объединенными в классы ассоциированных чисел, т. е. вместо мультипликативной группы $\mathsf{K}^\times$ будем рассматривать фактор-группу $\mathsf{K}^\times/\mathsf{E}$ по группе E единиц поля K. Тогда в качестве основы для описания мультипликативного строения поля K с помощью группы дивизоров $\mathfrak{D}$ нами получена

Теорема соответствия. *Фактор-группа $\mathsf{K}^\times/\mathsf{E}$ изоморфна некоторой подгруппе $\mathfrak{D}_0$ группы дивизоров $\mathfrak{D}$* (фиг. 9).

Таким образом, каждое число $\alpha \neq 0$ *из* K *вместе со своими ассоциированными* $\varepsilon\alpha$, *где* ε *пробегает единицы поля* K, *взаимно однозначно и мультипликативно-изоморфно соответствует некоторому дивизору* $\mathfrak{a}$ *из* $\mathfrak{D}$; *обозначается это так*:

$$\alpha \cong \mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}} \left\{ \begin{array}{l} a_{\mathfrak{p}} \text{ целые рациональные} \\ a_{\mathfrak{p}} \neq 0 \text{ лишь для конечного множества } \mathfrak{p} \end{array} \right\}.$$

Символы $\mathfrak{p}$, которые мы выше сопоставляли простым числам p и которые послужили нам исходным материалом (образующими элементами) для определения группы $\mathfrak{D}$, называются *простыми дивизорами* поля K. Таким образом, для каждого числа $\alpha \neq 0$ из K существует формально аналогичное III′ п. 5 § 1 однозначное представление в виде произведения степеней простых дивизоров, называемое *разложением* числа α *на простые дивизоры* в K; обратно, этим разложением число α определяется однозначно с точностью до произвольного единичного множителя ε из K (т. е. в смысле $\cong$ с точностью до ассоциированных чисел).



Фиг. 9.

Далее, при этом соответствии имеют место следующие законы:

Теорема о норме. *Если* $\alpha \cong \mathfrak{a}$ *в* K, *то* $N(\alpha) \cong \mathfrak{N}(\mathfrak{a})$ *в* P, *т. е.* $|N(\alpha)| = \mathfrak{N}(\mathfrak{a})$.

При этом $N(\alpha) = \alpha\alpha' \ldots \alpha^{(k-1)}$ есть уже известная нам *норма числа* α из K, а $\mathfrak{N}(\mathfrak{a})$ — определенная при введении дивизоров функция $\mathfrak{N}$ от элементов из $\mathfrak{D}$, которую в связи с этой теоремой называют *нормой дивизора* $\mathfrak{a}$.

Теорема целостности. *При соответствии* $\alpha \cong \mathfrak{a}$ *целым числам* $\alpha \neq 0$ *из* K, *т. е. числам* $\alpha \neq 0$ *из* I, *и только им, соответствуют целые дивизоры* $\mathfrak{a}$ *из* $\mathfrak{D}$, *т. е. такие дивизоры, у которых все показатели* $a_{\mathfrak{p}} \geqslant 0$.

Эта теорема является непосредственным обобщением теоремы целостности для поля рациональных чисел P, доказанной в конце § 1, п. 5. В частности, вопрос о делимости $\alpha \mid \beta$ в K мы можем поэтому решать с помощью соответствующих числам α, β дивизоров по тем же самым формальным правилам, что и для делимости $a \mid b$ в p с помощью разложения на простые множители (см. § 2, п. 1, критерий делимости).

Теорема о вложении. *При вложении поля* P *в* K *простому рациональному числу* p *соответствует дивизор, равный произведению степеней* $g_{\mathfrak{p}}$ *простых дивизоров* $\mathfrak{p}$, *сопоставленных числу* p *по определению, каждый из которых фигурирует с одним*

и тем же показателем e_p:

$$p \cong (\prod_{\mathfrak{p} \to p} \mathfrak{p})^{e_p};$$

при этом показатель e_p *определяется из соотношения*

$$e_p f_p g_p = k,$$

в которое входят еще и числа f_p *с* $\mathfrak{N}(\mathfrak{p}) = p^{f_p}$.

Последнее правило для определения e_p—см. относительно этого теоретико-групповую схему в п. 1, фиг. 6а—немедленно получается посредством применения теоремы о норме к разложению числа на простые дивизоры (если уже установлено, что это разложение имеет указанный вид); действительно, с одной стороны, $\mathfrak{N}(p) = p^k$, а с другой стороны, по определению, $\mathfrak{N}((\prod_{\mathfrak{p} \to p} \mathfrak{p})^{e_p}) = p^{e_p f_p g_p}$.

Теорема о вложении дает правило, с помощью которого из разложения рационального числа $a \neq 0$ на простые множители в P можно получить его разложение на простые дивизоры в K, и вместе с тем показывает, как мультипликативная арифметика поля P вкладывается в мультипликативную арифметику поля K.

Как было отмечено в I, п. 1, для всех не входящих в m простых чисел p уже $f_p g_p = k$ и потому $e_p = 1$, так что $e_p \neq 1$ имеет место самое большее для конечного множества простых чисел p, являющихся делителями числа m. Точнее, имеет место

Теорема о дискриминанте. $e_p \neq 1$ *тогда и только тогда, когда* p *входит в дискриминант* d *поля* K.

Существенное отличие описанной нами мультипликативной структуры поля K по сравнению со структурой поля P, которая описывается формально аналогичным утверждением III, п. 5, § 1, состоит в том, что группа $\mathfrak{D}_0$ тех дивизоров $\mathfrak{a}$, которые соответствуют числам $\alpha \neq 0$ из K и называются *главными дивизорами*, является, вообще говоря, собственной подгруппой всей группы дивизоров $\mathfrak{D}$ поля K. Причина этого заключается в том, что, вообще говоря, не все простые дивизоры $\mathfrak{p}$ поля K соответствуют числам π из K. Однако существуют поля, в которых это имеет место, например квадратичные поля $\mathsf{P}_4 = \mathsf{P}(\sqrt{-1})$, $\mathsf{P}_3 = \mathsf{P}(\sqrt{-3})$ (ср. уже § 10, п. 8, 9 и далее § 16, п. 6); тогда числа $\pi \cong \mathfrak{p}$ являются простыми в I, и после их введения однозначное разложение на простые дивизоры в K превращается в однозначное разложение на простые числа в K. Но в общем случае это не так; именно поэтому Куммер говорит об *идеальных простых числах* $\mathfrak{p}$, которые не обязательно соответствуют *реальным простым числам* π из I. Всегда, однако, имеет место

Теорема о конечности числа классов. *Подгруппа* $\mathfrak{D}_0$ *главных дивизоров имеет в группе* $\mathfrak{D}$ *всех дивизоров поля* K *конечный индекс* h.

Таким образом, фактор-группа $\mathfrak{D}/\mathfrak{D}_0$ состоит из конечного числа h классов, называемых *классами дивизоров* поля K; каждый такой класс представляет собой совокупность дивизоров вида $c\alpha$, где c некоторый фиксированный дивизор, и α пробегает все отличные от нуля числа из K (рассматриваемые как главные дивизоры). Индекс

$$h = [\mathfrak{D} : \mathfrak{D}_0]$$

(ср. выше фиг. 9) называется *числом классов* поля K. Этот арифметический инвариант поля K является, так сказать, мерилом того, насколько сильно отличается мультипликативная арифметика в K от мультипликативной арифметики в P в отношении *разложения на простые множители*.

7. Теперь мы сформулировали все понятия арифметики поля K, которые понадобятся нам для наших непосредственных целей, а именно, для выяснения арифметического значения произведения L-рядов $\zeta(s\,|\,\mathfrak{K})$ и арифметического доказательства необращения $L(1\,|\,\chi)$ в нуль.

В отношении *первого* вопроса—арифметического значения произведения L-рядов $\zeta(s\,|\,\mathfrak{K})$—мы можем теперь сказать, что произведение (I) распространено на все простые дивизоры $\mathfrak{p}$ поля K, а сумма (II)—на все целые дивизоры $\mathfrak{n}$ поля K. Поэтому отмеченная уже формальная аналогия с представлениями в виде произведения и ряда для дзета-функции Римана $\zeta(s)$ приобретает с точки зрения арифметики поля K содержательное значение. В связи с этим $\zeta(s\,|\,\mathfrak{K})$ называется *дзета-функцией Дедекинда* поля K, по имени Дедикинда, который впервые ввел и исследовал эту функцию, и обозначают ее через $\zeta_k(s)$. Таким образом,

$$\zeta_{\mathsf{K}}(s) = \prod_{\chi \text{ из } \mathfrak{K}} L(s\,|\,\chi),$$

где $\mathfrak{K}$—соответствующая полю K группа дивизоров (ср. фиг. 8), и

$$\zeta_{\mathsf{K}}(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{p})^s}} = \sum_{\mathfrak{n}} \frac{1}{\mathfrak{N}(\mathfrak{n})^s},$$

где $\mathfrak{p}$ пробегает все простые дивизоры, а $\mathfrak{n}$—все целые дивизоры поля K. В этом смысле дзета-функция Римана $\zeta(s)$ является дзета-функцией поля P. Фигурирующие в первоначальных представлениях (I_0) и (II_0) показатели f_p, g_p и коэффициенты $\sigma(n\,|\,\mathfrak{K})$ получают теперь следующее арифметическое истолкование:

g_p есть количество различных простых давизоров $\mathfrak{p}$ поля K, входящих в p, f_p есть показатель степени в их нормах $\mathfrak{N}(\mathfrak{p}) = p^{f_p}$.

$\sigma(n \mid \mathfrak{R}) = \sigma_k(n)$ есть количество целых дивизоров $\mathfrak{n}$ поля K с нормой $\mathfrak{N}(\mathfrak{n}) = n$.

С нашей точки зрения, теперь, когда мы исходим не из группы дивизоров $\mathfrak{R}$, а из поля K, данные в I, II п. 1 явные представления для этих чисел надо рассматривать как правила, с помощью которых можно определять эти важные для арифметики поля K факты, которые фигурируют, в частности, и в теореме вложения, определяющей закон разложения чисел из K на простые дивизоры.

В отношении *второго* вопроса—необращения $L(1 \mid \chi)$ в нуль—надо в связи с VIII, п. 4 доказать, что дзета-функция $\zeta_m(s)$ поля деления круга P_m имеет при $s = 1$ полюс или—если желательно обходиться только элементарно-аналитическими средствами—что $\lim\limits_{s \to 1+0} \zeta_m(s) = +\infty$. Если использовать произведенное в п. 2 элементарно-аналитическое сведение этого вопроса к вопросу о квадратичном характере χ, как это делал Дирихле, то будет достаточно доказать соответствующий факт только для дзета-функции $\zeta_h(s)$ квадратичного поля

$$\mathsf{K} = \mathsf{P}\left(\sqrt{\chi(-1) f(\chi)}\right).$$

8. Чтобы получить это доказательство, надо показать на основании значения целых дивизоров $\mathfrak{n}$ для арифметики поля K—причем мы снова сформулируем это для любого подполя K поля P_m—следующее:

Предельная теорема. *Для частичной суммы коэффициентов ряда Дирихле*

$$\zeta_{\mathsf{K}}(s) = \sum_{\mathfrak{n}} \frac{1}{\mathfrak{N}(\mathfrak{n})^s}$$

имеет место предельное соотношение вида

$$\sum_{\mathfrak{N}(\mathfrak{n}) \leqq N} 1 = A_{\mathsf{K}} N + O\left(N^{1-\frac{1}{k}}\right) \quad \text{для} \quad N \to \infty$$

с некоторой, зависящей только от поля K положительной константой A_{K}, и при этом эта константа мультипликативно выражается в виде

$$A_{\mathsf{K}} = \frac{(2\tilde{\omega})^{\frac{1}{2}k} Rh}{w\sqrt{|d|}} \quad \text{с} \quad \tilde{\omega} = \left\{ \begin{array}{l} 2, \text{ если } \mathsf{K} \text{ вещественно} \\ \pi, \text{ если } \mathsf{K} \text{ комплексно} \end{array} \right\}$$

через арифметические инварианты поля K:

степень k,
дискриминант d,

количество корней w из 1,
регулятор R,
число классов h.

Так как, в силу этой теоремы, частичная сумма коэффициентов для $\zeta_{\mathsf{K}}(s) - A_{\mathsf{K}}\zeta(s)$ имеет порядок $O(N^{1-1/k})$, то из общей теории сходимости для рядов Дирихле, о которой шла речь в п 4, получается, что ряд Дирихле $\zeta_{\mathsf{K}}(s) - A_{\mathsf{K}}\zeta(s)$ сходится при $\sigma > 1 + 1/k$ (соответственно, при вещественных $s > 1 + 1/k$). Тогда отсюда следует, в силу известного нам поведения $\zeta(s)$ при $s = 1$ (соответственно при вещественном $s \to 1 + 0$) доказываемое утверждение относительно $\zeta_{\mathsf{K}}(s)$, а отсюда, в свою очередь, предельное соотношение

$$\lim_{s \to 1} (s-1)\,\zeta_{\mathsf{K}}(s) = A_{\mathsf{K}}$$

(соответственно, с вещественным $s \to 1 + 0$), согласно которому вычет функции $\zeta_{\mathsf{K}}(s)$ при $s = 1$ как раз равен константе A_{K}.

Из последней формулы для вычета мы получаем для значения при $s = 1$ произведения L-рядов, лежащего в основе доказательства Дирихле, следующее выражение:

$$\prod_{\substack{\chi \text{ из } \mathfrak{K} \\ \chi \neq \varepsilon}} L(1\,|\,\chi) = A_{\mathsf{K}} = \frac{(2\tilde{\omega})^{\frac{1}{2}k} Rh}{w\sqrt{|d|}}$$

через арифметические инварианты поля K, из которого делается очевидным исобращение $L(1/\chi)$ в нуль.

Если эту формулу разрешить относительно числа классов h поля K, то она примет вид

$$h = \frac{w\sqrt{|d|}}{(2\tilde{\omega})^{\frac{1}{2}k} R} \cdot \prod_{\substack{\chi \text{ из } \mathfrak{K} \\ \chi \neq \varepsilon}} L(1\,|\,\chi),$$

где $\mathfrak{K}$ есть группа характеров группы Галуа $\mathfrak{G}/\mathfrak{H}$ поля K (ср. фиг. 8). Как было сказано раньше, эту последнюю формулу можно использовать для определения числа классов h поля K, если найти сумму бесконечных рядов $L(1\,|\,\chi) = \sum_n \frac{\chi(n)}{n}$ в конечном виде. Мы сделаем это в § 18, п. 2, 3.

В связи с замечанием в § 14, п. 1, относительно обеих последних формул нужно еще сказать, что они только тогда имеют указанный простой вид, когда под $L(1\,|\,\chi)$ понимаются *собственные* L-ряды. В противном случае в выражении для A_{K} фигурировали бы еще и добавочные множители, которые появились бы в соответствии с формулой (3) п. 1, § 14 для несобственных L-рядов.

В рамках нашего общего обзора мы сформулировали предельную теорему для любого подполя K m-го поля деления круга P_m. Для доказательства теоремы Дирихле о простых числах достаточно, как уже говорилось, ограничиться частным случаем $\mathsf{K}=\mathsf{P}_m$, или, если использовать способ сведения из п. 2, частным случаем $\mathsf{K}=\mathsf{P}\left(\sqrt{\chi(-1)f(\chi)}\right)$. Для последнего случая мы в четвертой главе (см. § 16—18) докажем все те теоремы, которые здесь были нами только сформулированы.

Алгебраическо-теоретико-числовой метод доказательства необращения в нуль L-рядов при $s=1$ дает более глубокое представление о причине этого, чем теоретико-функциональные доказательства из п. 4, ибо теперь отличие от нуля следует из полученного в конце явного представления для произведения L-рядов при $s=1$, т. е. сводится к отличию от нуля арифметических инвариантов поля алгебраических чисел K. Но лишь оба метода вместе делают полностью ясным это положение, играющее большую роль во многих разделах современной математики, потому что здесь переплетаются между собой теория чисел, алгебра и теория функций.

Глава IV

КВАДРАТИЧНЫЕ ПОЛЯ

§ 16. ЭЛЕМЕНТАРНАЯ ТЕОРИЯ ДЕЛИМОСТИ

1. Основные алгебраические сведения. В вышеизложенных исследованиях мы уже много раз имели дело с квадратичными полями. При этом мы предполагали известными из алгебры основные алгебраические факты, относящиеся к этим полям. Теперь мы коротко их напомним, прежде чем приступить к систематическому построению арифметики квадратичных полей.

Квадратичное поле K определяется как алгебраическое расширение второй степени поля рациональных чисел P. Таким образом, мы получим K, если присоединим к P корень θ неприводимого над P квадратного многочлена

$$f(x) = x^2 - ux - v,$$

т. е. образуем все рациональные выражения от θ с коэффициентами из P; коротко пишут

$$\mathsf{K} = \mathsf{P}(\theta) \quad \text{с} \quad f(\theta) = 0.$$

Посредством подстановки $\theta^* = \theta - (1/2)u$ порождающего элемента можно добиться того, что будет $u = 0$, т. е.

$$f(x) = x^2 - v$$

будет чисто квадратным многочленом. Требование неприводимости означает тогда, что v не является квадратом в P. Если, далее,

$$v = Dw^2$$

есть однозначно определенное разложение числа v на его свободное от квадратов ядро D (ср. § 7, п. 4) и некоторый квадрат w^2 из P, то посредством подстановки $\theta^* = \theta/w$ порождающего элемента можно добиться того, что $v = D$, и, таким образом,

$$f(x) = x^2 - D$$

будет выражением *с целым рациональным, свободным от квадратов числом* D. Требование неприводимости сводится при этом к $D \neq 1$. Тогда $\theta = \sqrt{D}$ (знак можно взять произвольный) и

соответственно этому пишут

$$\mathsf{K} = \mathsf{P}(\sqrt{D}).$$

Посредством производимой над числами из K подстановки

$$\sqrt{D} \to -\sqrt{D},$$

которая переводит один корень многочлена $f(x)$ в другой, определяется нетождественный *автоморфизм* поля K. Так как поле K обладает поэтому двумя различными автоморфизмами (этим и тождественным), т. е. столькими автоморфизмами, какова его степень, то K нормально. *Группа Галуа* поля K — циклическая, порядка 2, порождаемая автоморфизмом $\sqrt{D} \to -\sqrt{D}$.

Числа α из K, то есть рациональные выражения от $\theta = \sqrt{D}$ с коэффициентами из P, могут быть, в силу основного равенства $\theta^2 = D$, преобразованы сначала к виду

$$\alpha = \frac{s + t\sqrt{D}}{u + v\sqrt{D}}$$

с коэффициентами s, t, u, v из P, а затем элементарно преобразованы (посредством умножения числителя и знаменателя на $u - v\sqrt{D}$) к *нормальной форме*

$$\alpha = a + b\sqrt{D} \tag{1}$$

с коэффициентами a, b из P. В этой нормальной форме a и b определены для данного α однозначно, так как ввиду неприводимости $f(x) = x^2 - D$ (иррациональности $\sqrt{D}$, ср. § 1, п. 6) соотношение вида $u + v\sqrt{D} = 0$ с u, v из P может выполняться только тривиальным образом, с $u = 0$, $v = 0$, последнее уже было использовано, когда мы уничтожали знаменатель $u + v\sqrt{D}$.

При автоморфизме $\sqrt{D} \to -\sqrt{D}$ из чисел α, заданных в нормальной форме (1), получаются *сопряженные* с ними числа

$$\alpha' = a - b\sqrt{D}. \tag{1'}$$

Переход от числа α из K к сопряженному с ним α' будет все время в дальнейшем обозначаться посредством штриха. Однако для чисел a из P, которые, очевидно, совпадают со своими сопряженными, штрих будет иметь *другое* значение. Числа из K мы будем все время обозначать греческими, а числа из P — латинскими буквами, за небольшим числом исключений, как, например, $i = \sqrt{-1}$ и некоторых показателей степеней и индексов, обозначенных греческими буквами.

Каждая пара сопряженных чисел α, α' из K является двумя корнями соответствующего *главного многочлена*

$$g(x \mid \alpha) = (x - \alpha)(x - \alpha') = x^2 - 2ax + (a^2 - Db^2)$$

с коэффициентами из P. При этом

$$S(\alpha) = \alpha + \alpha' = 2a$$
$$N(\alpha) = \alpha\alpha' \quad = a^2 - Db^2$$

называются соответственно *следом* и *нормой* числа α. Как функции от α, они обладают следующими свойствами:

$$\left.\begin{array}{l} S(\alpha_1+\alpha_2) = S(\alpha_1) + S(\alpha_2) \\ S(c\alpha) = cS(\alpha) \text{ для } c \text{ из } \mathsf{P} \end{array}\right\} \text{(линейность над } \mathsf{P}), \qquad (2)$$

$$\left.\begin{array}{l} N(\alpha_1\alpha_2) = N(\alpha_1)\,N(\alpha_2) \text{ (мультипликативность)} \\ N(\alpha) = 0 \text{ равносильно с } \alpha = 0 \end{array}\right\}. \qquad (3)$$

Для главного многочлена осуществляется лишь одна из двух следующих возможностей:

$g(x \mid \alpha)$ приводим, α рационально (степени 1), если $b = 0$;

$g(x \mid \alpha)$ неприводим, α иррационально (степени 2), если $b \neq 0$.

В первом случае мы имеем $\alpha = a$, $g(x \mid \alpha) = (x-a)^2$ (двукратный рациональный корень). Во втором случае $\alpha \neq \alpha'$ (два различных иррациональных корня); тогда α может быть выбрано в качестве порождающего элемента поля K (вместо фигурирующего выше θ). При этом $g(x \mid \alpha)$ будет чисто квадратным многочленом тогда и только тогда, когда $a = 0$, и, таким образом, $\alpha = b\sqrt{D}$ и $g(x \mid \alpha) = x^2 - Db^2$. Отсюда следует, что целое рациональное свободное от квадратов число $D \neq 1$, которое сначала получалось из произвольно выбранного порождающего элемента θ, на самом деле не зависит от выбора θ. Поэтому это число D является арифметическим инвариантом поля K. Так как, обратно, каждое такое число D приводит к квадратичному полю $\mathsf{K} = \mathsf{P}(\sqrt{D})$, мы получаем

I. *Квадратичные поля* K *на основании соотношения*

$$\mathsf{K} = \mathsf{P}(\sqrt{D})$$

взаимно однозначно соответствуют целым рациональным свободным от квадратов числам $D \neq 1$.

В дальнейшем мы всегда будем понимать под D вышеуказанный инвариант поля K.

Часто важно различать два типа квадратичных полей $\mathsf{K} = \mathsf{P}(\sqrt{D})$ с $D > 0$ и $D < 0$.

Если $D > 0$, то $\sqrt{D}$ вещественно. Тогда все числа из K вещественны и K называется вещественным квадратичным полем.

Если $D < 0$, то $\sqrt{D}$ — чисто мнимо. Тогда все числа из K, не принадлежащие к P, мнимы (комплексны), и K называется мнимым квадратичным полем.

Пара чисел 1, $\sqrt{D}$ является на основании (1) некоторым специальным базисом поля K. Так как, согласно (1), каждые три числа из K линейно зависимы над P, то вообще каждая пара линейно независимых над P чисел θ_1, θ_2 из K является в этом смысле базисом K, то есть числа α из K, аналогично (1), представимы также в форме

$$\alpha = a_1\theta_1 + a_2\theta_2$$

с однозначно определенными коэффициентами a_1, a_2 из P. Для сопряженных тогда имеет место, аналогично (1),

$$\alpha' = a_1\theta_1' + a_2\theta_2'$$

с теми же самыми коэффициентами. Запишем оба последних равенства, линейных относительно a_1, a_2 в матричной форме

$$(\alpha\alpha') = (a_1a_2)\begin{pmatrix}\theta_1 & \theta_1'\\ \theta_2 & \theta_2'\end{pmatrix}.$$

Определитель двухстрочной квадратной матрицы, стоящей справа, обладает тем свойством, что его квадрат

$$d(\theta_1, \theta_2) = \begin{vmatrix}\theta_1 & \theta_1'\\ \theta_2 & \theta_2'\end{vmatrix}^2 \tag{4}$$

инвариантен относительно автоморфизма $\sqrt{D} \to -\sqrt{D}$ поля K, т. е. является рациональным числом. Этот квадрат определителя называется *дискриминантом пары чисел* θ_1, θ_2 из K. Пусть в матричной записи представления (1), (1′) для рассматриваемой пары чисел и сопряженной с ней имеют вид

$$\begin{pmatrix}\theta_1\\ \theta_2\end{pmatrix} = U\begin{pmatrix}1\\ \sqrt{D}\end{pmatrix}, \quad \begin{pmatrix}\theta_1'\\ \theta_2'\end{pmatrix} = U\begin{pmatrix}1\\ -\sqrt{D}\end{pmatrix}, \tag{5}$$

где U — рациональная двухстрочная квадратная матрица. Тогда имеет место матричное равенство

$$\begin{pmatrix}\theta_1 & \theta_1'\\ \theta_2 & \theta_2'\end{pmatrix} = U\begin{pmatrix}1 & 1\\ \sqrt{D} & -\sqrt{D}\end{pmatrix},$$

и потому, согласно правилу перемножения определителей,

$$d(\theta_1, \theta_2) = |U|^2 \cdot d(1, \sqrt{D}). \tag{6}$$

При этом дискриминант специального базиса

$$d(1, \sqrt{D}) = \begin{vmatrix}1 & 1\\ \sqrt{D} & -\sqrt{D}\end{vmatrix} = 4D \tag{7}$$

заведомо отличен от нуля. Далее, определитель $|U|$ отличен от нуля тогда и только тогда, когда пара чисел θ_1, θ_2 линейно независима над P. Объединяя полученные результаты, получаем:

II. *Дискриминант* $d(\theta_1, \theta_2)$ *пары чисел* θ_1, θ_2 *из* K, *определяемый равенством* (4), *является рациональным числом. Оно от-*

личается от инварианта D поля K *только множителем, являющимся квадратом рационального числа, а именно, равным учетверенному квадрату определителя матрицы перехода* (5) *от базиса* $1, \sqrt{D}$ *к паре чисел* θ_1, θ_2.

Пара чисел θ_1, θ_2 *тогда и только тогда линейно независима над* P, *то есть является базисом* K, *когда ее дискриминант* $d(\theta_1, \theta_2) \neq 0$.

2. **Геометрическая иллюстрация.** Аналогично представлению чисел из P на числовой прямой мы будем геометрически изображать числа

$$\alpha = a + b\sqrt{D}$$

из K точками на плоскости с декартовыми координатами

$$R(\alpha) = \frac{\alpha + \alpha'}{2}, \quad J(\alpha) = \left\{ \begin{array}{l} \frac{\alpha - \alpha'}{2} = b\sqrt{D} \text{ для } D > 0 \\ \frac{\alpha - \alpha'}{2i} = \frac{b\sqrt{D}}{i} \text{ для } D < 0 \end{array} \right\},$$

которые мы будем также называть соответственно *рациональной* и *иррациональной частями* числа α. В этом смысле будем говорить коротко о *представлении на* K*-плоскости*. Мы считаем при этом, что если числа из K вещественны, соответственно комплексны, то квадратный корень $\sqrt{D}$ взят *положительно вещественным* соответственно *положительно-мнимым*.

При переходе к сопряженному

$$\alpha' = a - b\sqrt{D}$$

$R(\alpha)$ остается неизменным, в то время как $I(\alpha)$ меняет знак. Таким образом, этому переходу соответствует отражение относительно рациональной оси. Для нормы в координатном представлении имеем

$$N(\alpha) = \alpha\alpha' = \left\{ \begin{array}{l} R(\alpha)^2 + I(\alpha)^2 \text{ для } D < 0 \\ R(\alpha)^2 - I(\alpha)^2 \text{ для } D > 0 \end{array} \right\}.$$

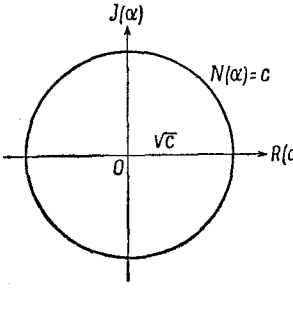
Если расширить область изменения коэффициентов a, b до совокупности всех вещественных чисел, то α, α' будут пробегать в случае $D < 0$ все пары комплексно сопряженных, а в случае $D > 0$ независимо друг от друга все пары вещественных чисел. Равенство

$$N(\alpha) = c$$

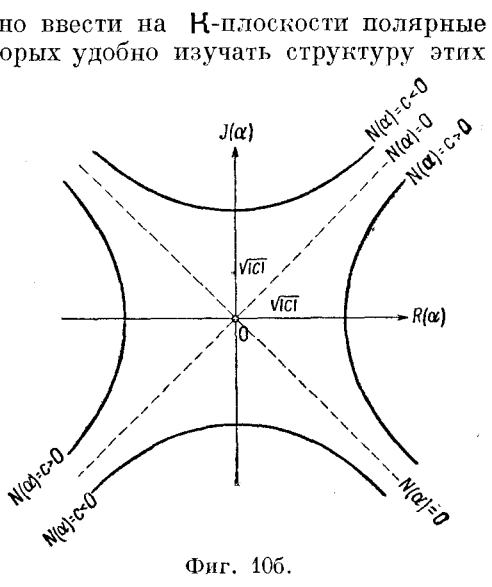
с постоянным вещественным c определяет тогда для $D < 0$ круг, для $D > 0$ — равностороннюю гиперболу, причем и круг, и гипербола имеют центр в начале координат. Для $D < 0$ нужно рассматривать только постоянные $c \geqslant 0$; радиус круга равен тогда $\sqrt{c}$ (фиг. 10а). Для $D > 0$ главной осью равносторонних

гипербол служит рациональная или иррациональная ось, в зависимости от того, $c > 0$ или $c < 0$, а полуоси гипербол равны $\sqrt{|c|}$; для $c = 0$ получается общая для всех этих гипербол пара асимптот $R(\alpha) = \pm I(\alpha)$, являющихся биссектрисами координатных углов (фиг. 10б).

Для многих целей уместно ввести на К-плоскости полярные координаты, с помощью которых удобно изучать структуру этих



Фиг. 10а.



Фиг. 10б.

кругов и гипербол. Для этого берут в качестве меры величины чисел α из К квадратный корень $\sqrt{|N(\alpha)|}$ из абсолютной величины нормы и определяют полярный угол $\varphi(\alpha)$ соотношением

$$\alpha = \left\{ \begin{array}{l} \sqrt{N(\alpha)}\, e^{i\varphi(\alpha)} \text{ для } D < 0 \\ \operatorname{sgn}\alpha \sqrt{|N(\alpha)|}\, e^{\varphi(\alpha)} \text{ для } D > 0 \end{array} \right\}.$$

Ввиду $N(\alpha') = N(\alpha)$ для сопряженного с α числа α' имеем

$$\alpha' = \left\{ \begin{array}{l} \sqrt{N(\alpha)}\, e^{-i\varphi(\alpha)} \text{ для } D < 0 \\ \operatorname{sgn}\alpha' \sqrt{|N(\alpha)|}\, e^{-\varphi(\alpha)} \text{ для } D > 0 \end{array} \right\}$$

и, таким образом, $\varphi(\alpha') = -\varphi(\alpha)$. Если снова представить себе область изменения a, b расширенной до совокупности всех вещественных чисел, то уравнения

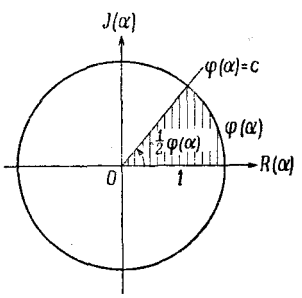
$$\varphi(\alpha) = c$$

с постоянным вещественным c определяют для $D < 0$ лучи, исходящие из начала координат, а для $D > 0$ пары прямых, прохо-

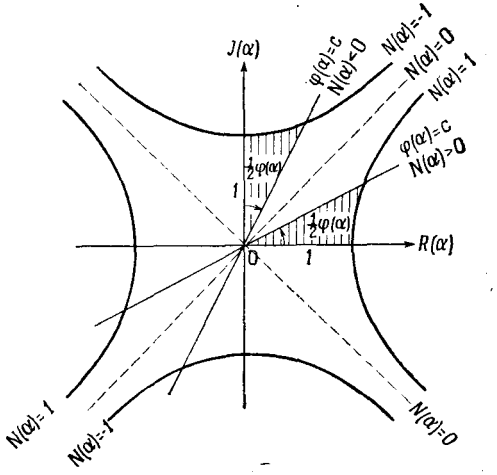
дящих через начало координат и симметричных относительно асимптот, которые соответствуют обоим возможным знакам

$$\operatorname{sgn} N(\alpha) = \operatorname{sgn} \alpha \operatorname{sgn} \alpha'.$$

Для случая $D < 0$ получаются обычные полярные координаты на комплексной плоскости; при этом полярный угол $\varphi(\alpha)$ может толковаться не только как длина дуги единичного круга, заключенной между положительной вещественной осью и лучом, проходящим через α, как это обычно делается, но также и как удвоенная площадь заштрихованного сектора (фиг. 11а). Для



Фиг. 11а.



Фиг. 11б.

случая $D > 0$ первое толкование $\varphi(\alpha)$ не имеет аналогии, однако второе переносится и на этот случай: полярный угол $\varphi(\alpha)$ равен здесь удвоенной площади заштрихованного сектора, который вырезается из области, внутренней для пары равносторонних единичных гипербол, лучом, проходящим через α, и рациональной или иррациональной осью, в зависимости от того, $N(\alpha) > 0$ или $N(\alpha) < 0$ (фиг. 11б).

Доказательство последнего утверждения получается так. Пусть, например, $N(\alpha) > 0$. Без ограничения общности можно считать, что $\alpha > 0$, $\alpha' > 0$ (иначе мы произвели бы отражение относительно начала координат), а также, что $\varphi(\alpha) \geqslant 0$ (этого можно добиться отражением относительно рациональной оси). Пусть

$$x,\ y,\ r,\ \varphi$$

непрерывные вещественные переменные, соответствующие фигурирующим выше

$$R(\alpha),\ I(\alpha),\ \sqrt{|N(\alpha)|},\ \varphi(\alpha).$$

Соотношения между последними величинами дают теперь

$$\left.\begin{matrix} x+y=re^{\varphi} \\ x-y=re^{-\varphi} \end{matrix}\right\}, \text{ откуда } \left\{\begin{matrix} x=r\operatorname{ch}\varphi \\ y=r\operatorname{sh}\varphi \end{matrix}\right\}.$$

Тогда гиперболический сектор, о котором идет речь, имеет площадь

$$\iint\limits_{\substack{0\leqslant r\leqslant 1\\ 0\leqslant\varphi\leqslant\varphi(\alpha)}} dx\,dy=\int\limits_{r=0}^{1}\int\limits_{\varphi=0}^{\varphi(\alpha)}\left|\frac{\partial(x,y)}{\partial(r,\varphi)}\right|dr\,d\varphi=\int\limits_{r=0}^{1}\int\limits_{\varphi=0}^{\varphi(\alpha)} r\,dr\,d\varphi={}^1/_2\,\varphi(\alpha).$$

3. Целые числа, дискриминант. Чтобы изучать арифметику квадратичного поля K, мы должны сначала дать определение основного понятия *целого числа из* K. В нашем общем обзоре арифметики полей алгебраических чисел в § 15, п. 5 мы уже говорили о том, как вводится это понятие для любого поля алгебраических чисел. Мы покажем здесь для случая квадратичного поля, каким образом мы с неизбежностью должны прийти к данному там определению.

От определения понятия целого числа из K естественно потребовать, чтобы оно удовлетворяло следующим требованиям:

А. *Целые числа из* K *образуют область целостности* I.

Она должна тогда содержать число 1 и вместе с ней всю область целостности Γ целых рациональных чисел.

Б. *Рациональное число является целым в* K *тогда и только тогда, когда оно целое рациональное.*

Другими словами, Γ есть пересечение I с P:

$$\mathsf{I}\cap\mathsf{P}=\Gamma.$$

В. *Вместе с числом* α *из* K *сопряженное с ним* α' *тоже является целым.*

Другими словами, область целостности I инвариантна относительно порождающего автоморфизма поля K:

$$\mathsf{I}'=\mathsf{I}.$$

Г. *Совокупность целых чисел из* K *не может быть больше расширена так, чтобы при этом требования* А, Б, В *попрежнему удовлетворялись.*

Другими словами, I есть *максимальная* область целостности со свойствами $\mathsf{I}\cap\mathsf{P}=\Gamma$ и $\mathsf{I}'=\mathsf{I}$.

Предположим, что мы имеем понятие целостности, удовлетворяющее требованиям А, Б, В. Если тогда α — целое, то, согласно В, также и α' — целое, а тогда, согласно А, целыми будут также $\alpha+\alpha'=S(\alpha)$ и $\alpha\alpha'=N(\alpha)$, и, ввиду Б, эти последние будут целыми рациональными. Итак, коэффициенты соответствующего α главного многочлена $g(x\,|\,\alpha)$ — целые рациональные, т. е. свойство, принятое в § 15, п. 5 за определение, выполняется.

Если мы, наоборот, примем это свойство за определение понятия целостности, т. е. назовем целыми *все* α, для которых главный многочлен $g(x\,|\,\alpha)$ имеет целые рациональные коэффициенты $S(\alpha)$, $N(\alpha)$, то, согласно только что приведенным соображениям, во всяком случае выполняется требование Г. Далее, выполняется, очевидно, также и В, а, ввиду того что для рационального a $S(a)=2a$, $N(a)=a^2$, — также и Б. Теперь мы покажем, что при этом определении выполняется также и А. Тогда мы получим, что нашим требованиям А, Б, В, Г можно удовлетворить только одним способом, именно, посредством уже данного в § 15, п. 5 общего определения:

Число из K *называется целым, если коэффициенты его главного многочлена, т. е. его след и норма, суть целые рациональные числа.*

Прежде чем доказывать, что при этом определении действительно выполняется свойство А, мы дадим явное представление для целых чисел из K. Для этого целесообразно записать представление (1′) п. 1 в несколько измененном виде

$$\alpha=\frac{a+b\sqrt{D}}{2} \tag{1}$$

с рациональными a, b, так что теперь

$$S(\alpha)=a,\quad N(\alpha)=\frac{a^2-Db^2}{4}. \tag{2}$$

Тогда мы покажем

III. *Число* α *из* K, *заданное в форме* (1), *будет целым тогда и только тогда, когда* a, b — *целые рациональные числа, удовлетворяющие сравнениям*

$$a\equiv b \mod 2 \quad \textit{для} \quad D\equiv 1 \mod 4$$
$$a\equiv b\equiv 0 \mod 2 \quad \textit{для} \quad D\equiv 2, 3 \mod 4.$$

Случай $D\equiv 0 \bmod 4$ для целого рационального свободного от квадратов числа D, конечно, невозможен.

Доказательство. а) Если a, b удовлетворяют этим соотношениям, то, согласно (2), $S(\alpha)$ и $N(\alpha)$ являются целыми рациональными, т. е. α — целое.

б) Пусть, обратно, α — целое, так что $S(\alpha)$ и $N(\alpha)$ целые рациональные. Тогда, согласно (2), a во всяком случае целое рациональное, и, далее, ввиду того что таковым является $(a^2-Db^2)/4$, также и $(a^2-4)\cdot(a^2-Db^2)/4=Db^2$ будет целым рациональным. Так как D свободно от квадратов, то знаменатель числа b^2 с ним сократиться не может, и потому b также должно быть целым рациональным. Тогда имеет место сравнение

$$a^2\equiv Db^2 \bmod 4.$$

Для $D \equiv 1 \bmod 4$ оно равносильно с $a \equiv b \bmod 2$, в то время как для $D \equiv 2, 3 \bmod 4$ оно имеет лишь решение $a \equiv b \equiv 0 \bmod 2$. Поэтому a, b удовлетворяют указанным условиям.

Для многих целей форма (1) с соотношениями из III для целых чисел α из K наиболее удобна. Для других целей, однако, оказывается нужным следующее элементарное преобразование. Введем специальное целое число

$$\left.\begin{array}{ll} \omega = \dfrac{1+\sqrt{D}}{2} & \text{для } D \equiv 1 \bmod 4 \\ \omega = \sqrt{D} & \text{для } D \equiv 2,3 \bmod 4 \end{array}\right\} \tag{3}$$

из K. Вместе с 1 оно заведомо образует базис поля K, так как оно линейно независимо от 1 над P. Если преобразовать представление (1) к этому новому базису 1, ω:

$$\alpha = \frac{a-b}{2} + b\omega \text{ для } D \equiv 1 \bmod 4,$$

$$\alpha = \frac{a}{2} + \frac{b}{2}\omega \text{ для } D \equiv 2,3 \bmod 4,$$

то на основании соотношений из III новые коэффициенты будут пробегать как раз все пары целых рациональных чисел, если α будет пробегать все целые числа из K. Этим доказано

IV. *Числа* 1, ω *образуют целочисленный базис поля* K, *т. е. такой базис, что целыми числами поля* K *являются числа*

$$\alpha = a + b\omega$$

с целыми рациональными коэффициентами a, b *и только они.*

Из этого последнего представления ясно, что целые числа из K образуют аддитивную группу. Чтобы доказать, что они образуют даже область целостности I, достаточно показать, что произведение ω^2 базисного числа ω самого на себя будет целым. Это вытекает из равенства $\omega^2 = S(\omega)\,\omega - N(\omega)$. Тем самым доказано, что при нашем определении целостности выполняется также и требование A.

Пусть аналогично (5) из п. 1 мы имеем пару целых чисел ω_1, ω_2 из K и пусть

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = U \begin{pmatrix} 1 \\ \omega \end{pmatrix},$$

где U — двухстрочная квадратная матрица с целыми рациональными элементами. Для того чтобы ω_1, ω_2 образовывали базис поля K, необходимо и достаточно, чтобы было $|U| \neq 0$. Однако при этом ω_1, ω_2 еще не обязательно образуют целочисленный базис поля K. Для того чтобы это имело место, необходимым и достаточным является условие $|U| = \pm 1$; тогда матрица U^{-1} обратного перехода от базиса ω_1, ω_2 к базису 1, ω будет иметь

целые рациональные элементы, т. е. 1, ω, а вместе с ними и все целые числа из K будут выражаться через базис ω_1, ω_2 с целыми рациональными коэффициентами. Как и в (6) п. 1, мы имеем

$$d(\omega_1, \omega_2) = |U|^2 d(1, \omega).$$

Отсюда, аналогично II, следует

V. *Дискриминант* $d(\omega_1, \omega_2)$ *пары целых чисел* ω_1, ω_2 *из* K *отличается от дискриминанта* $d(1, \omega)$ *целого базиса* $1, \omega$ *только множителем, являющимся квадратом целого рационального числа, а именно, равным квадрату определителя матрицы перехода от базиса* $1, \omega$ *к паре* ω_1, ω_2.

Пара целых чисел ω_1, ω_2 *образует целочисленный базис поля* K *тогда и только тогда, когда имеет место равенство* $d(\omega_1, \omega_2) = d(1, \omega)$.

Итак, дискриминанты всех целых базисов поля K имеют одно и то же значение

$$d = d(1, \omega).$$

Оно является поэтому арифметическим инвариантом поля K. Этот инвариант d называется *дискриминантом поля* K. Так как в (7) п. 1 уже было найдено, что $d(1, \sqrt{D}) = 4D$, и так как детерминант матрицы перехода от $1, \sqrt{D}$ к $1, \omega$, согласно (3), равен $1/2$ или 1, в зависимости от того, $D \equiv 1 \bmod 4$ или $D \equiv 2, 3 \bmod 4$, то получается следующая связь между дискриминантом d и инвариантом D из I п. 1:

$$d = \left\{ \begin{array}{lll} D & \text{для} & D \equiv 1 \mod 4 \\ 4D & \text{для} & D \equiv 2, 3 \mod 4 \end{array} \right\}. \tag{4}$$

Согласно общему определению (4) п. 1 дискриминанта $d(\theta_1, \theta_2)$ пары чисел θ_1, θ_2 из K, для дискриминанта поля мы получаем

$$d = d(1, \omega) = \begin{vmatrix} 1 & 1 \\ \omega & \omega' \end{vmatrix}^2 = (\omega - \omega')^2,$$

т. е. как раз то, что в алгебре называется дискриминантом соответствующего ω главного многочлена

$$g(x) = (x - \omega)(x - \omega') = x^2 - sx + t \quad \left(\begin{array}{l} s = S(\omega) \\ t = N(\omega) \end{array} \right),$$

а именно,

$$d = s^2 - 4t.$$

Как показывает сравнение формулы (4) с IV, п. 5, § 9, дискриминант d поля K может быть также определен как ведущий модуль символа Якоби $\left(\frac{D}{x}\right)$ как функции его знаменателя x.

При таком определении дискриминанта d должен предполагаться известным лежащий в основе IV, п. 5, § 9 квадратичный закон взаимности. И наоборот, доказательства квадратичного закона взаимности, опирающиеся на теорию квадратичных полей, основываются, как мы увидим в § 19, п. 3, 4, как раз на этой связи.

Для удобства дальнейшего изложения целесообразно описывать поле $\mathsf{K}=\mathsf{P}(\sqrt{D})$ не инвариантом D, а связанным с ним посредством (4) дискриминантом d, как основным инвариантом. При этом во всяком случае имеет место

$$\mathsf{K}=\mathsf{P}(\sqrt{d}).$$

Это соответствует сделанному в § 9, п. 6 обобщению символа Якоби $\left(\frac{D}{x}\right)$ до понятия символа Кронекера, который записывается в такой же форме $\left(\frac{d}{x}\right)$ и определяется в области чисел x, взаимно простых с его числителем и ведущим модулем d, как одна из единиц ± 1, а для чисел x, не взаимно простых с d, считается согласно (3) п. 6, § 13, равным нулю.

Так как квадратичное поле K полностью определяется своим дискриминантом d как основным инвариантом, то все другие арифметические инварианты поля K принципиально должны выражаться через d или, во всяком случае, их значения должны определяться значением d. Мы будем выполнять это по мере надобности для названных в общем обзоре в § 15, п. 5 арифметических инвариантов (количества w корней из 1, регулятора R, числа классов h).

В дальнейшем мы все время будем, не поясняя этого каждый раз специально, понимать под d дискриминант поля K. При случае мы будем использовать также и свободное от квадратов ядро D, относительно которого мы заключили аналогичное соглашение уже в связи с I, п. 1.

Представление (1) с соотношениями из III для целых α из K получает после введения d вместо D несколько более простой вид:

$$\alpha=\frac{a+b\sqrt{d}}{2};\ a,\ b-\text{целые рациональные},\ a\equiv db \bmod 2. \qquad (5)$$

Целое число, записываемое без помощи D, которое вместе с 1 образует целочисленный базис поля K, получается посредством видоизменения формулы (3) для ω в виде

$$\omega^*=\frac{d+\sqrt{d}}{2}.$$

Действительно, согласно (5), ω^* — целое и, кроме того,

$$d=(1,\ \omega^*)=\frac{1}{2^2}d\,(1,\sqrt{d})=\frac{1}{4}\cdot 4d=d.$$

Целочисленный базис 1, ω^* используется, однако, довольно редко, в то время как представление (5) для целых чисел оказывается очень нужным во многих случаях.

При введенном в п. 2 геометрическом представлении на K-плоскости целые числа поля K, как порожденная двумя линейно независимыми числами ω_1, ω_2 аддитивная абелева группа, будут изображаться точками некоторой параллельной решетки. При этом важны только сами точки решетки. Образующие их своими пересечениями параллельные прямые могут быть проведены многими способами соответственно различному выбору целочисленного базиса ω_1, ω_2 поля K. Точки, соответствующие числам этого базиса, определяют основной параллелограм, на который натягивается решетка. В случае специального целого базиса 1, ω из (3) для $D \equiv 2, 3 \bmod 4$, когда $\omega = \sqrt{D}$, в качестве основного параллелограма получается прямоугольник со сторонами, параллельными осям, и с площадью $\sqrt{|D|}$ (фиг. 12а). Для $D \equiv 1 \bmod 4$, когда $\omega = (1+\sqrt{D})/2$ для получения точек решетки целых чисел нужно взять, кроме вершин этих прямоугольников, также и их центры; основным параллелограмом будет тогда параллелограм с площадью $\sqrt{|D|}/2$ (фиг. 12б); можно взять в качестве основного параллелограма и определяемый базисом $(1+\sqrt{D})/2$, $(-1+\sqrt{D})/2$ ромб. Вообще, объем G основного параллелограма равен абсолютной величине определителя:

$$G = \left\| \begin{matrix} R(\omega_1) & I(\omega_1) \\ R(\omega_2) & I(\omega_2) \end{matrix} \right\| = \left\| \begin{matrix} \frac{\omega_1+\omega_1'}{2} & \frac{\omega_1-\omega_1'}{2} \\ \frac{\omega_2+\omega_2'}{2} & \frac{\omega_2-\omega_2'}{2} \end{matrix} \right\| = \frac{1}{2} \left\| \begin{matrix} \omega_1 & \omega_1' \\ \omega_2 & \omega_2' \end{matrix} \right\| \frac{1}{2}\sqrt{|d|}. \qquad (6)$$

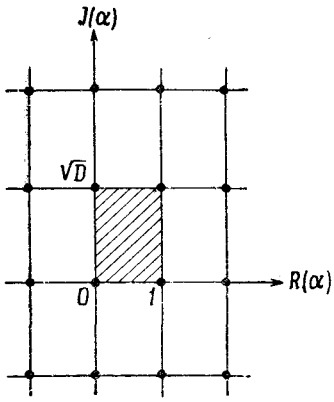
и, таким образом, не зависит от выбора основного параллелограма. Абсолютная величина дискриминанта $|d|$ допускает поэтому геометрическое истолкование как квадрат удвоенной площади основного параллелограма решетки целых чисел на K-плоскости.

После определения области целостности I на квадратичное поле K переносится элементарная теория делимости в смысле § 1, п. 2 вместе с определенными там основными понятиями делимости, кратного, единицы, ассоциированных чисел, из которых последние два понятия будут подробно объяснены в п. 4, 5. Здесь мы заметим прежде всего следующее. Ввиду свойства Б понятия целостности, эти основные понятия теории делимости для рациональных чисел остаются неизменными, если эти числа рассматривать как числа из поля K. Поэтому нет надобности в различных обозначениях для этих понятий в поле P и в поле K. Там же, где это будет необходимо, мы будем, конечно, отмечать

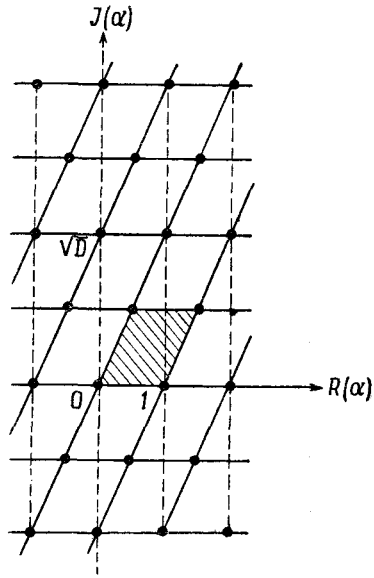
это различие, подобно тому, как мы говорили до сих пор о числах из Г всегда не просто «целое», а «целое рациональное».

Наша ближайшая задача заключается в том, чтобы немного подробнее осветить элементарную теорию делимости в К. Основной для этого является следующая связь между соотношением делимости в К и в Р, которая немедленно вытекает из мультипликативности (3) п. 1 нормы и определение целостности в К:

Правило для норм. *Из* α/β *следует* $N(\alpha)/N(\beta)$.



Фиг. 12а.



Фиг. 12б.

Так как для целостности β/α требуется, кроме целостности $N(\beta/\alpha)$, также и целостность $S(\beta/\alpha)$, то эта связь не является обратимой. Она означает только, что посредством образования нормы соотношения делимости в К гомоморфно отображаются в соотношения делимости в Р.

Правило цля норм является примером к сделанному выше замечанию относительно обозначений. Нет необходимости особо оговаривать, что второе соотношение делимости должно рассматриваться в поле Р, хотя суть дела заключается именно в этом.

4. Единицы. *Единицы* ε поля К определяются в элементарной теории делимости как такие целые числа, которые являются делителями числа 1:

ε *есть единица тогда и только тогда, когда* ε *целое и* $\varepsilon \mid 1$.

Единицы образуют мультипликативную группу E в ней содержится циклическая подгруппа второго порядка из единиц ± 1 поля P (корней второй степени из 1).

Из правила для норм вытекает следующий простой критерий

VI. *Число ε из K будет единицей тогда и только тогда, когда оно целое, и его норма является единицей в P, т. е. когда ε целое и $N(\varepsilon) = \pm 1$.*

Доказательство. а) Если ε — целое и $\varepsilon \mid 1$, то $N(\varepsilon)$ — целое и $N(\varepsilon) \mid 1$.

б) Если ε — целое и $N(\varepsilon) = \pm 1$, т. е. $\varepsilon\varepsilon' = \pm 1$, то, ввиду того что ε' тоже целое, $\varepsilon \mid 1$.

Если представить ε, соответственно (5) п. 3, в форме

$$\varepsilon = \frac{u + v\sqrt{d}}{2}; \quad u, v \text{ — целые рациональные, } u \equiv dv \bmod 2, \quad (1)$$

то из VI получается следующая характеристика единиц поля K через целые рациональные числа:

VII. *Единицы ε поля K на основании своего представления* (1) *взаимно однозначно соответствуют целым рациональным решениям u, v пары уравнений*

$$\frac{u^2 - dv^2}{4} = \pm 1.$$

Дополнительное условие $u \equiv dv \bmod 2$ можно при этом опустить. Оно будет само собой выполняться для целочисленных решений, потому что ввиду $d \equiv 1$ или $0 \bmod 4$ оно равносильно $u^2 \equiv dv^2 \bmod 4$.

Пара уравнений из VII будет коротко называться *уравнением Пелля*. Нахождение всех единиц поля K сводится к определению всех решений этого диофантова уравнения, причем, как обычно, слово *диофантово* означает, что нас интересуют только целые рациональные решения. При геометрическом представлении на K-плоскости речь идет об определении всех точек решетки целых чисел, лежащих на единичном круге соответственно на двух равносторонних единичных гиперболах.

При решении этого вопроса мы будем соответственно различию в геометрических картинах разбирать оба случая $d < 0$ и $d > 0$ отдельно.

Случай а: Мнимое квадратичное поле $\mathsf{K} = \mathsf{P}(\sqrt{d})$, $d < 0$. В этом случае уравнение Пелля имеет вид

$$\frac{u^2 + |d| v^2}{4} = 1,$$

причем справа нужно действительно брать только $+1$, так как оба члена слева неотрицательны.

При $|d|>4$ существуют только два решения $u=\pm 2$, $v=0$; им соответствуют обе рациональные единицы $\varepsilon=\pm 1$. Других единиц в этом случае нет.

Единственными дискриминантами $d<0$ с $|d|\leqslant 4$ являются $d=-3$ и $d=-4$. Им соответствуют поля деления круга $\mathsf{K}=\mathsf{P}(\sqrt{-3})=\mathsf{P}(\rho)=\mathsf{P}_3=\mathsf{P}_6$, которые мы уже знаем из § 10, п. 8, 9 (здесь $\rho=\frac{-1+\sqrt{-3}}{2}$ — первообразный 3-й корень из 1; $-\rho$ является первообразным 6-м корнем из 1), и $\mathsf{K}=\mathsf{P}(\sqrt{-1})=\mathsf{P}(i)=\mathsf{P}_4$ (где $i=\sqrt{-1}$ — первообразный 4-й корень из 1). В этих случаях уравнение Пелля имеет, кроме двух названных ранее решений, еще следующие:

$$d=-3 \quad u=\pm 1,\ v=\pm 1 \text{ с } \varepsilon=\frac{\pm 1\pm\sqrt{-3}}{2}=\pm\rho,\ \pm\rho^2$$

$$d=-4 \quad u=0, \quad v=\pm 1 \text{ с } \varepsilon=\pm\sqrt{-1}=\pm i$$

и никаких других.

Подытоживая вышесказанное, мы получаем

VIIIа. *В мнимом квадратичном поле* $\mathsf{K}=\mathsf{P}(\sqrt{d})$ $(d<0)$ *группа единиц* E *является конечной циклической, состоящей из* w *различных* w*-х корней из* 1, *где* w *имеет значения*

$$w=6 \quad \text{для} \quad d=-3,$$
$$w=4 \quad \text{для} \quad d=-4,$$
$$w=2 \quad \text{в остальных случаях.}$$

Единицы ε *поля* K *однозначно задаются представлением через базис в виде*

$$\varepsilon=\zeta^{\nu} \qquad (\nu \bmod w),$$

где ζ *— первообразный* w*-й корень из* 1.

Случай б: *Вещественное квадратичное поле* $\mathsf{K}=\mathsf{P}(\sqrt{d})$, $d>0$. В этом случае в уравнении Пелля нужно рассматривать оба знака

$$\frac{u^2-dv^2}{4}=\pm 1,$$

и теперь так просто, как в первом случае, определить совокупность решений нельзя, так как в левой части стоит один положительный и один отрицательный член, величины которых ничем не ограничены.

Чтобы доказать существование нетривиальных единиц, т. е. отличных от обеих рациональных единиц ± 1, мы докажем предварительно две леммы, из которых первая представляет собой общее апроксимационное высказывание относительно любого

вещественного числа Θ, в то время как вторая получается применением первой к нашему базисному числу ω.

Лемма 1. *Для данных вещественного числа Θ и натурального числа n существует пара целых рациональных чисел x, y, таких, что*

$$|\Theta y - x| < \frac{1}{n}, \quad 1 \leqslant y \leqslant n.$$

Вместо этого утверждения леммы в однородной форме часто используется утверждение в неоднородной форме

$$\left|\Theta - \frac{x}{y}\right| < \frac{1}{ny} \left(\leqslant \frac{1}{y^2}\right), \quad 1 \leqslant y \leqslant n,$$

где заключенное в скобки ослабленное неравенство означает, что каждое вещественное число может быть апроксимировано рациональным числом со знаменателем, не превосходящим заданного n, так, что ошибка будет меньше, чем обратная величина квадрата знаменателя.

Доказательство. Возьмем $n+1$ кратных $y\Theta$ с $y = 0, 1, \ldots, n$ и вычтем из каждого из них наибольшее целое, не превосходящее его число $x = [y\Theta]$. Мы получим лежащие в интервале $0 \leqslant z < 1$ остатки:

$$0 \leqslant y\Theta - x < 1.$$

Если разделить этот интервал на n частей

$$0 \leqslant z < \frac{1}{n}, \ \frac{1}{n} \leqslant z < \frac{2}{n}, \ \ldots, \ \frac{n-1}{n} \leqslant z < 1,$$

то из имеющихся $n+1$ остатков по крайней мере два будут лежать в одной и той же части интервала. Если $y'\Theta - x'$, $y''\Theta - x''$ — два таких остатка и, например, $y' > y''$, то их разность

$$(y'\Theta - x') - (y''\Theta - x'') = (y' - y'')\,\Theta - (x' - x'') = y\Theta - x$$

обладает свойством

$$|y\Theta - x| < \frac{1}{n}; \ x, y \text{ целые рациональные}; \ 1 \leqslant y \leqslant n,$$

что и требовалось доказать.

Лемма 2. *Для данного натурального числа n существует целое число $\alpha \neq 0$ из K, такое, что*

$$|\alpha| < \frac{1}{n}, \ |N(\alpha)| < 1 + \sqrt{d}.$$

Доказательство. Применим лемму 1 к $\Theta = -\omega$, где ω — базисное число поля K из (3) п. 3. Тогда мы получим целое число

$$\alpha = x + y\omega,$$

такое, что

$$|\alpha| < \frac{1}{n}, \quad 1 \leqslant y \leqslant n.$$

Ввиду того что $y \neq 0$, также и $\alpha \neq 0$. Для сопряженного α', принимая во внимание соотношение

$$\alpha' = x + y\omega' = (x + y\omega) + y(\omega' - \omega) = \alpha + y\sqrt{d},$$

получаем оценку

$$|\alpha'| \leqslant |\alpha| + y\sqrt{d} < \frac{1}{n} + n\sqrt{d}.$$

Для нормы $N(\alpha) = \alpha\alpha'$ получается оценка

$$|N(\alpha)| < \frac{1}{n^2} + \sqrt{d} \leqslant 1 + \sqrt{d},$$

что и требовалось доказать.

Используя лемму 2, мы докажем теперь следующую теорему:

Теорема существования. *В каждом вещественном квадратичном поле* K *существует нетривиальная единица* ε.

Доказательство. Если мы примем во внимание произвольность n в лемме 2, то получим, что в K существует бесконечно много целых $\alpha \neq 0$, таких, что

$$|N(\alpha)| < 1 + \sqrt{d}.$$

Для этого нужно только, исходя от одного такого α_1, построенного, например, для $n_1 = 1$, построить второе α_2 с $n_2 > 1/|\alpha_1|$, так что для него будет $|\alpha_2| < 1/n_2 < |\alpha_1|$ и т. д.

Если еще дважды применить рассуждение, аналогичное тому, которое использовалось при доказательстве леммы 2, то мы получим следующее:

1. Среди бесконечного множества различных целых $\alpha \neq 0$ из K, таких, что $|N(\alpha)| < 1 + \sqrt{d}$ существует бесконечно много различных с одной и той же абсолютной величиной нормы

$$|N(\alpha)| = m$$

из ряда натуральных чисел, $< 1 + \sqrt{d}$.

2. Среди бесконечного множества этих последних α существует бесконечно много различных, которые все, однако, сравнимы между собой по $\bmod m$. Для этого заметим, что, согласно изложенной в п. 3 элементарной теории делимости в K, целые числа из K разбиваются по $\bmod m$ на конечное количество, именно, на m^2 классов вычетов, представителями которых являются числа $r + s\omega$, где r, s — целые рациональные числа, пробегающие независимо друг от друга полную систему вычетов по $\bmod m$.

Поэтому наверное существуют натуральное m и два целых α, β из K, не равных между собой даже с точностью до знака,

с выполнением следующих двух требований:

$$|N(\alpha)| = |N(\beta)| = m$$
$$\alpha \equiv \beta \bmod m.$$

Посредством умножения на β' получаем

$$\alpha\beta' \equiv N(\beta) \equiv 0 \bmod m,$$

т. е.

$$\alpha\beta' = m\varepsilon$$

с некоторым целым ε из K, а отсюда делением на $N(\beta)$ получаем

$$\frac{\alpha}{\beta} = \pm\varepsilon.$$

Так как $|N(\alpha)| = |N(\beta)|$, то при этом $|N(\varepsilon)| = 1$. Поэтому ε является единицей, и притом нетривиальной, ввиду того что $\alpha \neq \pm\beta$.

Этим теорема существования доказана.

Нетривиальные единицы поля K могут быть объединены в четверки

$$\varepsilon,\ \varepsilon',\ -\varepsilon,\ -\varepsilon'.$$

Ввиду того что

$$N(\varepsilon) = \varepsilon\varepsilon' = \pm 1,$$

такая четверка имеет вид

$$\varepsilon,\ \varepsilon^{-1},\ -\varepsilon,\ -\varepsilon^{-1} \qquad (\text{если } N(\varepsilon) = 1)$$

или вид

$$\varepsilon,\ -\varepsilon^{-1},\ -\varepsilon,\ \varepsilon^{-1} \qquad (\text{если } N(\varepsilon) = -1).$$

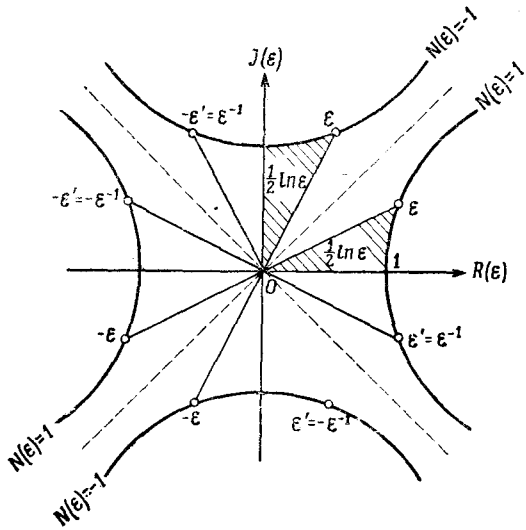
В каждой четверке можно выбрать единицу ε, *нормированную* посредством требования $\varepsilon > 1$. Единицы этой четверки имеют тогда полярные углы

$$\varphi(\varepsilon),\ -\varphi(\varepsilon),\ \varphi(\varepsilon),\ -\varphi(\varepsilon) \quad \text{с} \quad \varphi(\varepsilon) = \ln\varepsilon > 0.$$

Исследуем теперь их положение на паре равносторонних единичных гипербол $N(\varepsilon) = \pm 1$ в K-плоскости (фиг. 13).

Если представить себе ε изменяющимся непрерывно на каждой из гипербол $N(\varepsilon) = \pm 1$ и притом только на полуветвях $\varepsilon > 1$, то как $\varphi(\varepsilon)$, так и $R(\varepsilon)$, $I(\varepsilon)$ будут с ростом ε расти монотонно. Так как $R(\varepsilon) = u/2$, $I(\varepsilon) = v\sqrt{d}/2$, то и u, v будут расти монотонно с ростом ε. Так как, однако, значения u, v ограничены натуральными числами, то в K существует наименьшая единица $\varepsilon_1 > 1$. В полярных координатах она характеризуется тем, что ее полярный угол $\varphi(\varepsilon_1) = \ln\varepsilon_1$ положителен и имеет наименьшее возможное значение, а в декартовых коор-

динатах тем, что ее представление $\varepsilon_1 = \frac{u_1 + v_1\sqrt{d}}{2}$ дает наименьшее решение уравнения Пелля в натуральных числах. Справедливость последнего утверждения также и в отношении сравнения между собой единиц на различных полуветвях гипербол мы легко получим, используя рассматриваемый далее результат VIIIб. Определенная таким образом однозначно нормированная единица ε_1 называется *основной единицей* поля K.



Фиг. 13.

Если ε — какая-нибудь нормированная единица поля K, то существует однозначно определенное натуральное n, такое, что

$$\varepsilon_1^n \leqslant \varepsilon < \varepsilon_1^{n+1}.$$

Так как тогда

$$1 \leqslant \frac{\varepsilon}{\varepsilon_1^n} < \varepsilon_1,$$

то вследствие минимальности ε_1 должно быть $\varepsilon / \varepsilon_1^n = 1$, т. е.

$$\varepsilon = \varepsilon_1^n$$

есть степень основной единицы с натуральным показателем n. Если ε какая-нибудь (не обязательно нормированная) единица поля K, то посредством перехода к нормированной единице $\pm\varepsilon^{\pm 1}$ получается однозначное представление через базис:

$$\varepsilon = (-1)^{\nu}\varepsilon_1^n \left(\begin{array}{l} \nu \bmod 2 \\ n \text{ — целое рациональное} \end{array} \right).$$

Этим доказано

VIIIб. *В вещественном квадратичном поле* $\mathsf{K} = \mathsf{P}(\sqrt{d})$ $(d > 0)$ *группа единиц* E *есть прямое произведение циклической группы второго порядка, состоящей из обеих рациональных единиц* ± 1 *и бесконечной циклической группы.*

Таким образом, существует однозначно определенная единица $\varepsilon_1 > 1$ *– основная единица поля* K, *— такая, что единицы* ε *поля* K *задаются посредством однозначного представления через базис:*

$$\varepsilon = (-1)^{\nu} \varepsilon_1^n \left(\begin{array}{l} \nu \bmod 2 \\ n \text{ — целое рациональное} \end{array} \right).$$

Для нормы основной единицы ε_1 есть две возможности:

$$N(\varepsilon_1) = 1 \quad \text{или} \quad N(\varepsilon_1) = -1.$$

Соответственно этому вещественные квадратичные поля K бывают двух типов. В первом случае для всех единиц ε имеем $N(\varepsilon) = 1$; во втором случае единицы с $N(\varepsilon) = 1$ образуют лишь подгруппу индекса 2 в группе всех единиц E (характеризующуюся в представлении через базис тем, что $n \equiv 0 \bmod 2$). Определение того, к какому из двух типов принадлежит K, сводится к вопросу о том, имеет ли уравнение Пелля со знаком минус

$$\frac{u^2 - dv^2}{4} = -1$$

целое рациональное решение u, v. Ответ на этот вопрос должен принципиально определяться значением дискриминанта d. Однако до сих пор не известно критерия для этого, который был бы одновременно необходимым и достаточным. Один из простых необходимых критериев гласит:

IX. *Для того чтобы* $N(\varepsilon_1) = -1$, *необходимо, чтобы для каждого нечетного простого делителя* p *дискриминанта* d *имело место* $p \equiv 1 \bmod 4$.

Доказательство. Если мы рассмотрим уравнение Пелля со знаком минус как сравнение по $\bmod p$ для некоторого нечетного p, делящего d, то получим $u^2/4 \equiv -1 \bmod p$ и, таким образом, $\left(\frac{-1}{p}\right) = 1$, а потому, согласно первому дополнению к квадратичному закону взаимности, $p \equiv 1 \bmod 4$.

В I, п. 4, § 19 мы познакомимся с достаточным критерием. А сейчас мы только убедимся на двух примерах в том, что уравнение Пелля со знаком минус действительно может быть разрешено:

$$D = 2, \quad d = 8, \quad \varepsilon_1 = 1 + \sqrt{2}, \quad N(\varepsilon_1) = 1^2 - 2 \cdot 1^2 = -1,$$

$$D = 5, \quad d = 5, \quad \varepsilon_1 = \frac{1 + \sqrt{5}}{2}, \quad N(\varepsilon_1) = \frac{1^2 - 5 \cdot 1^2}{4} = -1.$$

В обоих случаях получается, очевидно, наименьшее натуральное решение уравнения Пелля, а потому ε_1 является основной единицей.

Полученные результаты согласуются с высказанными в § 15, п. 5 общими фактами относительно единиц полей алгебраических чисел. Определенные там два арифметических инварианта — *количество w корней из 1* и *регулятор* R — имеют для квадратичных полей следующие значения:

	$d<0$	$d>0$
w	$\begin{cases} 6 \text{ для } d=-3 \\ 4 \text{ для } d=-4 \\ 2 \text{ в остальных случаях} \end{cases}$	2
R	1	$\ln \varepsilon_1$

По отношению к w это следует из VIIIа, б. Что же касается R, то определитель из § 15, п. 5 сводится в мнимом случае $d<0$ к 1, в то время как для вещественного случая $d>0$ действительно получается

$$R=\begin{Vmatrix} \ln|\varepsilon_1| & \ln|\varepsilon_1'| \\ \frac{1}{2} & \frac{1}{2} \end{Vmatrix}=\begin{Vmatrix} \ln \varepsilon_1 & -\ln \varepsilon_1 \\ \frac{1}{2} & \frac{1}{2} \end{Vmatrix}=\ln \varepsilon_1.$$

5. Вычисление основной единицы. Итак, принципиально установлено, что уравнение Пелля

$$\frac{u^2-dv^2}{4}=\pm 1$$

в случае $d>0$ обладает наименьшим натуральным решением u_1, v_1, которое дает тогда основную единицу

$$\varepsilon_1=\frac{u_1+v_1\sqrt{d}}{2}$$

вещественного квадратичного поля $\mathsf{K}=\mathsf{P}(\sqrt{d})$. В каждом отдельном случае решение u_1, v_1 можно найти путем систематических проб, например, проверяя, когда выражение $dv^2\pm 4$ в первый раз обращается в некоторый квадрат u^2. Это может случиться очень быстро, как, например, для уже исследованных нами в п. 4 двух случаев наименьших положительных дискриминантов $d=5$, 8; однако уже для не очень больших d этот путь может оказаться настолько длинным, что нехватит терпения

довести его до конца; так, для $d=124$ ($D=31$), когда, согласно IX, п. 4, нужно рассматривать лишь уравнение со знаком плюс, выражение $4(31v^2+1)$ лишь при $v_1=273$ впервые дает квадрат u^2 именно для $u_1=2\cdot 1520$.

При вычислении было бы полезно по крайней мере знать верхнюю границу для наименьшего решения u_1, v_1 как функцию от d. Такую границу действительно можно указать, как мы увидим в § 18, п. 4. Правда, ее вычисление тоже до некоторой степени сложно. Однако существует совсем простой метод для вычисления основной единицы ε_1, похожий по своему типу на алгоритм Евклида (§ 2, п. 9); он получается с помощью уже упоминавшейся там теории разложения в непрерывную дробь. Мы развьем здесь эту теорию в такой мере и с такой точки, как это будет нам нужно для обоснования этого метода.

А. *Алгебраические основы теории.* Для вещественного числа Θ, которое без ограничения общности мы будем считать >1, *разложение в непрерывную дробь*

$$\Theta = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}} = \{a_1,\ a_2,\ a_3,\ \ldots\} \tag{1}$$

однозначно определяется рекуррентными соотношениями

$$\Theta_n = a_n + \frac{1}{\Theta_{n+1}} \qquad (a_n - \text{целое рациональное},\ \Theta_{n+1} > 1) \tag{2}$$

для $n=1,\ 2,\ 3,\ \ldots$ с исходным равенством $\Theta_1=\Theta$. Если для некоторого n Θ_n окажется целым рациональным, то разложение на этом заканчивается. Рекуррентные соотношения (2) означают, что в качестве a_n берется *целая часть* Θ_n, т. е.

$$a_n \leqslant \Theta_n < a_n + 1,$$

а остаток $\Theta_n - a_n$ представляется затем как обратная величина некоторого вещественного числа Θ_{n+1}. Числа a_n называются *неполными частными*, а Θ_n — *остаточными числами* разложения числа Θ. Все неполные частные являются натуральными числами, все остаточные числа вещественны и >1. Аналогично записи (1) можно записывать и кусок разложения до некоторого остаточного числа:

$$\Theta = a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n + \cfrac{1}{\Theta_{n+1}}}} = \{a_1,\ a_2,\ \ldots,\ a_n;\ \Theta_{n+1}\}. \tag{3}$$

Если при некотором n получаем $\Theta_n = a_n$ — целое рациональное и потому разложение на этом обрывается, то пишут:

$$\Theta = \{a_1,\ a_2,\ \ldots,\ a_n\}. \tag{4}$$

Согласно § 2, п. 9, это имеет место тогда и только тогда, когда разлагаемое число Θ рационально. Так как при этом $\Theta_n = a_n > 1$, то можно, если угодно, формально удлинить разложение на один член с помощью соотношения $a_n = (a_{n-1} - 1) + 1/1$, не нарушая при этом того условия, что все неполные частные должны быть натуральными числами. Таким образом, каждое рациональное число $\Theta > 1$ обладает двумя разложениями в непрерывную дробь (4) с натуральными неполными частными, причем одно разложение имеет четное, а другое — нечетное количество n неполных частных; у одного из них последнее неполное частное $a_n > 1$, а у другого $a_n = 1$.

Посредством введения целочисленных матриц

$$A_n = \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \quad \text{с определителем } |A_n| = -1$$

рекуррентные формулы (2) можно представить в виде

$$\begin{pmatrix} \Theta_n \\ 1 \end{pmatrix} \sim A_n \begin{pmatrix} \Theta_{n+1} \\ 1 \end{pmatrix}, \tag{2'}$$

причем знак пропорциональности $\sim$ между обеими одностолбцовыми матрицами означает, что соответствующие члены у них пропорциональны. Применяя последовательно это соотношение n раз, мы получим в матричной форме связь (3) между Θ и Θ_{n+1}

$$\begin{pmatrix} \Theta_1 \\ 1 \end{pmatrix} \sim P_n \begin{pmatrix} \Theta_{n+1} \\ 1 \end{pmatrix} \tag{3'}$$

с целочисленной матрицей

$$P_n = A_1 \dots A_n \quad \text{с определителем } |P_n| = (-1)^n.$$

Посредством полной индукции теперь сразу вытекают два следующих факта:

а) Матрицы P_n имеют вид

$$P_n = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix},$$

где последовательности p_n, q_n задаются рекуррентными соотношениями

$$\left\{ \begin{array}{l} P_n = a_n p_{n-1} + p_{n-2} \\ q_n = a_n q_{n-1} + q_{n-2} \end{array} \right\} \tag{5}$$

с исходными равенствами

$$\left\{ \begin{array}{ll} p_0 = 1, & p_{-1} = 0 \\ q_0 = 0, & q_{-1} = 1 \end{array} \right\} \text{ или, коротко, } P_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E. \tag{5$_0$}$$

б) Числа p_n, q_n образуют, начиная с p_1, q_2, монотонно возрастающие последовательности, члены которых, начиная с p_0, q_1,

являются натуральными числами. Так как $|P_n| = (-1)^n$, то все время $(p_n, q_n) = 1$ и, таким образом, дроби p_n/q_n несократимы.

Наряду с равенством $|P_n| = (-1)^n$, которое можно записать в виде

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^n}{q_n q_{n-1}} \qquad (n > 1),$$

мы имеем еще, согласно (3′) соотношение

$$\frac{p_n}{q_n} - \Theta = \frac{(-1)^n}{q_n (q_n \Theta_{n+1} + q_{n-1})} \qquad (n \geqslant 1),$$

из которого получаем следующую оценку:

$$\left| \frac{p_n}{q_n} - \Theta \right| < \frac{1}{q_n^2} \qquad (n \geqslant 1). \tag{6}$$

Поэтому последовательность несократимых дробей p_n/q_n сходится к Θ, колеблясь около него; таково фактическое значение формального равенства (1). Оценка (6) заключает в себе, впрочем, апроксимационное высказывание из п. 4, лемма 1 и, кроме того, показывает, что для иррационального Θ существует *бесконечная* последовательность приближений рассмотренного там вида с монотонно возрастающими знаменателями.

В связи с тем что дроби p_n/q_n апроксимируют число Θ, они называются *подходящими дробями*, а p_n и q_n — *подходящими числителями и знаменателями* разложения Θ. Для их вычисления по рекуррентным формулам (5) из получающихся при разложении в непрерывную дробь неполных частных a_n удобно пользоваться следующей схемой, которую надо заполнять справа налево:

...	a_n	...	a_2	a_1	
...	p_n	...	$a_2 a_1 + 1$	a_1	1 0
...	q_n	...	a_2	1	0 1

Б. *Разложение вещественных квадратичных иррациональностей.* Пусть теперь $\Theta = \theta$ — иррациональное число, принадлежащее вещественному квадратичному полю $\mathsf{K} = \mathsf{P}(\sqrt{d})$. Оно удовлетворяет однозначно определенному неприводимому квадратному уравнению

$$a\theta^2 - b\theta - c = 0 \tag{7}$$

с целыми рациональными взаимно простыми коэффициентами a, b, c и $a > 0$. Его дискриминант

$$b^2 + 4ac = m^2 d$$

отличается от дискриминанта d поля K только квадратом некоторого натурального числа m; мы имеем тогда (с неопределенным пока знаком квадратного корня)

$$\theta = \frac{b + m\sqrt{d}}{2a} = \frac{2c}{-b + m\sqrt{d}}, \tag{8}$$

причем $a\theta$, ввиду равенства $(a\theta)^2 - b(a\theta) - ac = 0$ является целым и потому имеет вид (5) п. 3. Число θ называется *принадлежащим дискриминанту* m^2d.

Мы будем называть θ *редуцированным*, если

как и раньше, $\theta > 1$ и, кроме того, $-\frac{1}{\theta'} > 1$.

Из (8) и

$$-\theta' = \frac{-b + m\sqrt{d}}{2a} = \frac{2c}{b + m\sqrt{d}} \tag{8'}$$

выводим, так как $a > 0$, что это имеет место тогда и только тогда, когда $\sqrt{d}$ понимается положительным (до сих пор у нас не было относительно этого никакого условия), и коэффициенты уравнения (7) удовлетворяют неравенствам

$$0 < b < m\sqrt{d}, \quad \frac{-b + m\sqrt{d}}{2} < \left\{ \begin{matrix} a \\ c \end{matrix} \right\} < \frac{b + m\sqrt{d}}{2}. \tag{9}$$

Так как тогда a, b, c – натуральные числа, лежащие между 0 и $m\sqrt{d}$, существует только конечное множество редуцированных θ, принадлежащих данному дискриминанту m^2d.

Теперь докажем следующее высказывание

X. *Вместе с любым иррациональным числом* θ, *принадлежащим дискриминанту* m^2d, *этому же дискриминанту принадлежат и все остатки* θ_n *разложения* θ *в непрерывную дробь.*

Начиная с некоторого места, эти остатки θ_n *редуцированы.*

Доказательство. Ввиду (2), (2') первое утверждение будет доказано, если показать, что вместе с θ к дискриминанту m^2d принадлежит также и число θ^*, определяемое подстановкой вида $\begin{pmatrix} \theta \\ 1 \end{pmatrix} \sim \begin{pmatrix} g & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \theta^* \\ 1 \end{pmatrix}$, т. е. $\theta = g + \frac{1}{\theta^*}$ с целым рациональным g. Но при этой подстановке уравнение (7) для θ переходит в уравнение

$$(ag^2 - bg - c)\,\theta^{*2} - (b - 2ag)\,\theta^* + a = 0$$

для θ^*. Его коэффициенты снова являются целыми рациональными взаимно простыми числами, а для его дискриминанта действительно получается

$$(b - 2ag)^2 - 4a(ag^2 - bg - c) = b^2 + 4ac = m^2d.$$

б) Так как, согласно определению, все остатки $\theta_{n+1} > 1$, то для доказательства второго утверждения нужно еще показать,

что, начиная с некоторого места, будет $-1/\theta'_{n+1} > 1$. Разрешая относительно θ_{n+1} (3′) и переходя к сопряженным, получаем

$$\begin{pmatrix} \theta'_{n+1} \\ 1 \end{pmatrix} \sim P_n^{-1} \begin{pmatrix} \theta' \\ 1 \end{pmatrix}.$$

При этом

$$(-1)^n P_n^{-1} = \begin{pmatrix} q_{n-1} & -p_{n-1} \\ -q_n & p_n \end{pmatrix}.$$

Поэтому

$$-\frac{1}{\theta'_{n+1}} = \frac{q_n\theta' - p_n}{q_{n-1}\theta' - p_{n-1}} = \frac{q_n}{q_{n-1}} - \frac{(-1)^n}{q_{n-1}(q_{n-1}\theta' - p_{n-1})} \quad (n > 1)$$

и, таким образом,

$$-\frac{1}{\theta'_{n+1}} - 1 = \frac{1}{q_{n-1}}\left[(q_n - q_{n-1}) - \frac{(-1)^n}{q_{n-1}\left(\theta' - \frac{p_{n-1}}{q_{n-1}}\right)}\right] \quad (n > 1).$$

В силу того, что

$$\frac{p_{n-1}}{q_{n-1}} \to \theta \neq \theta' \qquad \text{и} \quad q_{n-1} \to \infty,$$

второе слагаемое в квадратных скобках стремится к 0, в то время как первое (за исключением, быть может, $n = 2$) все время $\geqslant 1$. Отсюда получается, что действительно, начиная с некоторого места, $-1/\theta'_{n+1} - 1 > 0$.

Из X мы выведем далее

XI. *Разложение вещественной квадратичной иррациональности $\theta > 1$ в непрерывную дробь, начиная с некоторого места, периодично.*

Если θ редуцировано, то разложение будет чисто периодическим.

Доказательство. Так как остатки θ_{n+1}, начиная с некоторого места, являются редуцированными, принадлежащими тому же дискриминанту m^2d, что и θ, и так как, согласно (9), таких редуцированных чисел существует только конечное множество, то в последовательности остатков рано или поздно должно в первый раз получиться равенство $\theta_{l+k+1} = \theta_{l+1}$ с $l \geqslant 0$ и $k \geqslant 1$. Тогда, согласно (3),

$$\theta = \{a_1, \ldots, a_l; \theta_{l+1}\} = \{a_1, \ldots, a_l; a_{l+1}, \ldots a_{l+k}; \theta_{l+1}\} = \ldots,$$

т. е. мы получаем периодическое разложение

$$\theta = \{a_1, \ldots, a_l; a_{l+1}, \ldots, a_{l+k}\}$$

в обозначениях для периодических десятичных дробей (см. § 4, п. 13).

Если θ редуцировано и θ_{l+1} — первый остаток, совпадающий с некоторым, далее стоящим θ_{l+k+1}, то необходимо должно быть $l=0$. Именно, если бы было $l\geqslant 1$, т. е. существовал бы предшествующий остаток θ_l, то мы могли бы доказать равенство $\theta_l=\theta_{l+k}$, противоречащее минимальному выбору l, следующим образом. Из

$$\theta_l=a_l+\frac{1}{\theta_{l+1}},\quad \theta_{l+k}=a_{l+k}+\frac{1}{\theta_{l+k+1}} \tag{10}$$

следует

$$-\frac{1}{\theta'_{l+1}}=a_l+(-\theta'_l),\quad -\frac{1}{\theta'_{l+k+1}}=a_{l+k}+(-\theta'_{l+k}). \tag{10'}$$

В силу редуцированности θ, в последних равенствах a_l, a_{l+k} являются целыми частями, а $-\theta'_l$, $-\theta'_{l+k}$ — остатками чисел $-1/\theta'_{l+1}$, $-1/\theta'_{l+k+1}$. Так как эти числа совпадают, то то же самое имеет место и для их целых частей и остатков; таким образом, действительно имело бы место $\theta'_l=\theta'_{l+k}$, откуда $\theta_l=\theta_{l+k}$. Поэтому для редуцированного числа θ получается чисто периодическое разложение

$$\theta=\{\overline{a_1,\ \ldots,\ a_k}\}.$$

Утверждение XI допускает обращение

XII. *Каждая периодическая непрерывная дробь*

$$\theta=\{a_1,\ \ldots,\ a_l;\ \overline{a_{l+1},\ \ldots,\ a_{l+k}}\}$$

представляет вещественную квадратичную иррациональность $\theta>1$.

Если непрерывная дробь чисто периодическая ($l=0$), *то* θ *редуцировано.*

Оба высказывания XI и XII вместе называются также *теоремой Эйлера — Лагранжа.*

Доказательство. В силу того что $\theta=\{a_1,\ \ldots,\ a_l;\ \theta_{l+1}\}$ с $\theta_{l+1}=\{\overline{a_{l+1},\ \ldots,\ a_{l+k}}\}$, достаточно показать, что каждая чисто периодическая непрерывная дробь

$$\theta=\{\overline{a_1,\ \ldots,\ a_k}\}$$

представляет редуцированную вещественную квадратическую иррациональность. Из

$$\theta=\{a_1,\ \ldots,\ a_k;\ \theta\}$$

во всяком случае следует, согласно (3'),

$$\begin{pmatrix}\theta\\1\end{pmatrix}\sim P_k\begin{pmatrix}\theta\\1\end{pmatrix} \tag{11}$$

т. е. θ удовлетворяет квадратному уравнению

$$q_k\theta^2-(p_k-q_{k-1})\,\theta-p_{k-1}=0,\quad \theta=\frac{p_k\theta+p_{k-1}}{q_k\theta+q_{k-1}} \tag{12}$$

с целыми рациональными коэффициентами и дискриминантом

$$(p_k - q_{k-1})^2 + 4q_k p_{k-1} > 0.$$

Поэтому θ есть вещественная квадратичная иррациональность. Ясно, что $\theta > 1$. То, что имеет место также $-1/\theta' > 1$ и потому θ, как утверждается, редуцировано, получается из следующего дополнительного предложения

XII. *Если число θ представляется чисто периодической непрерывной дробью*

$$\theta = \{\overline{a_1, \ldots, a_k}\},$$

то число $-1/\theta'$ представляется чисто периодической непрерывной дробью

$$-\frac{1}{\theta'} = \{a_k, \ldots, a_1\}$$

с обратной последовательностью неполных частных в периоде.

Доказательство. Из сказанного выше в связи с (10), (10') следует, что разложение числа $-1/\theta'_{k+1}$ в непрерывную дробь начинается с

$$-\frac{1}{\theta'_{k+1}} = \left\{a_k, \ldots, a_1; -\frac{1}{\theta'_1}\right\}.$$

Так как $\theta_{k+1} = \theta_1 = \theta$, то отсюда и следует наше утверждение.

В. *Применение к вычислению основной единицы.* Получающаяся из чисто периодического разложения в непрерывную дробь пропорциональность (11) для редуцированного числа θ из $\mathsf{K} = \mathsf{P}(\sqrt{d})$ может быть записана в виде пары равенств

$$\varepsilon \begin{pmatrix} \theta \\ 1 \end{pmatrix} = P_k \begin{pmatrix} \theta \\ 1 \end{pmatrix} \tag{13}$$

с некоторым множителем пропорциональности ε из K. Как известно из алгебры, тогда удовлетворяется характеристическое уравнение

$$|\varepsilon E - P_k| = 0,$$

или, подробно,

$$\varepsilon^2 - (p_k + q_{k-1})\varepsilon + (-1)^k = 0.$$

Поэтому ε является единицей поля K с $N(\varepsilon) = (-1)^k$. Согласно (13), она выражается в явной форме

$$\varepsilon = q_k\theta + q_{k-1}. \tag{14}$$

Отсюда видно, что ε удовлетворяет нормирующему условию $\varepsilon > 1$.

Чтобы получить ε в представлении (5) п. 3 через $1, \sqrt{d}$, сравним получающееся для θ из разложения в непрерывную дробь

квадратное уравнение (12) с исходным уравнением (7), коэффициенты которого взаимно просты. Обозначим

$$(q_k,\ p_k - q_{k-1},\ p_{k-1}) = v \tag{15_1}$$

и

$$p_k + q_{k-1} = u. \tag{15_2}$$

Тогда сравнение коэффициентов наших уравнений дает

$$q_k = av,\ p_k - q_{k-1} = bv,\ p_{k-1} = cv \tag{16}$$

и представление (14) для числа ε посредством использования представления (8) для θ приводится к виду

$$\varepsilon = \frac{u + vm\sqrt{d}}{2}. \tag{17}$$

Полученная единица ε обладает тем свойством, что коэффициент при $\sqrt{d}$ делится на натуральное число m. Вообще, целые числа из K специального вида:

$$\alpha = \frac{a + bm\sqrt{d}}{2} \quad \begin{pmatrix} a,\ b \text{ целые рациональные} \\ a \equiv bmd \bmod 2 \end{pmatrix} \tag{18}$$

характеризуются также тем, что они сравнимы по $\bmod m$ с некоторым целым рациональным числом r:

$$\alpha \equiv r \bmod m. \tag{19}$$

Это следует из того, что коэффициент при $\sqrt{d}$ в положенном здесь в основу представлении через 1, $\sqrt{d}$ одновременно является также коэффициентом при ω в представлении через целочисленный базис 1, ω поля K. При этом последнем представлении $\alpha = r + s\omega$ условие $s \equiv 0 \bmod m$, очевидно, равносильно $\alpha \equiv r \bmod m$. Из характеристики (19) чисел α из (18) следует, что эти числа образуют область целостности $\mathfrak{l}_m$, являющуюся подобластью области целостности $\mathfrak{l}$ целых чисел поля K. Коротко называют $\mathfrak{l}_m$ *числовым кольцом по* $\bmod m$ поля K или также *кольцом дискриминанта* m^2d. Числа 1, $m\omega$ образуют базис $\mathfrak{l}_m$; однако в большинстве случаев числа из $\mathfrak{l}_m$ удобнее представлять не через 1, $m\omega$, а в аналогичной (5) п. 3 форме (18).

Так как вместе с единицей ε к $\mathfrak{l}_m$ принадлежит также обратная к ней величина $\varepsilon^{-1} = (-1)^k \varepsilon'$, ε не является делителем нуля в кольце классов вычетов по $\bmod m$ и потому принадлежит к мультипликативной группе тех чисел α из K, которые сравнимы по $\bmod m$ с некоторым, взаимно простым с m целым рациональным числом r. Образованные из этих чисел α классы вычетов по $\bmod m$ называются *рациональными классами вычетов по* $\bmod m$, *взаимно простыми с модулем, в области целостности* $\mathfrak{l}$. Они образуют изоморфную группе классов вычетов по $\bmod m$,

взаимно простых с модулем, области целостности Γ подгруппу $\mathfrak{g}_m$ группы $\mathfrak{G}_m$ *всех взаимно простых с модулем классов вычетов по* $\bmod m$ *в области целостности* $\mathfrak{l}$, которая состоит соответственно из *всех* неделителей нуля α в кольце классов вычетов по $\bmod m$ области $\mathfrak{l}$. Группа $\mathfrak{G}_m$ классов вычетов, взаимно простых с модулем, имеет конечный порядок $\Phi(m)$; мы определим его в XIII, п. 4, § 17. Подгруппа $\mathfrak{g}_m$ имеет определенный в § 4, п. 8 порядок $\varphi(m)$. Тогда фактор-группа $\mathfrak{G}_m/\mathfrak{g}_m$ имеет порядок $\Phi(m)/\varphi(m)$. Так как основная единица ε_1 поля K не является делителем нуля в кольце классов вычетов по $\bmod m$ и потому лежит в некотором классе вычетов из $\mathfrak{G}_m$, ее степень $\varepsilon_1^{\Phi(m)/\varphi(m)}$ лежит в некотором классе вычетов из $\mathfrak{g}_m$. Таким образом, существует такой однозначно определенный наименьший натуральный показатель g_m, входящий в $\Phi(m)/\varphi(m)$, что $\varepsilon_1^{g_m}$ лежит в некотором классе вычетов из $\mathfrak{G}_m$, т. е. принадлежит к $\mathfrak{l}_m$. Так, определенная степень

$$\varepsilon_1^{g_m} = \frac{u_1 + v_1 m\sqrt{d}}{2}$$

называется *основной единицей числового кольца по* $\bmod m$ *поля* K или также *основной единицей дискриминанта* m^2d. Через эту единицу представляются все остальные единицы из $\mathfrak{l}_m$, подобно тому как через ε_1, согласно VIIIб, представляются все единицы из $\mathfrak{l}$. Коэффициенты u_1, v_1 являются наименьшим натуральным решением принадлежащего дискриминанту m^2d уравнения Пелля

$$\frac{u^2 - v^2m^2d}{4} = \pm 1.$$

Полученный в (15), (17) результат может быть окончательно сформулирован так:

XIII. *Если* θ *есть принадлежащее дискриминанту* m^2d *редуцированное число из* $\mathsf{K} = \mathsf{P}(\sqrt{d})$, *то чисто периодическое разложение в непрерывную дробь*

$$\theta = \{\overline{a_1, \ldots, a_k}\}$$

определяет единицу

$$\varepsilon = \frac{u + vm\sqrt{d}}{2}$$

числового кольца по $\bmod m$ *поля* K; v, u *определяются по формулам*

$$v = (q_k,\ p_k - q_{k-1},\ p_{k-1}),$$
$$u = p_k + q_{k-1},$$

где p_{k-1}/q_{k-1}, p_k/q_k *являются последними подходящими дробями перед повторением периода. Эта единица обладает свойствами* $\varepsilon > 1$ *и* $N(\varepsilon) = (-1)^k$.

Определение ε *может быть также выражено в форме*

$$\varepsilon\begin{pmatrix}\theta\\1\end{pmatrix}=P_k\begin{pmatrix}\theta\\1\end{pmatrix}\quad\text{с}\quad P_k=\begin{pmatrix}p_k & p_{k-1}\\ q_k & q_{k-1}\end{pmatrix}$$

или

$$\varepsilon=q_k\theta+q_{k-1}.$$

Теперь мы докажем

XIII′. *Если в* XIII *мы имеем дело с простейшим периодом, то* $\varepsilon=\varepsilon_1^{gm}$ *есть основная единица числового кольца по* $\bmod p$ *поля* K.

При этом *простейший период* определяется, аналогично тому как в § 4, п. 13 для разложений в m-ичную дробь, посредством выбора наименьшей длины периода k.

Доказательство. Если применить использованный при выводе XIII метод к отрезку нашего разложения, состоящему из h периодов $a_1, \ldots, a_h$, то матрица $P_k=A_1\ldots A_k$ заменится степенью P_k^h. Тогда вместо множителя пропорциональности ε из (13) получится степень ε^h. Поэтому наше утверждение будет доказано, если мы покажем, что *каждая* единица $\varepsilon>1$ числового кольца по $\bmod m$ поля K (т. е. *каждая* степень ε_1^{gmh} с натуральным h) встречается для некоторого отрезка разложения числа θ, состоящего из нескольких периодов, в качестве множителя пропорциональности в соответствующем соотношении (13).

Поэтому пусть теперь

$$\varepsilon=\frac{u+vm\sqrt{d}}{2}$$

есть любая единица числового кольца по $\bmod m$ поля K, обладающая свойством $\varepsilon>1$, т. е. $u, v\geqslant 1$. Тогда аналогично формулам (15_2) (16) образуем из ее коэффициентов u, v и из коэффициентов a, b, c уравнения (7) для θ числа

$$\left.\begin{array}{ll} p=\dfrac{u+bv}{2}, & p'=cv\\ q=av, & q'=\dfrac{u-bv}{2}\end{array}\right\}, \tag{20}$$

которые будут целыми рациональными, в силу условий целостности $u\equiv vmd$, $b\equiv md \bmod 2$ для ε и $a\theta$. Так как q, $p-q'$, p' пропорциональны a, b, c, то θ удовлетворяет аналогичному (12) квадратному уравнению

$$q\theta^2-(p-q')\,\theta-p'=0,\quad \theta=\frac{p\theta+p'}{q\theta+q'}$$

или, в аналогичной (11) записи,

$$\begin{pmatrix}\theta\\1\end{pmatrix}\sim P\begin{pmatrix}\theta\\1\end{pmatrix}\quad\text{с}\quad P=\begin{pmatrix}p & p'\\ q & q'\end{pmatrix}. \tag{21}$$

При этом

$$|P| = \frac{u^2 - (b^2 + 4ac)v^2}{4} = \frac{u^2 - v^2 m^2 d}{4} = N(\varepsilon).$$

Из условий редуцированности (9), которые мы здесь используем в форме

$$b < m\sqrt{d}, \quad 2a - b < m\sqrt{d} < 2a + b,$$

и из предположения $\varepsilon > 1$ далее следуют неравенства

$$q' = \frac{u - bv}{2} > \frac{u - vm\sqrt{d}}{2} = \varepsilon' = \frac{N(\varepsilon)}{\varepsilon} > \\ > \begin{Bmatrix} 0 & \text{для} & N(\varepsilon) = 1 \\ -1 & \text{для} & N(\varepsilon) = -1 \end{Bmatrix},$$

$$q - q' = \frac{-u + (2a + b)v}{2} > \frac{-u + vm\sqrt{d}}{2} = -\varepsilon' = -\frac{N(\varepsilon)}{\varepsilon} > \\ > \begin{Bmatrix} -1 & \text{для} & N(\varepsilon) = 1 \\ 0 & \text{для} & N(\varepsilon) = -1 \end{Bmatrix},$$

$$p - q = \frac{u - (2a - b)v}{2} > \frac{u - vm\sqrt{d}}{2} = \varepsilon' = \frac{N(\varepsilon)}{\varepsilon} > \\ > \begin{Bmatrix} 0 & \text{для} & N(\varepsilon) = 1 \\ -1 & \text{для} & N(\varepsilon) = -1 \end{Bmatrix},$$

откуда

$$0 < q' \leqslant q, \quad \frac{p}{q} > 1 \quad \text{для } N(\varepsilon) = 1$$

$$0 \leqslant q' < q, \quad \frac{p}{q} \geqslant 1 \quad \text{для } N(\varepsilon) = -1.$$

Пусть теперь, в соответствии с установленным ранее,

$$\frac{p}{q} = \{a_1, \ldots, a_k\}$$

есть то однозначно определенное разложение несократимой дроби $p/q \geqslant 1$ в непрерывную дробь, для которого количество k неполных частных удовлетворяет условию

$$N(\varepsilon) = |P| = (-1)^k.$$

Тогда для двух последних подходящих дробей p_k/q_k, p_{k-1}/q_{k-1} этого разложения имеет место

$$\left.\begin{matrix} p_k = p, & p_{k-1} = p' \\ q_k = q, & q_{k-1} = q' \end{matrix}\right\} \quad \text{и, таким образом, } P_k = P. \tag{22}$$

Относительно последней подходящей дроби это очевидно. Для предпоследней заметим, что она *однозначно* определяется из послед-

ней посредством условия

$$|P_k| = p_k q_{k-1} - q_k p_{k-1} = (-1)^k$$

для определителя и неравенств

$$0 \leqslant q_{k-1} \leqslant q_k,$$

причем в первом неравенстве равенство имеет место только для $k=1$, а во втором, — быть может, только для $k=2$; действительно, этими условиями, с одной стороны, однозначно определяются классы вычетов $q_{k-1} \bmod q_k$, а с другой стороны, — их представители q_{k-1}. Но в силу выбора k, как уже показано, этим условиям удовлетворяют $p_{k-1}=p'$ и $q_{k-1}=q'$.

Согласно (22), соотношение (21) может быть также записано в виде

$$\begin{pmatrix} \theta \\ 1 \end{pmatrix} \sim P_k \begin{pmatrix} \theta \\ 1 \end{pmatrix} \tag{23}$$

или также

$$\theta = \{a_1, \ldots, a_k; \theta\};$$

тогда оно означает, что $a_1, \ldots, a_k$ являются также неполными частными некоторого (не обязательно простейшего) периода разложения в непрерывную дробь числа θ. Соотношения же (20) переходят, на основании (22), в формулы (15), (16), определяющие ε по разложению в непрерывную дробь числа θ. Поэтому ε действительно является множителем пропорциональности в (23), что и требовалось доказать.

Если мы захотим, пользуясь правилом из XIII, вычислить основную единицу ε_1 поля K, то надо будет исходить из редуцированного числа θ, принадлежащего самому дискриминанту d поля K; в этом случае будет $m=1$. Дискриминанту d принадлежит базисное число

$$\omega = \left\{ \begin{array}{ll} \dfrac{1+\sqrt{D}}{2} = \dfrac{1+\sqrt{d}}{2} & \text{для } D \equiv 1 \bmod 4,\ d = D \\ \sqrt{D} = \dfrac{0+\sqrt{d}}{2} & \text{для } D \equiv 2,\ 3 \bmod 4,\ d = 4D \end{array} \right\}.$$

Тогда, согласно X, это же будет и для всех остаточных чисел $\omega_1 = \omega$, ω_2, ω_3, ... разложения числа ω в непрерывную дробь, и, наконец, среди них обязательно встретится редуцированное. Это последнее высказывание можно уточнить следующим образом:

XIV. *Само базисное число $\omega = \omega_1$ является редуцированным только для наименьшего положительного дискриминанта $d=5$. Однако уже следующий за ним остаток*

$$\omega^* = \omega_2 = \frac{1}{\omega - \omega'}$$

всегда является редуцированным, здесь w *— целая часть числа* ω. *Таким образом, с помощью этого остатка* ω^* *можно по правилу из* XIII *получить основную единицу поля* K.

Доказательство. Во всяком случае, $\omega, \omega^* > 1$. Поэтому остается рассмотреть только $-1/\omega'$, $-1/\omega^{*\prime}$. Мы имеем

$$-\frac{1}{\omega'} = \left\{ \begin{array}{ll} \dfrac{2}{-1+\sqrt{D}} < 1 & \text{для } D > 9 \\ \dfrac{1}{\sqrt{D}} < 1 & \text{для } D > 1 \end{array} \right\},$$

так что ω действительно редуцировано только в частном случае $D = d = 5$. Напротив, всегда имеет место

$$-\frac{1}{\omega^{*\prime}} = w - \omega' = w - \omega - \left\{ \begin{array}{c} 1 \\ 0 \end{array} \right\} > 2w - 1 \geqslant 1,$$

и, таким образом, всегда ω^* редуцировано, что и утверждалось.

Между прочим, частный случай $d = 5$ приводит к простейшему разложению в непрерывную дробь

$$\frac{1+\sqrt{5}}{2} = \{\overline{1}\}$$

с одночленным периодом 1. Подходящие числители и знаменатели удовлетворяют здесь рекуррентным формулам

$$p_n = p_{n-1} + p_{n-2}$$
$$q_n = q_{n-1} + q_{n-2}.$$

Наше схематическое расположение в этом случае имеет вид:

. . .	1	1	1	1	1	1		
. . .	13	8	5	3	2	1	1	0
. . .	8	5	3	2	1	1	0	1

Получающаяся в обеих строчках, со сдвигом $p_{k-1} = q_k$, последовательность чисел называется рядом Фибоначчи. Из нашего правила в XIII для образования последовательности степеней

$$\varepsilon_1^k = \frac{u_k + v_k\sqrt{5}}{2}$$

основной единицы $\varepsilon_1 = (1+\sqrt{5})/2$ получается следующий закон для образования этих степеней:

$$u_k = p_k + q_{k-1} = q_{k+1} + q_{k-1},$$
$$v_k = (q_k,\ p_k - q_{k-1},\ p_{k-1}) = (q_k,\ q_k,\ q_k) = q_k,$$

где q_k — числа ряда Фибоначчи с начальными значениями $q_1 = 1$, $q_0 = 1$.

В качестве примера мы вычислим основную единицу ε_1 в уже упомянутом выше случае $D = 31$ ($d = 124$). Вообще, для получения разложения числа $\omega = \sqrt{D}$ в непрерывную дробь нам отнюдь не обязательно знать разложение D в десятичную дробь; нам вполне достаточно знания целой части w числа $\sqrt{D}$. В нашем случае $5^2 < 31 < 6^2$ и потому $w = 5$. Тогда разложение получается следующим образом:

$$\sqrt{31} = 5 + (\sqrt{31} - 5) = 5 + \frac{6}{\sqrt{31} + 5}$$

$$\frac{\sqrt{31} + 5}{6} = 1 + \frac{\sqrt{31} - 1}{6} = 1 + \frac{5}{\sqrt{31} + 1}$$

$$\frac{\sqrt{31} + 1}{5} = 1 + \frac{\sqrt{31} - 4}{5} = 1 + \frac{3}{\sqrt{31} + 4}$$

$$\frac{\sqrt{31} + 4}{3} = 3 + \frac{\sqrt{31} - 5}{3} = 3 + \frac{2}{\sqrt{31} + 5}$$

$$\frac{\sqrt{31} + 5}{2} \pm 5 + \frac{\sqrt{31} - 5}{2} = 5 + \frac{3}{\sqrt{31} + 5}$$

$$\frac{\sqrt{31} + 5}{3} = 3 + \frac{\sqrt{31} - 4}{3} = 3 + \frac{5}{\sqrt{31} + 4}$$

$$\frac{\sqrt{31} + 4}{5} = 1 + \frac{\sqrt{31} - 1}{5} = 1 + \frac{6}{\sqrt{31} + 1}$$

$$\frac{\sqrt{31} + 1}{6} = 1 + \frac{\sqrt{31} - 5}{6} = 1 + \frac{1}{\sqrt{31} + 5}$$

$$\sqrt{31} + 5 = 10 + (\sqrt{31} - 5) = 10 + \frac{6}{\sqrt{31} + 5}$$

Поэтому мы имеем

$$\omega = \sqrt{31} = \{5;\ \overline{1,\ 1,\ 3,\ 5,\ 3,\ 1,\ 1,\ 10}\}$$

$$\omega^* = \frac{\sqrt{31} + 5}{6} = \{\overline{1,\ 1,\ 3,\ 5,\ 3,\ 1,\ 1,\ 10}\}.$$

Схема для подходящих числителей и знаменателей числа ω^* выглядит так:

10	1	1	3	5	3	1	1		
2885	273	155	118	37	7	2	1	1	0
1638	155	88	67	21	4	1	1	0	1

и правило в XIII дает

$$u_1 = 2885 + 155 = 3040 = 2 \cdot 1520,$$
$$v_1 = (1638,\ 2730,\ 273) = 273,$$

откуда

$$\varepsilon_1 = 1520 + 273\sqrt{31}.$$

На этом примере читатель может убедиться в превосходстве метода непрерывных дробей над описанным сначала методом последовательных проб.

В связи с критерием IX, п. 4 мы отметим еще следующее правило, вытекающее из фигурирующей в доказательстве XIII, XIII′ общей формулы $N(\varepsilon) = |P_k| = (-1)^k$ для определителя:

XV. *Альтернатива $N(\varepsilon_1) = \pm 1$ для нормы основной единицы ε_1 поля $\mathsf{K} = P(\sqrt{d})$ равносильна альтернативе, имеет ли разложение базисного числа ω (или, более обще, какого-нибудь числа, принадлежащего дискриминанту d) в непрерывную дробь четную или нечетную длину k простейшего периода.*

Заметим еще, что, как показывает доказательство XIII и XIII′, при построении всех единиц $\varepsilon > 1$ числового кольца по $\bmod m$ поля K, а в специальном случае $m = 1$ — всех единиц $\varepsilon > 1$ поля k (и тем самым всех вообще единиц $\pm\varepsilon^{\pm 1}$ поля K) нет нужды считать известной теорему существования, доказанную в п. 4 другим (более коротким) способом, и непосредственно следующую за ней теорему VIIIб о представлении единиц через основную единицу. Напротив, теория непрерывных дробей дает новое, правда, более длинное, но зато менее искусственное доказательство этих основных теорем о единицах вещественных квадратичных полей.

Г. *Разложение в непрерывную дробь чистых квадратных корней.* В рассмотренном выше примере $\omega = \sqrt{31}$ $k - 1$ первых членов периода 1, 1, 3, 5, 3, 1, 1 образуют последовательность, симметричную относительно своей середины, а последний член 10 равен удвоенному числу 5, стоящему перед периодом. Обе эти особенности оказываются имеющими место для разложений в непрерывную дробь всех чисто квадратных корней, > 1, и притом они характеризуют этот случай:

XVI. *Если $\alpha = \sqrt{a}$ с рациональным числом $a > 1$, не являющимся квадратом, то разложение числа α в непрерывную дробь имеет следующий вид со свойством симметрии:*

$$\alpha = \{g;\ \overline{a_1,\ \ldots,\ a_{k-1},\ 2g}\} = \{g;\ \overline{a_{k-1},\ \ldots,\ a_1,\ 2g}\},$$

и обратно.

Доказательство. Пусть $\alpha = \sqrt{a}$ с рациональным $a > 1$, не являющимся квадратом, и пусть g есть целая часть числа α.

Тогда остаток

$$\theta = \frac{1}{\alpha - g} > 1$$

и, вследствие $\alpha' = -\alpha$, также и

$$-\frac{1}{\theta'} = \alpha + g > 2g > 1.$$

Поэтому θ редуцировано. Тогда согласно XI и XII′,

$$\theta = \{\overline{a_1, \ldots, a_k}\}, \qquad -\frac{1}{\theta'} = \{\overline{a_k, \ldots, a_1}\}.$$

Так как $-1/\theta'$ имеет целую часть $2g$, то прежде всего следует $a_k = 2g$. Если мы теперь из каждого из этих разложений восстановим разложение самого α, для чего в первом случае нужно добавить впереди неполное частное g, а во втором случае — уменьшить первое неполное частное $a_k = 2g$ до g (период тогда снова нужно пополнить присоединением $a_k = 2g$), то и получится доказываемое равенство

$$\alpha = \{g; \overline{a_1, \ldots, a_{k-1}, 2g}\} = \{g; \overline{a_{k-1}, \ldots, a_1, 2g}\}.$$

б) Пусть, обратно, α разлагается в непрерывную дробь указанного вида со свойством симметрии. Тогда для остатка получается

$$\frac{1}{\alpha - g} = \{\overline{a_1, \ldots, a_{k-1}, 2g}\},$$

откуда, согласно XII′,

$$-\alpha' + g = \{\overline{2g, a_{k-1}, \ldots, a_1}\},$$

и потому

$$-\alpha' = \{g; \overline{a_{k-1}, \ldots, a_1, 2g}\} = \alpha.$$

Отсюда следует, что $\alpha'^2 = \alpha^2 = a$ — рационально и, кроме того, $a > 1$, если, как мы все время делали раньше, ограничиться непрерывными дробями с первым неполным частным $g \geqslant 1$.

Рассмотрим теперь специально разложение в непрерывную дробь

$$\sqrt{D} = \{g; \overline{a_1, \ldots, a_{k-1}, 2g}\}.$$

Соответствующая чисто периодическая непрерывная дробь

$$\theta = \frac{1}{\sqrt{D} - g} = \{\overline{a_1, a_2, \ldots, a_{k-1}, 2g}\}$$

определяет, в силу пары уравнений

$$\varepsilon \begin{pmatrix} \theta \\ 1 \end{pmatrix} = P_k \begin{pmatrix} \theta \\ 1 \end{pmatrix} = P_{k-1} \begin{pmatrix} 2g & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \theta \\ 1 \end{pmatrix},$$

единицу ε поля K, а именно, согласно XIII, XIII′, принадлежащую дискриминанту $4D$ основную единицу; ее связью с основной единицей ε_1 поля K мы займемся позднее.

Сначала заметим, что для конструкции представления числа ε через базис могут быть использованы, вместо подходящих дробей p_n/q_n числа θ, также и подходящие дроби p_n^*/q_n^* самого $\sqrt{D}$. Пусть матрицы P_n^* для p_n^*/q_n^* определены так же, как матрицы P_n для p_n/q_n. Вследствие того, что $P_1^* = \begin{pmatrix} g & 1 \\ 1 & 0 \end{pmatrix}$, мы имеем $P_n^* = \begin{pmatrix} g & 1 \\ 1 & 0 \end{pmatrix} P_{n-1}$. Принимая во внимание

$$\begin{pmatrix} \sqrt{D} \\ 1 \end{pmatrix} = \begin{pmatrix} g & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \theta^{-1} \end{pmatrix} = \frac{1}{\theta} \begin{pmatrix} g & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \theta \\ 1 \end{pmatrix}$$

и

$$\begin{pmatrix} 1 \\ \theta^{-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -g \end{pmatrix} \begin{pmatrix} \sqrt{D} \\ 1 \end{pmatrix},$$

мы можем произвести следующие преобразования:

$$\varepsilon \begin{pmatrix} \sqrt{D} \\ 1 \end{pmatrix} = \frac{\varepsilon}{\theta} \begin{pmatrix} g & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \theta \\ 1 \end{pmatrix} = \frac{1}{\theta} \begin{pmatrix} g & 1 \\ 1 & 0 \end{pmatrix} P_{k-1} \begin{pmatrix} 2g & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \theta \\ 1 \end{pmatrix} =$$

$$= P_k^* \begin{pmatrix} 2g & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \theta^{-1} \end{pmatrix} = P_k^* \begin{pmatrix} 2g & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -g \end{pmatrix} \begin{pmatrix} \sqrt{D} \\ 1 \end{pmatrix} =$$

$$= P_k^* \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \sqrt{D} \\ 1 \end{pmatrix} = \begin{pmatrix} p_k^* & gp_k^* + p_{k-1}^* \\ q_k^* & gq_k^* + q_{k-1}^* \end{pmatrix} \begin{pmatrix} \sqrt{D} \\ 1 \end{pmatrix}.$$

Поэтому имеет место пара уравнений

$$\varepsilon\sqrt{D} = p_k^*\sqrt{D} + (gp_k^* + p_{k-1}^*),$$
$$\varepsilon = q_k^*\sqrt{D} + (gq_k^* + q_{k-1}^*).$$

Умножение второго уравнения на $\sqrt{D}$ и сравнение с первым дает

$$gq_k^* + q_{k-1}^* = p_k^*.$$

Поэтому

$$\varepsilon = p_k^* + q_k^*\sqrt{D}.$$

Коэффициенты p_k^* и q_k^* являются числителем и знаменателем предпоследней подходящей дроби разложения числа $\sqrt{D}$ перед повторением простейшего периода.

Как уже сказано, определенная таким образом единица ε является основной единицей дискриминанта $4D$.

В случае $D \equiv 2, 3 \bmod 4$, когда $d = 4D$, $\varepsilon = \varepsilon_1$ является основной единицей самого поля K.

В случае же $D \equiv 1 \bmod 4$, когда $d = D$, $\varepsilon = \varepsilon_2$ является основной единицей только числового кольца по $\bmod 2$ поля K. Как показано выше, $\varepsilon_2 = \varepsilon_1^{g_2}$ с некоторым натуральным делителем g_2 числа $\Phi(2)/\varphi(2) = \Phi(2)$, где $\Phi(2)$ есть количество классов вычетов по $\bmod 2$, взаимно простых с модулем, в области целостности I, т. е. количество тех из четырех классов вычетов 0, 1, ω, $1+\omega \bmod 2$, которые не являются делителями нуля. Как мы увидим в Ia, п. 1, § 17, в случае $D \equiv 1 \bmod 8$ рациональный класс вычетов $1 \bmod 2$ является единственным, который не есть делитель нуля, в то время как в случае $D \equiv 5 \bmod 8$ не являются делителями нуля также и оба нерациональных класса вычетов ω, $1+\omega \bmod 2$. Таким образом, $\Phi(2) = 1$ или 3, в зависимости от того, $D \equiv 1$ или $\equiv 5 \bmod 8$, и в соответствии с этим

$$\varepsilon = \varepsilon_2 = \varepsilon_1 \qquad \text{для } D \equiv 1 \bmod 8,$$
$$\varepsilon = \varepsilon_2 = \varepsilon_1 \text{ или } \varepsilon_1^3 \qquad \text{для } D \equiv 5 \bmod 8.$$

Согласно всему сказанному, мы получаем следующий результат:

XVII. *Предпоследняя перед повторением простейшего периода подходящая дробь p_k^*/q_k^* разложения в непрерывную дробь числа $\sqrt{D}$ определяет единицу*

$$\varepsilon = p_k^* + q_k^* \sqrt{D}$$

поля $\mathsf{K} = \mathsf{P}\sqrt{D}$. Она является

для $D \equiv 2, 3 \bmod 4$ и $D \equiv 1 \bmod 8$ основной единицей ε_1 поля K, для $D \equiv 5 \bmod 8$ основной единицей $\varepsilon_2 = \varepsilon_1$ или ε_1^3 числового кольца по $\bmod 2$ поля K.

Для $D = 31$ мы ранее нашли

$$\sqrt{31} = \{5; \overline{1, 1, 3, 5, 3, 1, 1, 10}\}.$$

Схема подходящих дробей для самого $\sqrt{31}$ имеет вид:

1	1	3	5	3	1	1	5		
1520	863	657	206	39	11	6	5	1	0
273	155	118	37	7	2	1	1	0	1

Таким образом,

$$\varepsilon_1 = 1520 + 273\sqrt{31},$$

как мы уже нашли это выше несколько иным способом.

Для случая $D \equiv 5 \bmod 8$ уже $D = 5$ дает пример того, что $\varepsilon_2 = \varepsilon_1^3$. Показателем степени 3 обусловлен в этом случае также и тот факт, что в ряде Фибоначчи первым четным членом является именно третий. То, что может быть и $\varepsilon_2 = \varepsilon_1$, показывает пример $D = 37$, который читатель может исследовать в качестве упражнения посредством разложения в непрерывную дробь чисел $\sqrt{37}$ и $(1+\sqrt{37})/2$. В последнем случае уравнение Пелля

$$\frac{u^2 - Dv^2}{4} = \pm 1$$

имеет поэтому только решения $u \equiv v \equiv 0 \bmod 2$.

6. Квадратичные поля с однозначным разложением на простые множители. В элементарной теории делимости, которая, как было сказано в конце п. 3, вводится посредством определения области целостности $\mathfrak{l}$ целых чисел поля K, наряду с названными там понятиями делимости, единицы, ассоциированности, устанавливается также понятие *простого числа поля* K:

Число π из $\mathfrak{l}$ называется простым числом поля K, если оно не является единицей и обладает только тривиальными делителями, а именно, ассоциированными с ним числами и единицами.

В отличие от того, что говорилось в конце п. 3 относительно остальных перечисленных выше понятий, простое число p поля P, рассматриваемое как число из K, не обязательно является простым числом поля K, хотя простое число p поля K, принадлежащее к P, необходимо является (положительным или отрицательным) простым числом поля P. Именно, вполне может быть, что хотя p обладает в P только тривиальными делителями, но в K может иметь также и нетривиальные делители. Поэтому впредь мы должны, говоря о простых числах — в отличие от целых чисел,—добавлять, имеется ли в виду поле P или поле K.

Следующие примеры показывают, что для простых чисел p поля P действительно могут иметь место обе названные возможности. В поле $\mathsf{K} = \mathsf{P}(\sqrt{-1}) = \mathsf{P}(i)$ имеет место:

2 не является простым числом; действительно, $2 = (1-i)(1+i)$

$$\text{и } 1 \mp i \neq \pm 1, \pm i.$$

3 есть простое число; действительно, из того, что $\alpha \mid 3$, $\alpha = a + bi$ целое, $\alpha \neq 1, 3$, следует $N(\alpha) \mid 3^2$, $N(\alpha) \neq 1, 3^2$ и, таким образом, $N(\alpha) = a^2 + b^2 = 3$, что при целых рациональных a, b невозможно. В последнем примере мы использовали правило для норм из п. 3, а также вытекающий из него критерий VI, п. 4 для единиц (последний как для α, так и для дополнительного делителя!).

Возникает вопрос, переносится ли с поля рациональных чисел P на квадратичные поля K основная теорема элементарной

теории чисел (см. § 1, п. 4) об однозначном разложении на простые множители, т. е. существует ли для каждого не являющегося единицей целого числа $\alpha \neq 0$ из K разложение

$$\alpha = \pi_1 \dots \pi_r$$

в произведение конечного множества простых чисел $\pi_1, \dots, \pi_r$ поля K, и если существует, то однозначно ли оно с точностью до порядка расположения сомножителей и их выбора среди ассоциированных с ними.

Тот факт, что по крайней мере одно такое разложение существует, является простым следствием правила для норм из п. 3. Действительно, в силу этого правила, на поле K можно перенести рассуждения из § 1, п. 3 (лемма) и § 1, п. 4 (доказательство существования), если обычную абсолютную величину рациональных чисел заменить абсолютной величиной нормы чисел из K. Заведомо существующий для $\alpha \neq 0$, $\alpha \not\equiv 1$, т. е. для $N(\alpha) \neq 0$, $|N(\alpha)| \neq 1$, целый делитель π числа α с наименьшей абсолютной величиной нормы $|N(\pi)| > 1$ является простым числом поля K, и последовательное отщепление от α простых чисел должно через конечное число шагов привести к оставшемуся множителю с абсолютной величиной нормы 1, т. е. к единице поля K (которая может быть тогда включена в последний простой сомножитель, ибо мы не имеем здесь аналога положительному нормированию простых рациональных чисел).

Одним из важнейших математических открытий XIX века является то, что разложение на простые множители в квадратичных полях — и, более обще, в любых конечных алгебраических расширениях поля рациональных чисел — не обязательно является однозначным. Мы подтвердим это четырьмя примерами.

В поле $\mathsf{P}(\sqrt{-6})$ имеет место $6 = 2 \cdot 3 = \sqrt{-6} \cdot -\sqrt{-6}$,

в поле $\mathsf{P}(\sqrt{-5})$ имеет место $21 = 3 \cdot 7 = (4 + \sqrt{-5})(4 - \sqrt{-5})$,

в поле $\mathsf{P}(\sqrt{10})$ имеет место $10 = 2 \cdot 5 = \sqrt{10} \cdot \sqrt{10}$,

в поле $\mathsf{P}(\sqrt{82})$ имеет место $-713 = -23 \cdot 21 =$

$$= (5 + 3\sqrt{82})(5 - 3\sqrt{82}).$$

Каждый раз получаются два существенно различных разложения на простые множители. То, что множители первого и второго разложения в каждом случае не ассоциированы друг с другом, ясно из того, что различны их нормы (или даже уже из того, что отношения их не являются целыми). То, что множители являются в рассматриваемых полях простыми числами, получается — как выше для 3 в $\mathsf{P}(\sqrt{-1})$, — из того, что уравнения

$$a^2+6b^2=2,\ 3,$$
$$a^2+5b^2=3,\ 7,$$
$$a^2-10b^2=\pm 2,\ \pm 5,$$
$$a^2-82b^2=\pm 23,\ \pm 31$$

неразрешимы в целых рациональных числах a, b. В первом и втором случаях это явствует уже из рассмотрения величины стоящих там выражений при целых значениях a, b. В третьем случае это следует из рассмотрения равенства как сравнения по mod 5, соответственно по mod 8. В четвертом случае к цели не приводит ни рассмотрение величины, ни рассмотрение равенства как сравнения по mod 41 или mod 8, ибо $\left(\frac{\pm 23}{41}\right)=1$, $\left(\frac{\pm 31}{41}\right)=1$, $23\equiv -1 \bmod 8$, $31\equiv -1 \bmod 8$, ни рассмотрение равенства как сравнения по mod 23, соответственно по mod 31, ибо $\left(\frac{82}{23}\right)=1$, $\left(\frac{82}{31}\right)=1$. Однако здесь можно указать метод, применимый вообще для всех $d>0$, который позволяет свести рассмотрение бесконечного множества значений a, b к рассмотрению некоторого конечного множества их, а для этого конечного множества значений неразрешимость уравнений можно проверить непосредственной подстановкой.

Пусть нам нужно исследовать в вещественном квадратичном поле $\mathsf{K}=\mathsf{P}(\sqrt{d})$ $(d>0)$ диофантово уравнение

$$|N(\xi)|=m, \text{ т. е. } \frac{x^2-dy^2}{4}=\pm m, \text{ где } \xi=\frac{x+y\sqrt{d}}{2},\ m>1.$$

Вместе с ξ решением этого уравнения является также $\varepsilon\xi$ для каждой единицы ε поля K. Без ограничения общности можно считать, что ξ выбрано среди ассоциированных с ним так, что

$$1<|\xi|<\varepsilon_1,$$

где ε_1 — основная единица поля K; этим условием ξ определяется с точностью до знака однозначно. Тогда

$$|\xi'|=\frac{|N(\xi)|}{|\xi|}<|N(\xi)|=m,$$

откуда

$$|\xi\pm\xi'|\leqslant|\xi|+|\xi'|<m+\varepsilon_1.$$

Если еще однозначно определить знак числа ξ и однозначно определить различие между ξ и ξ' посредством требований $x>0$, $y>0$, то для $x=\xi+\xi'$, $y=(\xi-\xi')/\sqrt{d}$ получаются оценки

$$1\leqslant x<m+\varepsilon_1 \qquad 1\leqslant y<\frac{m+\varepsilon_1}{\sqrt{d}}.$$

Таким образом, разрешимость рассматриваемого уравнения нужно исследовать только в этой области значений x, y.

В нашем случае $d=4\cdot 82$, где, очевидно, $\varepsilon_1=9+\sqrt{82}<19$, для $a=x/2$, $b=y$ получаются оценки

$$1\leqslant a<\frac{m+19}{2},\qquad 1\leqslant b<\frac{m+19}{2\cdot 9},$$

т. е.

$$1\leqslant a\leqslant 20,\quad 1\leqslant b\leqslant 2\quad \text{для } m=23,$$
$$1\leqslant a\leqslant 24,\quad 1\leqslant b\leqslant 2\quad \text{для } m=31.$$

Поэтому неразрешимость нашего уравнения становится очевидной.

На первый взгляд тот факт, что разложение на простые множители в квадратичных полях не обязательно однозначно, лишает всякой надежды на сколько-нибудь удовлетворительное построение мультипликативной арифметики квадратичных полей. Выход, который все же оказывается возможным, был найден Куммером. Эту идею Куммера, уже набросанную нами в общих чертах в § 15, п. 5, мы подробно изложим в § 17 и внесем абсолютную ясность в только что приведенные примеры.

Впрочем, сам Куммер в молодости придерживался ошибочного мнения, что разложение на простые множители в полях алгебраических чисел однозначно. Это предположение, если и не высказанное явно, лежало в основе его первого исследования, в котором делалась попытка доказать великую теорему Ферма (см. § 3, п. 8) о неразрешимости в целых рациональных x, y, $z\neq 0$ уравнения

$$x^n+y^n+z^n=0$$

для каждого натурального $n>1$, причем речь шла о полях P_n n-х корней из 1 для простых чисел n. Как только он познакомил со своим предполагаемым доказательством Дирихле, последний тотчас же указал ему ошибку. Таким образом, Дирихле уже знал, что разложение на простые множители в полях алгебраических чисел не обязательно однозначно. Именно критика Дирихле и побудила Куммера искать выход, чтобы спасти свое остроумное доказательство. Таким образом, занятия великой теоремой Ферма послужили непосредственным поводом к рождению одного из замечательнейших математических творений XIX века — арифметической теории алгебраических чисел. Однако непосредственная цель — доказательство великой теоремы Ферма — не была достигнута Куммером и на этом пути, и теорема Ферма до сих пор является одной из крупнейших нерешенных проблем. Все же с помощью своей новой теории Куммер смог получить доказательство для некоторого определенного класса показа-

телей n. От более подробного освещения этого вопроса мы должны здесь отказаться.

Если, как мы видели, не в каждом квадратичном поле разложение на простые множители однозначно, то все же существуют специальные квадратичные поля, в которых имеет место однозначность разложения. Сейчас мы займемся подробнее такими полями. Сначала мы будем ориентироваться на оба доказательства, которые были даны нами в § 1, п. 4 и § 2, п. 10 для однозначности разложения на простые множители в поле рациональных чисел P. Если мы хотим перенести эти доказательства на квадратичное поле K с заменой рассмотрения обычной абсолютной величины в P рассмотрением абсолютной величины нормы чисел из K, то нам понадобится высказывание типа теоремы о делении с остатком. Действительно, во втором из этих доказательств основное заключение делается с помощью алгоритма Евклида, который сводится к многократному применению деления с остатком (см. VIII, п. 10, § 2); в первом же доказательстве используется идущий в том же направлении, но формально более слабый факт, что после вычитания из простого числа q простого числа $p < q$ получается натуральное число $q - p < q$.

Что касается первого, принадлежащего Цермело доказательства из § 1, п. 4, то пример $\pi = \sqrt{-2}$, $\varkappa = 5$ показывает, что для двух простых чисел π, $\varkappa$ из $\mathsf{K} = \mathsf{P}(\sqrt{-2})$ с $|N(\pi)| < |N(\varkappa)|$ не обязательно имеет место $|N(\varkappa - \pi)| < |N(\varkappa)|$, причем даже и тогда, когда $\varkappa$ соответствующим образом выбрано среди ассоциированных с ним. Однако индукция в доказательстве Цермело может быть проведена и в том случае, если в положенной в основу паре равенств

$$a' = a - pc = \left\{ \begin{matrix} p(b-c) \\ (q-p)\,c \end{matrix} \right\} \quad (\text{где } a = pb = qc)$$

вместо pc рассмотреть кратное gpc:

$$a' = a - qpc = \left\{ \begin{matrix} p(b-gc) \\ (q-gp)\,c \end{matrix} \right\},$$

которое определено так, что $|q - gp| < |q|$; предполагавшиеся в § 1, п. 4 положительное нормирование простых чисел и ограничение, состоящее в рассмотрении только положительных целых чисел, не являются существенными для этого доказательства. Эта несколько более общая трактовка доказательства Цермело оказывается необходимой уже в элементарной алгебре, если мы хотим таким методом доказать однозначность разложения многочленов $a(x)$ от одного неизвестного x над некоторым полем Ω в произведение неприводимых многочленов $p(x)$ (причем вместо абсолютной величины здесь рассматривается степень многочлена

в качестве меры его величины). Применение этой же самой идеи к разложению на простые множители в квадратичном поле K (с заменой рассмотрения обычной абсолютной величины рассмотрением абсолютной величины нормы) дает нам, очевидно, следующее высказывание.

XVIII. *Если в квадратичном поле* K *для каждой пары целых чисел* $\alpha \neq 0$, β *с* $|N(\beta)| \geqslant |N(\alpha)|$ *существует такое целое число* γ_0, *что*

$$|N(\beta - \gamma_0\alpha)| < |N(\beta)|,$$

то разложение на простые множители в K *однозначно.*

Высказывая здесь это утверждение, мы тем самым уже молчаливо предполагаем, что квадратичные поля K, для которых выполняется сделанное предположение, действительно существуют. Прежде чем убедиться в этом, мы рассмотрим это предположение несколько более подробно. Оно напоминает предположение о возможности деления с остатком, но отличается от него тем, что здесь остаток $\beta - \gamma_0\alpha$ (в смысле абсолютной величины нормы) должен быть меньше, чем делимое β, а не делитель α. Кроме того, здесь накладывается еще дополнительное условие, что с самого начала делимое β должно быть (в смысле абсолютной величины нормы) больше или равно, чем делитель α, что представляет собой ослабление по сравнению с обычным делением с остатком. Благодаря последнему условию, $\gamma_0 = 0$ никогда не удовлетворяет поставленному требованию.

Если предположение из XVIII выполнено, то посредством повторного применения этого высказывания к делимым β, $\beta - \gamma_0\alpha$, $\beta - \gamma_0\alpha - \gamma_1\alpha$, ... и постоянному делителю α, т. е. посредством последовательного вычитания кратных $\gamma_0\alpha$, $\gamma_1\alpha$, ... можно уменьшать остаток до тех пор, пока он еще (в смысле абсолютной величины нормы) больше или равен делителю α. Через конечное число шагов этот процесс должен оборваться, так как мы получим остаток, меньший (в смысле абсолютной величины нормы) чем делитель. Следовательно, мы получаем формальную аналогию с обычным делением с остатком числа β на α (с частным $\gamma = \gamma_0 + \gamma_1 + \ldots$):

$$|N(\beta - \gamma\alpha)| < |N(\alpha)|.$$

Здесь дополнительное условие $|N(\beta)| \geqslant |N(\alpha)|$ уже излишне, так как в случае $|N(\beta)| < |N(\alpha)|$ нашему требованию удовлетворяет уже $\gamma = 0$. Поэтому в дополнение к XVIII имеет место

XVIII′. *Если в квадратичном поле* K *выполнено предположение из* XVIII, *то в* K *возможно деление с остатком, т. е. для каждой пары целых чисел* $\alpha \neq 0$, β *существует такое целое число* γ, *что*

$$|N(\beta - \gamma\alpha)| < |N(\alpha)|.$$

Обратно, из возможности деления с остатком в K *следует выполнение предположения из* XVIII.

Таким образом, в K имеет место аналог алгоритма Евклида (см. § 2, п. 9) и можно доказать однозначность разложения на простые множители, имеющую место согласно XVIII, аналогично классическому доказательству из § 2, п. 10.

Если все это выполнено, то коротко говорят о квадратичных полях с алгоритмом Евклида, хотя, собственно говоря, достаточно выполнения формально более слабого предположения о возможности деления с остатком или еще более слабого предположения из XVIII. Указанные факты, очевидно, имеют силу не только для квадратичных полей; действительно за исключением числовых примеров, нигде не использовалось, что K имеет степень 2.

Теперь мы, во-первых, точнее исследуем, какие квадратичные поля обладают алгоритмом Евклида и, во-вторых, подробнее рассмотрим однозначное разложение на простые множители в таких полях и выведем следствия отсюда.

1. Если мы введем дробное число $\xi = \beta/\alpha$ из K, то возможность деления с остатком, сформулированная в XVIII, может быть высказана также в виде следующего требования:

Существование достаточно близкого целого числа. *В* K *существует для каждого числа* ξ *целое число* γ *с*

$$|N(\xi-\gamma)|<1.$$

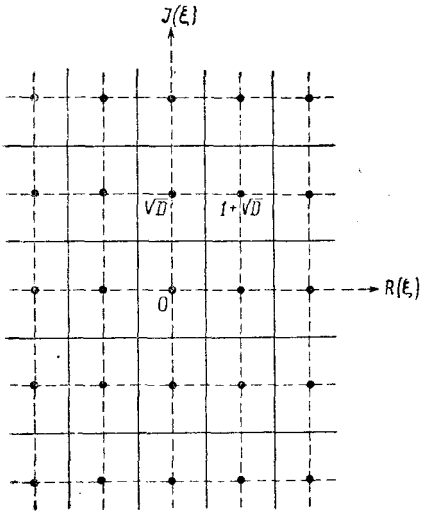
Это требование можно геометрически истолковать на K-плоскости. Представим себе, что решетка целых чисел (см. п. 3, фиг. 12а, б) параллельно перенесена так, что начало координат (или какая-нибудь точка решетки) попало в заданную точку ξ. Тогда внутри представленного на фиг. 11а, б круга, соответственно пары равносторонних гипербол с центром в начале координат и радиусом 1, должна лежать хотя бы одна точка решетки. Очевидно, что ничего не изменится, если мы оставим в покое решетку, а круг, соответственно равностороннюю гиперболу параллельно перенесем так, чтобы центр попал в ξ. Мы положим в основу дальнейшего именно это представление.

А. *Мнимый случай.* В этом случае легко получить необходимое и достаточное условие для выполнения поставленного требования. Именно здесь сразу видно геометрически, какая точка решетки γ лежит ближе всего к заданной точке ξ на K-плоскости в том смысле, что квадрат расстояния

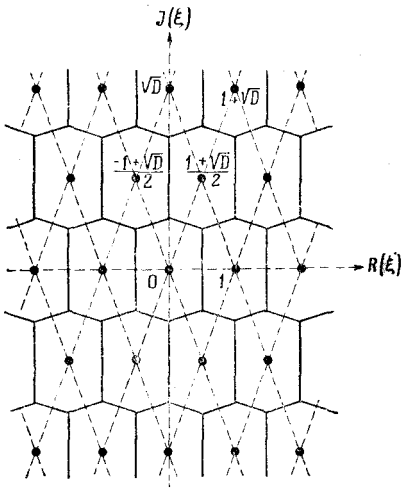
$$|N(\xi-\gamma)| \text{ минимален.} \qquad (A)$$

а) В случае $D \equiv 2, 3 \bmod 4$, когда целочисленным базисом поля K является $1, \sqrt{D}$, мы будем представлять себе решетку состоящей из вершин прямоугольников. Проведя в каждом из них

средние линии, мы получим новую систему прямоугольников (равных первоначальным), причем каждая точка γ решетки будет центром некоторого прямоугольника $\mathfrak{R}_\gamma$ и этой новой системы (см. фиг. 14Аа). Для точек из $\mathfrak{R}_\gamma$ ближайшей в смысле (А) точкой решетки является, очевидно, γ; если ξ лежит на границе $\mathfrak{R}_\gamma$, то наряду с γ существует еще одна ближайшая к ξ



Фиг. 14 Аа.



Фиг. 14 Аб.

целая точка, а для угловой точки прямоугольника $\mathfrak{R}_\gamma$ ближайших целых точек будет четыре.

Поставленное требование, очевидно, выполняется тогда и только тогда, когда квадрат расстояния от любой точки ξ из $\mathfrak{R}_0$ до начала координат будет меньше 1. Это расстояние является наибольшим, например, для угловой точки $\xi = (1+\sqrt{D})/2$. Поэтому необходимое и достаточное условие гласит

$$N\left(\frac{1+\sqrt{D}}{2}\right) = \frac{1+|D|}{4} < 1, \text{ или, другими словами, } |D| < 3.$$

Оно выполняется только для

$$D = -1, \ -2, \quad \text{т. е. } d = -4, \ -8.$$

б) В случае $D \equiv 1 \bmod 4$ к рассмотренным только что точкам решетки добавляются еще центры первоначальных прямоугольников. В качестве целочисленного базиса мы выберем $(-1+\sqrt{D})/2$, $(1+\sqrt{D})/2$; тогда решетка будет состоять из вершин ромбов. Проведя перпендикуляры к серединам сторон

этих ромбов и (бо́льшие) вертикальные диагонали, мы получим систему шестиугольников, причем каждая точка γ решетки будет центром некоторого шестиугольника $\mathfrak{S}_\gamma$ (фиг. 14Аб). Для точек ξ из $\mathfrak{S}_\gamma$ ближайшей в смысле (А) точкой решетки, очевидно, снова является γ; для точек, лежащих на стороне шестиугольника $\mathfrak{S}_\gamma$, ближайших целых точек будет две, а для угловых точек шестиугольника — три.

Поставленное требование, очевидно, снова выполняется тогда и только тогда, когда квадрат расстояния от любой точки ξ из $\mathfrak{S}_0$ до начала координат будет меньше 1. Это расстояние будет наибольшим, например, для угловой точки на положительной части мнимой оси; элементарно-геометрически мы получаем, что эта точка есть $\xi=(\sqrt{D}-1/\sqrt{D})/4$. Поэтому необходимое и достаточное условие гласит:

$$\left|N\left(\frac{1}{4}\left(\sqrt{D}-\frac{1}{\sqrt{D}}\right)\right)\right|=\frac{1}{16}\left(|D|+2+\frac{1}{|D|}\right)<1,$$

или, другими словами, $|D|<14$.

Оно выполняется только для

$$D=-3,\ -7,\ -11,\quad \text{т. е. } d=-3,\ -7,\ -11.$$

В итоге нами доказано

XIXA. *Среди мнимых квадратичных полей* $\mathsf{K}=\mathsf{P}(\sqrt{d})$ *алгоритмом Евклида обладают пять полей с наименьшими по абсолютной величине дискриминантами*

$$d=-3,\ -4,\ -7,\ -8,\ -11$$

и только они.

Таким образом, в этих полях разложение на простые множители однозначно.

Б. *Вещественный случай.* В этом случае установление одновременно и необходимого, и достаточного условия для выполнения поставленного требования является более трудным потому, что область внутри пары равносторонних гипербол простирается в бесконечность. Однако можно совсем просто получить по крайней мере достаточное условие, если выделить в этой области ограниченную выпуклую подобласть и наложить более сильное требование, чтобы уже эта подобласть при любом положении точки ξ содержала в себе точку решетки γ. В качестве этой подобласти внутренней части пары равносторонних гипербол мы выберем квадрат со сторонами, параллельными осям, центром в начале координат и длиной стороны 2 (фиг. 15). При этом требование

$$|N(\xi-\gamma)|=|R(\xi-\gamma)^2-I(\xi-\gamma)^2|<1$$

для абсолютной величины нормы заменяется соответственно более сильными неравенствами

$$|R(\xi-\gamma)|<1, \quad |I(\xi-\gamma)|<1$$

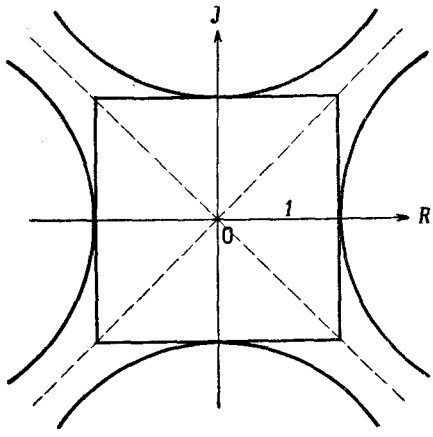
для абсолютных величин координат; эти неравенства могут быть также соединены в одно:

$$\max(|R(\xi-\gamma)|, |I(\xi-\gamma)|)<1.$$

Исследуем теперь, какая точка γ решетки лежит ближе всего к заданной точке ξ на K-плоскости, в том смысле, что максимум абсолютных величин разностей координат

$$\max(|R(\xi-\gamma)|, |I(\xi-\gamma)|)$$

минимален. (Б)



Фиг. 15.

а) В случае $D\equiv 2,3 \bmod 4$ положение обстоит так же, как и раньше, с той только разницей, что одновременно несколько целых точек γ могут быть ближайшими для ξ в смысле (Б) не только тогда, когда ξ лежит на границе прямоугольника $\mathfrak{R}_\gamma$, но и для некоторых внутренних точек ξ этого прямоугольника (на фиг. 14Ба эти точки заштрихованы). Однако для наших рассуждений это не имеет значения. Наше более сильное требование выполняется тогда и только тогда, когда максимумы абсолютных величин координат всех точек ξ из $\mathfrak{R}_0$ будут меньше 1. Этот максимум будет наибольшим, например, для угловой точки $\xi=(1+\sqrt{D})/2$ и будет при этом равен вертикальной координате $I(\xi)$ этой точки. Поэтому необходимое и достаточное условие гласит:

$$\frac{1}{2}\sqrt{D}<1, \text{ или, другими словами, } D<4.$$

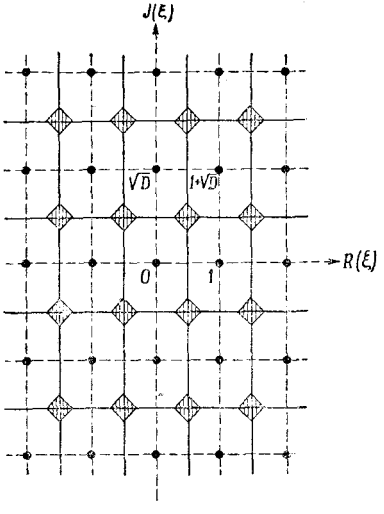
Оно выполняется для

$$D=2,\ 3, \qquad \text{т. е. } d=8,\ 12,$$

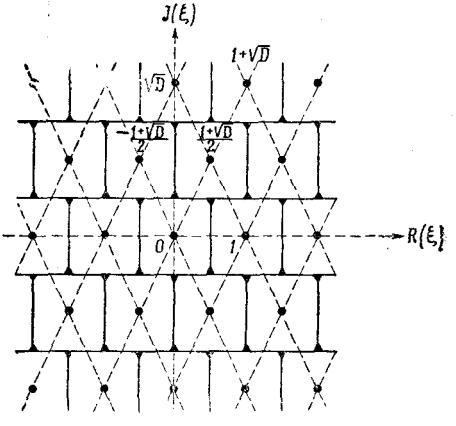
и только для них.

б) В случае $D\equiv 1 \bmod 4$, как легко видеть, ближайшая к ξ в смысле (Б) целая точка γ тоже определяется с помощью прямоугольников $\mathfrak{R}_\gamma$ со сторонами, параллельными осям, и центрами в точках γ, причем опять-таки ближайших целых точек может

быть несколько также и для некоторых внутренних точек этих прямоугольников (фиг. 14Бб). Как и перед этим, более сильное требование выполняется тогда и только тогда, когда максимум абсолютных величин координат для любой точки ξ из $\mathfrak{R}_0$ будет



Фиг. 14 Ба.



Фиг. 14 Бб.

меньше 1. Этот максимум будет наибольшим, например, для угловой точки $\xi = 1/2 + \sqrt{D}/4$, причем он равен вертикальной координате $I(\xi)$ этой точки. Поэтому необходимое и достаточное условие гласит

$$\frac{1}{4}\sqrt{D} < 1, \text{ или, другими словами, } D < 16.$$

Оно выполняется для

$$D = 5, 13, \text{ т. е. } d = 5, 13,$$

и только для них.

В итоге мы доказали

XIXБ. *Вещественные квадратичные поля* $\mathsf{K} = \mathsf{P}(\sqrt{d})$ *с четырьмя наименьшими дискриминантами*

$$d = 5,\ 8,\ 12,\ 3$$

обладают алгоритмом Евклида.

Таким образом, разложение на простые множители в этих полях однозначно.

В отличие от мнимого случая в вещественном случае алгоритмом Евклида обладают и поля с другими дискриминантами;

чтобы определить эти поля, нужно пользоваться первоначальным требованием относительно абсолютной величины нормы, а не более сильным требованием относительно максимума абсолютных величин разностей координат. Рассмотрение этого вопроса требует трудоемких исследований в каждом отдельном случае и здесь мы не будем детально излагать его, тем более, что этот вопрос не является особенно интересным с точки зрения общей структуры арифметики квадратичных полей. Мы ограничимся тем, что сообщим результат этих исследований. Оказывается, что и вещественных квадратичных полей с алгоритмом Евклида существует только конечное множество. Именно, кроме уже найденных нами, алгоритм Евклида существует только в вещественных квадратичных полях с дискриминантами

$$d = 17,\ 21,\ 24,\ 28,\ 29,\ 33,\ 37,\ 41,\ 44,\ 57,\ 73,\ 76,\ 97.$$

В связи с результатами XIXA, Б нужно еще сказать, что вполне могут быть другие квадратичные поля $\mathsf{K} = \mathsf{P}(\sqrt{d})$, в которых хотя и нет алгоритма Евклида, но тем не менее разложение на простые множители однозначно. Мы еще вернемся к этому в конце § 17, п. 5.

Отметим попутно, что формулировки результатов XIXA, Б показывают, насколько удобнее упорядочивать квадратичные поля по их дискриминантам d вместо свободных от квадратов ядер D.

2. Пусть теперь $\mathsf{K} = \mathsf{P}(\sqrt{d})$ — квадратичное поле с однозначным разложением на простые множители. Мы хотим получить обзор всех простых чисел π поля K, причем, конечно, ассоциированные между собой простые числа мы не будем считать существенно различными, т. е. будем рассматривать π только с точностью до соотношения $\cong$.

Каждое простое число π поля K является делителем некоторого целого рационального числа, например числа $N(\pi)$, а потому также и делителем по крайней мере одного простого рационального числа p. Так как из двух различных простых рациональных чисел всегда можно составить целочисленную линейную комбинацию, равную 1, то π не может быть делителем также и другого рационального простого числа. Таким образом, каждое простое число π поля K однозначно определяет такое рациональное простое число p, что $\pi \mid p$. Это число p называется принадлежащим числу π простым рациональным числом, а π называется простым делителем числа p в K.

Из $\pi \mid p$ следует $N(\pi) \mid p^2$, а так как по определению $N(\pi) \neq 1$ (π не является единицей), то необходимо имеет место

$$N(\pi) \cong p \quad \text{или} \quad p^2.$$

В первом случае

$$p \cong \pi\pi'$$

есть однозначное разложение числа p на простые множители в K, причем надо еще различать случаи $\pi \not\cong \pi'$ и $\pi \cong \pi'$. В случае же $N(\pi) \cong p^2$ однозначным разложением числа p^2 на простые множители будет $p^2 \cong \pi\pi'$ и потому разложение самого числа p на простые множители в K необходимо имеет вид

$$p \cong \pi \cong \pi'.$$

Если при этом заставить p пробегать все простые рациональные числа, то, согласно сказанному перед этим, получающиеся простые делители π, π' (после выбрасывания одного из π, π', если $\pi \cong \pi'$) дадут нам полную систему неассоциированных простых чисел поля K.

Теперь возникает вопрос о том, по какому закону рациональные простые числа распределяются по трем возможным типам разложения:

$$\begin{aligned} &p \cong \pi\pi' \quad \text{с} \quad \pi \not\cong \pi', \quad N(\pi) = N(\pi') \cong p, \\ &p \cong \pi^2 \quad \text{с} \quad \pi' \cong \pi, \quad N(\pi) = N(\pi') \cong p, \\ &p \cong \pi \quad \text{с} \quad \pi' \cong \pi, \quad N(\pi) = N(\pi') \cong p^2. \end{aligned}$$

Такой закон кратко называется законом разложения в K. Принципиально он должен определяться дискриминантом d поля K. Определение явного вида этого закона, которое может быть сделано многими формально различными способами, принадлежит к числу наиболее интересных и важных задач теории квадратичных полей, причем не только в случае рассматриваемых здесь специальных полей, но и в общем случае, в смысле понятий из § 15, п. 5, к которым мы вернемся в § 17.

Для тех квадратичных полей, которые рассматриваются здесь, ответ на этот вопрос дает следующий

Закон разложения в $\mathsf{K} = \mathsf{P}(\sqrt{d})$ (при однозначном разложении на простые множители). *Три возможных типа разложения*

$$p \cong \pi\pi', \quad p \cong \pi^2, \qquad p \cong \pi$$

соответствуют трем возможным значениям символа Кронекера

$$\left(\frac{d}{p}\right) = 1, \quad \left(\frac{d}{p}\right) = 0, \text{ т. е. } p \mid d, \quad \left(\frac{d}{p}\right) = -1.$$

Доказательство. а) Покажем сначала, что

$$p \cong \pi^2 \text{ равносильно } p \mid d.$$

Во-первых, пусть $p \mid d$.

Предположим, что $p \cong \pi$, т. е. p является простым числом поля K. Тогда, за исключением случая $p=2$, $D \equiv 3 \bmod 4$, мы имели бы, что $p \mid \sqrt{D}$ и потому $p^2 \mid D$, что противоречит тому, что D свободно от квадратов. В случае же $p=2$, $D \equiv 3 \bmod 4$ в силу $2 \mid 1-D=(1-\sqrt{D})(1+\sqrt{D})$, следовало бы, например, $2 \mid 1-\sqrt{D}$, откуда, согласно правилу для норм, $2^2 \mid 1-D$, что находится в противоречии с $D \equiv 3 \bmod 4$.

Поэтому обязательно $p \cong \pi\pi'$, и остается только доказать, что $\pi \cong \pi'$. Выразим для этого π и π' через базис:

$$\pi=\frac{a+b\sqrt{d}}{2}, \quad \pi'=\frac{a-b\sqrt{d}}{2}, \quad \text{откуда} \quad \pi-\pi'=b\sqrt{d}. \tag{1}$$

Из предположения $p \mid d$ следует, например, что $\pi \mid \sqrt{d}$, а отсюда далее вытекает $\pi \mid \pi-\pi'$, $\pi \mid \pi'$, $\pi' \cong \pi$, $p \cong \pi^2$, что и требовалось доказать.

Во-вторых, пусть $p \cong \pi^2$.

Тогда, повторяя предыдущие рассуждения в обратном порядке, мы получим, что во всяком случае $\pi \mid b\sqrt{d}$, т. е. $p \mid b^2 d$. Если бы теперь было $p \mid b$, то, в силу

$$p \cong \frac{a^2-db^2}{4}, \tag{2}$$

мы имели бы также $p \mid a$, что для $p \neq 2$ приводит к противоречию $p^2 \mid p$, а для $p=2$ к противоречию $2 \equiv (a/2)^2$ или $2 \equiv (a/2)^2-(b/2)^2 \bmod 4$. Поэтому $p \nmid b$ и, следовательно, $p \mid d$, что и утверждается.

б) Покажем далее, что

$$p \cong \pi\pi', \ \pi' \ncong \pi \text{ равносильно } \left(\frac{d}{p}\right)=1,$$

причем тем самым наше доказательство будет полностью закончено.

Во-первых, пусть $\left(\frac{d}{p}\right)=1$.

Тогда для $p \neq 2$ сравнение $x^2 \equiv D \bmod p$ имеет целочисленное решение. При этом, вследствие того что

$$(x-\sqrt{D})(x+\sqrt{D}) \equiv 0 \bmod \pi,$$

для простого делителя π числа p имеет место, например,

$$x-\sqrt{D} \equiv 0 \bmod \pi.$$

Однако последнее сравнение, очевидно, не выполняется по $\bmod p$, так как число $(x-\sqrt{D})/p$ является дробным. Поэтому $p \ncong \pi$, т. е. $p \cong \pi\pi'$, и, по уже доказанному, $\pi \ncong \pi'$, что и утверждалось.

Для $p=2$ $d=D\equiv 1 \bmod 8$ и потому

$$\left(1-\frac{1+\sqrt{D}}{2}\right)\left(1-\frac{1-\sqrt{D}}{2}\right)=\frac{1-D}{4}\equiv 0 \bmod 2.$$

Тогда для простого делителя π числа 2, как и перед этим, имеет место, например,

$$1-\frac{1+\sqrt{D}}{2}\equiv 0 \bmod \pi,$$

причем по mod 2 сравнение не выполняется, откуда снова следует наше утверждение.

Во-вторых, пусть $p\cong \pi\pi'$, $\pi \not\cong \pi'$.

Выше уже было показано, что в представлении (1) чисел π, π' через базис обязательно $p \nmid b$. Поэтому из (2), рассматриваемого как сравнение по mod p, следует для $p\neq 2$, что $\left(\frac{d}{p}\right)=1$, а для $p=2$, что $d\equiv 1 \bmod 8$, т. е. в обоих случаях $\left(\frac{d}{p}\right)=1$, что и требовалось доказать.

В качестве следствия из доказанного тем самым закона разложения мы выведем следующий факт

XX. *Для указанных в* XIXA, Б *дискриминантов* d *простое рациональное число* p *тогда и только тогда может быть представлено в одном из двух видов*

$$\pm p=\frac{a^2-db^2}{4}$$

с целыми рациональными a, b (*и с* $a\equiv db \bmod 2$), *когда* $\left(\frac{d}{p}\right)=1$ *или* $p \mid d$.

Это высказывание касается только поля рациональных чисел P. Оно является типичным примером того, как теория квадратичных полей K — или вообще теория полей алгебраических чисел — оказывается полезной для обогащения наших знаний о рациональных числах, а потому, в конце концов, и о натуральных числах, которые, несмотря на все самые высокие теории, все же представляют собственно предмет теории чисел.

Для обоих наименьших отрицательных дискриминантов $d=-3$, -4 утверждение XX дает нам новое доказательство наших результатов в VI, п. 9, § 10 и IV, п. 8, § 10, полученных там из теории распределения квадратичных вычетов. Читателю, уже вооруженному вышеизложенными результатами, будет полезно еще раз вернуться к указанным там нормированиям разложения простого рационального числа p; впрочем, мы и сами еще будем говорить об этом в § 18, п. 5 и § 20, п. 4.

§ 17. ТЕОРИЯ ДИВИЗОРОВ

1. Структура кольца классов вычетов по простому модулю. В элементарной теории делимости в квадратичном поле $\mathsf{K}=\mathsf{P}(\sqrt{d})$, которая строится на основе области целостности I целых чисел поля K, классы вычетов по $\bmod m$ в I для натурального числа m образуют кольцо из m^2 элементов, представителями которых являются m^2 чисел $a+b\omega$, заданных в базисном представлении, где a, b пробегают независимо друг от друга полную систему вычетов по $\bmod m$ из Γ. Это кольцо содержит кольцо классов вычетов по $\bmod m$ в Γ, получающееся при $b\equiv 0 \bmod m$.

В качестве подготовки к построению мультипликативной арифметики в K мы изучим структуру кольца классов вычетов по $\bmod p$ в I для рационального простого числа p. При этом будем пользоваться следующими обозначениями:

$\mathfrak{R}$ — кольцо классов вычетов по $\bmod p$ в I,

R — поле классов вычетов по $\bmod p$ в Γ.

В случае $\left(\frac{d}{p}\right)=1$ мы будем рассматривать также соответствующие кольца классов вычетов по $\bmod p^k$ для любого натурального k; они будут обозначаться через $\mathfrak{R}_k$, R_k.

Пусть как и до сих пор

$$\omega=\left\{\begin{array}{ll}\dfrac{1+\sqrt{D}}{2} & \text{для } D\equiv 1 \bmod 4\\ \sqrt{D} & \text{для } D\equiv 2,\ 3 \bmod 4\end{array}\right\}$$

есть введенное в (3) п. 3, § 16 базисное число поля K и

$$g(x)=x^2-sx+t=(x-\omega)(x-\omega') \qquad (s=S(\omega),\ t=N(\omega))$$

есть введенный в § 16, п. 3, согласно (4), соответствующий главный многочлен с дискриминантом

$$d=s^2-4t.$$

Теперь мы воспользуемся доказанной в (11) п. 1, § 10 формулой для числа решений

$$N[g(x)\equiv 0 \bmod p]=1+\left(\frac{d}{p}\right).$$

В приведенном там доказательстве предполагалось, что $p\neq 2$. Однако формула верна и для $p=2$, в чем можно убедиться, рассмотрев следующие четыре возможных здесь случая:

$s \bmod 2$	$t \bmod 2$	$d \bmod 4$, соотв. 8	$g(x) \bmod 2$	N
0	0	$0 \bmod 4$	x^2	1
0	1	$0 \bmod 4$	x^2+1	1
1	0	$1 \bmod 8$	x^2+x	2
1	1	$5 \bmod 8$	x^2+x+1	0

Поэтому для каждого отдельного случая мы имеем:

а) В случае $\left(\frac{d}{p}\right)=1$ сравнение $g(x) \equiv 0 \bmod p$ имеет два различных рациональных корня w, w' по $\bmod p$:

$$g(x) \equiv (x-w)(x-w') \bmod p; \quad w \not\equiv w' \bmod p.$$

б) В случае $\left(\frac{d}{p}\right)=0$, т. е. $p \mid d$, сравнение $g(x) \equiv 0 \bmod p$ имеет двукратный рациональный корень w по $\bmod p$:

$$g(x) \equiv (x-w)^2 \bmod p.$$

в) В случае $\left(\frac{d}{p}\right)=-1$ сравнение $g(x) \equiv 0 \bmod p$ не имеет рациональных корней по $\bmod p$ и, таким образом, $g(x)$ неприводим над полем классов вычетов по $\bmod p$.

Нетрудно заметить формальную аналогию между этими высказываниями и доказанным в § 16, п. 6 законом разложения для квадратичных полей с однозначным разложением на простые множители. Именно эта аналогия позволит нам посредством введения соответствующего понятия обобщить этот закон разложения на любые квадратичные поля. Предварительно мы перейдем для этого от высказываний относительно поведения $g(x)$ к рассмотрению поведения самого кольца классов вычетов по $\bmod p$ при расширении P до K.

а) Случай $\left(\frac{d}{p}\right)=1$.

Ia. *Кольцо классов вычетов* $\mathfrak{R}$ *изоморфно прямой сумме двух экземпляров поля классов вычетов* R, *т. е.*

$$\mathfrak{R} \cong R \oplus R.$$

Соответственно этому имеет место также

$$\mathfrak{R}_k \cong R_k \oplus R_k$$

для каждого натурального k.

Доказательство. Сопоставим каждому классу вычетов $\alpha \bmod p$ из $\mathfrak{R}$ однозначно определенную пару классов вычетов

$\alpha(w)$, $\alpha(w')$ из R по следующему правилу:

$$\alpha \equiv a + b\omega \bmod p \rightarrow \left\{ \begin{array}{l} \alpha(w) \equiv a + bw \bmod p \\ \alpha(w') \equiv a + bw' \bmod p \end{array} \right\} \qquad (1)$$

(w, w' означают определенные перед этим корни сравнения по $\bmod p$).

Прежде всего, оба соответствия (1) являются гомоморфизмами $\mathfrak{R}$ на R. Относительно сложения и вычитания это очевидно. Относительно же умножения заметим, что для того, чтобы произведение двух чисел из $\mathfrak{l}$ снова выразить через базис, надо воспользоваться соотношением $g(\omega) = 0$ (или в данном случае только $g(\omega) \equiv 0 \bmod p$) и что, согласно определению w, w', имеют место и соответствующие соотношения $g(w)$, $g(w') \equiv 0 \bmod p$.

Далее, посредством (1) класс вычетов $\alpha \bmod p$ из $\mathfrak{R}$ соответствует паре классов вычетов $\alpha(w)$, $\alpha(w')$ из R однозначно. Это следует из того, что соответствие (1) представляет собой линейное преобразование между координатами a, b ($\bmod p$) и компонентами $\alpha(w)$, $\alpha(w')$ ($\bmod p$) с определителем

$$\begin{vmatrix} 1 & w \\ 1 & w' \end{vmatrix} = w' - w \not\equiv 0 \bmod p.$$

Поэтому действия над классами вычетов $\alpha \bmod p$ из $\mathfrak{R}$ могут быть изоморфно описаны посредством действий с парами компонент $\alpha(w)$, $\alpha(w') \bmod p$ из R, и эти пары могут выбираться в R независимо друг от друга. Тем самым первое утверждение доказано.

Второе утверждение получается аналогичным образом, если только мы покажем, что рациональные корни w, w' сравнения $g(x) \equiv 0 \bmod p$ посредством подходящего выбора w, w' в их классах вычетов по $\bmod p$ могут быть превращены в рациональные корни w_k, w'_k сравнения $g(x) \equiv 0 \bmod p^k$. Мы покажем, что это действительно можно сделать и притом так, что все время будут выполняться соотношения

$$w_{k+1} \equiv w_k + g_k p^k, \quad w'_{k+1} \equiv w'_k + g'_k p^k \bmod p^{k+1} \qquad (k \geqslant 1)$$

с целыми рациональными g_k, g'_k, или, другими словами,

$$w_{k+1} \equiv w_k \bmod p^k, \quad w'_{k+1} \equiv w'_k \bmod p^k. \qquad (2)$$

Для первого корня сравнения, например, это получается методом полной индукции следующим образом. Для определения нормирующего члена $g_k p^k \bmod p^{k+1}$, т. е. множителя $g_k \bmod p$, мы имеем следующее требование:

$$g(w_{k+1}) = w_{k+1}^2 - s w_{k+1} + t \equiv g(w_k) + 2 w_k g_k p^k + \\ + g_k^2 p^{2k} - s g_k p^k \equiv 0 \bmod p^{k+1},$$

или, таким образом,

$$\frac{g(w_k)}{p^k} + (2w_k - s)\, g_k \equiv 0 \bmod p,$$

причем, по предположению индукции, $g(w_k) / p^k$ — целое и $w_{k_1} \equiv w \bmod p$, а потому последнее сравнение можно записать и так:

$$\frac{g(w_k)}{p^k} + (2w - s)\, g_k \equiv 0 \bmod p.$$

Так как $s \equiv w + w' \bmod p$, и потому $2w - s \equiv w - w' \not\equiv 0 \bmod p$, последнее линейное сравнение однозначно разрешимо через некоторый рациональный класс вычетов $g_k \bmod p$, что и доказывает наше утверждение.

Особо отметим играющие в дальнейшем важную роль два правила для компонент

$$\left.\begin{aligned} \alpha(w_k) &\equiv a + bw_k \\ \alpha(w'_k) &\equiv a + bw'_k \end{aligned}\right\} \bmod p^k \qquad (1_k)$$

числа $\alpha = a + b\omega$:

Правило вложения. *Для целого рационального* $\alpha = a$ *компонентами являются*

$$\alpha(w_k) \equiv a, \quad \alpha(w'_k) \equiv a \bmod p^k.$$

Правило для сопряженных. *Для числа* α', *сопряженного с* α, *компонентами являются*

$$\alpha'(w_k) \equiv \alpha(w'_k), \quad \alpha'(w'_k) \equiv \alpha(w_k) \bmod p^k.$$

Правило вложения непосредственно очевидно. Оно означает, что рациональные классы вычетов $\alpha \equiv a \bmod p^k$ характеризуются совпадением их обеих компонент между собой и с исходным классом вычетов.

Для доказательства правила для сопряженных заметим, что, ввиду того что $w_k \not\equiv w'_k \bmod p^k$, из $g(w_k) \equiv 0$, $g(w'_k) \equiv 0 \bmod p^k$, можно обычным образом получить тождество

$$g(x) = x^2 - sx + t \equiv (x - w_k)(x - w'_k) \bmod p^k$$

(хотя областью коэффициентов здесь служит не поле, а только кольцо). Поэтому наряду с $\omega + \omega' = s$ имеет место также $w_k + w'_k \equiv s \bmod p^k$. Вследствие того, что $\alpha' = a + b\omega' = a + b(s - \omega)$, мы имеем

$$\alpha'(w_k) \equiv a + b(s - w_k) \equiv a + bw'_k \equiv \alpha(w'_k) \bmod p^k,$$

что и утверждалось. Правило означает, что при переходе к сопряженному обе компоненты класса $\alpha \bmod p^k$ переставляются между собой (это находится в согласии с поведением рациональных классов вычетов).

Прямое разложение $\mathfrak{R}_k \cong R_k \oplus R_k$ осуществляется с помощью двух взаимно ортогональных идемпотентов из $\mathfrak{R}_k$, которые однозначно определяются как классы вычетов по $\bmod p^k$ с компонентами 1, 0, соответственно 0, 1 $\bmod p^k$, и, согласно правилу для сопряженных, могут быть представлены двумя сопряженными друг с другом числами ε_k, ε'_k из $\mathfrak{l}$:

$$\left.\begin{matrix} \varepsilon_k(w_k) \equiv 1, & \varepsilon_k(w'_k) \equiv 0 \\ \varepsilon'_k(w_k) \equiv 0, & \varepsilon'_k(w'_k) \equiv 1 \end{matrix}\right\} \bmod p^k. \tag{3}$$

Согласно общей схеме разложения в прямую сумму, классы вычетов $\alpha \bmod p^k$ выражаются однозначно через идемпотенты ε_k, ε'_k следующим образом:

$$\alpha \equiv \alpha(w_k)\,\varepsilon_k + \alpha(w'_k)\,\varepsilon'_k \bmod p^k, \tag{4}$$

т. е. с компонентами $\alpha(w_k)$, $\alpha(w'_k)$ в качестве коэффициентов. Если

$$\left.\begin{matrix} \varepsilon_k = u_k + v_k\omega \\ \varepsilon'_k = u'_k + v'_k\omega \end{matrix}\right\}$$

есть представления этих идемпотентов через базис, то

$$\left.\begin{matrix} u_k + v_k w_k \equiv 1, & u_k + v_k w'_k \equiv 0 \\ u'_k + v'_k w_k \equiv 0, & u'_k + v'_k w'_k \equiv 1 \end{matrix}\right\} \bmod p^k$$

и, таким образом,

$$\begin{vmatrix} u_k & v_k \\ u'_k & v'_k \end{vmatrix} \cdot \begin{vmatrix} 1 & 1 \\ w_k & w'_k \end{vmatrix} \equiv 1 \bmod p^k,$$

т. е. подстановка, переводящая базис 1, ω в пару идемпотентов ε_k, ε'_k имеет определитель, взаимно простой с p. Поэтому, наряду с 1, ω, также и идемпотенты ε_k, ε'_k (для каждого данного натурального k) образуют базис области целостности $\mathfrak{l}_p$ p-целых чисел

$$\alpha = a + b\omega \quad (a,\ b - \text{рациональные и } p\text{-целые}).$$

Для построенной ранее теории сравнений важна, согласно XII, п. 10, § 4, только эта расширенная область целостности $\mathfrak{l}_p$ всех p-целых чисел. За исключением случая $p = 2$, можно тогда вместо обычного целочисленного базиса 1, ω пользоваться и при $D \equiv 1 \bmod 4$ более простым p-целочисленным базисом 1, $\sqrt{D}$ и, таким образом, заменить w_k, $w'_k \bmod p^k$ парой корней $\pm w_k \bmod p^k$ многочлена вида:

$$x^2 - D \equiv (x - w_k)(x + w_k) \bmod p^k,$$

что удобнее в конкретных численных примерах.

В случае $p=2$, когда ввиду рассматриваемого здесь предположения $\left(\frac{d}{2}\right)=1$ имеет место $d=D\equiv 1 \bmod 4$, это не проходит; здесь мы должны применять базисное число $\omega=(1+\sqrt{D})/2$ и потому связаны не с чисто квадратным главным многочленом $g(x)=x^2-x+(1-D)/4$.

б) Случай $\left(\frac{d}{p}\right)=0$ $(p\mid d)$.

Iб. *Кольцо классов вычетов* $\mathfrak{R}$ *есть сумма (не прямая) поля классов вычетов* R *и кратного* $R\pi$ *с нильпотентным классом вычетов* $\pi \bmod p$ *показателя* 2, *т. е.*

$$\mathfrak{R}\cong R+R\pi \quad \text{с } \pi^2\equiv 0 \bmod p.$$

Доказательство. Если мы положим

$$\pi=\omega-w, \tag{5}$$

где w — определенный ранее двукратный корень сравнения по $\bmod p$, то получим

$$\pi^2=(\omega-w)^2\equiv g(\omega)\equiv 0 \bmod p.$$

Переход от целочисленного базиса 1, ω к целочисленному базису 1, π позволяет убедиться в правильности утверждения.

Для тех, кто знаком с теорией алгебр, добавим, что конечная коммутативная алгебра $\mathfrak{R}$ ранга 2 над полем R имеет радикалом нильпотентную алгебру $R\pi$ ранга 1 и показателя 2 и что для кольца классов вычетов по радикалу имеет место $\mathfrak{R}/R\pi\cong R$. Однако для нашей цели можно обойтись и без этого абстрактного толкования.

Принадлежащий π главный многочлен есть

$$f(x)=(x-\pi)(x-\pi')=g(x+w)=x^2+g'(w)\,x+g(w).$$

Ввиду того что w — двукратный корень по $\bmod p$, отсюда следует

$$S(\pi)\equiv 0 \bmod p, \quad N(\pi)\equiv 0 \bmod p. \tag{6}$$

Наряду с этим

$$N(\pi)\not\equiv 0 \bmod p^2. \tag{7}$$

Действительно, так как $f(x)$ тоже имеет дискриминант d, то

$$S(\pi)^2-4N(\pi)=d.$$

Для $p\neq 2$ отсюда сразу следует правильность (7), если принять во внимание (6) и то, что d свободно от квадратов, за исключением, быть может, множителя 4. Для $p=2$ в рассматриваемом

случае $d=4D$ с $D\equiv 2,\ 3 \bmod 4$ и, таким образом,

$$\left(\frac{S(\pi)}{2}\right)^2 - N(\pi) \equiv 2,\ 3 \bmod 4,$$

$$N(\pi) \equiv \left(\frac{S(\pi)}{2}\right)^2 + 2,\ 1 \bmod 4,$$

что, ввиду $\left(\frac{S(\pi)}{2}\right)^2 \equiv 0,\ 1 \bmod 4$ и второго из сравнений (6), снова доказывает правильность (7). Если опять положить в основу вместо $\mathfrak{l}$ расширенную область целостности $\mathfrak{l}_p$ p-целых чисел, то, за исключением случая $p=2$ $D\equiv 3 \bmod 4$ можно выбрать $w=s/2$, так что $\pi=\sqrt{d}/2$ будет корнем чисто квадратного многочлена. В случае $p=2$ $D\equiv 3 \bmod 4$ это рассуждение не проходит; именно, здесь $w\equiv 1 \bmod 2$, а потому $\pi\equiv 1+\sqrt{D} \bmod 2$ не является корнем чисто квадратного многочлена.

в) Случай $\left(\frac{d}{p}\right)=-1$.

Iв. *Кольцо классов вычетов* $\mathfrak{R}$ *есть поле, являющееся квадратичным расширением поля классов вычетов* R.

Доказательство. Так как $\mathfrak{R}$ является конечным коммутативным кольцом с единицей над полем R, то достаточно установить отсутствие делителей нуля (однозначность деления); тогда свойство поля (неограниченная возможность деления) будет следовать по обычной схеме такого заключения в теории групп.

Предположим теперь, что имеет место

$$\alpha\beta \equiv 0 \bmod p \quad \text{с целыми } \alpha,\ \beta \not\equiv 0 \bmod p.$$

Тогда мы имели бы

$$N(\alpha)\,N(\beta) \equiv 0 \bmod p,$$

и потому, например,

$$N(\alpha) \equiv 0 \bmod p, \text{ но } \alpha \not\equiv 0 \bmod p.$$

Для координат a, b из представления $\alpha=a+b\omega$ эти сравнения означают

$$(a+b\omega)(a+b\omega') = a^2+sab+tb^2 \equiv 0 \bmod p, \text{ но } (a,\ b) \not\equiv 0 \bmod p.$$

Из первого сравнения следует $b\equiv 0 \bmod p$, а тогда также и $a\equiv 0 \bmod p$, в противоречии со вторым, так как если бы было $b\not\equiv 0 \bmod p$, то следовало бы $g(-a/b)\equiv 0 \bmod p$, в то время как в рассматриваемом здесь случае сравнение $g(x)\equiv 0 \bmod p$ предполагается не имеющим рациональных корней. Тем самым отсутствие собственных делителей нуля в $\mathfrak{R}$ доказано.

Ясно, что $\mathfrak{R}$ является тогда квадратичным расширением поля R, именно,

$$\mathfrak{R}=R(\omega) \quad \text{с } g(\omega)\equiv 0 \bmod p.$$

В то время как в двух предшествующих случаях структура кольца $\mathfrak{R}$ выявлялась только после перехода к специальным базисам ε_k, ε_k' из (3), соответственно 1, π из (5), в настоящем случае уже первоначальный базис 1, ω пригоден для описания этой структуры.

Отметим также имеющее место в этом случае и важное для многих целей правило для сопряженных:

$$\alpha' \equiv \alpha^p \bmod p. \tag{8}$$

Действительно, порождающий автоморфизм $\alpha \to \alpha'$ расширения K/P определяет некоторый автоморфизм расширения $\mathfrak{R}/R$, и притом не тождественный, так как оба корня ω, ω' многочлена $g(x)$ различны по $\bmod p$, ибо $d \not\equiv 0 \bmod p$. Но $\alpha \to \alpha^p$ также определяет автоморфизм расширения $\mathfrak{R}/R$, и притом тоже не тождественный, потому что сравнение $x^p - x \equiv 0 \bmod p$ имеет только p корней из R. Так как $\mathfrak{R}/R$ имеет степень 2, то у него может быть только один нетождественный автоморфизм. Поэтому оба автоморфизма расширения $\mathfrak{R}/R$, определяемые через $\alpha \to \alpha'$ и $\alpha \to \alpha^p$, совпадают между собой. Вместо этого абстрактного доказательства можно доказать (8) также и следующим, более выкладочным способом. Достаточно рассмотреть $\alpha = \omega$. В силу того что поле не имеет делителей нуля, из

$$(\omega^p - \omega)(\omega^p - \omega') = g(\omega^p) \equiv g(\omega)^p \equiv 0 \bmod p$$

и

$$\omega^p - \omega \not\equiv 0 \bmod p \text{ (так как } \omega \bmod p \text{ не рационально)}$$

следует

$$\omega^p - \omega' \equiv 0 \bmod p.$$

Наконец, отметим, что изложенная сейчас теория проливает новый свет на доказательство закона разложения из § 16, п. 6 при специальных предположениях. Теперь это доказательство можно кратко провести следующим образом.

Для $\left(\frac{d}{p}\right) = 1$ и $\left(\frac{d}{p}\right) = 0$ $\mathfrak{R}$ обладает собственными делителями нуля, а именно (образованными для $k = 1$) ортогональными идемпотентами ε, $\varepsilon' \bmod p$, соответственно нильпотентным элементом $\pi \bmod p$ показателя 2; поэтому в этих случаях p не может быть простым числом в K и, следовательно, $p \cong \pi\pi'$ с $\pi \not\cong \pi'$ или $\pi \cong \pi'$. Для $\left(\frac{d}{p}\right) = 1$ $\mathfrak{R}$ не имеет собственных нильпотентных элементов; поэтому не может быть $p \cong \pi^2$ и, следовательно, $p \cong \pi\pi'$, где $\pi \not\cong \pi'$. Для $\left(\frac{d}{p}\right) = 0$ $\mathfrak{R}$ обладает собственным нильпотентным элементом показателя 2; поэтому здесь последний тип разложения невозможен и, таким образом, $p \cong \pi^2$.

Для $\left(\frac{d}{p}\right) = -1$ $\mathfrak{R}$ не имеет собственных делителей нуля; поэтому ни один из этих двух типов разложения не может иметь места и, следовательно, $p \cong \pi$.

2. Теория делимости и сравнений для степеней простых дивизоров. После этих подготовительных рассмотрений мы переходим к понятиям § 15, п. 5, причем будем изучать их здесь для нашего специального случая квадратичного поля K.

В § 15, п. 5 мы исходили из квадратичного характера χ с натуральным ведущим модулем f и в теореме X (а также и перед этим) установили, что соответствующее ему квадратичное подполе K поля P_f f-х корней из 1 определяется посредством

$$\mathsf{K} = \mathsf{P}\left(\sqrt{\chi(-1)f}\right),$$

причем, на основании квадратичного закона взаимности,

$$\chi(x) = \left(\frac{\chi(-1)f}{x}\right) \text{ для } x > 0.$$

Если заранее считать, что χ, а тем самым и f, нормированы в соответствии с (4) п. 7, § 13 так, что χ как числовая функция является четным, причем тогда $\chi(-1)f$ можно заменить на f, то, как уже было сказано в § 15, п. 1 после I, мы получаем формальное упрощение

$$\mathsf{K} = \mathsf{P}(\sqrt{f}), \quad \chi(x) = \left(\frac{f}{x}\right).$$

Согласно (4) п. 3, § 16 и XVI, XIX, § 13, ведущие модули f так нормированных квадратичных характеров χ пробегают как раз совокупность всевозможных дискриминантов d квадратичных полей. Поэтому рассматривавшиеся в § 15, п. 5 квадратичные поля $\mathsf{K} = \mathsf{P}(\sqrt{f})$ охватывают всю совокупность квадратичных полей $\mathsf{K} = \mathsf{P}(\sqrt{d})$, и соответствующие им квадратичные характеры $\chi(x)$ суть соответствующие символы Кронекера $\left(\frac{d}{x}\right)$, значение которых для теории квадратичных полей было отчетливо выяснено уже и ранее. В дальнейшем мы, однако, не хотим предполагать известным квадратичный закон взаимности; тогда мы, конечно, не сможем пользоваться тем, что символ Кронекера $\left(\frac{d}{x}\right)$ есть квадратичный характер $\chi(x)$ и что $\mathsf{K} = \mathsf{P}(\sqrt{d})$ получается указанным образом как подполе поля $\mathsf{P}_{|d|}$ корней из 1.

Однако мы еще на мгновение задержимся на этой связи именно для того, чтобы сопоставить результаты из (I_0), (I)

п. 5, § 15 относительно представления

$$\zeta_{\mathsf{K}}(s)=\zeta(s)\,L(s\,|\,\chi)=\prod_{p}\left(\frac{1}{1-\frac{1}{p^{f_p s}}}\right)^{g_p}=\prod_{\mathfrak{p}}\frac{1}{1-\frac{1}{\mathfrak{N}(\mathfrak{p})^s}}$$

для дзета-функции квадратичного поля K с только что выведенными результатами 1а,б,в относительно структуры кольца классов вычетов по $\mathrm{mod}\ p$ в K. Мы это сделаем в виде приводимой ниже схемы, в которой по трем случаям $\left(\frac{d}{p}\right)=1,\ 0,-1$ распределены, с одной стороны, определенные в I, п. 1, § 15 показатели e_p, f_p, g_p с

$$e_p f_p g_p = 2$$

и формально введенное в § 15, п. 5 разложение на простые дивизоры вместе с определенной там нормой простого дивизора и, с другой стороны, типы кольца классов вычетов $\mathfrak{R}$, а также типы разложения простого числа p для специального случая полей с однозначным разложением на простые множители (см. § 16, п. 6):

$\left(\frac{d}{p}\right)$	e_p	f_p	g_p	Простые дивизоры сопоставленные	$p\cong$	$\mathfrak{N}(\mathfrak{p})$	$\mathfrak{R}\cong$	$p\cong$	$N(\pi)\cong$
1	1	1	2	$\mathfrak{p},\mathfrak{p}'$	$\mathfrak{p}\mathfrak{p}'$	p	$R\oplus R$	$\pi\pi'$	p
0	2	1	1	$\mathfrak{p}$	$\mathfrak{p}^2$	p	$R+R\pi$	π^2	p
−1	1	2	1	$\mathfrak{p}$	$\mathfrak{p}$	p^2	поле	π	p^2

Из этого сопоставления видно, что формально введенные в § 15, п. 5 простые дивизоры $\mathfrak{p}$ поля K в точности отражают структуру простых чисел π в специальном случае квадратичных полей K с однозначным разложением на простые множители, установленную нами в § 16, п. 6, причем это относится как к разложению числа p, так и к норме; кроме того, структура кольца классов вычетов $\mathfrak{R}$ также находится в соответствии с указанным положением.

Чтобы выяснить теперь истинное значение простых дивизоров, выходящее за рамки чисто формального определения, мы должны обратиться без всяких ограничений к структуре кольца классов вычетов $\mathfrak{R}$. Подчеркнем, что при выяснении этой структуры в п. 1 мы при различении трех случаев $\left(\frac{d}{p}\right)=1,\ 0,\ -1$ руководствовались только первоначальным, содержащимся в опреде-

лении истолкованием символа $\left(\frac{d}{p}\right)$ как символа Лежандра (с элементарным расширением на случай $p=2$ посредством формул $\left(\frac{d}{2}\right)=(-1)^{(d-1)/4}$ для $d\equiv 1 \bmod 4$, $\left(\frac{d}{2}\right)=0$ для $d\equiv 0 \bmod 4$). Вытекающее из квадратичного закона взаимности истолкование этого символа как квадратичного характера $\left(\frac{d}{x}\right)=\chi(x)$ с ведущим модулем d мы можем теперь не использовать, после того как основывающееся на этом истолковании представление в виде произведения для $\zeta_{\mathsf{K}}(s)$ навело нас на мысль ввести простые дивизоры $\mathfrak{p}$. Мы лишь сохраним идею формального сопоставления простым рациональным числам p, в соответствии с тремя возможными значениями $\left(\frac{d}{p}\right)=1,\ 0,\ -1$ символа Лежандра, простых дивизоров

$$\mathfrak{p},\ \mathfrak{p}',\ \text{соответственно}\ \mathfrak{p},\ \text{соответственно}\ \mathfrak{p}$$

с нормами

$$\mathfrak{N}(\mathfrak{p})=\mathfrak{N}(\mathfrak{p}')=p,\ \text{соответственно}\ \mathfrak{N}(\mathfrak{p})=p,\ \text{соответственно}\ \mathfrak{N}(\mathfrak{p})=p^2.$$

Содержательное истолкование этих простых дивизоров мы получим благодаря тому, что сначала определим с помощью результатов из п. 1 относительно структуры кольца $\mathfrak{N}$ (отдельно для каждого из трех случаев), что должно означать отношение делимости

$$\mathfrak{p}^n \mid \alpha$$

для целых α из K и натуральных n. Далее мы определим, что означает непосредственно интересующее нас при разложении на простые дивизоры отношение

$$\mathfrak{p}^m \text{ есть точная степень дивизора } \mathfrak{p}, \text{ входящая в } \alpha,$$

для целого $\alpha\neq 0$ из K и докажем относительно этого понятия ряд теорем и правил, причем попутно получим также содержательное истолкование и для нормы $\mathfrak{N}(\mathfrak{p})$. Тем самым мы будем иметь в распоряжении все для того, чтобы определить уже приведенное в § 15, п. 5 разложение на простые дивизоры

$$\alpha \cong \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}},$$

сначала для целых, а потом и для любых $\alpha\neq 0$ из K, и доказать высказанные там основные теоремы арифметики.

В дальнейшем под $\mid$ мы будем, как и раньше, понимать область целостности целых чисел поля K.

а) *Случай* $\left(\frac{d}{p}\right)=1$; *два простых дивизора* $\mathfrak{p}$, $\mathfrak{p}'$, *нормы равны* p.
Мы определим отношения делимости:

$$\mathfrak{p}^n \mid \alpha \text{ посредством } p^n \mid \alpha(w_n),$$
$$\mathfrak{p}'^n \mid \alpha \text{ посредством } p^n \mid \alpha(w'_n),$$

где $\alpha(w_n)$, $\alpha(w'_n) \bmod p^n$ — введенные в (1_k) п. 1 рациональные компоненты класса вычетов $\alpha \bmod p^n$. Ввиду свойства (2) п. 1 для последовательностей компонент $\alpha(w_k)$, $\alpha(w'_k) \bmod p^k$ нам было бы также достаточно определить только:

$$\mathfrak{p}^n \mid \alpha \text{ посредством } p^n \mid \alpha(w_k) \text{ хотя бы для одного } k \geqslant n,$$
$$\mathfrak{p}'^n \mid \alpha \text{ посредством } p^n \mid \alpha(w'_k) \text{ хотя бы для одного } k \geqslant n;$$

действительно, тогда эти соотношения автоматически выполнялись бы для всех $k \geqslant n$, в частности и для $k=n$.

Большей частью мы будем применять это определение в его второй, общей форме. Отсюда очевидно, что выполняется следующее требование, которое естественно предъявить к определению делимости:

$$\text{из } \mathfrak{p}^n \mid \alpha \text{ следует } \mathfrak{p}^{n'} \mid \alpha \text{ для всех натуральных } n' \leqslant n,$$

и то же самое с $\mathfrak{p}'$ вместо $\mathfrak{p}$, что мы в дальнейшем не всегда будем специально отмечать.

Теперь прежде всего из правила вложения и правила для сопряженных из п. 1 мы получаем:

Правило вложения. *Для целого рационального* a

$$\mathfrak{p}^n \mid a \text{ равносильно } p^n \mid a.$$

Правило для сопряженных. $\mathfrak{p}^n \mid \alpha$ *равносильно* $\mathfrak{p}'^n \mid \alpha'$.

Таким образом, понятия делимости для $\mathfrak{p}$ и $\mathfrak{p}'$ связаны между собой посредством порождающего автоморфизма поля K; поэтому $\mathfrak{p}$ и $\mathfrak{p}'$ называются сопряженными друг с другом простыми дивизорами.

Далее, из гомоморфизма действий над компонентами действиям над целыми числами из K для этого понятия делимости получаются элементарные правила:

$$\text{из } \mathfrak{p}^n \mid \alpha,\ \mathfrak{p}^n \mid \beta \text{ следует } \mathfrak{p}^n \mid \alpha \pm \beta,$$
$$\text{из } \mathfrak{p}^n \mid \alpha \text{ следует } p^n \mid \gamma\alpha$$

для целых α, β, γ из K. Поэтому имеет место

На. *Числа* α *из* I, *являющиеся кратными* $\mathfrak{p}^n$, *образуют идеал в* I.

Относительно понятия идеала, которое мы здесь и в дальнейшем будем относить к области целостности I, нужно вспомнить определение, данное в § 2, п. 8. Оно было сформулировано

там как раз так, что автоматически обобщается на любые области целостности.

В соответствии с этим мы определим далее сравнимость

$$\alpha \equiv \beta \bmod \mathfrak{p}^n \text{ посредством } \mathfrak{p}^n \mid \alpha - \beta.$$

Тогда имеют место формальные правила для сложения, вычитания и перемножения сравнений:

IIIa. *Классы вычетов по* $\bmod \mathfrak{p}^n$ *области целостности* $\mathfrak{l}$ *образуют кольцо.*

В смысле этого обобщения понятия сравнимости для числа α из $\mathfrak{l}$ и его компонент $\alpha(w_k) \bmod p^k$ имеет место система сравнений

$$\alpha \equiv \alpha(w_k) \bmod \mathfrak{p}^n \text{ для всех } k \geqslant n.$$

Действительно, $\alpha - \alpha(w_k)$ имеет по $\bmod p^n$ компоненту $\alpha(w_n) - \alpha(w_k) \equiv 0 \bmod p^n$. Поэтому классы вычетов $\alpha \bmod \mathfrak{p}^n$ области целостности $\mathfrak{l}$ могут быть представлены уже числами из Γ. Согласно правилу вложения, при заданном α эти представители однозначно определяются по $\bmod p^n$, именно как классы вычетов $\alpha(w_n) \bmod p^n$, являющиеся компонентами. Тем самым мы получаем

IVa. *Кольцо классов вычетов по* $\bmod \mathfrak{p}^n$ *области целостности* $\mathfrak{l}$ *изоморфно кольцу классов вычетов по* $\bmod p^n$ *области целостности* Γ.

Поэтому количество классов вычетов по $\bmod \mathfrak{p}^n$ есть $p^n = \mathfrak{N}(\mathfrak{p}^n)$.

Последнее утверждение дает нам содержательное истолкование нормы дивизора, которая до этого была определена лишь формально.

Для частного случая $n = 1$ получается, что кольцо классов вычетов по $\bmod \mathfrak{p}$ области целостности $\mathfrak{l}$ является полем, изоморфным полю классов вычетов по $\bmod p$ области целостности Γ.

Наконец докажем

Va. *Для каждого* $\alpha \neq 0$ *из* $\mathfrak{l}$ *существует наивысшая степень* $\mathfrak{p}^m$ *с* $\mathfrak{p}^m \mid \alpha$.

В этом случае мы также будем коротко говорить: *в* α *входит точно* $\mathfrak{p}^m$.

Доказательство. Из $\mathfrak{p}^n \mid \alpha$ следует $\mathfrak{p}^n \mid \alpha\alpha' = N(\alpha)$, и потому, согласно правилу вложения, $p^n \mid N(\alpha)$. Так как для $\alpha \neq 0$ также и $N(\alpha) \neq 0$, n тем самым ограничено сверху.

Ясно, что показатель m характеризуется тем, что

$$p^m \mid \alpha(w_k), \quad \mathfrak{p}^{m+1} \nmid \alpha(w_k) \text{ хотя бы для одного } k > m,$$

а тогда также и для всех $k > m$, т. е. это такой показатель, с которым p входит во все члены последовательности компонент $\alpha(w_k)$, начиная с некоторого.

Как уже говорилось, предыдущие факты имеют силу, конечно, и для сопряженного простого дивизора $\mathfrak{p}'$. Рассмотрим теперь оба сопряженных простых дивизора $\mathfrak{p}$, $\mathfrak{p}'$ совместно.

В соответствии с установкой формальной теории дивизоров из § 15, п. 5, согласно которой простые дивизоры рассматриваются как образующие элементы свободной мультипликативной абелевой группы, мы определим здесь делимость

$$\mathfrak{p}^n\mathfrak{p}'^{n'} \mid \alpha \quad \text{посредством} \quad \mathfrak{p}^n \mid \alpha,\ \mathfrak{p}'^{n'} \mid \alpha,$$

или в явном виде

$$\mathfrak{p}^n\mathfrak{p}'^{n'} \mid \alpha \quad \text{посредством} \quad p^n \mid \alpha(w_k),\ p^{n'} \mid \alpha(w_k')$$

хотя бы для одного $k \geqslant n,\ n'$,

а тогда также и для всех $k \geqslant n,\ n'$; аналогично мы определим сравнимость

$$\alpha \equiv \beta \bmod \mathfrak{p}^n\mathfrak{p}'^{n'} \quad \text{посредством} \quad \alpha \equiv \beta \bmod \mathfrak{p}^n,\quad \alpha \equiv \beta \bmod \mathfrak{p}'^{n'}.$$

Тогда прежде всего мы получаем снова

IIa*. *Числа* α *и* $|$, *являющиеся кратными* $\mathfrak{p}^n\mathfrak{p}'^{n'}$, *образуют идеал в* $|$.

IIIa*. *Классы вычетов по* $\bmod \mathfrak{p}^n\mathfrak{p}'^{n'}$ *области целостности* $|$ *образуют кольцо.*

Согласно определению, эти классы вычетов $\alpha \bmod \mathfrak{p}^n\mathfrak{p}'^{n'}$ обладают однозначным разложением на компоненты, которые являются парой классов вычетов $\alpha \bmod \mathfrak{p}^n$, $\alpha \bmod \mathfrak{p}'^{n'}$; при этом операции сложения, вычитания и умножения можно выполнять покомпонентно. Мы покажем, что компоненты при этом независимы друг от друга, т. е. что это разложение прямое:

IVa*. *Для заданных* a, a' *из* Γ *существует* α *из* $|$ *с*

$$\alpha \equiv a \bmod \mathfrak{p}^n, \qquad \alpha \equiv a' \bmod \mathfrak{p}'^{n'}.$$

Кольцо классов вычетов по $\bmod \mathfrak{p}^n\mathfrak{p}'^{n'}$ *области целостности* $|$ *изоморфно поэтому прямой сумме колец классов вычетов по* $\bmod \mathfrak{p}^n$, $\bmod \mathfrak{p}'^{n'}$ *области целостности* $|$, *или также прямой сумме колец классов вычетов по* $\bmod p^n$, $\bmod p^{n'}$ *области целостности* Γ.

Количество классов вычетов по $\bmod \mathfrak{p}^n\mathfrak{p}'^{n'}$ *равно поэтому* $p^{n+n'} = \mathfrak{N}(\mathfrak{p}^n\mathfrak{p}'^{n'})$.

Доказательство. Требования, предъявляемые к α системой двух сравнений, означают

$\alpha(w_k) \equiv a \bmod p^n$, $\alpha(w_k') \equiv a' \bmod p^{n'}$ хотя бы для одного $k \geqslant n,\ n'$. Им удовлетворяет, например, с $k = \max(n,\ n')$

$$\alpha = a\varepsilon_k + a'\varepsilon_k',$$

где ε_k, ε_k' — введенные в (3) п. 1 ортогональные друг другу идемпотенты.

Для частного случая $n = n'$ мы получаем

$$(\mathfrak{p}\mathfrak{p}')^n \mid \alpha \quad \text{равносильно} \quad p^n \mid \alpha$$

и, таким образом,

$$\alpha \equiv \beta \bmod (\mathfrak{p}\mathfrak{p}')^n \quad \text{равносильно} \quad \alpha \equiv \beta \bmod p^n,$$

причем соотношения справа понимаются в смысле элементарной теории делимости в |. Действительно, $(\mathfrak{p}\mathfrak{p}')^n \mid \alpha$, согласно определению, означает

$$p^n \mid \alpha(w_n), \qquad p^n \mid \alpha(w_n'),$$

и, согласно (4) п. 1, α обладает представлением

$$\alpha \equiv \alpha(w_n)\,\varepsilon_n + \alpha(w_n')\,\varepsilon_n' \bmod p^n.$$

Из только что доказанного следует:

Правило замены. *В соотношениях делимости и сравнениях делитель, соответственно модуль p^n можно заменять на $(\mathfrak{p}\mathfrak{p}')^n$, и наоборот.*

Мы видим, что полученный в Ia, п. 1 результат относительно структуры кольца классов вычетов по $\bmod p^n$ области целостности | подчинен более общему результату относительно структуры кольца классов вычетов по $\bmod \mathfrak{p}^n\mathfrak{p}'^{n'}$ области целостности |, содержащемуся в IVa*.

Наконец, мы введем для $\alpha \neq 0$ из | следующий способ записи: «$\alpha \longrightarrow \mathfrak{p}^m\mathfrak{p}'^{m'}$ для p» равносильно тому, что в α входят точно $\mathfrak{p}^m$ и $\mathfrak{p}'^{m'}$. В явном виде это означает

$$\left\{\begin{array}{ll} p^m \mid \alpha(w_k) & p^{m'} \mid \alpha(w_k') \\ p^{m+1} \nmid \alpha(w_k) & p^{m'+1} \nmid \alpha(w_k') \end{array}\right\} \quad \text{хотя бы для одного } k > m,\ m',$$

а тогда также и для всех $k > m,\ m'$.

При этом сопоставлении числам $\alpha \neq 0$ из | произведений степеней обоих простых дивизоров $\mathfrak{p}$, $\mathfrak{p}'$, являющихся делителями p, прежде всего, в силу гомоморфизма операций над компонентами операциям над числами из |, имеет место

Правило гомоморфизма. *Из*

$$\alpha \longrightarrow \mathfrak{p}^m\mathfrak{p}'^{m'}, \quad \beta \longrightarrow \mathfrak{p}^n\mathfrak{p}'^{n'} \quad \textit{для } p$$

следует

$$\alpha\beta \longrightarrow \mathfrak{p}^{m+n}\mathfrak{p}'^{m'+n'} \quad \textit{для } p.$$

Из правила вложения и правила для сопряженных относительно делимости получаются соответствующие правила для сопоставления дивизоров числам:

Правило вложения. *Для целого рационального* $a \neq 0$ $a \to (\mathfrak{p}\mathfrak{p}')^m$ *для* p *равносильно тому, что* $a \to p^m$ *для* p, *т. е. тому, что в* a *входит точно* p^m.

В частности, имеет место

$$p \to \mathfrak{p}\mathfrak{p}' \quad \text{для } p$$

и, более обще,

$$p^m \to (\mathfrak{p}\mathfrak{p}')^m \quad \text{для } p.$$

В силу последнего соотношения, мы видим, что введенный нами способ записи для сопоставления числам дивизоров согласуется с установленным выше правилом замены.

Правило для сопряженных. *Из* $\alpha \to \mathfrak{p}^m\mathfrak{p}'^{m'}$ *для* p *следует* $\alpha' \to \mathfrak{p}'^m\mathfrak{p}^m$ *для* p.

Наконец, из этих трех правил вместе получается:

Правило для норм. *Из* $\alpha \to \mathfrak{p}^m\mathfrak{p}'^{m'}$ *для* p *следует* $N(\alpha) \to p^{m+m'} = \mathfrak{N}(\mathfrak{p}^m\mathfrak{p}'^{m'})$ *для* p, *т. е. в* $N(\alpha)$ *входит точно степень числа* p, *равная* $\mathfrak{N}(\mathfrak{p}^m\mathfrak{p}'^{m'})$.

Прежде чем приступить к рассмотрению двух других случаев $\left(\frac{d}{p}\right) = 0$ и $\left(\frac{d}{p}\right) = -1$, для которых дело обстоит значительно проще, так как там числу p сопоставляется только один простой дивизор $\mathfrak{p}$, мы сделаем еще замечание о том, как в конкретных случаях определять показатели m, m' в сопоставленном числу α дивизоре:

$$\alpha \to \mathfrak{p}^m\mathfrak{p}'^{m'} \quad \text{для } p.$$

Из предшествующих определений принципиально ясно, как это можно сделать. Нужно только вычислить последовательности компонент $\alpha(w_k)$, $\alpha(w_k')$ из (1_k) п. 1 настолько далеко, чтобы входящие в них точные степени числа p больше не изменялись. Для этого нужно было бы вычислить достаточно далеко корни w_k, $w_k' \bmod p^k$ соответствующего ω главного многочлена $g(x)$, применяя указанное в п. 1 индуктивное требование. Однако этого можно избежать. Именно, мы покажем, что достаточно знать корни w, $w' \bmod p$ и образованные с их помощью компоненты $\alpha(w)$, $\alpha(w')$ из (1) п. 1, правда не для самого числа α, а для другого числа α_0, которое получается из α следующим образом.

Каждое целое число $\alpha \neq 0$ из K обладает на основании его представления

$$\alpha = a + b\omega \quad (a,\ b — \text{целые рациональные})$$

через базис поля K однозначно определенным разложением

$$\alpha = g\alpha_0$$

на его наибольший натуральный делитель $g=(a, b)$ и первообразное число

$$\alpha_0=a_0+b_0\omega, \quad \text{где } (a_0, b_0)=1.$$

Согласно правилам гомоморфизма, замены и вложения, для сопоставленного числу α дивизора получается при этом разложение

$$\mathfrak{p}^m\mathfrak{p}'^{m'}=(\mathfrak{p}\mathfrak{p}')^l\,\mathfrak{p}^{m_0} \quad \text{или} \quad (\mathfrak{p}\mathfrak{p}')^l\,\mathfrak{p}'^{m_0'}$$

с

$$l=\min(m, m')=m' \quad \text{или } m$$

и

$$m_0=m-l, \quad \text{соответственно } m_0'=m'-l.$$

Число l определяется здесь просто как показатель точной степени числа p, входящей в g, и

$$\alpha_0\to\mathfrak{p}^{m_0}, \quad \text{соответственно } \mathfrak{p}'^{m_0'} \text{ для } p.$$

Тогда остается только решить, какой из двух этих случаев имеет место для первообразного числа α_0, и определить показатель m_0, соответственно m_0'.

Вопрос о том, какой из двух случаев имеет место, сводится к альтернативе $\mathfrak{p}\,|\,\alpha_0$ или $\mathfrak{p}'\,|\,\alpha_0$ и потому, в соответствии с определением, может быть решен просто проверкой того, имеет ли место

$$\alpha_0(w)\equiv a_0+b_0w \quad \text{или} \quad \alpha_0(w')\equiv a_0+b_0w'\equiv 0 \bmod p.$$

Пусть, например, оказалось, что имеет место первый случай. Тогда, согласно правилу для норм, показатель m_0 определяется как показатель точной степени числа p, входящей в $N(\alpha_0)$.

Пример. В $\mathsf{K}=\mathsf{P}(\sqrt{-5})$ предположению $\left(\frac{d}{p}\right)=1$ удовлетворяет $p=3$. В соответствии с определением, простые дивизоры $\mathfrak{p}$, $\mathfrak{p}'$ соответствуют обоим рациональным корням многочлена

$$g(x)=x^2+5\equiv(x-1)(x+1) \bmod 3,$$

и притом так, что для $\alpha=a+b\sqrt{-5}$

$\mathfrak{p}\,|\,\alpha$ равносильно $a+b\equiv 0 \bmod 3$, $\mathfrak{p}'\,|\,\alpha$ равносильно $a-b\equiv 0 \bmod 3$.

Пусть нужно определить дивизор, сопоставленный числу $\alpha=6+3\sqrt{-5}$ для 3. Мы имеем $g=3$, $\alpha_0=2+\sqrt{-5}$ и

$$\alpha_0(1)\equiv 2+1\equiv 0 \bmod 3, \quad \alpha_0(-1)\equiv 2-1\equiv 1 \bmod 3.$$

Поэтому $\mathfrak{p}\,|\,\alpha_0$. Так как $N(\alpha_0)=9=3^2$, отсюда следует

$$\alpha_0\to\mathfrak{p}^2, \quad \alpha\to\mathfrak{p}^3\mathfrak{p}' \quad \text{для } 3.$$

б) Случай $\left(\frac{d}{p}\right)=0$ (p/d); один простой дивизор $\mathfrak{p}$, норма равна p.

Мы положим в основу представление

$$\alpha = a + b\pi \quad (a,\ b - \text{целые рациональные})$$

для целых чисел α из K, где π есть введенное в (5) п. 1 базисное число, и в зависимости от того, имеет ли место $n = 1$, или $n = 2n_0$, или $n = 2n_0 + 1$ с натуральным n_0, определим делимость $\mathfrak{p}^n \mid \alpha$ следующим образом:

$\mathfrak{p} \mid \alpha$ равносильно тому, что $p \mid \alpha$,

$\mathfrak{p}^{2n_0} \mid \alpha$ равносильно тому, что $p^{n_0} \mid \alpha$, т. е. что $p^{n_0} \mid (a, b)$,

однако

$\mathfrak{p}^{2n_0+1} \mid \alpha$ равносильно тому, что $p^{n_0+1} \mid a$.

Очевидно, что это определение делимости снова корректно, в том смысле, что выполняется требование

из $\mathfrak{p}^n \mid \alpha$ следует $\mathfrak{p}^{n'} \mid \alpha$ для всех натуральных $n' \leqslant n$.

Далее, очевидно также

Правило вложения. *Для целого рационального a*

$$\mathfrak{p}^{2n_0} \mid a \text{ равносильно } p^{n_0} \mid a.$$

Вследствие того что

$$\alpha' = a + b\pi' = (a + bS(\pi)) - b\pi,$$

мы, принимая во внимание установленное в (6) п. 1 сравнение $S(\pi) \equiv 0 \bmod p$, имеем далее

Правило для сопряженных. $\mathfrak{p}^n \mid \alpha$ *равносильно* $\mathfrak{p}^n \mid \alpha'$.

В соответствии с этим обстоятельством мы формально определяем здесь:

$$\mathfrak{p}' = \mathfrak{p},$$

т. е. устанавливаем, что просто дивизор $\mathfrak{p}$ должен быть инвариантен относительно порождающего автоморфизма поля K.

Для целых α, β, γ из K снова имеют место элементарные правила делимости:

из $\mathfrak{p}^n \mid \alpha$, $\mathfrak{p}^n \mid \beta$ следует $\mathfrak{p}^n \mid \alpha \pm \beta$,

из $\mathfrak{p}^n \mid \alpha$ следует $\mathfrak{p}^n \mid \gamma\alpha$.

Первое из них непосредственно вытекает из определения делимости, второе же получается из формулы для умножения

$$\gamma\alpha = (g + h\pi)(a + b\pi) = ga + (ha + gb)\pi + hb\pi^2 =$$
$$= (ga - hbN(\pi)) + (ha + gb + hbS(\pi))\pi$$

и установленного в (6) п. 1 сравнения $N(\pi) \equiv 0 \bmod p$.

Далее, согласно этим правилам, снова имеет место

11б. *Числа α из I, являющиеся кратными $\mathfrak{p}^n$, образуют идеал в I.*

В соответствии с предыдущим мы определим сравнимость

$$\alpha \equiv \beta \bmod \mathfrak{p}^n \quad \text{посредством} \quad \mathfrak{p}^n \mid \alpha - \beta.$$

Тогда снова имеют силу формальные правила для сложения, вычитания и перемножения сравнений:

IIIб. *Классы вычетов по* $\bmod \mathfrak{p}^n$ *области целостности* | *образуют кольцо.*

Далее, из определения делимости тотчас же следует

IVб. *Классы вычетов по* $\bmod \mathfrak{p}^n$ *области целостности* | *выражаются заданными в представлении через базис числами*

$$\alpha \equiv a + b\pi \bmod \mathfrak{p}^n \quad c \quad \left\{ \begin{array}{lll} a \bmod p, & (b=0) & \text{для } n=1 \\ a \bmod p^{n_0}, & b \bmod p^{n_0} & \text{для } n=2n_0 \\ a \bmod p^{n_0+1}, & b \bmod p^{n_0} & \text{для } n=2n_0+1 \end{array} \right\}.$$

Количество классов вычетов по $\bmod \mathfrak{p}^n$ *равно поэтому* $p^n = \mathfrak{N}(\mathfrak{p}^n)$.

Последнее утверждение дает нам и в этом случае содержательное истолкование нормы дивизора, определенной до этого только формально.

Для частного случая $n=1$ получается, что кольцо классов вычетов по $\bmod \mathfrak{p}$ области целостности | также и в этом случае является полем, изоморфным полю классов вычетов по $\bmod p$ области целостности Γ.

Для $n=2n_0$, согласно определению

$$\mathfrak{p}^{2n_0} \mid \alpha \quad \text{равносильно} \quad p^{n_0} \mid \alpha,$$

и потому

$$\alpha \equiv \beta \bmod \mathfrak{p}^{2n_0} \quad \text{равносильно} \quad \alpha \equiv \beta \bmod p^{n_0},$$

причем соотношения справа понимаются в смысле элементарной теории делимости в |. Поэтому имеет место

Правило замены. *В соотношениях делимости и сравнениях делитель соответственно модуль* p^{n_0} *можно заменять на* $\mathfrak{p}^{2n_0}$, *и наоборот.*

Из этого видно ($n_0=1$), что полученный в Iб, п. 1 результат относительно структуры кольца классов вычетов по $\bmod p$ области целостности | подчинен содержащемуся в IVб более общему результату относительно кольца классов вычетов по $\bmod \mathfrak{p}^n$ области целостности |.

Наконец, здесь из определения делимости непосредственно очевидно

Vб. *Для каждого* $\alpha \neq 0$ *из* | *существует наивысшая степень* $\mathfrak{p}^m$ *с* $\mathfrak{p}^m \mid \alpha$.

Мы снова будем кратко говорить: *в* α *входит точно* $\mathfrak{p}^m$.

Показатель m проще всего определить из разложения

$$\alpha = g\alpha_0 \quad (g - \text{натуральное число}, \ \alpha_0 \text{ первообразно}).$$

Если m_0 есть точный показатель, с которым p входит в g, и

$$\alpha_0 = a_0 + b_0\pi, \quad \text{где } (a_0, b_0) = 1,$$

то, очевидно,

$$m = \left\{ \begin{array}{ll} 2m_0 & \text{для } p \nmid a_0 \\ 2m_0 + 1 & \text{для } p \mid a_0 \text{ и потому } p \nmid b_0 \end{array} \right\}.$$

Наконец, определим для $\alpha \neq 0$ из $\mathfrak{l}$ следующий способ записи: $\alpha \longrightarrow \mathfrak{p}^m$ для p равносильно тому, что в α входит точно $\mathfrak{p}^m$.

Тогда прежде всего снова имеет место

Правило гомоморфизма. *Из*

$$\alpha \longrightarrow \mathfrak{p}^m, \quad \beta \longrightarrow \mathfrak{p}^n \quad \textit{для } p$$

следует

$$\alpha\beta \longrightarrow \mathfrak{p}^{m+n} \quad \textit{для } p.$$

Доказательство. Пусть

$\alpha = g\alpha_0$, $\beta = h\beta_0$ (g, h натуральные числа, α_0, β_0 первообразны) и

$$\alpha_0 = a_0 + b_0\pi, \quad \beta_0 = c_0 + d_0\pi, \quad \text{где } (a_0, b_0) = 1, \ (c_0, d_0) = 1.$$

Тогда

$$\alpha\beta = gh \cdot \alpha_0\beta_0$$

и, согласно уже использованной выше формуле для умножения,

$$\alpha_0\beta_0 = A_0 + B_0\pi$$

с

$$A_0 = a_0c_0 - b_0d_0N(\pi), \quad B_0 = a_0d_0 + b_0c_0 + b_0d_0S(\pi).$$

Так как для входящих в g, h точных степеней числа p дело обстоит аналогично доказываемому здесь правилу гомоморфизма, то, в силу только что сказанного, достаточно установить следующее:

Если $p \nmid a_0$, $p \nmid c_0$, то $p \nmid A_0$.

Если $p \nmid a_0$, но $p \mid c_0$ и потому $p \nmid d_0$, то $p \mid A_0$, $p \nmid B_0$.

Если $p \mid a_0$, $p \mid c_0$ и потому $p \nmid b_0$, $p \nmid d_0$, то $p \mid A_0$, $p \mid B_0$, $p^2 \mid A_0$.

Правильность этих высказываний вытекает из установленных в (6), (7) п. 1 соотношений делимости

$$p \mid S(\pi), \ p \mid N(\pi), \ p^2 \nmid N(\pi).$$

Из правила вложения и правила для сопряженных относительно делимости получаются соответствующие правила для сопоставления дивизоров числам:

Правило вложения. *Для целого рационального* $a \neq 0$ $a \to \mathfrak{p}^{2m_0}$ *для* p *равносильно тому, что* $a \to p^{m_0}$ *для* p, *т. е. тому, что в* a *входит точно* p^{m_0}.

В частности, имеет место

$$p \to \mathfrak{p}^2 \text{ для } p$$

и, более обще,

$$p^{m_0} \to \mathfrak{p}^{2m_0} \text{ для } p.$$

Из последнего соотношения видно, что введенный нами способ записи для сопоставления числам дивизоров снова согласуется с доказанным выше правилом замены.

Правило для сопряженных. *Из* $\alpha \to \mathfrak{p}^m$ *для* p *следует* $\alpha' \to \mathfrak{p}^m$ *для* p.

Наконец, из этих трех правил вместе получается

Правило для норм. *Из* $\alpha \to \mathfrak{p}^m$ *для* p *следует* $N(\alpha) \to p^m = \mathfrak{N}(\mathfrak{p}^m)$ *для* p, *т. е. точная степень числа* p, *входящая в* $N(\alpha)$, *равна* $\mathfrak{N}(\mathfrak{p}^m)$.

в) *Случай* $\left(\frac{d}{p}\right) = -1$; *один простой дивизор* $\mathfrak{p}$, *норма равна* p^2. В этом случае мы определим делимость

$$\mathfrak{p}^n \mid \alpha \text{ посредством } p^n \mid \alpha$$

в смысле элементарной теории делимости в $\mathfrak{l}$, т. е. посредством $p^n \mid (a, b)$, если $\alpha = a + b\omega$ есть представление числа α через целочисленный базис поля $\mathfrak{K}$; в соответствии с этим мы определим и сравнимость

$$\alpha \equiv \beta \bmod \mathfrak{p}^n \text{ посредством } \alpha \equiv \beta \bmod p^n$$

в смысле элементарной теории делимости в $\mathfrak{l}$.

Так как при этих определениях дело только в введении нового способа записи, мы можем удовольствоваться кратким перечнем правил и теорем, аналогичных правилам и теоремам для двух предыдущих случаев.

Из $\mathfrak{p}^n \mid \alpha$ следует $\mathfrak{p}^{n'} \mid \alpha$ для всех натуральных $n' \leqslant n$.

Правило вложения. *Для целого рационального* a

$$\mathfrak{p}^n \mid a \text{ равносильно } p^n \mid a.$$

Правило для сопряженных. $\mathfrak{p}^n \mid \alpha$ *равносильно* $\mathfrak{p}^n \mid \alpha'$.

В соответствии с этим мы здесь снова определим

$$\mathfrak{p}' = \mathfrak{p}.$$

IIв. *Числа* α *из* $\mathfrak{l}$, *являющиеся кратными* $\mathfrak{p}^n$, *образуют идеал в* $\mathfrak{l}$.

IIIв. *Классы вычетов по* $\bmod \mathfrak{p}^n$ *области целостности* $\mathfrak{l}$ *образуют кольцо.*

IVв. *Классы вычетов по* $\bmod \mathfrak{p}^n$ *области целостности* $\mathfrak{l}$ *выражаются заданными в представлении через базис числами*

$$\alpha \equiv a + b\omega \bmod \mathfrak{p}^n \text{ с } a, b \bmod p^n.$$

Количество классов вычетов по $\bmod \mathfrak{p}^n$ *равно поэтому* $p^{2n} = \mathfrak{N}(\mathfrak{p}^n)$.

Последнее снова дает содержательное истолкование введенной раньше чисто формально нормы дивизора.

Правило замены. *В соотношениях делимости и сравнениях делитель соответственно модуль* p^n *можно заменять на* $\mathfrak{p}^n$, *и наоборот.*

Здесь это сразу следует из определения.

Vв. *Для каждого* $\alpha \neq 0$ *из* $\mathfrak{l}$ *существует наивысшая степень* $\mathfrak{p}^m$ *с* $\mathfrak{p}^m \mid \alpha$.

Мы снова будем кратко говорить: *в* α *входит точно* $\mathfrak{p}^m$.

Показатель m определяется из разложения

$$\alpha = g\alpha_0 \ (g \text{ натуральное число, } \alpha_0 \text{ первообразно}),$$

причем здесь он будет просто точным показателем, с которым p входит в g.

Для $\alpha \neq 0$ из $\mathfrak{l}$ мы снова определим способ записи:

«$\alpha \longrightarrow \mathfrak{p}^m$ для p» равносильно тому, что в α входит точно $\mathfrak{p}^m$.

Правило гомоморфизма. *Из*

$$\alpha \longrightarrow \mathfrak{p}^m, \ \beta \longrightarrow \mathfrak{p}^n \text{ для } p$$

следует

$$\alpha\beta \longrightarrow \mathfrak{p}^{m+n} \text{ для } p.$$

Доказательство. Подобно предыдущим случаям здесь проще показать, что $\mathfrak{p}$ не входит в произведение $\alpha_0\beta_0$ двух первообразных чисел α_0, β_0. Но если α_0, β_0 первообразны, то заведомо имеет место

$$\alpha_0 \not\equiv 0 \bmod p, \quad \beta_0 \not\equiv 0 \bmod p.$$

Так как в настоящем случае кольцо классов вычетов по $\bmod p$ области целостности $\mathfrak{l}$ является, согласно I в п. 1, полем, то действительно следует также

$$\alpha_0\beta_0 \not\equiv 0 \bmod p.$$

Правило вложения. *Для целого рационального* $a \neq 0$ $a \longrightarrow \mathfrak{p}^n$ *для* p *равносильно тому, что* $a \longrightarrow p^m$ *для* p, *т. е. тому, что в* a *входит точно* p^m.

В частности

$$p \longrightarrow \mathfrak{p} \text{ для } p,$$

и более обще

$$p^m \longrightarrow \mathfrak{p}^m \text{ для } p.$$

Правило для сопряженных. *Из* $\alpha \to \mathfrak{p}^m$ *для* p *следует* $\alpha' \to \mathfrak{p}^m$ *для* p.

Правило для норм. *Из* $\alpha \to \mathfrak{p}^m$ *для* p *следует* $N(\alpha) \to p^{2m} = \mathfrak{N}(\mathfrak{p}^m)$ *для* p, *т. е. точная степень* p, *входящая в* $N(\alpha)$, *равна* $\mathfrak{N}(\mathfrak{p}^m)$.

Для совместного обзора мы объединим полученные нами для трех случаев $\left(\frac{d}{p}\right) = 1,\ 0,\ -1$ результаты в виде следующей схемы.

Случай	$\left(\frac{d}{p}\right)=1$	$\left(\frac{d}{p}\right)=0$ $(p\mid d)$	$\left(\frac{d}{p}\right)=-1$
Простые дивизоры $\mathfrak{p}$, сопоставленные p . .	$\mathfrak{p},\ \mathfrak{p}'$	$\mathfrak{p}$	$\mathfrak{p}$
Дивизоры, сопряженные с $\mathfrak{p}$	$\mathfrak{p}',\ \mathfrak{p}$	$\mathfrak{p}$	$\mathfrak{p}$
Норма $\mathfrak{N}(\mathfrak{p})$	p	p	p^2
Количество классов вычетов по mod $\mathfrak{p}^n$ . .	$\mathfrak{N}(\mathfrak{p}^n) = p^n$	$\mathfrak{N}(\mathfrak{p}^n) = p^n$	$\mathfrak{N}(\mathfrak{p}^n) = p^{2n}$
Гомоморфное сопоставление дивизора числу $\alpha \neq 0$ из I	$\mathfrak{p}^m \mathfrak{p}'^{m'}$	$\mathfrak{p}^m$	$\mathfrak{p}^m$
Вложение $a \neq 0$ из Γ ($a \to p^m$ для p) . . .	$(\mathfrak{p}\mathfrak{p}')^m$	$\mathfrak{p}^{2m}$	$\mathfrak{p}^m$
Простое число $p \to$ . .	$\mathfrak{p}\mathfrak{p}'$	$\mathfrak{p}^2$	$\mathfrak{p}$
Сопряженное $\alpha' \to$ . . .	$\mathfrak{p}^{m'}\mathfrak{p}'^m$	$\mathfrak{p}^m$	$\mathfrak{p}^m$
Норма $N(\alpha) \to$	$p^{m+m'} = \mathfrak{N}(\mathfrak{p}^m \mathfrak{p}'^{m'})$	$p^m = \mathfrak{N}(\mathfrak{p}^m)$	$p^{2m} = \mathfrak{N}(\mathfrak{p}^m)$

В соотношениях из § 15, п. 5, повторенных еще раз в начале п. 2, мы для всех трех случаев имеем

$$p \to \left(\prod_{\mathfrak{p} \text{ для } p} \mathfrak{p}\right)^{e_p} \text{ для } p\,\mathfrak{N}(\mathfrak{p}) = p^{f_p},$$ количество простых дивизоров g_p.

При этом

e_p называется показателем ветвления простого дивизора $\mathfrak{p}$,

f_p называется порядком простого дивизора $\mathfrak{p}$.

Первое название связано с тем, как обстоит дело при сопоставлении простому числу p простых дивизоров. Порядок же f_p равен степени поля классов вычетов по mod $\mathfrak{p}$ области целостности I над простым полем (полем классов вычетов по mod p области целостности Γ). Относительно поведения p при сопоставлении

ему простых дивизоров в трех различных случаях также говорят:

p разлагается, если $g_p = 2$; случай $\left(\frac{d}{p}\right) = 1$.

p остается простым, если $f_p = 2$; случай $\left(\frac{d}{p}\right) = -1$.

p разветвляется, если $e_p = 2$; случай $\left(\frac{d}{p}\right) = 0$ $(p \mid d)$.

В дальнейшем мы будем располагать три различных типа простых чисел p именно в этом, с теоретической точки зрения самом лучшем порядке. До сих пор мы этого не делали потому, что в предшествовавших исследованиях случай разветвления стоял по методу исследования ближе к случаю разложения, чем к случаю, когда p остается простым.

3. Основные теоремы арифметики. Теперь мы будем считать, как уже делали это в § 15, п. 5 простые дивизоры $\mathfrak{p}$, сопоставленные всем простым рациональным числам p, образующими элементами свободной мультипликативной абелевой группы $\mathfrak{D}$, элементы которой

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_\mathfrak{p}} \left| \begin{array}{l} a_\mathfrak{p} - \text{целые рациональные} \\ a_\mathfrak{p} \neq 0 \text{ лишь для конечного множества } \mathfrak{p} \end{array} \right.$$

мы будем называть *дивизорами* поля K. В этой *группе дивизоров* $\mathfrak{D}$ поля K мы следующим образом определим понятие целого дивизора:

$\mathfrak{a}$ целый равносильно тому, что $\left\{ \begin{array}{r} a_\mathfrak{p} \text{ целые рациональные} \geqslant 0 \\ a_\mathfrak{p} > 0 \text{ лишь для конечного} \\ \text{множества } \mathfrak{p} \end{array} \right\}$,

т. е. формально аналогично разложению на простые множители целых рациональных чисел (см. § 1, п. 5, теорема целостности). Опираясь на это понятие целостности, мы определим понятие *делимости дивизоров* посредством:

$$\mathfrak{a} \mid \mathfrak{b} \text{ равносильно тому, что } \frac{\mathfrak{b}}{\mathfrak{a}} - \text{целый},$$

т. е. формально аналогично определению делимости для рациональных чисел. Тогда имеет место формальный аналог критерию делимости из § 2, п. 1:

$$\text{для } \mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_\mathfrak{p}},\ \mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{b_\mathfrak{p}} \left| \begin{array}{l} \mathfrak{a} \mid \mathfrak{b} \text{ равносильно тому, что} \\ a_\mathfrak{p} \leqslant b_\mathfrak{p} \text{ для всех } \mathfrak{p} \end{array} \right. .$$

Подобно этому мы перенесем на дивизоры также и другие понятия делимости: *общий наибольший делитель*, *общее наименьшее*

кратное, взаимная простота, числитель, знаменатель, введенные в § 2, п. 2—6. Далее мы определим, что уже делалось в § 15, п. 5, норму дивизора посредством формулы

$$\mathfrak{N}(\mathfrak{a}) = \prod_{\mathfrak{p}} \mathfrak{N}(\mathfrak{b})^{a_{\mathfrak{p}}};$$

она будет мультипликативной функцией элементов из $\mathfrak{D}$ со значениями, равными положительным рациональным числам. Для специальных целых дивизоров $\mathfrak{p}^n$, $\mathfrak{p}^n\mathfrak{p}'^{n'}$ мы молчаливо использовали это последнее определение уже и выше, в п. 2. Наконец, мы определим сопряженный с $\mathfrak{a}$ дивизор $\mathfrak{a}'$ посредством формулы

$$\mathfrak{a}' = \prod_{\mathfrak{p}} \mathfrak{p}'^{a_{\mathfrak{p}}},$$

т. е. так, что каждый простой дивизор $\mathfrak{p}$ заменяется сопряженным с ним простым дивизором $\mathfrak{p}'$ с сохранением показателя степени $a_{\mathfrak{p}}$.

Пусть теперь дано сначала целое число $\alpha \neq 0$ из K и пусть соответственно трем случаям из п. 2,

$$\alpha \longrightarrow \mathfrak{p}^{m_{\mathfrak{p}}}\,\mathfrak{p}'^{m_{\mathfrak{p}'}},\ \text{соответственно } \mathfrak{p}^{m_{\mathfrak{p}}},\ \text{соответственно } \mathfrak{p}^{m_{\mathfrak{p}}} \text{ для } p \quad (1)$$

с целыми рациональными $m_{\mathfrak{p}}$, $m_{\mathfrak{p}'}$, $\geqslant 0$, однозначно определенными числом α для каждого рационального простого числа p. Так как при этом, согласно правилам для норм из п. 2, имеет место

$$N(\alpha) \longrightarrow \mathfrak{p}^{m_{\mathfrak{p}}+m_{\mathfrak{p}'}},\ \text{соответственно } p^{m_{\mathfrak{p}}},\ \text{соответственно } p^{2m_{\mathfrak{p}}} \text{ для } p$$

и так как в целое рациональное число $N(\alpha) \neq 0$ входит лишь конечное множество рациональных простых чисел p с показателями > 0, то среди показателей $m_{\mathfrak{p}}$, $m_{\mathfrak{p}'}$ лишь конечное множество > 0. Поэтому определение

$$\alpha \longrightarrow \mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}}, \quad (2)$$

где $\mathfrak{p}$ должно теперь пробегать все простые дивизоры поля K, дает однозначно определенный числом α целый дивизор поля K в указанном выше смысле. Согласно правилам гомоморфизма, вложения, правилам для сопряженных и для норм из п. 2, для этого сопоставления числам дивизоров имеют место:

Правило гомоморфизма. *Из* $\alpha \longrightarrow \mathfrak{a}$, $\beta \longrightarrow \mathfrak{b}$ *следует* $\alpha\beta \longrightarrow \mathfrak{a}\mathfrak{b}$.

Правило вложения. *Для целого рационального*

$$a \cong \prod_{p} p^{m_p}$$

имеет место

$$\mathfrak{a} \to \prod_{p\text{—разложимое}} (\mathfrak{p}\mathfrak{p}')^{m_p} \cdot \prod_{p\text{—простое}} \mathfrak{p}^{m_p} \cdot \prod_{p\text{—разветвленное}} \mathfrak{p}^{2m_p}.$$

При этом мы различаем три случая из п. 2 с помощью указанных в конце п. 2 названий.

Правило для сопряженных. *Из* $\alpha \to \mathfrak{a}$ *следует* $\alpha' \to \mathfrak{a}'$.

Правило для норм. *Из* $\alpha \to \mathfrak{a}$ *следует* $N(\alpha) \cong \mathfrak{N}(\mathfrak{a})$.

В то время как в правиле для норм мы можем в силу основной теоремы элементарной теории чисел (см. II′, п. 5, § 1), поставить справа знак ассоциированности $\cong$, однако мы еще не имеем права ставить этот знак также и в определении (2) вместо знака сопоставления $\to$. Действительно мы еще не знаем, определяется ли число α однозначно с точностью до ассоциированных сопоставленным ему дивизором $\mathfrak{a}$; это будет установлено только ниже (при доказательстве утверждения VI). Заметим, однако, что в (2) нам, конечно, уже нет надобности делать какое-либо добавление вроде «для p» из п. 2, так как теперь α ставится в некоторое отношение не к отдельному простому рациональному числу p, а одновременно ко всем простым рациональным числам. Поэтому, в частности, особо выделенные утверждения в правилах вложения из п. 2 теперь могут быть записаны значительно проще:

$$\left.\begin{array}{ll} p \to \mathfrak{p}\mathfrak{p}' & \text{для } \left(\frac{d}{p}\right) = 1 \\ p \to \mathfrak{p} & \text{для } \left(\frac{d}{p}\right) = -1 \\ p \to \mathfrak{p}^2 & \text{для } \left(\frac{d}{p}\right) = 0 \end{array}\right\}. \tag{3}$$

Только что изложенные факты переносятся также и на любые (не обязательно целые) числа $\alpha \neq 0$ из K. Каждое такое число может быть различными способами представлено в виде отношения

$$\alpha = \frac{\mu_1}{\nu_1} = \frac{\mu_2}{\nu_2} = \dots$$

целых чисел $\mu_1, \mu_2, \dots, \nu_1, \nu_2, \dots$ из K. Одно из таких представлений, с натуральным знаменателем, мы получим, если в представлении $\alpha = a + b\omega$ через целочисленный базис $1, \omega$ поля K выделим общий наименьший знаменатель коэффициентов a, b; однако прибегать специально к этому, однозначно определенному представлению в виде отношения целых чисел нам нет необходимости. Если

$$\mu_1 \to \mathfrak{m}_1, \quad \mu_2 \to \mathfrak{m}_2, \dots$$
$$\nu_1 \to \mathfrak{n}_1, \quad \nu_2 \to \mathfrak{n}_2, \dots$$

в смысле нашего определения (2), то из числовых равенств

$$\mu_1 \nu_2 = \mu_2 \nu_1, \ \ldots$$

в силу правила гомоморфизма следуют равенства для дивизоров

$$\mathfrak{m}_1 \mathfrak{n}_2 = \mathfrak{m}_2 \mathfrak{n}_1, \ \ldots$$

Отсюда вытекает, что отношение дивизоров

$$\mathfrak{a} = \frac{\mathfrak{m}_1}{\mathfrak{n}_1} = \frac{\mathfrak{m}_2}{\mathfrak{n}_2} = \ldots$$

однозначно определено числом α, так что в качестве обобщения (2) мы получаем, что можно писать

$$\alpha \longrightarrow \mathfrak{a}.$$

Таким образом, любому числу $\alpha \neq 0$ из K однозначно сопоставляется некоторый дивизор $\mathfrak{a}$ поля K. При этом, очевидно, сохраняются все указанные выше правила.

После того как мы определили явный способ сопоставления $\alpha \longrightarrow \mathfrak{a}$ числам из K дивизоров из $\mathfrak{D}$, мы перечислим теперь основные теоремы арифметики квадратичных полей K в том виде, как они получаются для этого специального случая из общих формулировок § 15, п. 5, причем каждый раз мы будем отмечать, в какой мере эти теоремы уже доказаны установленными только что правилами и что еще остается показать для завершения их доказательств.

Теорема соответствия. *Посредством соответствия* $\alpha \longrightarrow \mathfrak{a}$ *фактор-группа* $\mathsf{K}^\times/\mathsf{E}$ *мультипликативной группы поля* K *по группе единиц поля* K *изоморфно отображается на некоторую подгруппу* $\mathfrak{D}_0$ *группы* $\mathfrak{D}$ *дивизоров поля* K (см. § 15, п. 5, фиг. 9).

Из правила гомоморфизма уже следует, что $\mathsf{K}^\times$ гомоморфно отображается на некоторую подгруппу $\mathfrak{D}_0$ группы $\mathfrak{D}$. Остается показать, что это отображение есть изоморфизм для $\mathsf{K}^\times/\mathsf{E}$, т. е. что в единичный дивизор 1 отображается в точности подгруппа E группы $\mathsf{K}^\times$. Говоря подробнее, нам остается доказать

VI. *Если* ε *есть единица поля* K, *то* $\varepsilon \longrightarrow 1$, *и наоборот.*

Теорема целостности. *При соответствии* $\alpha \longrightarrow \mathfrak{a}$ *целым числам* $\alpha \neq 0$ *из* K *соответствуют целые дивизоры* $\mathfrak{a}$ *из* $\mathfrak{D}$, *и наоборот.*

Согласно определению сопоставления числам дивизоров, мы уже можем считать установленным, что всем целым числам $\alpha \neq 0$ соответствуют целые дивизоры $\mathfrak{a}$. Остается показать, что целые дивизоры $\mathfrak{a}$ соответствуют только целым числам $\alpha \neq 0$. Точнее, нам остается доказать

VII. *Если* $\alpha \longrightarrow \mathfrak{a}$ *и* $\mathfrak{a}$ *целый, то* α *также целое.*

Теорема о вложении. *Для простого рационального числа p имеет место*

$$p \to \left(\prod_{\mathfrak{p}|p} \mathfrak{p}\right)^{e_p},$$

где показатель e_p определяется через количество g_p простых дивизоров $\mathfrak{p}$, делящих p, и показатель степени f_p в $\mathfrak{N}(\mathfrak{p}) = p^{f_p}$ посредством соотношения $e_p f_p g_p = 2$.

Это было полностью доказано выше в (3). Согласно правилу гомоморфизма, отсюда можно получить вид закона соответствия для любых рациональных чисел $a \neq 0$; поэтому нет необходимости указывать его явно, как мы делали в правилах вложения из п. 2 в целях достижения наибольшей ясности.

Теорема о сопряженных. *Из $\alpha \to \mathfrak{a}$ следует $\alpha' \to \mathfrak{a}'$.*

Эта теорема, представляющая собой просто доказанное выше правило для сопряженных, не была приведена в § 15, п. 5, так как в рассматривавшемся там более общем случае для точной ее формулировки пришлось бы вдаваться в излишние подробности.

Теорема о норме. *Из $\alpha \to \mathfrak{a}$ следует $N(\alpha) \cong \mathfrak{N}(\mathfrak{a})$; таким образом, $|N(\alpha)| = \mathfrak{N}(\mathfrak{a})$.*

Это есть попросту доказанное выше правило для норм.

Теорема о дискриминанте. *$e_p = 2$ имеют место тогда и только тогда, когда p входит в дискриминант d поля K.*

Правильность этой теоремы следует из (3).

Теорема о конечности числа классов. *Подгруппа $\mathfrak{D}_0$ тех дивизоров поля K, которые соответствуют некоторым числам из K, имеет конечный индекс h в группе $\mathfrak{D}$ всех дивизоров поля K.*

Как уже было сказано для общего случая в § 15, п. 5,

дивизоры из $\mathfrak{D}_0$ называются *главными дивизорами поля* K,

классы фактор-группы $\mathfrak{D}/\mathfrak{D}_0$ называются *классами дивизоров поля* K,

фактор-группа $\mathfrak{D}/\mathfrak{D}_0$ называется *группой классов дивизоров поля* K,

индекс $[\mathfrak{D} : \mathfrak{D}_0] = h$ называется *числом классов поля* K.

Таким образом, нам надо доказать

VIII. *Число классов h поля K конечно.*

Теперь мы обратимся к еще остающимся доказательствам, причем сначала мы докажем VII, затем опирающееся на него VI, а доказательством VIII, которое еще требует некоторой подготовки, мы займемся в конце этого параграфа.

Доказательство VII (нетривиальная часть теоремы целостности). Мы проведем доказательство косвенным путем, а именно, покажем, что:

Если $\alpha \to \mathfrak{a}$ и $\mathfrak{a}$ дробно, то и α также дробно.

Пусть

$$\alpha = g\alpha_0 \quad (g\text{—рациональное, } > 0,\ \alpha_0 \text{ первообразно})$$

есть разложение, неоднократно использованное в п. 2 для целых $\alpha \neq 0$ из K, которое для любого (не обязательно целого) $\alpha \neq 0$ из K определяется совершенно так же из представления $\alpha = a + b\omega$ числа α через базис поля K:

$$g = (a, b); \quad a = ga_0 \quad b = gb_0; \quad \alpha_0 = a_0 + b_0\omega \text{ с } (a_0, b_0) = 1.$$

При этом для дробного α рациональная часть g является дробной, в то время как первообразная часть α_0 попрежнему есть целое число. Пусть, далее, $\alpha_0 \longrightarrow \mathfrak{a}_0$. Тогда, согласно правилу гомоморфизма,

$$\mathfrak{a} = g\mathfrak{a}_0,$$

причем мы должны считать, что рациональная часть g разложена на простые множители, которые потом заменены дивизорами в соответствии с теоремой о вложении.

Так как α_0—целое, то, в силу тривиальной части теоремы целостности, верной уже в силу определения, будет целым также и $\mathfrak{a}_0$. Так как, кроме того, α_0 первообразно, то, согласно определениям соответствия из п. 2, множители, которые вносят в $\mathfrak{a}_0$

разлагающиеся, остающиеся простыми, разветвляющиеся

простые числа p, имеют вид

$$\mathfrak{p}^{m_\mathfrak{p}} \text{ или } \mathfrak{p}'^{m_{\mathfrak{p}'}}, \qquad \mathfrak{p}^0, \qquad \mathfrak{p}^0 \text{ или } \mathfrak{p}^1.$$

Так как α *по предположению дробно*, рациональная часть g имеет знаменатель $n > 1$ (общий наименьший знаменатель чисел a, b). Если этот знаменатель n разложить на простые множители и произвести замены

$$p \longrightarrow \mathfrak{p}\mathfrak{p}', \qquad \mathfrak{p}, \qquad \mathfrak{p}^2$$

в соответствии с (3), то мы убедимся, что при образовании произведения $g\mathfrak{a}_0$ от каждого простого делителя p числа n останется в знаменателе по крайней мере один простой дивизор $\mathfrak{p}$ (соответственно $\mathfrak{p}'$). Следовательно, $\mathfrak{a}$ также является дробным, что и требовалось доказать.

Доказательство VI (изоморфизм в теореме соответствия).

а) Пусть ε—единица и пусть $\varepsilon \longrightarrow \mathfrak{e}$. Тогда, в силу гомоморфизма в теореме соответствия, мы будем иметь $\varepsilon^{-1} \longrightarrow \mathfrak{e}^{-1}$. Так как ε, ε^{-1}—целые, то из тривиальной части теоремы целостности следует, что $\mathfrak{e}$, $\mathfrak{e}^{-1}$—также целые. Но это возможно только для $\mathfrak{e} = 1$.

б) Пусть $\varepsilon \longrightarrow 1$. Тогда, как только что перед этим, мы получаем $\varepsilon^{-1} \longrightarrow 1$. По нетривиальной части теоремы целостности это озна-

чает, что ε, ε^{-1}—целые. Поэтому, согласно определению, ε есть единица.

Доказав, таким образом, теорему соответствия, мы можем теперь для сопоставления числам дивизоров употреблять вместо знака сопоставления $\rightarrow$ знак ассоциированности $\cong$. Таким образом, теперь мы будем писать:

$$\alpha \cong \mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}} \left| \begin{array}{l} a_{\mathfrak{p}} \text{ целые рациональные} \\ a_{\mathfrak{p}} \neq 0 \text{ лишь для конечного множества } \mathfrak{p} \end{array} \right. ,$$

и говорить о разложении числа α на простые дивизоры поля K. Это разложение следует рассматривать как обобщение разложения на простые множители в P, а теорему соответствия—как обобщение основной теоремы элементарной теории чисел (см. § 1, п.4, 5).

Теорема целостности обобщает теорему целостности элементарной теории чисел (см. § 1, п. 5) и в этом смысле дает нам новую, чисто арифметическую характеристику области целостности целых чисел поля K. Действительно, согласно этой теореме, целые $\alpha \neq 0$ из K характеризуются тем, что все простые дивизоры $\mathfrak{p}$ поля K входят в α с показателями $a_{\mathfrak{p}} \geqslant 0$. В отличие от данного в § 16, п. 3 алгебраического определения понятия целостности, теперь уже мы не говорим об алгебраическом уравнении, которому удовлетворяет α.

Выражающие теорему вложения соотношения (3) будут теперь записываться в виде

$$\left\{ \begin{array}{l} p \cong \mathfrak{p}\mathfrak{p}' \ (\text{с } \mathfrak{p} \neq \mathfrak{p}' \text{ и } \mathfrak{N}(\mathfrak{p}) = \mathfrak{N}(\mathfrak{p}') = p) \ \text{для } \left(\frac{d}{p}\right) = 1 \\ p \cong \mathfrak{p} \ (\text{с } \mathfrak{N}(\mathfrak{p}) = p^2) \ \text{для } \left(\frac{d}{p}\right) = -1 \\ p \cong \mathfrak{p}^2 \ (\text{с } \mathfrak{N}(\mathfrak{p}) = p) \ \text{для } \left(\frac{d}{p}\right) = 0 \end{array} \right. , \qquad (4)$$

т. е. совершенно аналогично закону разложения для специальных полей в § 16, п. 6. Соотношения (4) вместе с высказываниями относительно нормы представляют собой закон разложения для поля K.

Теорема о норме дает содержательное истолкование формально введенного понятия нормы $\mathfrak{N}(\mathfrak{a})$ дивизора $\mathfrak{a}$ в случае главного дивизора $\mathfrak{a} \cong \alpha$; норма дивизора соответствует тогда норме $N(\alpha)$ числа α. Содержательное истолкование $\mathfrak{N}(\mathfrak{a})$ для любых целых дивизоров $\mathfrak{a}$ мы получим в п. 4 из других соображений.

Теорема о сопряженных вместе с теоремой о норме дает для главных дивизоров $\mathfrak{a} \cong \alpha$ правило

$$\mathfrak{N}(\mathfrak{a}) \cong \alpha\alpha',$$

аналогичное определению числовой нормы $N(\alpha) = \alpha\alpha'$. Это правило сохраняется в силе также и для любых дивизоров $\mathfrak{a}$;

действительно, для простых дивизоров, в соответствии с определением и в силу закона разложения, в каждом из трех случаев имеет место

$$\mathfrak{N}(\mathfrak{p}) \cong \mathfrak{p}\mathfrak{p}'.$$

Отметим еще, что равенства вида

$$\mathfrak{a} = \gamma\mathfrak{b}$$

между дивизорами $\mathfrak{a}$, $\mathfrak{b}$ поля K, в которых, кроме того, фигурирует еще числовой множитель $\gamma \neq 0$ из поля K, мы всегда понимаем в том смысле, что γ заменяется соответствующим главным дивизором $\mathfrak{c} \cong \gamma$, как мы это уже делали, в частности, для рационального $\gamma = g$ в доказательстве утверждения VII. В более общей форме, чем в указанном доказательстве, а именно, для любых дивизоров поля K, имеет место

IX. *Каждый дивизор $\mathfrak{a}$ поля K обладает однозначно определенным разложением*

$$\mathfrak{a} = g\mathfrak{a}_0$$

с рациональной частью $g > 0$ и первообразной частью $\mathfrak{a}_0$.

При этом дивизор $\mathfrak{a}_0$ поля K называется первообразным, если он целый и не имеет целых рациональных делителей, кроме 1. Указанное разложение получится, если из сомножителей

$$\mathfrak{p}^{a_\mathfrak{p}}\,\mathfrak{p}'^{a_{\mathfrak{p}'}}, \qquad \mathfrak{p}^{a_\mathfrak{p}}, \qquad \mathfrak{p}^{a_\mathfrak{p}},$$

соответствующих разлагающимся, остающимся простыми, разветвляющимся простым числам p, извлечь наибольшие рациональные части

$$p^{\min(a_\mathfrak{p}, a_{\mathfrak{p}'})}, \qquad \mathfrak{p}^{a_\mathfrak{p}}, \qquad \mathfrak{p}^{a_\mathfrak{p}},$$

где в последнем случае мы положили $a_\mathfrak{p} = 2q_\mathfrak{p} + 0, 1$. В соответствии с этим, первообразный дивизор $\mathfrak{a}_0$ составляется из сомножителей вида

$$\mathfrak{p}^{m_\mathfrak{p}}\,\mathfrak{p}'^{0} \text{ или } \mathfrak{p}^{0}\,\mathfrak{p}'^{m_{\mathfrak{p}'}}, \qquad \mathfrak{p}^{0}, \qquad \mathfrak{p}^{0} \text{ или } \mathfrak{p}^{1},$$

где в первом случае имеет место $m_{\mathfrak{p}'}$, соответственно $m_\mathfrak{p} = 0$. В частности, для главного дивизора $\mathfrak{a} \cong \alpha$ дивиз р $\mathfrak{a}_0 \cong \alpha_0$ также будет главным, причем число α_0 первообразно, что мы, исходя от чисел, установили уже при доказательстве утверждения VII.

Так как $\mathfrak{a}_0$ отличается от $\mathfrak{a}$ только множителем, равным главному дивизору, и потому $\mathfrak{a}_0$ и $\mathfrak{a}$ принадлежат к одному и тому же классу дивизоров, мы получаем в качестве следствия:

X. *Каждый класс дивизоров поля K может быть представлен посредством целого и даже первообразного дивизора.*

Если K имеет число классов $h = 1$, и потому каждый дивизор является главным, то это имеет место, в частности, для всех

простых дивизоров $\mathfrak{p}$ поля K. Соответствующие им числа $\pi \cong \mathfrak{p}$ являются простыми числами поля K, так как наличие нетривиального разложения числа π повлекло бы за собой наличие нетривиального разложения для $\mathfrak{p}$. Поэтому однозначное разложение на простые дивизоры превращается в этом случае в однозначное разложение на простые множители.

Обратно, если в K имеет место однозначное разложение на простые множители, то для него имеет силу закон разложения из § 16, п. 6. Тогда сравнение его с общим законом разложения (4) показывает, что все время $\pi \cong \mathfrak{p}$, так что все простые дивизоры, а потому и все вообще дивизоры поля K являются главными. Следовательно, K имеет в этом случае число классов $h = 1$.

Этим доказано

XI. *Однозначное разложение на простые множители в поле* K *имеет место тогда и только тогда, когда число классов* $h = 1$.

Как было показано в XVIII, п. 6, § 16, это обстоятельство заведомо имеет место, если в K существует алгоритм Евклида. Но существуют и квадратичные поля K с $h = 1$, но без алгоритма Евклида. Примеры таких полей мы укажем в конце п. 5.

4. Сравнимость, классы вычетов, идеалы. Пусть

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}} \left\{ \begin{array}{l} m_{\mathfrak{p}} \geqslant 0 \text{ целые рациональные} \\ m_{\mathfrak{p}} > 0 \text{ лишь для конечного множества } \mathfrak{p} \end{array} \right\}$$

есть целый дивизор поля K. Определим для чисел α из I отношение делимости

$$\mathfrak{m} \,|\, \alpha \text{ посредством } \mathfrak{p}^{m_{\mathfrak{p}}} \,|\, \alpha \text{ для всех } \mathfrak{p}$$

и соответственно этому определим для чисел α, β из I сравнимость

$$\alpha \equiv \beta \bmod \mathfrak{m} \text{ посредством } \alpha \equiv \beta \bmod \mathfrak{p}^{m_{\mathfrak{p}}} \text{ для всех } \mathfrak{p},$$

т. е. через одновременное выполнение соотношений делимости, соответственно сравнимости для всех входящих в $\mathfrak{m}$ степеней $\mathfrak{p}^{m_{\mathfrak{p}}}$ простых дивизоров; эти последние соотношения были определены нами еще в п. 2. При этом в действительности, конечно, речь идет лишь о конечном множестве простых дивизоров $\mathfrak{p}$ с $m_{\mathfrak{p}} > 0$, или, другими словами, простых делителях $\mathfrak{p}$ дивизора $\mathfrak{m}$. Согласно п. 3, наши определения могут быть высказаны также в форме

$$\mathfrak{m} \,|\, \alpha \text{ равносильно тому, что } \frac{\alpha}{\mathfrak{m}} \text{ целый},$$

$$\alpha \equiv \beta \bmod \mathfrak{m} \text{ равносильно тому, что } \frac{\alpha - \beta}{\mathfrak{m}} \text{ целый},$$

т. е. аналогично определениям для чисел из Γ в § 1, п. 2 и § 4, п. 1.

Если, в частности, $\mathfrak{m} \cong \mathfrak{p}$—главный дивизор, то, на основании теоремы целостности, эти соотношения переходят, с соответствующим изменением обозначений, в соотношения элементарной теории делимости в $\mathfrak{l}$.

На основании теорем IIa, б, в и IIIa, б, в из п. 2, имеет место

XII. *Числа α из $\mathfrak{l}$, являющиеся кратными дивизора $\mathfrak{m}$, образуют идеал в $\mathfrak{l}$. Классы вычетов по* $\bmod \mathfrak{m}$ *области целостности $\mathfrak{l}$ образуют кольцо.*

Для специального случая, когда $\mathfrak{m} = \mathfrak{p}^{m_\mathfrak{p}} \mathfrak{p}'^{m_{\mathfrak{p}'}}$ есть произведение степеней двух сопряженных простых дивизоров $\mathfrak{p}$, $\mathfrak{p}'$, являющихся делителями простого числа p, разлагающегося в $\mathfrak{K}$, необходимые определения были даны уже в п. 2 и там же в IIa*, IIIa* были высказаны соответствующие теоремы. Сейчас мы докажем общий аналог имеющейся там теоремы IVa*.

XIII. *Если для конечного множества простых дивизоров $\mathfrak{p}$, делящих $\mathfrak{m}$, задана система чисел $\alpha_\mathfrak{p}$ из $\mathfrak{l}$, то существует число α из $\mathfrak{l}$ с*

$$\alpha \equiv \alpha_\mathfrak{p} \bmod \mathfrak{p}^{m_\mathfrak{p}} \text{ для всех } \mathfrak{p} \mid \mathfrak{m}.$$

Поэтому кольцо классов вычетов по $\bmod \mathfrak{m}$ *области целостности $\mathfrak{l}$ изоморфно прямой сумме колец классов вычетов по* $\bmod \mathfrak{p}^{m_\mathfrak{p}}$ *области целостности $\mathfrak{l}$ для простых делителей $\mathfrak{p}$ дивизора $\mathfrak{m}$.*

Количество классов вычетов по $\bmod \mathfrak{m}$ *равно, таким образом,* $\prod_\mathfrak{p} \mathfrak{N}(\mathfrak{p}^{m_\mathfrak{p}}) = \mathfrak{N}(\mathfrak{m})$.

Для последнего утверждения следует принять во внимание соответствующие утверждения, содержащиеся уже в теоремах IVa, б, в из п. 2.

Доказательство. Без ограничения общности можно считать, что система сравнений, разрешимость которой нам нужно доказать, посредством присоединения некоторых новых требований и повышения показателей степеней в модулях приведена к такому виду, что для разлагающихся простых чисел p все время фигурируют оба сопряженных простых дивизора $\mathfrak{p}$, $\mathfrak{p}'$ с одинаковыми показателями $m_\mathfrak{p} = m_{\mathfrak{p}'} = m_p$, а для разветвляющихся простых чисел p показатели $m_\mathfrak{p} = 2m_p$ четны; действительно, требования, накладываемые на α, от этого могут только усилиться. Это сводится к повышению модуля $\mathfrak{m}$ до его наименьшего целого рационального кратного m (между прочим, если $\mathfrak{m} = g\mathfrak{m}_0$ с целым рациональным $g > 0$ и первообразным $\mathfrak{m}_0$, то m представляется в простой форме $m = g\mathfrak{N}(\mathfrak{m}_0)$).

Пусть теперь для каждого разлагающегося p система сравнений

$$\alpha_p \equiv \alpha_\mathfrak{p} \bmod \mathfrak{p}^{m_p}, \quad \alpha_p \equiv \alpha_{\mathfrak{p}'} \bmod \mathfrak{p}'^{m_p}$$

разрешена, в соответствии с IVa*, п. 2 посредством класса вычетов $\alpha_p \bmod p^{m_p}$. Тогда остается решить систему сравнений

$$\alpha \equiv \alpha_p \bmod p^{m_p}.$$

Пусть представления чисел α_p через базис имеют вид:

$$\alpha_p = a_p + b_p\omega, \quad (a_p,\ b_p \text{ из } \Gamma).$$

В соответствии с этим будем искать α в виде

$$\alpha = a + b\omega \quad (a,\ b \text{ из } \Gamma).$$

Тогда исследуемые сравнения в | сводятся к системе сравнений

$$\left.\begin{array}{l} a \equiv a_p \\ b \equiv b_p \end{array}\right\} \bmod p^{m_p}$$

в Γ. Но по основной теореме из § 4, п. 9, эта последняя система имеет в качестве решения некоторую пару классов вычетов a, $b \bmod m$.

Результат XIII сводит вопрос о структуре кольца классов вычетов по $\bmod \mathfrak{m}$ области целостности | к вопросу о структуре колец классов вычетов по модулям, равным степеням простых дивизоров. Для случая разложимости эта структура определяется в IVa, п. 2. Для двух других случаев результаты в IVб, п. 2 еще не полностью определяют эту структуру. Этот пробел нетрудно восполнить, однако мы не будем вдаваться здесь подробнее в этот вопрос.

Как было обещано в п. 3, результат XIII дает содержательное истолкование нормы $\mathfrak{N}(\mathfrak{m})$ любого целого дивизора $\mathfrak{m}$ как количества классов вычетов по $\bmod \mathfrak{m}$. Для частного случая целого рационального модуля $\mathfrak{m} \cong m$ этот результат согласуется с полученным еще из элементарной теории делимости в | фактом, что количество классов вычетов по $\bmod m$ области целостности | равно m^2.

Подобно применению X, XI в п. 9, § 4 результат XIII позволяет нам также изучить структуру группы классов вычетов по $\bmod \mathfrak{m}$, взаимно простых с модулем, о которой для частного случая $\mathfrak{m} \cong m$ мы говорили уже в § 16, п. 5 в связи с (18), (19). Как и в III, п. 3, § 4, все числа α одного и того же класса вычетов по $\bmod \mathfrak{m}$ области целостности | имеют с $\mathfrak{m}$ один и тот же общий наибольший делитель $(\alpha, \mathfrak{m})$. Классы вычетов с делителем $(\alpha, \mathfrak{m}) = 1$ называются взаимно простыми с модулем классами вычетов области целостности |. Они образуют мультипликативную группу, называемую группой классов вычетов по $\bmod \mathfrak{m}$, взаимно простых с модулем, области целостности |. Класс вычетов $\alpha \bmod \mathfrak{m}$ взаимно прост с модулем тогда и только тогда, когда взаимно просты с модулями все его компоненты $\alpha \bmod \mathfrak{p}^{m_p}$

для всех простых дивизоров $\mathfrak{p}$, делящих $\mathfrak{m}$. Поэтому группа классов вычетов по $\bmod \mathfrak{m}$, взаимно простых с модулем, есть прямое произведение групп классов вычетов по $\bmod \mathfrak{p}^{m_\mathfrak{p}}$, взаимно простых с модулем. Поэтому для количества $\Phi(\mathfrak{m})$ классов вычетов по $\bmod \mathfrak{m}$, взаимно простых с модулем, имеет место

$$\Phi(\mathfrak{m}) = \prod_{\mathfrak{p}|\mathfrak{m}} \Phi(\mathfrak{p}^{m_\mathfrak{p}}).$$

Класс вычетов $\alpha \bmod \mathfrak{p}^{m_\mathfrak{p}}$ взаимно прост с модулем тогда и только тогда, когда $\alpha \not\equiv 0 \bmod \mathfrak{p}$. Классы вычетов $\alpha \bmod \mathfrak{p}^{m_\mathfrak{p}}$ с $\alpha \equiv 0 \bmod \mathfrak{p}$ образуют аддитивную подгруппу всех $\mathfrak{N}(\mathfrak{p}^{m_\mathfrak{p}})$ классов вычетов по $\bmod \mathfrak{p}^{m_\mathfrak{p}}$; соответствующая фактор-группа представляется $\mathfrak{N}(\mathfrak{p})$ различными вычетами $\alpha \bmod \mathfrak{p}$, так что указанная подгруппа имеет индекс $\mathfrak{N}(\mathfrak{p})$ и, следовательно, порядок $\mathfrak{N}(\mathfrak{p}^{m_\mathfrak{p}})/\mathfrak{N}(\mathfrak{p})$. Поэтому

$$\Phi(\mathfrak{p}^{m_\mathfrak{p}}) = \mathfrak{N}(\mathfrak{p}^{m_\mathfrak{p}}) - \frac{\mathfrak{N}(\mathfrak{p}^{m_\mathfrak{p}})}{\mathfrak{N}(\mathfrak{p})} = \mathfrak{N}(\mathfrak{p}^{m_\mathfrak{p}})\left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p})}\right).$$

Тем самым мы получаем:

XIII′. *Группа классов вычетов по* $\bmod \mathfrak{m}$, *взаимно простых с модулем, области целостности* | *есть прямое произведение групп классов вычетов по* $\bmod \mathfrak{p}^{m_\mathfrak{p}}$, *взаимно простых с модулем, для всех простых дивизоров* $\mathfrak{p}$, *делящих* $\mathfrak{m}$.

Количество взаимно простых с модулем классов вычетов по $\bmod \mathfrak{m}$ *области целостности* | *равно*

$$\Phi(\mathfrak{m}) = \mathfrak{N}(\mathfrak{m}) \prod_{\mathfrak{p}|\mathfrak{m}} \left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p})}\right).$$

Последняя формула аналогична формуле (1) п. 8, § 4 для количества $\varphi(m)$ классов вычетов по $\bmod m$, взаимно простых с модулем, области целостности Γ. Для частного случая $\mathfrak{m} \cong m$, с которым мы имели дело в § 16, п. 5, отношение $\Phi(m)/\varphi(m)$ вычисляется следующим образом. Отношение $\varphi(m)/m$ есть произведение обратных величин тех сомножителей в выражении для дзета-функции $\zeta(s)$ при $s=1$, которые появляются там за счет простых делителей p числа m. Аналогично, $\Phi(m)/\mathfrak{N}(m) = \Phi(m)/m^2$ есть произведение обратных величин тех сомножителей в выражении для дзета-функции $\zeta_\kappa(s)$ при $s=1$, которые появляются там за счет простых делителей $\mathfrak{p}$ числа m. Поэтому отношение $\Phi(m)/m\varphi(m)$ равно произведению обратных величин тех сомножителей в выражении для L-функции $\dfrac{\zeta_\kappa(s)}{\zeta(s)} = L(s\,|\chi)$ при $s=1$, которые соответствуют простым делителям p числа m,

Следовательно,

$$\frac{\Phi(m)}{\varphi(m)} = m \prod_{p|m} \left(1 - \left(\frac{d}{p}\right)\frac{1}{p}\right).$$

В специальном случае $m = 2$ (для $2 \nmid d$) мы уже использовали этот факт в § 16, п. 5 при выводе утверждения XVII.

Аналогично утверждениям IV, V п. 3 § 4 здесь также возможно деление в кольце классов вычетов по $\bmod \mathfrak{m}$ области целостности $\mathfrak{l}$ на классы вычетов, взаимно простые с модулем, и только на них, причем если деление возможно, то оно однозначно; поэтому только эти классы вычетов не являются делителями нуля, в то время как все классы, не взаимно простые с модулем, являются собственными делителями нуля.

Наконец, аналогично II, п. 2, § 5 также и здесь имеет место то, что группа классов вычетов по $\bmod \mathfrak{p}$, взаимно простых с модулем, для простого дивизора $\mathfrak{p}$ поля $\mathfrak{K}$ циклична, потому что, согласно результатам IVa, б, в п. 2, она представляет собой мультипликативную группу конечного поля (из $\mathfrak{N}(\mathfrak{p}) = p$, соответственно p^2 элементов). Порождающий элемент этой группы снова называется первообразным корнем по $\bmod \mathfrak{p}$. В случаях разложимости и разветвления, когда $\mathfrak{N}(\mathfrak{p}) = p$, первообразный корень $w \bmod p$ является таковым и по $\bmod \mathfrak{p}$. В том случае, когда p остается простым и $\mathfrak{N}(\mathfrak{p}) = p^2$, это заведомо не так, потому что $w \bmod \mathfrak{p}$ имеет лишь порядок $p - 1$ вместо требуемого порядка $\mathfrak{N}(\mathfrak{p}) - 1 = p^2 - 1$; первообразный корень по $\bmod \mathfrak{p}$ в этом случае обязательно иррационален.

Идеал, который, согласно XII, образуют числа α из $\mathfrak{l}$, кратные $\mathfrak{m}$, мы будем кратко обозначать в дальнейшем через $(\mathfrak{m})$. В частности, (1) означает единичный идеал в $\mathfrak{l}$, состоящий из всех чисел α области целостности $\mathfrak{l}$.

Относительно идеала $(\mathfrak{m})$ мы докажем следующий факт, который будет важен для нас впоследствии:

Теорема о базисе. *Для каждого целого дивизора* $\mathfrak{m}$ *поля* $\mathfrak{K}$ *идеал* $(\mathfrak{m})$, *состоящий из чисел* α *из* $\mathfrak{l}$, *кратных* $\mathfrak{m}$, *обладает таким двучленным базисом* μ_1, μ_2, *что эти кратные* (*и только они*) *обладают однозначным представлением вида*

$$\alpha = a_1\mu_1 + a_2\mu_2 \quad (a_1, a_2 — \textit{целые рациональные}).$$

Если

$$\begin{pmatrix} \mu_1 \\ \mu_2 \end{pmatrix} = M \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

с матрицей M *из целых рациональных чисел, есть подстановка, переводящая целочисленный базис* ω_1, ω_2 *поля* $\mathfrak{K}$ (*единичного идеала* (1) *области целостности* $\mathfrak{l}$) *в базис* μ_1, μ_2

идеала $\mathfrak{m}$, *то для абсолютной величины определителя имеем*

$$\| M \| = \mathfrak{N}(\mathfrak{m}),$$

откуда для дискриминанта базиса получается

$$d(\mu_1, \mu_2) = \mathfrak{N}(\mathfrak{m})^2 d.$$

Последнее из этих утверждений получается после того, как будут доказаны два первых факта, подобно тому как в (5), (6) п. 1, § 16 и V, п. 3, § 16.

Доказательство. а) Выразим числа α из $(\mathfrak{m})$ в виде

$$\alpha = a + b\omega \quad (a, b — \text{целые рациональные})$$

через специальный целочисленный базис 1, ω поля K. Так как $(\mathfrak{m})$ есть идеал, то каждая из совокупностей: $(\mathfrak{m})_1$, состоящая из всех лежащих в $(\mathfrak{m})$ целых рациональных чисел $\alpha = a$, и $(\mathfrak{m})_2$, состоящая из целых рациональных чисел, фигурирующих в качестве коэффициента b в числах из $(\mathfrak{m})$, образует идеал в Γ. Отметим также, что $(\mathfrak{m})_1$, $(\mathfrak{m})_2$ состоят не только из 0, так как числа $\mathfrak{N}(\mathfrak{m})$, $\mathfrak{N}(\mathfrak{m})\,\omega$ заведомо лежат в $(\mathfrak{m})$. По основной теореме об идеалах в Γ (см. § 2, п. 8), каждое из множеств $(\mathfrak{m})_1$, $(\mathfrak{m})_2$ состоит из всех целых рациональных кратных от наименьших натуральных чисел m_1, m_2, содержащихся в этих множествах. Пусть в соответствии с этим

$$\left\{ \begin{array}{l} \mu_1 = m_1 \\ \mu_2 = m_2' + m_2\omega \end{array} \right\} \tag{1}$$

являются наименьшим натуральным числом из $(\mathfrak{m})$ и числом из $(\mathfrak{m})$ с наименьшим натуральным коэффициентом при ω. Тогда для любого $\alpha = a + b\omega$ из $(\mathfrak{m})$ прежде всего имеет место $b = a_2 m_2$ с целым рациональным a_2, и потому

$$\alpha - a_2\mu_2 = a - a_2 m_2'$$

есть целое рациональное число из $(\mathfrak{m})$, а тогда необходимо должно быть $a - a_2 m_2' = a_1 m_1$ с целым рациональным a_1, откуда

$$\alpha - a_2\mu_2 - a_1\mu_1 = 0,$$

что и дает нам искомое представление через базис; действительно, очевидно, что, наоборот, вместе с μ_1, μ_2 в $(\mathfrak{m})$ лежит также и каждое число $\alpha = a_1\mu_1 + a_2\mu_2$ с целыми рациональными a_1, a_2.

б) Для полученного только что специального базиса μ_1, μ_2 идеала $(\mathfrak{m})$ и специального целочисленного базиса 1, ω поля K матрица перехода от второго к первому имеет вид

$$M = \begin{pmatrix} m_1 & 0 \\ m_2' & m_2 \end{pmatrix}$$

с абсолютной величиной определителя

$$\| M \| = m_1 m_2.$$

Чтобы доказать, что количество классов вычетов по $\bmod \mathfrak{m}$ тоже равно $\mathfrak{N}(\mathfrak{m}) = m_1 m_2$, мы покажем, что $m_1 m_2$ целых чисел

$$\rho = r + s\omega \quad \text{с} \begin{cases} r = 0, \ldots, m_1 - 1 \\ s = 0, \ldots, m_2 - 1 \end{cases}$$

образуют полную систему вычетов по $\bmod \mathfrak{m}$. Действительно, если

$$\alpha = a + b\omega \quad (a, b — \text{целые рациональные})$$

есть любое число из $\mathfrak{l}$, то существует одна и только одна пара целых рациональных чисел a_1, a_2, таких, что в

$$\alpha - (a_1\mu_1 + a_2\mu_2) = (a + b\omega) - (a_1 m_1 + a_2 m_2' + a_2 m_2 \omega) =$$
$$= (a - a_1 m_1 - a_2 m_2') + (b - a_2 m_2)\,\omega$$

коэффициенты при $1, \omega$ принадлежат к наименьшим системам вычетов $r \bmod m_1$, $s \bmod m_2$, т. е. α сравнимо по $\bmod \mathfrak{m}$ с одним и только одним из таких чисел ρ.

Всевозможные базисы идеалов $(\mathfrak{m})$ соответственно $(1)^{-}$ получаются из μ_1, μ_2, соответственно ω_1, ω_2 посредством применения всех целочисленных линейных подстановок S, T с абсолютными величинами определителей $\| S \|, \| T \| = 1$. Так как при этом матрица M переходит в SMT^{-1}, т. е. абсолютная величина определителей $\| M \|$ не меняется, наше утверждение верно для любых базисов, а не только для специальных базисов, использованных в доказательстве.

Относительно сконструированного в доказательстве специального базиса μ_1, μ_2 идеала $(\mathfrak{m})$ мы заметим еще следующее. Числа m_1, m_2 имеют для $\mathfrak{m}$ инвариантное истолкование; именно,

m_1 есть наименьшее натуральное кратное дивизора $\mathfrak{m}$,

m_2 есть наибольший натуральный делитель дивизора $\mathfrak{m}$.

Первое непосредственно следует из определения m_1 как наименьшего натурального числа из $(\mathfrak{m})$. Второе не так очевидно; мы докажем его следующим образом.

Пусть

$$\mathfrak{m} = g\mathfrak{m}_0$$

есть разложение из IX, п. 3 целого дивизора $\mathfrak{m}$ на его наибольший натуральный делитель g и первообразную часть $\mathfrak{m}_0$. Как отмечалось уже в доказательстве утверждения XIII, наименьшее

натуральное кратное m_1 дивизора $\mathfrak{m}$ определяется тогда в виде

$$m_1 = g\,\mathfrak{N}(\mathfrak{m}_0).$$

Поэтому имеет место

$$gm_1 = g^2\,\mathfrak{N}(\mathfrak{m}_0) = \mathfrak{N}(g\mathfrak{m}_0) = \mathfrak{N}(\mathfrak{m}).$$

Так как, по доказанному, также

$$m_2 m_1 = \mathfrak{N}(\mathfrak{m}),$$

то мы действительно получаем $g = m_2$, что и требовалось доказать.

То, что m_2 является общим делителем всех чисел из $(\mathfrak{m})$, можно доказать еще и так. Вместе с μ_1, μ_2 к $(\mathfrak{m})$ принадлежат также и кратные $\omega\mu_1$, $\omega\mu_2$. Их представления через целочисленный базис $1, \omega$ имеют вид

$$\begin{aligned} \omega\mu_1 &= \qquad\qquad m_1\omega, \\ \omega\mu_2 &= -tm_2 + (sm_2 + m_2')\,\omega, \end{aligned}$$

где s, t, как и раньше, обозначают целые рациональные коэффициенты главного уравнения $\omega^2 = s\omega - t$. При этом, в соответствии с определением m_2, коэффициенты m_1, $sm_2 + m_2'$, а потому также и m_2', делятся на m_2. Если на основании этого записать базис (1) идеала $(\mathfrak{m})$ в виде

$$\left\{ \begin{aligned} \mu_1 &= m_2 m_0 \\ \mu_2 &= m_2(-w + \omega) \end{aligned} \right\} \tag{2}$$

с некоторым натуральным m_0 и целым рациональным w, то мы убедимся, что m_2 есть наибольший натуральный делитель всех чисел из $(\mathfrak{m})$. Отсюда, однако, сразу еще не следует доказанное выше более сильное высказывание относительно m_2, ибо мы нигде не получили, что m_2 делит дивизор $\mathfrak{m}$.

Обычно (2) называют канонической формой базиса идеала $(\mathfrak{m})$. Если сократить его на наибольший натуральный делитель $g = m_2$ дивизора $\mathfrak{m}$, то получится базис

$$\begin{aligned} \mu_{10} &= m_0 \\ \mu_{20} &= -w + \omega \end{aligned}$$

первообразной части $\mathfrak{m}_0$ и притом тоже в канонической форме. По теореме о базисе, m_0 имеет здесь значение

$$m_0 = \mathfrak{N}(\mathfrak{m}_0)$$

и w есть целое рациональное число со свойством

$$\omega \equiv w \bmod \mathfrak{m}_0,$$

т. е. мы получили обобщение положенных в п. 1, 2 в основу корней w, $w' \bmod p$. То, что для первообразного дивизора $\mathfrak{m}_0$

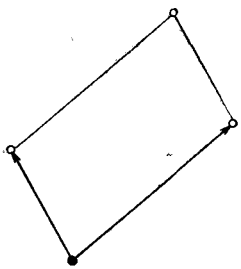
класс вычетов, в котором лежит ω, а тем самым и каждый класс вычетов по $\bmod \mathfrak{m}_0$, представим целым рациональным числом, для нас уже не является неожиданным.

При геометрической иллюстрации на K-плоскости из § 16, п. 2 идеал (1) целых чисел поля K представляется, согласно (6) п. 3, § 16, в виде точечной решетки с площадью основного параллелограма

$$G = \frac{1}{2}\sqrt{|d|}.$$

Аналогично, идеал $(\mathfrak{m})$, состоящий из чисел из I, кратных целому дивизору $\mathfrak{m}$ поля K, в силу теоремы о базисе, представляется в виде некоторой подрешетки решетки всех целых чисел; основной параллелограм этой подрешетки имеет площадь

$$G_{\mathfrak{m}} = \frac{1}{2}\mathfrak{N}(\mathfrak{m})\sqrt{|d|}. \qquad (3)$$



Фиг. 16.

Классы вычетов по $\bmod \mathfrak{m}$ мы получим, параллельно перенося подрешетку $(\mathfrak{m})$ так, чтобы ее нулевая точка попадала в точки основной решетки (1). Каждый класс вычетов, таким образом, состоит из полной системы точек основной решетки, гомологично расположенных по отношению к подрешетке. Поэтому полная система вычетов $\rho \bmod \mathfrak{m}$ получается в виде совокупности всех точек ρ основной решетки, лежащих в основном параллелограме подрешетки. При этом из каждых двух параллельных сторон к основному параллелограму нужно всегда причислять только одну и только одну из четырех угловых точек (фиг. 16).

Чтобы наглядно пояснить, как из основной решетки (1) выделяется подрешетка $(\mathfrak{m})$, целесообразно ввести в рассмотрение еще и промежуточную подрешетку $(\mathfrak{m}_0)$, соответствующую первообразной части $\mathfrak{m}_0$ дивизора $\mathfrak{m}$ и выбрать основные параллелограмы следующим образом:

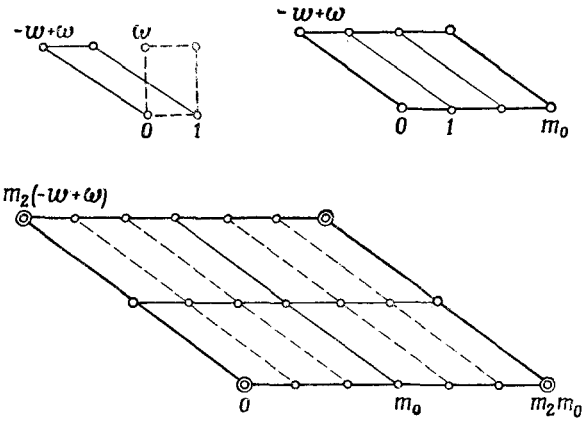
для подрешетки $(\mathfrak{m})$ посредством канонического базиса
$$m_2(m_0, -w+\omega),$$
для промежуточной решетки $(\mathfrak{m}_0)$ посредством канонического базиса $(m_0, -w+\omega)$,

для основной решетки (1) посредством базиса $(1, -w+\omega)$.

Для основной решетки (1) это означает сдвиг на $-w$ в направлении, параллельном первой оси основного параллелограма, соответствующего обычному базису $(1, \omega)$ (фиг. 17а). Промежу-

точная решетка $(\mathfrak{m}_0)$ получается тогда посредством растяжения с коэффициентом m_0 в направлении, параллельном первой оси (фиг. 17б), а подрешетка $(\mathfrak{m})$ получается из $(\mathfrak{m}_0)$ посредством растяжения с коэффициентом m_2 в обоих направлениях (фиг. 17в).

Нужно отчетливо подчеркнуть, что не всякая подрешетка основной решетки (1) имеет вид $(\mathfrak{m})$, т. е. соответствует некоторому целому дивизору $\mathfrak{m}$ поля K, в чем можно убедиться



Фиг. 17.

простым подсчетом. Так, например, существует ровно три подрешетки с удвоенной площадью основного параллелограмма, именно, подрешетки с основными параллелограммами

$$(2, \omega),\ (2, -1+\omega),\ (1, 2\omega),$$

в то время как целых дивизоров $\mathfrak{m}$ поля K с $\mathfrak{N}(\mathfrak{m}) = 2$ существует только 2, 0, 1, в зависимости от того, является ли в поле K число 2 разлагающимся, простым или разветвляющимся.

В то время как, следуя в обосновании арифметики в K идеям Куммера, мы в заключение получили теорию идеалов, Дедекинд, напротив, исходил из этой теории. В этот вопрос мы здесь вдаваться не будем, но заметим только, что при нашем обосновании мы определяли идеалы $(\mathfrak{m})$ как совокупности кратных целых дивизоров $\mathfrak{m}$; однако эти идеалы принципиально сами могут быть использованы для обоснования арифметики в K, причем дивизоры $\mathfrak{m}$ придется тогда вводить как общие наибольшие делители чисел из идеалов $(\mathfrak{m})$.

5. Конечность числа классов. Теперь мы приступаем к доказательству высказывания VIII из п. 3 о том, что число классов h поля K конечно.

Сначала мы дадим короткое чисто арифметическое доказательство, которое по методу примыкает к доказательству существования нетривиальной единицы вещественного квадратичного поля в § 16, п. 4, а именно, опирается на принцип Дирихле. В заключение мы дадим другое доказательство, использующее методы основанной Минковским геометрии чисел, а именно, опирающееся на знаменитую теорему Минковского о выпуклой области. Эту теорему мы докажем только для одного, нужного нам здесь случая.

Как уже установлено в X, п. 3, каждый класс дивизоров поля может быть представлен целым (и даже первообразным) дивизором. Таким образом, при заданном классе C дивизоров поля K в обратном классе C^{-1} существует целый дивизор $\mathfrak{m}$ поля K. Мы фиксируем этот дивизор $\mathfrak{m}$, а $\mathfrak{a}$ заставим пробегать все целые дивизоры из C. Тогда все время

$$\mathfrak{a}\mathfrak{m} \cong \mathfrak{a} \tag{1}$$

есть главный дивизор, и при этом α пробегает в точности все отличные от нуля числа из $\mathfrak{a}$, являющиеся кратными $\mathfrak{m}$, т. е. все отличные от нуля числа соответствующего $\mathfrak{m}$ идеала $(\mathfrak{m})$, если вместе с α рассматривать все время и все ассоциированные с ним. Если из каждого класса ассоциированных выбрать по одному представителю α, то по теореме соответствия из п. 3 мы получим взаимно однозначное соответствие между этой полной системой неассоциированных чисел $\alpha \neq 0$ из $(\mathfrak{m})$ и целыми дивизорами $\mathfrak{a}$ из C. При этом, согласно теореме о норме из п. 3, имеет место

$$\mathfrak{N}(\mathfrak{a})\,\mathfrak{N}(\mathfrak{m}) = |N(\alpha)|. \tag{2}$$

Отсюда получается:

XIV. *Целые дивизоры* $\mathfrak{a}$ *из класса* C *дивизоров поля* K *с*

$$\mathfrak{N}(\mathfrak{a}) \leqslant N$$

на основании (1) *взаимно однозначно соответствуют полной системе неассоциированных чисел* $\alpha \neq 0$ *из* $(\mathfrak{m})$ *с*

$$|N(\alpha)| \leqslant N\,\mathfrak{N}(\mathfrak{m}),$$

где $\mathfrak{m}$ *есть фиксированный целый дивизор из* C^{-1}, *и* N *— любое натуральное число.*

Этот факт явится основой обоих наших доказательств конечности числа классов h и, кроме того, также и основой для точного определения h в § 18. Для доказательства конечности мы используем тот факт (который непосредственно следует

из определения нормы дивизора), что для заданной — а потому также и для ограниченной — нормы существует лишь конечное множество целых дивизоров из K, и потому будем оперировать в XIV с постоянной границей N. Для точного определения h мы применим предельный переход $N \to \infty$.

Первое доказательство конечности числа классов. Имеет место

XV. *Для каждого целого дивизора* $\mathfrak{m}$ *поля* $\mathsf{K} = \mathsf{P}(\sqrt{d})$ *существует число* $\alpha \neq 0$ *из* $(\mathfrak{m})$ *с*

$$|N(\alpha)| \leqslant \left(\frac{3+\sqrt{|d|}}{2}\right)^2 \mathfrak{N}(\mathfrak{m}).$$

Отсюда, согласно XIV, следует

XVI. *В каждом классе* C *дивизоров поля* $\mathsf{K} = \mathsf{P}(\sqrt{d})$ *существует целый дивизор* $\mathfrak{a}$ *с*

$$\mathfrak{N}(\mathfrak{a}) \leqslant \left(\frac{3+\sqrt{|d|}}{2}\right)^2$$

Так как существует только конечное множество целых дивизоров $\mathfrak{a}$ поля K с этим свойством, отсюда и будет следовать далее, что существует только конечное число классов C дивизоров поля K.

Доказательство. Пусть m есть целая часть числа $\sqrt{\mathfrak{N}(\mathfrak{m})}$, т. е.

$$m^2 \leqslant \mathfrak{N}(\mathfrak{m}) < (m+1)^2$$

Так как, согласно XIII, п. 4, целые числа поля K распределены в $\mathfrak{N}(\mathfrak{m})$ классов вычетов по $\bmod \mathfrak{m}$, среди $(m+1)^2$ целых чисел

$$\rho = r + s\omega \quad \text{с } r,\ s = 0,\ 1,\ \ldots,\ m$$

заведомо существуют, в силу принципа Дирихле, два различных числа ρ_1, ρ_2 с $\rho_1 \equiv \rho_2 \bmod \mathfrak{m}$. Тогда их разность $\alpha = \rho_1 - \rho_2$ будет отличным от нуля числом из $(\mathfrak{m})$, представление которого через базис имеет вид

$$\alpha = a + b\omega \quad \text{с } |a|,\ |b| \leqslant m.$$

Отсюда следует

$$|N(\alpha)| \leqslant (1+|\omega|)(1+|\omega'|)m^2 \leqslant (1+|\omega|)(1+|\omega'|)\mathfrak{N}(\mathfrak{m}).$$

Так как всегда имеет место

$$|\omega|,\ |\omega'| \leqslant \frac{1+\sqrt{|a|}}{2},$$

мы получаем наше утверждение.

Последняя оценка, а вместе с ней и граница в XV, XVI в мнимом случае и в случае $D \equiv 2, 3 \bmod 4$ может быть еще несколько улучшена. Однако для нас это не так важно, потому что наше второе доказательство и без того даст нам лучшую оценку, из которой мы тогда выведем еще некоторые следствия. Для самой же теоремы о конечности числа классов важно только то, что вообще существует какая-то граница такого рода.

Пусть на плоскости $\mathfrak{E}$ дана точечная решетка. Одну из точек решетки (обозначим ее O) мы выберем в качестве начала координат и будем обычным образом оперировать с точками X на $\mathfrak{E}$ как с векторами $\overrightarrow{OX}$.

Под *выпуклой областью* $\mathfrak{B}$ *на плоскости* $\mathfrak{E}$ *с центром в* 0 мы будем понимать ограниченное замкнутое множество точек со следующими двумя свойствами:

1) *Выпуклость.* Вместе с каждыми двумя точками X_1, X_2 из $\mathfrak{B}$ к $\mathfrak{B}$ принадлежит также и каждая точка

$$X = \lambda_1 X_1 + \lambda_2 X_2 \quad (\lambda_1,\ \lambda_2 \text{ вещественные},\ \geqslant 0,\ \lambda_1 + \lambda_2 = 1).$$

соединяющего их отрезка. Если X_1, X_2 являются даже внутренними точками множества $\mathfrak{B}$, то и точки X должны быть внутренними точками этого множества.

2) *Наличие центра* $\mathfrak{B}$ *в точке* O. Вместе с каждой точкой X из $\mathfrak{B}$ к $\mathfrak{B}$ принадлежит также и симметрично расположенная относительно O точка $-X$. Если X является внутренней точкой множества $\mathfrak{B}$, то и $-X$ должна быть внутренней точкой этого множества.

Можно показать, что из выпуклости следует, что $\mathfrak{B}$ обладает некоторой площадью $|\mathfrak{B}|$. Однако в нашем применении область будет настолько простой, что это будет ясно из элементарно-геометрических соображений. Поэтому мы не будем здесь доказывать этот факт в общем виде.

С наглядной точки зрения очевидно, что область $\mathfrak{B}$ будет заведомо содержать в качестве внутренней точки, кроме своего центра O, еще хотя бы одну другую точку решетки P, если только $\mathfrak{B}$ достаточно велика в том смысле, что содержит, например, достаточно большой круг с центром в O. Однако заранее не ясно, достаточно ли потребовать того, чтобы $\mathfrak{B}$ была в известной мере велика по своей площади $|\mathfrak{B}|$. Если это верно всегда, т. е. для любой области $\mathfrak{B}$, то нужно требовать по меньшей мере, чтобы $|\mathfrak{B}| > 4G$, где G — площадь основного параллелограма нашей решетки; действительно, область $\mathfrak{B}$, состоящая из четырех основных параллелограмов, примыкающих к точке O, очевидно, удовлетворяет обоим предположениям, однако, кроме O, не имеет в качестве внутренней точки ни одной точки решетки.

В действительности имеет место

Теорема Минковского о выпуклой области. *Если на плоскости $\mathfrak{E}$ заданы решетка с площадью основного параллелограмма, равной G, и выпуклая область $\mathfrak{B}$ с центром в точке решетки O и площадью*

$$|\mathfrak{B}| > 4G,$$

то $\mathfrak{B}$ содержит внутри себя еще хотя бы одну точку P решетки.

Доказательство. Мы покажем, что, наоборот, из предположения, что $\mathfrak{B}$ не содержит в качестве внутренней точки ни одной точки решетки, кроме O, следует оценка

$$|\mathfrak{B}| \leqslant 4G.$$

Посредством умножения всех точек области $\mathfrak{B}$ на любое вещественное $\lambda\ (\neq 0)$ получается подобная $\mathfrak{B}$ и подобно расположенная выпуклая область $\lambda\mathfrak{B}$ с центром в O и площадью $|\lambda\mathfrak{B}| = |\lambda|^2 |\mathfrak{B}|$; при этом обозначении наличие центра в O выражается просто в виде $-\mathfrak{B} = \mathfrak{B}$. Для нашего доказательства мы рассмотрим область $\frac{1}{2}\mathfrak{B}$; для ее площади нужно будет получить оценку $\left|\frac{1}{2}\mathfrak{B}\right| \leqslant G$.

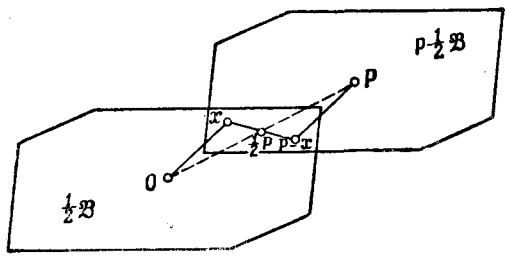
Представим себе, что область $\frac{1}{2}\mathfrak{B}$ параллельно переносится так, что ее центр из точки O попадает в каждую точку P нашей решетки; получающиеся при этом равные и одинаково расположенные выпуклые области с центрами в точках P мы будем обозначать через $P + \frac{1}{2}\mathfrak{B}$. Покажем тогда, что для двух различных точек $P_1 \neq P_2$ нашей решетки области $P_1 + \frac{1}{2}\mathfrak{B}$ и $P_2 + \frac{1}{2}\mathfrak{B}$ не имеют ни одной общей внутренней точки. Для этого достаточно показать, что при $P \neq 0$ области $\frac{1}{2}\mathfrak{B}$ и $P + \frac{1}{2}\mathfrak{B}$ не имеют общих внутренних точек.

Именно, если X есть общая внутренняя точка областей $\frac{1}{2}\mathfrak{B}$ и $P + \frac{1}{2}\mathfrak{B}$, то $P - X$ будет внутренней точкой области

$$P - \left(P + \frac{1}{2}\mathfrak{B}\right) = -\frac{1}{2}\mathfrak{B} = \frac{1}{2}\mathfrak{B}$$

и, по определению выпуклости, $\frac{1}{2}X + \frac{1}{2}(P - X) = \frac{1}{2}P$ будет внутренней точкой области $\frac{1}{2}\mathfrak{B}$ (фиг. 18). Но тогда P будет внутренней точкой области $\mathfrak{B}$. Поэтому, в силу сделанного в начале доказательства предположения, $P = 0$.

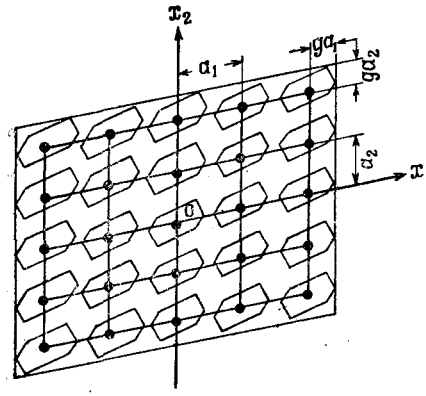
Мы убедились, что внутренние точки всех равных между собой областей $P+\frac{1}{2}\mathfrak{B}$ дают однократное и, возможно, имеющее просветы покрытие плоскости $\mathfrak{E}$. Все эти области имеют одну и



Фиг. 18.

ту же площадь $\left|\frac{1}{2}\mathfrak{B}\right|$. Так как посредством основных параллелограмов с площадью G получается не имеющее просветы покрытие плоскости $\mathfrak{E}$, то довольно очевидно, что должно быть $\left|\frac{1}{2}\mathfrak{B}\right| \leqslant G$. Строго это доказывается следующим образом (фиг. 19).

Фиксируем некоторый основной параллелограм решетки; пусть длины его сторон будут a_1, a_2. Далее, введем на плоскости $\mathfrak{E}$ систему координат x_1, x_2 с началом в точке O и осями, направленными по сторонам выбранного основного параллелограма; тогда существует такое положительное вещественное число g, что координаты x_1, x_2 всех точек X области $\mathfrak{B}$ удовлетворяют неравенствам



Фиг. 19.

$$|x_1| \leqslant g a_1, \quad |x_2| \leqslant g a_2.$$

Рассмотрим теперь $(2n+1)^2$ точек $P_i^{(n)}$ нашей решетки с координатами

$$p_{i1} = \nu_1 a_1, \quad p_{i2} = \nu_2 a_2 \quad (\nu_1, \nu_2 \text{ целые рациональные}, \quad |\nu_1|, |\nu_2| \leqslant n),$$

где n — достаточно большое натуральное число. Тогда для координат x_1, x_2 всех точек X из соответствующих областей $P_i^{(n)}+\frac{1}{2}\mathfrak{B}$ будет иметь место

$$|x_1| \leqslant \left(n+\frac{1}{2}g\right)a_1, \quad |x_2| \leqslant \left(n+\frac{1}{2}g\right)a_2.$$

Таким образом, внутренние точки $(2n+1)^2$ областей с площадью $\left|\frac{1}{2}\mathfrak{B}\right|$ дают однократное и, возможно, имеющее просветы покрытие определяемого этими неравенствами параллелограмма с площадью $(2n+g)^2 G$; этот параллелограм подобен выбранному нами основному параллелограму. Отсюда, согласно основным свойствам площади, следует неравенство

$$(2n+1)^2\left|\frac{1}{2}\mathfrak{B}\right| \leqslant (2n+g)^2 G,$$

или

$$\left|\frac{1}{2}\mathfrak{B}\right| \leqslant \left(\frac{1+\frac{g}{2n}}{1+\frac{1}{2n}}\right)^2 G.$$

При $n \longrightarrow \infty$ мы получаем наше утверждение $\left|\frac{1}{2}\mathfrak{B}\right| \leqslant G$.

Как показали Биркгоф, Бликфельд и Хлавка, заключительного предельного перехода можно избежать, если предшествующую часть доказательства видоизменить следующим образом. Перенесем пересечения области $\frac{1}{2}\mathfrak{B}$ с отдельными основными параллелограмами в некоторый выбранный основной параллелограм, так чтобы они расположились в этом параллелограме так же, как в исходных параллелограмах. Если $\left|\frac{1}{2}\mathfrak{B}\right| > G$, то при этом по крайней мере одна точка P этого основного параллелограма окажется покрытой двумя пересечениями. Пусть P_1, P_2 — прообразы этой точки в исходных пересечениях; тогда, подобно тому как выше, мы получаем, что вследствие 1) и 2) $P_1 - P_2$ является отличной от O точкой решетки, лежащей внутри области $\mathfrak{B}$.

Замечание 1. Очевидно, что доказательство переносится на решетки в k-мерном пространстве, с множителем 2^k вместо $4 = 2^2$ в оценке для объема.

Замечание 2. Посредством рассмотрения области $(1+\varepsilon)\mathfrak{B}$ с достаточно малым $\varepsilon > 0$ получается, что для $|\mathfrak{B}| \geqslant 4G$, включая и случай равенства, область $\mathfrak{B}$ содержит внутри или на границе хотя бы одну точку решетки, отличную от O.

Сба эти замечания мы здесь использовать не будем.

Второе доказательство конечности числа классов.

С помощью теоремы Минковского о выпуклой области мы докажем сейчас два утверждения, являющиеся усилением высказываний XV, XVI; из этих новых утверждений конечность числа классов будет следовать так же, как и из XV, XVI.

XV*. *Для каждого целого дивизора* $\mathfrak{m}$ *поля* $\mathsf{K}=\mathsf{P}(\sqrt{d})$ *существует число* $\alpha \neq 0$ *из* $(\mathfrak{m})$ *с*

$$|N(\alpha)| \leqslant \left\{\begin{matrix} \frac{2}{\pi}\sqrt{|d|}\,\mathfrak{N}(\mathfrak{m}) & для & d<0 \\ \frac{1}{2}\sqrt{|d|}\,\mathfrak{N}(\mathfrak{m}) & для & d>0 \end{matrix}\right\}.$$

XVI*. *В каждом классе* C *дивизоров поля* $\mathsf{K}=\mathsf{P}(\sqrt{d})$ *существует целый дивизор* $\mathfrak{a}$ *с*

$$\mathfrak{N}(\mathfrak{a}) \leqslant \left\{\begin{matrix} \frac{2}{\pi}\sqrt{|d|} & для & d<0 \\ \frac{1}{2}\sqrt{|d|} & для & d>0 \end{matrix}\right\}.$$

Доказательство. При представлении чисел α из K на K-плоскости числа α с

$$|N(\alpha)| \leqslant N\mathfrak{N}(\mathfrak{m})$$

лежат внутри круга, соответственно пары равносторонних гипербол с центром в начале координат и радиусом $\sqrt{N\mathfrak{N}(\mathfrak{m})}$ (см. § 16, п. 2, фиг. 10а, б), а числа α из $(\mathfrak{m})$ образуют решетку, для которой учетверенная площадь основного параллелограма, согласно (3) п. 4, равна

$$4G_{\mathfrak{m}} = 2\sqrt{|d|}\,\mathfrak{N}(\mathfrak{m}).$$

В случае $d<0$ внутренность круга есть выпуклая область $\mathfrak{K}_{\mathfrak{m}}(N)$ с центром в O и площадью

$$|\mathfrak{K}_{\mathfrak{m}}(N)| = \pi N\mathfrak{N}(\mathfrak{m}).$$

Таким образом, если выбрать

$$N > \frac{2}{\pi}\sqrt{|d|},$$

то $|\mathfrak{K}_{\mathfrak{m}}(N)| > 4G_{\mathfrak{m}}$. Тогда по теореме Минковского о выпуклой области круг $\mathfrak{K}_{\mathfrak{m}}(N)$ содержит в качестве внутренней точки некоторую точку $\alpha \neq 0$ решетки $(\mathfrak{m})$:

$$|N(\alpha)| < N\mathfrak{N}(\mathfrak{m}).$$

Если выбрать при этом в качестве N наименьшее натуральное число, удовлетворяющее указанному выше неравенству, и принять во внимание, что, согласно (2), $N(\alpha)$ есть кратное от $\mathfrak{N}(\mathfrak{m})$, то мы получим

$$|N(\alpha)| \leqslant (N-1)\,\mathfrak{N}(\mathfrak{m}) \leqslant \frac{2}{\pi}\sqrt{|d|}\,\mathfrak{N}(\mathfrak{m}),$$

что и требовалось доказать.

В случае $d > 0$ внутренняя область пары равносторонних гипербол содержит в качестве выпуклой подобласти квадрат $\mathfrak{D}_{\mathfrak{m}}(N)$ с центром в точке O и сторонами длины $2\sqrt{N\mathfrak{N}(\mathfrak{m})}$, параллельными осями координат (см. § 16, п. 6, фиг. 15). Площадь этого квадрата равна

$$|\mathfrak{D}_m(N)| = 4N\mathfrak{N}(\mathfrak{m}).$$

Поэтому, если выбрать

$$N > \frac{1}{2}\sqrt{|d|},$$

то $|\mathfrak{D}_{\mathfrak{m}}(N)| > 4G_{\mathfrak{m}}$. Тогда квадрат $\mathfrak{D}_{\mathfrak{m}}(N)$ содержит точку $\alpha \neq 0$ решетки $(\mathfrak{m})$ в качестве внутренней, которая подавно лежит внутри пары равносторонних гипербол:

$$|N(\alpha)| < N\mathfrak{N}(\mathfrak{m}).$$

Если снова выбрать в качестве N наименьшее натуральное число, удовлетворяющее нужному нам неравенству, то, как и в первом случае, мы получим

$$|N(\alpha)| \leqslant (N-1)\mathfrak{N}(\mathfrak{m}) \leqslant \frac{1}{2}\sqrt{|d|}\,\mathfrak{N}(\mathfrak{m}),$$

что и требовалось доказать.

Замечание. Вследствие трансцендентности числа π и алгебраичности (при $d < 0$), соответственно иррациональности (при $d > 0$) числа $\sqrt{|d|}$ в неравенствах из XV*, XVI* знак равенства можно опустить.

Полученное в XVI* усиление результата XVI имеет практическое значение, если мы захотим, исходя из доказательства конечности числа классов h, определять это число для заданных дискриминантов d. Согласно XVI*, мы получим систему представителей всех h классов дивизоров поля K, если переберем все целые дивизоры $\mathfrak{a}$ с $\mathfrak{N}(\mathfrak{a}) \leqslant \frac{2}{\pi}\sqrt{|d|}$, соответственно $\frac{1}{2}\sqrt{|d|}$ и выясним, какие из них лежат в одних и тех же классах.

Два дивизора $\mathfrak{a}$, $\mathfrak{b}$ поля K, лежащих в одном и том же классе дивизоров, называются *эквивалентными* между собой; обозначение: $\mathfrak{a} \sim \mathfrak{b}$. Эта эквивалентность означает выполнение соотношения $\mathfrak{a} = \gamma\mathfrak{b}$ с некоторым числом $\gamma \neq 0$ из K. Вследствие $\mathfrak{a}\mathfrak{a}' \cong \mathfrak{N}(\mathfrak{a})$ всегда имеет место $\mathfrak{a}\mathfrak{a}' \sim 1$, т. е. сопряженный с $\mathfrak{a}$ дивизор $\mathfrak{a}'$ лежит в классе C^{-1}, обратном классу C, определяемому дивизором $\mathfrak{a}$. Поэтому эквивалентность $\mathfrak{a} \sim \mathfrak{b}$ может быть выражена также в форме $\mathfrak{a}\mathfrak{b}' \sim 1$; этот способ записи имеет то преимущество, что если речь идет о целых дивизорах $\mathfrak{a}$, $\mathfrak{b}$, то мы должны будем оперировать только в области целых дивизоров. При этом

согласно IX, п. 3, можно еще отбросить наибольший натуральный делитель, т. е. ограничиться первообразными дивизорами.

После всего этого нахождение полной системы представителей h классов дивизоров поля K может быть сделано следующим способом. Сначала мы определяем систему $\mathfrak{S}$ всех первообразных дивизоров $\mathfrak{a}$ поля K с $\mathfrak{N}(\mathfrak{a}) \leqslant \frac{2}{\pi}\sqrt{|d|}$, соответственно $\frac{1}{2}\sqrt{|d|}$, затем образуем расширенную систему $\mathfrak{S}^*$ из первообразных частей $\mathfrak{a}^*$ произведений $\mathfrak{a}_1\mathfrak{a}_2$ каждых двух дивизоров $\mathfrak{a}_1$, $\mathfrak{a}_2$ из $\mathfrak{S}$ (заметим, что в $\mathfrak{S}$ входит $\mathfrak{a} = 1$ и вместе с каждым $\mathfrak{a}$ также и $\mathfrak{a}'$) и, наконец, для каждого дивизора $\mathfrak{a}^*$ из $\mathfrak{S}^*$ проверяем, имеет ли место $\mathfrak{a}^* \sim 1$, т. е. $\mathfrak{a}^* \cong \alpha$ с некоторым (тоже тогда первообразным) $\alpha \neq 0$ из K.

Для последнего обстоятельства необходимо, чтобы пара диофантовых уравнений

$$\pm N = N(\alpha) = \frac{a^2 - db^2}{4} \tag{3}$$

с $N = \mathfrak{N}(\mathfrak{a}^*)$ была разрешима в целых рациональных a, b (с $a \equiv db \bmod 2$ и притом так, что a, b нельзя сократить на натуральный делитель $g > 1$ с тем, чтобы сравнение попрежнему удовлетворялось – в этом случае говорят о *первообразном решении*). Обратно, каждому первообразному решению $\alpha = (a + b\sqrt{d})/2$ уравнений (3) соответствует первообразный дивизор $\mathfrak{a}^*$ с $\mathfrak{a}^* \sim 1$ и $\mathfrak{N}(\mathfrak{a}^*) = N$, причем ассоциированным между собой решениям α соответствует один и тот же дивизор $\mathfrak{a}^*$. Решение вопроса о разрешимости (3) и определение полной системы неассоциированных решений может быть в мнимом случае d 0 достигнуто посредством простых рассмотрений величины стоящего в правой части уравнений выражения; в вещественном случае $d > 0$, в нашем распоряжении уже имеется изложенный в § 16, п. 6 метод сведения к конечной совокупности чисел a, b, подлежащих исследованию. В обоих случаях для доказательства неразрешимости полезно рассматривать (3) как сравнение по простым делителям чисел d и N и часто таким путем можно окончательно достигнуть цели. Вопрос о том, какому дивизору $\mathfrak{a}^*$ из $\mathfrak{S}^*$ с нормой $\mathfrak{N}(\mathfrak{a}^*) = N$ соответствует найденное решение α уравнений (3), будет решен, если мы исследуем методами из п. 2, какие простые дивизоры из $\mathfrak{S}$ входят в α.

Когда будут определены все $\mathfrak{a}^* \sim 1$ из $\mathfrak{S}^*$, тем самым будут получены и все соотношения эквивалентности между дивизорами $\mathfrak{a}$ из $\mathfrak{S}$. Тогда после выбрасывания из $\mathfrak{S}$ эквивалентных дивизоров и получится искомая система представителей.

Теперь мы проиллюстрируем только что описанный метод определения полной системы представителей h классов дивизоров поля K на нескольких примерах.

Сначала мы рассмотрим те случаи, когда граница

$$\frac{2}{\pi}\sqrt{|d|} < 2, \text{ соответственно } \frac{1}{2}\sqrt{|d|} < 2,$$

или

$$|d| < \pi^2, \text{ соответственно } |d| < 16,$$

т. е. случаи

$$d = -3,\ -4,\ -7,\ -8, \text{ соответственно } d = 5,\ 8,\ 12,\ 13.$$

Так как из $\mathfrak{N}(\mathfrak{a}) < 2$ (для целых дивизоров $\mathfrak{a}$) следует $\mathfrak{N}(\mathfrak{a}) = 1$, в этих случаях наша система представителей состоит только из $\mathfrak{a} = 1$, т. е. $h = 1$. Тем самым мы, согласно XI, п. 3, вновь доказали результат XIXA, Б, § 16, полученный выше другим методом, за исключением лишь случая $d = -11$, который сейчас не был нами охвачен.

В этом последнем случае $d = -11$ граница $2\sqrt{11}/\pi < 3$, так что наряду с $\mathfrak{N}(\mathfrak{a}) = 1$ нужно рассмотреть еще возможность $\mathfrak{N}(\mathfrak{a}) = 2$. Но вследствие $\left(\frac{-11}{2}\right) = -1$ число 2 остается в $\mathsf{P}(\sqrt{-11})$ простым, так что равенство $\mathfrak{N}(\mathfrak{a}) = 2$ невозможно. Тем самым мы и в случае $d = -11$ снова доказали, что $h = 1$.

Рассмотрим далее те случаи, на которых мы иллюстрировали в § 16, п. 6, что разложение на простые множители в поле $\mathsf{K} = \mathsf{P}(\sqrt{d})$ не всегда однозначно, именно, четыре случая

$$D = -5,\ -6, \quad \text{соответственно} \quad D = 10,\ 82,$$

или

$$d = -20,\ -24, \text{ соответственно } d = 40,\ 328,$$

с границами

$$\frac{2}{\pi}\sqrt{|d|} < 3,4, \text{ соответственно } \frac{1}{2}\sqrt{|d|} < 4,10.$$

Согласно XI, п. 3, в этих случаях необходимо должно быть $h > 1$.

Для $d = -20$ надо исследовать первообразные $\mathfrak{a}$ с $\mathfrak{N}(\mathfrak{a}) = 1, 2$. Вследствие того, что $2 \mid d$, число 2 разветвляется, т. е.

$$2 \cong \mathfrak{p}^2 \quad \text{с} \quad \mathfrak{N}(\mathfrak{p}) = 2.$$

Уравнение $2 = a^2 + 5b^2$ неразрешимо в целых рациональных числах, и поэтому простой дивизор $\mathfrak{p} \not\sim 1$. Поэтому наша система представителей состоит из двух дивизоров $\mathfrak{a} = 1$, $\mathfrak{p}$ и, следовательно, $h = 2$.

Рассмотренный нами выше пример

$$21 = 3 \cdot 7 = (4 + \sqrt{-5})\,(4 - \sqrt{-5})$$

неоднозначного разложения мы можем теперь осветить с точки зрения имеющихся у нас результатов об арифметической структуре поля K. В силу $\left(\frac{-5}{3}\right)=1$, $\left(\frac{-5}{7}\right)=1$, числа 3, 7 разложимы в K, т. е.

$$3 \cong \mathfrak{q}\mathfrak{q}' \text{ с } \mathfrak{N}(\mathfrak{q}) = \mathfrak{N}(\mathfrak{q}') = 3, \quad 7 = \mathfrak{r}\mathfrak{r}' \text{ с } \mathfrak{N}(\mathfrak{r}) = \mathfrak{N}(\mathfrak{r}') = 7.$$

Так как уравнения $3, 7 = a^2 + 5b^2$ неразрешимы в целых рациональных числах, все простые дивизоры $\mathfrak{q}$, $\mathfrak{q}'$, $\mathfrak{r}$, $\mathfrak{r}'$, $\not\sim 1$. Но тогда из $h = 2$ необходимо следует

$$\mathfrak{q},\ \mathfrak{q}',\ \mathfrak{r},\ \mathfrak{r}' \sim \mathfrak{p},$$

и, так как $\mathfrak{p}^2 \cong 2 \sim 1$, произведение каждых двух из этих дивизоров ~ 1. Кроме уже известных нам произведений $\mathfrak{q}\mathfrak{q}' \cong 3$, $\mathfrak{r}\mathfrak{r}' \cong 7$ мы, таким обр зом, имеем еще два других

$$\mathfrak{q}\mathfrak{r} \cong \alpha, \quad \mathfrak{q}\mathfrak{r}' \cong \beta'$$

и сопряженных с ними

$$\mathfrak{q}'\mathfrak{r}' \cong \alpha', \quad \mathfrak{q}'\mathfrak{r} \cong \beta$$

с первообразными α, β. Поэтому, группируя различными способами четыре простых дивизора в

$$21 \cong \mathfrak{q}\mathfrak{q}' \cdot \mathfrak{q}\mathfrak{r}' = \mathfrak{q}\mathfrak{r} \cdot \mathfrak{r}'\mathfrak{r}' = \mathfrak{q}\mathfrak{r}' \cdot \mathfrak{q}'\mathfrak{r},$$

мы получим три существенно различных разложения

$$21 = 3 \cdot 7 = \alpha\alpha' = \beta\beta',$$

в которых вместо $\cong$ можно писать $=$, так как в K существуют только единицы ± 1 и произведения положительны. Одним из двух последних разложений должно быть указанное выше $21 = 4^2 + 5 \cdot 1^2 = N(4 + \sqrt{-5})$; другое есть $21 = 1^2 + 5 \cdot 2^2 = N(1 + 2\sqrt{-5})$. Если в соответствии с п. 2 различать друг от друга сопряженные $\mathfrak{q}$, $\mathfrak{q}'$ и $\mathfrak{r}$, $\mathfrak{r}'$ с помощью сравнений

$$\sqrt{-5} \equiv \left\{\begin{matrix} 1 \bmod \mathfrak{q} \\ -1 \bmod \mathfrak{q}' \end{matrix}\right\}, \quad \sqrt{-5} \equiv \left\{\begin{matrix} 3 \bmod \mathfrak{r} \\ -3 \bmod \mathfrak{r}' \end{matrix}\right\},$$

то

$$4 - \sqrt{-5} \equiv 0 \bmod \mathfrak{q}, \qquad 4 - \sqrt{-5} \equiv 0 \bmod \mathfrak{r}'$$
$$1 + 2\sqrt{-5} \equiv 0 \bmod \mathfrak{q}, \qquad 1 + 2\sqrt{-5} \equiv 0 \bmod \mathfrak{r}',$$

и, таким образом,

$$\alpha \cong 1 + 2\sqrt{-5}, \quad \beta \cong 4 - \sqrt{-5}.$$

Для $d = -24$ надо исследовать первообразные $\mathfrak{a}$ с $\mathfrak{N}(\mathfrak{a}) = 1, 2, 3$. Вследствие $2 \mid d$, $3 \mid d$, имеет место

$$2 \cong \mathfrak{p}^2 \text{ с } \mathfrak{N}(\mathfrak{p}) = 2, \quad 3 = \mathfrak{q}^2 \text{ с } \mathfrak{N}(\mathfrak{q}) = 3.$$

Поэтому мы получим нашу систему представителей после отбрасывания эквивалентных дивизоров среди 1, $\mathfrak{p}$, $\mathfrak{q}$. Уравнения $2,\ 3=a^2+6b^2$ неразрешимы в целых рациональных числах, и потому $\mathfrak{p},\ \mathfrak{q}\not\sim 1$. Однако, вследствие $\mathfrak{N}(\mathfrak{pq})=6=N(\sqrt{-6})$, $\mathfrak{pq}\cong\sqrt{-6}\sim 1$, и потому $\mathfrak{p}\sim\mathfrak{q}'=\mathfrak{q}$. Поэтому снова $h=2$, и система представителей состоит, например, из 1, $\mathfrak{p}$.

Другое двоякое представление

$$6=2\cdot 3=\sqrt{-6}\cdot-\sqrt{-6}$$

еще яснее, чем предыдущее. Оно получается посредством двух различных группировок сомножителей в

$$6\cong\mathfrak{pp}\cdot\mathfrak{qq}=\mathfrak{pq}\cdot\mathfrak{pq}.$$

Для $d=40$ снова нужно исследовать первообразные $\mathfrak{a}$ с $\mathfrak{N}(\mathfrak{a})=1,\ 2,\ 3$. Так как $2\mid d$ и $\left(\frac{10}{3}\right)=1$, мы имеем

$$2\cong\mathfrak{p}^2 \text{ с } \mathfrak{N}(\mathfrak{p})=2,\ 3\cong\mathfrak{qq}' \text{ с } \mathfrak{N}(\mathfrak{q})=\mathfrak{N}(\mathfrak{q}')=3.$$

Наша система представителей получается после отбрасывания эквивалентных дивизоров среди 1, $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{q}'$. Уравнения $\pm 2=a^2-10b^2$, вследствие $\left(\frac{\pm 2}{5}\right)=-1$, неразрешимы в целых рациональных числах, и потому $\mathfrak{p}\not\sim 1$. Далее, из $\mathfrak{N}(\mathfrak{pq})=\mathfrak{N}(\mathfrak{pq}')=6\cong N(2+\sqrt{10})$ снова следует — при соответствующем способе различать сопряженные $\mathfrak{q}$, $\mathfrak{q}'$, — что

$$2+\sqrt{10}\cong\mathfrak{pq},\quad 2-\sqrt{10}\cong\mathfrak{pq}',$$

и потому $\mathfrak{q}\sim\mathfrak{q}'\sim\mathfrak{p}$. Таким образом, снова $h=2$, и система представителей состоит, например, из 1, $\mathfrak{p}$.

Рассмотренное выше двоякое представление

$$10=2\cdot 5=\sqrt{10}\cdot\sqrt{10}$$

имеет, в силу $5\cong\mathfrak{r}^2$ с $\mathfrak{N}(\mathfrak{r})=5$, ту же самую структуру, что и последнее представление в предыдущем случае.

Для $d=328$ нужно исследовать первообразные $\mathfrak{a}$ с $\mathfrak{N}(\mathfrak{a})=1,\ 2,\ \ldots,\ 9$. Однако, вследствие того что $2\mid d$ и $\left(\frac{82}{3}\right)=1$, $\left(\frac{82}{5}\right)=-1$, $\left(\frac{82}{7}\right)=-1$, простыми дивизорами с нормой $\leqslant 9$ могут быть лишь делители чисел

$$2\cong\mathfrak{p}^2 \text{ с } \mathfrak{N}(\mathfrak{p})=2,\ 3\cong\mathfrak{qq}' \text{ с } \mathfrak{N}(\mathfrak{q})=\mathfrak{N}(\mathfrak{q}')=3.$$

Поэтому система $\mathfrak{S}$ первообразных дивизоров с нормой $\leqslant 9$ есть

$$\mathfrak{S}=\{1,\ \mathfrak{p},\ \mathfrak{q},\ \mathfrak{q}',\ \mathfrak{q}^2,\ \mathfrak{q}'^2,\ \mathfrak{pq},\ \mathfrak{pq}'\}.$$

Для того чтобы выбросить отсюда эквивалентные, надо образовать первообразные части произведений каждой пары из этих дивизоров и исследовать, какие из этих первообразных частей ~ 1. Расширенная система $\mathfrak{S}^*$ получается посредством присоединения системы дивизоров

$$\mathfrak{S}^* - \mathfrak{S} = \{\mathfrak{p}\mathfrak{q}^2,\ \mathfrak{p}\mathfrak{q}'^2,\ \mathfrak{q}^3,\ \mathfrak{q}'^3,\ \mathfrak{p}\mathfrak{q}^3,\ \mathfrak{p}\mathfrak{q}'^3\}.$$

Поэтому нужно было бы исследовать разрешимость диофантовых уравнений $\pm N = a^2 - 82b^2$ для $N = 2,\ 3,\ 6,\ 9,\ 18,\ 27,\ 54$ и в тех случаях, когда решение существует, определить полные системы неассоциированных первообразных решений. Однако можно достигнуть цели более коротким путем. Методом из § 16, п. 6 мы убеждаемся в неразрешимости уравнения для $N = 2$; таким образом,

$$\mathfrak{p} \neq 1.$$

Для $N = 18$ получается решение $\mathfrak{N}(\mathfrak{p}\mathfrak{q}^2) = \mathfrak{N}(\mathfrak{p}\mathfrak{q}'^2) = 18 = N(10 + \sqrt{82})$, откуда

$$\mathfrak{q}^2 \sim \mathfrak{q}'^2 \sim \mathfrak{p}.$$

Так как для четвертой степени дивизора $\mathfrak{q}$ впервые $\mathfrak{q}^4 \sim \mathfrak{p}^2 \sim 1$, то из теоретико-групповых соображений следует, что класс C, представителем которого является $\mathfrak{q}$, имеет порядок 4. Дивизоры

$$1,\ \mathfrak{q},\ \mathfrak{p},\ \mathfrak{q}'$$

являются тогда представителями классов из цикла

$$1,\ C,\ C^2,\ C^3.$$

Все остальные дивизоры из $\mathfrak{S}$ представляются через $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{q}'$ и потому тоже принадлежат к классам из этого цикла. Поэтому 1, $\mathfrak{q}$, $\mathfrak{p}$, $\mathfrak{q}'$ образуют полную систему представителей классов дивизоров. Следовательно, $h = 4$; кроме того, нами установлено, что группа классов дивизоров циклична.

Рассмотренное ранее двоякое представление

$$-713 = -23 \cdot 31 = (5 + 3\sqrt{82})(5 - 3\sqrt{82})$$

имеет, в силу того что $\left(\frac{82}{23}\right) = 1$, $\left(\frac{82}{31}\right) = 1$, т. е.

$$23 \cong \mathfrak{r}\mathfrak{r}' \quad \text{с } \mathfrak{N}(\mathfrak{r}) = \mathfrak{N}(\mathfrak{r}') = 23,$$
$$31 \cong \mathfrak{s}\mathfrak{s}' \quad \text{с } \mathfrak{N}(\mathfrak{s}) = \mathfrak{N}(\mathfrak{s}') = 31,$$

ту же самую структуру, что и двоякое представление в случае $d = -20$. Именно, наличие этого двоякого представления означает, что, например,

$$5 + 3\sqrt{82} \cong \mathfrak{r}\mathfrak{s}',\ \ 5 - 3\sqrt{82} \cong \mathfrak{r}'\mathfrak{s},$$

и потому оно соответствует двум различным группировкам

$$713 \cong \mathfrak{r}\mathfrak{r}' \cdot \mathfrak{s}\mathfrak{s}' = \mathfrak{r}\mathfrak{s}' \cdot \mathfrak{r}'\mathfrak{s}.$$

Третьему способу группировки

$$713 \cong \mathfrak{r}\mathfrak{s} \cdot \mathfrak{r}'\mathfrak{s}'$$

соответствует еще одно разложение

$$-713 = -23 \cdot 31 = (77 + 9\sqrt{82})\ (77 - 9\sqrt{82}),$$

в чем легко убедиться из того, что

$$\mathfrak{p}\mathfrak{r}' \cong 6 + \sqrt{82},\ \mathfrak{p}\mathfrak{s}' \cong 12 + \sqrt{82}.$$

Из последних соотношений, между прочим, следует, что $\mathfrak{r}$, $\mathfrak{s} \sim \mathfrak{p}$, т. е. $\mathfrak{r}$, $\mathfrak{s}$ лежат в классе C^2.

Для упражнения в этом методе читателю предоставляется доказать, что $d = -23$ является наименьшим по абсолютной величине дискриминантом мнимого квадратичного поля, для которого $h = 3$. В процессе этого доказательства читатель убедится, что для $d = -19$ еще имеет место $h = 1$. Это дает пример мнимого квадратичного поля с однозначным разложением на простые множители, но без алгоритма Евклида; о возможности такого положения уже говорилось в конце п. 3 и § 16, п. 6 после XIXA, Б. Другими примерами являются

$$d = -43,\ -67,\ -163.$$

Хейльброн и Линфут доказали [1] аналитическим путем, что, кроме этого, может существовать еще самое большее одно мнимое квадратичное поле с $h = 1$, а Лемер [1] установил, что дискриминант этого поля по абсолютной величине во всяком случае должен быть больше, чем $5 \cdot 10^9$.

В отличие от этого, число вещественных квадратичных полей с $h = 1$, повидимому, бесконечно. В связи со сказанным в § 16, п. 6 после XIXA, Б читателю предоставляется проверить, что $d = 53$ дает нам первый пример того, что $h = 1$, но алгоритма Евклида не существует.

§ 18. ОПРЕДЕЛЕНИЕ ЧИСЛА КЛАССОВ

1. Предельная формула. Теперь мы хотим доказать для случая квадратичного поля $\mathsf{K} = \mathsf{P}(\sqrt{d})$ сформулированную для общего случая в конце § 15, п. 5 предельную теорему.

Эта предельная теорема касается дзета-функции Дедекинда поля K, определяемой посредством

$$\zeta_{\mathsf{K}}(s) = \sum_{\mathfrak{n}} \frac{1}{\mathfrak{N}(\mathfrak{n})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{p})^s}},$$

где $\mathfrak{n}$ пробегает все целые, а $\mathfrak{p}$ — все простые дивизоры поля K, и связанной соотношением

$$\zeta_{\mathsf{K}}(s) = \zeta(s)\, L(s \mid \chi)$$

с дзета-функцией Римана и L-функцией, соответствующей характеру $\chi(x) = \left(\frac{d}{x}\right)$. Именно, речь идет о доказательстве того, что

$$\lim_{s \to 1+0} \zeta_{\mathsf{K}}(s) = +\infty,$$

или, точнее, что

$$\lim_{s \to 1+0} (s-1)\, \zeta_{\mathsf{K}}(s) = L(1 \mid \chi) = A_{\mathsf{K}}, \tag{1}$$

где $A_{\mathsf{K}} \neq 0$ есть определенное в § 15, п. 5 для общего случая число, выражающееся через арифметические инварианты поля K. Используя результаты из § 16, п. 4, мы получаем, что для квадратичного поля $\mathsf{K} = \mathsf{P}(\sqrt{d})$ это выражение принимает следующий вид:

$$A_{\mathsf{K}} = \begin{cases} \dfrac{2\pi}{w\sqrt{|d|}}\, h & \text{для } d < 0 \\ \dfrac{2 \ln \varepsilon_1}{\sqrt{|d|}}\, h & \text{для } d > 0 \end{cases}, \tag{2}$$

где w есть количество корней из 1, ε_1 — основная единица, и h — число классов поля K.

Как было показано в § 15, п. 5 в связи с формулировкой предельной теоремы, нам достаточно доказать предельную формулу

$$\sum_{\mathfrak{N}(\mathfrak{n}) \leqslant N} 1 = A_{\mathsf{K}} N + O(\sqrt{N}) \text{ при } N \to \infty, \tag{3}$$

где остаточный член имеет для рассматриваемых здесь квадратичных полей показатель $1 - 1/k = 1 - 1/2 = 1/2$. Теперь мы и хотим получить это доказательство.

Представим себе целые дивизоры $\mathfrak{n}$ поля K распределенными по h классам дивизоров C поля K и для целых дивизоров $\mathfrak{a}$, принадлежащих некоторому фиксированному классу C, применим содержащийся в XIV, п. 5, § 17 результат. Тогда мы получим, что интересующие нас целые дивизоры $\mathfrak{a}$ из C с $\mathfrak{N}(\mathfrak{a}) \leqslant N$ взаимно однозначно соответствуют неассоциированным числам $\alpha \neq 0$ из $(\mathfrak{m})$ с $|N(\alpha)| \leqslant N\mathfrak{N}(\mathfrak{m})$, где $\mathfrak{m}$ есть некоторый фиксированный целый дивизор из C^{-1}. Поэтому мы вместо суммы в левой стороне равенства (3) рассмотрим суммы

$$\sigma_{\mathfrak{m}}(N) = \sum_{\substack{\alpha \text{ из } (\mathfrak{m}) \\ |N(\alpha)| \leqslant N\mathfrak{N}(\mathfrak{m})}}^{*} 1, \tag{4}$$

где звездочка указывает на то, что суммирование должно производиться по полной системе неассоциированных $\alpha \neq 0$ с обоими указанными свойствами. Согласно вышеупомянутому результату,

$$\sum_{\mathfrak{N}(\mathfrak{n})\leqslant N}{}^{*} 1 = \sum_{\mathfrak{m}} \sigma_{\mathfrak{m}}(N),$$

где $\mathfrak{m}$ пробегает полную систему представителей h классов дивизоров поля K. Поэтому предельная формула (3) со значением A_{K} из (2) будет доказана, если мы докажем следующую предельную формулу для сумм $\sigma_{\mathfrak{m}}(N)$:

$$\sigma_{\mathfrak{m}}(N) = B_{\mathsf{K}} N + O\left(\sqrt{N}\right) \quad \text{при } N \longrightarrow \infty \tag{5}$$

с

$$B_{\mathsf{K}} = \begin{cases} \dfrac{2\pi}{w\sqrt{|d|}} & \text{для } d < 0 \\ \dfrac{2\ln \varepsilon_1}{\sqrt{|d|}} & \text{для } d > 0 \end{cases}.$$

При доказательстве мы будем опираться на введенное в § 16, п. 2 геометрическое представление чисел из K на K-плоскости. При этом $\sigma_{\mathfrak{m}}(N)$ будет количеством тех точек α решетки $(\mathfrak{m})$ (*о них уже шла речь в* § 17, п. 5), которые *лежат внутри* круга, соответственно пары равносторонних гипербол, с центром в начале координат и радиусом $\sqrt{N\mathfrak{N}(\mathfrak{m})}$ (*см. снова* § 16, п. 2, фиг. 10а, б). Однако теперь нам уже недостаточно, как в § 17, п. 5, доказать для *некоторого определенного*, достаточно большого N существование хотя бы одной такой точки $\alpha \neq 0$, а нужно при $N \longrightarrow \infty$ определить асимптотическое количество всех таких точек решетки, которые представляют полную систему неассоциированных $\alpha \neq 0$ с обоими указанными свойствами.

Чтобы выразить геометрически также и это последнее ограничение (неассоциированность), мы, в связи со сказанным в § 16, п. 2 относительно полярных координат на K-плоскости и в § 16, п. 4 относительно представления в полярных координатах единиц поля K, заметим следующее. Как в случае $d < 0$, так и в случае $d > 0$ каждому числу $\alpha \neq 0$ из K посредством умножения на однозначно определенную единицу

$$\varepsilon = \zeta^{\nu} \quad (\nu \bmod w),$$

$$\text{соответственно } \varepsilon = (-1)^{\nu}\varepsilon_1^{n} \begin{pmatrix} \nu \bmod 2 \\ n - \text{целое рациональное} \end{pmatrix}$$

поля K сопоставляется ассоциированное число $\alpha^* = \varepsilon\alpha$ со свойствами

$$0 \leqslant \varphi(\alpha^*) < \frac{2\pi}{w}, \text{ соответственно } \alpha^* > 0,\ 0 \leqslant \varphi(\alpha^*) < \ln \varepsilon_1, \tag{6}$$

где $\varphi(\alpha^*)$ обозначает полярный угол числа α^*. Геометрически неравенства (6) определяют сектор, соответственно пару секторов с вершиной в начале координат и обыкновенным углом при вершине, равным $2\pi/w$, соответственно гиперболическим углом при вершине, равным $\ln \varepsilon_1$ (см. § 16, п. 2, фиг. 11а, б и § 16, п. 4, фиг. 13). Каждое число $\alpha \neq 0$ из K ассоциировано с одним и только одним числом $\alpha^* \neq 0$ из этого сектора, соответственно пары секторов. Говорят также, что сектор соответственно пара секторов (6) образует фундаментальную область $\mathfrak{F}$ мультипликативной группы единиц поля K.

Пересечение этой фундаментальной области $\mathfrak{F}$ с круговой, соответственно гиперболической областью,

$$|N(\alpha)| \leqslant N\mathfrak{N}(\mathfrak{m}) \tag{7}$$

мы обозначим через $\mathfrak{F}_{\mathfrak{m}}(N)$. Тогда (4) можно представить также в виде

$$\sigma_{\mathfrak{m}}(N) = \sum_{\substack{\alpha \neq 0 \text{ из } (\mathfrak{m}) \\ \alpha \text{ из } \mathfrak{F}_{\mathfrak{m}}(N)}} 1,$$

где $\mathfrak{F}_{\mathfrak{m}}(N)$ определено неравенствами (6), (7). Поэтому геометрически $\sigma_{\mathfrak{m}}(N)$ означает просто количество точек $\alpha \neq 0$ решетки $(\mathfrak{m})$, лежащих в области $\mathfrak{F}_{\mathfrak{m}}(N)$.

Представим себе теперь, что область $\mathfrak{F}_{\mathfrak{m}}(N)$ и решетка $(\mathfrak{m})$ подобно уменьшены в линейном отношении $\sqrt{N}:1$, так что $\mathfrak{F}_{\mathfrak{m}}(N)$ переходит каждый раз в одну и ту же область $\mathfrak{F}_{\mathfrak{m}}(1)$, а решетка, в которую переходит $(\mathfrak{m})$, делается с ростом N сколь угодно мелкой; тогда из определения понятия площади вытекает, что определяемое нами количество точек $\sigma_{\mathfrak{m}}(N)$, умноженное на площадь $G_{\mathfrak{m}}/N$ основного параллелограмма, при $N \to \infty$ стремится к площади $|\mathfrak{F}_{\mathfrak{m}}(1)|$:

$$\lim_{N\to\infty} \sigma_{\mathfrak{m}}(N) \frac{G_{\mathfrak{m}}}{N} = |\mathfrak{F}_{\mathfrak{m}}(1)|$$

или

$$\lim_{N\to\infty} \frac{\sigma_{\mathfrak{m}}(N)}{N} = \frac{|\mathfrak{F}_{\mathfrak{m}}(1)|}{G_{\mathfrak{m}}}.$$

При этом, как в § 17, п. 5,

$$G_{\mathfrak{m}} = \frac{1}{2}\sqrt{|d|}\,\mathfrak{N}(\mathfrak{m}), \tag{8}$$

и, согласно § 16, п. 2 (фиг. 11а, б), мы имеем

$$|\mathfrak{F}_{\mathfrak{m}}(1)| = \frac{\pi}{w}\mathfrak{N}(\mathfrak{m}), \text{ соответственно } 2\cdot\frac{1}{2}\ln\varepsilon_1\,\mathfrak{N}(\mathfrak{m}). \tag{9}$$

Поэтому имеет место

$$\lim_{N\to\infty}\frac{\sigma_{\mathfrak{m}}(N)}{N}=\frac{2\pi}{w\sqrt{|d|}},\ \text{соответственно}\ \frac{2\ln\varepsilon_1}{\sqrt{|d|}}.$$

Это есть предельная формула (5) с указанным там значением константы $B_{\mathfrak{m}}$, но еще без оценки остаточного члена.

Чтобы показать далее, что остаточный член в (5) имеет порядок $O(\sqrt{N})$, мы должны более точно проследить процесс исчерпывания области $\mathfrak{F}_{\mathfrak{m}}(N)$ — которую целесообразно теперь рассматривать снова в ее первоначальной величине — параллелограммами решетки $(\mathfrak{m})$. Мы будем сопоставлять каждой точке решетки из $\mathfrak{F}_{\mathfrak{m}}(N)$ основной параллелограм, имеющий ее своей вершиной (причем так, что стороны этих параллелограмов выходят из соответствующих точек по одним и тем же направлениям). Совокупность этих параллелограмов покрывает некоторую область с площадью $\sigma_{\mathfrak{m}}(N)\,G_{\mathfrak{m}}$; с одной стороны, эта область не целиком покрывает область $\mathfrak{F}_{\mathfrak{m}}(N)$, с другой стороны, местами выходит за ее пределы. Если через R' и R'' обозначить площади непокрытой части области $\mathfrak{F}_{\mathfrak{m}}(N)$ и выходящей за пределы $\mathfrak{F}_{\mathfrak{m}}(N)$ части области, составленной из параллелограммов, то будет иметь место

$$\sigma_{\mathfrak{m}}(N)\,G_{\mathfrak{m}}=|\,\mathfrak{F}_{\mathfrak{m}}(N)\,|-R'+R''.$$

Если теперь вокруг каждой точки границы области $\mathfrak{F}_{\mathfrak{m}}(N)$ описать круг, радиус которого r равен максимальному расстоянию между двумя точками основного параллелограма, то каждая точка плоскости, не покрытая этими кругами и лежащая в области $\mathfrak{F}_{\mathfrak{m}}(N)$, будет покрыта системой основных параллелограмов, а каждая точка, не покрытая кругами и лежащая вне области $\mathfrak{F}_{\mathfrak{m}}(N)$, не покрывается этой системой; действительно, в каждом из этих случаев основной параллелограм, содержащий эту точку, в силу значения r не достигает границы области $\mathfrak{F}_{\mathfrak{m}}(N)$. Таким образом, если через $\mathfrak{F}_{\mathfrak{m}}^{(r)}(N)$ обозначить площадь области, покрытой кругами, то

$$R'+R''\leqslant|\,\mathfrak{F}_{\mathfrak{m}}^{(r)}(N)\,|,$$

и потому

$$|\,\sigma_{\mathfrak{m}}(N)\,G_{\mathfrak{m}}-|\,\mathfrak{F}_{\mathfrak{m}}(N)\,|\,|\leqslant|\,\mathfrak{F}_{\mathfrak{m}}^{(r)}(N)\,|.$$

Но с наглядной точки зрения очевидно, что площадь кольцевой области $\mathfrak{F}_{\mathfrak{m}}^{(r)}(N)$ при $N\to\infty$ имеет тот же порядок возрастания, что и длина границы области $\mathfrak{F}_{\mathfrak{m}}(N)$, потому что ширина $2r$ кольцевой области остается постоянной (фиг. 20а, б). Вследствие того что $\mathfrak{F}_{\mathfrak{m}}(N)=N\mathfrak{F}_{\mathfrak{m}}(1)$, длина границы области $\mathfrak{F}_{\mathfrak{m}}(N)$ имеет порядок возрастания $O(\sqrt{N})$. Таким образом, мы приходим

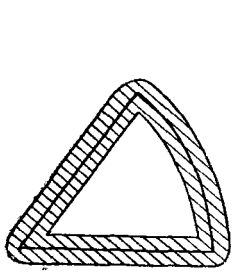
к оценке

$$\sigma_{\mathfrak{m}}(N)\,G_{\mathfrak{m}} - |\,\mathfrak{F}_{\mathfrak{m}}(N)\,| = O(\sqrt{N})$$

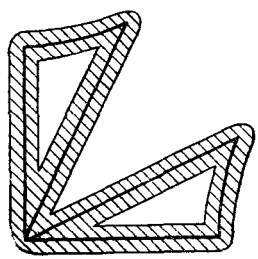
или также

$$\sigma_{\mathfrak{m}}(N) = \frac{|\,\mathfrak{F}_{\mathfrak{m}}(1)\,|}{G_{\mathfrak{m}}}\,N + O(\sqrt{N}),$$

откуда, на основании доказанных выше формул (8), (9) для площади, следует утверждение (5).



Фиг. 20а.



Фиг. 20б.

Однако нам еще нужно строго обосновать факт

$$|\,\mathfrak{F}_{\mathfrak{m}}^{(r)}(N)\,| = O(\sqrt{N}), \tag{10}$$

который перед этим мы вывели только из соображений наглядности. Для этого мы докажем следующее совершенно общее предложение (фиг. 21):

Лемма. *Пусть* $\mathfrak{C}$ *— отрезок кривой с непрерывно меняющейся кривизной, имеющий длину* $|\,\mathfrak{C}\,|$ *и радиус кривизны все время* $\geqslant r > 0$; *пусть, далее,* $\mathfrak{C}^{(r)}$ *есть область плоскости, которая покрывается всевозможными кругами радиуса* r, *имеющими центры на* $\mathfrak{C}$. *Тогда для площади этой области имеет место*

$$|\,\mathfrak{C}^{(r)}\,| \leqslant 2r\,|\,\mathfrak{C}\,| + \pi r^2.$$

Доказательство. Если декартовы координаты некоторой точки отрезка $\mathfrak{C}$ суть x, y, то точки ξ, η окружности радиуса r с центром в x, y определяются уравнением

$$(x-\xi)^2 + (y-\eta)^2 = r^2.$$

При этом, как известно,

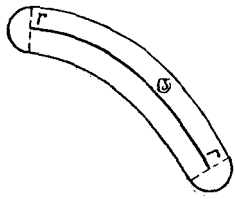
$$(x-\xi)\,dx + (y-\eta)\,dy = 0,$$

т. е. радиус-вектор $x-\xi$, $y-\eta$, идущий от x, y к точке ξ, η пересечения двух бесконечно близких кругов, перпендикулярен элементу дуги dx, dy, другими словами, есть нормаль к кривой $\mathfrak{C}$ в точке x, y. Но нормали к двум бесконечно близким точкам

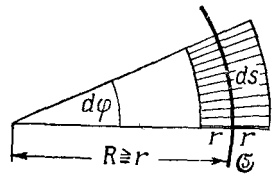
кривой пересекаются в центре кривизны. Таким образом, дело обстоит так, как показано на фиг. 22.

$$ds = \sqrt{dx^2 + dy^2} = R\,d\varphi, \quad R - \text{радиус кривизны.}$$

Элемент площади области $\mathfrak{C}^{(r)}$ представляется поэтому как разность площадей двух круговых секторов с центром в центре



Фиг. 21.



Фиг. 22.

кривизны кривой $\mathfrak{C}$, углом раствора $d\varphi$ и радиусами $R \pm r > 0$. Таким образом, этот элемент площади равен

$$\frac{1}{2}(R+r)^2\,d\varphi - \frac{1}{2}(R-r)^2\,d\varphi = 2Rr\,d\varphi = 2r\,ds.$$

Интегрируя вдоль $\mathfrak{C}$ и округляя концы круговыми дугами в соответствии с фиг. 21, мы получаем доказываемое нами неравенство (и притом даже в виде равенства, если только область нигде не накладывается сама на себя).

Дополнение. *Более обще, если* $\mathfrak{C}$ *составлена из* n *отрезков с непрерывно меняющимися кривизнами, то во всяком случае*

$$|\mathfrak{C}^{(r)}| \leqslant 2r\,|\mathfrak{C}| + n\pi r^2.$$

Заметим, что округления концов гладких кусков могут перекрываться между собой.

Для рассматриваемых нами замкнутых кривых, являющихся границами фундаментальных областей $\mathfrak{F}_m(N)$ (см. фиг. 20а, б) предположение леммы относительно кривизны будет, очевидно, выполнено для каждого из трех соответственно шести гладких кусков, если только выбрать N достаточно большим. Поэтому, если через l обозначить длину границы области $\mathfrak{F}_m(1)$, то по дополнению к лемме мы будем иметь

$$|\mathfrak{F}_m^{(r)}(N)| \leqslant 2rl\sqrt{N} + 6\pi r^2$$

для достаточно большого N, что и дает нам соотношение (10), которое нам еще оставалось доказать.

Заметим, что оценка остаточного члена в случае $d < 0$ может быть получена значительно проще. Именно, в этом случае мы

можем обойтись без рассмотрения фундаментальной области $\mathfrak{F}$. Так как здесь каждое $\alpha \neq 0$ из K имеет точно w различных ассоциированных, мы можем в (4) освободиться от ограничения, что суммирование распространяется только на неассоциированные числа, рассматривая $w\sigma_{\mathfrak{m}}(N)$ вместо $\sigma_{\mathfrak{m}}(N)$:

$$w\sigma_{\mathfrak{m}}(N) = \sum_{\substack{\alpha \neq 0 \text{ из } (\mathfrak{m}) \\ N(\alpha) \leqq N\mathfrak{N}(\mathfrak{m})}} 1.$$

При этом речь идет уже о количестве точек решетки во всем круге. Замкнутая область $\mathfrak{C}^{(r)}$ будет иметь тогда вид кругового кольца, площадь которого находится элементарно.

Выведенная предельная формула (5) доказывает для случая квадратичного поля K предельную теорему, сформулированную в общем виде в § 15, п. 5.

Как было показано в § 15, п. 5, отсюда как следствие вытекает уже указанная нами в начале этого параграфа формула (1), согласно которой дзета-функция поля K имеет при $s = 1$ полюс первого порядка с вычетом, равным фигурирующему в предельной формуле выражению A_{K}:

I. *Для дзета-функции*

$$\zeta_{\mathsf{K}}(s) = \zeta(s)\, L(s \mid \chi)$$

квадратичного поля $\mathsf{K} = \mathsf{P}(\sqrt{d})$ $\left(\text{*где квадратичный характер* } \chi \text{ *задается, следовательно, равенством* } \chi(x) = \left(\frac{d}{x}\right)\right)$ *имеет место предельное соотношение*

$$\lim_{s \to 1+0} (s-1)\,\zeta_{\mathsf{K}}(s) = L(1 \mid \chi) = \left\{ \begin{array}{l} \dfrac{2\pi}{w\sqrt{|d|}}\, h \text{ для } d < 0 \\ \dfrac{2 \ln \varepsilon_1}{\sqrt{|d|}}\, h \text{ для } d > 0 \end{array} \right\},$$

где w — количество корней из 1,

ε_1 — основная единица,

h — число классов поля K.

Таким образом тот основной факт, что

$$L(1 \mid \chi) = \sum_n \frac{\chi(n)}{n} = \sum_n \frac{1}{n}\left(\frac{d}{n}\right) \neq 0, \tag{11}$$

доказанный нами в § 15, п. 3 соответственно п. 4 элементарно-аналитическим, соответственно теоретико-функциональным методом, теперь снова доказан алгебраически-теоретико-числовым методом, и тем самым завершено классическое доказательство самого Дирихле его теоремы о простых числах, которое мы набросали в начале § 15, п. 5. Отметим, что для этого доказательства

используются оба истолкования характера $\chi(x) = \left(\frac{d}{x}\right)$. Именно, в алгебраически-теоретико-числовой части используется то, что для простых чисел

$\chi(p) = \left(\frac{d}{p}\right)$ есть символ Лежандра как квадратичный характер класса вычетов $d \bmod p$,

и в аналитической части то, что для натуральных чисел

$\chi(n) = \left(\frac{d}{n}\right)$ есть символ Кронекера как квадратичный характер класса вычетов $n \bmod |d|$.

Таким образом, это алгебраически-теоретико-числовое доказательство теоремы Дирихле о простых числах предполагает известным квадратичный закон взаимности, внутренний смысл которого как раз и заключается в совпадении этих двух толкований.

В виде дальнейшего следствия из предельной теоремы мы, как уже отмечалось в конце § 15, п. 5, получаем явное представление для числа классов h квадратичного поля K в аналитической форме:

II. *Для числа классов h квадратичного поля $\mathsf{K} = \mathsf{P}(\sqrt{d})$ имеет место формула*

$$h = \left\{ \begin{array}{l} \dfrac{w\sqrt{|d|}}{2\pi} L(1|\chi) \text{ для } d < 0 \\ \dfrac{\sqrt{|d|}}{2 \ln \varepsilon_1} L(1|\chi) \text{ для } d > 0 \end{array} \right\},$$

где w, ε_1 имеют значение из I *и $L(1|\chi)$ есть бесконечный ряд* (11) (*с натуральным порядком расположения членов*).

Эта формула может служить для фактического определения числа классов h, если найти в конечном виде сумму бесконечного ряда $L(1|\chi)$. Этим мы займемся в п. 2.

Для частного случая $\mathsf{K} = \mathsf{P}(\sqrt{-1})$ с $d = -4$ такая формула для суммы L-ряда известна из анализа, именно, в этом случае получается ряд Лейбница

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots = \frac{\pi}{4}.$$

Так как здесь $w = 4$, то из II мы получаем для числа классов формулу:

$$h = \frac{4 \cdot 2}{2\pi} \frac{\pi}{4} = 1,$$

что мы знаем уже из XIXA п. 6 § 16 и из § 17, п. 5. Наоборот, например, тот факт, что $\mathsf{K} = \mathsf{P}(\sqrt{-3})$ с $d = -3$ и $w = 6$ тоже

имеет число классов 1, дает нам формулу для суммы знакопеременного ряда:

$$1-\frac{1}{2}+\frac{1}{4}-\frac{1}{5}+\ldots=\frac{\pi}{3\sqrt{3}}.$$

2. Суммирование L-рядов. Мы поставим себе сейчас более общую задачу о суммировании в конечном виде L-ряда

$$L(1\,|\,\chi)=\sum_n \frac{\chi(n)}{n}$$

для любого характера $\chi\neq\varepsilon$ с натуральным ведущим модулем f.

Мы будем исходить из степенного ряда

$$G(u\,|\,\chi)=\sum_n \chi(n)\,\frac{u^n}{n}.$$

При $u=1$ этот ряд условно сходится к значению

$$G(1\,|\,\chi)=L(1\,|\,\chi),$$

а потому при $|u|<1$ сходится абсолютно. По теореме Абеля о непрерывности имеет место

$$\lim_{u\to 1-0} G(u\,|\,x)=G(1\,|\,\chi).$$

Далее,

$$G(0\,|\,\chi)=0,$$

и

$$G'(u\,|\,\chi)=\sum_n \chi(n)\,u^{n-1}$$

при $|u|<1$.

Так как коэффициенты $\chi(n)$ последнего ряда имеют период f, этот ряд можно просуммировать с помощью формулы для суммы геометрической прогрессии. Мы получаем

$$G'(u\,|\,\chi)=\sum_{k=0}^{\infty}\sum_{r=1}^{f}\chi(r)\,u^{kf+r-1}=\sum_{r=1}^{f}\chi(r)\,u^{r-1}\sum_{k=0}^{\infty}u^{kf}=-\frac{g(u\,|\,\chi)}{(u^f-1)\,u}$$

при $|u|<1$, где для краткости введено обозначение

$$g(u\,|\,\chi)=\sum_{r=1}^{f}\chi(r)\,u^r.$$

Теперь по основной теореме интегрального исчисления

$$G(u\,|\,\chi)=\int_0^u G'(v\,|\,\chi)\,dv=-\int_0^u \frac{g(v\,|\,\chi)}{v^f-1}\,\frac{dv}{v},$$

причем пока только для $|u|<1$. При $u\to 1-0$ левая часть этого равенства стремится, как уже говорилось, к значению $G(1|\chi)=L(1|\chi)$. Подинтегральное выражение в правой части при $v=1$ непрерывно; действительно, так как $\chi\neq\varepsilon$, мы имеем

$$g(1|\chi)=\sum_{r \bmod f}\chi(r)=0,$$

так что многочлен $g(v|\chi)$ делится на линейный множитель $v-1$ знаменателя (а также и на введенный из формальных соображений множитель v). Поэтому при $u\to 1-0$ интеграл $\int_0^u$ стремится к интегралу $\int_0^1$. Таким образом, указанная интегральная формула верна и для $u=1$, и тогда она дает интегральное представление

$$L(1|\chi)=-\int_0^1\frac{g(u|\chi)}{u^f-1}\frac{du}{u} \tag{1}$$

рассматриваемого L-ряда.

Так как подинтегральное выражение есть дробно рациональная функция, интеграл можно вычислить обычным способом посредством разложения подинтегральной функции на простейшие дроби. Отвлекаясь от фигурирующего только формально множителя u, мы получаем для знаменателя разложение

$$u^f-1=\prod_{x \bmod f}(u-\zeta^x)$$

на различные линейные множители, где ζ обозначает первообразный f-й корень из 1, причем для дальнейшего мы будем считать, что этот корень аналитически нормирован:

$$\zeta=e^{2\pi i/f}.$$

Числитель есть многочлен на 1 более низкой степени. Следовательно, разложение на простейшие дроби имеет простой вид

$$\frac{g(u|x)}{(u^f-1)\,u}=\sum_{x \bmod f}\frac{c_x}{u-\zeta^x}$$

с константами c_x, которые посредством умножения на $u-\zeta^x$ и подстановки значения $u=\zeta^x$ определяются так:

$$c_x=\frac{g(\zeta^x|\chi)}{\left.\frac{u^f-1}{u-\zeta^x}\right|_{u=\zeta^x}\cdot\zeta^x}=\frac{g(\zeta^x|\chi)}{f\zeta^{x(f-1)}\cdot\zeta^x}=\frac{1}{f}\,g(\zeta^x|\chi).$$

Поэтому имеет место

$$\frac{g(u\,|\,\chi)}{(u^f-1)\,u}=\frac{1}{f}\sum_{x \bmod f}\frac{g(\zeta^x\,|\,\chi)}{u-\zeta^x}. \tag{2}$$

Для x, взаимно простого с f,

$$g(\zeta^x\,|\,\chi)=\sum_{r \bmod f}\chi(r)\,\zeta^{xr}$$

есть введенная в X п. 5 § 15 гауссова сумма для характера χ с ζ^x вместо ζ. Таким образом, согласно имеющейся там формуле (2*), мы имеем

$$g(\zeta^x\,|\,\chi)=\bar{\chi}(x)\,\tau(\chi), \tag{3}$$

где

$$\tau(\chi)=g(\zeta\,|\,\chi)=\sum_{r \bmod f}\chi(r)\,\zeta^r$$

обозначает гауссову сумму для χ, образованную с помощью аналитически нормированного первообразного f-го корня $\zeta=e^{2\pi i/f}$ из 1. Однако формула (3) имеет силу также и для x, не взаимно простых с f, так как оказывается, что в этом случае $g(\zeta^x\,|\,\chi)=0$. В этом можно убедиться следующим образом.

Для любого $x \bmod f$ и c, взаимно простого с f, с одной стороны, имеет место

$$g(\zeta^{xc}\,|\,\chi)=\sum_{r \bmod f}\chi(r)\,\zeta^{xcr}=\sum_{r \bmod f}\chi(rc^{-1})\,\zeta^{xr}=\bar{\chi}(c)\,g(\zeta^x\,|\,\chi),$$

точно так же, как в § 15, п. 5 при доказательстве (2*). Если теперь $(x,\ f)=t>1$, то существует взаимно простое с f число $c\equiv 1 \bmod f/t$ с $\chi(c)\neq 1$, так как f есть ведущий модуль; с другой стороны, вследствие $xc\equiv x \bmod f$, мы имеем:

$$g(\zeta^{xc}\,|\,\chi)=g(\zeta^x\,|\,\chi).$$

Так как $\chi(c)\neq 1$, сравнение этих двух результатов необходимо дает $g(\zeta^x\,|\,\chi)=0$.

Если теперь в формулу (2) вместо $g(\zeta^x\,|\,\chi)$ подставить их выражения из (3) через нормированные гауссовы суммы $\tau(\chi)$, то для наших подинтегральных выражений получится представление

$$\frac{g(u\,|\,\chi)}{(u^f-1)\,u}=\frac{\tau(\chi)}{f}\sum_{x \bmod f}\frac{\bar{\chi}(x)}{u-\zeta^x}.$$

При этом суммирование может быть ограничено только системой вычетов $x \bmod f$, взаимно простых с модулем, что в дальнейшем все время будет молчаливо делаться для сумм, общий член кото-

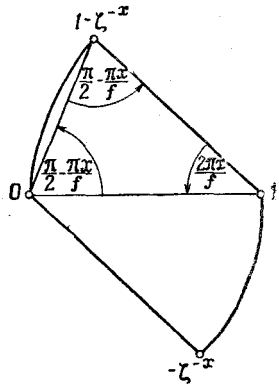
рых содержит множитель $\bar{\chi}(x)$ или $\chi(x)$. Таким образом, согласно интегральной формуле (1),

$$L(1|\chi) = -\frac{\tau(\chi)}{f} \sum_{x \bmod f} \bar{\chi}(x) \int_0^1 \frac{du}{u-\zeta^x},$$

причем из того, как была получена эта формула, явствует, что интеграл от комплексного подинтегрального выражения следует брать по прямолинейному отрезку. Чтобы перейти к обычной форме интеграла от логарифма, мы сделаем подстановку $u-\zeta^x = -\zeta^x v$. Тогда получится

$$L(1|\chi) = -\frac{\tau(\chi)}{f} \sum_{x \bmod f} \bar{\chi}(x) \int_1^{1-\zeta^{-x}} \frac{dv}{v}$$

снова с интегрированием по прямолинейному отрезку.



Фиг. 23.

Известно, что для комплексного z, не лежащего на отрицательной половине вещественной оси (включая и 0), имеет место общая формула

$$\int_1^z \frac{dv}{v} = \ln|z| + i \arg z \quad \text{с} \quad -\pi < \arg z < \pi,$$

если интегрировать по прямолинейному отрезку. Чтобы применить эту формулу к $z = 1-\zeta^{-x}$, мы в качестве $x \bmod f$ выберем наименьшую положительную систему вычетов, взаимно простых с модулем, т. е. будем считать, что

$$0 < x < f.$$

На то, что суммирование производится по этой системе вычетов, будет в дальнейшем указывать обозначение $\sum_{x \bmod f}^{+}$. Тогда, в соответствии с представлением

$$1-\zeta^{-x} = \zeta^{-\frac{x}{2}}\left(\zeta^{\frac{x}{2}} - \zeta^{-\frac{x}{2}}\right) = 2ie^{-\frac{\pi i x}{f}} \sin\frac{\pi x}{f},$$

нормирующее условие для $\arg(1-\zeta^{-x})$ будет иметь вид

$$\arg(1-\zeta^{-x}) = \frac{\pi}{2} - \frac{\pi x}{f}$$

(см. также фиг. 23), в то время как

$$|1-\zeta^{-x}| = \left|2\sin\frac{\pi x}{f}\right| = 2\sin\frac{\pi x}{f}.$$

Отсюда получается

$$L(1|\chi) = -\frac{\tau(\chi)}{f} \sum_{x \bmod f}^{+} \bar{\chi}(x) \left[\ln\left(2\sin\frac{\pi x}{f}\right) + \pi i \left(\frac{1}{2} - \frac{x}{f}\right)\right].$$

При преобразовании $x \to f - x$ наименьшей положительной системы вычетов $x \bmod f$, взаимно простых с модулем, переводящем каждый класс вычетов в симметричный ему относительно средней точки $f/2$, первый из членов этой формулы, стоящих в квадратных скобках, не изменяется, а второй меняет знак; значение $x = f/2$ при этом не встречается, так как если оно и является целым, то во всяком случае не взаимно просто с f, ибо $f > 2$. В соответствии с этим мы будем различать случаи четного и нечетного χ, как характера по модулю; согласно § 13, п. 7, эти случаи характеризуются соответствующим поведением значений характера $\chi(x)$ при преобразовании симметрии относительно среднего значения.

а) χ — *четный*. Тогда сумма вторых членов равна 0, и суммирование первых членов может быть сведено к наименьшей положительной полусистеме классов вычетов по $\bmod f$, взаимно простых с модулем, на что в дальнейшем (как уже и в § 10, п. 8) будет указывать обозначение $\sum\limits_{\pm x \bmod f}^{+}$; это обозначение, таким образом, указывает на то, что пары чисел $\pm x$ образуют полную систему вычетов по $\bmod f$, взаимно простых с модулем. Так получается окончательная формула:

$$L(1|\chi) = -\frac{2\tau(\chi)}{f(\chi)} \cdot \sum_{\pm x \bmod f(\chi)}^{+} \bar{\chi}(x) \ln\left(2\sin\frac{\pi x}{f(\chi)}\right). \qquad (4а)$$

При этом мы снова применяем для ведущего модуля f характера χ подробное обозначение $f(\chi)$, потому что в дальнейшем нам придется рассматривать эту формулу одновременно для нескольких характеров χ.

б) χ — *нечетный*. Тогда сумма первых членов равна 0, а в сумме вторых членов можно вследствие $\sum\limits_{x \bmod f} \bar{\chi}(x) = 0$ отбросить постоянные члены $\pi i / 2$. Тогда получается окончательная формула

$$L(1|\chi) = -\frac{\pi\tau(\chi)}{if(\chi)} \cdot \frac{\sum\limits_{x \bmod f(\chi)}^{+} \bar{\chi}(x)\, x}{f(\chi)}. \qquad (4б)$$

Формулы (4) дают решение нашей задачи суммирования рядов $L(1|\chi)$ в конечном виде.

3. Общая формула для числа классов. Мы воспользуемся полученными только что результатами (4) для вычисления в

конечном виде произведения L-рядов $L(1\,|\,\chi)$ для характеров $\chi \neq \varepsilon$ из какой-нибудь группы $\mathfrak{X}$, состоящей из k характеров по $\bmod m$, и тем самым получим в конечном виде указанную в конце § 15, п. 5 общую формулу для числа классов подполя K поля P_m m-х корней из 1.

Для этого мы должны заняться входящим в формулы (4) множителем $\tau(\chi)$. Согласно полученным при доказательстве X п. 5 § 15 формулам (1*), (2*), имеет место

$$\overline{\tau(\chi)} = \sum_{r \bmod f} \bar{\chi}(r)\,\zeta^{-r} = \chi(-1)\,\tau(\bar{\chi}),$$

и, таким образом,

$$\tau(\chi)\,\tau(\bar{\chi}) = \chi(-1)\,\tau(\chi)\,\overline{\tau(\chi)} = \chi(-1)\,f(\chi). \tag{1}$$

Поэтому для образования нашего произведения мы должны знать точные значения комплексных чисел $\tau(\chi)$ с абсолютной величиной $\sqrt{f(\chi)}$ только для частного случая квадратичного характера χ. В действительности эти точные значения и известны только в этом случае. Как уже было установлено в X п. 5 § 15, в случае квадратичного характера χ имеет место

$$\tau(\chi)^2 = \chi(-1)\,f(\chi),$$

так что остается «только» решить вопрос о том, какой следует брать знак квадратного корня

$$\tau(\chi) = \sqrt{\chi(-1)\,f(\chi)}.$$

Употребленное здесь словечко «только» не совсем уместно; действительно, этот вопрос отнюдь не решается элементарно, а требует применения глубоких методов анализа или арифметики. Впервые на него ответил Гаусс, причем оказывается, что знак положителен, так что нормированная квадратичная гауссова сумма

$$\tau(\chi) = \sqrt{\chi(-1)\,f(\chi)} \begin{cases} \text{вещественна и положительна} \\ \qquad\qquad\qquad \text{для } \chi(-1) = 1 \\ \text{положительно-мнима} \quad \text{для } \chi(-1) = -1 \end{cases}. \tag{2}$$

Мы дадим по возможности подробное арифметическое доказательство этого факта в § 20, п. 5, причем мы вообще в § 20 систематизируем и придадим законченный вид различным фактам относительно гауссовых сумм, разбросанным в ряде мест этой книги.

При перемножении формул (4) п. 2 нужно различать два случая.

Первый случай тот, когда все k характеров χ из заданной группы $\mathfrak{X}$ четны и потому, согласно XVIII, п. 7, § 13, все время

$\chi(-1)=1$. Тогда класс вычетов $-1 \bmod m$ лежит в соответствующей $\mathfrak{K}$ подгруппе $\mathfrak{H}$ группы классов вычетов по $\bmod m$, взаимно простых с модулем (см. § 15, п. 5, фиг. 8), т. е. автоморфизм $\zeta \to \zeta^{-1}$ оставляет инвариантным соответствующее подгруппе $\mathfrak{H}$ подполе K поля P_m m-х корней из 1; поэтому подполе K вещественно. Обратно, если K вещественно, то, рассуждая в обратном порядке, мы заключаем, что $\mathfrak{K}$ состоит только из четных характеров.

Второй случай тот, когда $\mathfrak{K}$ содержит также и нечетные характеры. Тогда четные характеры χ_0 из $\mathfrak{K}$ (т. е. характеры с $\chi_0(-1)=1$) образуют подгруппу $\mathfrak{K}_0$, а нечетные характеры χ_1 из $\mathfrak{K}$ (т. е. характеры с $\chi_1(-1)=-1$) образуют единственный смежный класс по этой подгруппе; поэтому $\mathfrak{K}$ имеет четный порядок $k=2k_0$, где k_0 — порядок $\mathfrak{K}_0$. В этом случае соответствующее группе $\mathfrak{K}$ поле K степени $k=2k_0$ комплексно и соответствующее $\mathfrak{K}_0$ поле K_0 степени k_0 есть его максимальное вещественное подполе.

После этих подготовительных соображений мы теперь перемножим формулы (4) п. 2. При этом мы будем обращать внимание только на множители

$$\frac{2\tau(\chi)}{f(\chi)} \qquad \text{для } \chi(-1)=1,$$

$$\frac{\pi\tau(\chi)}{if(\chi)} \qquad \text{для } \chi(-1)=-1$$

без знака минус, который мы отнесем к выражениям, содержащим суммы. Так как все $\tau(\chi)$ с $\chi \neq \varepsilon$ имеют абсолютную величину $\sqrt{f(\chi)}$ и $\tau(\varepsilon)=1$, $f(\varepsilon)=1$, то в произведении появится прежде всего положительный множитель

$$\frac{1}{\sqrt{F}} \quad \text{с} \quad F=\prod_{\chi \text{ из } \mathfrak{K}} f(\chi).$$

Далее, согласно формулам (1), (2) для $\tau(\chi)$, в каждом из двух различных случаев имеет место следующее.

а) K — *вещественно.* Каждая пара χ, $\bar{\chi}$ неквадратичных характеров вносит, согласно (1), множитель $\chi(-1)=1$.

Каждый квадратичный характер χ вносит, согласно (2), множитель 1.

Тогда остается учесть еще только $k-1$ множителей, равных 2. В результате получается окончательная формула

$$\prod_{\substack{\chi \text{ из } \mathfrak{K} \\ \chi \neq \varepsilon}} L(1\,|\,\chi)=\frac{2^{k-1}}{\sqrt{F}} \prod_{\substack{\chi \text{ из } \mathfrak{K} \\ \chi \neq \varepsilon}} \left(-\sum_{\pm x \bmod f(\chi)}{}^{+} \chi(x) \ln\left(2\sin\frac{\pi x}{f(\chi)}\right)\right). \quad (5a)$$

б) K — *комплексно*. В соответствии с предыдущим случаем k_0 четных характеров χ_0 вносят множитель 2^{k_0-1}.

Каждая пара χ_1, $\bar{\chi}_1$ нечетных неквадратичных характеров вносит, согласно (1), множитель $\chi_1(-1) = -1 = i^2$.

Каждый нечетный квадратичный характер χ_1 вносит, согласно (2), множитель i (корень четвертой степени из 1).

Поэтому k_0 нечетных характеров χ_1 вместе вносят множитель i^{k_0}, являющийся корнем четвертой степени из 1. Он как раз уничтожается k_0 множителями i, стоящими в знаменателях.

Остается еще учесть k_0 числовых множителей, равных π.

В результате получается окончательная формула

$$\prod_{\substack{\chi \text{ из } \mathfrak{R} \\ \chi \neq \varepsilon}} L(1|\chi) = \frac{2^{k_0-1}(2\pi)^{k_0}}{\sqrt{F}} \times$$

$$\times \prod_{\substack{\chi_0 \neq \varepsilon \text{ из } \mathfrak{R} \\ \chi_0(-1)=1}} \left(- \sum_{\pm x \bmod f(\chi_0)}^{+} \chi_0(x) \ln\left(2 \sin \frac{\pi x}{f(\chi_0)}\right)\right) \times$$

$$\times \prod_{\substack{\chi_1 \text{ из } \mathfrak{R} \\ \chi_1(-1)=-1}} \left(\frac{\sum_{x \bmod f(\chi_1)}^{+} \chi_1(x)\, x}{2f(\chi_1)} \right). \qquad (5б)$$

При желании мы можем вынести из знаменателя второго произведения k_0 множителей, равных 2, и сократить их с множителями 2 при π; это целесообразно с арифметической точки зрения.

Если теперь применить результаты (5) к выведенной в конце § 15, п. 5 формуле

$$h = \frac{w\sqrt{|d|}}{(2\tilde{\omega})^{\frac{1}{2}k} \cdot R} \prod_{\substack{\chi \text{ из } \mathfrak{R} \\ \chi \neq \varepsilon}} L(1|\chi) = \left\{ \begin{array}{c} \dfrac{\sqrt{|d|}}{2^{k-1}R} \\ \dfrac{w\sqrt{|d|}}{(2\pi)^{k_0} R} \end{array} \right\} \prod_{\substack{\chi \text{ из } \mathfrak{R} \\ \chi \neq \varepsilon}} L(1|\chi) \qquad (6)$$

для числа классов, то она примет сначала вид

$$h = \left\{ \begin{array}{ll} \dfrac{1}{R}\sqrt{\dfrac{|d|}{F}} \prod_{\chi \neq \varepsilon}, & \text{если } \mathsf{K} \text{ — вещественно} \\ \dfrac{w}{2^{-k_0+1} R}\sqrt{\dfrac{|d|}{F}} \cdot \prod_{\chi_0 \neq \varepsilon} \cdot \prod_{\chi_1}, & \text{если } \mathsf{K} \text{ — комплексно} \end{array} \right\},$$

где для краткости вместо произведений из формул (5) стоят только одни знаки произведений.

Относительно полученных таким образом конечных формул для числа классов нужно сделать еще два замечания.

Во-первых, можно показать, что введенное перед этим произведение ведущих модулей имеет значение

$$F = \prod_{\chi \text{ из } \mathfrak{R}} f(\chi) = |d|,$$

так что для стоящего перед произведением дополнительного множителя имеет место $\sqrt{|d|}/F = 1$. Мы получим этот факт, если в усиление теоремы о дискриминанте из § 15, п. 5 точно определим для полей K рассматриваемого здесь типа те показатели, с которыми входят в дискриминант d поля K отдельные простые числа, разветвляющиеся в K. Для квадратичных полей K мы знаем эту связь уже из рассуждений в начале § 17, п. 2.

Во-вторых, оказывается, что в случае комплексного поля K выражение $2^{-k_0+1}R$ совпадает или почти совпадает с регулятором R_0 максимального вещественного подполя K_0. Из формулы в § 15, п. 5, определяющей R, видно, что в комплексном случае из k_0-строчного определителя R можно вынести как раз множитель 2^{k_0-1}, после чего остается определитель только из логарифмов с абсолютными величинами, равными 1. Тогда можно показать, что между этим определителем $2^{-k_0+1}R$ и R_0 существует связь

$$R_0 = Q \cdot \frac{R}{2^{k_0-1}},$$

где дополнительный множитель

$$Q = 1 \quad \text{или} \quad 2,$$

в зависимости от того, является ли система основных единиц поля K_0 таковой также и для K или не является. Этот дополнительный множитель Q является еще одним арифметическим инвариантом поля K, который называется индексом единиц для K/K_0, так как он показывает, какой индекс имеет группа модулей единиц поля K_0 в группе модулей единиц поля K. Для мнимого квадратичного поля K тривиальным образом $Q = 1$.

Заметим теперь, что, согласно формуле для вещественного случая, частичное произведение $\frac{1}{R_0}\prod_{\chi_0 \neq \varepsilon}$, входящее в формулу для комплексного случая, как раз равно числу классов h_0 поля K_0, так что формула для числа классов h подполя K поля P_m корней из 1 принимает следующий окончательный вид:

$$h = \frac{1}{R}\prod_{\substack{\chi \text{ из } \mathfrak{R} \\ \chi \neq \varepsilon}} \left(- \sum_{\pm x \bmod f(\chi)}^{+} \chi(x) \ln\left(2 \sin \frac{\pi x}{f(\chi)}\right)\right), \tag{7a}$$

если K вещественно

$$h = Qwh_0 \prod_{\substack{\chi \text{ из } \mathfrak{X} \\ \chi(-1) = -1}} \left(\frac{\sum\limits_{-x \bmod f(\chi)}^{+} \chi(x)\, x}{2f(\chi)} \right), \tag{7б}$$

если K *комплексно.*

При этом

R — *регулятор поля* K,

w — количество корней из 1 поля K,

Q — индекс единиц для K/K_0,

h_0 — число классов поля K_0,

где K_0 есть максимальное вещественное подполе поля K и χ пробегает характеры (с указанными свойствами) из соответствующей полю K группы характеров $\mathfrak{X}$, которые получаются из характеров группы Галуа поля K, если представить ее как фактор-группу $\mathfrak{G}/\mathfrak{H}$ группы классов вычетов по $\bmod m$, взаимно простых с модулем.

Чтобы закончить доказательство формул (7) для числа классов нужно, конечно, доказать аналитическую формулу (6), которая в свою очередь является непосредственным следствием из предельной теоремы в § 15, п. 5. Для выполнения этого нужно обобщить на любые подполя K поля корней из 1 изложенную в § 16, 17 по методу Куммера арифметику квадратичных полей и доказать тогда предельную теорему посредством соответствующего обобщения на эти произвольные подполя K геометрического вывода из п. 1. Сам Куммер развил свой метод не для квадратичных полей, а для всего поля P_m корней из 1, причем сначала для частного случая простого числа $m = p$, а позднее и для общего случая; им была получена и формула (7) для числа классов. Этими указаниями мы здесь и ограничимся.

Весьма заманчиво подробнее рассмотреть арифметическую структуру куммеровской формулы (7) для числа классов. Так как h означает число классов, сложные выражения в правых частях представляют натуральные числа. Однако сразу этого не видно и сначала кажется даже, что для фактического вычисления таблиц чисел классов нужно привлекать тригонометрические функции и логарифмы, т. е. средства, которые с арифметической точки зрения являются чуждыми и нежелательными. В своей монографии [1] о куммеровской формуле для числа классов я подробно исследовал этот вопрос — так же как не менее трудный вопрос об определении индекса единиц Q — и изложил метод, с помощью которого из этих формул можно вычислять число классов чисто арифметически (т. е. не прибегая к таблицам).

Для случая квадратичного поля эти вопросы сейчас будут рассмотрены.

4. Формула для числа классов квадратичного поля. После этого отступления в п. 3 к общему случаю, где мы дополнили некоторыми выводами общий обзор из § 15, п. 5, мы снова возвращаемся к последовательному исследованию квадратичного случая из п. 1 и 2.

Из окончательных формул (4) п. 2 для сумм L-рядов, посредством их подстановки в аналитическую формулу II, п. 1 для числа классов, мы, принимая на веру определение знака (2) п. 3 нормированной квадратичной гауссовой суммы $\tau(\chi)$, которое будет сделано в § 20, п. 5, и замечая, что

$$f(\chi) = |d| \quad \text{и} \quad \chi(x) = \left(\frac{d}{x}\right),$$

немедленно получаем

III. *Для числа классов h квадратичного поля* $\mathsf{K} = \mathsf{P}(\sqrt{d})$, *имеют место формулы*

$$h = w \frac{-\sum_{x \bmod |d|}^{+} \left(\frac{d}{x}\right) x}{2|d|} \qquad \text{для } d < 0,$$

$$h = \frac{-\sum_{\pm x \bmod d}^{+} \left(\frac{d}{x}\right) \ln\left(2 \sin \frac{\pi x}{d}\right)}{\ln \varepsilon_1} \qquad \text{для } d > 0,$$

или также

$$\varepsilon_1^h = \prod_{\pm x \bmod d}^{+} \left(2 \sin \frac{\pi x}{d}\right)^{-\left(\frac{d}{x}\right)} \qquad \text{для } d > 0,$$

где w есть количество корней из 1, соответственно ε_1 — основная единица поля K.

При этом для $d > 0$ (K — вещественно) мы перешли от аддитивной записи с логарифмами к мультипликативной записи, что здесь — в отличие от общего случая (7а) п. 3 — возможно, потому что регулятор $R = \ln \varepsilon_1$ является здесь определителем матрицы первого порядка и фигурируют только два целых рациональных значения характера $\chi(x) = \left(\frac{d}{x}\right) = \pm 1$.

Часто записывают эти формулы также и в следующем сокращенном виде:

$$h = \frac{w}{2} \frac{\sum_{b}^{+} b - \sum_{a}^{+} a}{|d|} \qquad \text{для } d < 0, \qquad (1\text{а})$$

$$\varepsilon_1^h = \frac{\prod\limits_{\pm b}^{+} 2\sin\frac{\pi b}{d}}{\prod\limits_{\pm a} 2\sin\frac{\pi a}{d}} \qquad \text{для } d>0, \tag{1б}$$

где a, b пробегают числа наименьшей положительной системы вычетов, соответственно полусистемы по $\bmod|d|$ - т. е. в каждом случае (см. § 9, п. 5) числа наименьшей положительной полусистемы по $\bmod d$ – с $\left(\frac{d}{a}\right)=1$, $\left(\frac{d}{b}\right)=-1$. Согласно квадратичному закону взаимности, эти числа характеризуются также посредством теоретико-группового разбиения из VI, п. 6, § 9 классов вычетов по $\bmod d$, взаимно простых с модулем, именно, как числа a из определенной там группы $\mathfrak{H}$ и числа b из смежного класса $\mathfrak{G}-\mathfrak{H}$. В дальнейшем они будут кратко называться «вычетами» и «невычетами», хотя только в случае простого дискриминанта $d=p^*$ речь идет действительно о квадратичных вычетах и невычетах по $\bmod p$ в обычном смысле (ср. замечание к III, п. 2, § 9).

Для $d>0$ множители 2 в числителе и в знаменателе можно было бы сократить; действительно, для $d>0$ символ Кронекера $\left(\frac{d}{x}\right)$ является четным не только как числовая функция, но, согласно XVIII, п. 7, § 13, также и как характер по модулю, откуда следует $\sum\limits_{\pm x \bmod d}^{+}\left(\frac{d}{x}\right)=0$, так что «вычеты» a и «невычеты» b имеются в одном и том же количестве $\varphi(d)/4$. Однако из арифметических соображений, которые в дальнейшем станут понятны, целесообразнее эти множители 2 оставить и даже приписать к ним еще множители i.

В соответствии со значением h как числа классов поля $\mathfrak{K}$ выражения в правых частях первоначальных формул из III представляют натуральные, т. е. целые рациональные положительные числа. Однако непосредственно это не очевидно. В случае $d<0$ очевидна, по крайней мере, их рациональность, в случае же $d>0$ не очевидно и это. Мы поставим себе задачу сделать непосредственно ясным арифметический характер этих выражений. Эта задача распадается на две части: во-первых, нужно доказать положительность и, во-вторых, – рациональность и целостность.

А. *Положительность.* Положительность h в формулах (1) равносильна некоторому утверждению относительно распределения «вычетов» и «невычетов» в наименьшей положительной полусистеме по $\bmod d$. Формула (1а) в этом отношении гласит, что

среднее арифметическое невычетов больше, чем среднее арифметическое вычетов. Формула (1б) означает соответственно, что образованное с помощью функции $2\sin\frac{\pi x}{d}$ мультипликативное выражение имеет для невычетов большее значение, чем для вычетов.

Эти утверждения относительно распределения принадлежат к другому типу, чем те, которые для частного случая простого модуля $p \neq 2$ рассматривались в § 10. Теперешние утверждения лежат значительно глубже. Источником, из которого они получились, является доказанная аналитическим путем формула для числа классов. В недавнее время Б. А. Венков [1] дал для отрицательных дискриминантов $d \not\equiv 1 \bmod 8$ чисто арифметическое доказательство формул Дирихле для числа классов и тем самым также и первого из указанных высказываний о распределении; его доказательство опирается на теорию тройничной квадратичной формы $x^2+y^2+z^2$ и разложение в непрерывные дроби. Этим указанием мы здесь ограничимся.

Сделаем, однако, еще два замечания по этому вопросу.

Во-первых, отметим, что если не использовать точное определение (2) п. 3 знака нормированной квадратичной гауссовой суммы, то формулы из III получаются с неопределенным знаком, который равен как раз знаку этой гауссовой суммы. Прямое доказательство положительности выражений, о которых идет здесь речь, даст тогда окольное определение знака нормированной квадратичной гауссовой суммы.

Во-вторых, отметим, что прямое доказательство положительности для квадратичного случая тотчас же дает соответствующее высказывание о положительности числа классов в общей формуле (7) п. 3; действительно, в стоящих там произведениях члены, соответствующие неквадратичным характерам, объединяются в пары комплексно сопряженных чисел, произведение которых каждый раз положительно. Поэтому общая формула (7) п. 3 для числа классов не дает существенно новых высказываний относительно распределения значений характеров в системе вычетов по $\bmod m$, взаимно простых с модулем.

Б. *Рациональность и целочисленность.* Доказательство рациональности и целочисленности выражений для h из III мы свяжем в каждом из случаев $d \gtrless 0$ с преобразованием этих выражений к новому виду, который в случае $d<0$ удобнее для фактического вычисления h, а в случае $d>0$ вообще делает его впервые возможным чисто арифметическим способом.

а) *Мнимое квадратичное поле* ($d<0$). Согласно VIIIa, п. 4, § 16, вообще говоря, $w=2$; только для двух наименьших по абсолютной величине отрицательных дискриминантов $d=-3$, -4 будет $w=6$, 4.

Мы исследуем сначала эти исключительные случаи $d=-3$, -4, чтобы потом можно было отвлечься от них из соображений единообразия. Формула (1а) дает для них

$$h=3\cdot\frac{2-1}{3}=1, \quad \text{соответственно} \quad h=2\cdot\frac{3-1}{4}=1,$$

что нам известно уже из XIXA, п. 6, § 16 или § 17, п. 5.

Для всех остальных отрицательных дискриминантов d формула для числа классов из III принимает более простой вид:

$$h=\frac{-\sum\limits_{x \bmod |d|}^{+}\left(\frac{d}{x}\right)x}{|d|} \qquad (d\neq -3,\ -4). \tag{2а}$$

Сведем суммирование здесь к наименьшей положительной полусистеме вычетов по $\bmod|d|$, взаимно простых с модулем. Так как $\left(\frac{d}{x}\right)$ как характер по модулю является нечетным (см. XVIII, п. 7, § 13), это сведение дает

$$h=\sum_{\pm x \bmod |d|}^{+}\left(\frac{d}{x}\right)-\frac{2\sum\limits_{\pm x \bmod |d|}^{+}\left(\frac{d}{x}\right)x}{|d|} \qquad (d=-3,\ -4). \tag{3а}$$

Эта формула удобнее для численных подсчетов, так как в ней (подобно тому, как в случае $d>0$) нужно рассматривать только взаимно простые с модулем вычеты $x \bmod|d|$ с $0<x<|d|/2$.

Рациональная целостность h в формуле (3а) вытекает из следующего факта, который легко можно доказать чисто арифметически:

IVa. *Сумма*

$$S=\sum_{\pm x \bmod |d|}^{+}\left(\frac{d}{x}\right)x$$

обладает для $d\neq -3,\ -4$ *свойством*

$$S\equiv 0\left\{\begin{array}{lll}\bmod|d| & \text{для} & 2\nmid d\\ \bmod\frac{1}{2}|d| & \text{для} & 2\mid d\end{array}\right\}.$$

Доказательство. Чтобы сделать это высказывание независящим от выбора полусистемы $x \bmod|d|$, мы от символа Кронекера $\left(\frac{d}{x}\right)$ с ведущим модулем d, который хотя и нечетен как характер по модулю, но четен как числовая функция, перейдем к нечетному в том и другом смысле характеру

$$\chi(x)=\operatorname{sgn}x\left(\frac{d}{x}\right)$$

с ведущим модулем $|d|$ (см. § 13, п. 7). Так как $\chi(x)=\left(\frac{d}{x}\right)$ для $x>0$, в определении S можно заменить $\left(\frac{d}{x}\right)$ на $\chi(x)$ и, так как класс вычетов $x \bmod |d|$ тоже нечетен в том и другом смысле, а потому класс вычетов $\chi(x)\, x \bmod |d|$ является четным в обоих смыслах, мы получаем, что после этой замены значение по $\bmod |d|$

$$S \equiv \sum_{\pm x \bmod |d|} \chi(x)\, x \qquad \bmod |d|$$

не будет зависеть от выбора полусистемы по $\bmod |d|$.

Если a взаимно просто с d, то вместе с x также и ax пробегает полусистему классов вычетов по $\bmod |d|$, взаимно простых с модулем. Поэтому значение $S \bmod |d|$ имеет свойство

$$\chi(a)\, aS \equiv S \bmod |d| \quad \text{для } (a, d)=1.$$

Следовательно, утверждение будет доказано, если для каждого простого делителя $p \neq 2$ числа d удастся найти взаимно простое с d положительное a_p со свойством

$$\chi(a_p)\, a_p \not\equiv 1 \bmod p, \quad \text{или} \quad a_p \not\equiv \left(\frac{d}{a_p}\right) \bmod p,$$

и, в случае $2 \mid d$, еще и взаимно простое с d положительное a_2 со свойством

$$\chi(a_2)\, a_2 \not\equiv 1 \bmod 4, \quad \text{или} \quad a_2 \not\equiv \left(\frac{d}{a_2}\right) \bmod 4.$$

Это действительно можно сделать, если $d \neq -3, -4$.

Если сначала $p \neq 2, 3$, то существует взаимно простое с p число $a_p \not\equiv \pm 1 \bmod p$, которое при этом может быть выбрано еще взаимно простым с d и положительным. Тогда оно будет удовлетворять поставленному выше требованию.

Далее, если $p=3$ и $d=-3d_0$, то так как $d \neq -3$, d_0 будет положительным, не равным квадрату числом; если бы для всех взаимно простых с d положительных a выполнялось сравнение

$$a \equiv \left(\frac{d}{a}\right) \bmod 3,$$

то из него, в силу

$$a \equiv \left(\frac{-3}{a}\right) \bmod 3,$$

следовало бы, что для всех взаимно простых с d положительных a выполняется сравнение

$$1 \equiv \left(\frac{d_0}{a}\right) \bmod 3,$$

т. е. что для всех этих a — а потому и для всех взаимно простых только с d_0 чисел a любого знака — имеет место $\left(\frac{d_0}{a}\right)=1$. Но так как d_0 не есть квадрат, то, согласно VI, п. 6, § 9, это невозможно.

Если, наконец, $2\mid d$ и $d=-4d_0$, где d_0 вследствие $d\neq -4$ является в этом случае положительным, не равным квадрату числом, и если предположить, что для всех взаимно простых с d положительных a выполняется сравнение

$$a\equiv\left(\frac{d}{a}\right)\bmod 4,$$

то, в силу

$$a\equiv\left(\frac{-4}{a}\right)\bmod 4,$$

снова следовало бы, что все взаимно простые с d положительные a удовлетворяют сравнению

$$1\equiv\left(\frac{d_0}{a}\right)\bmod 4,$$

т. е. для всех этих a — а тогда и для всех взаимно простых только с d_0 чисел a любого знака — имеет место $\left(\frac{d_0}{a}\right)=1$. Но так как d_0 не есть квадрат, это снова невозможно, согласно VI, п. 6, § 9.

Этим доказано предложение IVa и, согласно вышесказанному, вместе с тем получено также чисто арифметическое доказательство целочисленности.

Помимо этого доказательства, которое является чисто арифметическим установлением уже полученного аналитическим путем факта, из формулы для числа классов можно получить и новые арифметические факты. Мы ограничимся здесь следующим утверждением, для которого в § 19, п. 4 будет дано чисто арифметическое доказательство:

Va. *Мнимые квадратичные поля* $\mathsf{K}=\mathsf{P}(\sqrt{d})$, *дискриминанты которых* d *содержат только одно простое число* p, *т. е. поля*

$$\mathsf{K}=\mathsf{P}(\sqrt{-1}),\ \mathsf{P}(\sqrt{-2}),\ \mathsf{P}(\sqrt{-p})\ \ (p\equiv -1\bmod 4),$$

имеют нечетное число классов h.

Доказательство. Для $\mathsf{P}(\sqrt{-1})$ $(d=-4)$ и $\mathsf{P}(\sqrt{-3})$ $(d=-3)$ $h=1$. Для $\mathsf{P}(\sqrt{-2})$ $(d=-8)$ согласно (2a), также

$$h=\frac{(5+7)-(1+3)}{8}=1.$$

Для $\mathsf{P}(\sqrt{-p})$ с $p \neq 2,\ 3$ и $p \equiv -1 \bmod 4$ $(d = -p)$ значение $h \bmod 2$ получается, согласно (2а) и вследствие $\left(\frac{-p}{x}\right) \equiv 1 \bmod 2$, в виде

$$h \equiv \sum_{x \bmod p}^{+} x = \frac{p(p-1)}{2} \equiv \frac{p-1}{2} \equiv 1 \bmod 2.$$

Заметим, что посредством обобщения этого приема можно доказать, что для любого отрицательного дискриминанта d, содержащего точно r различных простых чисел, число классов h делится на степень 2^{r-1}; по поводу этого вопроса мы отсылаем читателя к моей монографии [1]. Чисто арифметически этот факт вытекает из так называемой теории родов квадратичных полей, которую мы в настоящей книге рассматривать не будем.

Практическое вычисление h при заданном d с помощью формулы (3а) мы проиллюстрируем на примере $d = -23$, который мы уже предлагали читателю в § 17, п. 5:

x	1	2	3	4	5	6	7	8	9	10	11
$\left(\frac{d}{x}\right)$	+	+	+	+	−	+	−	+	+	−	−

$$\sum_{\pm x \bmod |d|}^{+} \left(\frac{d}{x}\right) = 3, \qquad \sum_{\pm x \bmod |d|} \left(\frac{d}{x}\right) x = 0,$$

$$h = 3 - \frac{2 \cdot 0}{23} = 3.$$

Этот пример показывает, что, в отличие от случая $d > 0$, для $d < 0$ наименьшая положительная полусистема по $\bmod |d|$ не обязательно содержит одинаковое количество «вычетов» a и «невычетов» b; наименьшая же положительная система вычетов по $\bmod |d|$, лежащая в основе первоначальной формулы (2а), конечно, содержит одинаковое количество $\varphi(|d|)/2$ тех и других.

б) *Вещественное квадратичное поле* $(d > 0)$. В формуле для числа классов из III фигурируют значения функций $2\sin(\pi x/d)$, к которым, как уже там говорилось, мы можем, в случае надобности, приписать еще множители i. В соответствии с получением этих значений в п. 2 мы запишем их снова в виде

$$2i \sin \frac{\pi x}{d} = \zeta^{\frac{x}{2}} - \zeta^{-\frac{x}{2}} = \mathsf{Z}^x - \mathsf{Z}^{-x},$$

где

$$\zeta = e^{\frac{2\pi i}{d}}, \quad \mathsf{Z} = \zeta^{\frac{1}{2}} = e^{\frac{\pi i}{d}}$$

суть аналитически нормированные первообразные корни из 1 степеней d и $2d$. Тогда формула для числа классов гласит:

$$\varepsilon_1^h = \prod_{\pm x \bmod d}^{+} (\mathsf{Z}^x - \mathsf{Z}^{-x})^{-\left(\frac{d}{x}\right)}. \tag{2б}$$

Целочисленность и рациональность числа h в этой формуле равносильна тому, что число

$$\varepsilon = \prod_{\pm x \bmod d}^{+} (\mathsf{Z}^x - \mathsf{Z}^{-x})^{-\left(\frac{d}{x}\right)}$$

из поля $\mathsf{P}_{2d} = \mathsf{P}(\mathsf{Z})$ $2d$-х корней из 1 в действительности принадлежит содержащемуся в нем (и даже уже в $\mathsf{P}_d = \mathsf{P}(\zeta)$), согласно X, п. 5, § 15, подполю $\mathsf{K} = \mathsf{P}(\sqrt{d})$ и является единицей. Число классов h есть тогда показатель степени основной единицы ε_1 поля K, дающей эту так называемую круговую единицу, и это значение может быть взято за исходный пункт при фактическом вычислении h при заданном d.

В соответствии с этим мы докажем сейчас чисто арифметически

IVб. *Число*

$$\varepsilon = \prod_{\pm x \bmod d}^{+} (\mathsf{Z}^x - \mathsf{Z}^{-x})^{-\left(\frac{d}{x}\right)}$$

из поля $\mathsf{P}_{2d} = \mathsf{P}(\mathsf{Z})$ *корней из* 1 *принадлежит квадратичному подполю* $\mathsf{K} = \mathsf{P}(\sqrt{d})$ *и является единицей.*

Доказательство. а) Как было выведено в § 15, п. 5, группа Галуа поля $\mathsf{P}_{2d} = \mathsf{P}(\mathsf{Z})$ определяется подстановками $\mathsf{Z} \to \mathsf{Z}^c$ с c, взаимно простыми с $2d$, и потому изоморфна группе $\mathfrak{G}$ классов вычетов $c \bmod 2d$, взаимно простых с модулем.

Подполе $\mathsf{P}_d = \mathsf{P}(\zeta)$ обладает различными свойствами, в зависимости от того, четно d или нечетно.

Для d нечетного будет $\mathsf{Z} = -\zeta^{(d+1)/2}$ и потому $\mathsf{P}_{2d} = \mathsf{P}_d$, что ясно также из равенства степеней $\varphi(2d) = \varphi(d)$ этих полей.

Для d четного $\varphi(2d) = 2\varphi(d)$, и потому степень $\mathsf{P}_{2d} = \mathsf{P}(\sqrt{\zeta})$ относительно P_d равна 2. В этом случае числа из P_d характеризуются среди всех чисел из P_{2d} тем, что они инвариантны относительно автоморфизма

$$(\sqrt{\zeta} \to -\sqrt{\zeta}) = (\mathsf{Z} \to -\mathsf{Z}) = (\mathsf{Z} \to \mathsf{Z}^{1+d}).$$

Согласно X, п. 5, § 15, числа подполя $\mathsf{K} = \mathsf{P}(\sqrt{d})$ характеризуются среди чисел из $\mathsf{P}_d = \mathsf{P}(\zeta)$ тем, что они инвариантны относительно автоморфизмов $\zeta \to \zeta^a$ с $\left(\frac{d}{a}\right) = 1$. Мы будем счи-

тать, что классы вычетов $a \bmod d$, взаимно простые с модулем, обладающие этим свойством, представлены нечетными и потому взаимно простыми даже с $2d$ числами (для нечетного d этого можно добиться, совершая в случае надобности переход от a к $a+d$, для четного d это заранее имеет место). Тогда автоморфизмы $\zeta \to \zeta^a$ поля P_d можно в каждом случае рассматривать как порожденные автоморфизмами $\mathsf{Z} \to \mathsf{Z}^a$ поля P_{2d} (причем последние при заданном $a \bmod d$ определены для нечетного d однозначно, а для четного d — с точностью только до произвольного дополнительного автоморфизма $\mathsf{Z} \to \pm \mathsf{Z}$).

Согласно всему сказанному, для того чтобы показать, что ε принадлежит подполю K, нужно установить два следующих факта:

1) (*Принадлежность к* P_d). *При четном* d, ε *инвариантно относительно автоморфизма* $\mathsf{Z} \to -\mathsf{Z}$.

2) (*Принадлежность даже к* K). *В каждом случае* ε *инвариантно относительно автоморфизмов* $\mathsf{Z} \to \mathsf{Z}^a$ *с нечетными* a, *для которых* $\left(\frac{d}{a}\right) = 1$.

Доказательство. 1) Для четного d полусистема вычетов $x \bmod d$, взаимно простых с модулем, состоит только из нечетных чисел x. Поэтому при $\mathsf{Z} \to -\mathsf{Z}$ для каждого сомножителя нашего произведения имеет место $(\mathsf{Z}^x - \mathsf{Z}^{-x}) \to -(\mathsf{Z}^x - \mathsf{Z}^{-x})$, и потому для всего произведения, вследствие $\sum\limits_{\pm x \bmod d}^{+} \left(\frac{d}{x}\right) = 0$, получается $\varepsilon \to \varepsilon$.

2) Это доказательство не так просто. Прежде всего заметим следующее. Отдельные сомножители $\mathsf{Z}^x - \mathsf{Z}^{-x}$ нашего произведения инвариантны относительно подстановок $x \to d - x$. Поэтому для нечетного d посредством таких подстановок можно перейти от наименьшей положительной полусистемы по $\bmod d$ к полусистеме $x \cdot \bmod d$, состоящей сплошь из нечетных чисел $0 < x < d$, именно, к наименьшей положительной полусистеме по $\bmod 2d$ (вычеты этой полусистемы будут взаимно просты с модулем $2d$, так как вычеты исходной системы были взаимно просты с d). Для четного d уже первоначальная наименьшая положительная полусистема вычетов по $\bmod d$, взаимно простых с модулем, состоит сплошь из нечетных x. В соответствии с этим мы запишем наше произведение в виде

$$\varepsilon = \prod_{\pm x \bmod \hat{d}}^{+} (\mathsf{Z}^x - \mathsf{Z}^{-x})^{-\left(\frac{d}{x}\right)} \quad \text{с} \quad \hat{d} = \begin{cases} 2d & \text{для } 2 \nmid d \\ d & \text{для } 2 \mid d \end{cases},$$

где все x теперь нечетны. Тогда нам нужно показать, что для нечетного a с $\left(\frac{d}{a}\right)=1$ имеет место

$$\varepsilon^{(a)}=\prod_{\pm x \bmod \hat{d}}{}^{+}\ (Z^{ax}-Z^{-ax})^{-\left(\frac{d}{x}\right)}=\varepsilon.$$

Для этого мы произведем сведение полусистемы $ax \bmod \hat{d}$ к наименьшей положительной полусистеме вычетов $x \bmod \hat{d}$, взаимно простых с модулем; мы будем действовать по образцу доказательства леммы Гаусса из § 6, п. 6, но в более общем виде. Наше сведение имеет вид

$$ax \equiv \left\{\begin{array}{ll}(-1)^{\alpha_x}x' \bmod 2d & \text{для } 2\nmid d\\ (-1)^{\alpha_x}x'+\beta_x d\equiv(-1)^{\alpha_x}x'\,(1+d)^{\beta_x} \bmod 2d & \text{для } 2\mid d\end{array}\right\}$$

с некоторой перестановкой x' вычетов x и показателями α_x, $\beta_x \bmod 2$. Так как $Z^{x'}-Z^{-x'}$, как при $x'\to -x'$, так и при $x'\to x'(1+d)$ только меняет свой знак, мы будем иметь

$$Z^{ax}-Z^{-ax}=\left\{\begin{array}{ll}(-1)^{\alpha_x}(Z^{x'}-Z^{-x'}) & \text{для } 2\nmid d\\ (-1)^{\alpha_x+\beta_x}(Z^{x'}-Z^{-x'}) & \text{для } 2\mid d\end{array}\right\},$$

и вследствие $\left(\frac{d}{x}\right)=\left(\frac{d}{ax}\right)=\left(\frac{d}{(-1)^{\alpha_x}x'}\right)=\left(\frac{d}{x'}\right)$ тем самым

$$\varepsilon^{(a)}=\left\{\begin{array}{ll}(-1)^{\alpha}\varepsilon & \text{для } 2\nmid d\\ (-1)^{\alpha+\beta}\varepsilon & \text{для } 2\mid d\end{array}\right\}$$

с

$$\alpha\equiv\sum_{\pm x \bmod \hat{d}}{}^{+}\alpha_x,\quad \beta\equiv\sum_{\pm x \bmod \hat{d}}{}^{+}\beta_x \bmod 2.$$

Таким образом, наше утверждение сводится к доказательству того, что для фигурирующих здесь сумм показателей имеет место α, соответственно $\alpha+\beta\equiv 0 \bmod 2$.

Подобно тому как в доказательстве леммы Гаусса, посредством перемножения $\varphi(d)/2$ сравнений, полученных в процессе редукции, мы приходим к сравнению

$$a^{\frac{1}{2}\varphi(d)}\equiv\left\{\begin{array}{ll}(-1)^{\alpha} \bmod 2d & \text{для } 2\nmid d\\ (-1)^{\alpha}(1+d)^{\beta}\equiv(-1)^{\alpha}+\beta d \bmod 2d & \text{для } 2\mid d\end{array}\right\}.$$

Отсюда можно следующим образом определить значения суммы показателей по $\bmod 2$.

Если $2 \nmid d$ и $d = p \,(\equiv 1 \bmod 4)$ — простое число, то, согласно предположению, $\left(\frac{p}{a}\right) = \left(\frac{a}{p}\right) = 1$, и потому, в силу критерия Эйлера,

$$a^{\frac{1}{2}\varphi(d)} = a^{\frac{p-1}{2}} \equiv 1 \bmod p, \text{ следовательно, и по } \bmod 2d, \qquad (4_1)$$

причем последнее заключение сделано потому, что a должно быть нечетным. Отсюда следует $\alpha \equiv 0 \bmod 2$.

Если $2 \nmid d$ и $d = pp' \ldots$ есть произведение нескольких (различных) простых чисел, то

$$\frac{1}{2}\varphi(d) = \frac{1}{2}\varphi(p)\varphi(p') \ldots \equiv 0 \bmod \varphi(p),\ \varphi(p'), \ldots,$$

и потому, согласно малой теореме Ферма, для отдельных простых множителей имеет место

$$a^{\frac{1}{2}\varphi(d)} \equiv 1 \bmod p,\ p', \ldots, \text{ следовательно, и по } \bmod 2d, \qquad (5_1)$$

причем последнее снова вытекает из того, что a должно быть нечетным. Отсюда опять вытекает $\alpha \equiv 0 \bmod 2$.

Если $2 \mid d$ и $d = 8$, то по предположению $\left(\frac{2}{a}\right) = 1$, откуда $a \equiv \pm 1 \bmod 8$, и потому

$$a^{\frac{1}{2}\varphi(d)} = a^2 \equiv 1 \bmod 16, \text{ следовательно и по } \bmod 2d. \qquad (4_2)$$

Отсюда следует $\alpha \equiv 0,\ \beta \equiv 0 \bmod 2$.

Если $2 \mid d$ и $d = 4p \ldots$ или $8p \ldots$ с по крайней мере одним нечетным простым числом, то как и перед этим,

$$\frac{1}{2}\varphi(d) \equiv 0 \bmod 2, \text{ соответственно } 4,\ \varphi(p), \ldots,$$

и потому

$$a^{\frac{1}{2}\varphi(d)} \equiv 1 \bmod 8, \text{ соответственно } 16,\ p, \ldots, \text{ следовательно, и по } \bmod 2d. \qquad (5_2)$$

Отсюда снова следует $\alpha \equiv 0,\ \beta \equiv 0 \bmod 2$.

Таким образом, согласно уже сказанному, принадлежность числа ε подполю K доказана.

б) Остается показать, что ε является единицей. При этом мы будем опираться (как уже в § 8, п. 4, 5) на элементарную теорию делимости в $\mathsf{P}_d = \mathsf{P}(\zeta)$, определяемую областью целостности $\mathfrak{l}_d = \Gamma[\zeta]$. Эта область целостности во всяком случае удовлетворяет соответствующим образом обобщенным требованиям А, Б, В из § 16, п. 3; то, что она удовлетворяет также и указанному там требованию максимальности Г, нам здесь не понадобится. Пересечение $\mathfrak{l}_d \cap \mathsf{K}$ содержится в области цело-

стности $\mathfrak{l}$ целых чисел поля K; действительно, для чисел этого пересечения главные многочлены, образованные по отношению к полю P_d, имеют целые рациональные коэффициенты, а потому, согласно теореме Гаусса (см. § 11, п. 2), целые рациональные коэффициенты имеют также соответствующий нормированный неприводимый многочлен, являющийся главным многочленом, образованным по отношению к полю K (ср. также общий факт § 15, п. 5А). Поэтому, для того чтобы доказать, что ε является единицей поля K, достаточно показать, что ε и ε^{-1} лежат в $\mathfrak{l}_d$.

Вынося в нашем произведении для ε множители Z^{-x} и замечая, что $\sum\limits^{+}_{\pm x \bmod d} \left(\frac{d}{x}\right) = 0$, мы получаем для ε выражение

$$\varepsilon = \mathsf{Z}^{S} \prod^{+}_{\pm x \bmod d} (1-\zeta^{x})^{-\left(\frac{d}{x}\right)},$$

где показатель

$$S = \sum^{+}_{\pm x \bmod d} \left(\frac{d}{x}\right) x$$

образуется аналогично сумме, фигурирующей в IVa, только суммирование теперь производится по наименьшей положительной полусистеме вычетов по mod d, взаимно простых с модулем. Согласно уже доказанному, Z^S принадлежит полю P_d. В этом можно легко убедиться и непосредственно. Для нечетного d будет $\mathsf{P}_{2d} = \mathsf{P}_d$, $\mathsf{Z} = -\zeta^{\frac{d+1}{2}}$. Для четного d $S \equiv 0 \bmod 2$, потому что в этом случае имеет место даже $d \equiv 0 \bmod 4$, и потому отдельные классы вычетов $\left(\frac{d}{x}\right) x \equiv x \bmod 2$ инвариантны относительно преобразования $x \to \frac{1}{2} d - x$.

Множитель $\mathsf{Z}^S = (-\zeta^{(d+1)/2})^S$, соответственно $\zeta^{S/2}$, очевидно, принадлежит к $\mathfrak{l}_d$, так же как и его обратная величина.

Множители $(1-\zeta^x)^{-\left(\frac{d}{x}\right)}$ можно соответственно $\varphi(d)/4$ «вычетам» a и $\varphi(d)/4$ «невычетам» b произвольно сгруппировать в пары $(1-\zeta^b)/(1-\zeta^a)$. Если определить тогда натуральное число $g \equiv (b/a) \bmod d$, то мы получим

$$\frac{1-\zeta^b}{1-\zeta^a} = \frac{1-\zeta^{ga}}{1-\zeta^a} = 1 + \zeta^a + \ldots + \zeta^{(g-1)a}, \tag{6}$$

откуда следует, что отношение $(1-\zeta^b)/(1-\zeta^a)$ принадлежит к $\mathfrak{l}_d$. В силу тех же соображений к $\mathfrak{l}_d$ принадлежит и обратное отношение $(1-\zeta^a)/(1-\zeta^b)$.

Следовательно, ε действительно есть единица.

После того как мы доказали высказывание IVб и тем самым чисто арифметически установили целочисленность и рациональность выражения для h из формулы для числа классов также и в вещественном случае, мы в качестве аналога высказыванию Vа докажем здесь следующее высказывание

Vб. *Для вещественных квадратичных полей* $\mathsf{K}=\mathsf{P}(\sqrt{d})$, *дискриминанты которых содержат только одно простое число* p, *т. е. для полей*

$$\mathsf{K}=\mathsf{P}(\sqrt{2}),\ \mathsf{P}(\sqrt{p}) \quad (p\equiv 1 \bmod 4)$$

норма основной единицы $N(\varepsilon_1)=-1$ *и число классов нечетно.*

Доказательство. Оба утверждения одновременно получатся из формулы

$$\varepsilon_1^h=\varepsilon$$

для числа классов, если мы покажем, что в указанных случаях для нормы круговой единицы имеет место

$$N(\varepsilon)=-1.$$

Это легко получается в форме

$$\varepsilon'=-\varepsilon^{-1}$$

из доказательства утверждения IVб. Именно, мы из ε получим ε', если применим какой-нибудь автоморфизм $\mathsf{Z}\to\mathsf{Z}^b$ с нечетным b, для которого $\left(\frac{d}{b}\right)=-1$; действительно, эти автоморфизмы образуют как раз единственный смежный класс по подгруппе автоморфизмов $\mathsf{Z}\to\mathsf{Z}^a$ с нечетными a, для которых $\left(\frac{d}{a}\right)=1$ (согласно теории Галуа, эта подгрупп соответствует подполю K поля P_{2d}). Поэтому, если в первой части доказательства утверждения IVб заменить нечетный «вычет» a нечетным «невычетом» b, то выражения в полученных там в процессе редукции сравнениях будут теперь $\left(\frac{d}{x}\right)=-\left(\frac{d}{bx}\right)=-\left(\frac{d}{x'}\right)$, и потому

$$\varepsilon^{(b)}=\left\{\begin{array}{ll}(-1)^{\alpha}\varepsilon^{-1} & \text{для } 2\nmid d\\ (-1)^{\alpha+\beta}\varepsilon^{-1} & \text{для } 2\mid d\end{array}\right\},$$

а в остальном изменения будут, очевидно, заключаться в следующем. В обеих формулах (4), которые соответствуют как раз рассматриваемым здесь случаям, теперь будет

$$\left(\frac{p}{b}\right)=\left(\frac{b}{p}\right)=-1,\ \text{соответственно}\ \left(\frac{2}{b}\right)=-1,$$
$$\text{и потому}\ b\equiv\pm 5 \bmod 8,$$

откуда

$$b^{\frac{1}{2}\varphi(d)} = b^{\frac{p-1}{2}} \equiv -1 \bmod p, \text{ следовательно, и по } \bmod 2d,$$

соответственно

$$b^{\frac{1}{2}\varphi(d)} = b^2 \equiv 1+8 \bmod 16, \text{ следовательно, и по } \bmod 2d.$$

Тогда отсюда следует здесь $\alpha \equiv 1 \bmod 2$, соответственно $\alpha \equiv 0$, $\beta \equiv 1 \bmod 2$, и это действительно дает $\varepsilon' = \varepsilon^{(b)} = -\varepsilon^{-1}$.

Так как в обеих формулах (5), соответствующих составным положительным дискриминантам d, при этом ничего не изменяется, мы получаем, кроме того, что для них норма круговой единицы

$$N(\varepsilon) = 1.$$

Из этого факта и из более детального рассмотрения арифметического характера круговой единицы ε можно также и здесь вывести принадлежащий теории родов факт, что для любого положительного дискриминанта d, содержащего точно r различных простых чисел, число классов делится на 2^{r-2}, соответственно 2^{r-1}, в зависимости от того, равна ли норма $N(\varepsilon_1)$ основной единицы $N(\varepsilon_1) = 1$ или -1; в связи с этим вопросом мы снова отсылаем читателя к моей монографии [1].

В заключение мы несколько подробнее остановимся на конкретном вычислении h при заданном d, которое для $d > 0$ сложнее, чем для $d < 0$. При этом целесообразно взять за основу использованное во второй части доказательства утверждения IVб представление для ε, где ε выражается не через Z, а через ζ; формула для числа классов примет тогда вид, аналогичный (3а):

$$\varepsilon_1^h = \varepsilon = \begin{cases} \left(-\zeta^{\frac{d+1}{2}}\right)^S \prod\limits_{\pm x \bmod d}^{+} (1-\zeta^x)^{-\left(\frac{d}{x}\right)} & \text{для } 2 \nmid d \\ \zeta^{\frac{1}{2}S} \prod\limits_{\pm x \bmod d}^{+} (1-\zeta^x)^{-\left(\frac{d}{x}\right)} & \text{для } 2 \mid d \end{cases} \tag{3б}$$

$$S = \sum_{\pm x \bmod d}^{+} \left(\frac{d}{x}\right) x.$$

Тогда дело сводится к тому, чтобы вычислить выражение справа, которое ведь является единицей $\varepsilon > 1$ поля $\mathsf{K} = \mathsf{P}(\sqrt{d})$, в нормальной форме

$$\varepsilon = \frac{u + v\sqrt{d}}{2},$$

т. е. чтобы определить натуральные числа u, v. Согласно X, п. 5, § 15, $\sqrt{d}$ вкладывается в поле $\mathsf{P}_d = \mathsf{P}(\zeta)$ посредством пред-

ставления

$$\sqrt{d}=\tau(\chi)=\sum_{x \bmod d}\chi(x)\zeta^x \quad \text{с} \quad \chi(x)=\left(\frac{d}{x}\right)$$

в виде гауссовой суммы. Поэтому в каждом конкретном случае мы в действительности можем решить эту задачу: нужно произвести фактическое перемножение в произведении (3б), при этом знаменатель уничтожится (это следует, например, из приведенной выше формулы (6)); получающийся при этом многочлен от ζ с целыми рациональными коэффициентами должен, в силу неприводимости уравнения деления круга, которому удовлетворяет ζ (см. § 11, п. 2), иметь вид $\frac{u+v\tau(\chi)}{2}$ с натуральными u, v.

Коэффициенты u, v круговой единицы ε представляют собой, между прочим, оценку сверху для коэффициентов u_1, v_1 основной единицы ε_1, что, как мы уже отмечали в начале § 16, п. 5, весьма полезно для нахождения основной единицы посредством проб.

Если u, v уже найдены, то остается только определить показатель h из уравнения

$$\varepsilon_1^h=\left(\frac{u_1+v_1\sqrt{d}}{2}\right)^h=\frac{u+v\sqrt{d}}{2}=\varepsilon.$$

Лучше всего делать это следующим образом. Если положить вообще

$$\varepsilon_1^n=\frac{u_n+v_n\sqrt{d}}{2},$$

то последовательности u_n, v_n на основании равенства

$$\varepsilon_1^2=u_1\varepsilon_1\mp 1 \quad \text{(в зависимости от } N(\varepsilon_1)=\pm 1)$$

определяются из u_1, v_1 и $u_0=2$, $v_0=0$ по рекуррентным формулам

$$u_{n+2}=u_1u_{n+1}\mp u_n,$$
$$v_{n+2}=u_1v_{n+1}\mp v_n.$$

Тогда нужно только посмотреть, для какого $n=h$ найденная пара коэффициентов u, v совпадает с u_n, v_n.

Пример. $\underline{K=P(\sqrt{2}),\ d=8;\ \zeta^4=-1.}$

$$2\sqrt{2}=\tau(\chi)=\zeta-\zeta^3-\zeta^5+\zeta^7=2(\zeta+\zeta^{-1}).$$
$$S=1-3=-2.$$
$$\varepsilon_1^h=(1+\sqrt{2})^h=\varepsilon=\zeta^{-1}\frac{1-\zeta^3}{1-\zeta}=\zeta^{-1}(1+\zeta+\zeta^2)=$$
$$=1+(\zeta+\zeta^{-1})=1+\sqrt{2}.$$
$$\underline{h=1}$$

Основанный на формуле (6) способ перемножения в произведении (3б) может применяться только в конкретных численных случаях. Для простого дискриминанта $d = p\ (\equiv 1 \bmod 4)$ мне удалось получить метод, который может служить для решения этой задачи в общем виде; Бергстрем [1] обобщил этот метод на составные дискриминанты. Ниже мы разберем этот метод для случая простого дискриминанта; относительно случая составного дискриминанта мы ограничимся ссылкой на работу Бергстрема [1].

5. Рациональное представление формулы для числа классов в случае положительного простого дискриминанта. Рассмотрим положительный дискриминант $d = p \equiv 1 \bmod 4$, равный простому числу; пусть $p = 1 + 4n$.

Мы будем исходить из формулы для числа классов в виде (2б) п. 4. Запишем эту формулу так же подробно, как и в (1б) п. 4 (ср. также сделанное там замечание относительно a, b), именно,

$$\varepsilon_1^h = \prod_{\pm x \bmod p}^{+} (\mathsf{Z}^x - \mathsf{Z}^{-x})^{-\left(\frac{x}{p}\right)} = \frac{\prod^{+}_{\pm b} (\mathsf{Z}^b - \mathsf{Z}^{-b})}{\prod^{+}_{\pm a} (\mathsf{Z}^a - \mathsf{Z}^{-a})},$$

где a, b пробегают $(p-1)/4 = n$ квадратичных вычетов, соответственно невычетов (здесь в обычном смысле!) по $\bmod p$ из наименьшей положительной полусистемы $1, \ldots, (p-1)/2$. Для обеих этих n-членных четверть-систем мы также введем более специальные обозначения

$$\mathfrak{a} = (a_1, \ldots, a_n), \quad \mathfrak{b} = (b_1, \ldots, b_n).$$

В (6) п. 4 мы после произвольного распределения на пары сомножителей в числителе и знаменателе сначала подсчитывали отношения отдельных пар, а затем эти отношения перемножали; теперь мы будем, наоборот, сначала подсчитывать произведения в числителе и знаменателе, а затем находить их отношение.

Переход от первообразного $2p$-го корня Z из 1 к первообразному p-му корню ζ из 1 в соответствии с

$$\mathsf{Z} = -\zeta^{\frac{p+1}{2}} = -\zeta_2$$

дает

$$\varepsilon_1^h = \left(\frac{2}{p}\right) \prod_{\pm x \bmod p}^{+} (\zeta_2^x - \zeta_2^{-x})^{-\left(\frac{x}{p}\right)} = (-1)^n \frac{\prod_{\nu=1}^{n} (\zeta_2^{b_\nu} - \zeta_2^{-b_\nu})}{\prod_{\nu=1}^{n} (\zeta_2^{a_\nu} - \zeta_2^{-a_\nu})}. \qquad (1)$$

При этом было использовано то, что для рассматривавшейся уже в IVa, п. 4 суммы $S = \sum_{\pm x \bmod d}^{+} \left(\frac{x}{p}\right) x$ имеет место

$$S = \sum_{\pm x \bmod p}^{+} \left(\frac{x}{p}\right) x \equiv \sum_{\pm x \bmod p}^{+} x = \frac{p^2-1}{8} \equiv \frac{p-1}{4} = n \bmod 2,$$

так что при этом преобразовании действительно появляется множитель $(-1)^S = (-1)^n = \left(\frac{2}{p}\right)$.

Произведя умножение в знаменателе и числителе, мы получаем две формулы вида

$$\left.\begin{aligned} \prod_{\nu=1}^{n} (\zeta_2^{a_\nu} - \zeta_2^{-a_\nu}) &= \sum_{r \bmod p} A_r \zeta_2^r \\ \prod_{\nu=1}^{n} (\zeta_2^{b_\nu} - \zeta_2^{-b_\nu}) &= \sum_{r \bmod p} B_r \zeta_2^r \end{aligned}\right\} \tag{2}$$

с коэффициентами A_r, B_r, которые, очевидно, выражаются следующим образом. Представим системы $\mathfrak{a}$, $\mathfrak{b}$ в виде одностолбцовых матриц и заставим

$$\mathfrak{e} = (e_1, \ldots, e_n)$$

пробегать всевозможные однострочные матрицы, все элементы которых $e_r = \pm 1$. Положим при этом

$$|\mathfrak{e}| = e_1 \ldots e_n;$$

позднее мы будем аналогично считать

$$|\mathfrak{a}| = a_1 \ldots a_n, \quad |\mathfrak{b}| = b_1 \ldots b_n.$$

Тогда имеет место

$$A_r = \sum_{\mathfrak{e}\mathfrak{a} \equiv r \bmod p} |\mathfrak{e}|, \quad B_r = \sum_{\mathfrak{e}\mathfrak{b} \equiv r \bmod p} |\mathfrak{e}|, \tag{3}$$

где условия суммирования, записанные подробно, означают сравнения

$$\mathfrak{e}\mathfrak{a} = e_1 a_1 + \ldots + e_n a_n \equiv r \bmod p,$$

соответственно

$$\mathfrak{e}\mathfrak{b} = e_1 b_1 + \ldots + e_n b_n \equiv r \bmod p.$$

Теперь мы должны исследовать определенные таким образом суммы A_r, B_r. Они зависят только от класса вычетов $r \bmod p$.

При умножении четвертьсистем $\mathfrak{a}$, $\mathfrak{b}$ на некоторый квадратичный вычет $a \bmod p$ получаются сравнения вида

$$aa_\nu \equiv (-1)^{\alpha_\nu} a_{\nu'}, \quad ab_\nu \equiv (-1)^{\alpha^*_\nu} b_{\nu'} \bmod p \tag{4}$$

с некоторыми перестановками ν', ν'' индексов ν и показателями α_ν, $\alpha_\nu^* \bmod 2$. Перемножение этих сравнений дает

$$a^n \equiv (-1)^\alpha \bmod p \quad \text{с} \quad \alpha \equiv \sum_{\nu=1}^{n} \alpha_\nu \equiv \sum_{\nu=1}^{n} \alpha_\nu^* \bmod 2. \tag{5}$$

Вследствие того что $\left(\frac{a}{p}\right) = 1$, имеет место $a^{2n} \equiv 1 \bmod p$, и потому во всяком случае $a^n \equiv \pm 1 \bmod p$. Аналогично критерию Эйлера для квадратичных вычетов здесь имеет место тот или другой случай, в зависимости от того, является ли a биквадратичным вычетом или невычетом по $\bmod p$; в этом легко убедиться посредством представления a через первообразный корень $w \bmod p$ (см. также даваемое ниже, в (28), обобщение критерия Эйлера на биквадратичные вычеты). Если, таким образом, χ есть один из двух, комплексно сопряженных биквадратичных характеров по $\bmod p$, введенных еще в § 10, п. 6, то

$$a^n \equiv \chi(a) \bmod p, \tag{6}$$

и потому

$$(-1)^\alpha = \chi(a). \tag{7}$$

Выбор этого характера χ среди пары комплексно сопряженных для нас здесь безразличен.

Если теперь в формуле (3) для сумм A_r произвести замену

$$e'_{\nu'} = (-1)^{\alpha_\nu} e_\nu \quad \text{с} \quad |e'| = (-1)^\alpha |e|$$

переменных суммирования, то в силу условий (4) мы получим следующее правило преобразования:

$$A_{a^{-1}r} = \sum_{ea \equiv a^{-1}r \bmod p} |e| = \sum_{e \cdot aa \equiv r \bmod p} |e| =$$

$$= (-1)^\alpha \sum_{e'a \equiv r \bmod p} |e'| = (-1)^\alpha A_r;$$

согласно (7), его можно записать также в виде

$$A_{a^{-1}r} = \chi(a) A_r.$$

Точно также получается

$$B_{a^{-1}r} = \chi(a) B_r.$$

Эти правила имеют место для каждого квадратичного вычета $a \bmod p$. Так как существует квадратичный вычет $a \bmod p$ с $\chi(a) = -1$ (например, $a \equiv w^2 \bmod p$), из этих правил следует прежде всего

$$A_0 = 0, \quad B_0 = 0. \tag{8_0}$$

Далее, полагая $a = r$ и принимая во внимание, что $\chi(a)^{-1} = \chi(a)$, мы получаем из этих правил сведение

$$A_a = \chi(a) A_1, \quad B_a = \chi(a) B_1 \tag{8}$$

всех сумм A_a, B_a с $\left(\frac{a}{p}\right)=1$ к специальным суммам A_1, B_1. Специальные формулы (8_0) так же будут содержаться в (8), если считать $\chi(0)=0$.

Теперь мы рассмотрим умножение на квадратичный невычет, откуда мы получим также и сведение к A_1, B_1 сумм A_b, B_b с $\left(\frac{b}{p}\right)=-1$. Для этого представим квадратичный невычет $b \bmod p$ в форме

$$b \equiv aw \bmod p \tag{9}$$

с некоторым фиксированным первообразным корнем $w \bmod p$, который мы в дальнейшем еще определенным образом нормируем, и в соответствии с § 10, п. 6 будем различать комплексно сопряженные биквадратичные характеры χ, $\bar{\chi}$ с помощью их значений для $w \bmod p$:

$$\chi(w)=i, \quad \bar{\chi}(w)=-i. \tag{10}$$

Умножая обе четвертьсистемы $\mathfrak{a}$, $\mathfrak{b}$ сначала на w, мы аналогично (4) получаем сравнения вида

$$wa_\nu \equiv (-1)^{\omega_\nu} b_{\bar{\nu}}, \quad wb_\nu \equiv (-1)^{\omega^*_{\bar{\nu}}} a_{\bar{\nu}} \bmod p \tag{11}$$

с новыми перестановками $\bar{\nu}$, $\bar{\bar{\nu}}$ индексов ν и новыми показателями ω_ν, $\omega^*_{\bar{\nu}} \bmod 2$. Перемножая эти сравнения, мы получаем соотношения несколько иного вида, чем (5), именно,

$$w^n |\mathfrak{a}| \equiv (-1)^{\omega} |\mathfrak{b}|, \quad w^n |\mathfrak{b}| \equiv -(-1)^{\omega} |\mathfrak{a}| \bmod p \tag{12}$$

с

$$\omega \equiv \sum_{\nu=1}^{n} \omega_\nu \equiv 1 + \sum_{\nu=1}^{n} \omega^*_{\bar{\nu}} \bmod 2. \tag{13}$$

Последнее соотношение между суммами показателей получается при этом из сравнивания друг с другом обоих сравнений (12), если учесть, что $w^{2n} \equiv -1 \bmod p$. Теперь посредством надлежащего выбора первообразного корня $w \bmod p$ можно добиться того, что будет иметь место

$$\omega \equiv 0 \bmod 2, \tag{14}$$

так что $(-1)^{\omega}=1$. В самом деле, если $\omega \equiv 1 \bmod 2$, то, очевидно, достаточно произвести замену $w \to w^{-1}$. Мы будем считать, что w нормировано таким образом; тогда, согласно (10), комплексно сопряженные биквадратичные характеры χ, $\bar{\chi}$ будут различаться уже вполне определенным образом.

Умножая далее (11) на a, мы, согласно (9) и (4), получаем сравнения

$$ba_\nu \equiv (-1)^{\omega_\nu + \alpha^*_\nu} b_{\bar{\nu}'}, \quad bb_\nu \equiv (-1)^{\omega^*_\nu + \alpha_{\bar{\nu}}} a_{\bar{\nu}}, \bmod p.$$

Поэтому, если в формуле (3) для сумм A_r снова произвести замену

$$e'_{\bar{\nu}''} = (-1)^{\omega_\nu + \alpha^*_\nu} e_\nu \quad \text{с} \quad |e'| = (-1)^{\omega+\alpha} |e| = (-1)^\alpha |e|$$

переменных суммирования, то, как и в предыдущем случае, мы получим следующее правило преобразования:

$$A_{b^{-1}r} = \sum_{ea \equiv b^{-1}r \bmod p} |e| = \sum_{eba \equiv r \bmod p} |e| = (-1)^\alpha \sum_{e'b \equiv r \bmod p} |e'| = (-1)^\alpha B_r,$$

которое, согласно (7) и (9), (10), может быть также записано в виде

$$A_{b^{-1}r} = \chi(a) B_r = \chi(b) \chi(w)^{-1} B_r = -\chi(b) i B_r.$$

Принимая во внимание (13), мы точно так же получаем

$$B_{b^{-1}r} = -\chi(a) A_r = -\chi(b) \chi(w)^{-1} A_r = \chi(b) i A_r.$$

Так как $\chi(b)^{-1} = -\chi(b)$, из этих формул при $b = r$ получается аналогичное (8) сведение

$$A_b = \chi(b) i B_1, \quad B_b = -\chi(b) i A_1 \tag{15}$$

к специальным суммам A_1, B_1 также и для сумм A_b, B_b с $\left(\frac{b}{p}\right) = -1$. Посредством введения целых чисел

$$\mathsf{A}_r = A_r + iB_r$$

из квадратичного поля $\mathsf{P}(i)$ можно объединить четыре формулы сведения (8), (15) в одну формулу

$$\mathsf{A}_r = \chi(r) \mathsf{A}_1,$$

верную для любого $r \bmod p$. Чтобы применять эту формулу к непосредственно интересующим нас суммам A_r, B_r, мы должны записывать их в виде

$$A_r = \frac{1}{2}(\mathsf{A}_r + \bar{\mathsf{A}}_r), \quad B_r = \frac{1}{2i}(\mathsf{A}_r - \bar{\mathsf{A}}_r).$$

Тогда для первого из произведений (2) получается дальнейшее преобразование

$$\prod_{\nu=1}^{n} (\zeta_2^{a_\nu} - \zeta_2^{-a_\nu}) = \frac{1}{2}\left[\sum_{r \bmod p} \mathsf{A}_r \zeta_2^r + \sum_{r \bmod p} \bar{\mathsf{A}}_r \zeta_2^r\right] =$$

$$= \frac{1}{2}\left[\left(\sum_{r \bmod p} \chi(r) \zeta_2^r\right) \mathsf{A}_1 + \left(\sum_{r \bmod p} \bar{\chi}(r) \zeta_2^r\right) \bar{\mathsf{A}}_1\right].$$

Здесь фигурируют принадлежащие биквадратичным характерам χ, $\bar{\chi}$ гауссовы суммы, образованные для p-го корня $\zeta_2 = \zeta^{\frac{p+1}{2}}$ из 1. При сведении к нормированному p-му корню $\zeta = e^{\frac{2\pi i}{p}}$ из 1 появляются, согласно (2*) п. 5, § 15, множители

$$\bar{\chi}\left(\frac{p+1}{2}\right) = \bar{\chi}\left(\frac{1}{2}\right) = \chi(2), \quad \chi\left(\frac{p+1}{2}\right) = \chi\left(\frac{1}{2}\right) = \bar{\chi}(2).$$

Поэтому мы получаем

$$\prod_{\nu=1}^{n} (\zeta_2^{a_\nu} - \zeta_2^{-a_\nu}) = \frac{\chi(2)\,\tau(\chi)\,\mathsf{A}_1 + \bar{\chi}(2)\,\tau(\bar{\chi})\,\bar{\mathsf{A}}_1}{2}, \tag{16а}$$

где $\tau(\chi)$, $\tau(\bar{\chi})$ обозначают нормированные гауссовы суммы, принадлежащие χ, $\bar{\chi}$. Для второго из произведений (2) совершенно так же следует

$$\prod_{\nu=1}^{n} (\zeta_2^{b_\nu} - \zeta_2^{-b_\nu}) = \frac{\chi(2)\,\tau(\chi)\,\mathsf{A}_1 - \bar{\chi}(2)\,\tau(\bar{\chi})\,\bar{\mathsf{A}}_1}{2i}. \tag{16б}$$

Теперь первая из наших задач, перемножение произведений в числителе и знаменателе формулы (1), решена уже настолько, что мы можем приступить ко второй задаче – образованию отношения. Эта задача упрощается благодаря тому, что произведение числителя и знаменателя из (1) можно определить элементарно.

Именно, мы имеем

$$\prod_{x=1}^{2n} (\zeta_2^{x} - \zeta_2^{-x}) = \left\{ \begin{array}{l} \zeta_2^{1+\ldots+2n} \prod_{x=1}^{2n} (1 - \zeta^{-x}) \\ \zeta_2^{-(1+\ldots+2n)} \prod_{x=1}^{2n} (1 - \zeta^{x}) \end{array} \right\},$$

и, таким образом,

$$\left[\prod_{x=1}^{2n} (\zeta_2^{x} - \zeta_2^{-x})\right]^2 = \prod_{x \not\equiv 0 \bmod p} (1 - \zeta^x) = \frac{x^p - 1}{x - 1}\Big|_{x=1} = p$$

Вследствие того что

$$\zeta_2^{x} - \zeta_2^{-x} = 2i \sin\frac{2\pi x}{p}\,\frac{p+1}{2} = 2i \sin\left(\frac{\pi x}{p} + \pi x\right),$$

эти $2n$ множителей попеременно то отрицательно-мнимы, то положительно-мнимы. Поэтому рассматриваемое произведение имеет значение

$$\prod_{x=1}^{2n} (\zeta_2^{x} - \zeta_2^{-x}) = (-1)^n i^{2n} \sqrt{p} = \sqrt{p} \tag{17}$$

с положительным квадратичным корнем. Этот факт, между прочим, мы будем использовать в § 20, п. 5 при определении знака нормированной квадратичной гауссовой суммы.

Поэтому мы получим отношение выражений (16) — причем в соответствии с (1) мы должны второе делить на первое — если второе выражение возведем в квадрат и разделим на $\sqrt{p}$. Согласно (1), нужно будет еще приписать множитель $(-1)^n$. Итак,

$$\varepsilon_1^h = \frac{(-1)^n}{\sqrt{p}} \left(\frac{\chi(2)\,\tau(\chi)\,\mathsf{A}_1 - \overline{\chi}(2)\,\tau(\overline{\chi})\,\overline{\mathsf{A}}_1}{2i} \right)^2.$$

Так как $\chi(2)^2 = \overline{\chi}(2)^2 = \left(\frac{2}{p}\right) = (-1)^n$, то, произведя возведение в квадрат, мы получаем

$$\varepsilon_1^h = \frac{1}{\sqrt{p}} \frac{-\frac{1}{2}\left(\tau(\chi)^2\,\mathsf{A}_1^2 + \tau(\overline{\chi})^2\,\overline{\mathsf{A}}_1^2\right) + (-1)^n\,\tau(\chi)\,\tau(\overline{\chi})\,\mathsf{A}_1\overline{\mathsf{A}}_1}{2}. \tag{18}$$

Так как, согласно (6), $\chi(-1) = (-1)^n$, мы имеем здесь в силу (1*), (2*) п. 5 § 15,

$$(-1)^n\,\tau(\chi)\,\tau(\overline{\chi}) = \chi(-1)\,\tau(\chi)\,\tau(\overline{\chi}) = \tau(\chi)\,\overline{\tau(\chi)} = p. \tag{19}$$

Остается вычислить только квадраты нормированных биквадратичных гауссовых сумм $\tau(\chi)$, $\tau(\overline{\chi})$. Это мы сделаем в (8) п. 4 § 20. Оказывается, что эти квадраты связаны с рассматривавшимися в § 10, п. 8 суммами для характеров (здесь мы заменили $-y$ на y)

$$\left.\begin{aligned} \pi(\chi, \psi) &= \sum_{x+y\equiv 1 \bmod p} \chi(x)\,\psi(y) \\ \pi(\overline{\chi}, \psi) &= \sum_{x+y\equiv 1 \bmod p} \overline{\chi}(x)\,\psi(y) \end{aligned}\right\} \tag{20}$$

из поля $\mathsf{P}(i)$ соотношениями

$$\frac{\tau(\chi)^2}{\tau(\psi)} = \psi(2)\,\pi(\chi, \psi), \quad \frac{\tau(\overline{\chi})^2}{\tau(\psi)} = \psi(2)\,\pi(\overline{\chi}, \psi). \tag{21}$$

При этом $\psi = \chi^2 = \overline{\chi}^2$ обозначает, как и там, квадратичный характер по $\bmod p$. Для него $\psi(2) = \left(\frac{2}{p}\right) = (-1)^n$ и, согласно (2) п. 3, для нормированной гауссовой суммы $\tau(\psi)$ имеет место $\tau(\psi) = \sqrt{p}$ с положительным квадратным корнем. Поэтому мы имеем

$$\tau(\chi)^2 = \left(\frac{2}{p}\right)\sqrt{p}\,\pi(\chi, \psi), \quad \tau(\overline{\chi})^2 = \left(\frac{2}{p}\right)\sqrt{p}\,\pi(\overline{\chi}, \psi). \tag{22}$$

Если результаты (19) и (22) подставить в (18), то мы получим далее

$$\varepsilon_1^h = \frac{-\left(\frac{2}{p}\right)\left(\frac{1}{2}\right)(\pi(\chi,\psi)\,\mathsf{A}_1^{2\prime}+\pi(\bar{\chi},\psi)\,\bar{\mathsf{A}}_1^2)+\mathsf{A}_1\bar{\mathsf{A}}_1\sqrt{p}}{p},$$

что с помощью следа и нормы в поле $\mathsf{P}(i)$ можно также записать в виде

$$\varepsilon_1^h = \frac{-\left(\frac{2}{p}\right)\frac{1}{2}S(\pi(\chi,\psi)\,\mathsf{A}_1^2)+N(\mathsf{A}_1)\sqrt{p}}{2}. \tag{23}$$

Для искомых коэффициентов u, v круговой единицы

$$\varepsilon = \frac{u+v\sqrt{p}}{2}$$

отсюда получаются выражения

$$u = -\left(\frac{2}{p}\right)\frac{1}{2}S(\pi(\chi,\psi)\,\mathsf{A}_1^2), \quad v = N(\mathsf{A}_1),$$

которые пока еще связаны с полем $\mathsf{P}(i)$.

Чтобы преобразовать нашу формулу (23) к чисто рациональному виду, мы обратимся к результатам из § 10, п. 8 относительно сумм $\pi(\chi,\psi)$, $\pi(\bar{\chi},\psi)$, которые мы в (20) записали в несколько ином виде, с y вместо $-y$, что удобнее для обобщения, которое и ничего не меняет, ибо $\psi(-1)=1$, и будет рассмотрено в § 20, п. 4. Если использовать еще определенный в § 10, п. 8 нормирующий множитель $-\left(\frac{2}{p}\right)$, то указанные результаты можно высказать так. Числа

$$\pi = -\left(\frac{2}{p}\right)\pi(\chi,\psi) = A+Bi, \quad \bar{\pi} = -\left(\frac{2}{p}\right)\pi(\bar{\chi},\psi) = A-Bi \tag{24}$$

приводят к однозначному разложению

$$p = \pi\bar{\pi} = A^2+B^2 \tag{25}$$

простого числа p на простые множители в поле $\mathsf{P}(i)$, причем с таким нормированием среди ассоциированных, что для оснований квадратов имеет место

$$A \equiv 1 \bmod 4, \quad B \equiv 0 \bmod 2. \tag{26}$$

Этим нормирующим условием разложение определяется однозначно с точностью до знака числа B, т. е. с точностью до различия между сопряженными простыми множителями π, $\bar{\pi}$ из $\mathsf{P}(i)$.

Хотя для нашего результата это и не очень важно, однако ради полноты мы рассмотрим здесь вопрос об этом нормировании и тем самым придадим совсем законченный вид содержа-

щемуся в V п. 8 § 10 результату. При этом нам будет достаточно только что изложенных сведений. Вопрос заключается в следующем. Согласно (10), нормирующее условие (14) для фигурирующего в (12) первообразного корня $w \bmod p$ определяет различие между двумя сопряженными биквадратичными характерами χ, $\bar{\chi}$. Этим, согласно (20), (24), определяется также различие между сопряженными простыми числами π, $\bar{\pi}$ из $\mathsf{P}(i)$. Какому дополнительному условию к уже известным нормирующим условиям (26) соответствует получаемое при этом установление знака числа B?

Для ответа на этот вопрос нам нужно обобщить критерий Эйлера на биквадратичные характеры χ, $\bar{\chi}$. Имеет место

$$0 \equiv w^{2n} + 1 \equiv (w^n - i)(w^n + i) \bmod p.$$

Поэтому $\pm w^n$ являются корнями по $\bmod p$ главного многочлена для базисного числа $\omega = \sqrt{-1} = i$ (см. § 17, п. 1). Нам нужно выяснить, как они сопоставляются сопряженным главным простым дивизорам $\mathfrak{p} \cong \pi$, $\bar{\mathfrak{p}} \cong \bar{\pi}$ в смысле § 17, п. 2. Для этого мы используем вытекающие из изложенной там теории сравнения

$$w^n \equiv i^{\pm 1} \bmod \pi, \quad w^n \equiv i^{\mp 1} \bmod \pi,$$

где показатели $\pm$, $\mp$ указывают на то, что знак при i пока не определен. Тогда, согласно (10), имеет место

$$\chi(w) \equiv w^{\pm n} \bmod \pi, \quad \chi(w) \equiv w^{\mp n} \bmod \bar{\pi},$$
$$\bar{\chi}(w) \equiv w^{\mp n} \bmod \pi, \quad \bar{\chi}(w) \equiv w^{\pm n} \bmod \bar{\pi},$$

и потому вообще

$$\left.\begin{array}{ll} \chi(x) \equiv x^{\pm n} \bmod \pi, & \chi(x) \equiv x^{\mp n} \bmod \bar{\pi} \\ \bar{\chi}(x) \equiv x^{\mp n} \bmod \pi, & \bar{\chi}(x) \equiv x^{\pm n} \bmod \bar{\pi} \end{array}\right\} \qquad (27)$$

для всех $x \not\equiv 0 \bmod p$, причем нужно брать или все время верхний, или все время нижний знак. Ограничение $x \not\equiv 0 \bmod p$ отпадает, если отрицательные показатели $-n$ заменить сравнимыми с ними по $\bmod p - 1$ положительными показателями $3n$, что мы и сделаем для дальнейшего. Если теперь подставить сравнения (27) и выполняющиеся согласно критерию Эйлера сравнения

$$\psi(y) \equiv y^{2n} \bmod p$$

в суммы (20), то мы получим

$$\pi(\chi, \psi) \equiv \sum_{x \bmod p} x^{(1+2g)n}(1-x)^{2n} \bmod \pi,$$
$$\pi(\bar{\chi}, \psi) \equiv \sum_{x \bmod p} x^{(1+2g)n}(1-x)^{2n} \bmod \bar{\pi}$$

с $g=0$ или 1 в зависимости от того, имеет ли место в (27) верхний или нижний знак. Но теперь отсюда следует, аналогично тому как в § 10, п. 4 при определении значения по $\bmod p$ рассматривавшихся там сумм для квадратичных характеров, что необходимо должно быть $g=0$; действительно, в противном случае, произведя разложение по правилу бинома и суммирование по x, мы получили бы противоречие

$$\pi(\chi, \psi) \equiv -1(-1)^n \binom{2n}{n} \not\equiv 0 \bmod \pi$$

(и точно так же для $\pi(\bar{\chi}, \psi)$). Поэтому в (27) должны стоять верхние знаки. Следовательно, соответствие между сопряженными биквадратичными характерами χ, $\bar{\chi}$ и сопряженными простыми числами π, $\bar{\pi}$ из $\mathsf{P}(i)$ получается таким, что при нем имеет место обобщение критерия Эйлера:

$$\chi(x) \equiv x^n \bmod \pi, \quad \bar{\chi}(x) \equiv x^n \bmod \bar{\pi}. \tag{28}$$

Для специального случая, когда $x \equiv a \bmod p$ есть квадратичный вычет, так что $\chi(a) = \bar{\chi}(a) = \pm 1$, мы установили это уже в (6), не обращаясь к представлению $p = \pi\bar{\pi}$. Обобщение по сравнению с критерием Эйлера для квадратичного характера по $\bmod p$ состоит как раз в привлечении этого разложения для p, которое необходимо потому, что для квадратичного невычета $x \equiv b \bmod p$ значения характеров $\chi(b) = \pm i$, $\bar{\chi}(b) = \mp i$ лежат уже не в P, а только в $\mathsf{P}(i)$. Поэтому, чтобы охарактеризовать эти характеры посредством сравнений, мы должны, согласно IVa п. 2 § 17, рассматривать классы вычетов по $\bmod p$ из P как классы вычетов по $\bmod \pi$, соответственно $\bmod \pi$ из $\mathsf{P}(i)$.

Из (28) следует, что нормирующие условия (10) и (12), (14) для χ и w могут быть также записаны в виде

$$\chi(w) = i \equiv \frac{|\mathfrak{b}|}{|\mathfrak{a}|} \bmod \pi,$$

т. е. в виде соотношения сравнимости в $\mathsf{P}(i)$. Тогда сопоставление их с выполняющимся, согласно определению (24), сравнением

$$i \equiv -\frac{A}{B} \bmod \pi$$

в $\mathsf{P}(i)$ доказывает существование сравнения

$$A|\mathfrak{a}| + B|\mathfrak{b}| \equiv 0 \bmod p \tag{29}$$

в P. Так как при $B \to -B$ это сравнение становится неверным, то оно и дает нам искомое нормирующее условие для знака числа B.

В силу формул (24), (25) с однозначно нормированными в соответствии с (26), (29) целыми рациональными числами A, B наша формула (23) легкими преобразованиями может быть приведена к чисто рациональному виду:

$$\varepsilon_1^h = \frac{(A(A_1^2 - B_1^2) - 2B \cdot A_1 B_1) + (A_1^2 + B_1^2)\sqrt{p}}{2}. \tag{30}$$

Таким образом, коэффициенты u, v круговой единицы

$$\varepsilon = \frac{u + v\sqrt{p}}{2}$$

рационально представляются в виде

$$u = A(A_1^2 - B_1^2) - 2B \cdot A_1 B_1, \quad v = A_1^2 + B_1^2.$$

При этом A_1, B_1 являются специальными суммами (3). Для этих выражений непосредственно очевидно выполнение условия целостности $u \equiv v \bmod 2$ (потому что A нечетно) и, кроме того, что $v > 0$. Однако тот факт, что также и $u > 0$, равносильный положительности h, получить из этих формул нельзя. Впрочем, в Vб, п. 4 доказано, что $N(\varepsilon) = -1$. Это дает нам еще одно нетривиальное соотношение между четырьмя числами A, B, A_1, B_1.

Содержащийся в окончательной формуле (30) результат мы сформулируем теперь вместе со всеми необходимыми для его понимания определениями:

VI. *Пусть для простого числа* $p \equiv 1 \bmod 4$

$$\mathfrak{a} = (a_1, \ldots, a_n), \quad \mathfrak{b} = (b_1, \ldots, b_n)$$

являются четверть-системами из $n = (p-1)/4$ *квадратичных вычетов* a_ν *и* $n = (p-1)/4$ *квадратичных невычетов* b_ν *из наименьшей положительной полусистемы* $1, \ldots, (p-1)/2$.

Пусть, далее,

$$A_1 = \sum_{\mathfrak{e}\mathfrak{a} \equiv 1 \bmod p} |\mathfrak{e}|, \quad B_1 = \sum_{\mathfrak{e}\mathfrak{b} \equiv 1 \bmod p} |\mathfrak{e}|$$

являются суммами, распространенными на произведения

$$|\mathfrak{e}| = e_1 \ \ldots \ e_n$$

всевозможных решений сравнений

$$\mathfrak{e}\mathfrak{a} = e_1 a_1 + \ldots + e_n a_n \equiv 1 \bmod p,$$

соответственно

$$\mathfrak{e}\mathfrak{a} = e_1 a_1 + \ldots + e_n a_n \equiv 1 \bmod p$$

в единицах $e_\nu = \pm 1$.

Наконец, пусть

$$p = A^2 + B^2$$

является таким однозначно определенным разложением числа p на сумму двух квадратов, при котором основания A, B квадратов удовлетворяют условиям

$$A \equiv 1 \bmod 4, \quad B \equiv 0 \bmod 2,$$

и

$$A\,|\mathfrak{a}| + B\,|\mathfrak{b}| \equiv 0 \bmod p,$$

где

$$|\mathfrak{a}| = a_1 \ \dots \ a_n, \quad |\mathfrak{b}| = b_1 \ \dots \ b_n.$$

Тогда число классов h вещественного квадратичного поля $k = \mathsf{P}(\sqrt{p})$ равно показателю той степени основной единицы

$$\varepsilon_1 = \frac{u_1 + v_1\sqrt{p}}{2},$$

которая равна круговой единице

$$\varepsilon = \frac{u + v\sqrt{p}}{2}$$

с коэффициентами

$$u = A(A_1^2 - B_1^2) - 2B \cdot A_1 B_1, \quad v = A_1^2 + B_1^2.$$

Как уже было сказано в п. 4, Бергстрем обобщил этот результат на любые вещественные квадратичные поля $\mathsf{K} = \mathsf{P}(\sqrt{d})$.

Заслуживает быть отмеченным тот факт, что коэффициент иррациональной части круговой единицы ε обладает разложением $v = A_1^2 + B_1^2$ на сумму двух квадратов, которое в VI оказывается связанным с разложением простого числа $p = A^2 + B^2$. Рассмотрение формулы (23) (см. стр. 450) делает эту связь еще более ясной с помощью соответствующих целых чисел $\mathsf{A}_1 = A_1 + iB_1$ и $\pi = A + iB$ из $\mathsf{P}(i)$.

Для практического вычисления h при заданном простом дискриминанте $p \equiv 1 \bmod 4$ можно обойтись без использования несколько более сложной формулы для u, так как при применении описанного в конце п. 4 рекуррентного метода достаточно оперировать только со вторыми коэффициентами v. Именно на основании этого нам, как уже говорилось выше, для результата VI не очень важно нормирование знака числа B.

Для конкретного вычисления h было бы, впрочем, предпочтительнее получить простой рекуррентный метод для прямого перемножения произведений в числителе и в знаменателе (1), потому что определение лежащих в основе сумм A_1, B_1 решений сравнений $\mathfrak{e}$ довольно сложно. Разработанный Бергстремом для этой последней цели рекуррентный метод по сути дела снова сводится к указанному перемножению.

Примеры. $p=5$. Четверть-системами являются

$$\mathfrak{a}=(1),\quad \mathfrak{b}=(2).$$

Разложение

$$5=1^2+2^2$$

при выборе знаков

$$A=1,\quad B=2$$

удовлетворяет нормирующим условиям. Первое из сравнений

$$\mathfrak{a}\varepsilon=e_1\equiv 1,\quad \mathfrak{b}\varepsilon=2e_1\equiv 1 \bmod 5$$

имеет в качестве решения с $e_1=\pm 1$ только

$$e_1\equiv 1 \bmod 5,$$

второе совсем не имеет таких решений. Поэтому

$$A_1=1,\quad B_1=0.$$

Отсюда

$$u=1\cdot 1-4\cdot 0=1,\qquad v=1,$$

и, таким образом,

$$\varepsilon_1^h=\varepsilon=\frac{1+\sqrt{5}}{2}=\varepsilon_1.$$

Следовательно, $h=1$.

$p=13$.

$$\mathfrak{a}=(1,3,4),\quad \mathfrak{b}=(2,5,6),$$

$$|\mathfrak{a}|\equiv -1,\qquad |\mathfrak{b}|\equiv -5 \bmod 13.$$

$$13=3^2+2^2,$$

$$A=-3,\quad B=-2.$$

$$\mathfrak{a}\varepsilon=e_1+3e_2+4e_3\equiv 1,\quad \mathfrak{b}\varepsilon=2e_1+5e_2+6e_3\equiv 1 \bmod 13.$$

$$\text{----------},\qquad 1\quad 1\quad -1,$$

$$A_1=0,\qquad B_1=-1.$$

$$u=-3\cdot -1+4\cdot 0=3,\qquad v=1,$$

$$\varepsilon_1^h=\varepsilon=\frac{3+\sqrt{13}}{2}=\varepsilon_1,\qquad h=1.$$

В качестве упражнения читателю предоставляется рассмотреть еще случай $p=17$, когда решения сравнений еще определяются легко.

§ 19. КВАДРАТИЧНЫЕ ПОЛЯ И КВАДРАТИЧНЫЙ ЗАКОН ВЗАИМНОСТИ

1. Квадратичные поля как поля классов. Закон разложения простых рациональных чисел p в квадратичном поле $\mathsf{K}=\mathsf{P}(\sqrt{d})$ определяется, согласно (4) п. 3 § 17, значением символа Кронекера $\left(\frac{d}{p}\right)$, причем простые числа p разлагаются на два множителя, остаются простыми или разветвляются в зависимости от того, какое из трех значений $1, -1, 0$ принимает символ $\left(\frac{d}{p}\right)$. Тип разложения p в K определяется, таким образом, классом вычетов, к которому принадлежит дискриминант $d \bmod p$ (соответственно по $\bmod 2^3$ при $p=2$).

Согласно закону взаимности для символа Кронекера в § 9, п. 6 для любого взаимного простого с d рационального числа имеет место

$$\left(\frac{d}{x}\right)=(\operatorname{sgn} x)^{\frac{\operatorname{sgn} d-1}{2}}\left(\frac{x^*}{d}\right),$$

где x^* получается из x заменой всех его нечетных простых делителей p на p^*, т. е. получается несколько более общим образом, чем в § 5, п. 7 (это различие существенно только при $2 \mid d$). Для простых рациональных чисел $p \nmid d$ отсюда следует:

$$\left(\frac{d}{p}\right)=\left(\frac{p^*}{d}\right),$$

где p^* для $p \neq 2$ определено так же, как в § 5, п. 7 и $p^*=2$ для $p=2$. Эта последняя формула верна и для $p \mid d$, так как тогда на основании дополнительных определений в (1) п. 1 § 10 и (3) п. 6 § 13 как символ Кронекера $\left(\frac{d}{p}\right)=0$, так и квадратичный характер с ведущим модулем d

$$\chi_d(x)=(\operatorname{sgn} x)^{\frac{\operatorname{sgn} d-1}{2}}\left(\frac{x^*}{d}\right),$$

совпадающий для $x>0$ с символом $\left(\frac{x^*}{d}\right)$, обладает свойством $\chi_d(p)=\left(\frac{p^*}{d}\right)=0$.

Благодаря этому истолкованию значений символа Кронекера $\left(\frac{d}{p}\right)$ для простых чисел p как значений квадратичного характера $\chi_d(p)$ с ведущим модулем d закон разложения в K приобретает новую форму. В этой форме тип разложения p в K определяется как раз наоборот, а именно классом вычетов $p \bmod d$. Эта новая форма уже с внешней стороны более удовлетвори-

тельна, так как в ней тип разложения характеризуется прямо через свойства исследуемых простых чисел по отношению к основному инварианту d поля K, в то время, как в первоначальной форме он характеризуется косвенно, через свойства d по отношению к исследуемому простому числу p.

Мы уже заранее подготовили эту новую форму закона разложения нашими рассуждениями в § 7, п. 4, 5, примыкавшими к доказательству квадратичного закона взаимности, и позже основным теоретико-групповым предложением в VI п. 6 § 9 и соответствующей теоремой единственности в V п. 5 § 9. Поэтому мы непосредственно перейдем к формулировке:

Закон разложения в квадратичных полях. *Пусть* $\mathsf{K}=\mathsf{P}(\sqrt{d})$ *— квадратичное поле с дискриминантом* d.

Пусть, далее,

$$\chi_d(x)=(\operatorname{sgn} x)^{\frac{\operatorname{sgn} x-1}{2}}\left(\frac{x^*}{d}\right)$$

однозначно определенный четный квадратичный характер с ведущим модулем d *и* $\mathfrak{H}$ *— подгруппа индекса* 2 *группы классов вычетов* $\bmod d$, *взаимно простых с* d, *определенная условием* $\chi_d(x)=1$.

Тогда простое рациональное число P *разлагается в* K, *если* $p\nmid d$ *и* p *лежит в* $\mathfrak{H}$; *остается простым в* K, *если* $p\nmid d$ *и* p *не лежит в* $\mathfrak{H}$; *разветвляется в* K, *если* $p\mid d$.

Имея в виду этот закон разложения, говорят, что поле K является полем классов к фактор-группе (группе классов) $\mathfrak{G}/\mathfrak{H}$ группы $\mathfrak{G}$ всех классов вычетов $\bmod d$, взаимно простых с d, по подгруппе $\mathfrak{H}$, так как тип разложения в K всех простых чисел p за исключением конечного числа делителей ведущего модуля d зависит только от того, какому из двух классов $\mathfrak{H}$ или $\mathfrak{G}-\mathfrak{H}$ принадлежит p.

Найденный нами закон разложения называют законом разложения теории полей классов в противоположность полученному в (4) п. 3 § 17 из куммеровой теории так называемому куммерову закону разложения.

Разложение на классы $\mathfrak{H}$ и $\mathfrak{G}-\mathfrak{H}$ уже играло ведущую роль в формулах для числа классов h поля K в § 18, п. 4, 5. То, что мы называли там «вычетами» и «невычетами», есть не что иное, как числа a из $\mathfrak{H}$ и b из $\mathfrak{G}-\mathfrak{H}$.

2. Взгляд на общую теорию полей классов. Понятие поля классов, выясненное нами на примере квадратичного поля, играет основную роль в теории большого класса полей алгебраических чисел.

Прежде всего, из нашего обзора в § 15, п. 5 видно, что рассмотренные там поля K степени k, а именно, подполя поля P_m

корня m-й степени из 1, являются в аналогичном смысле полями классов к соответствующим им по схеме § 15, п. 1 (фиг. 5 и 6) подгруппам индекса k группы $\mathfrak{G}$ классов вычетов $\bmod m$, взаимно простых с m. Именно, если перечисленные там основные арифметические теоремы для этих полей вывести исходя из обобщения изложенной в § 16, 17 куммеровой теории, то получится закон разложения для не делящих m простых рациональных чисел p в виде

$$p \cong \mathfrak{p}_1 \dots \mathfrak{p}_g \text{ с } \mathfrak{N}(\mathfrak{p}_i) = p^{f_p},\ f_p g_p = k,$$

где f_p есть наименьший натуральный показатель, для которого p^{f_p} лежит в $\mathfrak{H}$, т. е. порядок p в фактор-группе $\mathfrak{G}/\mathfrak{H}$ (см. I п. 1 § 15). Тип разложения p в K зависит, следовательно, и здесь только от класса, к которому принадлежит простое число p (или точнее класс вычетов $p \bmod m$) в фактор-группе $\mathfrak{G}/\mathfrak{H}$.

Если исходить из заданного поля K, то наименьшая степень m корня из 1, для которой K содержится в P_m и, следовательно, наименьший модуль m, по которому классы $\mathfrak{G}/\mathfrak{H}$ будут состоять из целых классов вычетов, совпадает, как это видно из результатов § 15, п. 1, с общим наименьшим кратным

$$m = \mathsf{M}_\chi f(\chi)$$

ведущих модулей $f(\chi)$ всех характеров χ из $\mathfrak{K}$. При этом, как уже неоднократно отмечалось, $\mathfrak{K}$ естественным образом изоморфна группе характеров группы Галуа $\mathfrak{G}/\mathfrak{H}$ поля K, если эту последнюю группу в соответствии с вложением K в P_m изоморфно отобразить на фактор-группу группы классов вычетов $\bmod m$, взаимно простых с m. Таким образом определенный модуль m называют ведущим модулем $\mathfrak{H}$ или также ведущим модулем разбиения на классы $\mathfrak{G}/\mathfrak{H}$.

Для любых простых чисел p закон разложения имеет вид

$$p = (\mathfrak{p}_1 \dots \mathfrak{p}_{g_p})^{e_p} \text{ с } \mathfrak{N}(\mathfrak{p}_i) = p^{f_p},\ e_p f_p g_p = k,$$

где e_p, f_p определены следующим образом. Пусть $\mathfrak{H}_p/\mathfrak{H}$ — наименьшая подгруппа $\mathfrak{G}/\mathfrak{H}$, такая, что ведущий модуль m_p группы $\mathfrak{H}_p$ не делится на p, и $\mathfrak{G}_p$ — группа классов вычетов $\bmod m_p$, взаимно простых с m_p; тогда

e_p — порядок $\mathfrak{H}_p/\mathfrak{H}$,

f_p — порядок $p \bmod m_p$ в $\mathfrak{G}_p/\mathfrak{H}_p$.

Выведенной формуле для ведущего модуля параллельна приведенная в § 18, п. 3 формула

$$|d| = \prod_\chi f(\chi)$$

для величины дискриминанта d поля K, которая ввиду закона разложения делает очевидной для этого случая теорему о дискриминанте из § 15, п. 5.

Все эти факты (за исключением последнего, для вывода которого нужны еще дополнительные теоретико-групповые рассмотрения) получаются, как уже говорилось, почти непосредственно из результатов § 15, п. 1, 5, если обобщить построенную в § 16, 17 для квадратичных полей куммерову теорию на подполя K поля корней m-й степени из 1 (для проведения чего, впрочем, требуются различные дополнения технического характера). Эти факты составляют содержание основных теорем так называемой *теории полей классов*. Кронекер завершил эту теорию, доказав, что такие поля K, которые все, конечно, абелевы, т. е. нормальны и имеют коммутативную группу Галуа, исчерпывают собой всю совокупность абелевых полей.

Теорема Кронекера. *Всякое абелево поле* K *есть подполе некоторого поля* P_m *корня* m*-й степени из* 1.

Мы доказали эту теорему для квадратичных полей $\mathsf{K} = \mathsf{P}(\sqrt{d})$ в X п. 5 § 15, указав способ вложения K в $\mathsf{P}_{|d|}$ при помощи принадлежащей к характеру $\chi_{|d|}(x) = \left(\frac{x^*}{d}\right)$ гауссовой суммы $\tau(\chi_{|d|})$. Мы вернемся к этому в п. 3.

Применимость теории полей классов не ограничена, однако, рассматривавшимися нами до сих пор *абсолютно абелевыми полями*, т. е. полями абелевыми над полем рациональных чисел P. Аналогичные факты имеют место и для относительно абелевых полей, т. е. абелевых расширений K произвольного поля алгебраических чисел $\varkappa$.

Каждому такому полю K относительной степени k над $\varkappa$ соответствует однозначное определенное разделение на k классов, причем теперь уже на классы разделяется группа $\mathfrak{D}_\mathfrak{m}$ всех дивизоров $\mathfrak{a}$ поля $\varkappa$, взаимно простых с некоторым целым дивизором $\mathfrak{m}$. При этом роль единичного класса $a \equiv 1 \bmod m$ играет единичный класс $\mathfrak{a} \sim 1 \bmod \mathfrak{m}$, состоящий из таких дивизоров $\mathfrak{a}$, что

$$\mathfrak{a} \cong \alpha \text{ с } \alpha \equiv 1 \bmod \mathfrak{m} \text{ в } \varkappa$$

при надлежащем выборе α среди ассоциированных с ним.

Роль группы классов $\bmod m$, взаимно простых с m, играет соответственно фактор-группа $\mathfrak{G}$ группы дивизоров $\mathfrak{D}_m$ по единичному классу как подгруппе. В этой группе $\mathfrak{G}$ классов вычетов дивизоров $\bmod \mathfrak{m}$ обычные классы дивизоров $\varkappa$ и классы вычетов чисел $\bmod \mathfrak{m}$, так сказать, смешиваются друг с другом; ввиду конечности числа классов дивизоров в $\varkappa$, с одной стороны, и классов вычетов чисел $\bmod \mathfrak{m}$ — с другой, конечно и число классов вычетов дивизоров $\bmod \mathfrak{m}$, т. е. $\mathfrak{G}$ является конечной

группой. Соответствующее полю K разделение дивизоров $\varkappa$ на k классов определяется тогда некоторой фактор-группой $\mathfrak{G}/\mathfrak{H}$ группы $\mathfrak{G}$ по подгруппе $\mathfrak{H}$, причем эта подгруппа, так же как и наименьший модуль $\mathfrak{m}$, при помощи которого ее можно определить, называемый ее ведущим модулем, определяется однозначно полем K.

При этом соответствии группа Галуа поля $\mathsf{K}/\varkappa$ оказывается изоморфной группе классов $\mathfrak{G}/\mathfrak{H}$. Доказывается, что тип разложения в K — теперь простых дивизоров $\mathfrak{p}$ из $\varkappa$ вместо простых чисел p — для $\mathfrak{p}$, не делящих $\mathfrak{m}$, характеризуется в полной аналогии с предшествующим порядком класса вычетов дивизоров $\mathfrak{p} \bmod \mathfrak{m}$ в группе классов $\mathfrak{G}/\mathfrak{H}$, причем имеет место и аналогичное обобщение для $\mathfrak{p}/\mathfrak{m}$. Этот закон разложения может быть так же, как в § 15, п. 5, формально выражен в виде аналитического тождества

$$\zeta_{\mathsf{K}}(s) = \prod_{\chi} L_{\varkappa}(s \mid \chi),$$

где

$$\zeta_{\mathsf{K}}(s) = \prod_{\mathfrak{P}} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{P})^s}} \qquad (\mathfrak{P} - \text{простые дивизоры } \mathsf{K})$$

есть $\zeta =$ функция Дедекинда поля K и

$$L_{\varkappa}(s \mid \chi) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s}} \qquad (\mathfrak{p} - \text{простые дивизоры } \varkappa)$$

соответствующие характерам χ группы $\mathfrak{G}/\mathfrak{H}$ L-ряды поля $\varkappa$. Для ведущего модуля $\mathfrak{m}$ и теперь уже относительного дискриминанта $\mathfrak{d}$ поля $\mathsf{K}/\varkappa$ имеют место аналогичные выведенным выше выражения их через ведущие модули $\mathfrak{f}(\chi)$ этих характеров. Наконец, для любой группы классов вычетов дивизоров $\mathfrak{G}/\mathfrak{H}$ в $\varkappa$ существует однозначно определенное относительно абелево поле классов K, для которого имеют место все эти теоремы.

Мы должны здесь ограничиться этим кратким обзором основных теорем общей теории полей классов. Читатель, желающий подробнее ознакомиться с этой теорией, может сделать это по моему подробному обзору [2].

Большая открытая проблема современных алгебраически-теоретико-числовых исследований заключается в обобщении этого описания относительно абелевых полей K и их законов разложения при помощи групп классов вычетов дивизоров в основном поле $\varkappa$ на любые нормальные расширения $\mathsf{K}/\varkappa$. Решение этой проблемы должно вскрыть множество новых теоретико-числовых закономерностей.

3. Доказательство закона взаимности путем вложения в поле корней из единицы. Как мы видели в п. 1, квадратичный закон взаимности

$$\left(\frac{d}{p}\right)=\left(\frac{p^*}{d}\right)$$

для символа Кронекера дает возможность вывести закон разложения теории полей классов для квадратичного поля $\mathsf{K}=\mathsf{P}(\sqrt{d})$ непосредственно из куммерова закона разложения, имеющего место в силу самого определения простых дивизоров. Естественно попытаться использовать эту связь в обратном направлении — *для вывода квадратичного закона взаимности.*

Правда, приведенное в § 7, п. 2, 3 элементарное доказательство очень просто, однако оно не вскрывает глубоких причин удивительной связи между свойствами классов вычетов $d \bmod p$ и $p \bmod d$, которая составляет содержание закона взаимности. Поэтому оправданы поиски новых доказательств, которые могли бы вскрыть эти глубокие причины, даже если вообще довольствоваться одним доказательством для каждого математического факта.

Ответ на наш вопрос сводится к тому, чтобы получить каким-либо прямым путем закон разложения теории полей классов в поле $\mathsf{K}=\mathsf{P}(\sqrt{d})$ или некоторое его ослабление, достаточное для наших целей. Сравнение обоих законов разложения и даст нам тогда ту более глубокую причину, в силу которой закон взаимности имеет место. Этот ход мысли будет особенно ясным, если предположить, что мы уже получили каким-то прямым путем закон разложения теории полей классов в его полном объеме. Действительно, из сравнения обоих законов разложения тогда непосредственно следует формула $\left(\frac{d}{p}\right)=\left(\frac{p^*}{d}\right)$ для числа d, являющегося дискриминантом квадратичного поля и любого не делящего d простого числа p. В свою очередь эта формула превращается в закон взаимности с обоими дополнениями к нему в первоначальной формулировке из § 7, п. 2, 3, если рассмотреть дискриминанты $d=(-1)^{(q-1)/2}\cdot q=q^*$ при простых нечетных q, а также дискриминанты $d=-4,\ 8$.

Естественным путем для прямого вывода закона разложения теории полей классов является вложение поля $\mathsf{K}=\mathsf{P}(\sqrt{d})$ в поле корней из единицы $\mathsf{P}_{|d|}$, которое было уже упомянуто в п. 2, как частный случай теоремы Кронекера. Действительно, раз закон разложения в $\mathsf{P}_{|d|}$ для не делящих d простых чисел p имеет согласно п. 2 (см. уже I п. 1 § 15) простую форму

$$p\cong\mathfrak{p}_1\dots\mathfrak{p}_{g_p}\ \text{с}\ \mathfrak{N}(\mathfrak{p}_i)=p^{f_p},\ f_pg_p=\varphi(|d|),$$

где f_p — порядок класса вычетов $p \bmod |d|$, то естественно предположить, что из него и для подполя K будет следовать закон разложения, который также будет зависеть только от класса вычетов $p \bmod |d|$, а это и есть закон разложения теории полей классов для $\mathsf{K} = \mathsf{P}(\sqrt{d})$.

Этот ход мыслей легко довести до конца, если иметь в распоряжении основные положения арифметики в поле корней из единицы $\mathsf{P}_{|d|}$. Для этого нужны только следующие два замечания:

А) *Если p уже в K разлагается на два множителя, то число g_p различных простых делителей p в $\mathsf{P}_{|d|}$ должно быть четным.*

Б) *Если p является в K простым дивизором порядка 2, то порядки f_p простых делителей p в $\mathsf{P}_{|d|}$ должны быть четными.*

Если применить эти замечания к специальному полю $\mathsf{K} = \mathsf{P}(\sqrt{q^*})$ с простым нечетным дискриминантом $d = q^*$ (и, следовательно, $\mathsf{P}_{|d|} = \mathsf{P}_q$), то получится:

а) Если $\left(\frac{q^*}{p}\right) = 1$, то $q_p = (q-1)/f_p$ четно, следовательно $(q-1)/2$ делится на порядок f_p числа $p \bmod q$, а значит $p^{(q-1)/2} \equiv 1 \bmod q$, т. е. $\left(\frac{p}{q}\right) = 1$.

б) Если $\left(\frac{q^*}{p}\right) = -1$, то порядок f_p числа $p \bmod q$ четен, а следовательно, для $q \equiv -1 \bmod 4$ $p^{(q-1)/2} \equiv -1 \bmod q$, т. е. $\left(\frac{p}{q}\right) = -1$.

Для того чтобы снять сделанное в «б» ограничение $q \equiv -1 \bmod 4$, надо применить замечания А) и В) к специальным полям $\mathsf{K} = \mathsf{P}(\sqrt{-1})$ и $\mathsf{P}(\sqrt{2})$ с дискриминантами $d = -4, 8$.

Поле $\mathsf{K} = \mathsf{P}(\sqrt{-1})$ совпадает с содержащим его полем корней из единицы P_4. Сравнение обоих законов разложения дает здесь непосредственно, что $\left(\frac{-1}{p}\right) = 1$ эквивалентно тому, что $p \equiv 1 \bmod 4$, а $\left(\frac{-1}{p}\right) = -1$ — тому, что $p \equiv -1 \bmod 4$, т. е. первое дополнение к закону взаимности.

Поле корней из единицы P_8, содержащее $\mathsf{K} = \mathsf{P}(\sqrt{2})$, содержит, кроме него, еще $\mathsf{K}' = \mathsf{P}(\sqrt{-1})$ и является их композитом

$$\mathsf{P}_8 = \mathsf{K}\mathsf{K}' = \mathsf{P}(\sqrt{-1}, \sqrt{2}).$$

Отсюда следует дополнение к А), Б), легко вытекающее из основных арифметических положений:

В) *Если p как в K, так и в K' разлагается на два различных простых дивизора порядка 1, то в P_8 p разлагается на $g_p = 4$ различных простых дивизора порядка 1.*

Для $p \neq 2$ можно теперь следующим образом устранить сделанное в «б» ограничение $q \equiv -1 \bmod 4$. Если $q \equiv 1 \bmod 4$, то, применив «а» и поменяв при этом ролями p и q, получим, что из $\left(\frac{q^*}{p}\right) = -1$, т. е. $\left(\frac{q}{p}\right) = -1$, следует $\left(\frac{p^*}{q}\right) = -1$, т. е. согласно уже доказанному первому дополнению, $\left(\frac{p}{q}\right) = 1$.

Для $p = 2$ ввиду ограничения $q \equiv -1 \bmod 4$, сделанного в «б», нам остается еще доказать, что для $q \equiv 1 \bmod 4$ из $\left(\frac{q^*}{2}\right) = -1$, т. е. $q \equiv 5 \bmod 4$, следует $\left(\frac{2}{q}\right) = -1$ или, следовательно, что для $q \equiv 1 \bmod 4$ из $\left(\frac{2}{q}\right) = 1$ следует $q \equiv 1 \bmod 8$, т. е. $\left(\frac{q}{2}\right) = 1$. Это же следует из приведенного замечания В) снова с заменой p на q. Действительно, предположение $q \equiv 1 \bmod 4$ и $\left(\frac{2}{q}\right) = 1$ означает как раз, что q как в $\mathsf{K}' = \mathsf{P}(\sqrt{-1}) = \mathsf{P}_4$, так и в $\mathsf{K} = \mathsf{P}(\sqrt{2})$ разлагается на два множителя. При разложении q в $\mathsf{P}_8 = \mathsf{K}\mathsf{K}'$ имеем тогда $f_q = 1$, а это означает, что класс вычетов $q \bmod 8$ имеет порядок 1, т. е. $q \equiv 1 \bmod 8$.

Таким образом, как закон взаимности, так и оба дополнения к нему получены нами, как непосредственное следствие сравнения закона разложения в использованных полях $\mathsf{K} = \mathsf{P}(\sqrt{d})$ с законом разложения содержащих их полей корней из единицы $\mathsf{P}_{|d|}$. Эти рассуждения, свободные от каких-либо выкладок, делают ясной ту глубокую причину, в силу которой имеет место закон взаимности. Об этом упоминалось в конце § 9, п. 5 и в § 9, п. 6.

Для этого доказательства необходимо, как уже указывалось, иметь в своем распоряжении основные предложения арифметики поля корней из единицы $\mathsf{P}_{|d|}$, не вошедшие в эту книгу, в частности, знать закон разложения в $\mathsf{P}_{|d|}$. В § 8, п. 3, 5 мы познакомились уже с доказательствами, которые также основаны на вложении полей $\mathsf{K} = \mathsf{P}(\sqrt{p^*})$, $\mathsf{P}(\sqrt{2})$ в поля корней из единицы P_p, P_8, однако обходятся вместо закона разложения элементарной теорией делимости в этих полях. Мы рекомендуем читателю еще раз просмотреть эти доказательства с новой точки зрения.

4. Чисто квадратичное доказательство квадратичного закона взаимности. Мы приведем в заключение еще одно, ставшее теперь уже классическим, доказательство квадратичного закона взаимности. Оно также основывается на той связи, которая существует между символом Кронекера $\left(\frac{d}{p}\right)$ и законом разложения в $\mathsf{K} = \mathsf{P}(\sqrt{d})$ с той разницей, что вывод этого

закона разложения из закона разложения в объемлющем поле $\mathsf{P}_{|d|}$ заменяется выводом некоторого ослабления этого закона при помощи арифметических рассмотрений в самом поле $\mathsf{K}=\mathsf{P}(\sqrt{d})$.

Это доказательство использует следующие два утверждения, выведенные нами в Va, б п. 4 § 18 из формулы для числа классов.

I. *Число классов h квадратичных полей $\mathsf{K}=\mathsf{P}(\sqrt{d})$, дискриминант которых делится только на одно простое число p, т. е. полей*

$$\mathsf{K}=\mathsf{P}(\sqrt{-1}),\ \mathsf{P}(\sqrt{\pm 2}),\ \mathsf{P}(\sqrt{p^*}),$$

нечетно. Если $d>0$, то норма основной единицы этих полей $N(\varepsilon_1)=-1$.

Так как доказательство формулы для числа классов было получено нами аналитическим путем и, кроме того, использовало доказываемый сейчас квадратичный закон взаимности (в виде утверждения о том, что $\left(\frac{d}{x}\right)$ есть характер с ведущим модулем d), то мы должны привести новое доказательство I, основывающееся на арифметике изучаемых полей.

Доказательство. Мы воспользуемся рассмотренным в IX п. 3 § 17 выделением из каждого дивизора $\mathfrak{a}$ его первообразной части $\mathfrak{a}_0$ и приведенным там выражением для $\mathfrak{a}_0$. Если $\mathfrak{a}$ инвариантно относительно образующего автоморфизма поля K, т. е. $\mathfrak{a}'=\mathfrak{a}$, то $\mathfrak{a}_0'=\mathfrak{a}_0$ и $\mathfrak{a}_0$ состоит только из простых дивизоров $\mathfrak{p}$, делящих простые числа p, разветвляющиеся в K.

При наших специальных предположениях относительно K тогда обязательно

$$\mathfrak{a}_0=1 \text{ или } \mathfrak{p},$$

где $\mathfrak{p}$ — простой делитель единственного разветвляющегося в K простого числа p. Но этот простой дивизор $\mathfrak{p}$ является обязательно главным дивизором в K, а именно

$$\mathfrak{p}\cong\pi \text{ с } \pi=1+\sqrt{-1},\ \sqrt{\pm 2},\ \sqrt{p^*}.$$

Отсюда следует, что $\mathfrak{a}_0\sim 1$, а, следовательно, и $\mathfrak{a}\sim 1$, если $\mathfrak{a}'=\mathfrak{a}$.

Заметим далее, что число $\gamma\neq 0$ из K, обладающее свойством $N(\gamma)=\gamma\gamma'=1$, предоставимо в виде

$$\gamma=\frac{\alpha}{\alpha'}$$

как отношение числа $\alpha\neq 0$ из K к его сопряженному, а именно, как легко видеть, можно положить

$$\alpha=\begin{cases}1+\gamma \text{ при } \gamma\neq -1\\ \sqrt{d} \text{ при } \gamma=-1.\end{cases}$$

Теперь мы докажем по очереди оба высказывания относительно $N(\varepsilon_1)$ и h.

1) Пусть $d > 0$. Предположим, что $N(\varepsilon_1) = 1$. Тогда при помощи второго из сделанных только что замечаний получаем

$$\varepsilon_1 = \frac{\alpha}{\alpha'} \qquad (\text{с } \alpha = 1 + \varepsilon_1).$$

Таким образом, число $\alpha \neq 0$ из K обладает свойством

$$\alpha = \varepsilon_1 \alpha', \quad \text{т. е.} \quad \alpha \cong \alpha'.$$

Для первообразной части α_0 этого числа имеет тогда место

$$\alpha_0 = \varepsilon_1 \alpha_0', \quad \text{т. е.} \quad \alpha_0 \cong \alpha_0'.$$

Согласно первому из сделанных в начале доказательства замечаний,

$$\alpha_0 \cong 1 \text{ или } \pi, \quad \text{т. е. } \alpha_0 = \varepsilon \text{ или } \varepsilon\pi$$

с некоторой единицей ε из K. Ввиду $\pi' = -\pi$ отсюда следует, что

$$\varepsilon_1 = \frac{\alpha_0}{\alpha_0'} = \pm \frac{\varepsilon}{\varepsilon'} = \pm \varepsilon^2,$$

в противоречии с тем, что ε_1 есть основная единица K. Таким образом, должно быть $N(\varepsilon_1) = -1$.

2) Для того чтобы доказать, что группа классов дивизоров имеет нечетный порядок h, достаточно доказать, что для каждого класса дивизоров C поля K из $C^2 = 1$ следует, что $C = 1$, или, что то же самое, что для каждого дивизора $\mathfrak{a}$ поля K из $\mathfrak{a}^2 \sim 1$ следует, что $\mathfrak{a} \sim 1$.

Пусть, таким образом, $\mathfrak{a}$ — такой дивизор поля K, что $\mathfrak{a}^2 \sim 1$. Как мы уже заметили в § 17, п. 5, это свойство может быть записано и в виде $\mathfrak{a} \sim \mathfrak{a}'$. Таким образом,

$$\frac{\mathfrak{a}}{\mathfrak{a}'} \cong \gamma$$

есть главный дивизор и при этом $N(\gamma) \cong 1$, т. е. $N(\gamma) = \pm 1$. Если $d < 0$, то отсюда непосредственно следует, что $N(\gamma) = 1$, если же $d > 0$, то, ввиду того что $N(\varepsilon_1) = -1$, этого можно добиться выбором γ среди ассоциированных ($\gamma \to \gamma$ или $\varepsilon_1\gamma$). Ввиду второго из сделанных в начале доказательства замечаний

$$\gamma = \frac{\alpha}{\alpha'}, \quad \text{т. е.} \quad \frac{\mathfrak{a}}{\mathfrak{a}} = \frac{\mathfrak{a}'}{\mathfrak{a}'}.$$

Ввиду первого замечания теперь имеем $\frac{\mathfrak{a}}{\mathfrak{a}} \sim 1$, а следовательно, и $\mathfrak{a} \sim 1$.

Таким образом, оба высказывания из I доказаны чисто арифметически. Мы заметим, что то из них, которое касается $N(\varepsilon_1)$, является частичным обращением доказанного в IX п. 4 § 16 необходимого условия. Согласно этому условию, $N(\varepsilon_1) = -1$ может иметь место только для дискриминантов $d > 0$, состоящих из простых чисел $p \equiv 1 \bmod 4$ и 2, нами же доказано, что для простых d это условие также и достаточно. Вопрос остается открытым для дискриминантов $d > 0$ и делящихся на несколько простых чисел $p \equiv 1 \bmod 4$ и 2.

Прежде чем мы обратимся к доказательству квадратичного закона взаимности, мы докажем следующее предложение, примыкающее к первому замечанию в начале доказательства I:

II. *В вещественных квадратичных полях* $\mathsf{K} = \mathsf{P}(\sqrt{pq})$ *с двумя простыми числами* $p, q \equiv -1 \bmod 4$ *простые делители* $\mathfrak{p}$ *и* $\mathfrak{q}$ *разветвляющихся простых чисел являются главными дивизорами.*

Доказательство. Согласно только что сказанному, здесь $N(\varepsilon_1) = 1$. Как и при доказательстве I, отсюда следует существование такого примитивного α_0 из K, что

$$\alpha_0 = \varepsilon_1 \alpha_0', \quad \text{т. е. } \alpha_0 \cong \alpha_0'.$$

Первообразными дивизорами, инвариантными относительно образующего автоморфизма поля K, здесь могут быть только 1, $\mathfrak{p}$, $\mathfrak{q}$ и $\mathfrak{pq}$. Возможность $\alpha_0 \cong 1$ или $\mathfrak{pq}$ исключаются, как и в доказательстве I, ввиду того что $\mathfrak{pq} \cong \sqrt{pq}$. Таким образом, должно быть, например, $\alpha_0 \cong \mathfrak{p}$. Но тогда $\mathfrak{p} \sim 1$, а ввиду того что $\mathfrak{pq} \sim 1$, будет также и $\mathfrak{q} \sim 1$.

Доказательство закона взаимности.

а) Рассмотрим квадратичное поле $\mathsf{K} = \mathsf{P}(\sqrt{p^*})$ с единственным разветвляющимся простым числом p, причем при $p = 2$ положим, как и в п. 1, $p^* = 2$. Согласно I, число классов идеалов h этого поля нечетно, а если поле вещественно ($p \equiv 1 \bmod 4$ или $p = 2$), то норма основной единицы $N(\varepsilon_1) = -1$.

Пусть q — отличное от p простое число и $\left(\frac{p^*}{q}\right) = 1$. По кумеровскому закону разложения, q разлагается в K на два множителя

$$q = \mathfrak{q}\mathfrak{q}' \text{ с } \mathfrak{N}(\mathfrak{q}) = q.$$

Из определения h следует тогда

$$\mathfrak{q}^h \sim 1, \quad \text{т. е.} \quad \mathfrak{q}^h \cong \alpha, \quad q^h \cong N(\alpha),$$

при некотором первообразном числе α из K. В мнимом случае отсюда непосредственно следует

$$q^h = N(\alpha),$$

а в вещественном этого можно добиться надлежащим выбором a среди ассоциированных, ввиду того что $N(\varepsilon_1) = -1$.

Таким образом, мы получим

$$q^h = \frac{a^2 - p^* b^2}{4} \text{ (при } p \neq 2\text{), соответственно } q^h = a^2 - 2b^2 \text{ (при } p = 2\text{)}$$

с целыми рациональными a и b. Отсюда следует

$$q^h \equiv \frac{a^2}{2^2} \bmod p, \text{ соответственно } q^h \equiv \pm 1 \bmod 8$$

и в любом случае $\left(\frac{q^h}{p}\right) = 1$. Так как h нечетно, то и $\left(\frac{q}{p}\right) = 1$.

Таким образом, для любого простого числа p и отличного от него простого числа q (из которых одно может совпадать с 2) доказано:

$$\text{из } \left(\frac{p^*}{q}\right) = 1 \qquad \text{следует } \left(\frac{q}{p}\right) = 1.$$

Предположим для простоты известным первое дополнение к закону взаимности, которое легко следует из определения символа Лежандра или критерия Эйлера. Тогда из доказанного следует закон взаимности и второе дополнение к нему, за исключением случая, когда $p, q \equiv -1 \bmod 4$. Для этого надо только поменять ролями p и q.

б) Чтобы разобрать и этот последний случай, рассмотрим вещественное поле $\mathsf{K} = \mathsf{P}(\sqrt{pq})$ с $p, q \equiv -1 \bmod 4$. Согласно II, простые дивизоры $\mathfrak{p}$, $\mathfrak{q}$, делящие разветвляющиеся в K простые числа p, q, являются в нем главными дивизорами. То, что, например, $\mathfrak{p} \sim 1$, можно записать, как и раньше, в виде

$$\pm p = \frac{\bar{a}^2 - pq\, b^2}{4}$$

с целыми рациональными $\bar{a}$ и b и неопределенным знаком, так как теперь $N(\varepsilon_1) = 1$. При этом обязательно $\bar{a} \equiv 0 \bmod p$. Уравнение может быть записано и в симметричной форме

$$\pm 1 = \frac{pa^2 - qb^2}{4}$$

с целыми рациональными a и b.

Пусть теперь $\left(\frac{p}{q}\right) = 1$. Так как, согласно первому дополнению, $\left(\frac{-1}{q}\right) = -1$, то полученное равенство, будучи рассмотрено как сравнение $\bmod q$, показывает, что левая часть обязана быть $+1$, т. е.

$$1 = \frac{pa^2 - qb^2}{4},$$

а это равенство, будучи рассмотрено как сравнение $\bmod p$, дает $\left(\frac{-q}{p}\right)=1$. Так как по первому дополнению $\left(\frac{-1}{p}\right)=-1$, то $\left(\frac{q}{p}\right)=-1$.

Исходя из предположения $\left(\frac{p}{q}\right)=-1$, получим таким же путем с заменой $+1$ на -1 в том же равенстве, что $\left(\frac{q}{p}\right)=1$.

Таким образом, закон взаимности доказан и в неразобранном ранее случае $p,\ q\equiv -1 \bmod 4$.

в) Чтобы сохранить полную чистоту метода, мы докажем тем же способом и первое дополнение к закону взаимности.

Рассуждение из первой части доказательства, будучи применено к полю $\mathsf{K}=\mathsf{P}(\sqrt{-1})$, дает, что из $\left(\frac{-1}{q}\right)=1$ следует $q\equiv 1 \bmod 4$. Чтобы вывести, наоборот, из $q\equiv 1 \bmod 4$ $\left(\frac{-1}{q}\right)=1$, рассмотрим вещественное квадратичное поле $\mathsf{K}=\mathsf{P}(\sqrt{q})$. В нем $N(\varepsilon_1)=-1$. Это означает разрешимость в целых числах u_1, v_1 уравнения

$$-1=\frac{u_1^2-qv_1^2}{4}.$$

Будучи рассмотрено как сравнение $\bmod q$, это уравнение дает $\left(\frac{-1}{q}\right)=1$.

Приведенное доказательство квадратичного закона взаимности и обоих дополнений к нему показывает, что этот закон имеет внутренний смысл и в рамках теории квадратичных полей. Он теснейшим образом связан с законом разложения, а также с нормой основной единицы ε_1 и четностью числа классов h. Однако этот внутренний смысл здесь не так прозрачен, как в доказательстве из п. 3, основанном на вложении в поле корней из единицы.

§ 20. СИСТЕМАТИЧЕСКАЯ ТЕОРИЯ ГАУССОВЫХ СУММ

1. Общее определение, редукция к простейшим случаям. В ряде мест этой книги мы имели дело с гауссовыми суммами, сначала в § 8, где было дано использующее эти суммы доказательство квадратичного закона взаимности, затем в X п. 5 § 15 при рассмотрении вопроса о вложении квадратичного поля в поле корней из 1, далее в § 18, п. 2, 3 при суммировании L-рядов и выводе общей формулы для числа классов и, наконец, в § 18, п. 5 при приведении к рациональному виду формулы для числа классов квадратичного поля в случае положительного простого дискриминанта.

В заключение мы объединим в более систематическом виде отдельные результаты относительно гауссовых сумм, которые мы получили или только приняли без доказательства в связи с перечисленными выше вопросами и дадим все недостающие пока доказательства.

Понятие гауссовой суммы в том виде, как мы использовали его до сих пор, в последнее время подвергалось различным обобщениям, именно, с одной стороны, на произвольное поле алгебраических чисел K конечной степени вместо поля рациональных чисел P в качестве области суммирования и, с другой стороны, для специального случая простого модуля p, на любое конечное поле характеристики p вместо простого поля (поля классов вычетов) по $\bmod p$ в качестве области суммирования. В соответствии с характером этой книги мы удовлетворимся здесь первоначальным понятием гауссовой суммы, однако для него дадим систематическую, законченную теорию.

Пусть χ — характер с натуральным ведущим модулем f. Мы можем рассматривать χ также как характер по $\bmod m$ для каждого натурального кратного m числа f, если мы сохраним только значения $\chi(x)$ с x, взаимно простыми с m. Для дальнейшего целесообразно указывать на это обстоятельство посредством обозначения χ_m. Под χ без индекса всегда будет пониматься собственный характер.

Пусть, далее, $\zeta_m = e^{2\pi i/m}$ обозначает аналитически нормированный первообразный m-й корень из 1. Тогда для каждого натурального делителя d числа m с $m = dm_0$ имеет место $\zeta_m^d = \zeta_{m_0}$. Под ζ без индекса все время будет подразумеваться нормированный первообразный f-й корень $\zeta = \zeta_f = e^{2\pi i/f}$ из 1. Причину того, почему мы выбрали именно *аналитическое* нормирование, мы выясним лишь позднее, в п. 5—7. Пока нам важно только *фиксировать* какой-нибудь первообразный корень из 1 степени, равной соответствующему определяющему модулю, чтобы все остальные корни можно было выразить через него.

Под гауссовыми суммами, принадлежащими характеру χ, определенному по $\bmod m$, мы понимаем однозначно соответствующие m классам вычетов $a \bmod m$, а тем самым и m корням ζ_m^a из 1 суммы

$$\tau(\chi_m | \zeta_m^a) = \sum_{\substack{x \bmod m \\ (x,\, m)=1}} \chi(x)\, \zeta_m^{ax}, \tag{1}$$

где суммирование производится по (произвольно выбранной) системе вычетов $x \bmod m$, взаимно простых с модулем.

Относительно этого общего определения гауссовых сумм заметим следующее. Фигурирующий в качестве второго аргумента корень ζ_m^a из 1 можно при заданном характере χ сделать посред-

ством соответствующего выбора определяющего модуля m (среди кратных ведущего модуля f) и класса вычетов $a \bmod m$ любым корнем $\zeta^* = e^{2\pi i r}$ (r рационально, $0 \leqslant r < 1$) из 1, и притом даже бесконечным числом способов, в соответствии с различными дробными представлениями $r = a/m = a'/m' = \ldots$ с кратными числа f в качестве знаменателей. Однако соответствующие гауссовы суммы $\tau(\chi_m | \zeta^*)$, $\tau(\chi_{m'} | \zeta^*)$, ... (по крайней мере формально) различны между собой, так как суммирование производится каждый раз по различным системам вычетов по $\bmod m$, $\bmod m'$, ... Именно вследствие этого и нужно указать также и в левой части (1) на зависимость суммы от выбора определяющего модуля m, что достигается посредством индекса m при χ.

Посредством замены $cx \longrightarrow x \bmod m$ переменной суммирования с c, взаимно простым с m, мы получаем функциональное уравнение

$$\tau(\chi_m | \zeta_m^{ac}) = \overline{\chi}(c)\, \tau(\chi_m | \zeta_m^a) \quad \text{при } (c, m) = 1, \tag{2}$$

с которым мы уже познакомились в рассматривавшихся ранее специальных случаях (1) п. 2 § 8 и (2*) п. 5 § 15 и которое мы в этих случаях использовали.

Поэтому $\tau(\chi_m | \zeta_m^a)$ существенно зависит не от самого класса вычетов $a \bmod m$, а только от его делителя $d = (a, m)$, который характеризует собой совокупность $ac \bmod m$ с $(c, m) = 1$. Однако мы вместо этого делителя будем рассматривать в качестве инварианта, описывающего гауссовой суммы порядок m_0 корня ζ_m^a из 1. Зная $d = (a, m)$, можно определить m_0 по схеме

$$a = da_0, \quad m = dm_0, \quad (a_0, m_0) = 1,$$

т. е. m_0 — дополнительный к d делитель числа m. Для положенного в основу корня из 1 получается при этом редуцированное представление

$$\zeta_m^a = \zeta_{m_0}^{a_0}$$

в виде первообразного m_0-го корня из 1.

Теперь мы покажем

I. *Имеет место*

$$\tau(\chi_m | \zeta_m^a) = 0, \text{ если } f \nmid m_0,$$

т. е. если порядок m_0 корня ζ_m^a не является определяющим модулем характера χ.

Доказательство. Согласно (2), из $\tau(\chi_m | \zeta_m^a) \neq 0$ следовало бы, что $\chi(c) = 1$ имеет место для всех взаимно простых с m чисел c со свойством $ac \equiv a \bmod m$, которое может быть записано также в виде $a_0 c \equiv a_0 \bmod m_0$ и потому равносильно $c \equiv 1 \bmod m_0$. Но тогда m_0 было бы определяющим модулем для χ, что противоречит предположению.

Этот способ вывода (только в прямой, а не в обратной форме) нам уже знаком из суммирования L-рядов в § 18, п. 2; фигурировавшие там суммы $g(\zeta^a|\chi)$ выражаются в наших новых обозначениях $\tau(\chi_f|\zeta_f^a)=\tau(\chi|\zeta^a)$ с любым $a \bmod f$. Как отмечалось там в связи с (3), мы можем в качестве следствия из (2) и I установить, что редукция

$$\tau(\chi|\zeta^a)=\overline{\chi}(a)\,\tau(\chi|\zeta) \tag{3}$$

имеет место для любых (не обязательно взаимно простых с модулем) $a \bmod f$.

Так как на основании I случай $f \nmid m_0$ становится тривиальным, мы будем предполагать в дальнейшем, что $f \mid m_0$. Говоря подробнее, порядок m_0 корня $\zeta_m^a=\zeta_{m_0}^{a_0}$ должен быть кратным ведущего модуля f характера χ.

Такие гауссовы суммы $\tau(\chi_m|\zeta_m^a)$ мы будем называть *правильными*.

Для правильных гауссовых сумм мы укажем две редукции. Посредством *первой редукции* суммирование по системе вычетов по $\bmod m$, взаимно простых с модулем, сводится к суммированию по системе вычетов по $\bmod m_0$, взаимно простых с модулем. Мы приходим при этом к гауссовым суммам $\tau(\chi_{m_0}|\zeta_{m_0}^{a_0})$, которые мы будем называть *первообразными*, потому что для них корень $\zeta_{m_0}^{a_0}$ из 1 является первообразным корнем порядка, равного определяющему модулю m_0. Посредством *второй редукции* суммирование по классам вычетов по $\bmod m_0$, взаимно простым с модулем, сводится к суммированию по классам вычетов по $\bmod f$, взаимно простым с модулем. При этом мы приходим к гауссовым суммам $\tau(\chi_f|\zeta_f^{a_0})=\tau(\chi|\zeta^a)$, которые мы будем называть *собственными*, так как для них характер χ является собственным. Если привлечь еще правило редукции (3), то мы придем к гауссовой сумме $\tau(\chi|\zeta)=\tau(\chi)$, которая фигурировала все время в наших предшествующих рассмотрениях; ее мы, как и раньше, будем называть нормированной собственной гауссовой суммой для характера χ и обозначать просто через $\tau(\chi)$.

II. *Для правильных гауссовых сумм имеет место редукция*

$$\tau(\chi_m|\zeta_m^a)=\frac{\varphi(m)}{\varphi(m_0)}\,\tau(\chi_{m_0}|\zeta_{m_0}^{a_0})$$

к соответствующим первообразным гауссовым суммам.

Доказательство. Суммирование в

$$\tau(\chi_m|\zeta_m^a)=\sum_{\substack{x \bmod m\\(x,\,m)=1}}\chi(x)\,\zeta_m^{ax}$$

мы сведем от системы вычетов по $\bmod m$, взаимно простых с модулем, к системе вычетов по $\bmod m_0$, взаимно простых с модулем, посредством последовательного исключения простых делителей p числа d (где $m = dm_0$). Достаточно провести исключение одного такого простого делителя.

Пусть p — простой делитель числа $d = (a, m)$ и

$$a = pa', \qquad m = pm'.$$

Вследствие предположения $f \mid m_0$ заведомо имеет место $f \mid m'$, т. е. m' также является еще определяющим модулем для χ. Представим тогда системы классов вычетов $x \bmod m$, взаимно простых с модулем, в виде

$$x \equiv x' + ym' \bmod m \text{ с } (x', m') = 1 \quad \text{и} \quad ym' \not\equiv -x' \bmod p,$$

где x' пробегает систему вычетов по $\bmod m'$, взаимно простых с модулем, а y — систему вычетов по $\bmod p$, с указанным ограничением. Тогда

$$\tau(\chi_m \mid \zeta_m^a) = \sum_{\substack{x' \bmod m \\ (x', m') = 1}} \chi(x')\, \zeta_{m'}^{a'x'} \sum_{\substack{y \bmod p \\ ym' \not\equiv -x' \bmod p}} 1.$$

Если теперь также $p \mid m'$, то ограничение для y автоматически выполняется в силу ограничения для x', и потому внутренняя сумма равна p. Если же $p \nmid m'$, то в силу ограничения для x' выпадает точно один класс вычетов $y \bmod p$; тогда, следовательно, внутренняя сумма равна $p - 1$. Так как одновременно в этих случаях имеет место также $\varphi(m) = p\varphi(m')$, соответственно $\varphi(m) = (p-1)\varphi(m')$, внутренняя сумма в каждом случае равна $\varphi(m)/\varphi(m')$. Поэтому

$$\tau(\chi_m \mid \zeta_m^a) = \frac{\varphi(m)}{\varphi(m')}\, \tau(\chi_{m'} \mid \zeta_{m'}^{a'}).$$

Повторное применение этой элементарной редукции доказывает наше утверждение.

III. *Для первообразных гауссовых сумм имеет место дальнейшая редукция*

$$\tau(\chi_{m_0} \mid \zeta_{m_0}^{a_0}) = \mu\left(\frac{m_0}{f}\right) \chi\left(\frac{m_0}{f}\right) \tau(\chi \mid \zeta^{a_0})$$

к соответствующим собственным гауссовым суммам.

Здесь μ обозначает функцию Мёбиуса.

Доказательство. Мы будем рассуждать по той же схеме, что и в предыдущем доказательстве; однако здесь рассуждения несколько сложнее.

Пусть p — такой простой делитель числа $m_0 = pm_0'$, что еще имеет место $f \mid m_0'$. Тогда тем же приемом, что и в предыдуще

случае, мы получаем

$$\tau(\chi_{m_0} | \zeta_{m_0}^{a_0}) = \sum_{\substack{x' \bmod m_0' \\ (x', m_0')=1}} \chi(x') \zeta_{m_0}^{a_0 x'} \sum_{\substack{y \bmod p \\ y m_0' \not\equiv -x' \bmod p}} \zeta_p^{a_0 y}.$$

а) Если теперь также $p | m_0'$, то ограничение для y снова выполняется само собой. Так как вследствие $(a_0, m_0) = 1$ подавно имеет место $(a_0, p) = 1$, внутренняя сумма тогда равна 0. Таким образом, в этом случае

$$\tau(\chi_{m_0} | \zeta_{m_0}^{a_0}) = 0. \qquad \text{(а)}$$

б) Если же $p \nmid m_0'$, то, в силу указанного ограничения, для каждого x' исключается однозначно определенный класс вычетов $y_0 \bmod p$, именно тот, для которого $y_0 m_0' \equiv -x' \bmod p$; поэтому внутренняя сумма имеет здесь зависящее от x' значение $-\zeta_p^{a_0 y_0} = -\zeta_{m_0}^{a_0 y_0 m'}$. Объединяя его с корнем $\zeta_{m_0}^{a_0 x'}$ внешней суммы, мы получаем $-\zeta_{m_0}^{a_0 (x' + y_0 m_0')}$. Если во внешней сумме произвести преобразование

$$x' + y_0 m_0' \equiv x'' p \bmod m_0,$$

которое, согласно определению $y_0 \bmod p$, действительно ставит в соответствие каждому $x' \bmod m_0'$, взаимно простому с модулем (x' предполагается выбранным из фиксированной системы вычетов), однозначно определенный взаимно простой с модулем класс $x'' \bmod m_0'$, то в этом случае у нас получится

$$\tau(\chi_{m_0} | \zeta_{m_0}^{a_0}) = -\sum_{\substack{x' \bmod m_0' \\ (x', m_0')=1}} \chi(x') \zeta_{m_0}^{a_0 (x' + y_0 m_0')} =$$

$$= -\sum_{\substack{x'' \bmod m_0' \\ (x'', m_0')=1}} \chi(x'' p) \zeta_{m_0'}^{a_0 x''} = -\chi(p) \tau(\chi_{m_0'} | \zeta_{m_0'}^{a_0}). \qquad \text{(б)}$$

Если произвести теперь эту элементарную редукцию для каждого отдельного простого делителя p числа m_0/f, то, согласно (а), значение 0 будет получаться тогда, когда m_0/f содержит простое число p по меньшей мере с показателем 2, т. е. когда m_0/f не свободно от квадратов, а также и тогда, когда m_0/f хотя и свободно от квадратов, но содержит хотя бы один простой делитель p числа f, т. е. когда m_0/f не взаимно просто с f. В остальных случаях, согласно (б), для каждого из различных простых делителей p числа m_0/f получается добавочный множитель $-\chi(p)$. В соответствии с определением функции Мёбиуса $\mu(m_0/f)$ и тем, что $\chi(m_0/f) = 0$ для $(m_0/f, f) \neq 1$, мы можем

сказать, что в каждом случае появляется как раз добавочный множитель $\mu(m_0/f)\chi(m_0/f)$, что нам и нужно было доказать.

Результаты I, II, III и (3) вместе дают нам следующее:

IV. *Гауссова сумма*

$$\tau(\chi_m, \zeta_m^a) = \sum_{\substack{x \bmod m \\ (x,m)=1}} \chi(x)\zeta_m^{ax},$$

принадлежащая характеру χ *с ведущим модулем* f, *определенному по* $\bmod m$, *может быть отлична от нуля только тогда, когда она правильная, т. е. когда порядок* m_0 *корня* $\zeta_m^a = \zeta_{m_0}^{a_0}$ *из 1 делится на* f.

В этом случае имеет место редукция

$$\tau(\chi_m \mid \zeta_m^a) = \frac{\varphi(m)}{\varphi(m_0)}\mu\left(\frac{m_0}{f}\right)\chi\left(\frac{m_0}{f}\right)\bar{\chi}(a_0)\tau(\chi)$$

к принадлежащей χ *нормированной собственной гауссовой сумме*

$$\tau(\chi) = \sum_{x \bmod f} \chi(x)\zeta^x.$$

Так как $\tau(\chi) \neq 0$, что мы знаем уже из (1*) п. 5 § 15 и еще раз покажем простым способом в п. 2, то мы можем утверждать, что $\tau(\chi_m \mid \zeta_m^a)$ отлична от нуля тогда и только тогда, когда, кроме необходимого условия $f \mid m_0$, еще m_0/f свободно от квадратов и взаимно просто с f.

Изложенная здесь теория редукции для общих гауссовых сумм находит себе применение во многих теоретико-числовых исследованиях, как, например, в упомянутом в конце § 18, п. 4 обобщении чисто арифметического представления формулы для числа классов на составные дискриминанты, причем не только в рассмотренном Бергстремом специальном случае квадратичного поля, но также и в соответствующей задаче для любого абелева поля, которая до сих пор не решена полностью.

2. Разложение на компоненты, формула для абсолютной величины гауссовой суммы. Сначала еще раз рассмотрим определенную в (1) п. 1 общую гауссову сумму

$$\tau(\chi_m \mid \zeta_m^a) = \sum_{\substack{x \bmod m \\ (x,m)=1}} \chi(x)\zeta_m^{ax}. \tag{1}$$

Пусть

$$m = m_1 \ldots m_r$$

есть некоторое разложение определяющего модуля m в произведение попарно взаимно простых натуральных чисел $m_1, \ldots, m_r$. Произведем по схеме из § 4, п. 9 прямое разложение кольца

классов вычетов по mod m на кольца классов вычетов по mod $m_1, \ldots, m_r$ (см. IX п. 9 § 4), откуда получится также разложение для соответствующих групп классов вычетов, взаимно простых с модулем (см. IX п. 9 § 4), причем будем исходить как и там, из представления

$$\frac{1}{m} = \frac{g_1}{m_1} + \ldots + \frac{g_r}{m_r}$$

с целыми рациональными $g_1, \ldots, g_r$. Тогда

$$\zeta_m = \zeta_{m_1}^{g_1} \ldots \zeta_{m_r}^{g_r}$$

и, более обще,

$$\zeta_m^{ax} = \zeta_{m_1}^{g_1 a_1 x_1} \ldots \zeta_{m_r}^{g_r a_r x_r},$$

где a_i, $x_i \bmod m_i$ являются компонентами классов a, $x \bmod m$, определяемыми сравнениями

$$a \equiv a_i, \quad x \equiv x_i \bmod m_i \qquad (i = 1, \ldots, r).$$

Пусть, далее,

$$\chi_m = \chi_{m_1} \ldots \chi_{m_r}$$

есть разложение на компоненты характера χ_m, соответствующее в смысле XII п. 6 § 13 нашему разложению определяющего модуля m; при этом компоненты χ_{m_i} определяются в виде

$$\chi_{mi}(x) = \chi_m(x_i) \qquad (i = 1, \ldots, r),$$

если предварительно нормировать $x_i \bmod m_i$ посредством дополнительного условия

$$x_i \equiv 1 \bmod \frac{m}{m_i} \qquad (i = 1, \ldots, r).$$

Тогда

$$\chi_m(x) = \chi_{m_1}(x_1) \ldots \chi_{m_r}(x_r).$$

Если в соответствии с этим разложением на компоненты свести в (1) суммирование по системе вычетов $x \bmod m$, взаимно простых с модулем, к суммированиям по системам вычетов $x_i \bmod m_i$, взаимно простых с модулем, то мы получим соответствующее разложение на компоненты для гауссовой суммы сначала в форме

$$\tau(\chi_m | \zeta_m^a) = \tau(\chi_{m_1} | \zeta_{m_1}^{g_1 a_1}) \ldots \tau(\chi_{m_r} | \zeta_{m_r}^{g_r a_r}).$$

Так как $(g_i, m) = 1$ и, точнее, $g_i (m/m_i) \equiv 1 \bmod m_i$, для компонент при этом, согласно правилу редукции (2) п. 1, имеет еще место

$$\tau(\chi_{m_i} | \zeta_{m_i}^{g_i a_i}) = \overline{\chi}_{m_i}(g_i)\, \tau(\chi_{m_i} | \zeta_{m_i}^{a_i}) = \chi_{m_i}\left(\frac{m}{m_i}\right) \tau(\chi_{m_i} | \zeta_{m_i}^{a_i})$$
$$(i = 1, \ldots, r).$$

V. *При разложении* $m = \prod_{i=1}^{r} m_i$ *определяющего модуля* m *на попарно взаимно простые множители* m_i *для соответствующей классу вычетов* $a \bmod m$ *гауссовой суммы, принадлежащей характеру* χ, *имеет место разложение на компоненты*

$$\tau(\chi_m \mid \zeta_m^a) = \prod_{i=1}^{r} \chi_{m_i}\left(\frac{m}{m_i}\right) \cdot \prod_{i=1}^{r} \tau(\chi_{m_i} \mid \zeta_{m_i}^{a_i}),$$

где $\chi_m = \prod_{i=1}^{r} \chi_{mi}$ *есть соответствующее разложение характера* χ, *определенного по* $\bmod m$, *и* $a_i \equiv a \bmod m_i$ *являются компонентами класса вычетов* $a \bmod m$.

Если положить в основу разложение на простые множители $m = \prod_{i=1}^{r} p_i^{\mu_i}$, то с помощью результата V мы могли бы формально несколько упростить обе редукции II, III из п. 1. Однако мы отказались от этого, потому что упрощение касается и без того совершенно ясного объединения результатов, полученных для отдельных простых сомножителей, в то время как редукция в этих отдельных случаях существенно не упрощается.

В дальнейшем мы ограничимся рассмотрением собственных гауссовых сумм

$$\tau(\chi \mid \zeta^a) = \sum_{x \bmod f} \chi(x)\, \zeta^{ax} = \bar{\chi}(a)\, \tau(\chi), \tag{2}$$

где, таким образом, χ есть собственный характер с ведущим модулем f, $\zeta = e^{2\pi i/f}$ — нормированный первообразный f-й корень из 1 и $a \bmod f$ — взаимно простой с модулем класс вычетов (ζ^a есть любой первообразный f-й корень из 1). Так как $\chi(x) = 0$ для $(x, f) \neq 1$, мы можем при желании отбрасывать или снова вводить ограничение $(x, f) = 1$, что мы уже и делали в § 15, п. 5 при доказательстве формул (1*), (2*).

Результат V о разложении на компоненты можно, принимая во внимание XIII п. 6 § 13, высказать для собственных гауссовых сумм так:

VI. *При разложении* $f = \prod_{i=1}^{r} f_i$ *ведущего модуля* f *на попарно взаимно простые множители* f_i *для соответствующей взаимно простому с модулем классу вычетов* $a \bmod f$ *гауссовой суммы, принадлежащей характеру* χ, *имеет место разложение на компоненты:*

$$\tau(\chi \mid \zeta^a) = \prod_{i=1}^{r} \chi_i\left(\frac{f}{f_i}\right) \cdot \prod_{i=1}^{r} \tau(\chi_i \mid \zeta_i^{a_i}),$$

где $\chi = \prod_{i=1}^{r} \chi_i$ *—соответствующее разложение характера* χ *с ведущим модулем* f *на компоненты, являющиеся характерами* χ_i *с ведущими модулями* f_i; $\zeta_i = \zeta^{f/f_i}$ *являются нормированными первообразными* f_i*-ми корнями из* 1; *и* $a_i \equiv a \bmod f_i$ *являются компонентами класса вычетов* $a \bmod f$.

Поэтому, в частности, для нормированной собственной гауссовой суммы, принадлежащей характеру χ, *имеет место разложение*

$$\tau(\chi) = \prod_{i=1}^{r} \chi_i\left(\frac{f}{f_i}\right) \cdot \prod_{i=1}^{r} \tau(\chi_i).$$

Если положить в основу разложение на простые множители $f = \prod_{i=1}^{r} p_i^{\nu_i}$, то, согласно VI (и IV п. 1), рассмотрение общих гауссовых сумм сводится к рассмотрению нормированных собственных гауссовых сумм с ведущими модулями $f = p^{\nu}$, равными степеням простого числа. В § 13, п. 6 мы для таких ведущих модулей определили в явном виде все существующие характеры χ.

Для квадрата абсолютной величины нормированной собственной гауссовой суммы мы доказали в (1*) п. 5 § 15 формулу

$$\tau(\chi)\,\overline{\tau(\chi)} = f, \tag{3}$$

которая, согласно правилу редукции (3) п. 1, не зависит от нормирования и потому имеет силу для всех собственных гауссовых сумм $\tau(\chi \mid \zeta^a)$.

Доказательство формулы (3) было довольно сложным. На основании же результата VI вопрос можно свести к частному случаю ведущего модуля $f = p^{\nu}$, равного степени простого числа, а тогда доказательство получается почти так же просто, как для частного случая $f = p$ в (2) п. 2 § 8:

$$\overline{\tau(\chi)}\,\tau(\chi) = \sum_{\substack{x \bmod p^{\nu} \\ x \not\equiv 0 \bmod p}} \chi(x^{-1})\,\zeta^{-x} \sum_{y \bmod p^{\nu}} \chi(y)\,\zeta^{y} =$$

$$= \sum_{\substack{x \bmod p^{\nu} \\ x \not\equiv 0 \bmod p}} \sum_{y \bmod p^{\nu}} \chi(x^{-1}y)\,\zeta^{y-x} =$$

$$= \sum_{\substack{x \bmod p^{\nu} \\ x \not\equiv 0 \bmod p}} \sum_{t \bmod p^{\nu}} \chi(t)\,\zeta^{x(t-1)} =$$

$$= \sum_{t \bmod p^\nu} \chi(t) \sum_{\substack{x \bmod p^\nu \\ x \not\equiv 0 \bmod p}} \zeta^{x(t-1)} =$$

$$= \sum_{t \bmod p^\nu} \chi(t) \sum_{x \bmod p^\nu} \zeta^{x(t-1)} - \sum_{t \bmod p^\nu} \chi(t) \sum_{x' \bmod p^{\nu-1}} \zeta^{px'(t-1)} =$$

$$= p^\nu - p^{\nu-1} \sum_{\substack{t \bmod p^\nu \\ t \equiv 1 \bmod p^{\nu-1}}} \chi(t) = p^\nu;$$

последнее равенство следует из (1) п. 2 § 13, ибо χ также и для подгруппы $t \equiv 1 \bmod p^{\nu-1}$ является характером, отличным от главного характера ε, потому что p^ν есть ведущий модуль.

3. Внутренний смысл собственных гауссовых сумм. Если характер χ с ведущим модулем f имеет порядок k, т. е. все его отличные от нуля значения являются k-ми корнями из 1, то соответствующие собственные гауссовы суммы

$$\tau(\chi \mid \zeta^a) = \sum_{x \bmod f} \chi(x) \zeta^{ax} \qquad (a, f) = 1 \tag{1}$$

суть числа из композита $\mathsf{P}_k\mathsf{P}_f$ двух полей P_k и P_f, являющиеся корнями из 1.

Лемма. *Композитом и пересечением полей* P_k, P_f *являются:*

$$\mathsf{P}_k\mathsf{P}_f = \mathsf{P}_m, \quad \mathsf{P}_k \cap \mathsf{P}_f = \mathsf{P}_d,$$

где

$$[k, f] = m, \quad (k, f) = d$$

соответственно общее наименьшее кратное и общий наибольший делитель чисел k, f, *так что имеет место*

$$kf = md.$$

Доказательство. Для композита утверждение очевидно. Действительно, с одной стороны, $\zeta_k = \zeta_m^{m/k}$, $\zeta_f = \zeta_m^{m/f}$, и потому $\mathsf{P}_k\mathsf{P}_f \leqslant \mathsf{P}_m$, с другой стороны, $\zeta_m = \zeta_k^u \zeta_f^v$, где u, v определяются из $d = uf + vk$, т. е. из $1/m = u/k + v/f$, и потому $\mathsf{P}_m \leqslant \mathsf{P}_k\mathsf{P}_f$.

Для пересечения заранее ясно только то, что $\mathsf{P}_d \leqslant \mathsf{P}_k \cap \mathsf{P}_f$, потому что $\zeta_d = \zeta_k^{k/d} = \zeta_f^{f/d}$. Но тогда для доказательства утверждения $\mathsf{P}_d = \mathsf{P}_k \cap \mathsf{P}_f$ достаточно установить равенство для степеней

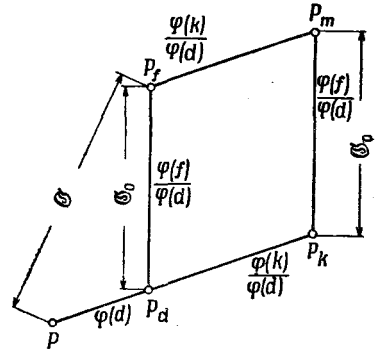
$$[\mathsf{P}_k : \mathsf{P}_d]\,[\mathsf{P}_f : \mathsf{P}_d] = [\mathsf{P}_m : \mathsf{P}_d]$$

(фиг. 24). Как было доказано в § 15, п. 5, P_n всегда имеет

степень $\varphi(n)$. Поэтому вопрос сводится к доказательству равенства

$$\frac{\varphi(k)}{\varphi(d)}\frac{\varphi(f)}{\varphi(d)}=\frac{\varphi(m)}{\varphi(d)}, \text{ или, другими словами, } \varphi(k)\varphi(f)=\varphi(d)\varphi(m).$$

Пусть p — любое простое число и пусть, для определенности, оно входит в f в степени, не меньшей чем в k. Тогда степень, в которой оно входит в d, равна степени, в которой оно входит в k, и степень, в которой оно входит в m, равна степени, в которой оно входит в f. Поэтому степени каждого простого числа, входящего в фигурирующие у нас значения функций Эйлера, связаны доказываемым соотношением. Тем самым лемма доказана.



Фиг. 24.

Как было показано в § 15, п. 5, группа Галуа $\mathfrak{G}$ расширения P_f/P состоит из подстановок $\zeta\to\zeta^a$ с $a \bmod f$, взаимно простыми с модулем, и изоморфна группе классов вычетов по $\bmod f$, взаимно простых с модулем. По основной теореме теории Галуа подполю P_d соответствует, на основании представления $\zeta_d=\zeta^{f/d}$ для его примитивного элемента, подгруппа $\mathfrak{G}_0$ подстановок $\zeta\to\zeta^{a_0}$ с $a_0 \bmod f$, взаимно простыми с модулем и обладающими свойством $a_0\equiv 1 \bmod d$. Тогда эта подгруппа $\mathfrak{G}_0$ является группой Галуа расширения $\mathsf{P}_f/\mathsf{P}_d$ и, по известной теореме из теории Галуа, также и расширения $\mathsf{P}_m/\mathsf{P}_k$.

Поэтому редукция из (3) п. 1 (в случае $a \bmod f$, взаимно простого с модулем), записанная нами еще в (2*) п. 5 § 15 в форме

$$\tau(\chi)\to\overline{\chi}(a)\tau(\chi) \quad \text{при} \quad \zeta\to\zeta^a, \tag{2}$$

служит также для специальных взаимно простых с модулем классов $a_0 \bmod f$ с $a_0\equiv 1 \bmod d$ указанием того, как ведет себя число $\tau(\chi)$ из $\mathsf{P}_m=\mathsf{P}_k\mathsf{P}_f$ при автоморфизмах группы Галуа $\mathfrak{G}_0$ расширения $\mathsf{P}_k\mathsf{P}_f/\mathsf{P}_k$. Для взаимно простых с модулем классов $a \bmod f$ с $a\not\equiv 1 \bmod d$ редукция формально тоже может быть представлена в виде (2). Однако тогда она уже не будет иметь только что указанного смысла; действительно, в этом случае при подстановке $\zeta\to\zeta^a$ будет изменяться значение характера χ, и потому в (2) будут фигурировать гауссовы суммы, принадлежащие различным характерам.

Для простоты мы сначала предположим, что $\mathsf{P}_k \cap \mathsf{P}_f = \mathsf{P}_d = \mathsf{P}$, т. е. что $(k, f) = d = 1$ или 2. Тогда ведущий модуль f характера χ не должен иметь общих делителей с порядком k характера χ, кроме, быть может, числа 2. В § 13, п. 6 был дан обзор всех характеров χ с данным ведущим модулем f посредством разложения на компоненты с ведущими модулями, равными степеням простых чисел; отсюда легко определить, для каких характеров χ с заданным порядком k ведущего модуля выполняется сделанное нами предположение. В качестве компонент, отличных от ε, подлежат рассмотрению только следующие (в обозначениях из § 13, п. 6):

а) для каждого простого нечетного числа p с $p \nmid k$ и $(k, p-1) \neq 1$ характеры

$$\chi_p^{\varkappa_p \frac{p-1}{k_p}} \quad (\varkappa_p \not\equiv 0 \bmod k_p) \text{ порядков } \frac{k_p}{(\varkappa_p, k_p)};$$

количество таких характеров есть $k_p - 1 = (k, p-1) - 1$;

б) для простого числа 2 (поскольку k делится точно на 2^1) три характера χ_4, χ_8, $\chi_4\chi_8$ порядка 2. Характер χ, все компоненты которого принадлежат к числу только что названных, будет удовлетворять сделанному предположению тогда и только тогда, когда общее наименьшее кратное порядков компонент равно k.

Тогда пересечение полей P_k, P_f равно P. Подгруппа $\mathfrak{G}_0$ совпадает со всей группой Галуа $\mathfrak{G}$ поля P_f. Поэтому правило замены (2) можно в этом случае рассматривать как правило применения к $\tau(\chi)$ автоморфизмов $\zeta \to \zeta^a$ из $\mathfrak{G}$ для всех $a \bmod f$, взаимно простых с модулем. Из этого правила следует, что $\tau(\chi)$ инвариантно относительно точно той подгруппы $\mathfrak{H}$ группы $\mathfrak{G}$, которая характеризуется условием $\chi(a) = 1$; это подгруппа имеет индекс k, и фактор-группа по ней циклична. Как и в § 15, п. 5, обозначим через K соответствующее этой подгруппе, в силу основной теоремы теории Галуа, подполе степени k поля P_f; это подполе циклично. Тогда из теории Галуа следует, что $\tau(\chi)$ есть примитивный элемент расширения $\mathsf{P}_k\mathsf{K}/\mathsf{P}_k$, получающегося посредством присоединения k-х корней из 1 (значений характера χ) к основному полю P и полю K (см. фиг. 25). Так как, согласно (2), $\tau(\chi)^k$ инвариантно относительно всех автоморфизмов $\zeta \to \zeta^a$ расширения $\mathsf{P}_k\mathsf{P}_f/\mathsf{P}_k$, эта степень лежит в основном поле P_k. Поэтому $\tau(\chi)$ удовлетворяет уравнению $\tau(\chi)^k = \omega(\chi)$ с $\omega(\chi)$ из P_k, причем многочлен $x^k - \omega(\chi)$ неприводим над P_k, ибо $\tau(\chi)$ как примитивный элемент расширения $\mathsf{P}_k\mathsf{K}/\mathsf{P}_k$ должен иметь ту же степень k, что и само расширение.

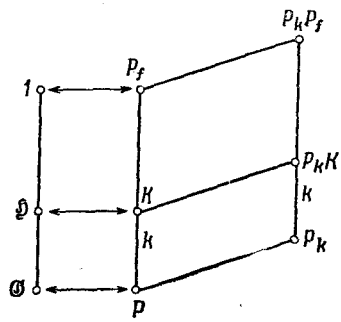
В силу всего изложенного, мы можем считать установленным следующий факт, являющийся обобщением результата X п. 5 § 15 для частного случая $k = 2$:

VII. *Пусть* χ *— характер порядка* k *с натуральным ведущим модулем* f *и пусть* f *не имеет общих делителей с* k, *кроме, быть может, числа* 2, *так что компоненты характера* χ *имеют тип* а) *или* б).

Пусть, далее, K *— циклическое подполе степени* k *поля* P_f, *инвариантное относительно автоморфизмов* $\zeta \to \zeta^a$ *поля* P_f *с* $\chi(a) = 1$.

Тогда, после присоединения к P *и* K k*-х корней из* 1, *расширение будет порождаться принадлежащей характеру* χ *нормированной собственной гауссовой суммой* $\tau(\chi)$, *т. е.*

$$\mathsf{P}_k\mathsf{K} = \mathsf{P}_k(\tau(\chi)).$$



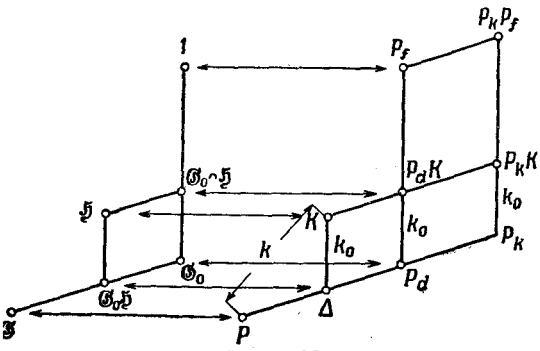
Фиг. 25.

При этом $\tau(\chi)$ *удовлетворяет неприводимому над полем* P_k *уравнению* k*-й степени вида*

$$\tau(\chi)^k = \omega(\chi),$$

где $\omega(\chi)$ *есть некоторое число из* P_k.

Если отбросить ограничительное предположение относительно $(k, f) = d$, то дело будет обстоять несколько сложнее (фиг. 26). В этом случае определенное выше поле K может нетривиально пересекаться с присоединяемым полем P_k корней из 1. Пересечению $\Delta = \mathsf{P}_k \cap \mathsf{K} = \mathsf{P}_d \cap \mathsf{K}$ соответствует объединение $\mathfrak{G}_0\mathfrak{H}$ подгрупп группы $\mathfrak{G}$, определяемых условиями $a_0 \equiv 1 \bmod d$ и $\chi(a) = 1$; это



Фиг. 26.

пересечение получается посредством расширения взаимно простых с модулем классов вычетов $a \bmod f$ с $\chi(a) = 1$ до взаимно простых с модулем классов вычетов $a \bmod f$, и потому (как группа классов вычетов, а не как группа автоморфизмов) это

пересечение является наименьшей группой классов вычетов, содержащей $\mathfrak{H}$, из числа тех, которые определены уже по $\bmod d$. Степень k_0 расширения K/Δ и потому также и расширения $\mathsf{P}_k\mathsf{K}/\mathsf{P}_k$ равна такому наименьшему делителю k_0 числа k, для которого χ^{k_0} определен уже по $\bmod d$. Снова имеет место

$$\mathsf{P}_k\mathsf{K} = \mathsf{P}_k(\tau(\chi)),$$

но теперь $\tau(\chi)$ удовлетворяет неприводимому над P_k уравнению такого же вида, как и раньше, но лишь k_0-й степени.

Результат VII мы осветим сначала с алгебраической точки зрения. Будем записывать автоморфизмы из $\mathfrak{G}$ в виде

$$A = (\zeta \to \zeta^a)$$

как операторы, и применение автоморфизма к некоторому числу будем обозначать посредством написания A в виде показателя степени (например, $\zeta^A = \zeta^a$). Пусть R — полная система представителей классов фактор-группы $\mathfrak{G}/\mathfrak{H}$ (в соответствии с циклической структурой $\mathfrak{G}/\mathfrak{H}$ эту систему можно представить в форме $R = R_0^\varkappa$ с $\varkappa \bmod k$); таким образом,

$$\mathfrak{G} = \sum_{R \text{ по } \mathfrak{H}} R\mathfrak{H}.$$

Если это разложение $\mathfrak{G}$ по $\mathfrak{H}$ применить к формуле (1), определяющей $\tau(\chi)$, то мы получим теоретико-групповую запись

$$\tau(\chi) = \sum_{R \text{ по } \mathfrak{H}} \chi(R)\,\theta^R \quad \text{с} \quad \theta = \sum_{X \text{ из } \mathfrak{H}} \zeta^X \tag{3}$$

для нормированной собственной гауссовой суммы, принадлежащей характеру χ. Фигурирующее здесь число θ принадлежит полю P_f и инвариантно относительно всех автоморфизмов из $\mathfrak{H}$, т. е. лежит в подполе K. Числа θ^R получаются из θ посредством применения автоморфизмов $R\mathfrak{H}$ из группы Галуа $\mathfrak{G}/\mathfrak{H}$ поля K и потому являются как раз всеми k сопряженными с θ числами из K. По Гауссу, их называют также принадлежащими подгруппе $\mathfrak{H}$ f-ми периодами деления круга.

Рассмотрим теперь вместе с χ сразу весь цикл $\chi^\varkappa(\varkappa \bmod k)$, т. е. соответствующую в смысле § 15, п. 1 группе $\mathfrak{H}$ группу характеров $\mathfrak{K}$, которая оказывается здесь группой характеров для $\mathfrak{G}/\mathfrak{H}$. Принадлежащие этим характерам гауссовы суммы при определении по $\bmod f$ имеют вид, аналогичный (3):

$$\tau(\chi_f^\varkappa \mid \zeta_f) = \sum_{R \text{ по } \mathfrak{H}} \chi^\varkappa(R)\,\theta^R \quad (\varkappa \bmod k). \tag{4}$$

Индекс f при аргументах в левой части равенства мы поставили потому, что здесь речь идет об общих гауссовых суммах в смысле 1, которые хотя и являются здесь правильными (так

как $f(\chi^x)$ делит $f=f(\chi)$) и даже первообразными, но не обязательно будут собственными (так как возможен случай собственного делителя). При применении к этим суммам автоморфизмов A из $\mathfrak{G}$, согласно общему правилу (2) п. 1, получается

$$\tau(\chi_f^x|\zeta_f)^A=\chi^x(A)\,\tau(\chi_f^x|\zeta_f), \tag{5}$$

что можно вывести и непосредственно из (4).

Ради простоты мы сделаем здесь более сильное предположение, чем раньше, именно, будем считать, что $(k, f)=1$, т. е. что характер χ порядка k имеет ведущий модуль f, взаимно простой с k. Это означает, что χ может иметь только компоненты указанного выше типа а) и не может иметь компонент типа б). Тогда, согласно III п. 1, для всех $\tau(\chi_f^x|\zeta_f)$ имеет место

$$\tau(\chi_f^x|\zeta_f)\neq 0. \tag{6}$$

Действительно, f есть произведение различных нечетных простых чисел $p\nmid k$, так что все время $\mu(f/f(\chi^x))\neq 0$ и, кроме того, $f/f(\chi^x)$ все время взаимно просто с $f(\chi^x)$, откуда $\chi^x(f/f(\chi^x))\neq 0$.

Из (5), (6) мы выведем, что k чисел $\tau(\chi_f^x|\zeta_f)$ из $\mathsf{P}_k\mathsf{K}$ образуют базис расширения $\mathsf{P}_k\mathsf{K}/\mathsf{P}_k$. Действительно, из линейного соотношения

$$\sum_{x \bmod k} c_x\tau(\chi_f^x|\zeta_f)=0$$

с коэффициентами c_x из P_k следует, согласно (5), система линейных уравнений

$$\sum_{x \bmod k}\bar{\chi}^x(R)\,c_x\tau(\chi_f^x|\zeta_f)=0 \quad (R \text{ по } \mathfrak{H});$$

согласно II п. 2 § 13 эта система имеет единственное решение $c_x\tau(\chi_f^x|\zeta_f)=0$, а это, в силу (6), означает, что для всех c_x имеет место $c_x=0$.

Разрешая аналогично систему линейных уравнений (4), мы получаем

$$\theta^R=\frac{1}{k}\sum_{x \bmod k}\chi^x(R)\,\tau(\chi_f^x|\zeta_f). \tag{7}$$

Поэтому сопряженные θ^R также образуют базис расширения $\mathsf{P}_k\mathsf{K}/\mathsf{P}_k$, и, будучи числами из K, также и базис расширения K/P. Отсюда вытекает, в частности, что

$$\mathsf{K}=\mathsf{P}(\theta),$$

т. е. соответствующее группе $\mathfrak{H}$ подполе K поля P_f порождается первой основной симметрической функцией (3) от ζ^X с X из $\mathfrak{H}$.

Следовательно, алгебраическое значение гауссовой суммы $\tau(\chi)$ состоит в том, что при переходе (3) от θ к $\tau(\chi)$ циклическое уравнение степени k над P, которому удовлетворяет θ, преобразуется в двучленное уравнение k-й степени для $\tau(\chi)$ над P. В классической алгебре говорят также, что $\tau(\chi)$ является *резольвентой Лагранжа* для θ. Состоящий из сопряженных между собой чисел θ^R так называемый *нормальный базис* поля K посредством линейного преобразования (4), допускающего обращение (7), переводится в базис $\tau(\chi_f^x \mid \zeta_f)$ расширения $\mathsf{P}_k\mathsf{K}/\mathsf{P}_k$, который в связи с его поведением (5) при автоморфизмах называется фактор-базисом расширения $\mathsf{P}_k\mathsf{K}/\mathsf{P}_k$.

При этом алгебраическом рассмотрении мы оставили в стороне тот случай, когда f и k имеют общий простой делитель. В этом случае дело обстоит несколько сложнее. Здесь мы не будем рассматривать этот случай.

Теперь мы выясним арифметическое значение результата VII. В частном случае $k=2$ квадратичного характера χ (когда сделанное предположение $(k,\ f)=1$ или 2 не представляет собой никакого ограничения) число $\tau(\chi)^2=\omega(\chi)$ из $\mathsf{P}_k=\mathsf{P}_2=\mathsf{P}$ у нас определено; именно, согласно X п. 5 § 15, $\tau(\chi^2)=\chi(-1)f$. Получающееся таким образом вложение квадратичного поля $\mathsf{K}=\mathsf{P}(\sqrt{\chi(-1)f})$ в поле P_f корней из 1 представляет собой основу невыкладочного доказательства квадратичного закона взаимности в § 19, п. 3, а также и доказательства в § 8, где непосредственно используются гауссовы суммы. В связи с этим представляет большой интерес определить в явном виде число $\tau(\chi)^k=\omega(\chi)$ из P_k также и при общих предположениях из VII, т. е. выразить это число через k-е корни из 1, например в виде значений характера χ.

На основании правила VI п. 2 разложения на компоненты эта задача сводится к тому частному случаю, когда $f=p^\nu$ есть степень простого числа p, так что χ имеет один из вышеназванных типов «а» «б». Так как квадратичный случай $k=2$ у нас уже исследован, нам остается решить следующую задачу: определить $\tau(\chi)^k=\omega(\chi)$ в явном виде как число из P_k для характера χ порядка $k\geqslant 3$ группы классов вычетов по нечетному простому модулю $p\equiv 1 \bmod k$, взаимно простых с модулем.

Мы решим эту задачу в п. 4. В тех случаях, когда нам известна арифметическая структура поля P_k корней из 1, мы выведем также арифметическую характеристику числа $\omega(\chi)$ из P_k. Поскольку основы арифметики подробно изложены нами лишь для квадратичных полей, к числу этих случаев относятся только те, когда P_k квадратично, т. е. случаи $k=3,\ 4,\ 6$ с $\mathsf{P}_3=\mathsf{P}_6=\mathsf{P}(\sqrt{-3})$, $\mathsf{P}_4=\mathsf{P}(\sqrt{-1})$.

Если отбросить ограничительное предположение в VII относительно $(k, f) = d$, то при заданном порядке k при сведении к компонентам с модулями $f = p^\nu$ каждый раз будет добавляться только конечное число случаев, соответствующих простым делителям p числа k; эти случаи легко могут быть рассмотрены посредством указания непосредственного значения $\tau(\chi)$, а тем самым также и $\tau(\chi)^{k_0}$ (с определенным выше показателем степени $k_0 \mid k$).

В частности, для $k = 3$, 6 и $k = 4$ это будут следующие случаи:

а) для $k = 3$ два комплексно сопряженных бикубических характера χ_9, $\bar{\chi}_9$ с ведущим модулем 9; для $k = 6$, кроме того, еще $\chi_3\chi_9$, $\bar{\chi}_3\chi_9$;

б) для $k = 4$ два комплексно сопряженных четных биквадратичных характера χ_{16}, $\bar{\chi}_{16}$ и, кроме того, два нечетных характера $\chi_4\chi_{16}$, $\bar{\chi}_4\chi_{16}$.

При этом все время $k_0 = k$, и прямым вычислением мы немедленно получаем значения:

$$\left.\begin{aligned} &\tau(\chi_9) = 3\zeta, \quad \tau(\chi_9)^3 = 3^3\rho \\ &\tau(\chi_3\chi_9) = 3\bar{\zeta}, \quad \tau(\chi_3\chi_9)^3 = 3^3\rho \end{aligned}\right\}, \qquad \text{если } \chi_9(2) = \rho,$$

$$\left.\begin{aligned} &\tau(\chi_{16}) = 4\zeta, \quad \tau(\chi_{16})^4 = 16^2 i \\ &\tau(\chi_4\chi_{16}) = 4\bar{\zeta}, \quad \tau(\chi_4\chi_{16})^4 = 16^2 i \end{aligned}\right\}, \qquad \text{если } \chi_{16}(3) = i.$$

Значения характеров, комплексно сопряженных с χ, получаются по общему правилу (1) в § 18, п. 3.

4. Связь гауссовых сумм с суммами для характеров в случае нечетного простого модуля. Решение задачи, поставленной в конце п. 3, связано с обобщением рассматривавшихся в § 10, п. 6, 8, 9 сумм $\pi(\chi, \psi)$ для характеров; при этом будет также доказано утверждение (21) п. 5 § 18, принятое там на веру.

Пусть p — нечетное простое число и пусть χ, ψ — два характера по $\bmod p$ порядков k, l; эти порядки являются делителями числа $p - 1$.

Определим

$$\pi(\chi, \psi) = \sum_{x+y=1} \chi(x)\,\psi(y), \tag{1}$$

где для упрощения записи x, y понимаются теперь, в отличие от предыдущего, как элементы простого поля Π характеристики p, т. е. как классы вычетов по $\bmod p$.

Эти суммы не являются травиальными лишь при условии

$$\chi \neq \varepsilon, \quad \psi \neq \varepsilon, \quad \chi\psi \neq \varepsilon, \tag{2}$$

где ε обозначает, как и выше, главный характер по mod p. Действительно, вследствие того, что $\sum_x \chi(x) = 0$ для $\chi \neq \varepsilon$, очевидно, имеет место

$$\pi(\varepsilon, \varepsilon) = p,$$

далее,

$$\pi(\chi, \varepsilon) = 0 \text{ для } \chi \neq \varepsilon,$$

и точно так же

$$\pi(\varepsilon, \psi) = 0 \text{ для } \psi \neq \varepsilon,$$

и, наконец,

$$\pi(\chi, \psi) = \pi(\chi, \bar{\chi}) = -\chi(-1) \text{ для } \chi \neq \varepsilon,\ \psi \neq \varepsilon,\ \chi\psi = \varepsilon,$$

$$\text{т. е. для } \psi = \bar{\chi} \neq \varepsilon.$$

Последнее следует из рассмотрения выражения

$$\pi(\chi, \chi^{-1}) = \sum_{x \neq 1} \chi\left(\frac{x}{1-x}\right),$$

если заметить, что когда x пробегает все отличные от 1 элементы из Π, дробно-линейная функция $x/(1-x)$ пробегает все элементы из Π, отличные от -1, причем каждый из них точно один раз.

Подобно специальным случаям $k = 4$, 3 и $l = 2$ из § 10, п. 8, 9, суммы $\pi(\chi, \psi)$ связаны с количеством решений уравнения

$$x^k + y^l = 1$$

в простом поле Π. Именно, аналогично указанным специальным случаям, мы, согласно VII п. 4 § 13, имеем в общем случае

$$N[x^k + y^l = 1] = \sum_{x^k + y^l = 1} 1 =$$

$$= \sum_{u+v=1} \sum_{\chi^k = \varepsilon} \chi(u) \sum_{\psi^l = \varepsilon} \psi(v) = \sum_{\chi^k = \varepsilon} \sum_{\psi^l = \varepsilon} \pi(\chi, \psi),$$

где χ, ψ пробегают k, l характеров по mod p с показателями k, l. Если подставить сюда полученные перед этим значения $\pi(\chi, \psi)$ для не удовлетворяющих условиям (2) тривиальных пар χ, ψ, то мы получим формулу

$$N[x^k + y^l = 1] = p + 1 - N_\infty + \sum_{\substack{\chi^k = \varepsilon,\ \psi^l = \varepsilon \\ \chi,\ \psi,\ \chi\psi \neq \varepsilon}} \pi(\chi, \psi), \tag{3}$$

где добавочный член N_∞ в правой части определяется следующим образом. Пусть $(k, l) = d$, так что существует точно d пар χ, ψ с $\chi\psi \neq \varepsilon$, а именно, решения χ уравнения $\chi^d = \varepsilon$ в (циклической) группе характеров по mod p, вместе со своими сопря-

женными $\psi = \bar{\chi}$. Тогда

$$N_\infty = \sum_{\chi^d = \varepsilon} \chi(-1) = \sum_{\delta \bmod d} (-1)^{\frac{p-1}{d}\delta} =$$

$$= \left\{ \begin{array}{l} d, \text{ если } \frac{p-1}{d} \text{ четно,} \\ 0, \text{ если } \frac{p-1}{d} \text{ нечетно, } d \text{ четно,} \\ 1, \text{ если } \frac{p-1}{d} \text{ нечетно, } d \text{ нечетно} \end{array} \right\}.$$

Подобно тому как в § 10 п. 3, этот добавочный член можно рассматривать как количество бесконечных решений рассматриваемого уравнения. Тогда формула (3) означает, что *полное количество решений* $N + N_\infty$ отличается от $p+1$ (что равно количеству элементов поля Π с присоединением ∞), как *среднего значения*, точно на сумму нетривиальных сумм $\pi(\chi, \psi)$ для характеров, играющую здесь роль *ошибки*; это является обобщением результатов для рассматривавшихся в § 10, п. 6, 8, 9 специальных случаев.

Докажем теперь следующую связь нетривиальных сумм $\pi(\chi, \psi)$ с принадлежащими характерам χ, ψ и $\chi\psi$ (собственными нормированными) гауссовыми суммами:

VIII. *Для* $\chi \neq \varepsilon$, $\psi \neq \varepsilon$, $\chi\psi \neq \varepsilon$ *имеет место*

$$\pi(\chi, \psi) = \frac{\tau(\chi)\tau(\psi)}{\tau(\chi\psi)}.$$

Доказательство. На основании редукции (3) п. 1 значения характеров в формуле (1) для $\pi(\chi, \psi)$ можно представить в виде отношений

$$\chi(x) = \frac{\tau(\bar{\chi} \mid \zeta^x)}{\tau(\bar{\chi})}, \quad \psi(y) = \frac{\tau(\bar{\psi} \mid \zeta^y)}{\tau(\bar{\psi})},$$

где ζ обозначает первообразный p-й корень из 1, положенный в основу нормирования. Тогда

$$\pi(\chi, \psi) = \frac{1}{\tau(\bar{\chi})\tau(\bar{\psi})} \sum_{x+y=1} \tau(\bar{\chi} \mid \zeta^x)\tau(\bar{\psi} \mid \zeta^y) =$$

$$= \frac{1}{\tau(\bar{\chi})\tau(\bar{\psi})} \sum_{x+y=1} \sum_{u,\,v} \bar{\chi}(u)\bar{\psi}(v)\zeta^{ux+vy} =$$

$$= \frac{1}{\tau(\bar{\chi})\tau(\bar{\psi})} \sum_{u,v} \bar{\chi}(u)\bar{\psi}(v) \sum_{x+y=1} \zeta^{ux+vy} =$$

$$= \frac{1}{\tau(\bar{\chi})\tau(\bar{\psi})} \sum_{u,v} \bar{\chi}(u)\bar{\psi}(v)\zeta^v \sum_x \zeta^{(u-v)x} =$$

$$= \frac{p}{\tau(\bar{\chi})\tau(\bar{\psi})} \sum_u \bar{\chi}(u)\bar{\psi}(u)\zeta^u = \frac{p\tau(\bar{\chi}\bar{\psi})}{\tau(\bar{\chi})\tau(\bar{\psi})}.$$

Согласно (1) п. 3 § 18, мы имеем

$$\tau(\bar{\chi}) = \frac{\chi(-1)\,p}{\tau(\chi)},\quad \tau(\bar{\psi}) = \frac{\psi(-1)\,p}{\tau(\psi)},\quad \tau(\bar{\chi}\bar{\psi}) = \frac{\chi(-1)\,\psi(-1)\,p}{\tau(\chi\psi)}.$$

Отсюда следует наше утверждение. При наших выкладках существенно использовались предположения $\chi \neq \varepsilon$, $\psi \neq \varepsilon$, $\chi\psi \neq \varepsilon$; действительно, в противном случае (при нашем понимании $\tau(\bar{\chi}|\zeta^x)$, $\tau(\bar{\psi}|\zeta^y)$ как гауссовых сумм, определенных по $\bmod p$) при включении в систему переменных суммирования значения 0 у нас получались бы отклонения (которые опять-таки сводились бы к определенным выше тривиальным значениям).

Относительно результата VIII нужно сделать следующее принципиальное замечание. Из поведения гауссовых сумм при автоморфизме $\zeta \to \zeta^a$ поля P_p следует, что выражение в правой части в VIII инвариантно относительно всех этих автоморфизмов и потому принадлежит полю $\mathsf{P}_k\mathsf{P}_l$ значений характеров. Если рассматривать произведенные нами выкладки в обратном порядке, то мы получим для этого выражения явное представление через значения характеров, причем как раз в виде суммы $\pi(\chi, \psi)$ для характеров χ, ψ.

Результат VIII можно истолковать еще и так. Пусть $\mathfrak{X}$ — группа всех характеров по $\bmod p$. Согласно IV п. 3 § 13, она изоморфна группе классов вычетов $\bmod p$, взаимно простых с модулем, и потому является циклической группой порядка $p-1$. Посредством нормированных собственных гауссовых сумм $\tau(\chi)$ характерам χ из $\mathfrak{X}$ сопоставляются числа из поля $\mathsf{P}_{p-1}\mathsf{P}_p$ корней из 1. Это соответствие, правда, не является гомоморфизмом, но все же произведение $\tau(\chi)\,\tau(\psi)$ отличается от $\tau(\chi\psi)$ только на множитель из поля P_{p-1} более низкой степени. Результат VIII дает в нетривиальных случаях явное выражение для этого множителя в виде суммы $\pi(\chi, \psi)$. В тривиальных случаях этот множитель может быть непосредственно определен вследствие того, что $\tau(\varepsilon) = 1$ (однако, вследствие уже отмеченного различия между собственными и несобственными гауссовыми суммами, принадлежащими главному характеру ε, определенному по $\bmod p$, этот множитель не будет совпадать с определенными выше значениями $\pi(\chi, \psi)$ для этих тривиальных случаев). В связи с таким истолкованием совокупность (нетривиальных) сумм $\pi(\chi, \psi)$ для характеров называется также *фактор-системой гауссовых сумм*, принадлежащих характерам по $\bmod p$.

Из формулы (3) п. 2 для абсолютных величин гауссовых сумм, согласно VIII, следует формула

$$|\pi(\chi, \psi)| = \sqrt{p} \tag{4}$$

для абсолютных величин нетривиальных сумм для характеров. Для количества решений N из (3) получается при этом оценка

ошибки:

$$|(N+N_\infty)-(p+1)|\leqslant[(k-1)(l-1)-(d-1)]\sqrt{p},$$

принадлежащая к общему типу, рассмотренному в § 10, п. 3. Множитель при $\sqrt{p}$ в действительности оказывается равным удвоенному роду $2g$ рассматриваемого уравнения $x^k+y^l=1$.

После этих замечаний принципиального характера к результату VIII мы переходим теперь к решению поставленной в конце 3 задачи, именно, к определению в явном виде чисел $\tau(\chi)^k=\omega(\chi)$ из P_k для характеров χ порядка k по простому модулю $p\equiv 1 \bmod k$.

Ясно, что зная фактор-систему гауссовых сумм, мы можем определить специальные множители $\omega(\chi)$ из

$$\tau(\chi)^k=\omega(\chi)\,\tau(\chi^k)=\omega(\chi)\,\tau(\varepsilon)=\omega(\chi),$$

соответствующие произведенному k раз умножению гауссовой суммы самое на себя.

Для этого надо образовать произведение следующих k отдельных равенств:

$$\begin{aligned}
\tau(\chi)\cdot\tau(\varepsilon) &= 1\cdot\tau(\chi)\\
\tau(\chi)\cdot\tau(\chi) &= \pi(\chi,\chi)\cdot\tau(\chi^2)\\
\tau(\chi)\cdot\tau(\chi^2) &= \pi(\chi,\chi^2)\,\tau(\chi^3)\\
&\cdots\cdots\cdots\cdots\\
\tau(\chi)\cdot\tau(\chi^{k-2}) &= \pi(\chi,\chi^{k-2})\cdot\tau(\chi^{k-1})\\
\tau(\chi)\cdot\tau(\chi^{k-1}) &= \chi(-1)\,p\cdot\tau(\varepsilon).
\end{aligned}$$

Так получается формула

$$\tau(\chi)^k=\chi(-1)\,p\,\pi(\chi,\chi)\,\pi(\chi,\chi^2)\ldots\pi(\chi,\chi^{k-2}), \tag{5}$$

где предполагается $\chi\neq\varepsilon$. Эта формула дает решение нашей задачи. Для $k=2$, когда произведение членов, стоящих после p, отсутствует, это дает нам результат, содержащийся еще в (2) п. 2 § 8, который, впрочем, получается и из последней строки нашей схемы доказательства. Для $k\geqslant 3$ искомое число $\omega(\chi)$ из P_k получается, согласно (5), в виде произведения тривиального множителя $\chi(-1)\,p$ и нетривиальных сумм для характеров, принадлежащих, с одной стороны, самому χ и, с другой стороны, его степеням χ^x.

Формула (5) была получена нами как простое формальное следствие из основной связи VIII между гауссовыми суммами и суммами для характеров по $\bmod p$, которая в свою очередь была выведена из определений этих обоих типов сумм посредством простых преобразований. Замечательно то, что, помимо

формулы (5), существует более общая система соотношений между гауссовыми суммами и суммами для характеров по mod p; однако доказать это столь же простым формальным способом можно только для некоторых частных случаев. Именно, имеет место:

IX. *Если l — произвольный делитель $p-1$, а χ — такой характер* mod p, *что $\chi^l \neq \varepsilon$, то*

$$\frac{\tau(\chi)^l}{\tau_l(\chi^l)} = \prod_{\substack{\psi^l=\varepsilon \\ \psi\neq\varepsilon}} \pi(\chi, \psi), \tag{6}$$

где положено

$$\tau_l(\chi^l) = \tau(\chi^l \mid \zeta^l) = \overline{\chi}^l(l)\,\tau(\chi^l),$$

а ψ пробегает все $l-1$ характеров mod p, *имеющих показатель l и отличных от главного характера.*

Это соотношение может быть также записано в форме

$$\prod_{\psi^l=\varepsilon} \tau(\chi\psi) = \tau_l(\chi^l) \prod_{\psi^l=\varepsilon} \tau(\psi). \tag{7}$$

Последнее получается сразу, если заменить в (6) $\pi(\chi, \psi)$ их выражениями согласно VIII, а также присоединить множители $\tau(\varepsilon)=1$ и $\tau(\chi\varepsilon)=\tau(\chi)$. Надо иметь в виду, что, так как в (6) $\chi^l \neq \varepsilon$, то всегда $\chi \neq \varepsilon$, $\psi \neq \varepsilon$, $\chi\psi \neq \varepsilon$, так что VIII действительно применимо. Соотношение в форме (7) содержит только гауссовы суммы mod p. Оно показывает, что между $p-1$ различными нормированными гауссовыми суммами существует нетривиальное мультипликативное соотношение. По всей вероятности, к этим соотношениям сводятся все соотношения такого типа.

Что касается доказательства IX, то мы приведем его только для случая $l=2$, где еще можно прийти к цели при помощи простых преобразований. Для общего случая известны два доказательства. Первое основывается на арифметической характеристике сумм $\pi(\chi, \psi)$ как чисел поля $\mathsf{P}_k\mathsf{P}_l$, аналогичной той, которая была получена нами в § 10 п. 8, 9 для частных случаев $k=3, 4$, $l=2$. Для проведения этого доказательства необходимо привлечь арифметику полей, являющихся полями корней из единицы. Второе доказательство основывается на том, что суммы $\pi(\chi, \psi)$ появляются как остаточный член в формуле (3) для числа решений уравнения $x^k+y^l=1$ в простом поле Π. Это доказательство привлекает *аналитические* средства, а именно, L-ряды, принадлежащие полю алгебраических функций $\Pi(x, y)$, определяемому этим уравнением. По поводу этих доказательств мы должны отослать читателя к исходной работе Давенпорта и Хассе [1].

Доказательство IX при $l=2$. Соотношение (6), которое нам надо доказать, означает в этом случае

$$\frac{\tau(\chi)^2}{\tau_2(\chi^2)} = \pi(\chi, \psi) \text{ для } \chi^2 \neq \varepsilon,\ \psi^2 = \varepsilon,\ \psi \neq \varepsilon, \tag{8}$$

т. е. для любого неквадратичного характера $\chi \neq \varepsilon$ и квадратичного характера $\psi \bmod p$ (символ Лежандра).

Мы имеем:

$$\tau(\chi)^2 = \sum_{x,y} \chi(xy)\,\zeta^{x+y} = \sum_t \zeta^t \sum_{x+y=t} \chi(xy).$$

При $t=0$, ввиду того что $\chi^2 \neq \varepsilon$, отсюда получается:

$$\sum_{x+y=0} \chi(xy) = \sum_x \chi(-x^2) = \chi(-1) \sum_x \chi(x^2) = 0.$$

При $t \neq 0$ подстановка $x \to \frac{xt}{2}$, $y \to \frac{yt}{2}$ дает:

$$\sum_{x+y=t} \chi(xy) = \chi^2\left(\frac{t}{2}\right) \sum_{x+y=2} \chi(xy).$$

Отсюда следует, далее,

$$\tau(\chi)^2 = \sum_t \chi^2\left(\frac{t}{2}\right)\zeta^t \sum_{x+y=2} \chi(xy) = \sum_t \chi^2(t)\,\zeta^{2t} \sum_{x+y=2} \chi(xy) =$$

$$= \tau_2(\chi^2) \sum_{x+y=2} \chi(xy).$$

Таким образом, нам остается только доказать формулу

$$\sum_{x+y=2} \chi(xy) = \pi(\chi, \psi) \quad \text{при} \quad \chi^2 \neq \varepsilon,\ \psi^2 = \varepsilon,\ \psi \neq \varepsilon. \tag{9}$$

Это доказательство получается из следующего красивого соображения. В сумме, стоящей в левой части равенства (9), встречаются обе основные симметрические функции $x+y$ и xy переменных суммирования x и y. Таким образом, нам нужно найти сумму значений характера $\chi(z)$ для тех значений z, для которых квадратный трехчлен t^2-2t+z разлагается в поле Π на два линейных множителя:

$$t^2-2t+z = (t-x)\,(t-y).$$

Так как дискриминант этого многочлена равен $4(1-z)$, то при задании z из Π многочлен имеет в Π $1+\psi(1-z)$ пар корней (x, y), если учитывать порядок корней. Таким образом,

$$\sum_{x+y=2} \chi(xy) = \sum_z (1+\psi(1-z))\,\chi(z) = \sum_z \chi(z)\,\psi(1-z) = \pi(\chi, \psi),$$

что и утверждалось в (9).

Мы применим теперь выведенную нами формулу (8), чтобы в частных случаях $k=4$ и $k=3, 6$ представить в более простой форме общее решение нашей задачи из конца п. 3, содержащееся в (5). Эта новая форма связана с полученной нами в § 10, п. 8, 9 и в § 18, п. 5 арифметической характеристикой сумм $\pi(\chi, \psi)$ в рассматриваемых сейчас частных случаях.

а) *Биквадратичный характер* ($k=4$). Пусть $p \equiv 1 \bmod 4$, а χ и $\bar{\chi}$ — оба имеющихся в этом случае комплексно сопряженных биквадратичных характера $\bmod p$. Тогда $\chi^2 = \bar{\chi}^2 = \psi$ является квадратичным характером $\bmod p$. Формула (8) дает в этом случае

$$\tau(\chi)^2 = \psi(2)\,\tau(\psi)\,\pi(\chi, \psi), \quad \tau(\bar{\chi})^2 = \psi(2)\,\tau(\psi)\,\pi(\bar{\chi}, \psi).$$

Это как раз те формулы, которые мы без доказательства привели в (21) п. 5 § 18. Теперь они доказаны. Согласно (22), (24) п. 5 § 18, мы получаем теперь

$$\tau(\chi)^2 = -\tau(\psi)\,\pi = -\sqrt{p}\,\pi, \quad \tau(\bar{\chi})^2 = -\tau(\psi)\,\bar{\pi} = -\sqrt{p}\,\bar{\pi}$$

и тем самым

$$\tau(\chi)^4 = p\pi^2, \quad \tau(\bar{\chi})^4 = p\bar{\pi}^2, \tag{10а}$$

где

$$\pi = -\psi(2)\,\pi(\chi, \psi), \quad \bar{\pi} = -\psi(2)\,\pi(\bar{\chi}, \psi)$$

являются комплексно сопряженными простыми делителями p в поле $\mathsf{P}_4 = \mathsf{P}(i)$ с нормировкой, принятой в (26) п. 5 § 18. Таким образом, в несколько других обозначениях, чем там, мы будем иметь:

$$\left.\begin{array}{l} \pi, \bar{\pi} = A \pm 2Bi \\ p = A^2 + 4B^2 \end{array}\right\} \text{ с } A \equiv 1 \bmod 4. \tag{11а}$$

Сравнение (10а) с общей формулой (5) дает, кроме того, нетривиальное соотношение между суммами характеров:

$$\pi(\chi, \psi) = \chi(-1)\,\pi(\chi, \chi), \quad \pi(\bar{\chi}, \psi) = \chi(-1)\,\pi(\bar{\chi}, \chi). \tag{12а}$$

б) *Кубические характеры* ($k=3$). Пусть $p \equiv 1 \bmod 3$, χ и $\bar{\chi}$ — имеющиеся в этом случае комплексно сопряженные кубические характеры, а ψ, как и раньше, квадратичный характер $\bmod p$. Тогда $\chi^2 = \bar{\chi}$, $\bar{\chi}^2 = \chi$ и, ввиду того что $\chi(-1) = 1$, из формулы для модуля $\tau(\chi)$ следует $\tau(\chi)\,\tau(\bar{\chi}) = p$. Формула (8) дает здесь, следовательно,

$$\tau(\chi)^3 = \chi(2)\,p\pi(\chi, \psi), \quad \tau(\bar{\chi})^3 = \bar{\chi}(2)\,p\pi(\bar{\chi}, \psi).$$

Таким образом, мы имеем

$$\tau(\chi)^3 = p\pi, \quad \tau(\bar{\chi})^3 = p\bar{\pi}, \tag{10б}$$

где

$$\pi = \chi(2)\,\pi(\chi, \psi), \quad \bar{\pi} = \bar{\chi}(2)\,\pi(\bar{\chi}, \psi)$$

являются комплексно сопряженными простыми делителями p в $\mathsf{P}_3 = \mathsf{P}(\rho)$, но здесь в другом нормировании, чем в § 10, п. 9.

Рассмотрим внимательнее это нормирование. Обозначим введенные в § 10, п. 9 суммы характеров через π^* и $\bar{\pi}^*$. Они получаются из определенных в (1) $\pi(\chi, \psi)$ и $\pi(\bar{\chi}, \psi)$ при помощи подстановки $y \to -y$ в переменной суммирования, следовательно,

$$\pi^* = \psi(-1)\,\pi(\chi, \psi), \quad \bar{\pi}^* = \psi(-1)\,\pi(\bar{\chi}, \psi).$$

Отщепляя множитель $\psi(-1)$, указывающий знак, мы превратим нормирование из § 10, п. 9 в

$$\pi(\chi, \psi) \equiv -1, \ \pi(\bar{\chi}, \psi) \equiv -1 \bmod 2\mathfrak{z},$$

где $\mathfrak{z} \cong 1-\rho \cong \sqrt{-3}$ означает простой делитель разветвляющегося в P_3 простого числа $3 \cong \mathfrak{z}^2$. Включение множителя 2 в модуль сравнения отражает то, что, как мы установили в § 10, речь идет о числах кольца $\bmod 2$ в P_3 (с четным коэффициентом при ρ). Эта нормировка соответствует тому, что шесть единиц ± 1, $\pm\rho$, $\pm\rho^2$, которые нам надо различить, не сравнимы друг с другом по $\bmod 2\mathfrak{z}$ (а ввиду того что $\Phi(2\mathfrak{z}) = \Phi(2)\,\Phi(\mathfrak{z}) = 3 \cdot 2 = 6$, составляют даже полную систему вычетов $\bmod 2\mathfrak{z}$). В рациональной форме наше нормирование записывается так:

$$\left\{\begin{array}{c} \pi(\chi, \psi), \ \pi(\bar{\chi}, \psi) = A \pm B\sqrt{-3} \\ p = A^2 + 3B^2 \end{array}\right\} \text{ с } A \equiv -1 \bmod 3. \qquad (11б_1)$$

Числа ± 1, $\pm\rho$, $\pm\rho^2$ не сравнимы друг с другом по $\bmod 3$ (и ввиду того что $\Phi(3) = \Phi(\mathfrak{z}^2) = 3 \cdot 2 = 6$ опять образуют полную систему вычетов по $\bmod 3$). Нормировка, полученная в (10б) для π и $\bar{\pi}$, может быть ввиду этого проще всего записана так:

$$\tau(\chi) = \sum_x \chi(x)\,\zeta^x \equiv \sum_{x \neq 0} \zeta^x \equiv -1 \bmod \mathfrak{z}.$$

По аналогии с леммой 3 п. 5 § 5 отсюда следует

$$\tau(\chi)^3 \equiv -1 \bmod \mathfrak{z}^3, \text{ т. е. } \bmod 3\mathfrak{z}.$$

Из (10б) следует, что, в силу $p \equiv 1 \bmod 3$, имеет место нормирование

$$\pi \equiv -1, \ \bar{\pi} \equiv -1 \bmod 3.$$

Оно показывает, что π и $\bar{\pi}$ принадлежат к кольцу $\bmod 3$ в P_3 и притом с вычетом $-1 \bmod 3$. В рациональной форме оно записывается так:

$$\left\{\begin{array}{c} \pi, \ \bar{\pi} = \dfrac{a \pm 3b\sqrt{-3}}{2} \\ p = \dfrac{a^2 + 27b^2}{4} \end{array}\right\} \text{ с } a \equiv 1 \bmod . 3. \qquad (11б_2)$$

Сравнение обоих нормирований (11б$_{1,2}$) на основании соотношения $\pi = \chi(2)\,\pi(\chi, \psi)$ дает следующее предложение, являющееся частным случаем кубического закона взаимности:

X. *Тогда и только тогда* $\chi(2) = 1$, *т. е. 2, является кубическим вычетом* mod p, *когда в разложениях* (11б$_{1,2}$) $B \equiv 0 \bmod 3$, *соответственно* $b \equiv 0 \bmod 2$.

Сравнивая (10б) с общей формулой (5), мы опять получаем нетривиальное соотношение между суммами характеров:

$$\pi(\chi, \psi) = \bar{\chi}(2)\,\pi(\chi, \chi), \quad \pi(\bar{\chi}, \psi) = \chi(2)\,\pi(\bar{\chi}, \bar{\chi}).$$

в) *Бикубические характеры* ($k = 6$). Этот случай сводится к предшествующему. При $p \equiv 1 \bmod 3$ мы будем иметь (в силу нечетности p), что $p \equiv 1 \bmod 6$ и в обозначениях предшествующего случая $\chi\psi$ и $\bar{\chi}\psi$ будут комплексно сопряженными бикубическими характерами mod p. Формула (7) из IX дает при $l = 2$ соотношение

$$\tau(\chi)\,\tau(\chi\psi) = \tau_2(\bar{\chi})\,\tau(\psi), \quad \tau(\bar{\chi})\,\tau(\bar{\chi}\psi) = \tau_2(\chi)\,\tau(\psi),$$

т. е. редукцию

$$\tau(\chi\psi) = \chi(2)\,\tau(\psi)\,\frac{\tau(\bar{\chi}^2)}{p}, \quad \tau(\bar{\chi}\psi) = \bar{\chi}(2)\,\tau(\psi)\,\frac{\tau(\chi)^2}{p}.$$

Согласно (10б) и ввиду того, что $\tau(\psi)^2 = p^*$, мы получаем отсюда

$$\tau(\chi\psi)^6 = p^{*3}\bar{\pi}^4, \quad \tau(\bar{\chi}\psi)^6 = p^{*3}\pi^4 \tag{10в}$$

с прежним значением для π и $\bar{\pi}$.

Сравнение с общей формулой (5) дает нетривиальные соотношения

$$\left.\begin{aligned} \pi(\bar{\chi}, \psi)^4 &= \psi(-1)\,\chi(2)\,\pi(\chi\psi, \chi)\,\pi(\chi\psi, \bar{\chi})\,\pi(\chi\psi, \psi)\,\pi(\chi\psi, \chi\psi) \\ \pi(\chi, \psi)^4 &= \psi(-1)\,\bar{\chi}(2)\,\pi(\bar{\chi}\psi, \bar{\chi})\,\pi(\bar{\chi}\psi, \chi)\,\pi(\bar{\chi}\psi, \psi)\,\pi(\bar{\chi}\psi, \bar{\chi}\psi). \end{aligned}\right\} \tag{12в}$$

Формулы (10а, б, в) дают для случаев $k = 4, 3, 6$ арифметическую характеристику чисел $\tau(\chi)^k = \omega(\chi)$ из VII п. 3. Чтобы получить ее в том же случае, который рассматривался там, нужно еще соединить в произведение полученные компоненты для отдельных простых делителей p ведущего модуля f. Таким образом получится разложение числа $\omega(\chi)$ на простые множители в поле P_k.

5. Определение знака для случая квадратичного характера. Мы обращаемся теперь к определению знака нормированной собственной гауссовой суммы, принадлежащей квадратичному характеру, о чем мы говорили уже в (2) п. 3 § 18.

Когда мы говорили в предшествующих частях этого параграфа о нормированных гауссовых суммах, то аналитическая нормировка $\zeta = e^{2\pi i/f}$ первообразного корня f-й степени из 1 не была

существенной. Речь шла собственно только о том, чтобы среди $\varphi(f)$ алгебраически сопряженных корней f-й степени из 1 выбрать один определенный. Тогда можно было свести все алгебраически сопряженные собственные гауссовы суммы $\tau(\chi|\zeta^a)$ с заданным характером χ и с ведущим модулем f к одной из них $\tau(\chi) = \tau(\chi|\zeta)$. Таким образом, речь шла только о значении ζ как алгебраического числа, и мы вполне могли положить в основу формальное понимание алгебраического числа. Можно было бы понимать под ζ просто элемент поля, удовлетворяющий уравнению деления круга $g_f(\zeta) = 0$ (см. § 11, п. 2), или, точнее, класс вычетов $x \bmod g_f(x)$, причем P_f было бы тогда полем классов вычетов поля рациональных функций $\mathsf{P}(x) \bmod g_f(x)$.

Для задачи, которой мы будем теперь заниматься, это чисто алгебраическая точка зрения недостаточна. Уже точная постановка вопроса носит существенно аналитический характер, а поэтому нет ничего удивительного в том, что и решение использует аналитические средства.

Для точной постановки вопроса необходимо иметь в виду следующее. С чисто алгебраической точки зрения для собственной гауссовой суммы

$$\tau(\chi) = \sum_{x \bmod f} \chi(x)\,\zeta^x$$

с квадратичным характером χ и с натуральным ведущим модулем f имеет место соотношение

$$\tau(\chi)^2 = \chi(-1)\,f,$$

не зависящее от выбора ζ. Таким образом,

$$\tau(\chi) = \sqrt{\chi(-1)\,f} \tag{1}$$

даже если алгебраическое число $\vartheta = \sqrt{\chi(-1)\,f}$ понимается чисто алгебраически, т. е. как такой элемент поля, для которого $\vartheta^2 = \chi(-1)\,f$. Точно так же чисто алгебраически выводится, что при применении автоморфизма $\zeta \to \zeta^a$ в уравнении (1) появляется влияющий на знак множитель $\chi(a)$. Ввиду (1) тогда сопоставляется одна, с теоретико-групповой точки зрения определенная, половина корней ζ^a многочлена $g_f(x)$ одному корню ϑ многочлена $x^2 - \chi(-1)\,f$, а другая — другому, $-\vartheta$. С чисто алгебраической точки зрения не имеет, однако, никакого смысла спрашивать, какая половина корней ζ^a сопоставляется какому из корней $\pm\vartheta$. Действительно, ни сопряженные корни ζ^a, ни сопряженные корни $\pm\vartheta$ не могут быть различены чисто алгебраически, т. е. при помощи алгебраического уравнения с рациональными коэффициентами, которое для одного из них выполняется, а для другого не выполняется. Точно так же алгебраические уравнения с коэффициентами из поля, не пересекающегося с полем P_f.

не могли бы служить для такого различения, как это следует из теорем теории Галуа, а допущение коэффициентов из поля, пересекающегося с P_f, привело бы нас к порочному кругу. Только допущение высказываний, использующих неалгебраические понятия, например понятие предела, может привести к такому различению. Так, например, при $\chi(-1)=1$ один из корней ϑ отличается от другого тем, что он является пределом последовательности отношений натуральных чисел — высказывание, использующее, кроме натуральных чисел, и понятие предела. Мы можем, используя построение поля вещественных чисел при помощи предельного перехода из рациональных чисел, определить это нормирование так: $\vartheta=\sqrt{f}$ является положительным корнем многочлена x^2-f в поле вещественных чисел. Для того чтобы включить и случай $\chi(-1)=-1$, надо присоединить еще к полю вещественных чисел фиксированное число $i=\sqrt{-1}$. В получаемом таким образом поле всех комплексных чисел всякий многочлен с целыми рациональными коэффициентами распадается на линейные множители, в силу основной теоремы алгебры комплексных чисел. Его корни можно, таким образом, различать при помощи высказываний, содержащих только понятие рационального числа и предела, если предварительно выделить одно из сопряженных чисел i и $-i$. Как раз таким нормированием одного из сопряженных алгебраических чисел ζ^a является аналитическое нормирование первообразного корня f-й степени из 1

$$\zeta=e^{2\pi i/f}=\cos\frac{2\pi}{f}+i\sin\frac{2\pi}{f},$$

использующее задание $\cos 2\pi/f$ и $\sin 2\pi/f$ в виде рядов. Точно так же алгебраическое число $\vartheta=\sqrt{\chi(-1)f}$ нормируется для различения от своего сопряженного $-\vartheta$ при помощи условия

$$\vartheta=\begin{cases}\sqrt{f} & \text{при } \chi(-1)=1\\ i\sqrt{f} & \text{при } \chi(-1)=-1\end{cases},$$

причем $\sqrt{f}$ понимается, как и выше, в смысле положительного значения корня. Точная формулировка нашей задачи заключается теперь в определении знака в равенстве $\tau(\chi)=\pm\vartheta$ при этом аналитическом нормировании обоих алгебраических чисел ζ и $\vartheta=\sqrt{\chi(-1)f}$, причем ударение стоит на выделенных курсивом словах.

По поводу самой постановки вопроса заметим еще, что кроме обычного понятия предельного перехода, основывающегося на понятии абсолютной величины, существует бесконечное множество понятий предельного перехода в поле рациональных чисел. Они все даются теорией метрик, выросшей из куммеровой

теории дивизоров и приводящей к обоснованию арифметики в произвольных полях алгебраических чисел. Для каждого из этих понятий предельного перехода на основании предшествующих рассуждений может быть поставлен совершенно аналогичный вопрос о знаке собственной квадратичной гауссовой суммы.

После этих общих предварительных замечаний мы перейдем к доказательству предложения, которое мы уже высказывали в (2) п. 3, § 18:

XI. *При аналитической нормировке* $\zeta = e^{2\pi i/f}$ *и* $\sqrt{f} > 0$ *знак собственной нормированной гауссовой суммы, соответствующей квадратичному характеру* χ *и натуральному ведущему модулю* f, *определяется из формул*

$$\tau(\chi) = \sum_{x \bmod f} \chi(x)\,\zeta^x = \begin{cases} \sqrt{f} & \text{при} \quad \chi(-1) = 1 \\ i\sqrt{f} & \text{при} \quad \chi(-1) = -1 \end{cases}.$$

Заметим, что это утверждение не зависит от различения i и $-i$, которое невозможно и аналитически, так как это нормирование входит как в нормирование ζ (а следовательно, $\tau(\chi)$), так и в нормирование $\sqrt{\chi(-1)f}$. При автоморфизме $i \to -i$ поля комплексных чисел слева $\zeta \to \zeta^{-1}$, следовательно, $\tau(\chi) \to \chi(-1)\tau(\chi)$, а правая часть ведет себя при этом совершенно аналогично.

Доказательство. 1) Мы покажем, что путем разложения на компоненты из VI, п. 2 доказательство может быть сведено к случаю, когда ведущий модуль f является степенью простого числа, т. е. равен 2^2, 2^3 или нечетному простому числу p. Для этого достаточно доказать, что если утверждение верно для нечетного ведущего модуля f, то оно верно для любого ведущего модуля F одного из трех типов:

$$F = 2^2 f, \quad 2^3 f, \quad pf,$$

причем в последнем случае p означает простое нечетное число, не делящее f. Этим трем типам расширения ведущего модуля f соответствуют три типа расширения квадратичного характера χ с ведущим модулем f до квадратичного характера с ведущим модулем F

$$\mathbf{X} = \chi_4\chi, \quad \chi_4^{\nu}\chi_8\chi, \quad \chi_p\chi,$$

причем во втором случае показатель $\nu \bmod 2$ может быть произвольным. При этом мы имеем

$$\mathbf{X}(-1) = -\chi(-1), \quad (-1)^{\nu}\chi(-1), \quad \chi_p(-1)\chi(-1),$$

и так как $\chi(-1)f = f^*$ и $\chi_p(-1)p = p^*$, то

$$\mathbf{X}(-1)F = -4f^*, \quad (-1)^{\nu}8f^*, \quad p^*f^*.$$

С одной стороны, гауссова сумма $\tau(\chi)$ отличается, согласно VI, п. 2, от произведения компонент

$$\tau(\chi_4)\,\tau(\chi),\quad \tau(\chi_4^{\nu}\chi_8)\,\tau(\chi),\quad \tau(\chi_p)\,\tau(\chi)$$

только множителем ± 1, который на основании квадратичного закона взаимности равен

$$\chi_4(f)\,\chi(4) = (-1)^{\frac{f-1}{2}},$$
$$\chi_4^{\nu}(f)\,\chi_8(f)\,\chi(8) = (-1)^{\nu\frac{f-1}{2}},$$
$$\chi_p(f)\,\chi(p) = (-1)^{\frac{p-1}{2}\frac{f-1}{2}}.$$

С другой стороны, произведения положительных или соответственно положительно-мнимых значений квадратных корней

$$\sqrt{-4}\sqrt{f^*},\ \sqrt{(-1)^{\nu}8}\sqrt{f^*},\ \sqrt{p^*}\sqrt{f^*}$$

отличается от также нормированных корней

$$\sqrt{\times(-1)F} = \sqrt{-4f^*},\ \sqrt{(-1)^{\nu}8f^*},\ \sqrt{p^*f^*}$$

тем же самым множителем. Это следует из того, что f^*, p^* положительны тогда и только тогда, когда $(f-1)/2$, $(p-1)/2 \equiv 0 \bmod 2$.

Таким образом, доказано, что наше утверждение можно переносить с f на F. Нам остается теперь доказать его для специальных характеров χ_4, $\chi_4^{\nu}\chi_8$, χ_p.

2) Для трех характеров χ_4, $\chi_4^{\nu}\chi_8$ мы имеем явные выражения:

$$\tau(\chi_4) = i - i^3 = 2i,$$
$$\tau(\chi_4^{\nu}\chi_8) = \zeta - (-1)^{\nu}\zeta^3 - \zeta^5 + (-1)^{\nu}\zeta^7 =$$
$$= 2(\zeta + (-1)^{\nu}\zeta^7) = 2(\zeta + (-1)^{\nu}\zeta^{-1}) \quad (\text{ввиду } \zeta^4 = -1)$$
$$= 2\left(\frac{\sqrt{2}+i\sqrt{2}}{2} + (-1)^{\nu}\frac{\sqrt{2}-i\sqrt{2}}{2}\right)$$
$$\left(\text{ввиду того, что } \zeta = \cos\frac{2\pi}{8} + i\sin\frac{2\pi}{8}\right)$$
$$= \begin{cases} 2\sqrt{2} & \text{при } \nu \equiv 0 \bmod 2 \\ 2i\sqrt{2} & \text{при } \nu \equiv 1 \bmod 2 \end{cases}.$$

Из этих формул следует наше утверждение для всех трех характеров.

3) Нам осталась центральная часть доказательства, а именно доказательство того, что для квадратичного характера χ по нечет-

ному простому модулю p имеет место формула

$$\tau(\chi) = \sqrt{p^*}$$

с положительным, соответственно положительно-мнимым значением для квадратного корня.

В (17) п. 5, § 18 мы нашли, что для дифференты

$$\delta = \prod_{x=1}^{m} (\zeta_2^x - \zeta_2^{-x}) \quad \text{с} \quad m = \frac{p-1}{2}, \quad \zeta_2 = \zeta^{\frac{p+1}{2}}$$

в случае $p \equiv 1 \bmod 4$, т. е. $m = 2n$, имеет место формула

$$\delta = \sqrt{p}$$

с положительным значением для квадратного корня. В случае $p \equiv -1 \bmod 4$, т. е. $m = 2n-1$, то же рассуждение дает, с одной стороны,

$$\delta^2 = -p,$$

в то время как, с другой стороны, среди $2n-1$ множителей опять чередуются положительно- и отрицательно-мнимые, так что здесь

$$\delta = (-1)^n i^{2n-1} \sqrt{p} = -\sqrt{-p}$$

является отрицательно-мнимым квадратным корнем. В обоих случаях число

$$(-1)^m \delta = \sqrt{p^*}$$

обладает как раз тем свойством, которое мы хотим доказать для $\tau(\chi)$. Ввиду этого нам достаточно доказать равенство

$$\tau(\chi) = (-1)^m \delta \quad \text{с} \quad m = \frac{p-1}{2}. \tag{2}$$

В этом совершенно элементарном сведении к алгебраической задаче и состоит аналитическая часть нашего доказательства. Теперь мы решим эту задачу, доказав арифметическим путем, что равенство (2) действительно имеет место.

Мы будем опираться на элементарную теорию делимости в поле $\mathsf{P}_p = \mathsf{P}(\zeta)$. При этом мы не будем пользоваться, как и в § 18, п. 4, при доказательстве IV тем, что область целостности $\mathsf{I}_p = \Gamma[\zeta]$ максимальна. Согласно доказанному там предложению (6), все множители произведения

$$\prod_{x \not\equiv 0 \bmod p} (1 - \zeta^x) = p$$

ассоциированы друг с другом. Так как число их $p-1$, то мы получаем, что в P_p

$$p \cong \pi^{p-1} \quad \text{с} \quad \pi = 1 - \zeta.$$

Мы не будем здесь пользоваться тем, что $\pi \cong \mathfrak{p}$ является представлением в виде главного дивизора единственного простого делителя $\mathfrak{p}$ единственного разветвляющегося в P_p простого числа $p \cong \mathfrak{p}^{p-1}$. Это следует из приведенного в § 19, п. 2 общего закона разложения для подполей поля корней из единицы, мы же привели этот факт только для того, чтобы сделать более понятным последующее доказательство. Нам нужно только знать, что для целого рационального a соотношение $\pi \mid a$ в I_p и соотношение $p \mid a$ эквивалентны, а это ясно из того, что $\pi^{p-1} \cong p$, или же может быть показано точно так же, как в IV, п. 4, § 8.

Так как мы знаем, что

$$\tau(\chi)^2 = p^* = \delta^2,$$

а следовательно, всегда $\tau(\chi) = \pm\delta$, то для доказательства (2) нам достаточно доказать сравнение

$$\tau(\chi) \equiv (-1)^m \delta \bmod \tilde{\omega} \tag{3}$$

по модулю $\tilde{\omega}$ из I_p, для которого

$$\delta \not\equiv -\delta \bmod \tilde{\omega}. \tag{4}$$

Мы докажем, что как сравнение (3), так и условие (4) выполняются для степени

$$\tilde{\omega} = \pi^{m+1}.$$

Чтобы определить вычет $\delta \bmod \pi^{m+1}$, мы определим сначала вычеты отдельных множителей $\zeta_2^x - \zeta_2^{-x}$ $(x = 1, \ldots, m)$. Ввиду того что

$$\zeta_2^x - \zeta_2^{-x} = -\zeta_2^{-x}(1 - \zeta^x) = -\zeta_2^{-x}[1 - (1-\pi)^x],$$

мы имеем

$$\zeta_2^x - \zeta_2^{-x} \equiv -\zeta_2^{-x} x\pi \equiv -x\pi \bmod \pi^2,$$

причем последнее, ввиду того что (как и для всякой степени ζ) $\zeta_2^{-x} \equiv 1 \bmod \pi$. Если мы представим себе эти сравнения записанными в виде равенств

$$\zeta_2^x - \zeta_2^{-x} = -(x + \gamma_x\pi)\ \pi \text{ с } \gamma_x \text{ из } \mathsf{I}_p$$

и все перемножим, то искомый вычет получится в виде

$$\delta \equiv (-1)^m m!\ \pi^m \bmod \pi^{m+1}. \tag{5}$$

Так как $m! \not\equiv 0 \bmod p$, а значит, ввиду сделанного замечания, и $m!\ 0 \not\equiv \bmod \pi$, то отсюда следует, что δ делится на π^m, но уже не делится на π^{m+1}. Это делает понятным наш выбор π^{m+1} в качестве модуля $\tilde{\omega}$.

Чтобы найти и вычет $\tau(\chi) \bmod \pi^{m+1}$, мы заметим, что во всяком случае

$$p \equiv 0 \bmod \pi^{2m}, \text{ т. е. заведомо} \equiv 0 \bmod \pi^{m+1},$$

так что мы можем сначала действовать по $\bmod p$, а потом по $\bmod \pi^{m+1}$.

В равенстве

$$\tau(\chi) = \sum_{x \bmod p} \chi(x) \zeta^x$$

ввиду критерия Эйлера $\chi(x) \equiv x^m \bmod p$. Поэтому заведомо

$$\tau(\chi) \equiv \sum_{x \bmod p} x^m (1-\pi)^x \bmod \pi^{m+1}.$$

Если исходить из наименьшей положительной системы представителей $x = 0, 1, \ldots p-1$, то путем раскрытия скобок и группировки получится

$$\tau(\chi) \equiv \sum_{\mu=0}^{m} \left(\sum_{x=0}^{p-1} x^m \binom{x}{\mu} \right) (-1)^\mu \pi^\mu \bmod \pi^{m+1}.$$

Добавленные нами здесь члены с $x < \mu \leqslant m$ (для $x < m$) равны нулю, так как для них

$$\binom{x}{\mu} = \frac{x(x-1)\ldots(x-(\mu-1))}{\mu!} = 0.$$

По теореме Вильсона (§ 4, п. 11), мы имеем

$$-1 \equiv (p-1)! = \prod_{x=1}^{m} x(p-x) \equiv (-1)^m (m!)^2 \bmod p,$$

т. е.

$$\frac{1}{m!} \equiv -(-1)^m m! \bmod p.$$

Ввиду этого, если мы положим

$$\frac{1}{\mu!} = \frac{g_\mu}{m!} \quad (\mu = 0, 1, \ldots m)$$

с целыми g_μ, то получим

$$\binom{x}{\mu} \equiv -(-1)^m m!\ g_\mu x(x-1)\ldots(x-(\mu-1)) \bmod p,$$

причем теперь справа стоят целочисленные многочлены μ-й степени и $g_m = 1$. Мы можем подставить эти значения для $\binom{x}{\mu} \bmod p$ в сравнение, полученное нами для $\tau(\chi) \bmod \pi^{m+1}$. Тогда

получится

$$\tau(\chi) \equiv -(-1)^m m! \sum_{\mu=0}^{m} \Big(\sum_{x \bmod p} x^m \cdot x(x-1)\dots$$

$$\dots(x-(\mu-1))\, g_\mu\, (-1)^\mu \pi^\mu\Big) \bmod \pi^{m+1}.$$

Если представить себе многочлены $(m+\mu)$-й степени во внутренней сумме развернутыми и применить формулу из § 10, п. 4 для вычета сумм $\sum_{x \bmod p} x^r \bmod p$ (для $r \geqslant 1$), то только при $\mu = m$ получится член $\not\equiv 0 \bmod p$, а именно, слагаемое, происходящее от старшего члена и дающее вычет $-1 \bmod p$. Если учесть еще, что $g_m = 1$, то искомый вычет получится в виде

$$\tau(\chi) \equiv m!\ \pi^m \bmod \pi^{m+1}. \tag{6}$$

Сопоставление результатов (5) и (6) показывает, что сравнение (3) действительно имеет место с $\omega = \pi^{m+1}$.

Легко видеть, что для $\omega = \pi^{m+1}$ выполнено также и условие (4), так как из $2\delta \equiv 0 \bmod \pi^{m+1}$ следовало бы

$$\delta \equiv (p+1)\,\delta \equiv \frac{p+1}{2}\, 2\delta \equiv 0 \bmod \pi^{m+1},$$

в то время как мы установили, что δ на π^{m+1} уже не делится.

Согласно сказанному, этим доказано равенство (2), а тем самым закончено доказательство XI.

Как мы уже отмечали, в этом методе для определения знака собственной нормированной гауссовой суммы, принадлежащем Кронекеру, роль анализа сведена к доказательству того, что среди выражений

$$\zeta_2^x - \zeta_2^{-x} = 2i \sin\Big(\frac{2\pi x}{p} \cdot \frac{p+1}{2}\Big) = 2i \sin\Big(\frac{\pi x}{p} + \pi x\Big)$$

при $x = 1, \dots, \frac{p-1}{2}$ положительно- и отрицательно-мнимые чередуются. Существуют другие доказательства, в которых, наоборот, арифметике отводится по возможности меньшая роль, а иногда она полностью вытесняется аналитическими рассуждениями. Эти доказательства не имеют уже такого элементарного характера, как только что приведенное аналитическое высказывание,—в некоторых из них применяются, например, ряды и интегралы Фурье.

В то время как мы в редукциях, составляющих первую часть нашего доказательства, использовали квадратичный закон взаимности, уже Гаусс применил эту связь для нового вывода квадратичного закона взаимности. При этом правило для знака гауссовой суммы с квадратичным характером и произвольным ведущим модулем выводится аналитическим путем.

6. Гипотеза Куммера для кубических характеров по простому модулю. Только что рассмотренный в п. 5 вопрос, касающийся гауссовых сумм $\tau(\chi)$, принадлежащих квадратичным характерам χ, в действительности не ограничивается этим частным случаем $k=2$, а имеет аналог и для гауссовых сумм $\tau(\chi)$, принадлежащих характерам χ более высокого порядка $k\geqslant 3$. Но, во-первых, уже постановка вопроса в общем случае связана с рядом трудностей арифметического характера, которых мы коротко коснемся ниже, и, во-вторых, ответа на этот вопрос до сих пор не получено даже для первого случая более высокой степени $k=3$, т. е. для кубических характеров.

Единственное, чем мы до сих пор располагаем в этом отношении, есть интересная гипотеза Куммера относительно кубических гауссовых сумм по простому модулю $p\equiv 1 \bmod 3$, которая, правда, не привлекает особенно большого внимания, хотя ее разработка была бы гораздо плодотворнее для теории чисел, чем усилия огромного количества профессионалов и дилетантов, направленные на доказательство великой теоремы Ферма (см. § 3, п. 8). Мы изложим здесь эту гипотезу в связи с уже полученными в п. 4 результатами относительно кубических гауссовых сумм, а также представим эти результаты в совершенно элементарной форме, свободной от арифметических понятий из п. 4.

Начнем с общей постановки вопроса. Пусть χ есть характер порядка $k\geqslant 3$, относительно которого мы, согласно правилу VI, п. 2 разложения на компоненты и заключительному замечанию в п. 3, можем без существенного ограничения общности предположить, что его ведущий модуль есть простое число $p\equiv 1 \bmod k$. Тогда, согласно VII, п. 3, нормированная собственная гауссова сумма

$$\tau(\chi)=\sum_{x \bmod p}\chi(x)\,\zeta^x$$

является резольвентой Лагранжа для единственного циклического подполя k-й степени

$$\mathsf{K}=\mathsf{P}(\theta)$$

поля (циклического, степени $p-1$) P_p корней из 1, причем, точнее, речь идет о резольвенте Лагранжа определенного в (3) п. 3 примитивного элемента

$$\theta=\sum_{\substack{x \bmod p\\ \chi(x)=1}}\zeta^x=\frac{1}{k}\sum_{y\not\equiv 0 \bmod p}\zeta^{y^k}$$

или нормированного p-го периода деления круга степени k. Согласно (5) п. 4, k-я степень

$$\tau(\chi)^k=\omega(\chi)=\chi(-1)\,p\prod_{x\not\equiv 0,\ -1 \bmod k}\pi(\chi,\chi^x)$$

является числом поля (более низкой степени, чем $\mathsf{P}_k\mathsf{P}_p$) P_k, причем это число не зависит от нормирования ζ, так как оно инвариантно относительно всех автоморфизмов $\zeta \to \zeta^a$ расширения $\mathsf{P}_k\mathsf{P}_p/\mathsf{P}_k$. Поэтому число $\tau(\chi) = \sqrt[k]{\omega(\chi)}$ из $\mathsf{P}_k\mathsf{P}_p$ определено точно k-значно. В силу $\tau(\chi) \to \overline{\chi}(a)\tau(\chi)$ при $\zeta \to \zeta^a$, k различным значениям корня k-й степени взаимно однозначно соответствуют различающиеся k значениями характера χ смежные классы по подгруппе степенных вычетов степени k по $\bmod p$.

Если теперь снова положить в основу аналитическое нормирование $\zeta = e^{2\pi i/p}$, то возникает вопрос, *какому из k различных корней k-й степени из $\omega(\chi)$ равно число $\tau(\chi)$*.

Этот вопрос снова имеет существенно аналитическую природу. Для его точной формулировки недостаточно знать число $\omega(\chi)$ алгебраически, т. е. как число из поля P_k; для того чтобы вообще различать корни k-й степени из $\omega(\chi)$, нужно знать это число аналитически, т. е. как комплексное число. Эта трудность не возникает в частном случае $k=2$, потому что там $\omega(\chi) = \chi(-1)\,p = \pm p^*$ рационально и тем самым тривиальным образом известно как комплексное число. Эта трудность будет преодолена, если мы дадим для $\omega(\chi)$ арифметическую характеристику того же типа, что и в п. 4 для частных случаев $k=3, 4, 6$; действительно, данные там арифметические характеристики, очевидно, определяют $\omega(\chi)$ так же как и комплексное число.

Правда, мы имеем некоторую арифметическую характеристику числа $\omega(\chi)$ для любого порядка k, именно, с одной стороны, посредством указания разложения на простые дивизоры в P_k, и, с другой стороны, посредством аналогичного (6) п. 5 свойства сравнимости; эти указания вместе с тем фактом, что $|\omega(\chi)| = \sqrt{p^h}$, определяют число $\omega(\chi)$ однозначно. Однако, вообще говоря, этим $\omega(\chi)$ не определяется как комплексное число, именно потому, что разложение на простые дивизоры в P_k в общем случае не является разложением на простые множители. Только если последнее имеет место, т. е. только если поле P_k корней из 1 имеет число классов $h=1$, можно таким способом охарактеризовать $\omega(\chi)$ как комплексное число и тем самым внести точность в сформулированную выше постановку вопроса. Для частных случаев

$$k=3, 4, 6 \text{ с } \mathsf{P}_3 = \mathsf{P}_6 = \mathsf{P}(\sqrt{-3}), \quad \text{соответственно} \quad \mathsf{P}_4 = \mathsf{P}(\sqrt{-1})$$

это имеет место.

Обратимся теперь к рассматривавшемуся Куммером кубическому случаю $k=3$; относительно случаев $k=6$ и $k=4$ мы будем говорить в заключение, в п. 7.

Согласно (10б), (11б$_2$) п. 4, мы имеем в кубическом случае арифметическую характеристику

$$\tau(\chi)^3 = p\pi, \quad \tau(\overline{\chi})^3 = p\overline{\pi}$$

с

$$\left\{ \begin{array}{l} \pi, \overline{\pi} = \dfrac{a \pm 3b\sqrt{-3}}{2}; \quad a \equiv 1 \bmod 3 \\ p = \dfrac{a^2 + 27b^2}{4} \end{array} \right\}. \tag{1}$$

Вместо арифметического различия между обоими сопряженными π, $\overline{\pi}$, которое здесь можно установить аналогично тому, как в (29) п. 5, § 18 для биквадратичного случая, нам будет нужно для рассматриваемого здесь вопроса аналитическое различие, определяемое условием

$$\pi \text{ положительно-мнимо, т. е. } b > 0. \tag{2}$$

Достаточно рассматривать одну гауссову сумму $\tau(\chi)$, соответствующую числу π, так как вторая сумма $\tau(\overline{\chi})$ будет комплексно сопряженной с первой. Аналогично тому как в (28) п. 5, § 18 для биквадратичного случая, можно показать и здесь, что это сопоставление характера χ, а вместе с ним и суммы $\tau(\chi)$ числу π определяется обобщенным критерием Эйлера

$$\chi(x) \equiv x^{\frac{p-1}{3}} \bmod \pi. \tag{3}$$

В силу всего сказанного, мы можем точно сформулировать наш вопрос следующим образом:

Пусть дано простое число $p \equiv 1 \bmod 3$, *пусть* (1) *есть его нормированное разложение на простые множители в* P_3 *и пусть* χ*—кубический характер по* $\bmod p$, *соответствующий по* (3) *простому сомножителю* π, *нормированному согласно* (2).

Какое из трех комплексных чисел $\sqrt[3]{p\pi}$ *равно тогда нормированной гауссовой сумме* $\tau(\chi)$?

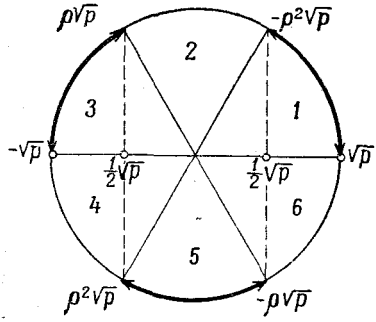
При нормировании (2) три кубических корня $\sqrt[3]{p\pi}$ лежат в 1-м, 3-м, 5-м секстантах комплексной числовой плоскости, причем вследствие $|\pi| = \sqrt{p}$ —на окружности радиуса $\sqrt{p}$ с центром в 0 и вследствие того, что π не вещественно,—внутри отмеченных на фиг. 27 дуг. Таким образом, наш вопрос приводит к разбиению всех простых чисел $p \equiv 1 \bmod 3$ на три класса p_1, p_2, p_3 в зависимости от того, лежит ли соответствующая числу нормированная гауссова сумма

$\tau(\chi)$ в 1-м, 3-м, 5-м секстанте

комплексной числовой плоскости.

Возникает вопрос, существует ли арифметический закон, по которому для данного простого числа $p \equiv 1 \bmod 3$ можно было бы решить, к какому из трех классов p_1, p_3, p_5 оно принадлежит, и если существует, то как его получить. Ответ на этот вопрос до сих пор не известен.

Заметим для предупреждения неправильного понимания и пояснения положения вещей, что три класса p_1, p_3, p_5 в кубическом случае не являются аналогом фигурирующих в квадратичном случае двух типов $p \equiv \pm 1 \bmod 4$ $(p^* \lesseqgtr 0)$. В квадратичном случае дело обстоит следующим образом. Для каждого типа из $\tau(\chi)^2 = p^*$ следует, что $\tau(\chi)$ есть один из двух квадратных корней $\sqrt{p^*}$. Две соответствующие точки на круге радиуса $\sqrt{p}$ с центром в 0 являются здесь аналогом для трех секторов в кубическом случае. Относительно определения знака можно поэтому сказать, что все нечетные простые числа p (вне всякой связи с их типом $p \equiv \pm 1 \bmod 4$) разбиваются на два класса p_1, p_3 в зависимости от того, является ли $\tau(\chi)$ правой, верхней или левой, нижней точкой, или, другими словами, в зависимости от того, лежит ли $\tau(\chi)$ в 1-м или в 3-м квадранте (включая границу!) комплексной числовой плоскости. Вопрос о нахождении закона этого распределения по классам решается здесь посредством определения знака в XI, п. 5. Этот закон гласит, что все нечетные простые числа p принадлежат классу p_1, в то время как класс p_3 пуст.



Фиг. 27.

По аналогии с этим положением в квадратичном случае естественно ожидать, что и в кубическом случае все простые числа $p \equiv 1 \bmod 3$ принадлежат одному и тому же из указанных трех классов p_1, p_3, p_5; тем более неожиданным является поэтому действительное положение дела, которое Куммер установил проверкой 45 конкретных простых чисел $p \equiv 1 \bmod 3$ с $p < 500$. Он нашел

24 простых числа $p_1 =$ 7, 31, 43, 67, 73, 79, 103, 127, 163, 181, 223, 229, 271, 277, 307, 313, 337, 349, 409, 421, 439, 457, 463, 499.

14 простых чисел $p_5 =$ 13, 19, 37, 61, 109, 157, 193, 241, 283, 367, 373, 379, 397, 487.

7 простых чисел $p_3 =$ 97, 139, 151, 199, 211, 331, 433.

Так как отношение 24 : 14 : 7 количеств чисел в каждом из трех

классов приблизительно равно 3 : 2 : 1, Куммер высказал на основании этого, впрочем, недостаточно обширного, конкретного материала следующую гипотезу:

Гипотеза Куммера. *В каждом из трех классов* p_1, p_5, p_3 *существует бесконечно много простых чисел, причем эти три класса имеют соответственно плотности* 1/2, 1/3, 1/6.

Относительно понятия плотности мы отсылаем к нашим рассмотрениям в § 14, п. 4.

Эта гипотеза также до сих пор не доказана и не опровергнута. Конечно, доказательство этой гипотезы еще не дало бы ответа на поставленный выше вопрос об арифметическом законе для распределения по классам p_1, p_3, p_5, но все же сделало бы существование такого закона более вероятным; точно так же и опровержение этой гипотезы еще не исключило бы возможности того, что такой закон все же существует.

Доказательство гипотезы Куммера приобретает особое значение в связи со следующим фактом, который мы можем здесь только сообщить без доказательства. Если закон разложения известен до сих пор только в абсолютно-абелевом случае (см. § 19, п. 2) и еще для тех полей K, которые можно вложить в поле, получающееся из P последовательными относительно-абелевыми расширениями, то мы тем не менее знаем, что всегда множества простых чисел, имеющих один из конечного количества возможных неразветвленных типов разложения, бесконечны и имеют определенные плотности, которые можно найти из теоретико-групповых соображений. На этом основании можно прийти к мысли, что куммеровское распределение по классам отражает закон разложения в некотором поле алгебраических чисел. И действительно, существуют поля, у которых множества простых чисел с различным типом разложения имеют как раз плотности 1/2, 1/3, 1/6; это суть как раз все неабелевы кубические поля, которые характеризуются среди всех вообще кубических полей тем, что их дискриминанты D не являются квадратами. Они могут быть вложены в поля, являющиеся результатом двух последовательных относительно-абелевых расширений; первое из этих расширений есть квадратичное поле $\mathsf{P}(\sqrt{D})$, а второе—нормальное поле, являющееся кубическим относительно-циклическим расширением поля $\mathsf{P}(\sqrt{D})$. Таким образом, закон разложения в указанных кубических неабелевых полях известен. Существует три неразветвленных типа разложения, именно, $p \cong \mathfrak{p}\cdot\mathfrak{p}'\mathfrak{p}''$ (степени равны 1), $p \cong \mathfrak{p}$ (степень равна 3),

$$p \cong \mathfrak{p}\mathfrak{p}' \text{ (степени равны 1, 2),}$$

где в скобках указаны показатели степени числа p в выражении для нормы простых дивизоров. Эти p имеют (в указанной последовательности) плотности 1/6, 1/3, 1/2; при этом последним из

названных типов разложения, с плотностью 1/2, обладают простые числа p с $\left(\frac{D}{p}\right) = -1$. Если куммеровское распределение по классам отражает закон разложения в некотором неабелевом кубическом поле K, то так как при этом идет речь только о распределении простых чисел вида $p \equiv 1 \bmod 3$, то во всяком случае это не может быть поле, дискриминант которого D имеет свободное от квадратов ядро—3, так как в этом случае тип разложения с плотностью 1/2 состоит из всех простых чисел вида $p \equiv -1 \bmod 3$. Но этим исключаются все поля, которые могут быть порождены корнем двучленного кубического многочлена, т. е. поля $\mathsf{K} = \mathsf{P}(\sqrt[3]{a})$ (a—рациональное, не являющееся кубом), в том числе и единственное поле, дискриминант которого содержит только простое число 3, именно поле $\mathsf{K} = \mathsf{P}(\sqrt[3]{3})$. Поэтому речь может идти только о кубических полях K, у которых в дискриминант D входят отличные от 3 простые числа q. Однако это маловероятно по двум причинам. Во-первых, те из этих простых чисел q, которые $\equiv 1 \bmod 3$, охватывались бы тогда куммеровским распределением по классам, но не охватывались бы законом разложения; в случае же, если бы для всех этих простых чисел имело бы место $q \equiv -1 \bmod 3$, они должны были бы входить уже в дискриминант d квадратичного поля $\mathsf{P}(\sqrt{D}) = \mathsf{P}(\sqrt{d})$. И кроме того, при чисто кубической структуре куммеровского распределения по классам было бы в высшей степени странным то, что некоторые простые числа q играют особую роль как делители дискриминанта соответствующего кубического поля K, причем это возражение весьма существенно в любом случае; можно было бы тотчас же спросить, какие это могут быть числа, и нельзя найти никаких оснований, почему, например, простое число $q = 23$ (ср. конец § 17, п. 5) или $q = 4027$ должно играть особую роль для куммеровского распределения по классам.

Но если и маловероятно, что куммеровское распределение по классам отражает некоторый закон разложения, то при сегодняшнем состоянии теории простых чисел во всяком случае было бы интересно знать нетривиальные (т. е. не состоящие из взаимно простых с модулем классов вычетов) множества простых чисел, имеющие определенную плотность. Поэтому решение гипотезы Куммера заведомо является благодарной, имеющей большое значение задачей. Это решение, видимо, не должно быть таким трудным, как для вопросов относительно простых чисел, поставленных в II, III, п. 8, § 3, которые имеют трансцендентную природу в сравнении с базирующимся на алгебраически-теоретико-числовой основе вопросом о гипотезе Куммера.

Возможно, что подход к решению этой задачи можно найти в обобщении распределения по классам для простых чисел

$p \equiv 1 \bmod 3$ на распределение всех не делящихся на 3 ведущих модулей f кубических характеров χ, т. е. на распределение всех произведений различных простых чисел такого вида. Для такого ведущего модуля $f = p_1 \dots p_n$ с n различными простыми сомножителями $p_\nu \equiv 1 \bmod 3$, согласно § 13, п. 6, существует всего 2^{n-1} пар комплексно сопряженных кубических характеров χ_ν, $\bar{\chi}_\nu$, которые соответствуют 2^{n-1} различным разложениям $f = (a_\nu^2 + 27 b_\nu^2)/4$ с $a_\nu \equiv 1 \bmod 3$, $b_\nu > 0$. Таким образом, дело касается распределения по классам не самих ведущих модулей f, а пар f, a_ν в зависимости от того, в каком секторе круга радиуса $\sqrt{f}$ с центром в 0 лежит соответствующая нормированная гауссова сумма $\tau(\chi_\nu)$. Если для такого распределения по классам существует арифметический закон, то его, вероятно, получить легче, чем при изолированном рассмотрении простых ведущих модулей $f = p$, подобно тому как тот факт, что все числа из одного класса вычетов по $\bmod m$, взаимно простых с модулем, имеют плотность $1/\varphi(m)$ (см. § 4, п. 8), доказывается легче (даже тривиально!), чем при ограничении только простыми числами (см. § 14, п. 4). То же самое можно сказать и об обобщении гипотезы Куммера на биквадратичный случай, который мы рассмотрим в п. 7. Арифметические сведения относительно циклических кубических и биквадратичных полей, необходимые для этого расширенного распределения по классам, я подробно изложил в моем недавно появившемся сочинении, примыкающем к монографии [1]. При этом целесообразно было бы начинать с исследования достаточно большого количества конкретных ведущих модулей f, чтобы составить себе представление о том, какого результата следует ожидать.

Теперь мы дадим более элементарное описание куммеровского распределения по классам. Именно, оказывается, что для его определения достаточно нормированного разложения (1) числа p в поле P_3 только в его рациональной форме, т. е. можно обойтись без нормирующих условий (2) и (3), касающихся алгебраического числа π и алгебраического значения характера χ.

Очевидно (см. выше, фиг. 27), что три класса p_1, p_3, p_5 различаются уже тем, что для них удвоенная вещественная часть

$$\eta = \tau(\chi) + \tau(\bar{\chi}) \tag{4}$$

лежит в открытых интервалах

$$\underset{(\text{класс } p_3)}{-2\sqrt{p} \dots -\sqrt{p}} \quad \underset{(\text{класс } p_5)}{-\sqrt{p} \dots \sqrt{p}} \quad \underset{(\text{класс } p_1)}{\sqrt{p} \dots 2\sqrt{p}}. \tag{5}$$

Здесь различие между сопряженными χ, $\bar{\chi}$ и π, $\bar{\pi}$ уже не играет роли. Это различие в виде нормирующих условий (2), (3) впервые становится необходимым тогда, когда мы хотим получить

из распределения по классам ответ на исходный вопрос относительно отдельных значений $\tau(\chi)$, $\tau(\bar{\chi})$, в то время как сумма η этих значений определяется только числами p, a из (1), что мы теперь увидели явно.

Число η связано с примитивным элементом θ того циклического кубического подполя K поля P_p, для которого $\tau(\chi)$ является резольвентой Лагранжа, соотношением

$$\theta = \frac{1}{3}(-1+\tau(\chi)+\tau(\bar{\chi})) = \frac{\eta-1}{3},$$

выполняющимся согласно (7) п. 3; поэтому η тоже есть примитивный элемент поля K. Сопряженные с θ числа, являющиеся p-ми периодами деления круга степени 3, представляются через нормированный первообразный p-й корень ζ из 1 следующим образом:

$$\left\{\begin{array}{l} \theta = \sum\limits_{\substack{x \bmod p \\ \chi(x)=1}} \zeta^x = \frac{1}{3} \sum\limits_{y \not\equiv 0 \bmod p} \zeta^{y^3} \\ \theta' = \sum\limits_{\substack{x' \bmod p \\ \chi(x')=\rho}} \zeta^{x'} = \sum\limits_{\substack{x \bmod p \\ \chi(x)=1}} \zeta^{rx} = \frac{1}{3} \sum\limits_{y \not\equiv 0 \bmod p} \zeta^{ry^3} \\ \theta'' = \sum\limits_{\substack{x'' \bmod p \\ \chi(x'')=\rho^2}} \zeta^{x''} = \sum\limits_{\substack{x \bmod p \\ \chi(x)=1}} \zeta^{r^2x} = \frac{1}{3} \sum\limits_{y \not\equiv 0 \bmod p} \zeta^{r^2y^3} \end{array}\right\}, \qquad (6)$$

где r есть кубический невычет по mod p с $\chi(r)=\rho=(-1+\sqrt{-3})/2$. Тогда числа, сопряженные с η, мы получим, прибавляя при суммировании по y еще член 1 с $y \equiv 0 \bmod p$:

$$\eta = \sum_{y \bmod p} \zeta^{y^3}, \quad \eta' = \sum_{y \bmod p} \zeta^{ry^3}, \quad \eta'' = \sum_{y \bmod p} \zeta^{r^2y^3}. \qquad (7)$$

Системы линейных уравнений (4), (7) из п. 3 имеют здесь вид:

$$\left\{\begin{array}{l} -1 = \theta + \theta' + \theta'' \\ \tau(\chi) = \theta + \rho\theta' + \rho^2\theta'' \\ \tau(\bar{\chi}) = \theta + \rho^2\theta' + \rho\theta'' \end{array}\right\}, \quad \left\{\begin{array}{l} 0 = \eta + \eta' + \eta'' \\ \tau(\chi) = \frac{1}{3}(\eta + \rho\eta' + \rho^2\eta'') \\ \tau(\bar{\chi}) = \frac{1}{3}(\eta + \rho^2\eta' + \rho\eta'') \end{array}\right\}$$

и

$$\left\{\begin{array}{l} \theta = \frac{1}{3}(-1 + \tau(\chi) + \tau(\bar{\chi}) \\ \theta' = \frac{1}{3}(-1 + \rho^2\tau(\chi) + \rho\tau(\bar{\chi}) \\ \theta'' = \frac{1}{3}(-1 + \rho\tau(\chi) + \rho^2\tau(\bar{\chi}) \end{array}\right\}, \quad \left\{\begin{array}{l} \eta = \tau(\chi) + \tau(\bar{\chi}) \\ \eta' = \rho^2\tau(\chi) + \rho\tau(\bar{\chi}) \\ \eta'' = \rho\tau(\chi) + \rho^2\tau(\bar{\chi}) \end{array}\right\}.$$

Если в последние уравнения подставить вместо $\tau(\chi)$ и $\tau(\bar{\chi})$ правильным образом нормированный $\sqrt[3]{p\pi}$ и комплексно сопряженный с ним $\sqrt[3]{\bar{p}\bar{\pi}}$, то у нас получатся формулы Кардана для решения циклических кубических уравнений, которым удовлетворяют θ, η. Второй коэффициент уравнения для η равен 0; это уравнение получается из уравнения для θ, в котором второй коэффициент равен -1, посредством обычной редукции.

Посредством вычисления двух других основных симметрических функций от η, η', η'', эти уравнения можно получить в явном виде. Мы имеем

$$\eta\eta'\eta'' = \tau(\chi)^3 + \tau(\bar{\chi})^3 = p\pi + \bar{p}\bar{\pi} = pa,$$

$$\eta\eta' + \eta\eta'' + \eta'\eta'' = -3\tau(\chi)\,\tau(\bar{\chi}) = -3p.$$

Поэтому уравнение для η получается следующее:

$$\eta^3 - 3p\eta - ap = 0. \tag{8}$$

Оно действительно определяется только числами p, a из (1). Его дискриминант равен

$$\frac{4p^3 - a^2p^2}{27} = b^2p^2.$$

В качестве уравнения для θ получается

$$\theta^3 + \theta^2 - \frac{p-1}{3}\theta - \frac{ap+3p-1}{27} = 0.$$

То, что последний коэффициент здесь также является целым, следует из соотношения (1) между p и a. С помощью этих уравнений мы явным образом выражаем, как порождается циклическое кубическое подполе $\mathsf{K} = \mathsf{P}(\theta) = \mathsf{P}(\eta)$ поля P_p.

Возвращаясь к нашему первоначальному вопросу, мы можем теперь сказать, что три корня η, η', η'' алгебраического кубического уравнения (8) лежат в трех интервалах (5), так как они соответствуют трем различным нормированиям корня $\sqrt[3]{p\pi}$, как удвоенные вещественные части. Тогда возникает вопрос, к какому из этих интервалов принадлежит аналитически нормированный посредством (4) корень η уравнения (8). Согласно (7), это аналитическое нормирование (4) может быть записано в виде

$$\eta = \sum_{y \bmod p} \zeta^{y^3} = 1 + 2 \sum_{\pm y \bmod p} \cos\frac{2\pi y^3}{p}$$

или, согласно (6), также в виде

$$\eta = 1 + 3 \sum_{\substack{x \bmod p \\ \chi(x)=1}} \zeta^x = 1 + 6 \sum_{\substack{\pm x \bmod p \\ \chi(x)=1}} \cos\frac{2\pi x}{p}.$$

Последняя форма наиболее удобна для ответа на этот вопрос в конкретных случаях.

Примеры. $p=7$. Абсолютно наименьшими кубическими вычетами являются $\pm 1 \bmod 7$. Поэтому

$$\eta = 1 + 6\cos\frac{2\pi}{7}.$$

С помощью простой оценки

$$\eta > 1 + 6\cos\frac{2\pi}{6} = 1 + 3 = 4 > \sqrt{7}$$

здесь можно без использования таблиц установить, что η принадлежит интервалу $\sqrt{7} \ldots 2\sqrt{7}$, т. е. 7 принадлежит классу p_1.

$p=13$. Абсолютно наименьшие кубические вычеты суть ± 1, $\pm 5 \bmod 13$. Поэтому

$$\eta = 1 + 6\cos\frac{2\pi}{13} + 6\cos\frac{10\pi}{13}.$$

Здесь оценки

$$\eta < 1 + 6\cos 0 + 6\cos\frac{3\pi}{4} = 1 + 6 - 3\sqrt{2} = 7 - 3\sqrt{2} < \sqrt{13},$$

$$\eta > 1 + 6\cos\frac{2\pi}{12} + 6\cos\frac{10\pi}{12} = 1 > -\sqrt{13}$$

показывают, что η лежит в интервале $-\sqrt{13} \ldots \sqrt{13}$, и потому 13 принадлежит классу p_5.

7. **Аналог для бикубических и биквадратичных характеров.** Бикубический случай может быть сведен к кубическому случаю, как это уже делалось в п. 4. Сейчас мы используем для этой цели основную формулу из VIII для фактор-системы гауссовых сумм; это значительно проще, чем опираться на более глубокую формулу (7) из IX, как мы делали в п. 4 перед (10в).

В обозначениях из п. 4 мы, согласно VIII п. 4, имеем

$$\tau(\chi\psi) = \frac{\tau(\chi)\,\tau(\psi)}{\pi(\chi,\psi)} = \chi(2)\frac{\tau(\chi)\,\tau(\psi)}{\pi}.$$

С помощью этого соотношения нормирование для 6-го корня из

$$\tau(\chi\psi)^6 = p^{*2}\bar{}^4$$

сводится к описанному в п. 6 нормированию для 3-го корня из $\tau(\chi)^3 = p\pi$ и произведенному в п. 5 определению знака квадратного корня из $\tau(\psi)^2 = p^*$:

$$\tau(\chi\psi) = \sqrt[6]{p^{*3}\bar{\pi}^4} = \chi(2)\frac{\sqrt[3]{p\pi}\,\sqrt{p^*}}{\pi}. \qquad (1)$$

Исследуемый корень $\sqrt[6]{p^*\bar{\pi}^4}$ имеет шесть значений, которые можно характеризовать тем, к какому из шести секстантов круга радиуса $\sqrt{p}$ с центром в 0 они принадлежат, но нельзя характеризовать посредством следующих через одну двенадцатых долей круга, потому что положительно-мнимое нормирование числа π не накладывает ограничения на расположение самого числа $p^*\bar{\pi}^4$ на комплексной плоскости. Если, однако, отсчитывать эти секстанты не от вещественной положительной оси, а от луча, проходящего через $\chi(2)\sqrt{p^*}/\pi$, то в соответствии с тремя классами p_1, p_3, p_5 простых чисел $p \mid \equiv 1 \bmod 3$, согласно (1), будут фигурировать только 1-й, 3-й, 5-й секстанты. Таким образом, разбиения каждого из трех классов на два полукласса, чего мы могли ожидать, в действительности не происходит. Поэтому бикубический случай не вносит ничего существенно нового.

В биквадратичном случае, к рассмотрению которого мы теперь переходим, напротив, имеет место аналог куммеровского распределения по классам, которое здесь переплетается с аналогичным квадратичному случаю распределением по типам. В связи с исследованиями относительно биквадратичного случая в п. 4 и на основании того, что мы уже имеем образец в виде кубического случая из п. 6, мы можем сейчас быть краткими.

Для простого числа $p \equiv 1 \bmod 4$, согласно (10а) п. 4, нам нужно получить нормирование корня четвертой степени из

$$\tau(\chi)^4 = p\pi^2, \quad \tau(\bar{\chi})^4 = p\bar{\pi}^2. \tag{2}$$

При этом арифметическое нормирование (11а) п. 4 чисел π, $\bar{\pi}$ можно заменить аналитическим нормированием

$$\left\{ \begin{array}{l} \pi,\ \bar{\pi} = a \pm 2bi \ \text{ с } \ a > 0,\ b > 0 \\ p = a^2 + 4b^2 \end{array} \right\}, \tag{3}$$

что не отражается на нашей постановке вопроса; таким образом, π нужно выбирать в первом квадранте комплексной плоскости, знак же числа π, согласно (2), действительно не имеет значения. Под χ мы тогда будем понимать биквадратичный характер по $\bmod p$, соответствующий этому простому сомножителю π числа p в P_4 на основании обобщенного критерия Эйлера

$$\chi(x) \equiv x^{\frac{p-1}{4}} \bmod \pi. \tag{4}$$

В отличие от кубического случая, $\tau(\chi)$ и $\tau(\bar{\chi})$ здесь не всегда комплексно сопряжены между собой, именно, имеет место

$$\tau(\bar{\chi}) = \chi(-1)\,\overline{\tau(\chi)}$$

с

$$\chi(-1) = (-1)^{\frac{p-1}{4}} = \left\{ \begin{array}{ll} 1 & \text{для } p \equiv 1 \bmod 8 \\ -1 & \text{для } p \equiv 5 \bmod 8 \end{array} \right\}.$$

Эта альтернатива определяет распределение рассматриваемых простых чисел $p \equiv 1 \bmod 4$ на два типа.

При нормировании (3) подкоренное выражение $p\pi^2$ положительно-мнимо. Поэтому простые числа $p \equiv 1 \bmod 4$ каждого из обоих типов разбиваются на

четыре класса p_1, p_3, p_5, p_7

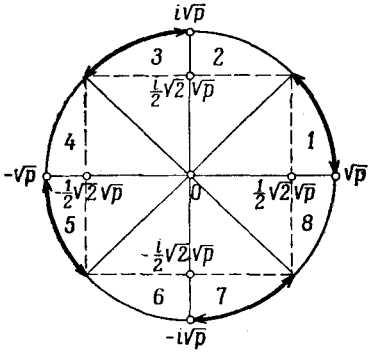
в зависимости от того, лежит ли соответствующая указанным образом числу π нормированная гауссова сумма $\tau(\chi)$ в 1-м, 3-м, 5-м, 7-м октанте комплексной плоскости (фиг. 28). Если положить

$$\tau(\chi) \quad \rho + i\sigma, \quad \overline{\tau(\chi)} = \rho - i\sigma,$$

откуда

$$\rho = \frac{1}{2}(\tau(\chi) + \chi(-1)\,\tau(\overline{\chi})),$$

$$\sigma = \frac{1}{2i}(\tau(\chi) - \chi(-1)\,\tau(\overline{\chi})), \qquad (5)$$



Фиг. 28.

то это распределение, очевидно, будет определяться также и тем, к какому из четырех (открытых) интервалов

$$-\sqrt{p} \ldots -\frac{1}{2}\sqrt{2}\sqrt{p} \quad (\text{класс } p_5) \qquad -\frac{1}{2}\sqrt{2}\sqrt{p} \ldots 0 \quad (\text{класс } p_3)$$

$$0 \ldots \frac{1}{2}\sqrt{2}\sqrt{p} \quad (\text{класс } p_7) \qquad \frac{1}{2}\sqrt{2}\sqrt{p} \ldots \sqrt{p} \quad (\text{класс } p_1)$$

принадлежит вещественная часть

$$\rho = \frac{1}{2}(\tau(\chi) + \tau(\overline{\chi})) \text{ для } p \equiv 1 \bmod 8,$$

соответственно, к какому из четырех (открытых) интервалов

$$-\sqrt{p} \ldots -\frac{1}{2}\sqrt{2}\sqrt{p} \quad (\text{класс } p_7) \qquad -\frac{1}{2}\sqrt{2}\sqrt{p} \ldots 0 \quad (\text{класс } p_5)$$

$$0 \ldots \frac{1}{2}\sqrt{2}\sqrt{p} \quad (\text{класс } p_1) \qquad \frac{1}{2}\sqrt{2}\sqrt{p} \ldots \sqrt{p} \quad (\text{класс } p_3)$$

принадлежит мнимая часть

$$\sigma = \frac{1}{2i}(\tau(\chi) + \tau(\overline{\chi})) \text{ для } p \equiv 5 \bmod 8.$$

Как мы увидим, это сведение к сумме

$$\eta = \tau(\chi) + \tau(\bar{\chi}) = \begin{cases} 2\rho & \text{для } p \equiv 1 \bmod 8 \\ 2i\sigma & \text{для } p \equiv 5 \bmod 8 \end{cases}$$

оказывается целесообразным для практического исследования этого распределения в конкретных случаях.

Снова возникает вопрос о том, существует ли арифметический закон, определяющий однозначно установленное посредством (2), (3), (4) распределение всех простых чисел $p \equiv 1 \bmod 4$ каждого из двух типов $p \equiv 1,5 \bmod 8$ по четырем классам p_1, p_3, p_5, p_7, и если такой закон существует, то как его получить. Ответ на этот вопрос тоже до сих пор не известен.

Что касается алгебраического значения числа η, то η, как, согласно (7) п. 3, и число

$$\vartheta = \frac{1}{4}(-1 + \sqrt{p} + \tau(\chi) + \tau(\bar{\chi})) = \frac{1}{4}(-1 + \sqrt{p} + \eta),$$

является примитивным элементом (единственного) циклического биквадратичного подполя K поля P_p, причем квадратичное подполе поля K обязательно изоморфно $\mathsf{P}(\sqrt{p})$.

Согласно соотношениям, положенным в основу (10а) п. 4, мы имеем

$$\eta^2 = \tau(\chi)^2 + \tau(\bar{\chi})^2 + 2\tau(\chi)\tau(\bar{\chi}) =$$
$$= -\sqrt{p}(\pi^* + \bar{\pi}^*) + 2\chi(-1)p = -2a^* + \sqrt{p} + 2\chi(-1)p,$$

где, в соответствии с нормированием (11а) п. 4, $a^* = (-1)^{(a-1)/2}a$ и π^*, $\bar{\pi}^* = (-1)^{(a-1)/2}(a \pm 2bi)$. Поэтому η удовлетворяет двучленному квадратному уравнению над подполем $\mathsf{P}(\sqrt{p})$ поля K. Отсюда, согласно (5), для вещественной части ρ и мнимой части σ числа $\tau(\chi)$ для обоих типов получаются двучленные квадратные уравнения над $\mathsf{P}(\sqrt{p})$:

$$\rho^2 = \sqrt{p}\,\frac{-a^* + \sqrt{p}}{2} \quad \text{для } p \equiv 1 \bmod 8,$$

$$\sigma^2 = \sqrt{p}\,\frac{a^* + \sqrt{p}}{2} \quad \text{для } p \equiv 5 \bmod 8,$$

правые части которых оба раза имеют норму b^2p. Эти уравнения определяют в явном виде, как порождается циклическое биквадратичное подполе $\mathsf{K} = \mathsf{P}(\vartheta) = \mathsf{P}(\eta)$ $\mathsf{P}(\rho)$, соответственно $\mathsf{P}(i\sigma)$ поля P_p.

Аналитически число η представляется в форме

$$\eta = 2 \sum_{\substack{x \bmod p \\ \psi(x)=1}} \chi(x)\zeta^x,$$

где $\psi = \chi^2 = \bar{\chi}^2$ снова обозначает квадратичный характер по mod p; действительно, для $\psi(x) = 1$ имеет место $\chi(x) + \bar{\chi}(x) = 2\chi(x)$ и для $\psi(x) = -1$ $-\chi(x) + \bar{\chi}(x) = 0$. Отсюда, согласно (5), для вещественной части ρ, соответственно мнимой части σ числа $\tau(\chi)$ получаются представления

$$\rho = 2 \sum_{\substack{\pm x \bmod p \\ \psi(x)=1}} \chi(x) \cos \frac{2\pi x}{p} \quad \text{для } p \equiv 1 \bmod 8,$$

$$\sigma = 2 \sum_{\substack{\pm x \bmod p \\ \psi(x)=1}} \chi(x) \sin \frac{2\pi x}{p} \quad \text{для } p \equiv 5 \bmod 8.$$

Примеры. $p = 5$. Абсолютно наименьшими квадратичными вычетами являются $\pm 1 \bmod 5$ и $\chi(1) = 1$. Поэтому

$$\sigma = 2 \sin \frac{2\pi}{5}.$$

Посредством простой оценки

$$\sigma = 2 \sin \frac{2\pi}{5} > 2 \sin \frac{2\pi}{6} = \sqrt{3} > \frac{1}{2} \sqrt{2} \sqrt{5}$$

мы, не прибегая к таблицам, убеждаемся в том, что σ лежит в интервале $\frac{1}{2}\sqrt{2} \ldots \sqrt{5}$, т. е. число 5 принадлежит классу p_3.

$p = 17$. Абсолютно наименьшими квадратичными вычетами являются

$$\pm 1, \ \pm 2, \ \pm 4, \ \pm 8 \bmod 17$$

и

$$\chi(1) = 1, \ \chi(2) = -1, \ \chi(4) = 1, \ \chi(8) = -1.$$

Поэтому

$$\rho = 2 \left[\cos \frac{2\pi}{17} - \cos \frac{4\pi}{17} + \cos \frac{8\pi}{17} - \cos \frac{16\pi}{17} \right].$$

Произведя вычисления, мы найдем, что ρ лежит в интервале $0 \ldots \frac{1}{2}\sqrt{2} \sqrt{17}$, т. е. число 17 принадлежит классу p_7.

По моему предложению, Калуза на основании этих формул исследовал распределение по классам p_1, p_3, p_5, p_7 для 37-ми простых чисел $p \equiv 1 \bmod 8$ и 43-х простых чисел $p \equiv 5 \bmod 8$ с $p < 1000$. Результат этого исследования приводится в нижеследующей таблице.

Класс и тип	Простые числа	Количество	
$p_1 \equiv 1 \bmod 8$	73, 113, 193, 409, 449, 521, 593, 673, 937, 977	10	21
$p_1 \equiv 5 \bmod 8$	13, 109, 149, 229, 373, 397, 557, 797, 829, 853, 997	11	
$p_3 \equiv 1 \bmod 8$	41, 97, 233, 281, 433, 809, 881, 953	8	23
$p_3 \equiv 5 \bmod 8$	5, 37, 61, 181, 197, 269, 293, 389, 541, 613, 653, 661, 677, 757, 877	15	
$p_5 \equiv 1 \bmod 8$	137, 241, 617, 761, 929	5	12
$p_5 \equiv 5 \bmod 8$	53, 157, 317, 421, 461, 709, 733	7	
$p_7 \equiv 1 \bmod 8$	17, 89, 257, 313, 337, 353, 401, 457, 569, 577, 601, 641, 769, 857	14	24
$p_7 \equiv 5 \bmod 8$	29, 101, 173, 277, 349, 509, 701, 773, 821, 941	10	
$p \equiv 1 \bmod 8$		37	80
$p \equiv 5 \bmod 8$		43	

Этот конкретный материал вдвое обширнее куммеровского. Тем не менее было бы рискованно из того факта, что отношение количеств простых чисел обоих типов в различных классах (а с меньшей точностью и для каждого типа в отдельности) приблизительно есть $2:2:1:2$, делать определенное предположение относительно плотностей, тем более, что, если бы отношение плотностей было таким же, в качестве общего наименьшего знаменателя плотностей фигурировало бы чуждое биквадратичному случаю число 7. Но во всяком случае мне представляется вероятным следующий

Аналог гипотезы Куммера. *Для каждого из двух типов* $p \equiv 1,5 \bmod 8$ *в каждом из четырех классов* p_1, p_3, p_5, p_7 *существует бесконечно много простых чисел этого типа, причем плотности одних и тех же классов для обоих типов совпадают.*

ЛИТЕРАТУРА

Бахман (P. Bachmann)

[1] Das Fermatproblem in seiner bisherigen Entwicklung. Berlin—Leipzig, 1919.

Бергстрём (H. Bergström)

[1] Die Klassenzahlformel für reelle quadratische Zahikörper mit zusammengesetzer Diskriminante als Produkt verallgemeinerter Gaußscher Summen.—J. f. Math., **186** (1945), 91—115.

Бильгард (H. Bilharz)

[1] Primdivisoren mit vorgegebener Primitivwurzel. Math. Ann., **114** (1937), 476—492.

Вейль (A. Weil)

[1] Sur les courbes algébriques et les variétés qui s'en déduisent. Actual. Scientif. Industr., № 1041, Paris, 1948.

Венков Б. А.

[1] Über die Klassenanzahl positiver binärer quadratischer Formen. Math. Ztschr., **33** (1931), 350—374.

Гекке (E. Hecke)

[1] Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. Math. Ztschr., **1** (1918), 357—376; **6** (1920), 11—51.

Давенпорт и Хассе (H. Davenport, H. Hasse)

[1] Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen.—J. f. Math., **172** (1934), 151—182.

Дирихле (P. G. L. Dirichlet)

[1] Beweis des Satzes, daß jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Faktor sind, unendlich viele Primzahlen enthält. Werke 1, S. 313.

Канольд (H. J. Kanold)

[1] Untersuchungen über ungerade volkommene Zahlen J. f. Math., **183** (1941), 98—109.

[2] Verschärfung einer notweldigen Bedingung für die Existens einer ungeraden volkommenen Zahl. J. f. Math., **184** (1942), (116—123).

[3] Volgerungen aus den Vorkommen einer Gaussschen Primzahl in der Primfaktorzerlegung einer ungeraden J. f. Math., **186** (1944), 25—29.

Лемер (D. H. Lehmer)

[1] On imaginary quadratic fields whose class-number is unity. Bull. Amer. Math. Soc., **39** (1933), 360.

Линник Ю. В.

[1] О наименьшем простом числе в арифметической прогрессии. Мат. сб., **15** (1944), 139—178, 347—368.

Морхед (Morehead)

[1] Bull. Amer. Math. Soc., **12** (1906), 449—451

[2] Ann. of Math. (2), **10** (1908/09), 88—104.

Хассе (H. Hasse)
[1] Über die Klassenzahl abelscher Zahlkörper. Berlin, 1952.
[2] Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper.—Jahresbericht Deutsche Math.—Ver., **35** (1926), **36** (1927); Erg.—Bd. **6** (1930).
[3] Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage. Math. Ztschr., **31** (1930), 565—582.
[4] Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern.—Abh. Deutsche Akad. d. Wiss. Berlin, Jahrgang 1948, № 2, Berlin, 1950.
Хейльброн и Линфут (H. Heilbronn, E. H. Linfoot)
[1] On the imaginary quadratic corpora of class—number one. Quarterly Journ. of Math. Oxford, ser. 5 (1934), 293—301.
Цасенхаус (H. Zassenhaus)
[1] Über die Existenz von Primzahlen in arithmetischen Progression.—Comment. Math. Helvetici, **22** (1949), 232—259.

УКАЗАТЕЛЬ

ОГЛАВЛЕНИЕ

Глава II. КВАДРАТИЧНЫЕ ВЫЧЕТЫ

ЗАМЕЧЕННЫЕ ОПЕЧАТКИ

Страница	*Строка*	*Напечатано*	*Следует читать*
25	17 сн.	$p + a,\ p + b$	$p \nmid a,\ p \nmid b$
26	19 св.	$p + b$	$p \nmid b$
35	9 сн.	$p + a$	$p \nmid a$
55	1 сн.	$3 = 3 \cdot \underline{1} + 0$	$\underline{\underline{3}} = 3 \cdot \underline{1} + \underline{0}$
89	4 св.	$w \equiv \overline{w} + gp$	$\overline{w} \equiv w + gp$
251	2 сн.	p_s	p^s
406	18 св.	$21 \cong \mathfrak{q}\mathfrak{q}' \cdot \mathfrak{q}\mathfrak{r}' = \mathfrak{q}\mathfrak{r} \cdot \mathfrak{r}'\mathfrak{r}'$	$21 \cong \mathfrak{q}\mathfrak{q}' \cdot \mathfrak{r}\mathfrak{r}' = \mathfrak{q}\mathfrak{r} \cdot \mathfrak{q}'\mathfrak{r}'$
466	6 сн.	$q = \mathfrak{q}\mathfrak{q}'$	$q \cong \mathfrak{q}\mathfrak{q}'$

Г. Хассе