А.И.Галочкин, Ю.В.Нестеренко, А.Б.Шидловский
Под общ. ред. А. Б. Шидловского

ВВЕДЕНИЕ В ТЕОРИЮ ЧИСЕЛ

М.: Изд-во Моск. ун-та, 1984. — 152 с.

Содержание книги составляет применение методов анализа и теории функций комплексного переменного к некоторым задачам теории чисел. В книге рассматриваются три основных вопроса: 1) асимптотический закон распределения простых чисел; 2) теорема о бесконечности множества простых чисел в арифметических прогрессиях; 3) приближение действительных и алгебраических чисел рациональными числами и трансцендентность чисел e и π.

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ

$\mathbf{N}$ — множество натуральных чисел.
$\mathbf{Z}$ — кольцо целых рациональных чисел.
$\mathbf{Q}$ — поле рациональных чисел.
$\mathbf{C}$ — поле комплексных чисел.
$\mathbf{A}$ — поле всех алгебраических чисел над $\mathbf{Q}$.
$\mathbf{Z}_{\mathbf{A}}$ — кольцо целых алгебраических чисел поля $\mathbf{A}$.
(a, b) — общий наибольший делитель целых чисел a и b.
$(a_1, \ldots, a_n)$ — общий наибольший делитель чисел $a_1, \ldots, a_n$.
$b \mid a$ — целое число b делит целое число a.
$b \nmid a$ — целое число b не делит целое число a.
$\binom{m}{k}$ — число сочетаний из m элементов по k.
$\{x\}$ — дробная часть числа x.
$[x]$ — целая часть числа x.
$|\alpha|$ — максимум модулей сопряженных для алгебраического числа α.
$\mathbf{K}[x]$ — кольцо многочленов от x с коэффициентами из поля или кольца $\mathbf{K}$.
$\mathbf{K}[x_1, \ldots, x_n]$ — кольцо многочленов от $x_1, \ldots, x_n$ с коэффициентами из поля или кольца $\mathbf{K}$.
$\sum_{p \leqslant x} f(p)$ — сумма по всем простым числам p, не превосходящим x.
$\sum_{p} f(p)$ — сумма по всем простым числам p.
$\prod_{p \leqslant x} f(p)$ — произведение по всем простым числам p, не превосходящим x.
$\prod_{p} f(p)$ — произведение по всем простым числам p.

Квадратные скобки употребляются в двух случаях: при обозначении целой части числа и при обозначении символа кольца многочленов над каким-либо полем или кольцом. Фигурные скобки употребляются только для обозначения дробной доли числа.

ПРЕДИСЛОВИЕ

Эта книга подготовлена и издается в связи с включением в новый учебный план механико-математического факультета Московского университета курса теории чисел и должна служить пособием по этому курсу. Она включает в себя материал, соответствующий программе, подготовленной кафедрой теории чисел. Эта программа составлена с учетом того, что курс будет читаться студентам на 9-м семестре. Ее содержание — применение методов анализа и теории функций комплексного переменного к некоторым задачам теории чисел.

Для читателя, владеющего основными понятиями анализа и теории функций комплексного переменного, книга может служить введением в теорию чисел, знакомя его сразу с некоторыми задачами теории чисел, решаемыми аналитическими методами, без детального рассмотрения ее основ.

Книга также может быть использована при чтении специальных курсов и в работе семинаров по теории чисел в университетах и педагогических институтах.

В книге рассматриваются три основных вопроса:

1) асимптотический закон распределения простых чисел;
2) теорема о бесконечности множества простых чисел в арифметических прогрессиях;
3) приближение действительных и алгебраических чисел рациональными числами и трансцендентность чисел e и π.

Изложению этих вопросов посвящены соответственно вторая, третья и четвертая главы. Первая глава содержит простейшие сведения о простых числах и некоторые теоремы о распределении простых чисел, доказываемые элементарными методами.

В конце каждой главы приводятся замечания, связанные с ее содержанием, и список задач различной степени трудности.

За основным текстом следует два дополнения.

В первом рассматривается задача об оценке остаточного члена в асимптотическом законе. Цель этого дополнения — показать идеи, на которых основывается такая оценка, а также зависимость точности оценки от имеющихся сведений о расположении нулей дзета-функции Римана. Для упрощения рассуждений рассматривается случай условной оценки. Ознакомившись с дополнением, читатель сможет детально изучить вопрос об оценке остаточного члена по специальным монографиям о распределении простых чисел.

Во втором дополнении показывается, как качественный факт трансцендентности какого-либо числа может получить количественную характеристику. С помощью метода Эрмита в теории трансцендентных чисел устанавливается

оценка снизу модуля многочлена с целыми коэффициентами от числа e, зависящая от степени многочлена и величины его коэффициентов.

В список литературы включен ряд книг на русском языке, по которым читатель может самостоятельно продолжить дальнейшее изучение проблем теории чисел, рассмотренных в этой книге.

Каждая глава имеет свою нумерацию формул, лемм и теорем.

Авторы выражают благодарность *Н. И. Фельдману*, прочитавшему рукопись, *А. В. Малышеву* и *В. И. Нечаеву*, взявшим на себя труд по ее рецензированию, а также коллективу кафедры теории чисел Московского государственного педагогического института им. В. И. Ленина за ее обсуждение. Их ценные замечания способствовали улучшению книги. Авторы благодарят *П. В. Трупашову* за большую помощь при оформлении рукописи.

ВВЕДЕНИЕ

Теория чисел является одним из древнейших разделов математики. Она возникла как наука, изучающая свойства натуральных чисел. Понятия натурального числа и арифметических действий над числами являются одними из первых математических абстракций, имеющими важнейшее значение для математики, других наук и всей практической деятельности человечества.

В дальнейшем круг рассматриваемых в теории чисел вопросов значительно расширился. В ней изучаются свойства различных классов чисел: целых, рациональных, алгебраических, трансцендентных. Но и в настоящее время целые числа являются важнейшим объектом исследований.

По основной теореме арифметики каждое натуральное число, начиная с 2, единственным способом представляется в виде произведения простых чисел. Таким образом, простые числа — это те элементы, из которых при помощи умножения строятся натуральные числа. Поэтому одной из важнейших задач теории чисел является изучение свойств простых чисел.

Некоторые результаты о простых числах были получены еще в Древней Греции. В книге Евклида «Начала» (IV—III вв. до н. э.) содержится доказательство бесконечности множества простых чисел. Древнегреческий ученый Эратосфен (276—194 гг. до н. э.) нашел способ составления таблиц простых чисел, названный позднее «решетом Эратосфена». На его идее разработаны некоторые современные методы решения задач, связанных с простыми числами (методы решета).

Ряд важных результатов о простых числах получил Л. Эйлер (1707—1783). В его рассуждениях впервые использовалось тождество

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}, \quad s > 1,$$

где произведение распространяется на все простые числа.

Проблемы, связанные с распределением простых чисел в натуральном ряде, обычно являются очень трудными. Многие выдающиеся математики проявляли к ним большой интерес. Существенный прогресс в исследовании этих проблем был достигнут только в середине XIX в. русским ученым П. Л. Чебы-

шевым (1821—1894). Изучая поведение функции $\pi(x)$ — количества простых чисел, не превосходящих x, он, в частности, с помощью элементарных методов оценил порядок роста этой функции, показав, что при некоторых положительных постоянных a и b для всех $x \geqslant 2$ выполняются неравенства

$$a\frac{x}{\ln x} < \pi(x) < b\frac{x}{\ln x}.$$

В конце XIX в. Ж. Адамар (1865—1963) и Ш. Ж. де ла Валле-Пуссен (1866—1962) доказали асимптотический закон распределения простых чисел, утверждающий, что

$$\lim_{x \to +\infty} \frac{\pi(x)}{x/\ln x} = 1.$$

В их доказательствах существенное значение имело изучение свойств дзета-функции Римана — аналитической функции комплексного переменного s, которая при $\operatorname{Re} s > 1$ задается рядом

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

а затем аналитически продолжается в область $\operatorname{Re} s \leqslant 1$.

Как функцию комплексного переменного эту функцию первым стал рассматривать Б. Риман (1826—1866), обнаруживший глубокую связь ее аналитических свойств с вопросами распределения простых чисел.

В 1837 г. Г. П. Лежен-Дирихле (1805—1859) доказал, что в любой арифметической прогрессии, разность и первый член которой взаимно простые числа, содержится бесконечное множество простых чисел. Методы комплексного анализа позволили позднее найти более простое доказательство этой важной теоремы.

К настоящему времени получено много глубоких результатов о простых числах. Однако имеется и целый ряд нерешенных проблем.

В трудах Евклида и особенно Диофанта (III в. н. э.) излагаются методы решения в целых числах некоторых уравнений. Эти труды положили начало большому разделу теории чисел, носящему название «теория диофантовых уравнений».

В теории диофантовых уравнений исследуются вопросы, связанные с решением уравнений в целых числах, в частности вопросы о существовании решений, конечности или бесконечности множества решений, о числе решений в случае их конечности, о способах нахождения решений.

В теории диофантовых приближений изучаются задачи о решении неравенств в целых, рациональных и алгебраических числах, в частности вопросы о приближении чисел рациональными и алгебраическими числами.

В глубокой древности возникла проблема квадратуры круга — проблема построения с помощью циркуля и линейки квадрата, равновеликого кругу. Первое упоминание о ней содержится в папирусе Ринда, составленном около двух тысяч лет до н. э. Эта проблема оказалась связанной с арифметическими свойствами числа π. Она была решена в отрицательном смысле только в 1882 г. Ф. Линдеманом (1852—1939), который доказал трансцендентность числа π. Этот результат был получен им с помощью аналитического метода, созданного в 1873 г. Ш. Эрмитом (1822—1901) для доказательства трансцендентности числа e.

С давних пор в теории чисел сложилось направление, называемое аддитивной теорией чисел. В этой теории рассматриваются задачи о представлении целых чисел в виде суммы слагаемых определенного вида, например в виде суммы степеней целых чисел, суммы нескольких простых чисел.

Замечательным достижением в теории чисел явилось полученное в 1937 г. И. М. Виноградовым (1891—1983) доказательство теоремы, утверждающей, что каждое достаточно большое нечетное натуральное число представимо в виде суммы трех простых чисел. Эта задача, известная как проблема Гольдбаха, не поддавалась решению около двухсот лет. Ее решение стало возможным в результате создания И. М. Виноградовым нового аналитического метода оценки тригонометрических сумм. Метод тригонометрических сумм оказался очень эффективным при решении многих проблем теории чисел.

Выше отмечены только некоторые разделы теории чисел, в основном связанные с содержанием предлагаемой вниманию читателя книги. Имеются и другие важные направления исследований со своей тематикой и методами.

В теории чисел много задач, которые просто формулируются, но решения которых очень трудны. Некоторые из них не решены до сих пор.

Например, не доказано и не опровергнуто утверждение о том, что всякое четное число, начиная с 4, представимо в виде суммы двух простых чисел. Это предположение является усилением упомянутой выше проблемы Гольдбаха.

Рассмотрение таблиц показывает, что имеется много пар простых чисел, разность между которыми равна 2 (11 и 13, 41 и 43 и т. д.). Такие числа называются простыми числами-близнецами. До сих пор неизвестно, конечно или бесконечно множество пар близнецов.

Известно, что числа e, π и e^{π} трансцендентны. Но неизвестно даже, являются ли числа $e+\pi$ и $e\pi$ иррациональными.

В теории чисел широко используются методы теории функций, алгебры, геометрии, теории вероятностей. Особенно большое значение имеют аналитические методы, основанные на применении к задачам теории чисел теории функций комплексного переменного.

Решение теоретико-числовых задач стимулировало развитие других разделов математики. Например, развитие методов, связанных с изучением распределения простых чисел, в значительной мере способствовало развитию теории целых и мероморфных функций. Проблемы теории диофантовых уравнений привели к развитию теории алгебраических чисел и некоторых разделов современной алгебры.

Теория чисел в основном является наукой теоретической. Однако ее результаты и методы успешно применяются в других разделах математики, многих других науках, а также при решении ряда практических задач.

В развитие теории чисел внесли свой вклад такие выдающиеся математики, как П. Ферма (1601—1665), Л. Эйлер, Ж. Лагранж (1736—1813), А. Лежандр (1752—1833), К. Гаусс (1777—1855), Г. П. Лежен-Дирихле, Б. Риман, Ш. Эрмит, Д. Гильберт (1862—1943).

Большое значение имели работы русских математиков петербургской школы теории чисел, основанной П. Л. Чебышевым: А. Н. Коркина (1837—1908), Е. И. Золотарева (1847—1878), Г. Ф. Вороного (1868—1908), А. А. Маркова (1856—1922).

Замечательные достижения в теории чисел связаны с именами советских математиков. Среди них в первую очередь следует отметить И. М. Виноградова, Ю. В. Линника (1915—1972), А. Я. Хинчина (1894—1959), А. О. Гельфонда (1906—1968).

ГЛАВА 1

ЭЛЕМЕНТАРНЫЕ ТЕОРЕМЫ О ПРОСТЫХ ЧИСЛАХ

§ 1. Делимость целых чисел

Рассмотрим множество целых чисел. Оно образует кольцо относительно операций сложения и умножения, обозначаемое **Z**. В этом параграфе будут рассматриваться только числа из **Z**.

Операция деления, обратная умножению, выполняется не для всех пар чисел из кольца **Z**.

Число a *делится* на число $b\neq 0$, если существует число q такое, что $a=bq$. В этом случае говорят также, что число b *делит* число a.

Если a делится на b, то b называется *делителем* числа a, а число a *кратным* числа b. Число q называется *частным* от деления a на b.

Число 0 делится на любое целое $b\neq 0$. Если $a\neq 0$, то очевидно, что множество всех делителей a конечно.

Утверждение о том, что b делит a, принято обозначать символом $b\mid a$ (читается «b делит a»). Если же b не делит a, то этот факт обозначают символом $b\nmid a$ (читается «b не делит a»).

Простейшие свойства делимости целых чисел известны читателю. Докажем те из них, которые будут использоваться в дальнейшем.

Лемма 1. *Если* $c\mid b$ *и* $b\mid a$, *то* $c\mid a$.

Доказательство. По определению из $c\mid b$ и $b\mid a$ имеем, что $b=q_1c$ и $a=q_2b$, откуда $a=q_2q_1c=qc$ и снова, по определению $c\mid a$.

Лемма 2. *Если* $m=a+b$, a $d\mid m$ *и* $d\mid a$, *то* $d\mid b$.

Доказательство. По определению $m=q_1d$ и $a=q_2d$. Поэтому из равенства $m=a+b$ получаем $b=(q_1-q_2)d=qd$, откуда следует, что $d\mid b$.

Аналогично доказывается, что если $m=a_1+\ldots+a_{n-1}+a_n$ и d делит числа m, $a_1, \ldots, a_{n-1}$, то $d\mid a_n$.

Общим делителем двух или нескольких чисел называется число, являющееся делителем каждого из этих чисел.

Пусть $a_1, \ldots, a_n$ числа из **Z**, из которых хотя бы одно отлично от нуля. Тогда множество их общих делителей конечно, и поэтому среди них существует наибольшее число.

Наибольшим общим делителем чисел $a_1, \ldots, a_n$ называется наибольший из их общих делителей. Он обозначается $(a_1, \ldots, a_n)$.

Если $(a_1, \ldots, a_n) = 1$, то числа $a_1, \ldots, a_n$ называются *взаимно простыми.*

Примеры: $(258, 42) = 6$, $(60, 210, 360) = 30$, $(10, 21) = 1$.

Лемма 3. *Если a, b и c — целые числа, $(a, b) = 1$ и $b \mid ac$, то $b \mid c$.*

Доказательство. Очевидно, что достаточно доказать утверждение леммы для случая, когда a, b и c — натуральные числа.

Сначала докажем более общее утверждение: *если a, b, u, v — натуральные числа u*

$$au = bv, \quad (a, b) = 1, \tag{1}$$

то $a \mid v$ и $b \mid u$.

Доказательство проведем, пользуясь индукцией по величине суммы $a+b$. При $a+b=2$ имеем, что $a=1$, $b=1$, $(a, b)=1$, и утверждение выполняется. Предположим, что оно справедливо для всех пар a, b, $(a, b)=1$, с суммой $a+b<k$, $k>2$. Докажем, что тогда оно имеет место и для пар a, b, $(a, b)=1$, с суммой $a+b=k$.

Из условий $(a, b)=1$, $a+b>2$ следует, что $a \neq b$. Ввиду симметрии равенства (1) для определенности можно считать, что $a>b$. Тогда из равенства (1) имеем, что

$$(a-b)u = b(v-u), \quad (a-b, b) = 1, \tag{2}$$

и сумма $(a-b)+b=a<k$. Поэтому по предположению индукции из равенства (2) следует, что $b \mid u$, и по определению делимости $u = u_1 b$. Подставляя это значение в равенство (1) и сокращая обе его части на b, получим, что

$$au_1 = v,$$

откуда следует, что $a \mid v$. Утверждение доказано.

Лемма 3 для натуральных a, b и c следует из доказанного утверждения. Если $(a, b)=1$ и $b \mid ac$, то $ac = bd$ и по доказанному $b \mid c$.

Лемма 4. *Если целое число b взаимно просто с каждым из целых чисел $a_1, \ldots, a_n$, то b взаимно просто с их произведением $a_1 \cdot \ldots \cdot a_n$.*

Доказательство. Проведем доказательство с помощью индукции по n. При $n=1$ утверждение очевидно. Допустим, что $n>1$ и для значения $n-1$ утверждение доказано. Если d — общий делитель чисел b и $a_1 \cdot \ldots \cdot a_n$, то $(d, a_n)=1$ и из леммы 3 следует, что $d \mid a_1 \cdot \ldots \cdot a_{n-1}$. По индуктивному предположению $(b, a_1 \cdot \ldots \cdot a_{n-1}) = 1$. Значит, $d=1$. Лемма доказана.

Если a не делится на b, то принято говорить о *делении a на b с остатком.*

Теорема о делении с остатком. *Если a и b — целые числа, $b>0$, то существуют единственные целые числа q и r такие, что*

$$a = bq + r, \quad 0 \leqslant r < b. \tag{3}$$

Доказательство. Существует наибольшее целое q такое, что $bq \leqslant a$. Тогда $bq \leqslant a < b(q+1)$, откуда $0 \leqslant a - bq < b$. Обозначая $a - bq = r$, получаем представление (3).

Докажем единственность этого представления. Если кроме представления (3) имеется другое представление

$$a = bq_1 + r_1, \quad 0 \leqslant r_1 < b, \tag{4}$$

то из равенств (3) и (4) находим, что

$$0 = b(q - q_1) + r - r_1, \quad |r - r_1| < b. \tag{5}$$

Из равенства (5) следует, что число b делит разность $r - r_1$. Но $|r - r_1| < b$ и поэтому $r = r_1$, а тогда из равенства (5) получаем $q = q_1$. Теорема доказана.

Число q в равенстве (3) называется *неполным частным* при делении a на b, а r — *остатком* от деления a на b. Если в равенстве (3) $r = 0$, то это означает, что $b \mid a$.

Примеры. Пусть $b = 12$. Полагая $a = 110, -53, 156$, находим

$$\begin{aligned} 110 &= 12 \cdot 9 + 2, & 0 < 2 < 12, \\ -53 &= 12 \cdot (-5) + 7, & 0 < 7 < 12, \\ 156 &= 12 \cdot 13 + 0, & 0 < 12. \end{aligned}$$

§ 2. Простые числа

Рассмотрим множество натуральных чисел $\mathbf{N}$. Число 1 имеет единственный натуральный делитель. Каждое натуральное число n, $n > 1$, делится на 1 и n.

Натуральное число $n > 1$ называется *простым*, если оно не имеет других натуральных делителей, кроме 1 и n.

Натуральное число n называется *составным*, если оно имеет натуральный делитель, отличный от 1 и n.

Из этого определения следует, что каждое составное число представляется в виде

$$n = ab, \ a, b \in \mathbf{N}, \ 1 < a < n, \ 1 < b < n.$$

В этом параграфе будем рассматривать только натуральные делители целых чисел.

Лемма 5. *Наименьший отличный от единицы делитель натурального числа $n > 1$ есть простое число.*

Доказательство. Число $n > 1$ имеет хотя бы два различных делителя и, следовательно, имеет делитель, отличный от 1. Среди всех делителей n, отличных от 1, имеется наименьший. Пусть это будет q. Число q должно быть простым, так как в противном случае оно было бы составным и по определению имело бы делитель q_1 такой, что $1 < q_1 < q$. Но $q_1 \mid q$ и $q \mid n$, а тогда по лемме 1 $q_1 \mid n$. Это противоречит тому, что q — наименьший делитель n. Значит, q — простое число.

Следствие. *Каждое натуральное число $n>1$ имеет хотя бы один простой делитель.*

Лемма 6. *Наименьший простой делитель составного числа n не превосходит $\sqrt{n}$.*

Доказательство. Пусть p, $p>1$ — наименьший делитель n, являющийся по лемме 5 простым числом. Так как n — составное число, то $n=pq$, где $q\geqslant p$. Поэтому $n\geqslant p^2$. Отсюда следует, что $p\leqslant\sqrt{n}$.

Лемма 7. *Если p — простое число, то любое целое число a либо взаимно просто с p, либо делится на p.*

Доказательство. Наибольший общий делитель (a, p) является делителем p и поэтому может быть равен только 1 или p. В первом случае a взаимно просто с p, а во втором — a делится на p.

Основная теорема арифметики. *Любое натуральное число $n>1$ представляется в виде произведения простых чисел, причем единственным образом, если не учитывать порядок следования сомножителей.*

Доказательство. По лемме 5 число n имеет наименьший простой делитель p_1. Тогда $n=p_1a_1$. Если $a_1>1$, то аналогично получим $a_1=p_2a_2$, где p_2 — наименьший простой делитель числа a_1 и т. д. Поскольку числа $a_1, a_2, \ldots$ убывают, то на некотором шаге будем иметь, что $a_r=1$ и $a_{r-1}=p_r$. Перемножая все полученные равенства, после сокращения на $a_1a_2\cdots a_{r-1}$ получим разложение числа n на простые сомножители

$$n=p_1p_2\cdots p_r. \tag{6}$$

Докажем теперь единственность разложения (6). Предположим, что для некоторого n имеются два разложения на простые множители

$$p_1p_2\cdots p_k=q_1q_2\cdots q_s. \tag{7}$$

Правая часть этого равенства делится на q_1. Значит, и его левая часть делится на q_1. Тогда по лемме 4 хотя бы один из сомножителей левой части делится на q_1. Пусть это будет p_1. Тогда $p_1=q_1$, так как p_1 делится только на 1 и p_1. Сокращая обе части равенства (7) на $p_1=q_1$, получим, что

$$p_2\cdots p_k=q_2\cdots q_s. \tag{8}$$

Повторяя проведенное рассуждение для равенства (8), получим $p_2=q_2$ и $p_3\cdots p_k=q_3\cdots q_s$ и т. д., до тех пор пока в одной из частей получающихся равенств, например правой, сократятся все сомножители. Но тогда и в левой части должны сократиться все сомножители, так как равенство $p_{s+1}\cdots p_k=1$ невозможно, поскольку все числа $p_{s+1}, \ldots, p_k$ больше единицы. Следовательно, в равенстве (7) разложения совпадают. Теорема доказана.

Пусть $n>1$ и равенство (6) есть разложение n на простые сомножители. Среди чисел $p_1, p_2, \ldots, p_r$ могут быть и одинако-

вые. Пусть $p_1, p_2, \ldots, p_k$ — различные из этих чисел, а $\alpha_1, \alpha_2, \ldots, \alpha_k$ — кратности, с которыми они входят в разложение (6). Тогда равенство (6) можно переписать следующим образом:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}. \tag{9}$$

Представление (9) называется *каноническим разложением* натурального числа $n>1$ на простые сомножители.

Пример. $261360 = 2^4 \cdot 3^3 \cdot 5 \cdot 11^2$.

С помощью канонического разложения (9) можно представить все делители n. Они имеют вид

$$d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}, \quad 0 \leqslant \beta_i \leqslant \alpha_i, \quad i = 1, \ldots, k. \tag{10}$$

Действительно, если $d \mid n$, то по лемме 1 каждый простой делитель числа d делит n. Поэтому он содержится среди чисел $p_1, \ldots, p_k$ и входит в каноническое разложение числа d в степени, не большей, чем в разложении (9) числа n. Поэтому d представляется в виде (10). Очевидно и обратное, что каждое число вида (10) есть делитель n.

В дальнейшем потребуются две функции, часто рассматриваемые в теории чисел.

Пусть x — любое действительное число. Обозначим $[x]$ — наибольшее целое число, не превосходящее x. Тогда

$$[x] \leqslant x < [x] + 1.$$

Функция $[x]$ называется *целой частью числа* x.

Функция $\{x\} = x - [x]$ называется *дробной частью числа* x. Всегда

$$0 \leqslant \{x\} < 1.$$

Очевидно, что $\{x\}$ является периодической функцией с периодом 1, т. е. при любом $a \in \mathbf{Z}$

$$\{x + a\} = \{x\}.$$

Установим вспомогательное предложение, с помощью которого находится каноническое разложение числа $n!$

Лемма 8. *Показатель $\alpha_p = \alpha_p(n)$, с которым простое число p входит в каноническое разложение числа $n!$, определяется равенством*

$$\alpha_p = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots. \tag{11}$$

Замечание. Ясно, что сумма в правой части равенства (11) будет конечной. Все слагаемые, для которых $p^k > n$, равны нулю.

Доказательство. Среди чисел $1, 2, \ldots, n$ имеется $\left[\frac{n}{p}\right]$, делящихся на p, среди таких $\left[\frac{n}{p^2}\right]$, делящихся на p^2, а сре-

ди последних $\left[\frac{n}{p^3}\right]$, делящихся на p^3, и т. д. Поэтому среди чисел $1, 2, \ldots, n$ ровно $\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]$ делится на p^k, но не делится на p^{k+1}. Каждое из таких чисел вносит как слагаемое в состав α_p число k, а все они — число $k\left(\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]\right)$. Если m_p удовлетворяет неравенствам $p^{m_p} \leqslant n < p^{m_p+1}$, то тогда

$$\alpha_p = \sum_{k=1}^{m_p} k\left(\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]\right) = \sum_{k=1}^{m_p}\left[\frac{n}{p^k}\right],$$

что доказывает утверждение леммы.

В дальнейшем будем пользоваться следующими обозначениями. Суммы и произведения

$$\sum_{n \leqslant x} f(n), \quad \prod_{n \leqslant x} f(n), \quad \sum_{p \leqslant x} f(p), \quad \prod_{p \leqslant x} f(p)$$

будут распространены соответственно на все натуральные числа и все простые числа, не превосходящие числа x, а

$$\sum_{p} f(p), \quad \prod_{p} f(p)$$

— на все простые p.

Следствие из леммы 8. *При* $n > 1$

$$n! = \prod_{p \leqslant n} p^{\left(\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots\right)}. \tag{12}$$

§ 3. Теоремы Евклида и Эйлера

Рассуждения, с помощью которых для натурального числа n было установлено существование канонического разложения (9), не позволяют получить никакого утверждения о количестве различных простых чисел. Естественно возникает вопрос о том, конечно или бесконечно множество всех простых чисел. Ответ на этот вопрос содержится в IX книге «Начал» древнегреческого математика Евклида.

Теорема Евклида. *Множество простых чисел бесконечно.*

Доказательство. Допустим противное, что простые числа образуют конечное множество и p — наибольшее простое число. Рассмотрим число

$$N = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p + 1.$$

Число N не делится ни на одно из простых чисел 2, 3, 5..., p, так как при делении N на любое из этих чисел остаток равен 1. Но $N>1$ и по следствию из леммы 5 N должно иметь простой делитель. Полученное противоречие показывает, что сделанное предположение не верно и теорема справедлива.

Занумеруем простые числа $p_1=2$, $p_2=3, ..., p_n, ...$ в порядке их возрастания. Доказательство теоремы Евклида позволяет получить грубую оценку для числа p_n.

Докажем по индукции, что

$$p_{n+1} < 2^{2^n}, \quad n = 1, 2, \ldots . \tag{13}$$

При $n=1$ утверждение (13) верно, $p_2=3<2^2$. Допустим, что оно выполняется для $n-1$, и докажем, что тогда оно имеет место и для n.

Поскольку p_{n+1} не больше наименьшего простого делителя числа $p_1p_2\cdot \ldots \cdot p_n+1$, а $p_1=2$, то

$$p_{n+1} \leqslant p_1 p_2 \cdot \ldots \cdot p_n + 1 < 2^{1+2+\ldots+2^{n-1}} + 1 < 2^{2^n}.$$

По индукции утверждение справедливо при любом n.

Для того чтобы составить таблицу простых чисел, не превосходящих натурального числа N, имеется простой метод, который был известен еще древнегреческому математику Эратосфену. Этот метод называется *решетом Эратосфена.*

Напишем одно за другим числа

$$2, 3, ..., N. \tag{14}$$

Число 2, являющееся простым, оставляем и зачеркиваем после него все четные числа. Первое следующее за 2 незачеркнутое число есть 3. Оно не делится на 2. Значит, оно не имеет делителей, отличных от 1 и 3, и поэтому является простым. Оставляем 3 и зачеркиваем после него все числа, кратные 3. Продолжая этот процесс, найдем все простые числа, не превосходящие некоторого простого числа p_k. При этом будут зачеркнуты все составные числа, кратные $2, 3, ..., p_k$. Первое незачеркнутое после p_k число будет простым числом p_{k+1}, так как оно не делится на $2, 3, ..., p_k$ и поэтому имеет делителями только 1 и p_{k+1}. Если найдено $p_k \geqslant \sqrt{N}$, то все оставшиеся незачеркнутыми числа будут простыми, поскольку все кратные чисел $2, 3, ..., p_k$ уже вычеркнуты, а по лемме 6 любое составное число n имеет простой делитель $\leqslant \sqrt{n}$.

Итак, составление таблицы простых чисел, не превосходящих N, указанным процессом закончено, как только зачеркнуты все числа, кратные простым числам $\leqslant \sqrt{N}$.

Пример. $N=40$. В приводимой ниже таблице подчеркнуты все числа, которые должны быть вычеркнуты в процессе применения решета Эратосфена.

	2,	3,	4,	5,	6,	7,	8,	9,	10,
11,	12,	13,	14,	15,	16,	17,	18,	19,	20,
21,	22,	23,	24,	25,	26,	27,	28,	29,	30,
31,	32,	33,	34,	35,	36,	37,	38,	39,	40.

Числа 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37 составляют таблицу простых чисел, не превосходящих 40.

Решето Эратосфена — быстрый и удобный алгоритм для нахождения всех простых чисел на отрезке от 1 до некоторого натурального числа N. В 1668 г. Д. Пелль (1610—1685) составил таблицу простых чисел до 10^5. С тех пор она много раз расширялась. В 1914 г. Д. Н. Лемер опубликовал таблицу простых чисел до 10^7.

Реализация решета Эратосфена при больших значениях N на ЭВМ встречается с трудностями, связанными с тем, что необходима большая машинная память для хранения всех чисел от 1 до N. Существуют модификации этого алгоритма, работающие столь же быстро, но использующие значительно меньшую машинную память. Они выдают всю последовательность простых чисел в пределах от 1 до N отдельными отрезками. При существующих мощностях ЭВМ не составляет проблемы получить все простые числа до 10^{12}. Однако выписать все эти числа в таблицу сложно, так как их количество — 37607912018 — очень велико.

В то же время с помощью некоторых алгоритмов найдены отдельные очень большие простые числа. Например, $2^{19937}-1$ и $2^{44497}-1$.

Таблицы простых чисел показывают, что простые числа встречаются все реже и реже с ростом их величины. Например, в первой сотне натуральных чисел — 25 простых чисел, во второй — 21, в третьей — 16 и т. д. В первой тысяче — 168, во второй — 135, в третьей — 120 и т. д.

Простые числа распределены в натуральном ряде весьма нерегулярно.

Можно указать сколь угодно длинные отрезки натурального ряда, свободные от простых чисел. Так, при любом n числа

$$N_k = 2\cdot 3\cdot\ldots\cdot(n+1)+k,\ k=2, 3, \ldots, n+1,$$

следуют одно за другим и все являются составными, так как $k \mid N_k$, $k=2, \ldots, n+1$.

С другой стороны, существует много пар простых чисел вида p и $p+2$ с разностью, равной 2. Такие пары называют *простыми числами-близнецами*. Среди них имеются очень большие пары. До сих пор неизвестно, конечно или бесконечно множество пар близнецов. В этом состоит знаменитая проблема близнецов. Приведем примеры близнецов: 3 и 5, 11 и 13, 17 и 19, 41 и 43, 10016957 и 10016959, $156\cdot 5^{202}\pm 1$.

В теории чисел разработаны методы, позволяющие изучать распределение простых чисел.

Пусть $x>0$ — действительное число. Рассмотрим функцию $\pi(x)$, выражающую число простых чисел $\leqslant x$. Ее можно записать следующим образом:

$$\pi(x)=\sum_{p\leqslant x} 1.$$

Примеры. $\pi(1)=0$, $\pi(2)=1$, $\pi(10)=4$, $\pi(40)=12$, $\pi(10^{12})=37607912018$, $\pi(p_n)=n$, если p_n есть n-е простое число.

Для функции $\pi(x)$ неизвестно никакой простой формулы, которая позволяла бы изучать ее поведение. Важнейшей проблемой теории чисел является изучение асимптотического поведения функции $\pi(x)$.

Теорему Евклида можно сформулировать следующим образом: $\pi(x)\to+\infty$ при $x\to+\infty$.

Установим вспомогательное предложение, с помощью которого будут доказаны две теоремы о распределении простых чисел.

Обозначим

$$P(x)=\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)^{-1}, \quad x\geqslant 2. \tag{15}$$

Лемма 9. *$P(x)>\ln x$ и, следовательно, $P(x)\to+\infty$ при $x\to+\infty$.*

Доказательство. При любом $m\in\mathbf{N}$ имеем, что

$$\frac{1}{1-t}=\sum_{k=0}^{\infty} t^k>\sum_{k=0}^{m} t^k, \quad 0<t<1.$$

Полагая в этом неравенстве $t=1/p$, получаем неравенство

$$\left(1-\frac{1}{p}\right)^{-1}=\frac{1}{1-\frac{1}{p}}>1+\frac{1}{p}+\ldots+\frac{1}{p^m}.$$

Отсюда при любом $m\in\mathbf{N}$

$$P(x)>\prod_{p\leqslant x}\left(1+\frac{1}{p}+\ldots+\frac{1}{p^m}\right).$$

После перемножения скобок в правой части этого неравенства, получим сумму вида $\sum_k \frac{1}{k}$, распространенную на некоторые натуральные значения k.

Если выбрать число m так, чтобы $2^{m+1}>x$, то по основной теореме арифметики в эту сумму войдут все слагаемые, соответствующие значениям k от 1 до $[x]$, и еще какие-то слагае-

мые, соответствующие другим значениям k. Отбрасывая последние слагаемые, будем иметь неравенство

$$P(x) > \sum_{k=1}^{[x]} \frac{1}{k}. \tag{16}$$

Пользуясь неравенством

$$\ln(1+t) < t,\ 0 < t \leqslant 1,$$

при $t = 1/k$, $k \in \mathbf{N}$, находим, что

$$\ln(k+1) - \ln k = \ln\left(1 + \frac{1}{k}\right) < \frac{1}{k},\ k = 1, 2, \ldots .$$

Складывая почленно последние неравенства при $k = 1, \ldots, n$, получаем неравенство

$$\sum_{k=1}^{n} \frac{1}{k} > \ln(n+1). \tag{17}$$

Из неравенств (16) и (17) имеем

$$P(x) > \ln([x]+1) > \ln x,$$

что доказывает утверждение леммы.

Из того, что $P(x) \to +\infty$ при $x \to +\infty$, следует новое доказательство бесконечности множества простых чисел. Оно было получено Эйлером.

Рассмотрим сумму

$$S(x) = \sum_{p \leqslant x} \frac{1}{p}, \quad x \geqslant 2.$$

Теорема 1. *$S(x) > \ln\ln x - 1/2$, и поэтому ряд $\sum_p \frac{1}{p}$ расходится.*

Доказательство. Пользуясь разложением функции $\ln(1+t)$, $0 < t < 1$, в ряд Тейлора, получаем неравенство

$$-(\ln(1-t) + t) = \frac{t^2}{2} + \frac{t^3}{3} + \frac{t^4}{4} + \ldots$$

$$\ldots < \frac{t^2}{2}(1 + t + t^2 + \ldots) = \frac{t^2}{2(1-t)}.$$

Полагая в этом неравенстве $t = 1/p$ и пользуясь равенством (15), имеем, что

$$\ln P(x) - S(x) = -\sum_{p \leqslant x}\left(\ln\left(1 - \frac{1}{p}\right) + \frac{1}{p}\right) < \sum_{p < x} \frac{p^{-2}}{2(1-p^{-1})} =$$

$$= \sum_{p \leqslant x} \frac{1}{2p(p-1)} < \sum_{n=2}^{\infty} \frac{1}{2n(n-1)} = \frac{1}{2}.$$

Отсюда по лемме 9 находим, что $S(x) > \ln\ln x - 1/2$. Теорема доказана.

Неравенство (17) можно получить другим способом с помощью нижеследующей леммы, которая окажется полезной в главах 2 и 3 для установления ряда других неравенств.

Лемма 10. *Пусть* m *и* n *— натуральные числа,* $n > m$. *Функция* $f(x)$ *не возрастает на множестве* $m \leqslant x < +\infty$. *Тогда выполняется неравенство*

$$\int_m^{n+1} f(x)\,dx \leqslant \sum_{k=m}^{n} f(k) \leqslant f(m) + \int_m^n f(x)\,dx,$$

а если сходится интеграл

$$\int_m^{+\infty} f(x)\,dx,$$

то и неравенства

$$\int_m^{+\infty} f(x)\,dx \leqslant \sum_{k=m}^{\infty} f(k) \leqslant f(m) + \int_m^{+\infty} f(x)\,dx.$$

Доказательство. Ввиду монотонности функции $f(x)$ при любом $k \geqslant m$ имеем, что

$$f(k+1) \leqslant f(x) \leqslant f(k), \quad k \leqslant x \leqslant k+1.$$

Так как монотонная функция интегрируема, то, интегрируя почленно эти неравенства на отрезке $k \leqslant x \leqslant k+1$, получим

$$f(k+1) \leqslant \int_k^{k+1} f(x)\,dx \leqslant f(k).$$

Теперь, складывая левые из последних неравенств для значений $k = m, m+1, \ldots, n-1$, а правые из них для значений $k = m, m+1, \ldots, n$, находим неравенства

$$\sum_{k=m+1}^{n} f(k) \leqslant \int_m^n f(x)\,dx, \quad \int_m^{n+1} f(x)\,dx \leqslant \sum_{k=m}^{n} f(k),$$

из которых следует первое утверждение.

Второе утверждение получается из первого переходом к пределу при $n \to \infty$.

Покажем, что плотность распределения простых чисел в натуральном ряде равна нулю.

Теорема Эйлера.

$$\pi(x)/x \to 0, \text{ при } x \to +\infty.$$

Рассуждения Эйлера не доказывали полностью этот результат. Строгое доказательство было дано А. Лежандром.

Докажем теорему Эйлера методом, основанным на идее решета Эратосфена.

Пусть $N(x, r)$ обозначает количество натуральных чисел n, $n \leqslant x$, не делящихся ни на какое из r первых простых чисел $p_1, \ldots, p_r$ и $N(x, 0)$ — количество натуральных чисел, не превосходящих x.

Все числа n, $n \leqslant x$, не делящиеся на $p_1, \ldots, p_{r-1}$ разбиваются на два класса: не делящиеся на p_r и делящиеся на p_r. Чисел первого класса будет $N(x, r)$. Каждое число n из второго класса представляется в виде $n = p_r m$, где

$$m \leqslant \frac{x}{p_r}, \quad p_i \nmid m, \quad i = 1, \ldots, r-1.$$

Следовательно, второй класс содержит $N\left(\frac{x}{p_r}, r-1\right)$ чисел, и справедливо равенство

$$N(x, r-1) = N(x, r) + N\left(\frac{x}{p_r}, r-1\right).$$

Отсюда

$$N(x, r) = N(x, r-1) - N\left(\frac{x}{p_r}, r-1\right). \tag{18}$$

При $r = 1$ равенство (18) также справедливо.

С помощью индукции и равенства (18) легко доказываем, что

$$N(x, r) = N(x, 0) - \sum_i N\left(\frac{x}{p_i}, 0\right) +$$

$$+ \sum_{i,j} N\left(\frac{x}{p_i p_j}, 0\right) - \sum_{i,j,k} N\left(\frac{x}{p_i p_j p_k}, 0\right) + \ldots,$$

где суммирование ведется по всем возможным сочетаниям из $p_1, \ldots, p_r$ по одному, по два, по три и т. д.

Так как $N(x, 0) = [x]$, то последнее равенство принимает вид

$$N(x, r) = [x] - \sum_i \left[\frac{x}{p_i}\right] + \sum_{i,j} \left[\frac{x}{p_i p_j}\right] - \sum_{i,j,k} \left[\frac{x}{p_i p_j p_k}\right] + \ldots. \tag{19}$$

Пусть ξ удовлетворяет неравенствам $2 < \xi < x$, а r таково, что $p_r \leqslant \xi < p_{r+1}$. Тогда

$$\pi(x) \leqslant r + N(x, r), \tag{20}$$

поскольку любое простое число либо равно одному из r первых простых чисел, либо содержится во множестве натуральных чисел, не делящихся ни на одно из этих простых чисел.

Подставим в правую часть неравенства (20) значение $N(x, r)$ из равенства (19). Затем опустим у всех слагаемых

знак целой части, заменяя этим целые части соответствующих чисел на сами числа. При такой замене каждого слагаемого допускается погрешность, меньшая единицы, а при замене всех слагаемых — погрешность, меньшая, чем 2^r, так как число всех слагаемых равно

$$\sum_{k=0}^{r} \binom{r}{k} = 2^r.$$

Тогда ввиду неравенства $r+2^r<2^{r+1}<2^{\xi+1}$ и по лемме 9 имеем, что

$$\pi(x) < r + 2^r + x - \sum_i \frac{x}{p_i} + \sum_{i,j} \frac{x}{p_i p_j} - \sum \frac{x}{p_i p_j p_k} + \ldots$$

$$\ldots < 2^{\xi+1} + x \prod_{p \leqslant \xi} \left(1 - \frac{1}{p}\right) < 2^{\xi+1} + \frac{x}{\ln \xi},$$

откуда

$$\frac{\pi(x)}{x} < \frac{2^{\xi+1}}{x} + \frac{1}{\ln \xi}. \tag{21}$$

Выбирая в качестве ξ функцию от x, такую, что $\xi \to +\infty$ и $\frac{2^{\xi+1}}{x} \to 0$ при $x \to +\infty$, получаем, что $\pi(x)/x \to 0$ при $x \to +\infty$.

Замечание. Если выбрать $\xi = \gamma \ln x$, $0<\gamma<1/\ln 2$, то из неравенства (21) получаем более точное утверждение

$$\pi(x) = O\left(\frac{x}{\ln \ln x}\right), \quad x \to +\infty.$$

§ 4. Оценки Чебышева для функции $\pi(x)$

Простые числа являются простейшими объектами, из которых с помощью умножения строятся все натуральные числа, большие единицы. Поэтому проблема распределения простых чисел всегда представляла большой интерес. Все попытки после Евклида установить какие-либо новые утверждения о распределении простых чисел долгое время не приводили к успеху.

А. Лежандр, пользуясь таблицами простых чисел, указал формулу, которая приближенно выражала функцию $\pi(x)$ с некоторой точностью в пределах существовавших таблиц простых чисел. Эта формула имела вид

$$\pi(x) \approx \frac{x}{\ln x - B}, \quad B = 1{,}08366. \tag{22}$$

К. Ф. Гаусс утверждал, что более точной является формула

$$\pi(x) \approx \int_2^x \frac{dt}{\ln t}. \tag{23}$$

Заметим, что при $x \to +\infty$ правые части соотношений (22) и (23) эквивалентны (т. е. предел их отношения равен 1).

Первым существенного успеха в изучении распределения простых чисел добился П. Л. Чебышев, который в 1850 г. элементарным методом строго установил истинный порядок роста функции $\pi(x)$ при $x \to +\infty$.

Теорема Чебышева. *Существуют положительные постоянные a и b такие, что при всех $x \geqslant 2$ выполняются неравенства*

$$a \frac{x}{\ln x} < \pi(x) < b \frac{x}{\ln x}. \tag{24}$$

Для доказательства теоремы докажем вспомогательные предложения. Рассмотрим следующие функции, введенные впервые Чебышевым:

$$\theta(x) = \sum_{p \leqslant x} \ln p, \quad x > 0, \tag{25}$$

и

$$\psi(x) = \sum_{p^m \leqslant x} \ln p, \quad x > 0, \tag{26}$$

где в сумме, определяющей функцию $\psi(x)$, суммирование распространяется на все пары простых p и натуральных m, удовлетворяющих неравенству $p^m \leqslant x$.

При фиксированном p все значения m такие, что $p^m \leqslant x$ удовлетворяют также неравенству $m \leqslant \frac{\ln x}{\ln p}$, и поэтому число их равно $[\ln x / \ln p]$. Отсюда следует, что функцию $\psi(x)$ (26) можно представить следующим образом:

$$\psi(x) = \sum_{p \leqslant x} \left[\frac{\ln x}{\ln p} \right] \ln p, \quad x > 0. \tag{27}$$

Функции $\theta(x)$ и $\psi(x)$ имеют большое значение при решении задач, связанных с распределением простых чисел. Это объясняется тем, что асимптотическое поведение функций $\theta(x)$, $\psi(x)$ и $\pi(x)$ тесно связано. Если известно асимптотическое поведение одной из этих функций, то определено и асимптотическое поведение двух других функций. Это утверждение содержится в доказываемой ниже лемме.

Лемма 11. *Пусть* λ_1, λ_2, λ_3 и μ_1, μ_2, μ_3 *обозначают соответственно нижние и верхние пределы при* $x\to+\infty$ *функций*

$$\frac{\theta(x)}{x},\quad \frac{\psi(x)}{x},\quad \frac{\pi(x)}{\frac{x}{\ln x}}. \tag{28}$$

Тогда

$$\lambda_1=\lambda_2=\lambda_3,\ \mu_1=\mu_2=\mu_3.$$

Доказательство. Из равенств (25) и (27), опуская знак целой части, находим

$$\theta(x)\leqslant\psi(x)=\sum_{p\leqslant x}\left[\frac{\ln x}{\ln p}\right]\ln p\leqslant$$

$$\leqslant\sum_{p\leqslant x}\frac{\ln x}{\ln p}\ln p=\ln x\sum_{p\leqslant x}1=\pi(x)\ln x$$

и

$$\frac{\theta(x)}{x}\leqslant\frac{\psi(x)}{x}\leqslant\frac{\pi(x)}{\frac{x}{\ln x}}.$$

Из последних неравенств следует, что

$$\lambda_1\leqslant\lambda_2\leqslant\lambda_3. \tag{29}$$

С другой стороны, при любом α, $0<\alpha<1$, и любом $x>1$ имеем

$$\theta(x)\geqslant\sum_{x^\alpha<p<x}\ln p\geqslant\ln(x^\alpha)\sum_{x^\alpha<p\leqslant x}1=\alpha\ln x\,(\pi(x)-\pi(x^\alpha)).$$

Но $\pi(x^\alpha)<x^\alpha$, поэтому

$$\frac{\theta(x)}{x}>\alpha\left(\frac{\pi(x)}{\frac{x}{\ln x}}-\frac{\ln x}{x^{1-\alpha}}\right). \tag{30}$$

При $\alpha<1$ имеем $\lim\limits_{x\to+\infty}\ln x/x^{1-\alpha}=0$, а тогда из неравенства (30) получаем, что $\lambda_1\geqslant\alpha\lambda_3$. Но ввиду произвольности α, $0<\alpha<1$, его можно взять сколь угодно близким к 1. Поэтому

$$\lambda_1\geqslant\lambda_3. \tag{31}$$

Из неравенств (29) и (31) находим, что $\lambda_1=\lambda_2=\lambda_3$. Аналогично доказываются равенства $\mu_1=\mu_2=\mu_3$.

В дальнейшем будет показано, что символы λ_1, λ_2, λ_3, μ_1, μ_2, μ_3 являются конечными и положительными.

Из леммы 11 следует, что если при $x\to+\infty$ одна из трех функций (28) имеет конечный предел, то и две другие из них при $x\to+\infty$ имеют тот же предел.

В главе 2 будет доказан *асимптотический закон распределения простых чисел,* который утверждает, что

$$\lim_{x\to+\infty}\frac{\pi(x)}{\frac{x}{\ln x}}=1.$$

Из леммы 11 следует, что этому результату эквивалентно каждое из двух следующих утверждений:

$$\lim_{x\to+\infty}\frac{\theta(x)}{x}=1,\quad \lim_{x\to+\infty}\frac{\psi(x)}{x}=1.$$

Лемма 12. *При любом действительном x разность* $[2x]-2[x]$ *равна либо* 0, *либо* 1.

Доказательство. Так как $[x]=x-\{x\}$, то

$$[2x]=2x-\{2x\},\ 2[x]=2x-2\{x\}.$$

Вычитая, получим

$$[2x]-2[x]=2\{x\}-\{2x\}. \tag{32}$$

Поскольку $0\leqslant\{x\}<1$, то выполняются неравенства

$$-1<2\{x\}-\{2x\}<2. \tag{33}$$

С другой стороны, левая часть равенства (32) есть целое число. Поэтому из неравенств (33) следует, что разность $2\{x\}-\{2x\}$ может принимать только одно из двух значений 0 или 1, что ввиду равенства (32) доказывает утверждение леммы.

Перейдем к доказательству теоремы Чебышева.

По лемме 11 три функции (28) имеют общие нижние и верхние пределы. Обозначим их λ и μ.

1) Оценка сверху. Рассмотрим число

$$N=\binom{2n}{n}=\frac{(n+1)\ldots(2n)}{n!},\quad n\in\mathbf{N}. \tag{34}$$

Число $N\in\mathbf{N}$ как биномиальный коэффициент, причем N — наибольший из $2n+1$ биномиальных коэффициентов $\binom{2n}{k}$, $k=0, 1, \ldots, 2n$. Поэтому из равенства

$$\sum_{k=0}^{2n}\binom{2n}{k}=(1+1)^{2n}=2^{2n} \tag{35}$$

следует, что выполняются неравенства

$$N<2^{2n}<(2n+1)N. \tag{36}$$

В числитель дроби (34) входят все простые числа p такие, что $n<p\leqslant 2n$, и эти числа не входят в знаменатель той же дро-

би. Поэтому число N делится на все такие простые числа и, значит, делится на их произведение. Отсюда следует, что

$$N \geqslant \prod_{n<p\leqslant 2n} p. \tag{37}$$

Из неравенств (36) и (37) имеем

$$2^{2n} > \prod_{n<p\leqslant 2n} p.$$

Логарифмируя последнее неравенство, получим

$$2n \ln 2 > \sum_{n<p\leqslant 2n} \ln p = \theta(2n) - \theta(n). \tag{38}$$

Положим в неравенстве (38) последовательно $n=2^{l-1}$, $l=1, \ldots, k$, и сложим все полученные неравенства. В результате, замечая, что $\theta(1)=0$, приходим к неравенствам

$$\theta(2^k) < \sum_{l=1}^{k} 2^l \ln 2 < 2^{k+1} \ln 2. \tag{39}$$

Пусть $x>1$. Выберем натуральное число k, удовлетворяющим неравенствам $2^{k-1}\leqslant x<2^k$. Тогда неравенства (39) позволяют получить следующую оценку:

$$\theta(x) \leqslant \theta(2^k) < 2^{k+1} \ln 2 \leqslant 4x \ln 2, \quad x>1,$$

из которой находим, что

$$\mu \leqslant 4 \ln 2. \tag{40}$$

2) Оценка снизу. Число N, определенное равенством (34), можно представить в виде

$$N = \frac{(2n)!}{(n!)^2}$$

и поэтому, пользуясь леммой 8, найти его каноническое разложение на простые сомножители

$$N = \frac{(2n)!}{(n!)^2} = \prod_{p\leqslant 2n} p^{\beta_p}, \tag{41}$$

где

$$\beta_p = \beta_p(n) = \left(\left[\frac{2n}{p}\right] + \left[\frac{2n}{p^2}\right] + \ldots\right) - 2\left(\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots\right). \tag{42}$$

Так как $[\alpha]=0$ при $0<\alpha<1$, то в каждой из двух сумм в скобках в равенстве (42) все слагаемые после m_p-го, где $m_p=$

$=[\ln(2n)/\ln p]$, будут равны нулю. Поэтому, пользуясь леммой 12, находим

$$\beta_p = \sum_{k=1}^{m_p} \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right) \leqslant m_p. \tag{43}$$

Из равенства (27) имеем, что

$$e^{\psi(2n)} = \prod_{p \leqslant 2n} p^{m_p},$$

откуда ввиду равенства (41) и оценки (43) получаем, что $N < e^{\psi(2n)}$. Логарифмируя неравенство $2^{2n} < (2n+1)N$ (см. (36)), находим неравенства

$$2n \ln 2 - \ln(2n+1) < \ln N \leqslant \psi(2n). \tag{44}$$

Пусть $x \geqslant 2$. Положим в неравенствах (44) $n = \left[\frac{1}{2} x \right]$. Тогда $x - 2 < 2n \leqslant x$. Получим, что

$$\psi(x) \geqslant \psi(2n) > (x-2)\ln 2 - \ln(x+1),$$

или

$$\frac{\psi(x)}{x} > \ln 2 - \frac{2\ln 2}{x} - \frac{\ln(x+1)}{x},$$

откуда следует неравенство

$$\lambda \geqslant \ln 2. \tag{45}$$

Объединяя неравенства (40) и (45), приходим к неравенствам

$$\ln 2 \leqslant \lambda \leqslant \mu \leqslant 4 \ln 2.$$

Поскольку λ и μ общие нижние и верхние пределы трех функций (28), то

$$\ln 2 \leqslant \varliminf_{x \to +\infty} \frac{\pi(x)}{\frac{x}{\ln x}} \leqslant \varlimsup_{x \to +\infty} \frac{\pi(x)}{\frac{x}{\ln x}} \leqslant 4 \ln 2.$$

Уменьшая и увеличивая постоянные в этих оценках, если это необходимо, получим неравенства (24), справедливые при всех $x \geqslant 2$.

Теорема 2. *Существуют положительные постоянные α и β такие, что при всех $n \geqslant 2$ выполняются неравенства*

$$\alpha n \ln n < p_n < \beta n \ln n \tag{46}$$

где p_n — n-е простое число.

Доказательство. Положим в теореме Чебышева в неравенствах (24) $x=p_n$. Тогда

$$a\frac{p_n}{\ln p_n} < \pi(p_n) < b\frac{p_n}{\ln p_n}.$$

Но $\pi(p_n)=n$. Поэтому

$$a\frac{p_n}{\ln p_n} < n < b\frac{p_n}{\ln p_n}. \qquad (47)$$

Логарифмируя неравенство (47) и перемножая почленно получившееся неравенство и неравенство (47), находим

$$a\frac{p_n}{\ln p_n}(\ln a + \ln p_n - \ln\ln p_n) <$$

$$< n\ln n < b\frac{p_n}{\ln p_n}(\ln b + \ln p_n - \ln\ln p_n).$$

Из этих неравенств получаем, что при некоторых положительных α и β выполняются неравенства

$$\frac{1}{\beta}p_n < n\ln n < \frac{1}{\alpha}p_n, \quad n \geqslant 2,$$

из которых следуют неравенства (46).

Из доказанной теоремы легко получается новое доказательство утверждения о том, что ряд чисел, обратных простым числам, расходится.

Чебышев установил более точные границы для отношения

$$\frac{\pi(x)}{\frac{x}{\ln x}} \qquad (48)$$

чем в приведенном доказательстве неравенства (24). Более того, в статье, опубликованной в 1848 г., он доказал, что если существует предел отношения (48) при $x\to+\infty$, то этот предел должен быть равен 1. Но доказать существования предела он не смог.

В той же работе Чебышев показал, что при условии существования предела отношения (48) в формуле Лежандра (22) лучшим значением для постоянной B должно быть $B=1$, а не указанное Лежандром значение $B=1{,}08366$. Он также установил, что функция

$$\int_2^x \frac{dt}{\ln t},$$

рассмотренная им независимо от Гаусса, приближает $\pi(x)$ лучше, чем функция $x/\ln x$.

Своими работами П. Л. Чебышев внес самый существенный вклад со времен Евклида в изучение распределения простых

чисел. Его работы были очень высоко оценены математиками во всем мире.

Асимптотический закон распределения простых чисел (существование предела отношения (48) при $x \to +\infty$) был установлен с помощью аналитических методов только почти через полвека после работ Чебышева.

ЗАМЕЧАНИЯ

С вопросами делимости чисел можно ознакомиться по книгам И. М. Виноградова [2], Г. Хассе [13] и К. Чандрасекхарана [16]. С элементарными результатами о распределении простых чисел — по книгам К. Прахара [9], А. Е. Ингама [7], Э. Троста [10] и К. Чандрасекхарана [16]. Работы П. Л. Чебышева о простых числах содержатся в т. 1 его собрания сочинений [19].

Метод решета, которым в § 3 была доказана теорема Эйлера, в работах В. Бруна (1885—1981), А. А. Бухштаба (р. 1905), А. Сельберга (р. 1917), Ю. В. Линника и других математиков получил существенное развитие и обобщение. С его помощью установлено много результатов о распределении простых чисел, часто не окончательных, но пока не получаемых с помощью аналитических методов. Отметим лишь некоторые из этих результатов, связанные с проблемой близнецов.

В. Брун в 1919 г. доказал, что ряд чисел, обратных простым числам-близнецам, либо конечен, либо сходится. Он также показал, что существует бесконечное множество пар чисел n и $n+2$, каждое из которых состоит не более чем из 9 простых множителей. А. А. Бухштаб в 1940 г. заменил число 9 на 4.

А. Реньи (1921—1970) в 1948 г. доказал, что существуют постоянная k и бесконечное множество пар p и $p+2$, где p — простое число, а $p+2$ состоит не более чем из k простых множителей. А. А. Бухштаб в 1965 г. показал, что в результате Реньи можно положить $k=3$, а Ван-Юань в 1973 г. снизил это число до 2.

В своей работе о простых числах (1850 г.) П. Л. Чебышев доказал постулат Бертрана, в котором утверждается, что при $n>3$ между числами n и $2n-2$ имеется простое число. Это предположение было высказано И. Бертраном (1822—1900), которому оно потребовалось в связи с его исследованиями по теории групп.

Чебышев также доказал, что начиная с некоторого x выполняется неравенство

$$0{,}92129 < \frac{\pi(x)}{x/\ln x} < 1{,}10555.$$

Многие авторы уточняли постоянные в этом неравенстве. Но доказать методом Чебышева существование предела

$\pi(x) \Big/ \frac{x}{\ln x}$ при $x \to +\infty$ они не смогли. Эта проблема была решена другими методами, использующими функции комплексного переменного.

ЗАДАЧИ

1) Пусть a, $b \in \mathbf{Z}$, $(a, b) = 1$. Доказать по индукции, что уравнение

$$ax + by = 1$$

разрешимо в целых числах.

2) С помощью результата задачи 1 дать другое доказательство леммы 3.

3) Пусть a, $b \in \mathbf{Z}$, $|a| + |b| \neq 0$, а $d = ax_0 + by_0$ — наименьшее положительное число вида $ax + by$, где x, $y \in \mathbf{Z}$. Доказать, что $d = (a, b)$.

4) Общим кратным нескольких целых чисел называется целое число, являющееся кратным каждого из этих чисел. Наименьшим общим кратным нескольких целых чисел называется наименьшее из их положительных общих кратных.

Доказать, что если натуральные числа $a_1, \ldots, a_k$ попарно взаимно просты, то их общее наименьшее кратное равно их произведению.

5) Пусть M_n — наименьшее общее кратное чисел $1, \ldots, n$. Доказать, что существует постоянная $c > 0$ такая, что $M_n < c^n$.

6) Пусть $m \geqslant 2$, а q_n — наименьшее общее кратное чисел

$$\frac{(mk)!}{(k!)^m}, \quad k = 1, \ldots, n.$$

Доказать, что существует постоянная $c = c(m) > 0$ такая, что

$$q_n < c^n, \quad n = 1, 2, \ldots.$$

7) Доказать, что если $2^n > (1+n)^k$, то среди чисел $1, 2, 3, \ldots, 2^n$ существует по крайней мере $k+1$ простое число. Тем самым будет получено новое доказательство бесконечности множества простых чисел.

8) Доказать, что среди чисел $1, 2, \ldots, N$ существует не более $\frac{3}{4}N$ чисел, делящихся на квадрат простого числа, и, значит, не менее $\frac{1}{4}N$ чисел, не делящихся на квадрат простого числа. Получить из этого утверждения еще одно доказательство бесконечности множества простых чисел.

9) Доказать, что

$$\sum_{p \leqslant n} \frac{\ln p}{p} = \ln n + O(1).$$

10) Установить неравенство

$$\sum_{p \mid n} \frac{\ln p}{p} < \ln \ln n + c,$$

где $c > 0$ — постоянная.

11) Функция Эйлера $\varphi(n)$ определяется как количество чисел среди $1, 2, \ldots, n$, взаимно простых с n.

Пусть $d \mid n$ и A_d — множество чисел a из совокупности $1, 2, \ldots, n$, удовлетворяющих условию $(a, n) = d$. Доказать, что количество элементов в A_d равно $\varphi(n/d)$, и вывести отсюда равенство

$$\sum_{d \mid n} \varphi(d) = n,$$

где суммирование ведется по всем натуральным числам d, делящим n.

12) Функция Мебиуса $\mu(n)$ определяется следующим образом: $\mu(1) = 1$, $\mu(n) = (-1)^r$, если n есть произведение r различных простых чисел, и $\mu(n) = 0$, если n делится на квадрат простого числа.

Доказать, что

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n > 1. \end{cases}$$

13) С помощью задач 11 и 12 доказать равенство

$$\varphi(n) = n \sum_{d \mid n} \frac{\mu(d)}{d}.$$

14) С помощью задачи 13 установить равенство

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

15) Пусть a и b — взаимно простые натуральные числа. Каждому числу r из совокупности

$$1, 2, 3, \ldots, ab$$

поставлены в соответствие два остатка u и v от деления его соответственно на a и b. Доказать, что

$$(r, ab) = 1$$

тогда и только тогда, когда

$$(u, a)=1 \text{ и } (v, b)=1.$$

С помощью этого утверждения установить при $(a, b)=1$ равенство

$$\varphi(ab)=\varphi(a)\varphi(b).$$

16) Доказать, что для простого числа p и натурального k выполняется равенство

$$\varphi(p^k)=p^k-p^{k-1}.$$

17) С помощью задач 15, 16 и основной теоремы арифметики доказать утверждение задачи 14.

18) Доказать, что

$$\lim_{m\to\infty}\frac{1}{m}\sum_{n\leqslant m}\frac{\varphi(n)}{n}=\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}.$$

19) Доказать, что существует постоянная $c>0$ такая, что между числами n и cn при любом $n\geqslant 1$ содержится простое число.

ГЛАВА 2

АСИМПТОТИЧЕСКИЙ ЗАКОН РАСПРЕДЕЛЕНИЯ ПРОСТЫХ ЧИСЕЛ

§ 1. Дзета-функция Римана

После работ Чебышева важнейшим стимулом для дальнейших исследований, связанных с распределением простых чисел, послужила работа Б. Римана, опубликованная в 1859 г. Риман установил связь между распределением простых чисел и свойствами функции

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s} \tag{1}$$

как функции комплексного переменного s, особенно с расположением ее нулей. Функция $\zeta(s)$ получила название дзета-функции Римана.

Работа Римана и развитие теории целых функций Ж. Адамаром подготовили появление доказательства асимптотического закона распределения простых чисел.

Теорема (*асимптотический закон распределения простых чисел*).

$$\lim_{x\to+\infty}\frac{\pi(x)}{\frac{x}{\ln x}}=1.$$

Эту теорему одновременно и независимо друг от друга доказали в 1896 г. Ж. Адамар и Ш. Ж. де ла Валле-Пуссен.

Для доказательства теоремы изучим некоторые свойства дзета-функции. Положим

$$s=\sigma+it,$$

где $\sigma=\operatorname{Re} s$ и $t=\operatorname{Im} s$ — действительная и мнимая части комплексной переменной s. Определим функцию x^s для $x>0$ равенством

$$x^s=e^{s\ln x}.$$

Тогда

$$n^s=n^\sigma n^{it}=n^\sigma e^{it\ln n},\quad |n^s|=n^\sigma.$$

Лемма 1. *Ряд* (1) *абсолютно сходится при* $\sigma>1$, *определяемая им функция* $\zeta(s)$ *является аналитической в области* $\sigma>1$, *а равенство* (1) *можно почленно дифференцировать в этой области.*

Доказательство. Абсолютная сходимость ряда (1) при $\sigma>1$ следует из равенства

$$\left|\frac{1}{n^s}\right| = \frac{1}{n^\sigma}.$$

По признаку Вейерштрасса равномерной сходимости рядов при $\delta>0$ в области $\sigma>1+\delta$ ряд (1) сходится равномерно. Поэтому по теореме Вейерштрасса о равномерно сходящихся рядах аналитических функций в этой области сумма ряда (1) является аналитической, и равенство (1) можно почленно дифференцировать. Ввиду произвольности δ последние утверждения справедливы в области $\sigma>1$.

Следствие. *В области* $\operatorname{Re} s=\sigma>1$ *выполняется равенство*

$$\zeta'(s) = -\sum_{n=2}^{\infty}\frac{\ln n}{n^s}. \tag{2}$$

Обозначим

$$\Lambda(n) = \begin{cases} \ln p & \text{при } n = p^k, \\ 0 & \text{при } n \neq p^k, \end{cases}$$

где p — простое число.

Функцию Чебышева $\psi(x)$, рассмотренную в гл. 1, можно представить в виде

$$\psi(x) = \sum_{n\leqslant x}\Lambda(n). \tag{3}$$

Лемма 2. *Дзета-функция не имеет нулей в области* $\operatorname{Re} s>1$, *и в этой области выполняется равенство*

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=2}^{\infty}\frac{\Lambda(n)}{n^s}. \tag{4}$$

Доказательство. Так как $|\Lambda(n)|\leqslant\ln n$, то ряд (4) равномерно сходится в области $\operatorname{Re} s>1+\delta$, $\delta>0$, и по теореме Вейерштрасса представляет в этой области аналитическую функцию. Отсюда следует ввиду произвольности δ, что правая часть равенства (4) аналитична в области $\operatorname{Re} s>1$. Поскольку

$$\left|\frac{\Lambda(n)}{n^s}\right| \leqslant \frac{\ln n}{n^\sigma},$$

то ряд (4) абсолютно сходится в области $\sigma>1$. Умножим ряд (4) на ряд (1). Это допустимо, так как оба ряда абсолютно сходятся в области $\sigma>1$. Тогда получим, что

$$\left(\sum_{l=1}^{\infty}\frac{1}{l^s}\right)\left(\sum_{k=2}^{\infty}\frac{\Lambda(k)}{k^s}\right) = \sum_{n=2}^{\infty}\frac{1}{n^s}\left(\sum_{kl=n}\Lambda(k)\right),$$

где в правой части во внутренней сумме суммирование распространяется на все натуральные значения k и l, произведение которых равно n. Действительно, после перемножения рядов в левой части равенства будем иметь сумму всевозможных слагаемых вида

$$\frac{1}{l^s}\,\frac{\Lambda(k)}{k^s}=\frac{\Lambda(k)}{n^s}.$$

Собирая все слагаемые с одинаковым значением $lk=n$ и суммируя по n, получим правую часть рассматриваемого равенства.

Функция $\Lambda(k)$ отлична от нуля только в случае, когда k есть степень простого числа. Поэтому для $n=p_1^{r_1}\ldots p_t^{r_t}$ имеем, что

$$\sum_{kl=n}\Lambda(k)=\sum_{i=1}^{t}\sum_{j=1}^{r_i}\Lambda(p_i^j)=\sum_{i=1}^{t}r_i\ln p_i=\ln n. \tag{5}$$

Следовательно,

$$\zeta(s)\sum_{k=2}^{\infty}\frac{\Lambda(k)}{k^s}=\sum_{n=2}^{\infty}\frac{\ln n}{n^s}=-\zeta'(s)$$

и равенство (4) имеет место во всех точках области $\operatorname{Re}s>1$, где $\zeta(s)\neq 0$. Ввиду единственности аналитического продолжения получаем, что функция $\zeta'(s)/\zeta(s)$ аналитична в области $\operatorname{Re}s>1$. Отсюда следует, что $\zeta(s)\neq 0$ в области $\operatorname{Re}s>1$, так как нулям функции $\zeta(s)$ соответствуют полюсы функции $\zeta'(s)/\zeta(s)$. Лемма доказана.

Теперь представим функцию $\zeta(s)$ в области $\sigma>1$ в виде бесконечного произведения по простым числам. Для этого докажем вспомогательное предложение.

Комплекснозначная функция $f(n)$ натурального аргумента n называется *вполне мультипликативной*, если $f(n)\not\equiv 0$ и

$$f(mn)=f(m)f(n)$$

при любых натуральных m и n.

Из равенства $f(n\cdot 1)=f(n)f(1)$ следует, что $f(1)=1$.

Лемма 3. *Пусть функция $f(n)$ вполне мультипликативна и ряд*

$$S=\sum_{n=1}^{\infty}f(n) \tag{6}$$

абсолютно сходится. Тогда выполняется равенство

$$S=\prod_{p}(1-f(p))^{-1}. \tag{7}$$

Доказательство. Заметим прежде всего, что $|f(n)|<1$ при любом натуральном $n>1$. В противном случае при каждом $m\in\mathbf{N}$

$$|f(n^m)|=|f(n)|^m\geqslant 1,$$

что противоречит сходимости ряда (6). Поэтому при каждом простом p ряд

$$\sum_{k=0}^{\infty} f(p^k)=\sum_{k=0}^{\infty} f^k(p)$$

абсолютно сходится, и его сумма как сумма бесконечно убывающей геометрической прогрессии равна $(1-f(p))^{-1}$. Перемножая конечное число таких рядов и используя то, что $f(n)$ есть вполне мультипликативная функция, получим

$$S(x)=\prod_{p\leqslant x}(1-f(p))^{-1}=\prod_{p\leqslant x}\sum_{k=0}^{\infty} f(p^k)=\sum_{l=1}^{\infty} f(n_l),$$

где в сумме в правой части равенства содержатся такие и только такие слагаемые $f(n_l)$, что все простые делители n_l не превосходят x. Следовательно, в разности

$$S-S(x)=\sum_{l=1}^{\infty} f(m_l)$$

остаются те и только те слагаемые $f(m_l)$, для которых у числа m_l имеется хотя бы один простой делитель $p>x$. Тогда

$$|S-S(x)|\ll\sum_{n>x}|f(n)|,$$

и из абсолютной сходимости ряда (6) следует, что

$$\lim_{x\to+\infty} S(x)=S.$$

Это доказывает, что бесконечное произведение (7) сходится и выполняется утверждение леммы.

Если в лемме 3 положить $f(n)=\dfrac{1}{n^s}$, то получим тождество, устанавливающее связь функции $\zeta(s)$ с простыми числами.

Тождество Эйлера. *В области* $\operatorname{Re} s>1$ *справедливо следующее представление функции* $\zeta(s)$ *в виде бесконечного произведения по всем простым числам:*

$$\zeta(s)=\prod_{p}(1-p^{-s})^{-1}. \tag{8}$$

Отметим, что утверждение леммы 2 можно получить также, вычисляя логарифмическую производную от обеих частей тождества Эйлера.

Важное значение в дальнейшем будут иметь некоторые свойства дзета-функции вблизи прямой $\operatorname{Re} s=1$, в частности, оценки сверху ее модуля $|\zeta(s)|$.

Простейшая из этих оценок получается с помощью ряда (1). Если $\sigma=\operatorname{Re} s>1$, то, пользуясь леммой 10 гл. 1, находим

$$|\zeta(s)|=\left|\sum_{n=1}^{\infty}\frac{1}{n^s}\right|\leqslant\sum_{n=1}^{\infty}\frac{1}{n^\sigma}\leqslant 1+\int_1^{\infty}\frac{dx}{x^\sigma}=$$

$$=1+\frac{1}{\sigma-1}=\frac{\sigma}{\sigma-1}. \tag{9}$$

Эта оценка, однако, является очень неточной для $s=\sigma+it$, удаленных достаточно далеко от точки $s=1$. Правая часть неравенства (9) при $s\to(1+it_0)$, $t_0\neq 0$, неограниченно возрастает, в то время как левая имеет конечный предел (это будет доказано ниже).

Для того чтобы изучить свойства дзета-функции в окрестности прямой $\sigma=1$, преобразуем ряд (1), определяющий $\zeta(s)$. Это преобразование основывается на следующей лемме.

Лемма 4 (преобразование Абеля). *Пусть* a_n, $n=1, 2, \ldots,$ — *последовательность комплексных чисел,* $x>1$,

$$A(x)=\sum_{n\leqslant x}a_n$$

а $g(t)$ — *комплекснозначная функция, непрерывно дифференцируемая на множестве* $1\leqslant t<+\infty$. *Тогда*

$$\sum_{n\leqslant x}a_n g(n)=A(x)\,g(x)-\int_1^x A(t)\,g'(t)\,dt, \tag{10}$$

если же

$$\lim_{x\to+\infty}A(x)\,g(x)=0,$$

то

$$\sum_{n=1}^{\infty}a_n g(n)=-\int_1^{+\infty}A(t)\,g'(t)\,dt, \tag{11}$$

при условии, что ряд в левой части равенства сходится.

Доказательство. Положим $A(0)=0$ и $B(x)$ равным левой части равенства (10). Тогда при любом натуральном N

$$B(N)=\sum_{n=1}^{N}a_n g(n)=\sum_{n=1}^{N}(A(n)-A(n-1))\,g(n)=$$

$$=\sum_{n=1}^{N}A(n)\,g(n)-\sum_{n=0}^{N-1}A(n)\,g(n+1)=$$

$$= A(N)\,g(N) - \sum_{n=1}^{N-1} A(n)\,(g(n+1) - g(n)),$$

так как $A(0) = 0$. Далее,

$$B(N) = A(N)\,g(N) - \sum_{n=1}^{N-1} A(n) \int_n^{n+1} g'(t)\,dt =$$

$$= A(N)\,g(N) - \int_1^N A(t)\,g'(t)\,dt,$$

поскольку функция $A(x)$ постоянна на каждом полуинтервале $n \leqslant t < n+1$. Следовательно, равенство (10) доказано при целых значениях x.

Пусть теперь $x \geqslant 1$ — произвольное число. Положим $N = [x]$; значит, $N \leqslant x < N+1$. Тогда $A(x) = A(N)$, $B(x) = B(N)$, а

$$\int_N^x A(t)\,g'(t)\,dt = A(N)\,(g(x) - g(N)) =$$

$$= A(x)\,g(x) - A(N)\,g(N).$$

Следовательно,

$$B(x) = B(N) = A(N)\,g(N) - \int_1^x A(t)\,g'(t)\,dt +$$

$$+ A(x)\,g(x) - A(N)\,g(N) = A(x)\,g(x) - \int_1^x A(t)\,g'(t)\,dt.$$

Тем самым доказано, что равенство (10) верно и для нецелых значений x.

Равенство (11) получается из равенства (10) переходом к пределу при $x \to +\infty$. Лемма доказана.

Пусть N — натуральное число. Положим в лемме 4 $a_n = 1$, $n = 1, 2, \ldots$, $g(x) = (x+N)^{-s}$. Тогда $A(x) = [x]$ и при $\sigma > 1$

$$\lim_{x \to \infty} A(x)\,g(x) = 0.$$

Поэтому из равенства (11) следует, что при $\operatorname{Re} s > 1$

$$\sum_{n=N+1}^{\infty} \frac{1}{n^s} = s \int_1^{+\infty} [x]\,(x+N)^{-s-1}\,dx =$$

$$= s\int_0^{+\infty} [x]\,(x+N)^{-s-1}\,dx = s\int_N^{+\infty} [x-N]\,x^{-s-1}\,dx =$$

$$= s\int_N^{+\infty} \frac{x-N-\{x\}}{x^{s+1}}\,dx = \frac{N^{1-s}}{s-1} - s\int_N^{+\infty} \frac{\{x\}}{x^{s+1}}\,dx.$$

Таким образом,

$$\zeta(s) = \sum_{n=1}^{N} \frac{1}{n^s} + \frac{N^{1-s}}{s-1} - s\int_N^{+\infty} \frac{\{x\}}{x^{s+1}}\,dx. \tag{12}$$

В частности, при $N=1$ получаем

$$\zeta(s) = 1 + \frac{1}{s-1} - s\int_1^{+\infty} \frac{\{x\}}{x^{s+1}}\,dx. \tag{13}$$

Перепишем равенство (13) следующим образом:

$$\zeta(s) = 1 + \frac{1}{s-1} - s\sum_{n=1}^{\infty}\int_n^{n+1} \frac{x-n}{x^{s+1}}\,dx. \tag{14}$$

Из неравенства

$$\left|\int_n^{n+1} \frac{x-n}{x^{s+1}}\,dx\right| \leqslant \frac{1}{n^{\sigma+1}}$$

следует, что ряд в правой части равенства (14) сходится равномерно в области $\sigma \geqslant \delta > 0$. Каждый из интегралов в равенстве (14) является аналитической функцией от s в той же области. Поэтому по теореме Вейерштрасса о равномерно сходящихся рядах аналитических функций правая часть равенства (14) есть аналитическая функция в области $\sigma \geqslant \delta$, $s \neq 1$, а ввиду произвольности δ и в области $\sigma > 0$, $s \neq 1$. В точке $s=1$ она имеет простой полюс с вычетом 1.

Напомним, что до сих пор функция $\zeta(s)$ была определена только при $\sigma > 1$ рядом (1). Из доказанного следует, что эту функцию можно аналитически продолжить в полосу $0 < \sigma \leqslant 1$, $s \neq 1$, полагая, что $\zeta(s)$ в этой полосе равна правой части равенства (13). Итак, доказано следующее утверждение.

Теорема 1. *Правая часть равенства* (13) *является аналитическим продолжением функции* $\zeta(s)$, *определенной равенством* (1), *в область* $\sigma > 0$. *В этой области* $\zeta(s)$ *имеет единственную особую точку* $s=1$, *являющуюся полюсом первого порядка с вычетом* 1.

Замечание. Риман в 1859 г. нашел аналитическое продолжение дзета-функции на всю комплексную плоскость. При этом значения дзета-функции, расположенные слева и справа

от прямой $\operatorname{Re} s = 1/2$, оказались связанными функциональным уравнением

$$\zeta(1-s) = 2^{1-s}\pi^{-s}\cos\frac{\pi s}{2}\Gamma(s)\zeta(s),$$

где $\Gamma(s)$ — гамма-функция Эйлера.

Из сказанного выше и единственности аналитического продолжения следует, что равенство (12) выполняется в области $\operatorname{Re} s > 0$ для каждого натурального N.

Лемма 5. *В области комплексной плоскости* $s = \sigma + it$,

$$|t| \geqslant 3,\ 1 \leqslant \sigma \leqslant 2 \tag{15}$$

выполняются неравенства

$$|\zeta(s)| \leqslant 6 \ln |t|,$$
$$|\zeta'(s)| \leqslant 8 \ln^2 |t|.$$

Заметим, что величины постоянных, стоящих перед логарифмами, для дальнейшего несущественны.

Доказательство. Положим в равенстве (12) $N = [|t|]$. Тогда по лемме 10 гл. 1 выполняется неравенство

$$\left|\sum_{n=1}^{N}\frac{1}{n^s}\right| \leqslant \sum_{n=1}^{N}\frac{1}{n^\sigma} \leqslant 1 + \int_1^N \frac{dx}{x} = 1 + \ln N < 2\ln|t|. \tag{16}$$

Так как все точки области (15) удалены от точки 1 на расстояние, не меньшее, чем 3, то $|s-1| \geqslant 3$ и

$$\left|\frac{N^{1-s}}{s-1}\right| \leqslant \frac{1}{3}N^{1-\sigma} \leqslant \frac{1}{3}. \tag{17}$$

Далее, так как $N \leqslant |t| < N+1$, то

$$\left|s\int_N^{+\infty}\frac{\{x\}}{x^{s+1}}\,dx\right| \leqslant (|t|+\sigma)\int_N^{+\infty}\frac{dx}{x^2} \leqslant \frac{|t|+2}{N} \leqslant$$
$$\leqslant \frac{|t|+2}{|t|-1} = 1 + \frac{3}{|t|-1} < 3. \tag{18}$$

С помощью оценок (16)—(18) из равенства (12) получаем неравенство

$$|\zeta(s)| \leqslant 2\ \ln|t| + 4 < 6\ \ln|t|.$$

Дифференцируя равенство (12), будем иметь

$$\zeta'(s) = -\sum_{n=1}^{N}\frac{\ln n}{n^s} - \frac{N^{1-s}}{(s-1)^2} - \frac{N^{1-s}\ln N}{s-1} -$$
$$-\int_N^{+\infty}\frac{\{x\}}{x^{s+1}}\,dx + s\int_N^{+\infty}\frac{\{x\}\ln x}{x^{s+1}}\,dx. \tag{19}$$

Функция, стоящая под знаком интеграла в равенстве (12), разрывна в целых точках, однако возможность дифференцирования под знаком интеграла легко проверяется. Действительно,

$$\int_N^\infty \frac{\{x\}}{x^{s+1}}\,dx = \sum_{n=N}^{\infty} \int_n^{n+1} \frac{x-n}{x^{s+1}}\,dx,$$

и, как было доказано ранее, ряд, стоящий в правой части, сходится равномерно в области (15), а его члены — аналитические функции. Поэтому ряд можно почленно продифференцировать:

$$\frac{d}{ds} \sum_{n=N}^{\infty} \int_n^{n+1} \frac{x-n}{x^{s+1}}\,dx = -\sum_{n=N}^{\infty} \int_n^{n+1} \frac{x-n}{x^{s+1}} \ln x\,dx = -\int_N^{+\infty} \frac{\{x\}\ln x}{x^{s+1}}\,dx.$$

Из неравенства (17) следуют оценки

$$\left|\frac{N^{1-s}}{(s-1)^2}\right| \leqslant \frac{1}{9}, \quad \left|\frac{N^{1-s}\ln N}{s-1}\right| \leqslant \frac{1}{3}\ln N \leqslant \frac{1}{3}\ln|t|. \tag{20}$$

Кроме того, выполняются неравенства

$$\left|\int_N^{+\infty} \frac{\{x\}}{x^{s+1}}\,dx\right| \leqslant \int_N^{+\infty} \frac{dx}{x^2} = \frac{1}{N} \leqslant \frac{1}{|t|-1} \leqslant \frac{1}{2}, \tag{21}$$

$$\left|s\int_N^{+\infty} \frac{t\{x\}\ln x}{x^{s+1}}\,dx\right| \leqslant (|t|+2)\int_N^{+\infty} \frac{\ln x}{x^2}\,dx =$$

$$= -(|t|+2)\left(\frac{\ln x}{x}+\frac{1}{x}\right)\Big|_N^{+\infty} = (|t|+2)\left(\frac{\ln N}{N}+\frac{1}{N}\right) \leqslant$$

$$\leqslant \frac{|t|+2}{|t|-1}(\ln|t|+1) < 3(\ln|t|+1). \tag{22}$$

Далее, функция $\frac{\ln x}{x}$ монотонно убывает при $x \geqslant e$. Поэтому в области (15) по лемме 10 гл. I выполняется неравенство

$$\left|\sum_{n=2}^{N} \frac{\ln n}{n^s}\right| \leqslant \sum_{n=2}^{N} \frac{\ln n}{n} \leqslant \frac{\ln 2}{2} + \frac{\ln 3}{3} + \int_3^N \frac{\ln x}{x}\,dx =$$

$$= \frac{\ln 2}{2} + \frac{\ln 3}{3} + \frac{\ln^2 N}{2} - \frac{\ln^2 3}{2} < \ln^2|t|. \tag{23}$$

Подставляя в равенство (19) оценки (20) — (23), находим, что

$$|\zeta'(s)| < \ln^2|t| + \frac{1}{9} + \frac{1}{3}\ln|t| + \frac{1}{2} + 3(\ln|t|+1) < 8\ln^2|t|.$$

Лемма доказана.

§ 2. Нули дзета-функции

Важнейшую роль в изучении распределения простых чисел играет информация о расположении нулей дзета-функции в области $0 \leqslant \sigma \leqslant 1$. Область $0 \leqslant \sigma \leqslant 1$ называется *критической полосой* дзета-функции.

В 1859 г. Риман выдвинул предположение, что все нули дзета-функции, расположенные в критической полосе, лежат на прямой $\sigma = 1/2$. Гипотеза Римана к настоящему времени не доказана и не опровергнута. Ее доказательство привело бы к существенному прогрессу в задачах, связанных с распределением простых чисел.

Для доказательства асимптотического закона распределения простых чисел, которое будет изложено ниже, требуется установить, что $\zeta(s)$ не обращается в нуль на прямой $\sigma = 1$. Для этого докажем вспомогательное утверждение.

Лемма 6. *Пусть* $0 < r < 1$, а φ — *действительное число, тогда выполняется неравенство*

$$|(1-r)^3(1-re^{i\varphi})^4(1-re^{2i\varphi})|^{-1} \geqslant 1. \tag{24}$$

Доказательство. Для всех z из круга $|z| < 1$ имеет место разложение

$$-\ln(1-z) = \sum_{n=1}^{\infty} \frac{z^n}{n}.$$

Так как $\ln|t| = \operatorname{Re}\ln t$, то, обозначая $M(r, \varphi)$ левую часть неравенства (24), получим

$$\ln M(r, \varphi) = -3\ln(1-r) - 4\ln|1-re^{i\varphi}| - \ln|1-re^{2i\varphi}| =$$

$$= -3\ln(1-r) - 4\operatorname{Re}\ln(1-re^{i\varphi}) - \operatorname{Re}\ln(1-re^{2i\varphi}) =$$

$$= \sum_{n=1}^{\infty} \frac{r^n}{n} \operatorname{Re}(3 + 4e^{in\varphi} + e^{2in\varphi}) = \sum_{n=1}^{\infty} \frac{r^n}{n}(3 + 4\cos n\varphi + \cos 2n\varphi) =$$

$$= \sum_{n=1}^{\infty} \frac{2r^n}{n}(1 + \cos n\varphi)^2 \geqslant 0.$$

Следовательно, $M(r, \varphi) \geqslant 1$. Лемма доказана.

Лемма 7. *Функция* $\zeta(s)$ *не имеет нулей на прямой* $\operatorname{Re} s = 1$.

Доказательство. Пусть $\sigma > 1$. Из тождества Эйлера (8) следует, что

$$|\zeta^3(\sigma)\zeta^4(\sigma + it)\zeta(\sigma + 2it)| =$$

$$= \prod_p |(1-p^{-\sigma})^3(1-p^{-(\sigma-it)})^4(1-p^{-\sigma-2it})|^{-1}. \tag{25}$$

Полагая в лемме 6 $r = p^{-\sigma}$ и $e^{i\varphi} = p^{-it}$, ввиду неравенства (24) получим, что каждый сомножитель в произведении (25) не меньше, чем 1. Поэтому

$$|\zeta^3(\sigma)\zeta^4(\sigma + it)\zeta(\sigma + 2it)| \geqslant 1. \tag{26}$$

Предположим, вопреки утверждению леммы, что $\zeta(1 + it_0) = 0$, $t_0 \neq 0$. Ввиду того, что $\zeta(s)$ является аналитической функцией в точке $s = 1 + it_0$ будем иметь

$$\zeta(\sigma + it_0) = O(\sigma - 1),\ \sigma \to 1. \tag{27}$$

Из неравенства (9) следует, что при $1 < \sigma \leqslant 2$ выполняется неравенство

$$|\zeta(\sigma)| \leqslant \frac{\sigma}{\sigma - 1} \leqslant \frac{2}{\sigma - 1}. \tag{28}$$

Из неравенства (27) и неравенства (28) получаем оценку

$$\zeta^3(\sigma)\zeta^4(\sigma + it_0) = O(\sigma - 1),\quad \sigma \to 1. \tag{29}$$

Но функция $\zeta(\sigma + 2it_0)$ непрерывна и, следовательно, ограничена на отрезке $1 \leqslant \sigma \leqslant 2$. Поэтому неравенство (26) и оценка (29) при $\sigma \to 1 + 0$ противоречивы. Полученное противоречие доказывает утверждение леммы.

Неравенство (26) было основным в доказательстве леммы 7. С его помощью, поскольку известны оценки сверху для $|\zeta(\sigma)|$ и $|\zeta(\sigma + 2it)|$, можно оценить снизу $|\zeta(\sigma + it)|$, а также доказать следующую лемму.

Лемма 8. *В области комплексной плоскости* $s = \sigma + it$,

$$|t| \geqslant 3,\ 1 \leqslant \sigma \leqslant 2,$$

выполняется неравенство

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \leqslant c \ln^9 |t|,$$

где $c = 2^{23}$.

Заметим, что величина постоянной c не существенна для доказательства асимптотического закона.

Доказательство. Для действительных σ и t, удовлетворяющих неравенствам

$$2 \geqslant \sigma \geqslant 1 + \frac{1}{c \ln^9 |t|} = \sigma_1,\ |t| \geqslant 3,\ c = 2^{23},$$

ввиду оценки (28) выполняется неравенство

$$|\zeta(\sigma)| \leqslant \frac{2}{\sigma - 1} \leqslant 2c \ln^9 |t|, \tag{30}$$

а по лемме 5 — неравенство

$$|\zeta(\sigma + 2it)| \leqslant 6 \ln(2|t|) < 16 \ln|t| \tag{31}$$

Из неравенств (26), (30) и (31) получаем, что

$$|\zeta(\sigma+it)| \geqslant |\zeta(\sigma)|^{-\frac{3}{4}} |\zeta(\sigma+2it)|^{-\frac{1}{4}} \geqslant$$

$$\geqslant \frac{1}{2}(2c)^{-\frac{3}{4}} \ln^{-7}|t| = 16c^{-1}\ln^{-7}|t|. \tag{32}$$

Для σ из области $1 \leqslant \sigma \leqslant \sigma_1$, пользуясь леммой 5, находим

$$|\zeta(\sigma+it) - \zeta(\sigma_1+it)| = \left|\int_{\sigma}^{\sigma_1} \zeta'(u+it)\,du\right| \leqslant$$

$$\leqslant 8(\sigma_1-\sigma)\ln^2|t| \leqslant 8c^{-1}\ln^{-7}|t|. \tag{33}$$

Из неравенства (33) и оценки (32), в которой положено $\sigma = \sigma_1$, следует, что

$$|\zeta(\sigma+it)| \geqslant |\zeta(\sigma_1+it)| - |\zeta(\sigma_1+it) - \zeta(\sigma+it)| \geqslant$$

$$\geqslant 16c^{-1}\ln^{-7}|t| - 8c^{-1}\ln^{-7}|t| = 8c^{-1}\ln^{-7}|t|.$$

Вместе с оценкой (32) это означает, что для всех σ и t из области

$$1 \leqslant \sigma \leqslant 2, \quad |t| \geqslant 3$$

выполняется неравенство

$$|\zeta(\sigma+it)| \geqslant 8c^{-1}\ln^{-7}|t|. \tag{34}$$

Из неравенства (34) и леммы 5 имеем

$$\left|\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)}\right| \leqslant \frac{8\ln^2|t|}{8c^{-1}\ln^{-7}|t|} = c\ln^9|t|.$$

Лемма доказана.

§ 3. Доказательство асимптотического закона распределения простых чисел

По лемме 11 из гл. 1 для установления асимптотического соотношения

$$\pi(x) \sim \frac{x}{\ln x}, \quad x \to +\infty,$$

достаточно доказать, что $\psi(x) \sim x$ при $x \to +\infty$. По причинам, которые выяснятся несколько позднее, удобнее вместо $\psi(x)$ рассматривать функцию

$$\omega(x) = \int_1^x \frac{\psi(t)}{t}\,dt. \tag{35}$$

Для доказательства асимптотического закона достаточно доказать асимптотическое равенство

$$\omega(x) = x + o(x), \quad x \to +\infty. \tag{36}$$

Действительно, допустим, что это равенство доказано. Пусть ε произвольное число, такое, что $0 < \varepsilon < 1$. Тогда ввиду монотонности функции $\psi(t)$ находим

$$\omega((1+\varepsilon)x) - \omega(x) = \int_x^{(1+\varepsilon)x} \frac{\psi(t)}{t}\, dt \geqslant \psi(x) \int_x^{(1+\varepsilon)x} \frac{dt}{t} =$$

$$= \psi(x) \ln(1+\varepsilon),$$

откуда, пользуясь равенством (36), получаем

$$\overline{\lim_{x\to+\infty}} \frac{\psi(x)}{x} \leqslant \frac{1}{\ln(1+\varepsilon)} \lim_{x\to+\infty} \frac{\omega((1+\varepsilon)x) - \omega(x)}{x} = \frac{\varepsilon}{\ln(1+\varepsilon)}.$$

Так как это неравенство верно при любом положительном ε, то, переходя к пределу при $\varepsilon \to +0$, будем иметь, что

$$\overline{\lim_{x\to+\infty}} \frac{\psi(x)}{x} \leqslant 1.$$

Аналогично получается оценка и для нижнего предела. Имеем

$$\omega(x) - \omega((1-\varepsilon)x) = \int_{(1-\varepsilon)x}^{x} \frac{\psi(t)}{t}\, dt \leqslant$$

$$\leqslant \psi(x) \int_{(1-\varepsilon)x}^{x} \frac{dt}{t} = \psi(x) \ln \frac{1}{1-\varepsilon},$$

откуда следует, что

$$\underline{\lim_{x\to+\infty}} \frac{\psi(x)}{x} \geqslant \frac{1}{-\ln(1-\varepsilon)} \lim_{x\to+\infty} \frac{\omega(x) - \omega((1-\varepsilon)x)}{x} = \frac{\varepsilon}{-\ln(1-\varepsilon)},$$

а после перехода к пределу при $\varepsilon \to +0$

$$\underline{\lim_{x\to+\infty}} \frac{\psi(x)}{x} \geqslant 1.$$

Из неравенств

$$1 \leqslant \underline{\lim_{x\to+\infty}} \frac{\psi(x)}{x} \leqslant \overline{\lim_{x\to+\infty}} \frac{\psi(x)}{x} \leqslant 1$$

следует, что предел отношения $\psi(x)/x$ при $x \to +\infty$ существует и равен 1.

В следующих двух леммах будет найдено интегральное представление функции $\omega(x)$, связывающее эту функцию с

дзета-функцией Римана. Дальнейшее исследование полученного интеграла приведет к установлению асимптотики для $\omega(x)$.

Лемма 9. *При положительных a и b справедливы равенства*

$$\frac{1}{2\pi i}\int\limits_{a-i\infty}^{a+i\infty}\frac{b^s}{s^2}\,ds=\begin{cases}\ln b & \text{при } b\geqslant 1,\\ 0 & \text{при } 0<b<1,\end{cases} \tag{37}$$

где интеграл вычисляется по вертикальной прямой $\operatorname{Re} s=a$.

Доказательство. Из равенства

$$\left|\frac{b^s}{s^2}\right|=\frac{b^a}{a^2+t^2},\quad s=a+it,$$

следует, что интеграл (37) абсолютно сходится.

Рассмотрим при $b\geqslant 1$ интеграл

$$I_1(u)=\frac{1}{2\pi i}\int\limits_{\Gamma_1}\frac{b^s}{s^2}\,ds,\quad u>0,$$

где Γ_1 — замкнутый контур, состоящий из отрезка с концами в точках $a-iu$ и $a+iu$, параллельного мнимой оси, и дуги окружности

$$C_1:\begin{cases}|s|=\sqrt{a^2+u^2},\\ \operatorname{Re} s\leqslant a\end{cases}$$

(рис. 1).

Подынтегральная функция имеет полюс порядка 2 в точке $s=0$ с вычетом $\ln b$, поскольку

$$b^s=e^{s\ln b}=1+s\ln b+\frac{s^2\ln^2 b}{2!}+\ldots.$$

Отсюда по теореме Коши о вычетах

$$I_1(u)=\ln b.$$

Следовательно,

$$\frac{1}{2\pi i}\int\limits_{a-iu}^{a+i}\frac{b^s}{s^2}\,ds=\ln b-\frac{1}{2\pi i}\int\limits_{C_1}\frac{b^s}{s^2}\,ds. \tag{38}$$

Так как при $b\geqslant 1$ на кривой C_1 выполняется неравенство $|b^s|=b^{\operatorname{Re} s}\leqslant b^a$ и

$$\left|\frac{1}{s^2}\right|=\frac{1}{|s|^2}=\frac{1}{a^2+u^2},$$

то

$$\left|\frac{1}{2\pi i}\int\limits_{C_1}\frac{b^s}{s^2}\,ds\right|\leqslant\sqrt{a^2+u^2}\cdot b^a\cdot\frac{1}{a^2+u^2}\leqslant\frac{b^a}{u}.$$

Поэтому

$$\lim_{u\to+\infty}\frac{1}{2\pi i}\int_{C_1}\frac{b^s}{s^2}\,ds=0,$$

и в соответствии с равенством (38)

$$\lim_{u\to+\infty}\frac{1}{2\pi i}\int_{a-iu}^{a+iu}\frac{b^s}{s^2}\,ds=\ln b.$$

Тем самым равенство (37) в случае $b\geqslant 1$ доказано.

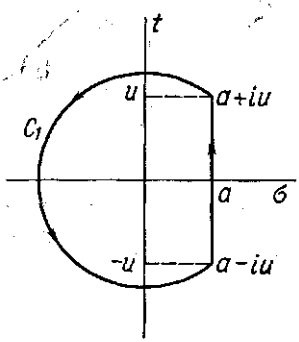

Рис. 1

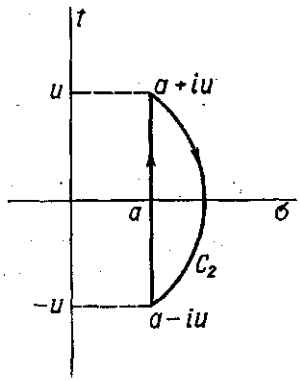

Рис. 2

В случае, когда b удовлетворяет неравенствам $0<b<1$, рассмотрим интеграл

$$I_2(u)=\frac{1}{2\pi i}\int_{\Gamma_2}\frac{b^s}{s^2}\,ds,$$

где контур Γ_2 также состоит из отрезка с концами в точках $a-iu$ и $a+iu$ и дуги окружности

$$C_2:\begin{cases}|s|=\sqrt{a^2+u^2},\\ \operatorname{Re}s\geqslant a\end{cases}$$

(рис. 2).

Подынтегральная функция b^s/s^2 является аналитической внутри контура Γ_2. Поэтому по теореме Коши

$$\frac{1}{2\pi i}\int_{\Gamma_2}\frac{b^s}{s^2}\,ds=0$$

и

$$\frac{1}{2\pi i}\int_{a-iu}^{a+iu}\frac{b^s}{s^2}\,ds=-\frac{1}{2\pi i}\int_{C_2}\frac{b^s}{s^2}\,ds.$$

Если b таково, что $0 < b < 1$, то на контуре C_2 выполняется неравенство

$$|b^s| = b^{\operatorname{Re} s} \leqslant b^a.$$

Следовательно,

$$\left| \frac{1}{2\pi i} \int\limits_{a-iu}^{a+iu} \frac{b^s}{s^2}\, ds \right| = \left| \frac{1}{2\pi i} \int\limits_{C_2} \frac{b^s}{s^2} ds \right| \leqslant \sqrt{a^2+u^2} \cdot b^a \cdot \frac{1}{a^2+u^2} \leqslant \frac{b^a}{u},$$

и, значит,

$$\lim_{u \to +\infty} \frac{1}{2\pi i} \int\limits_{a-iu}^{a+iu} \frac{b^s}{s^2}\, ds = 0.$$

Это доказывает равенство (37) во втором случае. Лемма доказана.

Пользуясь леммой 9, получим интегральное представление функции $\omega(x)$, определенной посредством (35).

Лемма 10. *При $a > 1$ и $x \geqslant 2$ выполняется равенство*

$$\omega(x) = \frac{1}{2\pi i} \int\limits_{a-i\infty}^{a+i\infty} \left(-\frac{\zeta'(s)}{\zeta(s)} \right) \frac{x^s}{s^2}\, ds, \tag{39}$$

где интегрирование ведется по прямой $\operatorname{Re} s = a$. Интеграл (39) абсолютно сходится.

Доказательство. Из леммы 2 получаем, что на прямой $\operatorname{Re} s = a$ выполняется неравенство

$$\left| \frac{\zeta'(s)}{\zeta(s)} \right| \leqslant \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^a} \leqslant \sum_{n=1}^{\infty} \frac{\ln n}{n^a},$$

откуда следует, что интеграл (39) абсолютно сходится.

Положим в лемме 4 $a_n = \Lambda(n)$ и $g(t) = \ln(x/t)$. Тогда $A(t) = \psi(t)$, и из равенства (10) находим

$$\sum_{n \leqslant x} \Lambda(n) \ln \frac{x}{n} = \psi(x) \cdot \ln 1 + \int\limits_1^x \frac{\psi(t)}{t}\, dt = \omega(x). \tag{40}$$

По лемме 9 имеют место равенства

$$\frac{1}{2\pi i} \int\limits_{a-i\infty}^{a+i\infty} \left(\frac{x}{n} \right)^s \frac{1}{s^2}\, ds = \begin{cases} \ln \dfrac{x}{n} & \text{при } n \leqslant x, \\ 0 & \text{при } n > x, \end{cases} \tag{41}$$

а из леммы 2 следует, что

$$\left(-\frac{\zeta'(s)}{\zeta(s)} \right) \frac{x^s}{s^2} = \sum_{n=1}^{\infty} \Lambda(n) \left(\frac{x}{n} \right)^s \frac{1}{s^2}. \tag{42}$$

Если ряд (42) проинтегрировать почленно по вертикальной прямой $\operatorname{Re} s = a$, то ввиду равенств (40) и (41) и получится интегральное представление (39) для функции $\omega(x)$. Обоснуем только возможность почленного интегрирования.

На прямой $\operatorname{Re} s = a$ ряд в правой части равенства (42) сходится равномерно по s по признаку Вейерштрасса равномерной сходимости рядов, что следует из оценки

$$\left|\frac{\Lambda(n)}{s^2}\left(\frac{x}{n}\right)^s\right| \leqslant \frac{\ln n}{a^2}\left(\frac{x}{n}\right)^a,$$

поскольку по условию $a > 1$. Отсюда для каждого $u > 0$, интегрируя почленно ряд (42) по отрезку с концами в точках $a - iu$ и $a + iu$, имеем, что

$$\frac{1}{2\pi i}\int\limits_{a-iu}^{a+iu}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\frac{x^s}{s^2}\,ds = \sum_{n=1}^{\infty}\frac{1}{2\pi i}\int\limits_{a-iu}^{a+iu}\frac{\Lambda(n)}{s^2}\left(\frac{x}{n}\right)^s ds. \quad (43)$$

Из оценки

$$\left|\frac{1}{2\pi i}\int\limits_{a-iu}^{a+iu}\frac{\Lambda(n)}{s^2}\left(\frac{x}{n}\right)^s ds\right| \leqslant \frac{\ln n}{2\pi}\left(\frac{x}{n}\right)^a\int\limits_{-\infty}^{+\infty}\frac{dt}{a^2+t^2} = \frac{\ln n}{2a}\left(\frac{x}{n}\right)^a$$

следует, что ряд в правой части равенства (43) сходится на множестве $u > 0$ равномерно по u. Поэтому в равенстве (43) можно перейти к пределу при $u \to +\infty$. Тогда пользуясь равенствами (40) и (41), получим

$$\frac{1}{2\pi i}\int\limits_{a-i\infty}^{a+i\infty}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\frac{x^s}{s^2}\,ds = \sum_{n=1}^{\infty}\frac{1}{2\pi i}\int\limits_{a-i\infty}^{a+i\infty}\Lambda(n)\left(\frac{x}{n}\right)^s\frac{ds}{s^2} =$$

$$= \sum_{n\leqslant x}\Lambda(n)\ln\frac{x}{n} = \omega(x).$$

Лемма доказана.

Можно показать, что при $a > 1$ и нецелом $x > 2$

$$\psi(x) = \frac{1}{2\pi i}\int\limits_{a-i\infty}^{a+i\infty}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\frac{x^s}{s}\,ds. \quad (44)$$

Однако для доказательства асимптотического закона интеграл (39) использовать проще ввиду его абсолютной сходимости. В этом и состоит причина, из-за которой в рассматриваемом доказательстве асимптотического закона используется функция $\omega(x)$, а не функция $\psi(x)$.

На контуре $\operatorname{Re} s = a$ справедливо равенство

$$|x^s| = x^a,$$

из которого следует, что чем левее расположен контур интегрирования в интеграле (39), тем меньшие значения при больших x

принимает модуль функции x^s. Будем стремиться перенести контур интегрирования по возможности левее. Препятствием к этому будут служить особые точки подынтегральной функции. Первой из них будет точка $s=1$ — полюс функции $\zeta(s)$, а следовательно, и функции $\frac{\zeta'(s)}{\zeta(s)}$. Вычет в этой точке дает главный член асимптотики для $\omega(x)$. Остальные особые точки лежат в нулях функции $\zeta(s)$. Имеющаяся в нашем распоряжении информация о нулях, а именно то, что они отсутствуют на прямой $\operatorname{Re} s=1$, позволит получить асимптотическое равенство $\omega(x)=x+o(x)$.

Улучшение остаточного члена $o(x)$ связано с возможностью дальнейшего продвижения контура интегрирования влево, а значит, с получением информации о расположении нулей дзета-функции Римана левее прямой $\operatorname{Re} s=1$. Известно, что в критической полосе $0\leqslant \operatorname{Re} s\leqslant 1$ функция $\zeta(s)$ имеет бесконечное множество нулей, а из функционального уравнения для $\zeta(s)$ следует, что нули ее в критической полосе расположены симметрично относительно прямой $\operatorname{Re} s=1/2$. Справедливость гипотезы Римана о том, что все нули дзета-функции в критической полосе лежат на прямой $\operatorname{Re} s=1/2$, дала бы возможность сдвинуть контур интегрирования достаточно близко к прямой $\operatorname{Re} s=1/2$, что привело бы к наилучшей оценке остаточного члена (см. дополнение 1).

Обозначим $\Gamma(T,\eta)$, $T>0$, $0<\eta<1$, ломаную линию (рис. 3), состоящую из отрезков прямых, соединяющих последовательно точки $1-i\infty$, G, F, E, D, $1+i\infty$, т. е. точки $1-i\infty$, $1-iT$, $\eta-iT$, $\eta+iT$, $1+iT$, $1+i\infty$.

Лемма 11. *Пусть функция $\zeta(s)$ не обращается в нуль в замкнутом прямоугольнике $\eta\leqslant\sigma\leqslant 1$, $-T\leqslant t\leqslant T$ $(0<\eta<1$, $T>0)$. Тогда выполняется равенство*

$$\omega(x)=x(1+R(x)),$$

где

$$R(x)=\frac{1}{2\pi i}\int\limits_{\Gamma(T,\eta)}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\frac{x^{s-1}}{s^2}\,ds. \tag{45}$$

Доказательство. При $U>T$ обозначим $\Gamma(U,T,\eta)$ контур (рис. 4), являющийся периметром многоугольника P с вершинами A, B, C, D, E, F, G, H, т. е. вершинами $2-iU$, $2+iU$, $1+iU$, $1+iT$, $\eta+iT$, $\eta-iT$, $1-iT$, $1-iU$, $2-iU$.

Как было доказано в § 1, 2, функция $\zeta(s)$ не обращается в нуль при $\sigma\geqslant 1$ и в полуплоскости $\sigma>0$ не имеет особых точек, кроме простого полюса в точке $s=1$ с вычетом 1. Поэтому

$$\zeta(s)=\frac{1}{s-1}+f(s),$$

где $f(s)$ — аналитическая функция при $\sigma > 0$, а

$$\frac{\zeta'(s)}{\zeta(s)} = -\frac{1-(s-1)^2 f'(s)}{1+(s-1)f(s)} \cdot \frac{1}{s-1}.$$

Следовательно, функция $-\frac{\zeta'(s)}{\zeta(s)} \frac{x^s}{s^2}$ в многоугольнике P имеет единственную особую точку $s=1$ — полюс первого порядка с вычетом x, и по теореме Коши о вычетах

$$\frac{1}{2\pi i} \int\limits_{\Gamma(U,T,\eta)} \left(-\frac{\zeta'(s)}{\zeta(s)}\right) \frac{x^s}{s^2} ds = x. \tag{46}$$

Оценим интеграл (46) по отрезкам BC и HA. По лемме 8

$$\left| \frac{1}{2\pi i} \int\limits_{2+iU}^{1+iU} \left(-\frac{\zeta'(s)}{\zeta(s)}\right) \frac{x^s}{s^2} ds \right| < c \frac{\ln^9 U}{U^2} x^2. \tag{47}$$

Такая же оценка справедлива для интеграла по отрезку HA.

Правая часть неравенства (47) стремится к нулю при $U \to +\infty$. Для завершения доказательства леммы осталось в

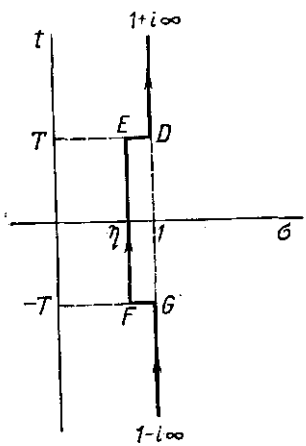

Рис. 3

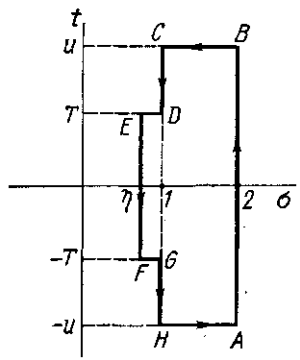

Рис. 4

равенстве (46) перейти к пределу при $U \to +\infty$ и для интеграла по прямой $2 - i\infty$, $2 + i\infty$ воспользоваться равенством (39).

Перейдем непосредственно к доказательству асимптотического закона. В начале параграфа было выяснено, что для доказательства асимптотического соотношения $\pi(x) \sim \frac{x}{\ln x}$ достаточно установить, что $\omega(x) \sim x$. Для этого же достаточно доказать, что в лемме 11 $R(x) = o(1)$. Поэтому оценим сверху $|R(x)|$. Путь интегрирования в интеграле (45) изображен на рис. 3.

Пусть $\varepsilon>0$ — произвольное число. Из оценки

$$\left|\frac{\zeta'(1+it)}{\zeta(1+it)}\,\frac{x^{it}}{(1+it)^2}\right|\leqslant\frac{c\ln^9|t|}{1+t^2},$$

справедливой при $|t|\geqslant 3$, следует, что можно выбрать число $T=T(\varepsilon)$, $T>3$, не зависящее от x, так, чтобы выполнялись неравенства

$$J_1=\left|\frac{1}{2\pi i}\int\limits_{1+iT}^{1+i\infty}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\frac{x^{s-1}}{s^2}\,ds\right|\leqslant\frac{1}{2\pi}\int\limits_{T}^{+\infty}\frac{c\ln^9 t}{1+t^2}\,dt<\frac{\varepsilon}{5},\quad(48)$$

$$J_2=\left|\frac{1}{2\pi i}\int\limits_{1-i\infty}^{1-iT}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\frac{x^{s-1}}{s^2}\,ds\right|\leqslant\frac{1}{2\pi}\int\limits_{T}^{+\infty}\frac{c\ln^9 t|}{1+t^2}\,dt<\frac{\varepsilon}{5}.\quad(49)$$

По лемме 7 функция $\zeta(s)$ не имеет нулей на отрезке с концами в точках $1-iT$, $1+iT$. Поэтому можно выбрать число $\eta=\eta(T)$, $0<\eta<1$, так, чтобы в замкнутом прямоугольнике

$$\eta\leqslant\sigma\leqslant 1,\ -T\leqslant t\leqslant T$$

функция $\zeta(s)$ не обращалась в нуль. Функция

$$\left|\frac{\zeta'(s)}{\zeta(s)}\,\frac{1}{s^2}\right|$$

непрерывна на ломаной $DEFG$ (см. рис. 4). Следовательно, существует постоянная $M=M(T,\eta)$, такая, что в каждой точке этой ломаной справедливо неравенство

$$\left|\frac{\zeta'(s)}{\zeta(s)}\,\frac{1}{s^2}\right|\leqslant M.$$

Поэтому получаем неравенства

$$J_3=\left|\frac{1}{2\pi i}\int\limits_{1+iT}^{\eta+iT}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\frac{x^{s-1}}{s^2}\,ds\right|\leqslant$$

$$=\frac{1}{2\pi}M\int\limits_{\eta}^{1}x^{\sigma-1}\,d\sigma<\frac{M}{2\pi}\int\limits_{-\infty}^{1}x^{\sigma-1}\,d\sigma=\frac{M}{2\pi\ln x};$$

$$J_4=\left|\frac{1}{2\pi i}\int\limits_{\eta-iT}^{1-iT}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\frac{x^{s-1}}{s^2}\,ds\right|\leqslant\frac{1}{2\pi}M\int\limits_{-\infty}^{1}x^{\sigma-1}\,d\sigma=\frac{M}{2\pi\ln x};$$

$$J_5=\left|\frac{1}{2\pi i}\int\limits_{\eta-iT}^{\eta+iT}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\frac{x^{s-1}}{s^2}\,ds\right|\leqslant\frac{1}{2\pi}Mx^{\eta-1}\int\limits_{-T}^{T}dt=\frac{T}{\pi}Mx^{\eta-1}.$$

Из полученных неравенств следует, что существует $x_0=x_0(M,T,\eta)$ такое, что для $x>x_0$ выполняются неравенства

$$J_3 < \frac{\varepsilon}{5},\ J_4 < \frac{\varepsilon}{5},\ J_5 < \frac{\varepsilon}{5}. \tag{50}$$

Из неравенств (48) — (50) имеем, что для $x > x_0$

$$\left|\frac{\omega(x)}{x} - 1\right| = |R(x)| \leqslant J_1 + \ldots + J_5 < \varepsilon,$$

и поэтому $\lim\limits_{x \to +\infty} \frac{\omega(x)}{x} = 1,$

что завершает доказательство асимптотического закона распределения простых чисел.

Асимптотический закон позволяет получить асимптотическую формулу n-го простого числа.

Теорема 2. При $n \to \infty$

$$p_n \sim n \ln n,$$

где p_n — n-е простое число.

Доказательство. Из асимптотического закона следует, что при $n \to \infty$

$$n = \pi(p_n) \sim \frac{p_n}{\ln p_n},$$

или

$$n = \frac{p_n}{\ln p_n}(1 + \alpha_n),$$

где $\alpha_n \to 0$ при $n \to \infty$. Следовательно, при $n \to \infty$

$$n \ln n = \frac{p_n}{\ln p_n}(1 + \alpha_n)(\ln p_n - \ln \ln p_n + \ln(1 + \alpha_n)) \sim p_n.$$

Теорема доказана.

Этот результат усиливает теорему, доказанную в § 4 гл. 1.

Точнее, чем функцией $x/\ln x$, величина $\pi(x)$ приближается функцией

$$\operatorname{li} x = \int_2^x \frac{dt}{\ln t}, \tag{51}$$

которая при $x \to +\infty$ эквивалентна $x/\ln x$.

Изложенный в этой главе метод позволяет оценить величину остаточного члена в асимптотическом законе, т. е. $\pi(x) - \operatorname{li} x$.

ЗАМЕЧАНИЯ

Различные варианты доказательства асимптотического закона распределения простых чисел можно найти в книгах Г. Давенпорта [6], А. Е. Ингама [7], А. А. Карацубы [8], К. Прахара [9], К. Чандрасекхарана [16] и [17].

Долгое время не удавалось найти элементарное доказательство асимптотического закона (не использующее теорию функций комплексного переменного). В 1949 г. А. Сельберг и П. Эрдеш (р. 1913) получили такое доказательство. Элементарное доказательство асимптотического закона можно найти в книгах К. Прахара [9], Э. Троста [10] и К. Чандрасекхарана [17].

В классической работе Римана 1859 г. (единственной его работе по теории чисел) функция $\zeta(s)$ была аналитически продолжена на всю комплексную плоскость и было выведено ее функциональное уравнение. Оказалось при этом, что дзета-функция имеет единственную особую точку $s = 1$ — полюс первого порядка с вычетом 1.

Риман показал, что распределение простых чисел тесно связано со свойствами дзета-функции как функции комплексного переменного s, особенно с распределением ее нулей в критической полосе $0 \leqslant \sigma \leqslant 1$.

В той же работе Риман выдвинул ряд гипотез о нулях дзета-функции и среди них знаменитую гипотезу о том, что все нули $\zeta(s)$, расположенные в критической полосе, лежат на прямой $\sigma = 1/2$.

К настоящему времени эта гипотеза не доказана. Получены, однако, результаты, в некоторой степени подтверждающие ее справедливость.

Доказано, что по крайней мере одна треть нулей $\zeta(s)$ лежит на критической прямой $\sigma = 1/2$. Кроме того, с использованием вычислений на ЭВМ было доказано, что первые два миллиона нулей дзета-функции расположены в точности на прямой $\sigma = 1/2$.

Из асимптотического закона распределения простых чисел следует, что

$$\pi(x) = \operatorname{li} x + R(x), \quad R(x) = o\left(\frac{x}{\ln x}\right), \quad x \to +\infty,$$

где функция $\operatorname{li} x$ определена равенством (51). Функция $R(x)$ называется остаточным членом в асимптотическом законе.

Следующей задачей после доказательства асимптотического закона является получение оценки сверху для $|R(x)|$. Основным моментом при решении этой задачи является доказательство того, что дзета-функция не обращается в нуль на некотором множестве, лежащем левее прямой $\sigma = 1$.

В 1899 г. Валле-Пуссен доказал, что $\zeta(s)$ не обращается в нуль в области

$$\sigma > 1 - \frac{c_1}{\ln(|t| + 2)}$$

с некоторой постоянной $c_1 > 0$ и, исходя из этого, показал, что

$$R(x) = O\left(xe^{-c_2\sqrt{\ln x}}\right), \quad x \to +\infty. \tag{52}$$

Функция вида $e^{(\ln x)^\beta}$ при $0 < \beta < 1$ возрастает быстрее любой постоянной степени $\ln x$ и медленнее любой степенной функции. Поэтому из равенства (52) следует, что для любой постоянной $a > 0$

$$R(x) = O\left(\frac{x}{(\ln x)^a}\right), \quad x \to +\infty.$$

Результат Валле-Пуссена впоследствии неоднократно улучшался. Эти улучшения достигаются за счет нахождения более широкой области, лежащей левее прямой $\sigma = 1$, где функция $\zeta(s)$ не обращается в нуль.

И. М. Виноградов и Н. М. Коробов (р. 1917) доказали, что при $\alpha > 2/3$ существует постоянная $b = b(\alpha) > 0$, такая, что $\zeta(s)$ не обращается в нуль в области

$$\sigma > 1 - \frac{b}{\ln^\alpha (|t| + 2)},$$

и вывели из этого асимптотическую формулу

$$\pi(x) = \operatorname{li} x + O\left(xe^{-(\ln x)^\beta}\right)$$

при любой постоянной $\beta < 0{,}6$.

Однако если справедлива гипотеза Римана, то

$$\pi(x) = \operatorname{li} x + O(x^{1/2} \ln x) \tag{53}$$

(см. дополнение 1).

В пределах имеющихся к настоящему времени таблиц простых чисел $\pi(x) < \operatorname{li} x$. Например, при $x = 10^7$, $x = 10^8$ и $x = 10^9$ отношения $\pi(x)/\operatorname{li} x$ приблизительно равны 0,9994; 0,99986; 0,99996.

Предполагалось, что вообще при всех достаточно больших x $\pi(x) < \operatorname{li} x$. Это предположение оказалось неверным. Д. Литтлвуд (1885—1957) в 1914 г. доказал, что разность $\pi(x) - \operatorname{li} x$ бесконечное число раз меняет знак. Более того, было доказано, что при любом $\varepsilon > 0$ эта разность принимает бесконечное число раз значения как большие $x^{1/2-\varepsilon}$, так и меньшие $-x^{1/2-\varepsilon}$. Доказательство этой теоремы можно найти в книге [7]. Из этого утверждения следует, что в асимптотическом равенстве (53) постоянную 1/2 в показателе в остаточном члене нельзя заменить на меньшую постоянную.

Большое внимание в теории чисел уделяется решению так называемых аддитивных задач. Постановки этих задач связаны с возможностью представления натуральных чисел в виде сумм чисел заданного вида.

Наиболее известная из этих задач — проблема Гольдбаха. В 1742 г. Х. Гольдбах (1690—1764) в письме к Л. Эйлеру высказал предположение, что всякое нечетное число, большее 6, можно представить в виде суммы трех простых чисел. Эйлер высказал более сильную гипотезу о том, что всякое четное

число, начиная с 4, можно представить в виде суммы двух простых чисел.

Первым результатом, связанным с проблемой Гольдбаха, была теорема Л. Г. Шнирельмана (1905—1938), утверждающая, что существует постоянная k такая, что каждое натуральное число, большее 1, есть сумма не более чем k простых чисел.

Большим достижением в теории чисел стала доказанная И. М. Виноградовым теорема, утверждающая, что всякое достаточно большое нечетное число представимо в виде суммы трех простых чисел.

Доказательство этой теоремы основывалось на разработанном И. М. Виноградовым новом методе оценок тригонометрических сумм [3]. О развитии метода тригонометрических сумм, его приложениях, а также о некоторых других методах в теории чисел можно прочитать в книге [15].

Утверждение о представлении четных чисел в виде суммы двух простых к настоящему времени не доказано. Однако при помощи метода решета установлено, что всякое достаточно большое четное число можно представить в виде суммы простого числа и числа, имеющего не более двух простых делителей.

О решении аддитивных проблем, связанных с простыми числами, можно прочитать в книгах А. А. Карацубы [8] и К. Прахара [9].

ЗАДАЧИ

1) Доказать, что

$$\zeta^2(s) = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s}, \quad \operatorname{Re} s > 1,$$

где $\tau(n)$ — число делителей числа n.

2) Установить тождество

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}, \quad \sigma > 1,$$

где $\mu(n)$ — функция Мёбиуса, которая была определена в задаче 12 гл. 1.

3) Доказать равенство

$$-\frac{\zeta'(s)}{\zeta(s)} = s \int_0^{+\infty} \frac{\psi(x)}{x^{s+1}}\, dx, \quad \sigma > 1.$$

Вывести из него, что если существует $\lim\limits_{x \to +\infty} \dfrac{\psi(x)}{x}$, то этот предел равен 1.

4) Установить равенство

$$\Gamma(s)\zeta(s) = \int_0^{+\infty} \frac{x^{s-1}}{e^x - 1}\, dx, \quad \sigma > 1.$$

5) Доказать, что дзета-функцию можно аналитически продолжить в область $0 < \sigma < 1$ посредством равенства

$$(1 - 2^{1-s})\zeta(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \ldots.$$

Вывести отсюда, что при действительном s, $0 < s < 1$, $\zeta(s) \neq 0$.

6) Доказать, что при любом $\varepsilon > 0$ и $n > n_0(\varepsilon)$ между числами n и $(1 + \varepsilon)n$ содержится простое число.

7) Проверить, что в области

$$\sigma > 1 - \frac{1}{\ln|t|}, \quad |t| \geqslant 3$$

справедливы оценки

$$\zeta(s) = O(\ln|t|), \quad \zeta'(s) = O(\ln^2|t|).$$

8) Установить, что существует постоянная $c > 0$, такая, что в области

$$\sigma > 1 - \frac{c}{\ln^9|t|}, \quad |t| \geqslant 3$$

имеет место оценка

$$\frac{\zeta'(s)}{\zeta(s)} = O(\ln^9|t|).$$

9) Доказать формулу (44).

10) Из тождества (44) вывести, что $\psi(x) \sim x$ при $x \to +\infty$ (не вводя функцию $\omega(x)$).

11) Доказать, что при $a > 1$ и нецелом $x > 1$

$$\sum_{n \leqslant x} \mu(n) = \frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} \frac{1}{\zeta(s)} \frac{x^s}{s}\, ds.$$

Указание: использовать задачу 2.

12) Из равенства, полученного в предыдущей задаче, вывести, что

$$\sum_{n \leqslant x} \mu(n) = o(x).$$

ГЛАВА 3

ТЕОРЕМА ДИРИХЛЕ О ПРОСТЫХ ЧИСЛАХ В АРИФМЕТИЧЕСКОЙ ПРОГРЕССИИ

§ 1. Простейшие частные случаи теоремы Дирихле

Простые числа расположены в натуральном ряде весьма неравномерно. Тем не менее в их распределении можно усмотреть определенные закономерности. Некоторые из них были рассмотрены выше. Целью этой главы является доказательство следующей теоремы о простых числах в арифметической прогрессии.

Теорема Дирихле. *Если разность и первый член арифметической прогрессии есть взаимно простые натуральные числа, то она содержит бесконечное множество простых чисел.*

Пусть

$$mn + l,\ n = 1,\ 2, ..., \tag{1}$$

прогрессия, удовлетворяющая условию теоремы. Условие $(m,\ l) = 1$, наложенное на числа m и l в формулировке теоремы, естественно, поскольку в случае, когда $d = (m,\ l) > 1$, все члены прогрессии (1) делятся на d и поэтому не являются простыми числами.

Количественный аналог теоремы, который может быть получен с помощью развития методов, излагаемых в этой и предыдущей главах, показывает, что при фиксированном m простые числа распределяются между различными прогрессиями (1) с $(m,\ l) = 1$ примерно поровну.

Сформулированная теорема была впервые высказана Л. Эйлером в 1783 г. В 1798 г. А. Лежандр опубликовал доказательство для четных m, использовавшее, как выяснилось позднее, одну ошибочную лемму.

Полностью доказал теорему в 1837—1839 гг. Г. П. Леженг-Дирихле. С тех пор она носит его имя.

Следуя доказательству Евклида теоремы о бесконечности множества простых чисел, нетрудно показать, что существует бесконечное множество простых чисел вида $4n + 3$.

Предположим противное, что множество таких чисел конечно. Перенумеруем их в порядке возрастания:

$$p_1 = 3,\ p_2 = 7,\ p_3 = 11, ..., p_r \tag{2}$$

и рассмотрим целое число

$$N = 4p_1 ... p_2 - 1.$$

Это число нечетно, и поэтому все его простые делители нечетны. Произведение любых двух чисел вида $4n+1$ имеет, как легко проверить, такой же вид. Отсюда, ввиду того что N имеет вид $4n+3$, следует, что у N есть простой делитель вида $4n+3$. Обозначим его буквой p. Так как N не делится ни на одно из чисел $p_1, \ldots, p_r$, то p отлично от всех чисел (2). Это приводит к противоречию с тем, что в совокупности (2) содержатся все простые числа вида $4n+3$. Тем самым доказано, что множество простых чисел вида $4n+3$ бесконечно.

Столь же просто доказывается бесконечность множества простых чисел вида $6n+5$.

Элементарное доказательство того, что существует бесконечное множество простых чисел вида $4n+1$, несколько сложнее и требует привлечения новой идеи. Предшествующее рассуждение основывалось на утверждении:

а) *натуральное число вида* $4n+3$ *имеет простой делитель того же вида.*

Теперь нужно использовать другое утверждение:

б) *пусть* a *и* b *— взаимно простые целые числа. Тогда каждый простой нечетный делитель числа* a^2+b^2 *имеет вид* $4n+1$.

Этот факт будет доказан ниже. Но пока воспользуемся им без доказательства.

Предположим, что простые числа вида $4n+1$ образуют конечное множество. Обозначим их

$$p_1 = 5,\ p_2 = 13,\ p_3 = 17, \ldots, p_r \tag{3}$$

и рассмотрим число

$$N = (2p_1 \cdots p_r)^2 + 1.$$

Если p — простой делитель N, то очевидно, что p — нечетное число и отлично от $p_1, \ldots, p_r$. В то же время из утверждения б) следует, что простое число p имеет вид $4n+1$. Это противоречит тому, что совокупность (3) содержит все простые числа вида $4n+1$. Полученное противоречие доказывает бесконечность множества простых чисел вида $4n+1$.

Утверждения того же типа, что и а) и б), можно использовать совместно и получить еще ряд результатов, аналогичных уже доказанным.

Предположим, например, что множество простых чисел вида $8n+5$ конечно. Пусть оно состоит из чисел

$$p_1 = 5,\ p_2 = 13,\ p_3 = 29, \ldots, p_r. \tag{4}$$

Рассмотрим число

$$N = (p_1 \cdot p_2 \cdot \ldots \cdot p_r)^2 + 2^2.$$

Квадрат нечетного числа при делении на 8 дает, как легко проверить, в остатке 1. Поэтому число N при делении на 8 дает в остатке 5. Так как произведение нескольких чисел вида $8n+1$

есть снова число того же вида, то существует простой делитель числа N, не содержащийся в прогрессии $8n+1$. Ввиду утверждения б) число p имеет вид $4n+1$ и, значит, содержится в прогрессии вида $8n+5$.

Итак, число N имеет простой делитель p вида $8n+5$ и не делится ни на одно из чисел совокупности (4). Поэтому p отлично от всех чисел (4). Но это противоречит тому, что совокупность (4) содержит все простые числа вида $8n+5$. Тем самым доказано, что в прогрессии $8n+5$ содержится бесконечное множество простых чисел.

Пользуясь аналогичными рассуждениями, нетрудно доказать, что в каждой из прогрессий $8n\pm1$, $8n\pm3$, $12n\pm1$, $12n\pm5$ содержится бесконечное множество простых чисел. Несколько сложнее доказывается бесконечность множеств простых чисел вида $mn+1$ и $mn-1$ для любого натурального m.

В настоящее время не известно доказательство теоремы о бесконечности множества простых чисел в арифметической прогрессии произвольного вида с помощью элементарных рассуждений, обобщающих идею Евклида.

Метод, с помощью которого Дирихле доказал эту теорему, существенно использует аналитические средства. Простейший вариант этого метода будет изложен в § 2, где снова будут рассмотрены прогрессии вида $4n+1$ и $4n-1$.

Прежде чем приступить к доказательству теоремы Дирихле, приведем некоторые сведения о сравнениях, необходимые в дальнейшем, а также докажем утверждение б) о простых делителях чисел вида a^2+b^2.

Пусть $m\in\mathbf{N}$. Целые числа a и b называются *сравнимыми* по модулю m, если разность $a-b$ делится на m.

Сравнимость чисел a и b по модулю m обозначают символом

$$a\equiv b\,(\mathrm{mod}\,m),$$

называемым *сравнением* по модулю m.

Числа a и b сравнимы по модулю m тогда и только тогда, когда

$$a=b+mt,\ t\in\mathbf{Z},$$

а также тогда и только тогда, когда они имеют одинаковые остатки при делении на m (см. § 1 гл. 1).

Отсюда следует, что все целые числа по модулю m разбиваются на m непересекающихся классов сравнимых между собой чисел (т. е. имеющих одинаковые остатки при делении на m).

Каждое число, входящее в какой-либо из классов, называется *вычетом* этого класса, а сами классы — *классами вычетов* по модулю m.

Простейшие свойства сравнений напоминают свойства обычных числовых равенств. Укажем только некоторые из них:

1) *Два числа, сравнимые с третьим, сравнимы между собой.*

2) *Сравнения по одному и тому же модулю можно почленно складывать.*

3) *Сравнения по одному и тому же модулю можно почленно перемножать.*

Правила сокращения несколько отличаются от правил сокращения равенств.

4) *Если*

$$au \equiv av \pmod{m}$$

и $(a, m) = 1$, *то*

$$u \equiv v \pmod{m}.$$

5) *Если*

$$au \equiv av \pmod{am},$$

то

$$u \equiv v \pmod{m}.$$

Пусть $f(x)$ — многочлен с целыми коэффициентами. Сравнение

$$f(x) \equiv 0 \pmod{m}$$

называют *сравнением с неизвестной величиной.*

Если число $x_0 \in \mathbf{Z}$ таково, что

$$f(x_0) \equiv 0 \pmod{m},$$

то говорят, что x_0 *удовлетворяет* рассматриваемому сравнению. Задача о решении сравнения с неизвестной величиной состоит в отыскании всех значений x, которые ему удовлетворяют.

Рассмотрим простейшее линейное сравнение:

$$ax \equiv b \pmod{m}, \quad (a, m) = 1. \tag{5}$$

Лемма 1. *Сравнение* (5) *разрешимо. Множество удовлетворяющих ему чисел составляет некоторый класс вычетов по модулю* m.

Доказательство. Из свойства сравнений 4) следует, что числа

$$a, 2a, 3a, \ldots, ma \tag{6}$$

не сравнимы между собой по модулю m. Следовательно, все эти числа лежат в разных классах вычетов по модулю m. Ввиду того что имеется ровно m различных классов вычетов по модулю m, получаем, что одно из чисел (6) содержится в классе вычетов, содержащем b. Значит, сравнение разрешимо.

Если $ar \equiv b \pmod{m}$, то, очевидно, все числа из класса вычетов, содержащего r, удовлетворяют сравнению (5) (свойства 3) и 1)), и любое решение лежит в классе вычетов, содержащем r (свойства 1) и 4)). Лемма доказана.

Для каждого m, $m > 1$, обозначаем через $\varphi(m)$ количество чисел совокупности

$$0, 1, \ldots, m-1, \tag{7}$$

взаимно простых с m.

Примеры: $\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$, $\varphi(6)=2$; если p — простое, то $\varphi(p)=p-1$.

Существует ровно $\varphi(m)$ различных арифметических прогрессий (1) с условием $(l, m)=1$, $0 \leqslant l < m$.

Функция $\varphi(m)$ называется *функцией Эйлера*.

Теорема Эйлера. *Если* $a \in \mathbb{Z}$, $(a, m)=1$, *то*

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

Доказательство. Пусть

$$r_1, r_2, \ldots, r_c,$$

где $c=\varphi(m)$ — все числа из совокупности (7), взаимно простые с m. Пусть r — одно из чисел r_i. Тогда произведение ar можно представить в виде

$$ar = qm + r_0, \quad 0 \leqslant r_0 < m.$$

Если r_0 и m имеют общий простой делитель p, то $p \mid ar$. Но это невозможно, так как $(a, m)=1$ и $(r, m)=1$. Следовательно, $(r_0, m)=1$ и число r_0 содержится среди $r_1, \ldots, r_c$. Таким образом для каждого индекса i, $1 \leqslant i \leqslant c$,

$$ar_i \equiv r_{a(i)} \pmod{m} \tag{8}$$

Если $a(j)=a(i)$, то

$$ar_j \equiv ar_i \pmod{m}$$

или $m \mid a(r_j - r_i)$. Поскольку $(a, m)=1$, то по лемме 3 гл. 1 $m \mid (r_j - r_i)$, что невозможно, так как $1 \leqslant |r_j - r_i| < m$. Итак, набор чисел $(a(1), a(2), \ldots, a(c))$ есть некоторая перестановка чисел $(1, 2, \ldots, c)$ и

$$r_1 \cdot r_2 \cdot \ldots \cdot r_c = r_{a(1)} \cdot \ldots \cdot r_{a(c)}. \tag{9}$$

Перемножив теперь сравнения (8), получим

$$a^c \cdot r_1 \cdot \ldots \cdot r_c \equiv r_1 \cdot \ldots \cdot r_c \pmod{m}$$

и так как $(r_1 \cdot \ldots \cdot r_c, m)=1$, то по свойству 4) сравнений $a^c \equiv 1 \pmod{m}$. Теорема доказана.

Следствие 1 (малая теорема Ферма). *Если* p — *простое число, и* $p \nmid a$, *то*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Утверждение очевидно, так как $\varphi(p)=p-1$.

Докажем теперь утверждение б), которое использовалось выше.

Пусть p — нечетный простой делитель числа a^2+b^2. Тогда

$$a^2 \equiv -b^2 \pmod{p}. \tag{10}$$

Если p делит a, то из условия следует, что p делит b. Но это противоречит равенству $(a, b)=1$. Итак, $(a, p)=1$ и, аналогично, $(b, p)=1$.

Возведем обе части сравнения (10) в степень $\frac{p-1}{2}$ и воспользуемся малой теоремой Ферма. Получим

$$1 \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Так как $p \geqslant 3$ и $|1-(-1)^{\frac{p-1}{2}}| \leqslant 2$, то из последнего сравнения находим

$$1 = (-1)^{\frac{p-1}{2}}.$$

Это равенство означает, что с некоторым целым n имеем $\frac{p-1}{2} = 2n$ или $p = 4n+1$.

Рассмотрим фактор-кольцо $\mathbf{Z}/m\mathbf{Z}$ кольца целых чисел $\mathbf{Z}$ по идеалу $m\mathbf{Z}$, состоящему из чисел, кратных m, элементами которого являются классы вычетов по модулю m. Из леммы 1 следует, что классы вычетов, состоящие из чисел, взаимно простых с m, являются обратимыми элементами этого кольца. И каждый класс вычетов, обратимый в кольце $\mathbf{Z}/m\mathbf{Z}$, как легко видеть, состоит из чисел, взаимно простых с m. Таким образом, в кольце $\mathbf{Z}/m\mathbf{Z}$ имеется в точности $\varphi(m)$ обратимых элементов, и мультипликативная группа $(\mathbf{Z}/m\mathbf{Z})^*$ обратимых элементов кольца $\mathbf{Z}/m\mathbf{Z}$ состоит из $\varphi(m)$ элементов. Так как по теореме Лагранжа порядок каждого элемента группы делит порядок группы, т. е. $\varphi(m)$, то получаем еще одно доказательство теоремы Эйлера.

§ 2. Другое доказательство бесконечности множества простых чисел в прогрессиях вида $4n \pm 1$

В этом параграфе на простейших примерах прогрессий вида $4n \pm 1$ будет показана основная идея доказательства теоремы о бесконечности множества простых чисел в арифметической прогрессии. Соответствующее обобщение этой идеи позволит в конце главы изложить доказательство теоремы Дирихле в общем случае.

Рассмотрим два ряда, члены которых являются функциями действительной переменной s:

$$L_0(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \ldots = \sum_{k=1}^{\infty} \frac{1}{(2k+1)^s},$$

$$L_1(s) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \ldots = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)^s}.$$

Они оба сходятся при $s > 1$, а $L_1(s)$ сходится даже при $s > 0$. Из признака равномерной сходимости Дирихле следует, что ряд для $L_1(s)$ равномерно сходится в любой области вида $s > \delta$, где $\delta > 0$. Поскольку члены этого ряда непрерывны в той же области, то по теореме о непрерывности суммы функционального ряда функция $L_1(s)$ непрерывна в области $s > \delta$, а ввиду произвольности δ — и в области $s > 0$.

Так как абсолютная величина суммы знакочередующегося ряда, удовлетворяющего признаку сходимости Лейбница, не превосходит абсолютной величины его первого члена, то

$$L_1(1) = 1 - \frac{1}{3} + \frac{1}{5} - \ldots = 1 - \left(\frac{1}{3} - \frac{1}{5} + \ldots\right) > 1 - \frac{1}{3} = \frac{2}{3}.$$

С помощью леммы 10 гл. 1 при $s > 1$ находим

$$L_0(s) = \sum_{k=0}^{\infty} \frac{1}{(2k+1)^s} \geqslant \int_0^{+\infty} \frac{dx}{(2x+1)^s} = \frac{1}{2(s-1)},$$

откуда следует, что

$$\lim_{s \to 1+0} L_0(s) = +\infty. \tag{11}$$

Для функций $L_0(s)$ и $L_1(s)$ существуют разложения в бесконечные произведения по простым числам, аналогичные тождеству Эйлера для дзета-функции Римана.

Действительно, определим функции $\chi_0(n)$, $\chi_1(n)$ натурального аргумента n следующим образом:

$$\chi_0(n) = \begin{cases} 0, & \text{если } n \text{ четно,} \\ 1, & \text{если } n \text{ нечетно,} \end{cases} \qquad \chi_1(n) = \begin{cases} 0, & \text{если } n \text{ четно,} \\ (-1)^{\frac{n-1}{2}}, & \text{если } n \text{ нечетно.} \end{cases}$$

Тогда

$$L_0(s) = \sum_{n=1}^{\infty} \frac{\chi_0(n)}{n^s}, \quad L_1(s) = \sum_{n=1}^{\infty} \frac{\chi_1(n)}{n^s}. \tag{12}$$

Функции $\chi_0(n)$, $\chi_1(n)$, как легко видеть, вполне мультипликативны, т. е. для любых целых u и v

$$\chi(uv) = \chi(u)\chi(v)$$

и $\chi(1) = 1$. Для функции $\chi_1(n)$ это проще всего доказать, заметив, что $\chi_1(n) \neq 0$ тогда и только тогда, когда n нечетно, и $\chi_1(n) = 1$ тогда и только тогда, когда $n \equiv 1 \pmod 4$.

По лемме 3 гл. 2 при $s > 1$ имеем

$$L_0(s) = \prod_p \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1}, \quad L_1(s) = \prod_p \left(1 - \frac{\chi_1(p)}{p^s}\right)^{-1},$$

откуда получаем, что

$$\ln L_0(s) = -\sum_p \ln\left(1 - \frac{\chi_0(p)}{p^s}\right),$$

$$\ln L_1(s) = -\sum_p \ln\left(1 - \frac{\chi_1(p)}{p^s}\right).$$

Пользуясь разложением в ряд Тейлора функции $-\ln(1-t)$

$$-\ln(1-t) = \sum_{k=1}^{\infty} \frac{t^k}{k}, \quad |t| < 1,$$

находим при $s > 1$ для $i = 0, 1$

$$\ln L_i(s) = \sum_p \sum_{k=1}^{\infty} \frac{(\chi_i(p))^k}{k \cdot p^{ks}} = \sum_p \frac{\chi_i(p)}{p^s} + \sum_p \sum_{k=2}^{\infty} \frac{(\chi_i(p))^k}{k \cdot p^{ks}}. \quad (13)$$

Оценим сверху двойную сумму в правой части полученного равенства. Так как $|\chi_i(p)| \leqslant 1$, то при $s \geqslant 1$

$$\left|\sum_{k=2}^{\infty} \frac{(\chi_i(p))^k}{k \cdot p^{ks}}\right| \leqslant \sum_{k=2}^{\infty} \frac{1}{k \cdot p^{ks}} < \frac{1}{2} \sum_{k=2}^{\infty} \frac{1}{p^{ks}} = \frac{1}{2(p^{2s} - p^s)} \leqslant \frac{1}{p^{2s}}.$$

Тогда, пользуясь неравенством

$$\sum_{n=2}^{\infty} \frac{1}{n^{2s}} \leqslant \sum_{n=2}^{\infty} \frac{1}{n^2},$$

получаем оценку

$$\left|\sum_p \sum_{k=2}^{\infty} \frac{(\chi_i(p))^k}{p^{ks}}\right| \leqslant \sum_p \left|\sum_{k=2}^{\infty} \frac{(\chi_i(p))^k}{p^{ks}}\right| \leqslant \sum_p \frac{1}{p^{2s}} \leqslant \sum_{n=2}^{\infty} \frac{1}{n^{2s}} \leqslant \sum_{n=2}^{\infty} \frac{1}{n^2}.$$

Таким образом, при $s \to 1 + 0$ двойная сумма в правой части равенства (13) остается ограниченной. Поэтому при $s \to 1 + 0$

$$\ln L_i(s) = \sum_p \frac{\chi_i(p)}{p^s} + O(1), \quad i = 0, 1.$$

Из этих равенств имеем

$$\sum_p \frac{\chi_i(p)}{p^s} = \ln L_i(s) + O(1), \quad i = 0, 1. \quad (14)$$

Пользуясь теперь определением $\chi_i(p)$ и абсолютной сходимостью рядов в левой части равенств (14) при $s > 1$, находим, что

$$\sum_{p \equiv 1 \pmod 2} \frac{1}{p^s} = \ln L_0(s) + O(1), \tag{15}$$

$$\sum_{p \equiv 1 \pmod 4} \frac{1}{p^s} - \sum_{p \equiv 3 \pmod 4} \frac{1}{p^s} = \ln L_1(s) + O(1). \tag{16}$$

Равенство (15) можно представить аналогично равенству (16) в виде

$$\sum_{p \equiv 1 \pmod 4} \frac{1}{p^s} + \sum_{p \equiv 3 \pmod 4} \frac{1}{p^s} = \ln L_0(s) + O(1). \tag{17}$$

Из равенств (16) и (17) следует, что

$$\begin{aligned} \sum_{p \equiv 1 \pmod 4} \frac{1}{p^s} &= \frac{1}{2}(\ln L_0(s) + \ln L_1(s)) + O(1), \\ \sum_{p \equiv 3 \pmod 4} \frac{1}{p^s} &= \frac{1}{2}(\ln L_0(s) - \ln L_1(s)) + O(1). \end{aligned} \tag{18}$$

Поскольку функция $L_1(s)$ непрерывна в точке $s = 1$ и, как доказано выше $L_1(1) > \frac{2}{3} > 0$, то функция $\ln L_1(s)$ ограничена в окрестности точки $s = 1$. Но функция $L_0(s)$ стремится к бесконечности при $s \to 1 + 0$ (см. (11)). Поэтому из равенств (18) находим, что

$$\lim_{s \to 1+0} \sum_{p \equiv 1 \pmod 4} \frac{1}{p^s} = +\infty,$$

$$\lim_{s \to 1+0} \sum_{p \equiv 3 \pmod 4} \frac{1}{p^s} = +\infty.$$

Последние равенства означают, что в каждой из прогрессий $4n + 1$, $4n + 3$, $n = 0, 1, 2, \ldots$, содержится бесконечное множество простых чисел.

Подобные рассуждения были проведены Дирихле в общем случае для любой арифметической прогрессии вида (1). Для этого потребовалось построить $\varphi(m)$ (это число различных арифметических прогрессий вида (1) с условием $(m, l) = 1$, $0 \leqslant l < m$) различных мультипликативных и периодических с периодом m функций $\chi(n)$ (они называются характерами) и соответствующих им $L(s, \chi)$-функций (они носят название L-функций Дирихле).

Как ни странно на первый взгляд, но наибольшие трудности в этом обобщении пришлось преодолеть, доказывая утверждение

$$L(1, \chi) \neq 0 \tag{19}$$

для характеров $\chi(n)$, не равных тождественно 1 на всех числах n, взаимно простых с m (неглавных характеров). В настоящее время наиболее короткий путь доказательства утверждений (19) связан с определением $L(s, \chi)$ рядами, подобными рядам (12), для комплексного s и исследованием аналитических свойств функций $L(s, \chi)$ комплексного переменного s.

§ 3. Характеры

Пусть G — конечная абелева группа. В дальнейшем потребуется понятие группового характера.

Характером группы G называется комплекснозначная функция χ, определенная на G, не равная тождественно нулю и такая, что для любых элементов $a, b \in G$ выполняется равенство

$$\chi(ab) = \chi(a)\chi(b).$$

Это определение означает, что характер χ есть гомоморфизм группы G в мультипликативную группу поля комплексных чисел.

Отметим некоторые свойства характеров.

1. *Функция $\chi_0(a)$, равная 1 для каждого элемента $a \in G$, является характером и называется главным характером. Остальные характеры называются неглавными.*

2. *Если e — единица группы, то для каждого характера χ*

$$\chi(e) = 1. \tag{20}$$

Действительно, из равенства

$$\chi(a) = \chi(ae) = \chi(a)\chi(e),$$

справедливого для каждого элемента $a \in G$, имеем, что $\chi(e) \neq 0$. Теперь из равенства

$$\chi(e) = \chi(ee) = \chi(e)\chi(e)$$

следует равенство (20).

3. *Из равенства*

$$1 = \chi(e) = \chi(aa^{-1}) = \chi(a)\chi(a^{-1})$$

получаем, что для каждого элемента $a \in G$ выполнено неравенство $\chi(a) \neq 0$ и

$$\chi(a^{-1}) = (\chi(a))^{-1}.$$

4. *Если h — порядок группы G (количество ее элементов), то для каждого элемента $a \in G$ значение $\chi(a)$ есть некоторый корень из 1 степени h.* Действительно, по теореме Лагранжа $a^h = e$ и

$$1 = \chi(e) = \chi(a^h) = (\chi(a))^h.$$

Особенно просто построить характеры для циклической группы.

Пример. Пусть H — циклическая группа порядка r и a — ее образующий элемент. Обозначим через ξ произвольный корень степени r из 1 и, воспользовавшись тем, что каждый элемент группы H равен некоторой степени a, определим функцию ψ на H, положив

$$\psi(a^k) = \xi^k.$$

Это определение корректно. Действительно, если $a^k = a^l$ — два представления одного и того же элемента группы H, то $l = k + rq$, $q \in \mathbf{Z}$ и

$$\psi(a^l) = \xi^{k+rq} = \xi^k = \psi(a^k).$$

Легко видеть, что функция ψ мультипликативна и, следовательно, является характером группы H. Существует ровно r корней из 1 степени r: $\xi_1, \ldots, \xi_r$. Значит, таким способом можно построить r различных характеров $\psi_1, \ldots, \psi_r$,

$$\psi_i(a^k) = \xi_i^k, \quad i = 1, \ldots, r.$$

Других характеров группа H не имеет. Действительно, по свойству 4 характеров для каждого характера ψ значение $\psi(a)$ равно одному из чисел ξ_i. Из равенства $\psi(a) = \psi_i(a)$, ввиду того, что a — образующий элемент группы H, и мультипликативности характеров, следует совпадение ψ и ψ_i на всей группе H.

Для каждой конечной группы G будем обозначать в дальнейшем символом $|G|$ количество элементов в G.

Теорема 1. *Пусть G — конечная абелева группа, H — подгруппа G и ψ — некоторый характер группы H. Существует в точности $|G|/|H|$ характеров группы G, совпадающих с ψ на подгруппе H.*

Доказательство. Предположим, что утверждение теоремы неверно. Можно считать, что H — наибольшая по количеству элементов подгруппа группы G и $\psi = \psi(x)$ — соответствующий характер, для которых утверждение теоремы не выполняется. Тогда $H \neq G$. Выберем элемент $a \in G$, не содержащийся в подгруппе H.

Существуют натуральные числа k такие, что $a^k \in H$. Например, $a^h = e \in H$, где h — порядок группы G. Обозначим через r наименьшее натуральное число такое, что $a^r \in H$ и через H_1 подгруппу G, состоящую из элементов вида

$$a^k b,$$

где b пробегает все элементы подгруппы H, а k — любое число из $\mathbf{Z}$. Так как по теореме о делении с остатком (см. гл. 1) существуют целые числа u, v такие, что

$$k = ur + v,\ 0 \leqslant v < r,$$

и $a^r \in H$, то каждый элемент x группы H_1 представим в виде

$$x = a^v b,\ 0 \leqslant v < r,\ b \in H. \tag{21}$$

Это представление единственно. Действительно, из равенства

$$a^{v_1} b_1 = a^{v_2} b_2,\quad 0 \leqslant v_2 \leqslant v_1 < r,\quad b_i \in H, \tag{22}$$

следовало бы, что

$$a^{v_1 - v_2} = b_2 b_1^{-1} \in H.$$

Целые числа v_1 и v_2 удовлетворяют неравенствам $0 \leqslant v_2 \leqslant v_1 < r$ и из определения r следует равенство $v_1 = v_2$. Теперь из равенств (22) находим, что $b_1 = b_2$.

Из единственности представления (21) следует, что подгруппа $H_1 \subset G$ содержит ровно $r\,|H|$ элементов, т. е.

$$|H_1| = r|H|.$$

Поскольку $a^r \in H$, то $\psi(a^r) = \omega$ — некоторый корень из 1 (свойство 4). Обозначим через ξ какой-либо корень степени r из ω и определим функцию $g(x)$ на группе H_1, положив для элемента x вида (21)

$$g(x) = \xi^v \psi(b).$$

Докажем, что функция $g(x)$ является характером группы H_1. Пусть

$$x_1 = a^{k_1} b_1,\ x_2 = a^{k_2} b_2,\ 0 \leqslant k_i < r,\ b_i \in H,$$

и

$$x_1 x_2 = a^k b,\ 0 \leqslant k < r,\ b \in H.$$

Тогда $k_1 + k_2 = k + rj$, $j \in \mathbf{Z}$, и $b = (a^r)^j b_1 b_2$.
Имеем

$$g(x_1 x_2) = \xi^k \psi(b) = \xi^k (\psi(a^r))^j \psi(b_1)\,\psi(b_2) =$$
$$= \xi^k \omega^j \psi(b_1)\,\psi(b_2) = \xi^{k+rj} \psi(b_1)\,\psi(b_2) = g(x_1)\,g(x_2).$$

Итак, $g(x)$ — характер группы H_1, совпадающий, как легко проверить, на подгруппе H с характером $\psi(x)$.

Поскольку существует r различных корней степени r из ω, то таким образом можно построить r различных характеров $g_1, \ldots g_r$ группы H_1, совпадающих с $\psi(x)$ на подгруппе H.

Так как $a \notin H$, то $r > 1$ и $|H_1| = r|H| > |H|$. Следовательно, по первоначальному предположению, для каждого из характеров g_i группы H_1 существует ровно $\nu = |G|/|H_1|$ характеров $\chi_{i1}, \ldots, \chi_{i\nu}$ группы G, совпадающих с g_i на подгруппе H_1

и, значит, с $\psi(x)$ на подгруппе H. Следовательно, приведенная конструкция позволяет построить

$$r \cdot \nu = r \frac{|G|}{|H_1|} = \frac{|G|}{|H|}$$

различных характеров группы G, совпадающих с $\psi(x)$ на подгруппе H. Других характеров с этим свойством не существует. Действительно, пусть $\chi(x)$ характер группы G, совпадающий с $\psi(x)$ на подгруппе H. Так как $a^r \in H$, то

$$(\chi(a))^r = \chi(a^r) = \psi(a^r) = \omega,$$

и, значит, $\chi(a)$ есть некоторый корень степени r из ω. Следовательно, найдется индекс i, для которого $\chi(a) = g_i(a)$. Поскольку для подгруппы H_1 утверждение теоремы верно, то с некоторым индексом k, $1 \leqslant k \leqslant \nu$, имеем $\chi = \chi_{ik}$ на G.

Итак, утверждение теоремы выполняется для подгруппы H, что противоречит ее выбору. Это противоречие означает, что первоначальное предположение неверно, и поэтому теорема справедлива.

Доказательство теоремы конструктивно и позволяет фактически строить характеры. Ниже это будет показано на примере мультипликативной группы $(\mathbf{Z}/m\mathbf{Z})^*$ классов вычетов по модулю m, взаимно простых с m.

Следствие 1. *Пусть G — конечная абелева группа. Существует ровно $|G|$ характеров группы G.*

Выше этот факт был установлен для циклических групп прямым построением всех характеров.

Для доказательства достаточно применить теорему 1 с $H = (e)$ подгруппой, состоящей из одного элемента e и единственным характером ψ этой подгруппы, равным 1.

Следствие 2. *Пусть a — некоторый элемент группы G, r — наименьшее натуральное число такое, что $a^r = e$. Тогда множество чисел $\chi(a)$, где χ пробегает характеры группы G, состоит из всех корней степени r из 1. При этом каждый корень повторяется $|G|/r$ раз.*

Доказательство. Обозначим через H циклическую группу, порожденную элементом a, $|H| = r$. Из примера, разобранного перед теоремой 1, следует, что существует ровно r характеров $\psi_1(x), \ldots, \psi_r(x)$ группы H. При этом числа $\psi_i(a)$, $i = 1, \ldots, r$, составляют множество всех корней степени r из 1. По теореме 1 для каждого i существует ровно $|G|/|H| = |G|/r$ характеров $\chi(x)$ группы G, совпадающих с $\psi_i(x)$ на H, т. е. таких, что $\chi(a) = \psi_i(a)$. Значит, во множестве чисел $\chi(a)$, где χ пробегает все характеры группы G, встречается каждый корень степени r из 1, причем не менее $|G|/r$ раз. Так как по следствию 1 это множество состоит из $|G|$ чисел, то следствие 2 доказано.

Теорема 2. *Имеют место равенства*

$$\sum_a \chi(a) = \begin{cases} |G|, & \text{если } \chi = \chi_0, \\ 0, & \text{если } \chi \neq \chi_0; \end{cases}$$

$$\sum_\chi \chi(a) = \begin{cases} |G|, & \text{если } a = e, \\ 0, & \text{если } a \neq e, \end{cases}$$

где в первой сумме суммирование ведется по всем элементам a группы G, а во второй — по всем характерам $\chi = \chi(x)$ группы G.

Доказательство. 1) Докажем сначала первое равенство. Если $\chi = \chi_0$, то первое утверждение очевидно. Пусть $\chi \neq \chi_0$. Тогда найдется элемент $b \in G$ такой, что $\chi(b) \neq 1$. Имеем

$$\chi(b) \sum_a \chi(a) = \sum_a \chi(ba) = \sum_a \chi(a). \tag{23}$$

Последнее равенство выполняется ввиду того, что произведение ba пробегает всю группу G, если a пробегает G. Из равенства (23) получаем, что

$$(\chi(b) - 1) \sum_a \chi(a) = 0,$$

откуда, ввиду того что $\chi(b) \neq 1$, следует доказываемое равенство.

2) Теперь докажем второе равенство. Если $a = e$, то утверждение имеет место ввиду следствия 1 из теоремы 1 и равенства (20). Пусть теперь $a \neq e$ и r — наименьшее натуральное число такое, что $a^r = e$. Тогда $r \geqslant 2$, и по следствию 2 из теоремы 1

$$\sum_\chi \chi(a) = \frac{|G|}{r} \cdot \sum_{i=1}^{r} \xi_i,$$

где $\xi_1, \ldots, \xi_r$ — все корни из 1 степени r. Числа $\xi_1, \ldots, \xi_r$ составляют полный набор корней уравнения $x^r - 1 = 0$. По теореме Виета $\xi_1 + \ldots + \xi_r = 0$.

Теорема 2 доказана.

Пусть $m \geqslant 1$ — целое число. Определим числовые характеры по модулю m.

Комплекснозначная функция $\chi(n)$, определенная для всех целых чисел n, называется *числовым характером* по модулю m, если она удовлетворяет условиям:

а) $\chi(n) = 0$ тогда и только тогда, когда $(n, m) \neq 1$;

б) $\chi(n)$ периодична с периодом m;

в) для любых целых чисел u и v

$$\chi(uv) = \chi(u)\chi(v).$$

Функция

$$\chi_0(n) = \begin{cases} 0, & \text{если } (n, m) \neq 1, \\ 1, & \text{если } (n, m) = 1 \end{cases}$$

является, как легко проверить, числовым характером и называется *главным характером*. Остальные числовые характеры по модулю m называются *неглавными*.

Имеет место следующее утверждение о числовых характерах.

Теорема 3. *Существует ровно $\varphi(m)$ числовых характеров по модулю m. Если $\chi = \chi(n)$ — числовой характер по модулю m, то:*

1) *Для n, взаимно простых с модулем m, значение $\chi(n)$ есть корень из 1 степени $\varphi(m)$.*

2) *Для всех n выполняется неравенство*

$$|\chi(n)| \leqslant 1.$$

3) *Имеет место равенство*

$$\sum_{n=1}^{m} \chi(n) = \begin{cases} \varphi(m), & \text{если } \chi = \chi_0, \\ 0, & \text{если } \chi \neq \chi_0. \end{cases}$$

4) *Для каждого целого числа n*

$$\sum_{\chi} \chi(n) = \begin{cases} \varphi(m), & \text{если } n \equiv 1 \pmod m, \\ 0, & \text{если } n \not\equiv 1 \pmod m, \end{cases}$$

где суммирование проводится по всем числовым характерам по модулю m.

Доказательство. Пусть $\chi(n)$ — некоторый числовой характер по модулю m. Из пункта б) определения следует, что $\chi(n)$ задает некоторую функцию $\psi(\bar{n})$ на мультипликативной группе $G_m = (\mathbf{Z}/m\mathbf{Z})^*$ классов вычетов по модулю m, взаимно простых с m, а именно

$$\psi(\bar{n}) = \chi(n);$$

здесь и в дальнейшем $\bar{n}$ обозначает класс вычетов по модулю m, содержащий n. Так как $\chi(1) \neq 0$, то $\psi(\bar{n})$ не равняется тождественно нулю, а из пункта в) определения числового характера следует, что

$$\psi(\bar{u}\bar{v}) = \psi(\overline{uv}) = \chi(uv) = \chi(u)\chi(v) = \psi(\bar{u})\psi(\bar{v}).$$

Таким образом, $\psi(\bar{n})$ есть характер мультипликативной группы G_m.

Обратно, по каждому характеру $\psi(\bar{n})$ группы G_m можно построить числовой характер $\chi(n)$ по модулю m, положив

$$\chi(n) = \begin{cases} 0, & \text{если } (n, m) \neq 1, \\ \psi(\bar{n}), & \text{если } (n, m) = 1. \end{cases}$$

Установленное соответствие, очевидно, является взаимно-однозначным. И все утверждения теоремы 3 следуют теперь из доказанного выше для групповых характеров применительно к группе G_m, если учесть, что $|G_m| = \varphi(m)$, где $\varphi(m)$ — функция Эйлера.

В дальнейшем слово *характер* будет обозначать числовой характер по некоторому модулю m, если не оговорено, что рассматривается групповой характер.

Рассмотрим некоторые примеры.

1. $m=2$. Так как $\varphi(2)=1$, то существует единственный характер по модулю 2:

$$\chi_0(n) = \begin{cases} 0, & \text{если } n \text{ четно,} \\ 1, & \text{если } n \text{ нечетно.} \end{cases}$$

2. $m=3$. Существуют $\varphi(3)=2$ характера:

$$\chi_0(n) = \begin{cases} 0, & \text{если } 3 \mid n, \\ 1, & \text{если } 3 \nmid n, \end{cases}$$

$$\chi_1(n) = \begin{cases} 0, & \text{если } n \equiv 0 \pmod 3, \\ 1, & \text{если } n \equiv 1 \pmod 3, \\ -1, & \text{если } n \equiv 2 \pmod 3. \end{cases}$$

3. $m=4$. Мультипликативная группа классов вычетов G_4 является циклической порядка 2. Она порождается классом вычетов по модулю 4, содержащим число 3. Поэтому существуют только два характера по модулю 4:

$$\chi_0(n) = \begin{cases} 0, & \text{если } n \text{ четно,} \\ 1, & \text{если } n \text{ нечетно.} \end{cases}$$

$$\chi_1(n) = \begin{cases} 0, & \text{если } n \text{ четно,} \\ -1, & \text{если } n \equiv 3 \pmod 4, \\ 1, & \text{если } n \equiv 1 \pmod 4. \end{cases}$$

Эти характеры использовались в доказательстве частных случаев теоремы Дирихле, рассмотренных в § 2.

4. $m=5$. Мультипликативная группа классов вычетов G_5 является циклической порядка 4. Она порождается, как легко проверить, классом вычетов, содержащим число 2. Поэтому существуют четыре характера χ_0, χ_1, χ_2, χ_3 по модулю 5, которые можно задать равенством

$$\chi(n) = \begin{cases} 0, & \text{если } n \equiv 0 \pmod 5 \\ \omega^k, & \text{если } n \equiv 2^k \pmod 5, \ k = 0, 1, 2, 3, \end{cases}$$

где $\omega = \chi(2)$ — некоторый корень четвертой степени из 1, т. е. одно из чисел $1, -1, i, -i$.

5. $m=8$. Группа классов вычетов $G_8 = (\mathbf{Z}/8\mathbf{Z})^*$ имеет порядок 4. Значит, существуют 4 характера по модулю 8. Исполь-

зуем снова обозначение $\bar{a}$ для класса вычетов по модулю 8, содержащего число a. Циклическая подгруппа $H=\{\bar{1}, \bar{3}\}\subset G_8$, порождаемая элементом $\bar{3}$, имеет порядок 2. Значит, она имеет два групповых характера ψ_0, ψ_1, задаваемые равенствами

$$\psi_0(\bar{1})=1, \quad \psi_0(\bar{3})=1,$$
$$\psi_1(\bar{1})=1, \quad \psi_1(\bar{3})=-1.$$

По теореме 1 каждый из групповых характеров $\psi(x)$ имеет в точности два продолжения на группу G_8. Так как $\bar{5}\notin H$ и в группе G_8 имеет место равенство $\bar{5}^2=\bar{1}$, то, полагая $\chi(x)=\psi(x)$ на H и $\chi(\bar{5})$ равным квадратному корню из 1, получим все 4 групповых характера группы G_8:

	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}=\bar{3}\cdot\bar{5}$
χ_0	1	1	1	1
χ_1	1	1	−1	−1
χ_2	1	−1	1	−1
χ_3	1	−1	−1	1.

(24)

Здесь характеры χ_0, χ_1 являются продолжениями ψ_0, а χ_2 и χ_3 продолжают ψ_1. При этом положено $\chi(\bar{7})=\chi(\bar{3}\cdot\bar{5})=\chi(\bar{3})\chi(\bar{5})$.

Числовые характеры по модулю 8 получаются из групповых характеров (24) с помощью равенств

$$\chi(n)=\begin{cases} 0, & \text{если } n \text{ четно},\\ \chi(\bar{n}), & \text{если } n \text{ нечетно}.\end{cases}$$

Например,

$$\chi_3(n)=\begin{cases} 0, & \text{если } n\equiv 0 \pmod 2,\\ 1, & \text{если } n\equiv 1,7 \pmod 8,\\ -1, & \text{если } n\equiv 3,5 \pmod 8).\end{cases}$$

В дальнейшем потребуется еще одно утверждение о числовых характерах. Обозначим для каждого x, $x\geqslant 1$,

$$S(x)=\sum_{n\leqslant x}\chi(n),$$

где суммирование ведется по всем натуральным числам n, не превосходящим x.

Лемма 2. *Пусть $\chi(n)$ — неглавный характер. Тогда для каждого x, $x\geqslant 1$, справедливо неравенство*

$$|S(x)|<m.$$

Доказательство. Функция $\chi(n)$ периодична с периодом m и по теореме 3

$$\sum_{n=1}^{m}\chi(n)=0.$$

Поэтому, представив $[x]$ — целую часть числа x — в виде

$$[x]=mq+r,\ 0\leqslant r<m,$$

будем иметь

$$S(x)=S([x])=q\sum_{n=1}^{m}\chi(n)+\sum_{n=mq+1}^{[x]}\chi(n)=\sum_{n=mq+1}^{[x]}\chi(n).$$

Ввиду неравенства $|\chi(n)|\leqslant 1$ отсюда получаем

$$|S(x)|\leqslant r<m.$$

§ 4. L-функции Дирихле

Пусть $\chi(n)$ — произвольный характер по модулю m. Рассмотрим ряд

$$\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}, \tag{25}$$

члены которого являются функциями комплексного переменного s. В области сходимости он определяет функцию, которая называется *L-функцией Дирихле*, соответствующей характеру $\chi(n)$, и обозначается $L(s, \chi)$.

Функции $L_0(s)$, $L_1(s)$, встречавшиеся в § 2, являются L-функциями, соответствующими характерам по модулю 4. В этом параграфе будут изучены некоторые свойства L-функций, необходимые для доказательства теоремы Дирихле.

Лемма 3. 1°. *Если $\chi\neq\chi_0$, то ряд* (25) *сходится в области* $\operatorname{Re} s>0$ *и определяемая им функция $L(s, \chi)$ является аналитической в этой области.*

2°. *Ряд, определяющий $L(s, \chi_0)$, сходится в области* $\operatorname{Re} s>1$. *Функция $L(s, \chi_0)$ является аналитической в области* $\operatorname{Re} s>1$.

Доказательство. Пусть $\chi(n)$ — произвольный характер по модулю m, а δ — некоторое положительное число. Так как $|\chi(n)|\leqslant 1$, то в области $\operatorname{Re} s>1+\delta$ справедливо неравенство

$$\left|\frac{\chi(n)}{n^s}\right|\leqslant\frac{1}{|n^s|}\leqslant\frac{1}{n^{1+\delta}}.$$

Следовательно, ряд (25) равномерно сходится в области $\operatorname{Re} s>1+\delta$. Определяемая им функция $L(s, \chi)$ по теореме Вейерштрасса о сумме равномерно сходящегося ряда аналитических функций является аналитической в этой области. Ввиду произвольности δ это доказывает второе утверждение леммы 3.

Для неглавных характеров $\chi(n)$ потребуется более сложное исследование ряда (25). Воспользовавшись леммой 4 гл. 2, получим равенство

$$\sum_{n=1}^{N}\frac{\chi(n)}{n^s}=\frac{S(N)}{N^s}+s\int_1^N S(x)\,x^{-s-1}\,dx, \tag{26}$$

где

$$S(x)=\sum_{n\leqslant x}\chi(n)$$

— функция, введенная в конце § 3. Для $s=\sigma+it$ из области $\sigma=\operatorname{Re}s>\delta$, где δ — некоторое положительное число, пользуясь леммой 2, находим

$$|S(x)x^{-s-1}|\leqslant m x^{-\delta-1}.$$

Поэтому интеграл

$$\int_1^{+\infty} S(x)x^{-s-1}dx$$

сходится в области $\operatorname{Re}s>\delta$. Поскольку в этой области выполняется неравенство

$$\left|\frac{S(N)}{N^s}\right|\leqslant\frac{m}{N^\delta},$$

то из равенства (26) следует, что ряд (25), определяющий функцию $L(s,\chi)$ сходится в области $\operatorname{Re}s>\delta$. Эти рассуждения справедливы для любого положительного числа δ. Значит, ряд (25) сходится в полуплоскости $\operatorname{Re}s>0$.

Из равенства (26) следует, что в этой полуплоскости для L-функции, соответствующей неглавному характеру $\chi(n)$, справедливо представление

$$L(s,\chi)=s\int_1^{+\infty} S(x)x^{-s-1}dx. \tag{27}$$

Интеграл, стоящий в правой части равенства (27), можно также представить в виде

$$\int_1^{+\infty} S(x)x^{-s-1}dx=\sum_{n=1}^{\infty}\int_n^{n+1} S(x)x^{-s-1}dx. \tag{28}$$

Члены ряда (28) являются аналитическими функциями в области $\operatorname{Re}s>\delta$, что следует из равенств

$$\int_n^{n+1} S(x)x^{-s-1}dx=S(n)\int_n^{n+1} x^{-s-1}dx=\frac{S(n)}{s}\cdot\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right).$$

При этом использовано, что на полуинтервале $n\leqslant x<n+1$ функция $S(x)$ принимает значение $S(n)$. Поскольку

$$\left|\int_n^{n+1} S(x)x^{-s-1}dx\right|\leqslant m\int_n^{n+1} x^{-\delta-1}dx=\frac{m}{\delta}\left(\frac{1}{n^\delta}-\frac{1}{(n+1)^\delta}\right),$$

то ряд (28) равномерно сходится в области $\operatorname{Re} s>\delta$. Отсюда, как и выше, получаем, что сумма его, т. е.

$$\int_1^{+\infty} S(x)\, x^{-s-1}\, dx$$

является аналитической функцией в области $\operatorname{Re} s>\delta$.

Из представления (27) следует теперь, что $L(s, \chi)$ есть аналитическая функция в полуплоскости $\operatorname{Re} s>\delta$, а ввиду произвольности δ — и в полуплоскости $\operatorname{Re} s>0$. Лемма 3 доказана.

Следствие. *Пусть $\chi(n)$ — произвольный характер. Тогда в области $\operatorname{Re} s>1$ справедливо равенство*

$$L'(s, \chi) = -\sum_{n=1}^{\infty} \frac{\chi(n) \ln n}{n^s}. \tag{29}$$

Действительно, ряд (25) по доказанному равномерно сходится в области $\operatorname{Re} s>1+\delta$, где $\delta>0$. Значит, по теореме Вейерштрасса о равномерно сходящихся рядах аналитических функций в этой области ряд (25) можно почленно дифференцировать. Поэтому в полуплоскости $\operatorname{Re} s>1+\delta$ выполняется равенство (29). Так как в этом рассуждении δ — любое положительное число, то равенство (29) справедливо в полуплоскости $\operatorname{Re} s>1$.

Для L-функций имеет место представление в виде бесконечного произведения по простым числам, аналогичное тождеству Эйлера для дзета-функции Римана.

Лемма 4. *Для каждого характера $\chi(n)$ в области $\operatorname{Re} s>1$ справедливо представление*

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Доказательство. Эта лемма является следствием леммы 3 гл. 2, поскольку функция $\chi(n)$ вполне мультипликативна и выполняется неравенство $|\chi(n)| \leqslant 1$.

Следствие 1. *В области $\operatorname{Re} s>1$ для главного характера χ_0 по модулю m справедливо равенство*

$$L(s, \chi_0) = \zeta(s) \prod_{p/m} \left(1 - \frac{1}{p^s}\right), \tag{30}$$

и поэтому функция $L(s, \chi_0)$ может быть аналитически продолжена в область $\operatorname{Re} s>0$, где она имеет единственный полюс (первого порядка) в точке $s=1$.

Действительно, по определению характера $\chi_0(n)$ имеет место равенство

$$\chi_0(p) = \begin{cases} 0, & \text{если } p \mid m, \\ 1, & \text{если } (p, m) = 1, \end{cases}$$

Поэтому

$$L(s, \chi_0) = \prod_{\substack{p \\ (p, m)=1}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Пользуясь теперь тождеством Эйлера для дзета-функции Римана (§ 1 гл. 2), получаем равенство (30). Остальные утверждения легко следуют из этого равенства, поскольку дзета-функция является аналитической в области $\operatorname{Re} s > 0$ с единственным полюсом первого порядка в точке $s = 1$.

Следствие 2. *Для каждого характера χ функция $L(s, \chi)$ не обращается в нуль в области* $\operatorname{Re} s > 1$.

Доказательство. Если $\sigma = \operatorname{Re} s > 1$, то

$$|L(s, \chi)| = \prod_p \left|1 - \frac{\chi(p)}{p^s}\right|^{-1} \geqslant \prod_p \left(1 + \frac{1}{p^\sigma}\right)^{-1}.$$

Пользуясь неравенством (9) из гл. 2, находим:

$$\prod_p \left(1 + \frac{1}{p^\sigma}\right) \leqslant \prod_p \left(1 - \frac{1}{p^\sigma}\right)^{-1} = \zeta(\sigma) \leqslant \frac{\sigma}{\sigma - 1},$$

поэтому

$$|L(s, \chi)| \geqslant \frac{\sigma - 1}{\sigma} > 0.$$

Ближайшей целью дальнейших рассуждений будет доказательство утверждения, что L-функция, соответствующая неглавному характеру χ, в точке $s = 1$ отлична от нуля. Для этого понадобятся две леммы, при помощи которых необходимый факт будет установлен в лемме 7.

Рассмотрим в области $\operatorname{Re} s > 0$ функцию

$$F(s) = \prod_\chi L(s, \chi), \tag{31}$$

где произведение берется по всем характерам по модулю m. Все сомножители, соответствующие неглавным характерам χ, по лемме 3 являются аналитическими функциями в рассматриваемой области. По следствию 1 леммы 4 $L(s, \chi_0)$ — также аналитическая функция в этой области, за исключением единственной точки $s = 1$, где она имеет полюс первого порядка. Значит, если среди L-функций, соответствующих неглавным характерам χ, найдется функция, имеющая в точке $s = 1$ нуль, то этот нуль погасит полюс $L(s, \chi_0)$, и функция $F(s)$ будет аналитической во всей области $\operatorname{Re} s > 0$. В противном случае $F(s)$ имеет полюс первого порядка в точке $s = 1$. Ниже будет проведено исследование аналитических свойств функции $F(s)$.

Лемма 5. *В области* $\operatorname{Re} s>1$ *функция* $F(s)$ (31) *представляется рядом*

$$F(s)=\sum_{n=1}^{\infty}\frac{a_n}{n^s}, \tag{32}$$

где a_n — *целые неотрицательные числа, причем для индексов* n, *имеющих вид*

$$n=r^{\varphi(m)},\ r\in\mathbf{Z},\ (r,\ m)=1,$$

справедливо неравенство $a_n\geqslant 1$. *В области* $\operatorname{Re} s>1$ *ряд* (32) *можно почленно дифференцировать, т. е.*

$$F^{(k)}(s)=(-1)^k\sum_{n=2}^{\infty}\frac{a_n(\ln n)^k}{n^s},\quad k=1,2,\ldots. \tag{33}$$

Доказательство. По лемме 4 в области $\operatorname{Re} s>1$ справедливо равенство

$$F(s)=\prod_{\chi}\prod_{p}\left(1-\frac{\chi(p)}{p^s}\right)^{-1}=\prod_{p}\left(\prod_{\chi}\left(1-\frac{\chi(p)}{p^s}\right)^{-1}\right).$$

Здесь используется то, что произведение по χ конечно.

Для каждого простого числа p, не делящего m, обозначим f_p наименьшее из натуральных чисел h, удовлетворяющих условию

$$p^h\equiv 1\pmod m.$$

По следствию 2 из теоремы 1 для таких p множество чисел $\chi(p)$, где χ пробегает все характеры по модулю m, состоит из всех корней степени f_p из 1, причем каждый корень повторяется $g_p=\varphi(m)/f_p$ раз. Таким образом выполняется равенство

$$\prod_{\chi}(1-\chi(p)\,t)=(1-t^{f_p})^{g_p}$$

и, значит,

$$F(s)=\prod_{\substack{p\\(p,m)=1}}(1-p^{-f_p s})^{-g_p}, \tag{34}$$

где произведение берется по всем простым числам p, не делящим m.

Функция $(1-z)^{-g}$ разлагается в ряд Тейлора следующим образом:

$$(1-z)^{-g}=\sum_{r=0}^{\infty}\frac{(g+r-1)!}{(g-1)!\,r!}\,z^r. \tag{35}$$

Этот ряд абсолютно сходится в круге $|z|<1$. Полагая в равенстве (35) $g=g_p$, $z=p^{-f_p s}$, где p — простое число, не делящее m, и s — комплексное число из области $\operatorname{Re} s>1$, получим

$$(1-p^{-f_p s})^{-g_p}=\sum_{k=0}^{\infty}\frac{u_{p,k}}{p^{ks}}, \tag{36}$$

где

$$u_{p,k}=\begin{cases}0, & \text{если } k \text{ не делится на } f_p,\\ \dfrac{(g_p+r-1)!}{(g_p-1)!\,r!}, & \text{если } k=rf_p.\end{cases} \tag{37}$$

Из абсолютной сходимости рядов (36) и основной теоремы арифметики (§ 2 гл. 1) следует, что имеет место равенство

$$\prod_{\substack{p\leqslant N\\(p,m)=1}}(1-p^{-f_p s})^{-g_p}=\sum_{n=1}^{\infty}{}'\frac{a_n}{n^s}, \tag{38}$$

где

$$a_n=\begin{cases}0, & \text{если } (n,m)\neq 1,\\ u_{p_1,k_1}\dots u_{p_l,k_l}, & \text{если } (n,m)=1,\ n=p_1^{k_1}\dots p_l^{k_l},\end{cases} \tag{39}$$

а штрих означает, что суммирование ведется только по тем натуральным числам n, все простые делители которых не превосходят N.

Пусть σ — действительное число, $\sigma>1$. Тогда из равенства (38), ввиду того что $a_n\geqslant 0$, получаем

$$\sum_{n=1}^{N}\frac{a_n}{n^\sigma}\leqslant\sum_{n=1}^{\infty}{}'\frac{a_n}{n^\sigma}\leqslant\prod_{\substack{p\\(p,m)=1}}(1-p^{-f_p\sigma})^{-g_p}=F(\sigma).$$

Следовательно, ряд

$$\sum_{n=1}^{\infty}\frac{a_n}{n^\sigma} \tag{40}$$

сходится.

Пользуясь равенством (38), находим для $s=\sigma+it$ из области $\operatorname{Re} s>1$

$$\left|\prod_{\substack{p\leqslant N\\(p,m)=1}}(1-p^{-f_p s})^{-g_p}-\sum_{n=1}^{N}\frac{a_n}{n^s}\right|=\left|\sum_{n=N+1}^{\infty}{}'\frac{a_n}{n^s}\right|\leqslant$$

$$\leqslant\sum_{n=N+1}^{\infty}{}'\frac{a_n}{n^\sigma}\leqslant\sum_{n=N+1}^{\infty}\frac{a_n}{n^\sigma}.$$

Переходя в этом неравенстве к пределу при $N \to +\infty$ и пользуясь равенством (34), а также сходимостью ряда (40), получаем при s из области $\operatorname{Re} s > 1$ равенство (32), где коэффициенты a_n задаются формулами (39), (37). Из этих формул следует, что $a_n \in \mathbf{Z}$ и $a_n \geqslant 0$.

Пусть теперь

$$n = r^{\varphi(m)}, \text{ где } (r, m) = 1. \tag{41}$$

Так как $(n, m) = 1$, то ввиду условия (39) имеем

$$a_n = u_{p_1, k_1} \dots u_{p_l k_l},$$

где

$$n = p_1^{k_1} \dots p_l^{k_l}$$

— каноническое представление числа n.

Из равенства (41) теперь получаем, что для каждого индекса i показатель k_i делится на $\varphi(m)$ и, значит, $f_{p_i} | k_i$, что ввиду (37) дает $u_{p_i k_i} \geqslant 1$ и $a_n \geqslant 1$. Утверждение о почленной дифференцируемости ряда (32) в полуплоскости $\operatorname{Re} s > 1 + \delta$, $\delta > 0$, следует по теореме Вейерштрасса из равномерной сходимости ряда (32) в этой области. Ряд же сходится равномерно, поскольку в этой полуплоскости справедливо неравенство

$$\left| \frac{a_n}{n^s} \right| \leqslant \frac{a_n}{n^{1+\delta}}$$

и ряд (40) сходится при $\sigma = 1 + \delta$. Так как число δ можно взять произвольно малым, то равенство (33) имеет место в области $\operatorname{Re} s > 1$.

Лемма 5 доказана полностью.

Лемма 6. *Если функция* $F(s)$ (31) *не имеет особых точек в области* $\operatorname{Re} s > 0$, *то ряд*

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} \tag{42}$$

сходится к $F(s)$ *в области* $\operatorname{Re} s > 0$.

Доказательство. Из равенства (33), в частности, находим

$$F^{(k)}(2) = (-1)^k \sum_{n=1}^{\infty} \frac{a_n (\ln n)^k}{n^2}, \quad k = 0, 1, 2, \dots . \tag{43}$$

Разложим функцию $F(s)$ в ряд Тейлора в точке $s = 2$:

$$F(s) = \sum_{k=0}^{\infty} \frac{F^{(k)}(2)}{k!} (s-2)^k. \tag{44}$$

Предположим, что $F(s)$ — аналитическая функция в области $\operatorname{Re} s>0$. Тогда радиус сходимости ряда (44) не меньше, чем 2. Пусть σ — действительное число из полуинтервала $0<\sigma\leqslant 1$. Так как $|\sigma-2|<2$, то, пользуясь разложениями (44) и (43), находим

$$F(\sigma)=\sum_{k=0}^{\infty}\frac{(\sigma-2)^k}{k!}(-1)^k\sum_{n=1}^{\infty}\frac{a_n(\ln n)^k}{n^2}=\sum_{k=0}^{\infty}\sum_{n=1}^{\infty}\frac{(2-\sigma)^k(\ln n)^k a_n}{k!\quad n^2}.$$

Члены последнего двойного ряда неотрицательны, поэтому он сходится абсолютно, и в нем можно поменять порядок суммирования. Имеем

$$F(\sigma)=\sum_{n=1}^{\infty}\frac{a_n}{n^2}\sum_{k=0}^{\infty}\frac{(2-\sigma)^k(\ln n)^k}{k!}=\sum_{n=1}^{\infty}\frac{a_n}{n^2}e^{(2-\sigma)\ln n}=\sum_{n=1}^{\infty}\frac{a_n}{n^{\sigma}}.$$

Следовательно, функция $F(s)$ представима рядом (42) в каждой точке действительной полупрямой $s>0$.

Для комплексных s *из области* $\operatorname{Re} s>\delta>0$ имеем неравенство

$$\left|\frac{a_n}{n^s}\right|\leqslant\frac{a_n}{n^{\delta}},$$

из которого ввиду сходимости ряда (40) при $\sigma=\delta$ по теореме Вейерштрасса следует, что сумма ряда (42) есть аналитическая функция в области $\operatorname{Re} s>\delta$. Ввиду единственности аналитического продолжения заключаем, что равенство (32) имеет место в области $\operatorname{Re} s>\delta$. Это доказывает лемму 6, поскольку положительное число δ может быть взято сколь угодно малым.

Лемма 7. *Если* χ — *неглавный характер, то*

$$L(1,\chi)\neq 0.$$

Доказательство. Предположим, что существует неглавный характер χ такой, что $L(1,\chi)=0$. В этом случае из замечания, сделанного перед леммой 5, следует, что функция $F(s)$ является аналитической в полуплоскости $\operatorname{Re} s>0$. Поэтому ввиду леммы 6 ряд (42) сходится в области $\operatorname{Re} s>0$ и сумма его равна $F(s)$.

Рассмотрим точку $s_0=1/\varphi(m)$, лежащую в области $\operatorname{Re} s>0$. Из доказанного выше получаем, что ряд

$$\sum_{n=1}^{\infty}\frac{a_n}{n^{s_0}} \tag{45}$$

сходится, причем из-за неравенства $a_n\geqslant 0$, члены его неотрицательны.

Пусть k — произвольное натуральное число и $r=mk+1$. Тогда $(r, m)=1$ и для $n=r^{\varphi(m)}$ по лемме 5 имеем $a_n \geqslant 1$. Следовательно, для таких n

$$\frac{a_n}{n^{s_0}} \geqslant \frac{1}{n^{s_0}} = \frac{1}{r^{\varphi(m)s_0}} = \frac{1}{r} = \frac{1}{mk+1}.$$

Отсюда и из сходимости ряда (45) следует, что должен сходиться ряд

$$\sum_{k=1}^{\infty} \frac{1}{mk+1}.$$

Но это утверждение неверно. Полученное противоречие завершает доказательство леммы 7.

По следствию 2 из леммы 4 функция $\dfrac{L'(s, \chi)}{L(s, \chi)}$ является аналитической в области $\operatorname{Re} s>1$. Для дальнейшего необходимо представление этой функции в виде ряда, аналогичного ряду (42) (такие ряды называются рядами Дирихле).

Лемма 8. *Для каждого характера* $\chi(n)$ *в области* $\operatorname{Re} s>1$ *справедливо равенство*

$$-\frac{L'(s, \chi)}{L(s, \chi)} = \sum_{n=2}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s}, \tag{46}$$

где

$$\Lambda(n) = \begin{cases} \ln p, & \text{если } n = p^k, \\ 0, & \text{если } n \neq p^k, \end{cases}$$

— *функция, использовавшаяся* в § 1 гл. 2.

Доказательство. Так как для $s=\sigma+it$ имеет место неравенство

$$\left|\frac{\Lambda(n)\chi(n)}{n^s}\right| \leqslant \frac{\ln n}{n^{\sigma}},$$

то ряд, стоящий в правой части равенства (46), абсолютно сходится в области $\sigma>1$. Умножим этот ряд на ряд, определяющий $L(s, \chi)$. Получим

$$L(s, \chi) \sum_{k=2}^{\infty} \frac{\Lambda(k)\chi(k)}{k^s} = \sum_{u=1}^{\infty} \frac{\chi(u)}{u^s} \sum_{k=2}^{\infty} \frac{\Lambda(k)\chi(k)}{k^s} =$$

$$= \sum_{n=2}^{\infty} \frac{\chi(n)}{n^s} \left(\sum_{k \mid n} \Lambda(k)\right) = \sum_{n=2}^{\infty} \frac{\chi(n) \cdot \ln n}{n^s} = -L'(s, \chi).$$

Предпоследнее равенство имеет место ввиду равенства (5) из гл. 2, а последнее — по следствию из леммы 3. Лемма 8 доказана.

§ 5. Доказательство теоремы Дирихле

Рассмотрим равенство (46), справедливое по лемме 8 в области $\operatorname{Re} s>1$. Поскольку $\Lambda(n)=0$ для всех n, не являющихся степенями простых чисел, то все отличные от нуля члены ряда в правой части (46) имеют вид

$$\frac{\ln p\cdot\chi(p^k)}{p^{ks}},$$

где p — простое и k — натуральное числа. Ряд (46) абсолютно сходится, следовательно, его можно представить в виде двойного ряда*, и, значит, в области $\operatorname{Re} s>1$

$$-\frac{L'(s,\chi)}{L(s,\chi)}=\sum_p\frac{\ln p\cdot\chi(p)}{p^s}+\sum_p\sum_{k=2}^{\infty}\frac{\ln p\cdot\chi(p^k)}{p^{ks}}. \tag{47}$$

Второе слагаемое в правой части равенства (47) равномерно ограничено по s в области $\operatorname{Re} s\geqslant 3/4$. Действительно, если $s=\sigma+it$, $\sigma\geqslant 3/4$, то

$$\left|\sum_p\sum_{k=2}^{\infty}\frac{\ln p\cdot\chi(p^k)}{p^{ks}}\right|\leqslant\sum_p\ln p\sum_{k=2}^{\infty}\frac{1}{p^{k\sigma}}=\sum_p\frac{\ln p}{p^{2\sigma}}(1-p^{-\sigma})^{-1}\leqslant$$

$$\leqslant 3\sum\frac{\ln p}{p^{2\sigma}}<3\sum_{n=2}^{\infty}\frac{\ln n}{n^{2\sigma}}\leqslant 3\sum_{n=2}^{\infty}\frac{\ln n}{n^{3/2}},$$

следовательно, при $s\to 1+0$ для каждого характера χ имеет место равенство

$$\sum_p\frac{\ln p\cdot\chi(p)}{p^s}=-\frac{L'(s,\chi)}{L(s,\chi)}+O(1). \tag{48}$$

Здесь и в дальнейшем $s\to 1+0$ обозначает, что s стремится к 1 по действительной оси справа.

Пусть v — некоторое натуральное число, удовлетворяющее сравнению

$$vl\equiv 1\pmod m. \tag{49}$$

Умножим обе части равенства (48) на $\chi(v)$ и просуммируем получившиеся равенства по всем числовым характерам χ. Тогда получим

$$\sum_p\frac{\ln p}{p^s}\left(\sum_\chi\chi(v)\chi(p)\right)=-\sum_\chi\chi(v)\frac{L'(s,\chi)}{L(s,\chi)}+O(1). \tag{50}$$

*) См.: Привалов И. И. Введение в теорию функций комплексного переменного. М.: Наука, 1977, гл. 1.

Если простое число p удовлетворяет сравнению $p \equiv l \pmod m$, то $pv \equiv 1 \pmod m$, и по теореме 3

$$\sum_{\chi} \chi(v)\chi(p) = \sum_{\chi} \chi(pv) = \varphi(m).$$

Если же $p \not\equiv l \pmod m$, то $pv \not\equiv 1 \pmod m$, и по той же теореме

$$\sum_{\chi} \chi(v)\chi(p) = \sum_{\chi} \chi(pv) = 0.$$

Таким образом, равенство (50) можно переписать в виде

$$\sum_{\substack{p \\ p \equiv l \pmod m}} \frac{\ln p}{p^s} = -\frac{1}{\varphi(m)} \sum_{\chi} \chi(v) \frac{L'(s, \chi)}{L(s, \chi)} + O(1). \qquad (51)$$

По леммам 3 и 7 для неглавного характера χ функция $\frac{L'(s, \chi)}{L(s, \chi)}$ является аналитической в точке $s=1$. Поэтому для таких характеров при $s \to 1+0$ имеем

$$\frac{L'(s, \chi)}{L(s, \chi)} = O(1). \qquad (52)$$

По следствию 1 леммы 4 функция $L(s, \chi_0)$ имеет в точке $s=1$ полюс первого порядка. Значит, при $s \to 1+0$

$$\frac{L'(s, \chi_0)}{L(s, \chi_0)} = -\frac{1}{s-1} + O(1). \qquad (53)$$

Ввиду равенств (52) и (53) из равенства (51) получаем, что

$$\sum_{\substack{p \\ p \equiv l \pmod m}} \frac{\ln p}{p^s} = \frac{\chi_0(v)}{\varphi(m)} \frac{1}{s-1} + O(1).$$

Так как число v удовлетворяет сравнению (49), то $(v, m) = 1$ и $\chi_0(v) = 1$. Итак, при $s \to 1+0$

$$\sum_{\substack{p \\ p \equiv l \pmod m}} \frac{\ln p}{p^s} = \frac{1}{\varphi(m)} \frac{1}{s-1} + O(1). \qquad (54)$$

Правая часть равенства (54) при $s \to 1+0$ имеет бесконечный предел. Значит, сумма, стоящая в левой части этого равенства, имеет бесконечное множество слагаемых. Поэтому существует бесконечное множество простых чисел, удовлетворяющих сравнению

$$p \equiv l \pmod m.$$

Теорема Дирихле доказана.

В 1775 г. Л. Эйлер опубликовал аналитическое доказательство бесконечности множества простых чисел в прогрессиях вида $4n\pm1$ (Euler L. Opera omnia, ser. I, v. 4, 146—162). Точнее, он доказал расходимость двух рядов

$$\frac{1}{5}+\frac{1}{13}+\frac{1}{17}+\ldots, \qquad \frac{1}{3}+\frac{1}{7}+\frac{1}{11}+\ldots, \tag{55}$$

члены которых имеют вид $1/p$, где в первом случае простые числа p берутся из прогрессии $4n+1$, а во втором — из прогрессии $4n-1$. Осознавая справедливость общего утверждения для прогрессий вида $mn+1$, он утверждал, что расходится ряд с членами $1/p$, где p пробегает простые числа из прогрессии $100n+1$.

Во втором параграфе этой главы по существу излагаются рассуждения Эйлера. Необходимо только отметить, что Эйлер оперировал не функциями, а рядами, соответствующими значениям L-функций в точке $s=1$. Вместо функции $L_0(s)$ он рассматривал гармонический ряд и, не доказывая, что $L_1(1)\neq0$, пользовался точным значением суммы ряда

$$L_1(1)=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{9}-\ldots,$$

равным $\pi/4$. Это равенство установил еще Г. В. Лейбниц (1646—1716).

Доказательство утверждения о рядах (55) имеет много общего с эйлеровским доказательством бесконечности множества простых чисел. А доказательство, предложенное Дирихле в общем случае, является естественным развитием этих рассуждений Эйлера. Нужно отметить, что Дирихле, по-видимому, не знал указанной выше работы Эйлера и в своей статье ссылался на доказательство бесконечности множества простых чисел, содержавшееся в знаменитой книге Эйлера «Введение в анализ бесконечных» (т. 1, гл. XV).

В 1837 г. вышли две работы Дирихле, посвященные теореме о простых числах в арифметической прогрессии. Они содержали формулировку теоремы в общем виде, однако доказательство проводилось только для случая, когда разность прогрессии есть простое число. В конце второй работы содержится построение характеров для произвольного модуля и некоторые замечания о том, как можно доказать утверждение $L(1, \chi)\neq0$ для неглавных характеров χ в общем случае (именно это место в рассуждениях представило наибольшие трудности для обобщения). В 1839 г. Дирихле опубликовал полное доказательство теоремы о простых числах в арифметической прогрессии.

Изложение содержания работ Дирихле можно найти в книге Г. П. Лежен-Дирихле «Лекции по теории чисел» (М.: ОНТИ, 1936) или, на более современном языке, в книгах Г. Хассе [13] и З. И. Боревича и И. Р. Шафаревича [1].

Заметим, что Дирихле проводил все рассуждения с рядами, определяющими L-функции, считая s действительным переменным. Его доказательство в части, связанной с установлением того, что $L(1, \chi) \neq 0$, принципиально отличается от использованного в этой главе. Основываясь на классической теории квадратичных форм, развитой Лагранжем и Гауссом, Дирихле установил в случае действительного неглавного характера χ (это наиболее сложный случай) явные формулы для $L(1, \chi)$, выражающие это число в конечном виде через некоторые характеристики совокупности всех бинарных квадратичных форм фиксированного дискриминанта, связанного с характером χ. Из этих формул и следовало, что $L(1, \chi) \neq 0$.

Построение характеров, осуществленное в § 3, отличается от проведенного Дирихле. Дирихле выписывал характеры в явном виде, используя доказанные Гауссом результаты о существовании так называемых первообразных корней.

После знаменитой работы Римана о дзета-функции L-функции стали изучаться как функции комплексного переменного. Привлечение новых методов исследования позволило сделать намного короче первоначальное доказательство Дирихле и, более того, получить ряд новых количественных результатов.

Для произвольного характера χ функция $L(s, \chi)$ аналитически продолжается на всю комплексную плоскость. При этом для так называемых примитивных характеров ее значения оказываются связанными функциональным уравнением, подобным функциональному уравнению для дзета-функции. Так же, как и дзета-функция, L-функции Дирихле имеют в критической полосе $0 < \operatorname{Re} s < 1$ бесконечное число нулей, и информация о их расположении оказывается весьма важной при изучении вопросов распределения простых чисел в прогрессиях.

В 1899 г. Валле-Пуссен установил асимптотическую формулу для $\pi(x, m, l)$ — количества простых чисел в прогрессии (1), не превосходящих некоторой величины x. Оказалось, что независимо от числа l, $(m, l) = 1$,

$$\pi(x, m, l) \sim \frac{1}{\varphi(m)} \frac{x}{\ln x} \text{ при } x \to +\infty,$$

т. е. простые числа распределяются примерно поровну между всеми арифметическими прогрессиями (1).

Валле-Пуссен установил в действительности более сильный результат. Он, как и в асимптотическом законе распределения простых чисел, получил оценку остаточного члена в асимптотической формуле для количества простых чисел в прогрессии.

Существует предположение, так называемая расширенная гипотеза Римана, что не только у дзета-функции, но и у всех L-функций Дирихле нули в критической полосе лежат на прямой $\operatorname{Re} s = 1/2$. В настоящее время доказаны намного более слабые результаты. Важную роль при исследовании теоретико-числовых задач играют утверждения об отсутствии нулей

L-функций в некоторых областях, а также верхние оценки числа нулей одной или многих L-функций в прямоугольных областях критической полосы — так называемые плотностные теоремы.

Из теоремы Дирихле следует, что в каждой арифметической прогрессии (1) существуют простые числа. Сколь большим может быть наименьшее из них? В 1944 г., используя идею плотности нулей, Ю. В. Линник доказал, что существует абсолютная постоянная c такая, что в каждой прогрессии вида (1) есть простое число, не превосходящее m^c.

Со свойствами L-функций Дирихле и их применениями при исследовании различных задач теории чисел можно познакомиться, например, по книгам А. А. Карацубы [8], К. Прахара [9], К. Чандрасекхарана [16] и [17] и Н. Г. Чудакова [18].

Существует элементарное доказательство теоремы Дирихле (см., например, [9]).

В настоящее время мало что известно о распределении простых чисел в последовательностях, растущих быстрее арифметических прогрессий. В частности, ни для одного многочлена с целыми коэффициентами степени, большей 1, не доказано, что среди его значений при натуральных значениях аргумента содержится бесконечное множество простых чисел. Например, неизвестно, конечно или бесконечно множество простых чисел в последовательности n^2+1, $n=1, 2, \ldots$.

Неизвестно также, конечное или бесконечное множество простых чисел содержится в последовательности 2^n-1, $n=1, 2, \ldots$. В то же время самые большие из найденных к настоящему времени простых чисел имеют как раз такой вид (см. § 3 гл. 1).

ЗАДАЧИ

1) Пусть p — простое число, $p>3$. Доказать, что если сравнение

$$x^2+x+1\equiv 0 \pmod p$$

разрешимо, то p имеет вид $6n+1$. Вывести отсюда, что множество простых чисел вида $6n+1$ бесконечно.

2) Пусть p — простое число, $p>5$. Доказать, что если сравнение

$$x^4+x^3+x^2+x+1\equiv 0 \pmod p$$

разрешимо, то p имеет вид $5n+1$. Вывести отсюда, что множество простых чисел вида $5n+1$ бесконечно.

3) Пусть p — простое нечетное число. Доказать, что если сравнение

$$x^4+1\equiv 0 \pmod p$$

разрешимо, то p имеет вид $8n+1$. Вывести отсюда, что множество простых чисел вида $8n+1$ бесконечно.

Пусть p — простое нечетное число. Определим для каждого целого числа a так называемый символ Лежандра $\left(\frac{a}{p}\right)$, положив

$$\left(\frac{a}{p}\right) = 0, \text{ если } p \mid a;$$

$$\left(\frac{a}{p}\right) = 1, \text{ если сравнение } x^2 \equiv a \pmod{p} \text{ разрешимо;}$$

$$\left(\frac{a}{p}\right) = -1, \text{ если сравнение } x^2 \equiv a \pmod{p} \text{ неразрешимо.}$$

4) Доказать, что

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

5) Доказать, что символ Лежандра $\left(\frac{a}{p}\right)$ является характером по модулю p, т. е.

а) для любого a

$$\left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right);$$

б) для любых a, b

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

(использовать утверждение задачи 4);

в) $\left(\frac{1}{p}\right) = 1$.

6) С помощью задачи 4 доказать, что

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

7) Пусть p — простое нечетное число. Для двух комплексных чисел $a+bi$, $c+di$ из кольца $\mathbf{Z}[i]$ будем писать

$$a+bi \equiv c+di \pmod{p},$$

если сравнимы по модулю p их действительные и мнимые части.

а) Доказать, что выполняется сравнение

$$(1-i)^p \equiv 1-i^p \pmod{p}.$$

б) Пользуясь результатом пункта а) и равенством $(1-i)^2 = -2i$, доказать, что

$$2^{\frac{p-1}{2}} \equiv \frac{1-i^p}{1-i} i^{\frac{p-1}{2}} \pmod{p}.$$

в) Вывести из пункта б), пользуясь результатом задачи 4, что

$$\left(\frac{2}{p}\right)=\begin{cases} 1, & \text{если } p\equiv 1, 7 \pmod 8,\\ -1, & \text{если } p\equiv 3, 5 \pmod 8.\end{cases}$$

г) Проверить, используя пункт в), что

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

8) Доказать с помощью задачи 7, что простых чисел вида $8n-1$ бесконечно много.

9) Доказать, что если сравнение

$$x^2+2\equiv 0 \pmod p$$

разрешимо, то либо p имеет вид $8n+1$, либо p имеет вид $8n+3$. Вывести с помощью этого утверждения, что простых чисел вида $8n+3$ бесконечно много.

10) Целью этого упражнения является доказательство так называемого квадратичного закона взаимности, позволяющего вместе с результатами задач 5—7 легко вычислять значение $\left(\frac{a}{p}\right)$ для любого целого a.

Пусть q — простое нечетное число и $\zeta=e^{2\pi i/q}$ — корень степени q из 1.

а) Пользуясь результатом задачи 3 гл. 4, доказать, что каждое число из кольца $\mathbf{Z}[\zeta]$ единственным способом представимо в виде

$$a_0+a_1\zeta+\ldots+a_{q-2}\zeta^{q-2},\quad a_j\in\mathbf{Z}. \tag{56}$$

Для любых двух чисел ξ, $\eta\in\mathbf{Z}[\zeta]$ будем писать при простом p

$$\xi\equiv\eta \pmod p,$$

если в представлениях чисел ξ, η в виде (56) попарно сравнимы по модулю p соответствующие коэффициенты. Проверить, что для сравнений по модулю p в кольце $\mathbf{Z}[\zeta]$ выполнены свойства 1—3 из § 1.

Обозначим

$$\tau=\sum_{k=0}^{q-1}\left(\frac{k}{q}\right)\zeta^k\in\mathbf{Z}[\zeta].$$

б) Доказать, что

$$\tau^{p-1}\equiv\left(\frac{p}{q}\right) \pmod p.$$

в) Доказать, что

$$\tau^2=\left(\frac{-1}{q}\right)q=(-1)^{\frac{q-1}{2}}q.$$

г) Вывести из утверждений б), в) квадратичный закон взаимности:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

11) Найти все простые числа p, для которых разрешимо сравнение

$$x^2+2x-2\equiv 0 \pmod p.$$

Доказать, что в прогрессии $12n-1$ содержится бесконечно много простых чисел.

12) Пусть χ_1, χ_2 — числовые характеры по модулю m. Доказать, что функция $\chi_1\chi_2$, определенная равенством

$$\chi_1\chi_2(n)=\chi_1(n)\chi_2(n),$$

является характером. Доказать, что характеры образуют группу относительно так введенной операции умножения.

13) Пусть χ — характер по модулю m, принимающий комплексные значения, и $\bar{\chi}$ — характер, значения которого комплексно сопряжены со значениями χ, т. е. для любого натурального n справедливо равенство

$$\bar{\chi}(n)=\overline{\chi(n)}.$$

Предполагая, что $L(1, \chi)=0$, доказать, что

а) имеет место равенство $L(1, \bar{\chi})=0$;

б) функция $F(s)=\prod_{\chi} L(s, \chi)$ аналитична в точке $s=1$ и обращается в этой точке в нуль.

Приведите утверждение пункта б) к противоречию с помощью леммы 5 из § 4 гл. 3.

14) Пусть χ — комплексный характер по модулю m.

а) Пользуясь разложениями L-функций в бесконечные произведения по простым числам, доказать, так же как в лемме 8 гл. 2, что функция

$$F(s)=L^3(s, \chi_0)L^4(s, \chi)L(s, \chi^2)$$

для всех действительных s из области $s>1$ удовлетворяет неравенству

$$|F(s)|\geqslant 1.$$

б) Доказать, что из предположения

$$L(1, \chi)=0$$

следует, что функция $F(s)$ имеет в точке $s=1$ нуль. Это будет противоречить неравенству из пункта а).

15) Пусть χ — характер, принимающий только действительные значения. Обозначим

$$G(s)=L(s, \chi_0)L(s, \chi).$$

а) Доказать, что в области $\operatorname{Re} s>1$ справедливо представление

$$G(s)=\sum_{n=1}^{\infty}\frac{b_n}{n^s}, \tag{57}$$

где

$$b_n=\sum_{k|n}\chi(k).$$

б) Доказать, что b_k — целые неотрицательные числа и $b_{n^2}\geqslant 1$.

в) Доказать, что ряд (57) расходится в точке $s=1/2$.

г) Обозначим

$$A(x)=\sum_{n\leqslant x}b_n.$$

Доказать, что из предположения $L(1,\ \chi)=0$ следует равенство $A(x)=O(\sqrt{x})$.

д) Пользуясь утверждением леммы 4 гл. 2 доказать, что в предположении пункта г) ряд (57) сходится к функции $G(s)$ в области $\operatorname{Re} s>1/2$.

е) Пользуясь аналитичностью функции $G(s)$ в точке $s=1/2$, привести к противоречию утверждения пунктов в) и д).

ГЛАВА 4

АЛГЕБРАИЧЕСКИЕ И ТРАНСЦЕНДЕНТНЫЕ ЧИСЛА. ТРАНСЦЕНДЕНТНОСТЬ ЧИСЕЛ e И π

§ 1. Алгебраические числа

В дальнейшем потребуются некоторые свойства многочленов с коэффициентами из поля рациональных чисел $\mathbf{Q}$. Множество таких многочленов образует кольцо, которое обозначают $\mathbf{Q}[x]$.

Многочлен $f(x) \in \mathbf{Q}[x]$ *делится* на многочлен $\varphi(x) \in \mathbf{Q}[x]$, если существует многочлен $q(x) \in \mathbf{Q}[x]$ такой, что

$$f(x) = q(x)\varphi(x).$$

В случае делимости $f(x)$ на $\varphi(x)$ многочлен $\varphi(x)$ называется *делителем* многочлена $f(x)$, а $f(x)$ — *кратным* многочлена $\varphi(x)$.

Если $f(x)$ делится на $\varphi(x)$, то говорят также, что $\varphi(x)$ *делит* многочлен $f(x)$.

Многочлен положительной степени $f(x) \in \mathbf{Q}[x]$ называется *приводимым*, если существуют два многочлена положительной степени $f_1(x)$ и $f_2(x)$ из $\mathbf{Q}[x]$ таких, что

$$f(x) = f_1(x) f_2(x).$$

В противном случае многочлен $f(x)$ называется *неприводимым*.

Из определения следует, что любой многочлен первой степени неприводим.

В кольце многочленов $\mathbf{Q}[x]$ имеет место теорема о делении с остатком:

Если $f(x)$ и $\varphi(x)$ — любые многочлены из $\mathbf{Q}[x]$, а $\varphi(x)$ имеет положительную степень, то существуют многочлены $q(x)$ и $r(x)$ из $\mathbf{Q}[x]$ такие, что

$$f(x) = q(x)\varphi(x) + r(x), \tag{1}$$

а степень $r(x)$ меньше степени $\varphi(x)$.

Лемма 1. *Неприводимый многочлен $f(x) \in \mathbf{Q}[x]$ степени n не может иметь общего корня с не равным тождественно нулю многочленом $\varphi(x) \in \mathbf{Q}[x]$ степени, меньшей, чем n.*

Доказательство. Допустим противное, что $f(x)$ и $\varphi(x)$ имеют общий корень α. Среди всех не равных тождественно нулю многочленов из $\mathbf{Q}[x]$, которые имеют своим корнем число α, найдется многочлен наименьшей степени m, где, по предположению, $1 \leqslant m < n$. Будем считать, что $\varphi(x)$ обладает этим свойством.

По теореме о делении с остатком выполняется равенство (1), где $q(x)$ и $r(x)$ — многочлены из $\mathbf{Q}[x]$, а степень $r(x)$ меньше степени $\varphi(x)$. Положим в этом равенстве $x=\alpha$. Тогда $f(\alpha)=0$ и $\varphi(\alpha)=0$. Поэтому и $r(\alpha)=0$. Но число m выбрано так, что α не может быть корнем не равного тождественно нулю многочлена из $\mathbf{Q}[x]$ степени, меньшей, чем m. Поэтому $r(x)\equiv 0$ и

$$f(x)=q(x)\varphi(x),$$

что противоречит неприводимости многочлена $f(x)$. Лемма доказана.

Лемма 2. *Если многочлен $\varphi(x)\in\mathbf{Q}[x]$ имеет общий корень с неприводимым многочленом $f(x)\in\mathbf{Q}[x]$, то $f(x)$ есть делитель $\varphi(x)$, а поэтому каждый корень $f(x)$ является корнем $\varphi(x)$.*

Доказательство. Пусть m и n — соответственно степени многочленов $\varphi(x)$ и $f(x)$. Если $m=0$, то $\varphi(x)\equiv 0$, так как $\varphi(\alpha)=0$, и лемма справедлива. Пусть $m>0$. Применяя теорему о делении с остатком, получим

$$\varphi(x)=q(x)f(x)+r(x),\ q(x),\ r(x)\in\mathbf{Q}[x],$$

где степень $r(x)$ меньше, чем n. Полагая в этом равенстве $x=\alpha$, получим $r(\alpha)=0$, а тогда по лемме 1 $r(x)\equiv 0$ и

$$\varphi(x)=q(x)f(x),$$

что завершает доказательство леммы.

Следствие. *Если два неприводимых многочлена из $\mathbf{Q}[x]$ имеют общий корень, то они отличаются на постоянный множитель из $\mathbf{Q}$.*

Действительно, по лемме 2 неприводимые многочлены, имеющие общий корень, делят друг друга и поэтому отличаются только постоянным множителем из $\mathbf{Q}$.

Лемма 3. *Неприводимый многочлен $f(x)\in\mathbf{Q}[x]$ не может иметь кратных корней.*

Доказательство. Если бы $f(x)$ имел кратный корень, то он имел бы общий корень со своей производной $f'(x)$, которая есть многочлен из $\mathbf{Q}[x]$ степени, меньшей, чем степень $f(x)$ и $f'(x)\not\equiv 0$. Но последнее по лемме 1 для неприводимого многочлена невозможно.

Число α называется *алгебраическим*, если оно является корнем многочлена

$$\varphi(x)=a_nx^n+\ldots+a_1x+a_0,\quad \varphi(x)\not\equiv 0,$$

с рациональными коэффициентами.

Примеры алгебраических чисел.

$$\alpha_1=\sqrt[3]{2},\ \varphi_1(x)=x^3-2,$$

$$\alpha_2=\sqrt{3}+1,\ \varphi_2(x)=x^2-2x-2,$$

$$\alpha_3=i,\ \varphi_3(x)=x^2+1.$$

Любое рациональное число a является алгебраическим, как корень многочлена $\varphi(x)=x-a$.

Действительное или комплексное число α называется *трансцендентным*, если оно не является алгебраическим.

Следовательно, трансцендентное число не может быть корнем никакого многочлена $\varphi(x)$ с рациональными коэффициентами, $\varphi(x)\neq 0$.

Примеры трансцендентных чисел будут приведены позднее. Будет доказано также, что числа e и π являются трансцендентными числами.

Если α — алгебраическое число, то по определению оно является корнем многочлена $\varphi(x)\in\mathbf{Q}[x]$. Среди делителей $\varphi(x)$ найдется неприводимый многочлен $f(x)\in\mathbf{Q}[x]$ такой, что $f(\alpha)=0$.

Итак, если α — алгебраическое число, то существует неприводимый многочлен $f(x)\in\mathbf{Q}[x]$, корнем которого является α.

Степенью алгебраического числа α называется степень неприводимого многочлена $f(x)\in\mathbf{Q}[x]$, имеющего α своим корнем.

Следствие из леммы 2 показывает, что данное определение степени корректно.

Из леммы 1 следует, что степень алгебраического числа α есть наименьшая из степеней всех не равных тождественно нулю многочленов из $\mathbf{Q}[x]$, имеющих α своим корнем. Это свойство также можно было взять за определение степени алгебраического числа.

Рациональные числа и только они являются алгебраическими числами первой степени.

Действительно, если $a\in\mathbf{Q}$, то a есть корень многочлена $f(x)=x-a$. Обратно, корень многочлена $f(x)=bx+c$, где $b, c\in\mathbf{Q}$, $b\neq 0$, является числом из $\mathbf{Q}$.

В приведенных выше примерах число α_1 имеет степень 3, а числа α_2 и α_3 — степень 2. Неприводимость соответствующих многочленов легко доказать.

Нетрудно доказать, что при любом $n\in\mathbf{N}$ существует неприводимый многочлен $f(x)\in\mathbf{Q}[x]$ степени n. Например, $f(x)=x^n-2$. Доказательство этого утверждения предоставляется читателю как упражнение. Построить примеры неприводимых многочленов любой степени n можно с помощью критериев неприводимости, имеющихся в алгебре, например критерия Эйзенштейна (см. задачу 2 к гл. 4).

Из существования неприводимого многочлена степени n следует, что при любом $n\in\mathbf{N}$ существуют алгебраические числа степени n.

Пусть α — алгебраическое число степени n. Существует неприводимый многочлен из $\mathbf{Q}[x]$ степени n, имеющий α своим корнем. Разделим все коэффициенты этого многочлена на его старший коэффициент. Получим неприводимый многочлен $f(x)$ степени n из $\mathbf{Q}[x]$ со старшим коэффициентом, равным 1,

также имеющий α своим корнем. Многочлен $f(x)$, удовлетворяющий указанным условиям, по следствию из леммы 2 единствен.

Минимальным многочленом алгебраического числа α называется неприводимый многочлен из $\mathbf{Q}[x]$ со старшим коэффициентом 1, имеющий α своим корнем.

Если α — алгебраическое число степени n, то корни $\alpha_1, \ldots, \alpha_n$ его минимального многочлена $f(x)$ называются *числами, сопряженными с* α.

Среди чисел, сопряженных с α, содержится и само число α. Поэтому всегда будем считать, что $\alpha_1 = \alpha$.

Числа $\alpha_1, \ldots, \alpha_n$ — сопряженные с α — обладают следующими свойствами:

1) *Все они являются алгебраическими числами степени* n *и имеют один и тот же минимальный многочлен* $f(x)$.

2) *Числа* $\alpha_1, \ldots, \alpha_n$ — *сопряженные с любым из этих чисел (понятие сопряженности является взаимным).*

3) *Числа* $\alpha_1, \ldots, \alpha_n$ *по лемме 3 различны, как корни одного неприводимого многочлена* $f(x)$.

Если α — алгебраическое число степени n и $\alpha_1, \ldots, \alpha_n$ — числа, сопряженные с α, то будем обозначать

$$\overline{|\alpha|} = \max_{1 \leqslant i \leqslant n} |\alpha_i|.$$

Лемма 4. *Если* α — *алгебраическое число степени* n, $\alpha \neq 0$, *то* $1/\alpha$ *также алгебраическое число степени* n.

Доказательство. По условию α является корнем неприводимого многочлена из $\mathbf{Q}[x]$ степени n:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0.$$

Поэтому

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots + a_0 = 0.$$

Разделив обе части последнего равенства на α^n, получим

$$a_n + a_{n-1} \left(\frac{1}{\alpha}\right) + \ldots + a_0 \left(\frac{1}{\alpha}\right)^n = 0.$$

Обозначим

$$\varphi(x) = a_0 x^n + \ldots + a_{n-1} x + a_n.$$

Тогда $\varphi(1/\alpha) = 0$. Многочлен $\varphi(x)$ неприводим, так как в противном случае $f(x)$ был бы приводим. Тем самым утверждение леммы доказано.

В дальнейшем будет необходима известная теорема о симметрических многочленах.

Пусть $\mathbf{K}$ — коммутативное кольцо с единицей, $\mathbf{K}[\alpha_1, \ldots, \alpha_n]$ обозначает кольцо многочленов с коэффициентами из $\mathbf{K}$ от переменных

$$\alpha_1, \ldots, \alpha_n. \qquad (2)$$

Многочлен

$$P(\alpha_1, \ldots, \alpha_n) \in \mathbf{K}[\alpha_1, \ldots, \alpha_n] \tag{3}$$

называется *симметрическим многочленом* от переменных (2), если он не изменяется при любой перестановке этих переменных.

Обозначим

$$\begin{aligned} \sigma_1 &= \alpha_1 + \ldots + \alpha_n, \\ \sigma_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n, \\ &\ldots\ldots\ldots\ldots\ldots \\ \sigma_n &= \alpha_1 \cdots \alpha_n \end{aligned} \tag{4}$$

элементарные симметрические многочлены переменных (2). Они равны с точностью до знака соответствующим коэффициентам многочлена

$$(x - \alpha_1) \cdots (x - \alpha_n).$$

Теорема о симметрических многочленах. *Любой многочлен* (3), *симметрический от переменных* (2), *единственным образом представляется в виде*

$$P(\alpha_1, \ldots, \alpha_n) = H(\sigma_1, \ldots, \sigma_n),$$

где

$$H(\sigma_1, \ldots, \sigma_n) \in \mathbf{K}[\sigma_1, \ldots, \sigma_n]$$

— многочлен от элементарных симметрических многочленов (4) *переменных* (2).

Рассмотрим несколько систем переменных

$$\alpha_1, \ldots, \alpha_n; \ \ldots; \ \delta_1, \ldots, \delta_s, \tag{5}$$

и пусть

$$\sigma_1, \ldots, \sigma_n; \ \ldots; \ \eta_1, \ldots, \eta_s \tag{6}$$

— соответственно их элементарные симметрические многочлены.

Многочлен

$$P(\alpha_1, \ldots, \alpha_n; \ \ldots; \ \delta_1, \ldots, \delta_s) \in \mathbf{K}[\alpha_1, \ldots, \alpha_n; \ \ldots; \ \delta_1, \ldots, \delta_s] \tag{7}$$

называется *симметрическим многочленом от нескольких систем переменных* (5), если он не изменяется при любой перестановке переменных в каждой из этих систем.

Пример. Многочлен

$$P(\alpha_1, \alpha_2, \alpha_3, \alpha_4; \ \beta_1, \beta_2, \beta_3) = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3$$

является симметрическим многочленом от двух систем величин $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ и $\beta_1, \beta_2, \beta_3$.

Теорема о симметрических многочленах легко обобщается на случай нескольких систем переменных.

Теорема. *Любой многочлен* (7), *симметрический от нескольких систем переменных* (5), *единственным образом представляется в виде*

$$P(\alpha_1, \ldots, \alpha_n; \ldots; \delta_1, \ldots, \delta_s) = H(\sigma_1, \ldots, \sigma_n; \ldots; \eta_1, \ldots, \eta_s),$$

где

$$H(\sigma_1, \ldots, \sigma_n; \ldots; \eta_1, \ldots, \eta_s) \in \mathbf{K}[\sigma_1, \ldots, \sigma_n; \ldots; \eta_1, \ldots, \eta_s]$$

— многочлен от элементарных симметрических многочленов (6) *систем переменных* (5).

Лемма 5. *Пусть* $\alpha, \ldots, \delta$ *— алгебраические числа, а* (5) *— соответственно сопряженные с* $\alpha, \ldots, \delta$. *Далее,*

$P = P(x; \alpha_1, \ldots, \alpha_n; \ldots; \delta_1, \ldots, \delta_s) \in \mathbf{Q}[x; \alpha_1, \ldots, \alpha_n; \ldots; \delta_1, \ldots, \delta_s]$, *и* P *как многочлен от величин* (5) *с коэффициентами из* $\mathbf{Q}[x]$ *является симметрическим многочленом от нескольких систем величин* (5).

Тогда

$$P = P(x) \in \mathbf{Q}[x],$$

а если P *не зависит от* x, *то* $P \in \mathbf{Q}$.

Доказательство. Рассмотрим P как многочлен от величин (5) с коэффициентами из $\mathbf{Q}[x]$. Поскольку P является симметрическим многочленом от нескольких систем величин (5), а элементарные симметрические многочлены (6) величин (5) равны с точностью до знака соответствующим коэффициентам минимальных многочленов чисел $\alpha, \ldots, \delta$, являющихся числами из $\mathbf{Q}$, то по теореме о симметрических многочленах от нескольких систем переменных P есть многочлен из $\mathbf{Q}[x]$, а если P не зависит от x, то $P \in \mathbf{Q}$.

Теорема 1. *Если* α *и* β *— алгебраические числа, то числа* $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, *а в случае если* $\beta \neq 0$, *то и* α/β *являются алгебраическими числами, т. е. множество всех алгебраических чисел образует поле.*

Доказательство. Пусть $\alpha_1, \ldots, \alpha_n$ — числа, сопряженные с α, а $\beta_1, \ldots, \beta_s$ — числа, сопряженные с β. Рассмотрим многочлены

$$P_1(x) = \prod_{i=1}^{n} \prod_{j=1}^{s} (x - (\alpha_i \pm \beta_j)),$$

$$P_2(x) = \prod_{i=1}^{n} \prod_{j=1}^{s} (x - \alpha_i \beta_j).$$

Как многочлены от $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_s$ с коэффициентами — многочленами из $\mathbf{Z}[x]$ они являются симметрическими многочленами по двум системам величин. Поэтому по лемме 5

$$P_1(x),\ P_2(x) \in \mathbf{Q}[x].$$

Но многочлены $P_1(x)$ и $P_2(x)$ имеют своими корнями соответственно числа $\alpha \pm \beta$ и $\alpha\beta$ и отличны от нуля. Значит, числа $\alpha \pm \beta$ и $\alpha\beta$ являются алгебраическими числами.

Так как $\alpha/\beta=\alpha\cdot 1/\beta$, то соответствующее утверждение для частного следует из доказанного для произведения и леммы 4.

Из доказательства теоремы 1 следует также, что степень суммы, разности, произведения и частного двух алгебраических чисел не превосходит произведения их степеней.

Обозначим через **A** *поле всех алгебраических чисел.*

Поле **Q** рациональных чисел можно расширить до поля **A** всех алгебраических чисел путем присоединения к **Q** корней всех многочленов из **Q**[x]. Естественно возникает следующая проблема. Можно ли расширить подобным образом поле **A**, если к нему присоединить корни всех многочленов с коэффициентами из **A**? Докажем, что образованное таким способом поле будет совпадать с полем **A**.

Теорема 2. *Если число* ξ *— корень многочлена*

$$\psi(x)=x^m+\alpha x^{m+1}+\ldots+\delta, \tag{8}$$

коэффициенты которого α, ..., δ *— алгебраические числа, то* ξ *также есть алгебраическое число.*

Доказательство. Пусть величины (5) обозначают соответственно сопряженные для α, ..., δ. Рассмотрим многочлен

$$P(x)=\prod_{l=1}^{n}\ldots\prod_{l=1}^{s}(x^m+\alpha_l x^{m-1}+\ldots+\delta_l).$$

Как многочлен от величин (5) с коэффициентами из **Z**[x] он является симметрическим многочленом от m систем величин (5). Поэтому по лемме 5 получаем, что $P(x)\in\mathbf{Q}[x]$. Но $P(x)$ делится на $\psi(x)$. Отсюда следует, что $P(\xi)=0$. Это доказывает, что ξ — алгебраическое число.

Из этой теоремы следует, что поле **A** является алгебраически замкнутым. Напомним, что поле **K** называется *алгебраически замкнутым*, если в кольце **K**[x] любой многочлен разлагается на линейные множители.

Изучая арифметические свойства чисел поля **A** и его подполей, целесообразно обобщить понятие целого числа на алгебраические числа.

Алгебраическое число α называется *целым алгебраическим*, если его минимальный многочлен $f(x)$ имеет целые коэффициенты.

Данное определение означает, что целое алгебраическое число есть корень неприводимого многочлена из **Z**[x] со старшим коэффициентом, равным единице.

Если $m\in\mathbf{Z}$, то m является корнем неприводимого многочлена $f(x)=x-m$. Это означает, что все числа из **Z** — целые алгебраические числа.

Все сопряженные с целым алгебраическим числом являются целыми алгебраическими числами, так как они имеют один и тот же минимальный многочлен.

Пример 1. Число $1+\sqrt{3}$ является целым, как корень неприводимого многочлена $f(x)=x^2-2x-2$.

Пример 2. Сопряженные числа $\frac{1\pm i\sqrt{3}}{2}$ являются целыми, как корни неприводимого многочлена $f(x)=x^2-x+1$.

Теорема 3. *Если число α есть корень многочлена $\psi(x)\in\mathbf{Z}[x]$ со старшим коэффициентом, равным 1 (не обязательно неприводимого), то α — целое алгебраическое число.*

Доказательство. Пусть

$$\psi(x)=x^m+b_{m-1}x^{m-1}+\ldots+b_0,$$

а

$$\varphi(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_0,\ a_n>0,$$

— неприводимый и примитивный многочлен с коэффициентами из $\mathbf{Z}$, имеющий своим корнем число α. Напомним, что многочлен из $\mathbf{Z}[x]$ называется примитивным, если его коэффициенты взаимно просты.

По лемме 2 многочлен $\varphi(x)$ является делителем многочлена $\psi(x)$. Поэтому

$$\frac{\psi(x)}{\varphi(x)}=\frac{c}{d}g(x),\ c,\ d\in\mathbf{N},\ (c,\ d)=1,$$

где $g(x)\in\mathbf{Z}[x]$ и является примитивным многочленом. Тогда из равенства

$$d\psi(x)=c\varphi(x)g(x)$$

получаем, что $c=d$, так как многочлен $\varphi(x)g(x)$ как произведение двух примитивных многочленов по известной лемме Гаусса есть примитивный многочлен, а $\psi(x)$ — примитивный многочлен по условию леммы.

Теперь из равенства

$$\psi(x)=\varphi(x)g(x),$$

сравнивая в его обеих частях старшие коэффициенты, получаем, что коэффициент a_n многочлена $\varphi(x)$ должен делить старший коэффициент многочлена $\psi(x)$, равный 1. Отсюда следует, что $a_n=1$, а тогда $\varphi(x)$ — минимальный многочлен числа α, и по определению α есть целое алгебраическое число.

Теорема 3 более удобна, чем определение, для проверки того, является ли α целым алгебраическим числом. Пользуясь ею, не надо проверять неприводимость многочлена, корнем которого является число α, что часто связано с большими трудностями.

Лемма 6. *Пусть α, ..., δ — целые алгебраические числа, а числа* (5) *— соответственно сопряженные с α, ..., δ. Далее, $P=P(x;\ \alpha_1,\ \ldots,\ \alpha_n;\ \ldots;\ \delta_1,\ \ldots,\ \delta_s)\in\mathbf{Z}[x;\ \alpha_1,\ \ldots,\ \alpha_n;\ \ldots;\ \delta_1,\ \ldots,\ \delta_s]$ и P как многочлен от величин* (5) *с коэффициентами из $\mathbf{Z}[x]$*

является симметрическим многочленом от нескольких систем величин (5). *Тогда*

$$P = P(x) \in \mathbf{Z}[x],$$

а если P *не зависит от* x, *то* $P \in \mathbf{Z}$.

Доказательство повторяет доказательство леммы 5 и отличается только тем, что теперь элементарные симметрические многочлены всех систем величин (5) являются числами из $\mathbf{Z}$.

Теорема 4. *Сумма, разность и произведение двух целых алгебраических чисел* α *и* β *также являются целыми алгебраическими числами, т. е. множество всех целых алгебраических чисел образует кольцо.*

Доказательство теоремы 4 аналогично доказательству теоремы 1. Но только в нем вместо леммы 5 используется лемма 6, а в конце рассуждений используется теорема 3.

Кольцо всех целых алгебраических чисел будем обозначать символом $\mathbf{Z}_A$.

Пример 1. Число $\sqrt{2} \in \mathbf{Z}_A$, как корень многочлена $f(x) = x^2 - 2$. Поэтому все числа $a + b\sqrt{2}$ принадлежат $\mathbf{Z}_A$ при $a, b \in \mathbf{Z}$.

Пример 2. Число $i \in \mathbf{Z}_A$, как корень многочлена $f(x) = x^2 + 1$. Поэтому все числа $a + bi$ принадлежат $\mathbf{Z}_A$ при $a, b \in \mathbf{Z}$.

Теорема 5. *Если число* ξ — *корень многочлена* $\psi(x)$ (8), *коэффициенты которого* $\alpha, \ldots, \delta$ — *целые алгебраические числа, то* ξ — *также целое алгебраическое число.*

Эта теорема доказывается аналогично теореме 2, но с помощью леммы 6 и теоремы 3 вместо леммы 5.

Пример. Если $\alpha \in \mathbf{Z}_A$, то все корни k-й степени из α, $k \geqslant 2$, также принадлежат $\mathbf{Z}_A$.

Если α — рациональное число, то существует $r \in \mathbf{N}$ такое, что $r\alpha$ есть целое число. Действительно, пусть

$$\alpha = \frac{a}{b}, \quad a \in \mathbf{Z}, \quad b \in \mathbf{N}.$$

Полагая $r = b$, получим, что $r\alpha = a$, т. е. $r\alpha \in \mathbf{Z}$.

Аналогичное утверждение выполняется и для целых алгебраических чисел.

Теорема 6. *Если* $\alpha \in \mathbf{A}$, *то существует число* $r \in \mathbf{N}$ *такое, что* $r\alpha \in \mathbf{Z}_A$.

Доказательство. Пусть многочлен

$$g(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0, \quad a_n > 0, \quad g(x) \in \mathbf{Z}[x]$$

имеет α своим корнем. Тогда

$$g(\alpha) = a_n \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0.$$

Обозначим $r = a_n$ и умножим обе части последнего равенства на r^{n-1}. Получим

$$r^{n-1}g(\alpha) = (r\alpha)^n + a_{n-1}(r\alpha)^{n-1} + ra_{n-2}(r\alpha)^{n-2} + \ldots$$
$$\ldots + r^{n-1}a_0 = \psi(r\alpha) = 0, \qquad (9)$$

где

$$\psi(x) = x^n + a_{n-1}x^{n-1} + ra_{n-2}x^{n-2} + \ldots + r^{n-1}a_0.$$

Из равенства (9) по теореме 3 следует, что $r\alpha$ есть целое алгебраическое число.

Из теоремы 6 следует, что любое алгебраическое число α можно представить в следующей форме:

$$\alpha = \frac{\beta}{r}, \ \beta \in \mathbf{Z}_A, \ r \in \mathbf{N}.$$

В этом параграфе были рассмотрены самые простейшие сведения об алгебраических числах. Следует заметить, что теория алгебраических чисел является большим и важным разделом математики, имеющим свои методы и глубокие проблемы. Читатель может ознакомиться с основами этой теории по книгам [1, 5].

§ 2. Приближение действительных чисел рациональными числами

Пусть α — действительное число. Как в теоретических, так и в практических задачах часто приходится приближенно заменять число α рациональной дробью p/q, где p и q — целые числа, $q>0$. При этом возникает вопрос об оценке погрешности при такой замене. Поэтому в теории чисел изучают поведение величины

$$\left|\alpha - \frac{p}{q}\right| \qquad (10)$$

и ее оценку при различных значениях p и q.

Поскольку множество рациональных чисел всюду плотно во множестве действительных чисел, то при соответствующем выборе чисел p и q величина (10) может быть сделана меньше любого наперед заданного числа. Поэтому интересно изучать относительную малость величины (10), т. е. выяснять, сколь малой может она быть, если q не превосходит некоторого натурального числа q_0 или, иначе, сколь хорошо действительное число α может быть приближено (аппроксимировано) рациональными дробями p/q в зависимости от величины знаменателя q.

Поведение величины (10) обычно оценивают следующим образом. Пусть $\varphi(q)$ — некоторая положительная функция

от q, убывающая с ростом q. Исследуется, для каких функций $\varphi(q)$ неравенство

$$\left|\alpha-\frac{p}{q}\right|<\varphi(q)$$

имеет бесконечное, а для каких — конечное множество решений в целых числах p и q, $p/q\neq\alpha$.

Будем говорить, что действительное число α *допускает приближение рациональными числами* p/q *порядка* $\varphi(q)$, если существует постоянная $c>0$, зависящая только от α и функции $\varphi(q)$, такая, что неравенство

$$\left|\alpha-\frac{p}{q}\right|<c\varphi(q)$$

имеет бесконечное множество решений в числах p/q, $p/q\neq\alpha$.

Часто в качестве функции $\varphi(q)$ выбирают функцию

$$\varphi(q)=\frac{1}{q^{\nu}},\ \nu>0.$$

Придавая ν и c различные положительные значения, выясняют, когда неравенство

$$\left|\alpha-\frac{p}{q}\right|<\frac{c}{q^{\nu}}$$

имеет бесконечное или конечное множество решений.

Пусть $\alpha=a/b$, $a\in\mathbf{Z}$, $b\in\mathbf{N}$, $(a, b)=1$. В этом случае вопрос о поведении разности (10) решается просто.

При любом $q\in\mathbf{N}$ существует число $p\in\mathbf{Z}$ такое, что

$$\frac{p}{q}\leqslant\frac{a}{b}<\frac{p+1}{q}.$$

Тогда

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{q}. \tag{11}$$

Придавая q различные значения, не кратные b, убеждаемся в том, что существует бесконечное множество дробей p/q, $p/q\neq\alpha$, удовлетворяющих неравенству (11). Это означает, что α допускает приближение рациональными дробями p/q порядка $1/q$.

С другой стороны, для любой дроби p/q, $p/q\neq a/b$,

$$\left|\alpha-\frac{p}{q}\right|=\left|\frac{a}{b}-\frac{p}{q}\right|=\frac{|aq-bp|}{bq}\geqslant\frac{1}{bq}. \tag{12}$$

Отсюда следует, что при любой постоянной c, $0<c\leqslant 1/b$, неравенство

$$\left|\alpha-\frac{p}{q}\right|<\frac{c}{q} \tag{13}$$

не имеет решений в числах p/q, $p/q\neq\alpha$.

Порядок приближения рациональными числами для различных действительных чисел различен. В дальнейшем будет показано, что все действительные иррациональные числа допускают приближение рациональными дробями порядка $1/q^2$, а также что среди них существуют числа, допускающие приближение сколь угодно хорошего порядка $1/q^\nu$, где $\nu>0$ — любое действительное число.

Теорема Дирихле. *Пусть α — действительное число, а t — натуральное число. Тогда существуют целые числа p и q такие, что выполняются неравенства*

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{qt},\quad 0<q\leqslant t. \tag{14}$$

Доказательство. Применим принцип Дирихле, который основан на очень простой идее: если m предметов распределить по n ящикам, то при $m>n$ хотя бы в один ящик попадет не менее двух предметов.

Рассмотрим $t+1$ чисел:

$$\{\alpha x\}=\alpha x-[\alpha x],\quad x=0,\ 1,\ \ldots,\ t. \tag{15}$$

По свойству дробных долей

$$0\leqslant\{\alpha x\}<1. \tag{16}$$

Разделим полуинтервал $0\leqslant y<1$ на t равных полуинтервалов

$$\frac{k}{t}\leqslant y<\frac{k+1}{t},\quad k=0,\ 1,\ \ldots,\ t-1. \tag{17}$$

Каждое из чисел (15) ввиду неравенств (16) будет принадлежать только одному из полуинтервалов (17), так как последние не имеют общих точек. Но чисел (15) ровно $t+1$, а полуинтервалов (17) ровно t. Поэтому среди полуинтервалов (17) найдется такой, который содержит две из точек (15). Пусть это будут числа

$$\{\alpha x_1\}=\alpha x_1-[\alpha x_1],\ \{\alpha x_2\}=\alpha x_2-[\alpha x_2],\ x_2>x_1.$$

Тогда

$$|\{\alpha x_2\}-\{\alpha x_1\}|=|\alpha(x_2-x_1)-([\alpha x_2]-[\alpha x_1])|<\frac{1}{t}. \tag{18}$$

Положим

$$x_2-x_1=q,\ [\alpha x_2]-[\alpha x_1]=p.$$

Очевидно, что $0<q\leqslant t$. Вводя эти обозначения в неравенство (18), получим неравенства

$$|\alpha q-p|<\frac{1}{t},\quad 0<q\leqslant t,$$

из которых следует утверждение теоремы (14).

Ранее было показано, что для рационального числа $\alpha=a/b$

неравенство (12) выполняется при любой дроби p/q, $p/q \neq \alpha$. Поэтому при $t \geqslant b$ неравенство (14) имеет лишь тривиальное решение $p/q = a/b$. При $t < b$ по теореме Дирихле неравенство (14) имеет решение со знаменателем q, $q \leqslant t < b$. Значит, знаменатели всех нетривиальных решений неравенств (14) при различных t ограничены. Следовательно, при рациональном α теорема Дирихле дает некоторую информацию о приближении рациональных чисел рациональными числами с меньшими знаменателями.

Если же α иррационально, то с ростом t знаменатели решений неравенства (14) также возрастают.

Действительно, обозначим для каждого натурального N

$$C_N = \min \left| \alpha - \frac{p}{q} \right|,$$

где минимум берется по конечному множеству рациональных чисел p/q, лежащих на отрезке $\alpha - 1 \leqslant x \leqslant \alpha + 1$ и имеющих знаменатель, не превосходящий N. Тогда если $t \geqslant 1/C_N$, то каждое решение неравенства (14) имеет знаменатель, больший, чем N.

Следовательно, при иррациональном α множество решений в рациональных числах p/q неравенства (14) при всевозможных значениях t бесконечно.

Из неравенства (14), поскольку $q \leqslant t$, имеем неравенство

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}. \tag{19}$$

Из доказанного выше следует, что неравенство (19) при иррациональном α имеет решения p/q со сколь угодно большими знаменателями. Тем самым доказано следующее утверждение.

Теорема 7. *Для любого иррационального $\alpha \in \mathbf{R}$ неравенство (19) имеет бесконечное множество решений в рациональных числах p/q, $q > 0$.*

Эта теорема утверждает, что все действительные иррациональные числа допускают приближение рациональными дробями p/q порядка $1/q^2$.

Из теоремы 7 следует, что любое иррациональное число $\alpha \in \mathbf{R}$ представляется в форме

$$\alpha = \frac{p}{q} + \frac{\theta_q}{q^2}, \quad p \in \mathbf{Z}, \quad q \in \mathbf{N}, \quad |\theta_q| < 1, \tag{20}$$

где q может быть выбрано сколь угодно большим.

Представление иррационального числа α в виде (20) широко используется в теории чисел, других разделах математики и практических задачах.

Приведем пример иррационального числа, допускающего сколь угодно хороший степенной порядок приближения рациональными числами. Положим

$$\alpha = \sum_{n=1}^{\infty} \frac{1}{a^{n!}}, \quad a \in \mathbf{N}, \quad a \geqslant 2. \tag{21}$$

Обозначим

$$\sum_{n=1}^{k} \frac{1}{a^{n!}} = \frac{p_k}{q_k}, \quad q_k = a^{k!}, \quad p_k \in \mathbf{N}, \quad k = 1, 2, \ldots.$$

Тогда

$$0 < \alpha - \frac{p_k}{q_k} = r_k, \quad k = 1, 2, \ldots,$$

где

$$r_k = \frac{1}{a^{(k+1)!}} \left(1 + \frac{1}{a^{(k+2)!-(k+1)!}} + \ldots\right) <$$

$$< \frac{1}{a^{(k+1)!}} \left(1 + \frac{1}{a} + \frac{1}{a^2} + \ldots\right) =$$

$$= \frac{a}{a-1} \cdot \frac{1}{a^{(k+1)!}} = \frac{a}{a-1} \cdot \frac{1}{q_k^{k+1}} \leqslant \frac{1}{q_k^k}.$$

Поэтому

$$0 < \alpha - \frac{p_k}{q_k} < \frac{1}{q_k^k}, \quad k = 1, 2, \ldots.$$

Из последнего неравенства следует, что при любом натуральном k неравенство

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^k} \tag{22}$$

имеет решение p/q. Но каждое решение неравенства (22) с заданным значением k является решением того же неравенства с любым меньшим значением k. Отсюда следует, что неравенство (22) при любом k имеет бесконечное множество решений в рациональных числах p/q.

Если положить $a=10$, то ряд (21) будет десятичным разложением представляемого им числа

$$\alpha = 0{,}110001000\ldots,$$

у которого цифры на местах с номером $k!$ вправо от запятой равны единице, а все остальные цифры равны нулю.

В практических задачах часто иррациональное число α приближенно заменяют рациональным числом, являющимся отрезком его десятичного разложения. Пусть α имеет десятичное разложение:

$$\alpha = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_k}{10^k} + \ldots, \quad a_0 \in \mathbf{Z},$$

$$0 \leqslant a_k \leqslant 9, \quad k = 1, 2, \ldots.$$

Обозначим

$$\frac{A_k}{B_k} = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_k}{10^k},\ A_k \in \mathbf{Z},\ B_k = 10^k.$$

Тогда

$$\alpha = \frac{A_k}{B_k} + r_k,$$

где

$$r_k < \frac{9}{10^{k+1}}\left(1 + \frac{1}{10} + \frac{1}{10^2} + \ldots\right) = \frac{1}{10^k} = \frac{1}{B_k},$$

и поэтому

$$0 < \alpha - \frac{A_k}{B_k} < \frac{1}{B_k}. \tag{23}$$

Отсюда следует, что если положить приближенно $\alpha \approx A_k/B_k$, то погрешность при такой замене меньше, чем $1/B_k$.

Заменяя $\alpha \approx p/q$, где p/q есть решение неравенства (19), получим приближение для α с существенно лучшей погрешностью, меньшей, чем $1/q^2$.

Итак, теорема Дирихле позволила установить, что для любого иррационального числа α существует последовательность рациональных дробей p_k/q_k с растущими знаменателями, которая приближает α с точностью до $1/q_k^2$. Но теорема Дирихле является только теоремой существования и мало пригодна для нахождения соответствующих приближений на практике. Удобным средством для нахождения таких приближений являются цепные дроби. Соответствующие приближения для числа α находятся из его разложения в цепную дробь (см. [14, 20]).

§ 3. Приближение алгебраических чисел рациональными числами. Существование трансцендентных чисел

В 1844 г. Ж. Лиувилль (1809—1882), изучая приближение алгебраических чисел рациональными числами, показал, что алгебраические числа не могут слишком хорошо приближаться числами из $\mathbf{Q}$. В доказанной им теореме дается оценка порядка приближения алгебраического числа рациональными числами, зависящая от степени приближаемого числа.

Поскольку существуют иррациональные числа, допускающие сколь угодно хороший порядок приближения рациональными числами, то теорема Лиувилля позволила впервые построить примеры трансцендентных чисел.

Теорема Лиувилля. *Пусть α — действительное алгебраическое число степени n, $n \geqslant 2$. Тогда существует положительная постоянная c, зависящая только от α, такая, что при*

любых целых рациональных p и q, $q>0$, выполняется неравенство

$$\left|\alpha-\frac{p}{q}\right|>\frac{c}{q^n}. \tag{24}$$

Доказательство. Пусть $\alpha=\alpha_1, \ldots, \alpha_n$ — числа, сопряженные с α, и

$$\varphi(x)=a_nx^n+\ldots+a_1x+a_0=a_n(x-\alpha)\prod_{i=2}^{n}(x-\alpha_i),\ a_n>0, \tag{25}$$

— неприводимый и примитивный многочлен с целыми рациональными коэффициентами, имеющий α своим корнем, а p и q, $q>0$, — любые целые рациональные числа. Возможны два случая.

1) p и q таковы, что

$$\left|\alpha-\frac{p}{q}\right|\geqslant 1.$$

Тогда тем более, так как $q\geqslant 1$, имеем

$$\left|\alpha-\frac{p}{q}\right|\geqslant\frac{1}{q^n}. \tag{26}$$

2) p и q таковы, что

$$\left|\alpha-\frac{p}{q}\right|<1.$$

Следовательно,

$$\left|\frac{p}{q}\right|<|\alpha|+1. \tag{27}$$

Подставляя в равенство (25) $x=p/q$, ввиду неравенства (27) получим

$$\left|\varphi\left(\frac{p}{q}\right)\right|=a_n\left|\alpha-\frac{p}{q}\right|\prod_{i=2}^{n}\left|\alpha_i-\frac{p}{q}\right|\leqslant$$

$$\leqslant a_n\left|\alpha-\frac{p}{q}\right|\prod_{i=2}^{n}\left(|\alpha_i|+\left|\frac{p}{q}\right|\right)<$$

$$<a_n\left|\alpha-\frac{p}{q}\right|\prod_{i=2}^{n}(|\alpha_i|+|\alpha|+1)\leqslant a_n\left|\alpha-\frac{p}{q}\right|(2|\overline{\alpha}|+1)^{n-1}. \tag{28}$$

Неприводимый многочлен $\varphi(x)$ степени $n\geqslant 2$ не имеет рациональных корней. Поэтому $\varphi(p/q)\neq 0$ и

$$\left|\varphi\left(\frac{p}{q}\right)\right|=\frac{|a_np^n+a_{n-1}p^{n-1}q+\ldots+a_0q^n|}{q^n}\geqslant\frac{1}{q^n}. \tag{29}$$

Полагая

$$c = \frac{1}{a_n (2|\alpha| + 1)^{n-1}},$$

из неравенств (28) и (29) получаем неравенство

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n}. \tag{30}$$

Так как $c<1$, то из неравенств (26) и (30) следует, что последнее неравенство выполняется и в первом, и во втором случаях. Теорема доказана.

Теорема Лиувилля справедлива и при $n=1$, когда $\alpha=a/b$ есть рациональное число, но только с ограничением, что $p/q \neq \alpha$. Этот результат был установлен еще в § 3 в неравенстве (12).

Из неравенства (24) следует, что при условиях теоремы Лиувилля неравенство

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{c}{q^n} \tag{31}$$

не имеет решений в числах p и q, $q>0$. Это означает, что алгебраическое число степени n не может допускать приближение рациональными числами p/q порядка $1/q^\nu$, где $\nu>n$.

Если α — действительная квадратичная иррациональность (т. е. корень квадратного уравнения с рациональными коэффициентами), то по теореме Лиувилля существует постоянная $c>0$, такая, что неравенство

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^2} \tag{32}$$

не имеет решений в числах p и q. Но по теореме 7 неравенство

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2} \tag{33}$$

имеет бесконечное множество решений в числах p и q.

Неравенства (32) и (33) означают, что $1/q^2$ — в некотором смысле наилучший порядок приближения рациональными числами p/q для действительных квадратичных иррациональностей.

Теорема Лиувилля дает некоторый необходимый признак алгебраичности числа α и, следовательно, достаточный признак трансцендентности. Из нее легко получаем следующее утверждение.

Теорема 8. *Если для действительного числа α при любом натуральном k неравенство*

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^k} \tag{34}$$

имеет бесконечное множество решений в целых числах p и q, $q>0$, то α — трансцендентное число.

Доказательство. Допустим противное, что α удовлетворяет условиям теоремы 8, но является алгебраическим числом степени n. Тогда по теореме Лиувилля существует число $c=c(\alpha)>0$ такое, что неравенство (31) не имеет решений в числах p и q.

Положим в неравенстве (34) $k=n+1$. Оно имеет бесконечное множество решений в числах p и q. Будем рассматривать решения этого неравенства только со знаменателями q такими, что $1/q<c$. Тогда неравенство

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^n}\cdot\frac{1}{q}<\frac{c}{q^n}$$

имеет бесконечное множество решений. Но это противоречит предположению о решениях неравенства (31). Противоречие завершает доказательство теоремы.

В § 3 было показано, что для числа

$$\alpha=\sum_{n=1}^{\infty}\frac{1}{a^{n!}},\quad a\in\mathbf{N},\ a\geqslant 2,$$

неравенство (34) при любом $k\in\mathbf{N}$ имеет бесконечное множество решений в числах p и q, $q>0$. Поэтому по теореме 8 число α трансцендентно.

Из теоремы 8 и приведенного примера следует

Теорема 9. *Существуют трансцендентные числа.*

Заметим, что еще за 100 лет до опубликования теоремы Лиувилля Л. Эйлер высказал утверждение о существовании трансцендентных чисел. Но доказать его он не мог.

В 1874 г. Г. Кантор (1845—1918) другим методом доказал существование трансцендентных чисел. Развивая начала теории множеств, он показал, что множество всех алгебраических чисел счетно, а множество действительных чисел несчетно. Следовательно, существуют трансцендентные числа. Более того, почти все числа в смысле меры Лебега трансцендентны.

С помощью теоремы Лиувилля можно строить примеры трансцендентных чисел только из узкого класса чисел, допускающих очень хорошее приближение рациональными числами. Доказательства трансцендентности чисел других классов обычно сопряжены с большими трудностями.

Высотой многочлена $P(x)$ называют наибольший из модулей его коэффициентов.

Перепишем неравенство (24) в теореме Лиувилля при $n\geqslant 1$ следующим образом:

$$|q\alpha-p|>\frac{c}{q^{n-1}},\quad \frac{p}{q}\neq\alpha. \tag{35}$$

Если обозначить

$$P(x)=a_1x+a_0,\ a_1,\ a_0\in\mathbf{Z},$$

и H — высота многочлена $P(x)$, то из неравенства (35) следует, что если $P(\alpha)\neq 0$, то выполняется неравенство

$$|P(\alpha)|>\frac{c}{|a_1|^{n-1}}\geqslant\frac{c}{H^{n-1}}.$$

Аналогичное утверждение выполняется и для многочлена $P(x)$ любой степени k.

Теорема 10. *Пусть α — алгебраическое число степени n, $n\geqslant 1$. Тогда существует постоянная $c>0$, зависящая только от числа α, такая, что для любого многочлена $P(x)$ степени k, $k\geqslant 1$, с целыми рациональными коэффициентами и высоты H либо $P(\alpha)=0$, либо выполняется неравенство*

$$|P(\alpha)|\geqslant\frac{c^k}{H^{n-1}}. \tag{36}$$

Доказательство. Пусть

$$P(x)=a_kx^k+\ldots+a_1x+a_0, \tag{37}$$

а $\alpha=\alpha_1, \ldots, \alpha_n$ — числа, сопряженные с α. Предположим, что $P(\alpha)\neq 0$. Тогда по лемме 2 $P(\alpha_i)\neq 0$, $i=1, \ldots, n$. По теореме 6 существует число $r=a_k$ такое, что $\beta=r\alpha$ есть целое алгебраическое число. Имеем

$$r^{k-1}P(\alpha)=Q(\beta),$$

где

$$Q(x)=x^k+a_{k-1}x^{k-1}+ra_{k-2}x^{k-2}+\ldots+r^{k-1}a_0$$

— многочлен с целыми рациональными коэффициентами. Произведение

$$Q(\beta_1)Q(\beta_2)\cdots Q(\beta_n),\quad \beta_i=r\alpha_i,\ i=1, \ldots, n,$$

есть симметрический многочлен с целыми рациональными коэффициентами от величин $\beta_1, \ldots, \beta_n$, которые, очевидно, являются сопряженными для числа β. Так как β — целое алгебраическое число, то по лемме 6 это произведение есть целое рациональное число. Но $P(\alpha_i)\neq 0$, $i=1, \ldots, n$. Поэтому $Q(\beta_i)\neq 0$, $i=1, \ldots, n$. Значит,

$$|Q(\beta)|\prod_{i=2}^{n}|Q(\beta_i)|\geqslant 1,$$

или

$$r^{kn}|P(\alpha)|\prod_{i=2}^{n}|P(\alpha_i)|\geqslant 1. \tag{38}$$

Ввиду равенства (37) получаем оценки:

$$|P(\alpha_i)| \leqslant H(1 + |\alpha_i| + \ldots + |\alpha_i|^k) \leqslant$$

$$\leqslant H(1 + |\alpha_i|)^k \leqslant H(1 + |\overline{\alpha}|)^k, \quad i = 2, \ldots, n. \tag{39}$$

Из неравенств (38) и (39) находим, что

$$(r^n(1 + |\overline{\alpha}|)^{n-1})^k H^{n-1} |P(\alpha)| \geqslant 1.$$

Полагая

$$c = \frac{1}{r^n(1 + |\overline{\alpha}|)^{n-1}},$$

получаем неравенство (36). Теорема доказана.

Теорема Лиувилля была существенно усилена. Она положила начало развитию большого и очень важного раздела теории чисел — теории приближения алгебраических чисел.

§ 4. Трансцендентность числа e

Покажем сначала, что число e иррационально, т. е. не является алгебраическим числом первой степени. Это доказательство весьма просто. Оно было приведено еще в опубликованном в 1815 г. курсе анализа Ш. Фурье (1768—1830).

Теорема 11. *Число e иррационально.*

Доказательство. Из представления числа e в виде ряда

$$e = \sum_{k=0}^{\infty} \frac{1}{k!}$$

следует, что для каждого натурального n выполняется равенство

$$n!\, e = A_n + \frac{r_n}{n+1}, \tag{40}$$

где

$$A_n = n! \sum_{k=0}^{n} \frac{1}{k!} \in \mathbf{Z}, \quad r_n = (n+1)! \sum_{k=n+1}^{\infty} \frac{1}{k!} > 0. \tag{41}$$

Оценивая величину r_n, получим

$$r_n = 1 + \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} + \ldots$$

$$\ldots < 1 + \frac{1}{2} + \frac{1}{2^2} + \ldots = 2. \tag{42}$$

Предположим, что число e рационально. Положим n равным знаменателю числа e. Тогда $n!e$ — целое число. Но это

противоречит равенству (40), поскольку из условий (41) и неравенства (42) следует, что A_n — целое число, а

$$0 < \frac{r_n}{n+1} < \frac{2}{n+1} \leqslant 1.$$

Полученное противоречие доказывает теорему 11.

Докажем теперь более общее утверждение, установленное в 1840 г. Ж. Лиувиллем.

Теорема 12. *Число e не является квадратичной иррациональностью.*

Доказательство. Допустим противное. Тогда имеет место равенство

$$ae^2+be+c=0,\ a,\ b,\ c\in\mathbf{Z}, \tag{43}$$

где не все числа a, b, и c равны нулю. Ввиду теоремы 11 должны выполняться условия $a\neq 0$, $c\neq 0$. Можно считать, что $a>0$. Из равенства (43) следует, что

$$ae+b+ce^{-1}=0,\ a>0,\ c\neq 0. \tag{44}$$

Так как

$$e^{-1} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!},$$

то

$$n!\, e^{-1} = B_n + \frac{(-1)^{n+1}\rho_n}{n+1}, \tag{45}$$

где

$$B_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \in \mathbf{Z},\ \rho_n = (n+1)! \sum_{k=n+1}^{\infty} \frac{(-1)^{k-n-1}}{k!}.$$

Число ρ_n есть сумма знакочередующего ряда:

$$\rho_n = 1 - \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} - \ldots$$

с монотонно убывающими по абсолютной величине членами. Следовательно, по признаку сходимости Лейбница имеем, что $\rho_n<1$ и

$$\rho_n = 1 - \left(\frac{1}{n+2} - \frac{1}{(n+2)(n+3)} + \ldots\right) > 1 - \frac{1}{n+2} > 0.$$

Итак, выполняются неравенства

$$0<\rho_n<1. \tag{46}$$

Умножив равенство (44) на $n!$ и воспользовавшись равенствами (45) и (40), получим

$$0 = n!\,(ae + b + ce^{-1}) =$$

$$= aA_n + bn! + cB_n + \frac{ar_n + (-1)^{n+1} c\,\rho_n}{n+1}. \tag{47}$$

Выберем число n удовлетворяющим условиям

$$n>2a+|c|, \quad (-1)^{n+1}c>0. \tag{48}$$

Тогда из неравенств (41), (42), (46) и (48) находим, что

$$ar_n+(-1)^{n+1}c\rho_n>0 \tag{49}$$

и

$$\frac{ar_n+(-1)^{n+1}c\rho_n}{n+1}<\frac{2a+|c|}{n+1}<1. \tag{50}$$

Поскольку

$$aA_n+bn!+cB_n$$

есть целое число, то из неравенств (49) и (50) следует, что правая часть равенства (47) не является целым числом. Но это противоречит тому, что она равна нулю.

Таким образом, получено противоречие, доказывающее теорему 12.

Замечание. Доказательство теоремы 11 основано на том, что число e допускает приближение рациональными числами p/q более высокого порядка $\varphi(q)$, чем $1/q$, т. е. такого, что $\varphi(q)q\to 0$ при $q\to\infty$.

Для доказательства трансцендентности числа e необходимо показать, что e не может быть корнем многочлена с целыми коэффициентами любой степени. Попытки доказать это элементарными рассуждениями, подобными приведенным выше, к успеху не привели. Проблема была решена в 1873 г. Ш. Эрмитом с помощью созданного им аналитического метода.

Доказательство трансцендентности числа e основывается на одном интегральном равенстве, называемом тождеством Эрмита.

Пусть $f(x)$ — некоторый многочлен с действительными коэффициентами степени ν. Интегрируя по частям, приходим к равенству

$$\int_0^x f(t)\,e^{-t}\,dt=\int_0^x f(t)\,d(-e^{-t})=f(0)-f(x)\,e^{-x}+\int_0^x f'(t)\,e^{-t}\,dt. \tag{51}$$

Повторяя эту операцию последовательно $\nu+1$ раз, из равенства (51) получим, что

$$\int_0^x f(t)\,e^{-t}\,dt=F(0)-F(x)\,e^{-x}, \tag{52}$$

где многочлен $F(x)$ имеет вид

$$F(x)=f(x)+f'(x)+\ldots+f^{(\nu)}(x). \tag{53}$$

Равенство (52) называется тождеством Эрмита.

Из равенства (52) следует, что для каждого целого числа k, $k \geqslant 0$, выполняется равенство

$$\int_0^k f(t)\, e^{-t}\, dt = F(0) - e^{-k} F(k),$$

или равенство

$$F(0)\, e^k - F(k) = e^k \int_0^k f(t)\, e^{-t}\, dt. \tag{54}$$

Докажем одно простое вспомогательное предложение.

Лемма 7. *Если* $g(x) \in \mathbf{Z}[x]$, *то все коэффициенты многочлена* $g^{(k)}(x)$, $k \geqslant 1$, *делятся на* $k!$.

Доказательство. Ввиду линейности операции дифференцирования утверждение леммы достаточно доказать для многочленов x^s, $s \geqslant 0$. В этом случае оно следует из равенств

$$(x^s)^{(k)} = \begin{cases} 0, & \text{если } k > s, \\ k! \binom{s}{k} \cdot x^{s-k}, & \text{если } 1 \leqslant k \leqslant s, \end{cases}$$

так как $\binom{s}{k}$ — целое число.

Теорема 13. *Число* e *трансцендентно.*

Доказательство. Допустим противное, что e — алгебраическое число степени m. Тогда выполняется равенство

$$a_m e^m + \ldots + a_1 e + a_0 = 0, \quad a_0 \neq 0, \tag{55}$$

где $a_0, a_1, \ldots, a_m$ — целые рациональные числа.

Положим в тождестве Эрмита

$$f(x) = \frac{1}{(n-1)!}\, x^{n-1} ((x-1) \cdots (x-m))^n, \tag{56}$$

где n — достаточно большое натуральное число. Сложим равенства (54) для значений $k = 0, 1, \ldots, m$, умножив их соответственно на a_k. Так как выполняется равенство (55), то в результате получаем, что

$$-\sum_{k=0}^{m} a_k F(k) = \sum_{k=0}^{m} a_k e^k \int_0^k f(t)\, e^{-t}\, dt. \tag{57}$$

Покажем, что при некотором достаточно большом n левая часть равенства (57) будет отличным от нуля целым числом, а его правая часть по абсолютной величине меньше 1. Тогда это равенство будет противоречиво, и теорема будет доказана.

Так как многочлен $f(x)$ (56) имеет число 0 корнем кратности $n-1$, а числа $1, \ldots, m$ — корнями кратности n, то

$$f^{(l)}(0)=0,\ l=0,\ 1,\ldots,n-2, \tag{58}$$

$$f^{(n-1)}(0)=(-1)^{mn}(m!)^n \tag{59}$$

и

$$f^{(l)}(k)=0,\ l=0,\ 1,\ldots,n-1,\ k=1,\ldots,m. \tag{60}$$

По лемме 7 коэффициенты производной порядка l многочлена $x^{n-1}((x-1)\cdots(x-m))^n$ есть целые числа, делящиеся на $l!$. Следовательно, все производные $f^{(l)}(x)$ при $l\geqslant n$ имеют целые коэффициенты, делящиеся на число n.

Поэтому из равенств (53), (58) и (59) находим, что

$$F(0)=\sum_{l=n-1}^{(m+1)n-1} f^{(l)}(0)=(-1)^{mn}(m!)^n+nA,\ A\in\mathbf{Z}, \tag{61}$$

а из равенств (60) аналогично имеем, что

$$F(k)=\sum_{l=n}^{(m+1)n-1} f^{(l)}(k)=nB_k,\ B_k\in\mathbf{Z},\ k=1,\ \ldots,\ m. \tag{62}$$

Пусть теперь число n удовлетворяет условиям

$$(n,\ m!)=1,\quad n>|a_0|. \tag{63}$$

Тогда из равенств (61) и (62) имеем, что все слагаемые в левой части равенства (57) являются целыми числами, причем $a_0F(0)$ не делится на n, а все остальные слагаемые $a_kF(k)$ делятся на n. Отсюда следует, что левая часть равенства (57) есть отличное от нуля целое число и, значит,

$$\Big|\sum_{k=0}^{m} a_k F(k)\Big|\geqslant 1. \tag{64}$$

Оценим теперь правую часть равенства (57). На отрезке $0\leqslant x\leqslant m$ каждый сомножитель $x-k$, $0\leqslant k\leqslant m$, входящий в произведение (56), не превышает по модулю числа m. Следовательно, справедлива оценка

$$|f(x)|<\frac{m^{(m+1)n-1}}{(n-1)!},\quad 0\leqslant x\leqslant m,$$

а тогда

$$\Big|\sum_{k=0}^{m} a_k e^k\int_0^k f(t)\,e^{-t}\,dt\Big|<\frac{m^{(m+1)n}}{(n-1)!}\sum_{k=0}^{m}|a_k|\,e^k\int_0^k e^{-t}\,dt<$$

$$<\frac{m^{(m+1)n}}{(n-1)!}\,e^m\sum_{k=0}^{m}|a_k|=c_0\frac{c^n}{(n-1)!}, \tag{65}$$

где постоянные c_0 и c не зависят от числа n.

Из равенства (57), условий (63) и неравенств (64) и (65) получаем, что

$$1 \leqslant \left| \sum_{k=0}^{m} a_k F(k) \right| < c_0 \frac{c^n}{(n-1)!}. \qquad (66)$$

Правая часть неравенства (66) стремится к нулю при $n \to \infty$. Выберем число n так, чтобы выполнялись условия (63) и неравенство

$$c_0 \frac{c^n}{(n-1)!} < 1.$$

Тогда неравенство (66) будет противоречиво, и теорема доказана.

Существует много доказательств трансцендентности числа e. Большинство из них основывается на методе Эрмита, а друг от друга они отличаются лишь в деталях.

Замечание. Рассмотрим равенство (54). Из равенств (61) и (62) имеем, что $F(k)$, $k=0, 1, \ldots, m$, — являются целыми числами. Оценивая правую часть равенства (54) аналогично тому, как была оценена правая часть равенства (57), получим, что она стремится к нулю при $n \to \infty$. Отсюда следует, что дроби

$$\frac{F(k)}{F(0)}, \quad k = 1, \ldots, m,$$

при каждом n являются совместными приближениями к степеням e^k, $k=1, \ldots, m$. Так называют рациональные приближения к нескольким числам, имеющие одинаковые знаменатели.

Это показывает, что основой рассматриваемого метода является построение с помощью тождества Эрмита последовательности совместных приближений к степеням числа e.

§ 5. Трансцендентность числа π

Попытки решить проблему квадратуры круга привлекали внимание к исследованию арифметической природы числа π очень давно. Важным шагом в этом направлении был результат И. Ламберта (1728—1777), который в 1766 г. доказал иррациональность числа π с помощью разложения в цепную дробь функции $\operatorname{tg} x$. Он доказал иррациональность чисел $\operatorname{tg} x$ при любом рациональном $x \neq 0$, откуда и следовало, что π есть иррациональное число.

Ниже приводится доказательство Эрмита иррациональности числа π, построенное на идее, с помощью которой им была доказана трансцендентность числа e.

Теорема 14. *Число π иррационально.*

Доказательство. Пусть $f(x)$ — произвольный многочлен с действительными коэффициентами. Положим

$$F(x)=f(x)-f''(x)+f^{(4)}(x)-f^{(6)}(x)+\ldots.$$

Очевидно, что $F(x)$ — многочлен, так как $f^{(k)}(x)\equiv 0$, начиная с некоторого k. Имеем

$$\frac{d}{dx}\left(F'(x)\sin x-F(x)\cos x\right)=\left(F''(x)+F(x)\right)\sin x=f(x)\sin x.$$

Интегрируя, получаем равенство

$$\int_0^{\pi} f(x)\sin x\,dx=F(\pi)+F(0), \tag{67}$$

представляющее собой аналог тождества Эрмита.

Допустим противное, что π — рациональное число, $\pi=a/b$, $b>0$. Положим в равенстве (67)

$$f(x)=\frac{b^n}{n!}x^n(\pi-x)^n=\frac{1}{n!}x^n(a-bx)^n$$

при достаточно большом натуральном n.

Так как многочлен $f(x)$ имеет число 0 корнем кратности n, то

$$f(0)=f'(0)=\ldots=f^{(n-1)}(0)=0.$$

По лемме 7 все коэффициенты производной многочлена $x^n(a-bx)^n$ порядка l делятся на $l!$. Поэтому все производные многочлена $f(x)$ порядка $l\geqslant n$ имеют целые коэффициенты. Отсюда следует, что все числа

$$f(0),\ f'(0),\ \ldots,\ f^{(2n)}(0),\ \ldots$$

являются целыми.

Поскольку $f(x)=f(\pi-x)$, то

$$f^{(l)}(x)=(-1)^l f^{(l)}(\pi-x),\ l=0,\ 1,\ 2,\ldots,$$

откуда при $x=\pi$

$$f^{(l)}(\pi)=(-1)^l f^{(l)}(0),\ l=0,\ 1,2,\ldots.$$

Поэтому $f^{(l)}(\pi)\in\mathbf{Z}$, $l=0,1,2,\ldots$. Значит, $F(\pi)+F(0)$ есть число из $\mathbf{Z}$.

Итак, правая часть равенства (67) есть целое рациональное число.

Покажем, что при достаточно большом n будет выполняться неравенство

$$0<\int_0^{\pi} f(x)\sin x\,dx<1.$$

Тогда равенство (67) будет противоречиво, и теорема будет доказана.

Действительно, $f(x)>0$ на интервале $0<x<\pi$. По непрерывности $f(x)$ имеем, что

$$\int_0^\pi f(x)\sin x\,dx>0.$$

С другой стороны, существует число $n_0\in\mathbf{N}$ такое, что

$$\int_0^\pi f(x)\sin x\,dx\leqslant\int_0^\pi f(x)\,dx<\frac{b^n}{n!}\pi^{2n}\int_0^\pi dx=\pi\frac{(a^2/b)^n}{n!}<1$$

для каждого $n\geqslant n_0$, так как при любом постоянном c

$$\lim_{n\to\infty}\frac{c^n}{n!}=0.$$

Трансцендентность числа π доказал в 1882 г. Ф. Линдеман, пользуясь методом Эрмита. Тем самым было получено отрицательное решение проблемы квадратуры круга.

Ниже будет приведено другое доказательство трансцендентности π. В основе его лежит построение с помощью аналитического метода многочленов $P_n(x)\in\mathbf{Z}[x]$, принимающих в точке π отличные от нуля малые значения. Получающиеся при этом оценки сверху для $|P_n(\pi)|$ оказываются сильнее, чем оценки снизу, справедливые по теореме 10 для многочленов от алгебраических чисел. Отсюда будет следовать, что π не может быть алгебраическим числом.

Числа $P_n(\pi)$ получаются с помощью разложения функции $\sin\pi z$ в интерполяционный ряд Ньютона. Поэтому сначала рассмотрим интерполяционную формулу и интерполяционный ряд Ньютона.

Пусть $f(z)$ — аналитическая функция в области D, а $z_1,\ldots,z_n$ — фиксированный набор точек из D, среди которых могут быть и совпадающие.

Положим

$$F_0(\zeta)=1,\ F_k(\zeta)=(\zeta-z_1)\cdots(\zeta-z_k),\ k=1,\ \ldots,\ n. \tag{68}$$

Тогда

$$F_k(\zeta)=(\zeta-z_k)F_{k-1}(\zeta),\ k=1,\ldots,n. \tag{69}$$

Пусть $z\in D$. Для каждого k, $k=1,\ldots,n$, справедливо тождество

$$\frac{1}{\zeta-z}\left(1-\frac{z-z_k}{\zeta-z_k}\right)=\frac{1}{\zeta-z_k}.$$

Умножая обе его части на $F_{k-1}(z)/F_{k-1}(\zeta)$ и пользуясь равенствами (69), находим

$$\frac{1}{\zeta-z}\left(\frac{F_{k-1}(z)}{F_{k-1}(\zeta)}-\frac{F_k(z)}{F_k(\zeta)}\right)=\frac{F_{k-1}(z)}{F_k(\zeta)},\ k=1,\ \ldots,\ n. \tag{70}$$

Складывая почленно все тождества (70), ввиду того что $F_0(\zeta)=1$, получаем тождество

$$\frac{1}{\zeta-z}-\frac{F_n(z)}{F_n(\zeta)(\zeta-z)}=\sum_{k=1}^{n}\frac{F_{k-1}(z)}{F_k(\zeta)},$$

или

$$\frac{1}{\zeta-z}=\sum_{k=1}^{n}\frac{F_{k-1}(z)}{F_k(\zeta)}+\frac{F_n(z)}{F_n(\zeta)(\zeta-z)}. \tag{71}$$

Выберем простой замкнутый контур C, лежащий в D, такой, что ограниченная им область принадлежит D и содержит все точки $z_1,\ldots,z_n$ и z. Умножим обе части тождества (71) на $\frac{1}{2\pi i}f(\zeta)$ и после этого проинтегрируем по контуру C в положительном направлении. В результате, пользуясь формулой Коши, получим равенство

$$f(z)=\frac{1}{2\pi i}\int_C\frac{f(\zeta)}{\zeta-z}\,d\zeta=$$

$$=\sum_{k=1}^{n}F_{k-1}(z)\,\frac{1}{2\pi i}\int_C\frac{f(\zeta)}{F_k(\zeta)}\,d\zeta+\frac{1}{2\pi i}\int_C\frac{F_n(z)f(\zeta)}{F_n(\zeta)(\zeta-z)}\,d\zeta. \tag{72}$$

Обозначим

$$A_{k-1}=\frac{1}{2\pi i}\int_C\frac{f(\zeta)}{F_k(\zeta)}\,d\zeta,\quad k=1,\ldots,n, \tag{73}$$

$$R_n(z)=\frac{1}{2\pi i}\int_C\frac{F_n(z)f(\zeta)}{F_n(\zeta)(\zeta-z)}\,d\zeta. \tag{74}$$

Заметим, что по теореме Коши интегралы (73) и (74) не зависят от выбора контура C, удовлетворяющего указанным условиям. Из равенств (72), (73) и (74) имеем

$$f(z)=\sum_{k=0}^{n-1}A_kF_k(z)+R_n(z),\quad z\in D. \tag{75}$$

Равенство (75) называется интерполяционной формулой Ньютона для функции $f(z)$ с узлами интерполяции $z_1,\ldots,z_n$.

Теперь рассмотрим бесконечную последовательность $z_1,\ldots,z_n,\ldots$ точек из D. Если предположить, что

$$\lim_{n\to\infty}R_n(z)=0$$

для всех z, принадлежащих области $D_0\subset D$, то

$$f(z)=\sum_{n=0}^{\infty}A_nF_n(z)=\sum_{n=0}^{\infty}A_n(z-z_1)\cdots(z-z_n),\ z\in D_0. \tag{76}$$

Ряд (76) называется интерполяционным рядом Ньютона для функции $f(z)$ в области D_0 с узлами интерполяции $z_1, \ldots, z_n \ldots$.

Если все узлы интерполяции совпадают, то ряд Ньютона переходит в ряд Тейлора.

Если функция $f(z)$ не является многочленом, то из равенства (76) следует, что $A_n \neq 0$ для бесконечного множества значений n.

Разложим теперь в ряд Ньютона функцию $f(z) = \sin \pi z$, выбирая за узлы интерполяции следующую бесконечную периодическую последовательность точек с периодом m:

$$z_1, z_2, \ldots, z_n, \ldots, \tag{77}$$

где

$$z_n = n \text{ для } n = 1, \ldots, m,$$
$$z_{n+m} = z_n \text{ для всех } n \geqslant 1, \tag{78}$$

а m — некоторое фиксированное натуральное число.

Выберем любое $R > m$ и рассмотрим остаточный член (74) интерполяционной формулы Ньютона для функции $\sin \pi z$ с узлами интерполяции (77) при $n > 2R$:

$$R_n(z) = \frac{1}{2\pi i} \int_C \frac{(z - z_1) \cdots (z - z_n) \sin \pi \zeta}{(\zeta - z_1) \cdots (\zeta - z_n)(\zeta - z)} d\zeta, \quad |z| \leqslant R, \tag{79}$$

где C — окружность $|\zeta| = n$.

Оценим интеграл (79). Из условий (78) следует, что $1 \leqslant z_k \leqslant m$, $k = 1, \ldots, n$, а

$$|z - z_k| \leqslant |z| + |z_k| \leqslant R + m$$

для всех z таких, что $|z| \leqslant R$. Поэтому для таких z

$$\left| \prod_{k=1}^{n} (z - z_k) \right| \leqslant (R + m)^n. \tag{80}$$

Далее, на окружности $|\zeta| = n$ имеем, что

$$|\zeta - z_k| \geqslant |\zeta| - |z_k| \geqslant n - m > \frac{n}{2},$$

так как $n > 2R > 2m$. Аналогично,

$$|\zeta - z| \geqslant n - R > \frac{n}{2}.$$

Тогда

$$\left| (\zeta - z) \prod_{k=1}^{n} (\zeta - z_k) \right| > \left(\frac{n}{2} \right)^{n+1}. \tag{81}$$

На той же окружности $|\zeta| = n$ имеем

$$|\sin \pi \zeta| = \left| \frac{e^{\pi \zeta i} - e^{-\pi \zeta i}}{2i} \right| \leqslant e^{\pi |\zeta|} = e^{\pi n}. \tag{82}$$

Пользуясь неравенствами (80), (81) и (82) для оценки интеграла (79), получим

$$|R_n(z)| \leqslant \frac{1}{2\pi} 2\pi n \frac{e^{\pi n}(R+m)^n}{\left(\frac{n}{2}\right)^{n+1}} = \frac{2^{n+1} e^{\pi n}(R+m)^n}{n^n}, \quad |z| \leqslant R. \tag{83}$$

Поскольку числа R и m фиксированы, то из неравенства (83) следует, что

$$\lim_{n\to\infty} R_n(z) = 0 \tag{84}$$

для всех z таких, что $|z| \leqslant R$.

Число R можно выбрать сколь угодно большим. Поэтому при любом комплексном z выполняется равенство (84) и имеет место разложение функции $\sin \pi z$ в интерполяционный ряд Ньютона (76), где A_n и $F_n(\zeta)$ определяются формулами (73) и (68).

Итак,

$$\sin \pi z = \sum_{n=0}^{\infty} A_n (z - z_1) \cdots (z - z_n), \tag{85}$$

где

$$A_n = \frac{1}{2\pi i} \int_C \frac{\sin \pi\zeta}{(\zeta - z_1) \cdots (\zeta - z_{n+1})} d\zeta. \tag{86}$$

Выбирая за контур C окружность $|\zeta| = n$, где $n > 2m$, и рассуждая так же, как в случае оценки интеграла (79), получим оценку сверху для A_n:

$$|A_n| \leqslant \frac{1}{2\pi} 2\pi n \frac{e^{\pi n}}{\left(\frac{n}{2}\right)^{n+1}} = \frac{e^{\pi n + (n+1)\ln 2}}{n^n} < e^{5n} n^{-n}. \tag{87}$$

В дальнейшем потребуется оценка A_n снизу. Для этого введем некоторые обозначения и докажем одно вспомогательное предложение.

Из условий (78), определяющих последовательность (77), следует, что

$$F_{n+1}(\zeta) = (\zeta - z_1) \cdots (\zeta - z_{n+1}) = \prod_{k=1}^{m} (\zeta - k)^{r_k + 1}, \tag{88}$$

где целые числа r_k удовлетворяют условиям

$$r_1 + \ldots + r_m + m = n + 1,$$

$$r_1 - 1 \leqslant r_m \leqslant r_{m-1} \leqslant \ldots \leqslant r_1 \leqslant \frac{n}{m}. \tag{89}$$

Тогда равенство (86) примет вид

$$A_n = \frac{1}{2\pi i}\int_C \frac{\sin \pi\zeta}{F_{n+1}(\zeta)}\,d\zeta = \frac{1}{2\pi i}\int_C \frac{\sin \pi\zeta}{(\zeta-1)^{r_1+1}\ldots(\zeta-m)^{r_m+1}}\,d\zeta. \tag{90}$$

Обозначим $r = r_1 = \max\limits_{1\leqslant k\leqslant m} r_k$, а M — общее наименьшее кратное чисел $1, \ldots, m$.

Лемма 8. *Существует многочлен $P_n(x)$ с целыми рациональными коэффициентами степени, не большей r, высоты, не превосходящей $r!(2M)^n$, такой, что*

$$M^{n-1}r!A_n = P_n(\pi).$$

Доказательство. По теореме Коши из равенства (90) имеем

$$A_n = \sum_{k=1}^{m} \frac{1}{2\pi i}\int_{\Gamma_k} \frac{\sin \pi\zeta}{(\zeta-1)^{r_1+1}\ldots(\zeta-m)^{r_m+1}}\,d\zeta, \tag{91}$$

где Γ_k — окружность с центром в точке k и радиуса $1/2$, $|\zeta-k|=1/2$, с обходом в положительном направлении.

Разложим функцию $\sin \pi\zeta$ в ряд Тейлора по степеням $\zeta-k$:

$$\sin \pi\zeta = \sin(\pi k + \pi(\zeta-k)) = (-1)^k \sin \pi(\zeta-k) =$$

$$= \sum_{l=0}^{\infty} \frac{(-1)^{l+k}\pi^{2l+1}}{(2l+1)!}(\zeta-k)^{2l+1}.$$

Из этого представления следует, что

$$\sin \pi\zeta = \sum_{0\leqslant l\leqslant \frac{r_k-1}{2}} \frac{(-1)^{l+k}\pi^{2l+1}}{(2l+1)!}(\zeta-k)^{2l+1} + R_k(\zeta),$$

где $R_k(\zeta)$ есть целая функция, имеющая в точке $\zeta=k$ нуль порядка не меньше, чем r_k+1. Поэтому выполняется равенство

$$\int_{\Gamma_k} \frac{R_k(\zeta)}{(\zeta-1)^{r_1+1}\ldots(\zeta-m)^{r_m+1}}\,d\zeta = 0$$

и

$$\frac{1}{2\pi i}\int_{\Gamma_k} \frac{\sin \pi\zeta}{(\zeta-1)^{r_k+1}\ldots(\zeta-m)^{r_m+1}}\,d\zeta =$$

$$= \sum_{0\leqslant l\leqslant \frac{r_k-1}{2}} \frac{(-1)^{l+k}\pi^{2l+1}}{(2l+1)!} \times$$

$$\times \frac{1}{2\pi i}\int\limits_{\Gamma_k}\frac{(\zeta-k)^{2l+1}}{(\zeta-1)^{r_1+1}\dots(\zeta-m)^{r_m+1}}\,d\zeta. \tag{92}$$

Обозначим при каждом k, $1\leqslant k\leqslant m$,

$$a_{k,l}=\frac{1}{2\pi i}\int\limits_{\Gamma_k}\frac{(\zeta-k)^{2l+1}}{(\zeta-1)^{r_1+1}\dots(\zeta-m)^{r_m+1}}\,d\zeta,\ 0\leqslant l\leqslant\frac{r_k-1}{2}. \tag{93}$$

Докажем, что $a_{k,l}$ — рациональные числа, такие, что все произведения $M^{n-1}a_{k,l}$ являются целыми числами.

Число $a_{k,l}$ равно вычету в точке $\zeta=k$ подынтегральной функции в интеграле (93), т. е. коэффициенту при $(\zeta-k)^{-1}$ в разложении этой функции в ряд Лорана по степеням $\zeta-k$. Найдем это разложение.

Пусть $s\in\mathbf{N}$, $1\leqslant s\leqslant m$, $s\neq k$. Рассмотрим функцию

$$\frac{1}{\zeta-s}=\frac{1}{(\zeta-k)+(k-s)}=\frac{1}{k-s}\cdot\frac{1}{1-\dfrac{\zeta-k}{s-k}}. \tag{94}$$

Положим

$$\zeta-k=Mt. \tag{95}$$

Тогда по формуле суммы бесконечно убывающей геометрической прогрессии получим разложение функции (94) в ряд:

$$\frac{1}{\zeta-s}=\frac{1}{k-s}\sum_{\nu=0}^{\infty}\left(\frac{M}{s-k}\right)^{\nu}t^{\nu}=\frac{-1}{M}\sum_{\nu=0}^{\infty}\left(\frac{M}{s-k}\right)^{\nu+1}t^{\nu}=$$

$$=\frac{1}{M}\sum_{\nu=0}^{\infty}b_{\nu}t^{\nu},\quad b_{\nu}=-\left(\frac{M}{s-k}\right)^{\nu+1}. \tag{96}$$

Так как выполняются неравенства $1\leqslant|k-s|\leqslant m-1$, а M — общее наименьшее кратное чисел $1,\dots,m$, то все $M/(k-s)$ — целые рациональные числа и, следовательно, все $b_{\nu}\in\mathbf{Z}$.

Ряд в равенстве (96), очевидно, абсолютно сходится в круге $|t|<1/M$.

Функция

$$\prod_{\substack{s=1\\ s\neq k}}^{m}\frac{1}{(\zeta-s)^{r_s+1}},\quad 1\leqslant k\leqslant m,$$

является произведением $n-r_k$ сомножителей вида $1/(\zeta-s)$, $s\neq k$, среди которых имеются и равные. Поэтому, перемножая соответствующие всем таким функциям $1/(\zeta-s)$ ряды вида (96), ввиду равенства (95) получим

$$\prod_{\substack{s=1\\ s\neq k}}^{m} \frac{1}{(\zeta-s)^{r_s+1}} = \frac{1}{M^{n-r_k}} \sum_{\nu=0}^{\infty} c_\nu t^\nu =$$

$$= \frac{1}{M^{n-r_k}} \sum_{\nu=0}^{\infty} \frac{c_\nu}{M^\nu} (\zeta-k)^\nu, \tag{97}$$

где все c_ν — целые числа. По теореме о перемножении рядов, ряды в равенстве (97) будут сходиться соответственно в кругах $|t|<1/M$ и $|\zeta-k|<1$.

Из равенств (97) и (93) по теореме о вычетах имеем

$$a_{k,l} = \frac{c_{r_k-2l-1}}{M^{n-2l-1}}, \quad 0 \leqslant l \leqslant \frac{r_k-1}{2}, \quad 1 \leqslant k \leqslant m. \tag{98}$$

Из равенств (98) и следует, что все $a_{k,l}$ — рациональные числа, а $M^{n-1} a_{k,l}$ — целые рациональные числа.

Из равенств (91), (92) и (93) находим, что

$$A_n = \sum_{k=1}^{m} \sum_{0 \leqslant l \leqslant \frac{r_k-1}{2}} \frac{(-1)^{l+k} a_{k,l} \pi^{2l+1}}{(2l+1)!}, \tag{99}$$

откуда ввиду равенства (98) следует, что

$$r! M^{n-1} A_n = P_n(\pi), \tag{100}$$

где $P_n(x)$ — многочлен с целыми рациональными коэффициентами, степени, не большей, чем r.

Оценим теперь числа $a_{k,l}$, пользуясь равенством (93). Если $\zeta \in \Gamma_k$, то $|\zeta-k|=1/2$, а при $s \neq k$ $|\zeta-s| \geqslant 1/2$. Поэтому

$$|a_{k,l}| \leqslant \frac{1}{2\pi} \pi \frac{1}{\left(\frac{1}{2}\right)^{n-2l}} \leqslant 2^{n-1},$$

$$0 \leqslant l \leqslant \frac{r_k-1}{2}, \quad 1 \leqslant k \leqslant m. \tag{101}$$

Из равенства (99) и неравенства (101) находим, что коэффициенты многочлена $P_n(x)$ (100) не превосходят числа

$$mr!2^{n-1}M^{n-1} \leqslant r!(2M)^n.$$

Лемма доказана.

Теорема 15. *Число π трансцендентно.*

Доказательство. Допустим противное, что π есть алгебраическое число степени ν, $\nu \geqslant 1$. Положим $m=\nu+1$ и с этим значением m рассмотрим разложение (85) функции $\sin \pi z$ в интерполяционный ряд Ньютона. Тогда, по доказанному выше,

для коэффициентов A_n этого разложения выполняется оценка сверху (87).

С другой стороны, по лемме 8 имеет место равенство (100), где $P_n(x)$ — многочлен с целыми рациональными коэффициентами степени k и высоты H, где

$$k \leqslant r, \quad H \leqslant r!(2M)^n. \tag{102}$$

Пусть c, c_1 и c_2 обозначают положительные постоянные, зависящие только от числа ν.

По теореме 10 ввиду предположения, что π есть алгебраическое число степени ν, выполняется либо равенство $P_n(\pi)=0$, либо неравенство

$$|P_n(\pi)| \geqslant \frac{c^k}{H^{\nu-1}} = e^{k \ln c-(\nu-1)\ln H}. \tag{103}$$

Если $P_n(\pi)\neq 0$, то из неравенств (102) и (103) получаем оценку

$$|P_n(\pi)| \geqslant e^{-|\ln c|r-(\nu-1)(r \ln r+n \ln (2M))}. \tag{104}$$

Но из условий (89) имеем, что

$$r = \max_{1 \leqslant k \leqslant m} r_k \leqslant \frac{n}{m},$$

а $m=\nu+1$. Поэтому из неравенства (104) следует оценка

$$|P_n(\pi)| > e^{-\frac{m-2}{m} n \ln n-c_1 n}. \tag{105}$$

Из равенства (100) и неравенства (87) находим, что

$$|P_n(\pi)| < e^{5n-n \ln n+(n-1)\ln M+r \ln r} < e^{-\frac{m-1}{m} n \ln n+c_2 n}. \tag{106}$$

Неравенства (105) и (106) при достаточно большом n противоречивы. Значит, существует число n_0 такое, что $A_n=0$ при всех $n \geqslant n_0$, а функция $\sin \pi z$ должна быть многочленом. Но она не является многочленом, например, потому, что имеет бесконечное множество нулей. Следовательно, получено противоречие, опровергающее предположение об алгебраичности числа π. Теорема доказана.

Из теоремы 15 следует, что квадратура круга невозможна с помощью циркуля и линейки.

Действительно, площадь круга равна πR^2. Полагая $R=1$, получим, что задача сводится к построению квадрата со стороной, равной $\sqrt{\pi}$. В 1837 г. П. Ванцель (1814—1848) показал, что с помощью циркуля и линейки могут быть построены только те отрезки, длины которых выражаются числами, являющимися корнями квадратных уравнений с рациональными коэффициентами, корнями квадратных уравнений, коэффициенты которых являются корнями квадратных уравнений с рациональными коэффициентами, и т. д., и, следовательно, отрезки, дли-

ны которых выражаются числами, получающимися после последовательного решения ряда квадратных уравнений. Поскольку множество таких чисел есть подмножество множества алгебраических чисел, то из доказательства трансцендентности числа π следует отрицательное решение проблемы квадратуры круга.

Линдеман, доказывая трансцендентность числа π, установил более общее утверждение.

Теорема Линдемана. *Если* α — *алгебраическое число,* $\alpha \neq 0$, *то число* e^{α} *трансцендентно.*

Следствие. *Если* α — *алгебраическое число,* $\alpha \neq 0; 1$, *то число* $\ln \alpha$ *трансцендентно.*

Действительно, $e^{\ln \alpha} = \alpha$, и поэтому предположение о том, что α и $\ln \alpha$ являются одновременно алгебраическими числами, приводит к противоречию с теоремой Линдемана.

Так как выполняется равенство $e^{\pi i} = -1$, то из теоремы Линдемана следует трансцендентность числа π.

Теорема Линдемана может быть доказана методом, которым была доказана трансцендентность числа π. Только для этого необходимо иметь оценку снизу для модуля многочлена с целыми коэффициентами от двух алгебраических чисел.

Линдеман доказал также более общее утверждение.

Теорема Линдемана. *Пусть* $\alpha_1, \ldots, \alpha_n$ — *различные алгебраические числа, а* $c_1, \ldots, c_n$ — *алгебраические числа, не все равные нулю. Тогда*

$$c_1 e^{\alpha_1} + \ldots + c_n e^{\alpha_n} \neq 0.$$

Очевидными следствиями теоремы Линдемана являются утверждения о трансцендентности чисел e и π и теорема Линдемана о трансцендентности чисел e^{α} при $\alpha \in \mathbf{A}$, $\alpha \neq 0$.

В течение свыше сорока лет метод Эрмита — Линдемана был единственным аналитическим методом доказательства трансцендентности чисел. Но в конце 20-х годов текущего столетия в работах А. О. Гельфонда и К. Зигеля (1896—1981) были развиты мощные аналитические методы в теории трансцендентных чисел. За последние 50 лет эти методы в работах ряда математиков получили дальнейшее развитие. С их помощью установлена трансцендентность значений многих аналитических функций.

ЗАМЕЧАНИЯ

С теорией алгебраических чисел читатель может ознакомиться по книгам З. И. Боревича и И. Р. Шафаревича [1] и Э. Гекке [5]. Вопросы, связанные с приближением действительных чисел рациональными числами, изложены в книгах А. Я. Хинчина [14] и А. Б. Шидловского [20].

Теорема Лиувилля о приближении алгебраических чисел

дает оценку снизу для порядка приближения алгебраического числа α рациональными числами. После ее опубликования естественно возникла проблема об улучшении такой оценки. Первый результат в этом направлении был получен А. Туэ (1863—1922) в 1908 г., а в 1909 г. Туэ опубликовал метод, с помощью которого доказал следующую теорему.

Теорема Туэ. *Пусть α — действительное алгебраическое число степени $n \geqslant 2$, а ε — любое положительное число. Тогда неравенство*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\frac{n}{2}+1+\varepsilon}} \tag{107}$$

имеет только конечное число решений в числах $p \in \mathbf{Z}$ и $q \in \mathbf{N}$.

Эту теорему Туэ применил к решению задачи о существовании целочисленных решений у одного класса диофантовых уравнений.

Теорема Туэ о диофантовом уравнении. *Пусть*

$$H(x, y) = a_n x^n + a_{n-1} x^{n-1} y + \ldots + a_1 x y^{n-1} + a_0 y^n,$$

$$n \geqslant 3,\ a_j \in \mathbf{Z},\ a_n \neq 0,$$

— неприводимый многочлен, а m — любое целое число. Тогда уравнение

$$H(x, y) = m$$

либо не имеет решений, либо имеет только конечное множество решений в целых числах x и y.

Теорема Туэ о приближении алгебраических чисел уточнялась К. Зигелем, А. Дайсоном, А. О. Гельфондом, К. Ф. Ротом. Приведем формулировку теоремы Рота (1955 г.).

Теорема Рота. *Пусть α — действительное алгебраическое число степени $n \geqslant 2$, а ε — любое положительное число. Тогда неравенство*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}$$

имеет только конечное число решений в числах $p \in \mathbf{Z}$ и $q \in \mathbf{N}$.

Теорема Рота была также обобщена на случай приближения алгебраического числа алгебраическими числами.

В настоящее время теория приближения алгебраических чисел представляет собой большой и важный раздел теории чисел, имеющий многочисленные приложения. На результатах теории приближения алгебраических чисел основаны некоторые методы доказательства трансцендентности чисел.

С проблемами приближения алгебраических чисел можно ознакомиться по книгам Н. И. Фельдмана [11] и А. Б. Шидловского [20].

После работ Эрмита и Линдемана возникли попытки обобщить их метод и распространить полученные ими результаты на другие функции. Но это не удавалось почти 50 лет. Многие математики внесли упрощения и улучшения в доказательства Эрмита и Линдемана, но существенно новых результатов не получили. Только в 1929 г. были созданы новые методы доказательства трансцендентности чисел.

А. О. Гельфонд в 1929 г. опубликовал аналитический метод, с помощью которого получил в частном случае решение известной 7-й проблемы Гильберта о трансцендентности чисел вида α^β, где α — алгебраическое число, $\alpha \neq 0; 1$, а β — алгебраическое иррациональное число. Результат Гельфонда относился к случаю, когда β — мнимая квадратичная иррациональность. Ввиду равенства $i^{-2i} = e^{\pi}$ было доказано, что число e^{π} трансцендентно.

Доказательство трансцендентности числа π в § 5 проведено методом, основанным на идеях метода Гельфонда 1929 г.

В 1934 г. с помощью нового метода А. О. Гельфонд дал полное решение 7-й проблемы Гильберта.

В том же году независимо Т. Шнейдер (р. 1911) получил другое решение проблемы.

В 1929 г. К. Зигель создал аналитический метод доказательства трансцендентности чисел, являющийся обобщением метода Эрмита—Линдемана. Этим методом он доказал трансцендентность значений в алгебраических точках некоторых аналитических функций, в частности трансцендентность функции Бесселя $J_0(z)$ в любой алгебраической точке $z \neq 0$.

За последние 50 лет методы Гельфонда и Зигеля получили существенное развитие и обобщение и являются в настоящее время основными методами теории трансцендентных чисел. С их помощью доказана трансцендентность значений очень многих аналитических функций.

Аналитические методы теории трансцендентных чисел позволяют получать и количественные характеристики трансцендентности чисел в виде оценок линейных форм и многочленов с целыми коэффициентами от рассматриваемых трансцендентных чисел (см. Дополнение 2).

С проблемами теории трансцендентных чисел можно ознакомиться по книгам Н. И. Фельдмана [12] и А. Б. Шидловского [20], а также по работам А. О. Гельфонда, содержащимся в томе его избранных трудов [4].

ЗАДАЧИ

1) Доказать, что при любом $n \in \mathbf{N}$ многочлен $f(x) = x^n - 2$ неприводим.

2) Установить критерий Эйзенштейна.

Пусть

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,\ f(x) \in \mathbf{Z}[x],$$

и существует простое число p, делящее все коэффициенты a_0, a_1, ..., a_{n-1}, но такое, что $p^2 \nmid a_0$. Тогда $f(x)$ неприводим.

3) С помощью утверждения задачи 2 доказать, что при любом простом p многочлен

$$f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$$

неприводим.

4) Доказать, что множество $\mathbf{A}$ счетно.

5) Доказать, что существует только конечное множество чисел $\xi \in \mathbf{Z}_\mathbf{A}$, ограниченной степени, удовлетворяющих условию $\overline{|\xi|} \leqslant C$, где постоянная $C \geqslant 1$.

6) Пусть $f(x) \in \mathbf{Z}_\mathbf{A}[x]$, а ξ — корень $f(x)$. Доказать, что

$$\frac{f(x)}{x - \xi} \in \mathbf{Z}_\mathbf{A}[x].$$

7) Высотой H_α алгебраического числа α называют наибольший из модулей коэффициентов неприводимого и примитивного многочлена $\varphi(x) \in \mathbf{Z}[x]$, имеющего α своим корнем.

Пусть α и β — алгебраические числа степеней и высот соответственно n_α, n_β и H_α, H_β. Установить оценки сверху для $H_{\alpha+\beta}$ и $H_{\alpha\beta}$ как функций от

$$n_\alpha,\ n_\beta,\ H_\alpha \text{ и } H_\beta.$$

8) Доказать, что множество действительных чисел α, для которых неравенство

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}},\ \varepsilon > 0,$$

имеет бесконечное множество решений в целых числах p и q, $q > 0$, является множеством меры нуль.

9) Доказать, что для любой функции натурального аргумента $\varphi(q) > 0$ существует число α такое, что неравенство

$$\left|\alpha - \frac{p}{q}\right| < \varphi(q)$$

имеет бесконечное множество решений в рациональных числах p/q, $q > 0$.

10) Доказать, что при любых целых p и q, $q \geqslant 2$, выполняется неравенство

$$\left|\sqrt{2} - \frac{p}{q}\right| > \frac{1}{4q^2}.$$

11) Пусть $P(x, y) \in \mathbf{Z}[x, y]$, α и β — целые алгебраические числа степеней соответственно n и m такие, что $P(\alpha, \beta) \neq 0$, $\alpha_1, \ldots, \alpha_n$ — числа, сопряженные с α, а $\beta_1, \ldots, \beta_m$ — числа, сопряженные с β. Доказать, что произведение всех тех из чисел

$$P(\alpha_i, \beta_j),\ i = 1, \ldots, n;\ j = 1, \ldots, m,$$

которые отличны от нуля, есть целое рациональное число.

12) Пусть α и β — алгебраические числа степеней соответственно n и m. Доказать, что существует постоянная $C>0$, зависящая только от α, такая, что при любом $P(x, y)\in\mathbf{Z}[x, y]$ степени $k\geqslant 1$ по переменным x и y и высоты $H\geqslant 1$, либо $P(\alpha, \beta)=0$, либо

$$|P(\alpha, \beta)|>\frac{C^k}{H^{mn-1}}.$$

13) Обобщить теорему Лиувилля на случай приближения алгебраического числа α алгебраическими числами θ в следующей форме.

Пусть α — фиксированное алгебраическое число степени n, $n\geqslant 1$. Существует постоянная $C>0$, зависящая только от α, такая, что при любом алгебраическом θ, $\theta\neq\alpha$, степени k, $k\geqslant 1$, и высоты H, $H\geqslant 1$, выполняется неравенство

$$|\alpha-\theta|\geqslant\frac{C^k}{H^n}.$$

14) Доказать, что число $\log_2\pi$ иррационально.

15) Доказать, что для числа $\alpha=\sum\limits_{n=0}^{\infty}2^{-3^n}$ неравенство

$$\left|\alpha-\frac{p}{q}\right|<\frac{C}{q^3}$$

имеет бесконечное число решений в натуральных числах p и q при любой постоянной $C>1$ и конечное число решений при $C=1$.

16) Доказать иррациональность значений функции Бесселя

$$J_0(x)=\sum_{n=0}^{\infty}\frac{(-1)^n}{(n!)^2}\left(\frac{x}{2}\right)^{2n},$$

в точках $x=1/k$, где $k\in\mathbf{N}$.

17) Пользуясь методом, которым была доказана иррациональность числа π, доказать, что число π^2 иррационально.

19) Пользуясь утверждением задачи 12 и методом, изложенным в § 5, доказать теорему Линдемана: Если $\alpha\in\mathbf{A}$, $\alpha\neq 0$, то число e^α трансцендентно.

20) С помощью теоремы Линдемана доказать трансцендентность следующих чисел:

а) $\sin\alpha$, $\cos\alpha$, $\operatorname{tg}\alpha$, при любом $\alpha\in\mathbf{A}$, $\alpha\neq 0$,

б) $\arcsin\alpha$, $\arccos\alpha$, $\operatorname{arctg}\alpha$, при любом $\alpha\in\mathbf{A}$, $\alpha\neq 0$,

в) решений уравнения $e^{2x+1}=x^2+x+1$.

ДОПОЛНЕНИЕ 1

ОБ ОСТАТОЧНОМ ЧЛЕНЕ В АСИМПТОТИЧЕСКОМ ЗАКОНЕ РАСПРЕДЕЛЕНИЯ ПРОСТЫХ ЧИСЕЛ

В дополнении ставится задача показать, как влияет информация о расположении нулей дзета-функции на оценку остаточного члена в асимптотическом законе, т. е. разности $\pi(x)-\operatorname{li} x$, а также ознакомить читателя с основными идеями получения таких оценок.

Для простоты изложения ограничимся условной оценкой остаточного члена. Она будет основываться на недоказанном к настоящему времени предположении о том, что функция $\zeta(s)$ не имеет нулей в полосе $\theta<\operatorname{Re} s\leqslant 1$, где θ — некоторое число из полуинтервала $1/2\leqslant\theta<1$. Это предположение при $\theta=1/2$ совпадает с гипотезой Римана.

Однако способ доказательства тесно связан с методами, при помощи которых получены полностью обоснованные оценки остаточного члена в асимптотическом законе (см. замечания к гл. 2).

Сформулируем основной результат.

Теорема. *Допустим, что функция $\zeta(s)$ не имеет нулей в области $\operatorname{Re} s>\theta$, где θ — число из полуинтервала $1/2\leqslant\theta<1$. Тогда при любом $\varepsilon>0$*

$$\psi(x)=x+O(x^{\theta+\varepsilon}); \tag{1}$$

$$\pi(x)=\operatorname{li} x+O(x^{\theta+\varepsilon}). \tag{2}$$

Следствие. *Если справедлива гипотеза Римана, то при любом $\varepsilon>0$*

$$\psi(x)=x+O(x^{\frac{1}{2}+\varepsilon}),\quad \pi(x)=\operatorname{li} x+O(x^{\frac{1}{2}+\varepsilon}).$$

Сначала докажем несколько вспомогательных утверждений.

Лемма 1. *Существует постоянная c_1 такая, что в области*

$$\operatorname{Re} s=\sigma\geqslant\frac{1}{2},\quad |t|\geqslant 1,\quad s=\sigma+it, \tag{3}$$

справедливо неравенство

$$|\zeta(s)|\leqslant c_1\sqrt{|t|}. \tag{4}$$

Доказательство. Если $\sigma>2$, то $|\zeta(s)|<\zeta(2)$. Если же $\sigma\leqslant 2$, то, рассуждая так же, как при доказательстве леммы 5

гл. 2, получим, что в области (3) все три слагаемые в правой части равенства (12) гл. 2

$$\sum_{n=1}^{N}\frac{1}{n^s},\quad \frac{N^{1-s}}{s-1},\quad -s\int_N^{\infty}\frac{\{x\}}{x^{s+1}}dx$$

при $N=[|t|]$ являются величинами порядка $O(\sqrt{|t|})$. Отсюда следует оценка (4).

Лемма 2. *Пусть $f(s)$ — аналитическая функция в круге $|s-s_0|\leqslant R$, удовлетворяющая условиям:*

1) $f(s_0)=0$; (5)

2) $\operatorname{Re} f(s)\leqslant C$ *при* $|s-s_0|\leqslant R$,

где C — положительная постоянная.

Тогда для каждого r такого, что $0<r<R$, справедливо неравенство

$$|f(s)|\leqslant\frac{2Cr}{R-r}\ \text{при}\ |s-s_0|\leqslant r.$$

Доказательство. Рассмотрим функцию

$$g(s)=\frac{f(s)}{(s-s_0)(2C-f(s))}. \tag{6}$$

Обозначим

$$u=u(s)=\operatorname{Re} f(s),\quad v=v(s)=\operatorname{Im} f(s).$$

Тогда из неравенства (5) и того, что $C>0$, следует, что в круге $|s-s_0|\leqslant R$ выполняется неравенство

$$|2C-u(s)|=2C-u(s)\geqslant\max(u(s),-u(s))=|u(s)|.$$

Поэтому ввиду равенства (6) на окружности $|s-s_0|=R$

$$|g(s)|=\frac{(u^2+v^2)^{1/2}}{R((2C-u)^2+v^2)^{1/2}}\leqslant\frac{(u^2+v^2)^{1/2}}{R(u^2+v^2)^{1/2}}=\frac{1}{R}.$$

Из условий $f(s_0)=0$ и $u(s)\leqslant C$, $C>0$, легко следует, что $g(s)$ — аналитическая функция в круге $|s-s_0|\leqslant R$. Поэтому по принципу максимума модуля

$$|g(s)|\leqslant\frac{1}{R}\ \text{при}\ |s-s_0|\leqslant R.$$

Ввиду обозначения (6) отсюда следует, что в круге $|s-s_0|\leqslant r$

$$|f(s)|=\left|\frac{2C(s-s_0)g(s)}{1+(s-s_0)g(s)}\right|\leqslant\frac{2Cr\frac{1}{R}}{1-r\frac{1}{R}}=\frac{2Cr}{R-r}.$$

Лемма доказана.

Лемма 3. *Если функция $\zeta(s)$ не обращается в нуль при $\sigma>\theta$, где θ — число из полуинтервала $1/2\leqslant\theta<1$, то при любом $\varepsilon>0$ в области*

$$\sigma\geqslant\theta+\varepsilon, \quad |t|\geqslant 3$$

справедлива оценка

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right|<c_2\ln(|t|+2),\ c_2=c_2(\theta,\varepsilon)>0. \tag{7}$$

Следствие. *Если выполнены условия леммы 3 и $\theta+\varepsilon<1$, то на прямой $\sigma=\theta+\varepsilon$ выполняется неравенство*

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right|<c_3\ln(|t|+2),\ c_3=c_3(\theta,\varepsilon)>0. \tag{8}$$

Действительно, по теореме 1 гл. 2 и по условиям леммы на отрезке с концами $\theta+\varepsilon\pm 3i$ функция $\zeta'(s)/\zeta(s)$ непрерывна и, следовательно, ограничена. Поэтому из неравенства (7) следует, что с некоторой постоянной c_3 справедливо неравенство (8) на всей прямой $\sigma=\theta+\varepsilon$.

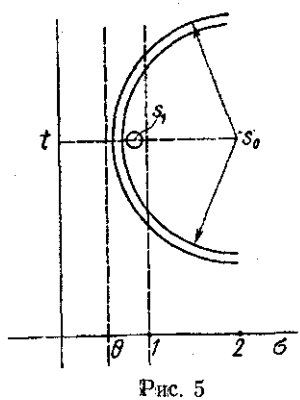

Рис. 5

Доказательство леммы 3. Ввиду тождества (4) гл. 2 в области $\sigma>2$ функция $\zeta'(s)/\zeta(s)$ ограничена. Поэтому утверждение леммы достаточно доказать при $\sigma\leqslant 2$.

Пусть $s_1=\sigma+it$ принадлежит области

$$\theta+\varepsilon\leqslant\sigma\leqslant 2,\ |t|\geqslant 3.$$

Обозначим $s_0=2+it$ и рассмотрим два круга (рис. 5) с центрами в точке s_0 и радиусами

$$R=2-\theta-\frac{\varepsilon}{4},\ r=2-\theta-\frac{\varepsilon}{2},\ R>r,\ 0<\varepsilon<1. \tag{9}$$

Функция $\dfrac{\zeta(s)}{\zeta(s_0)}$ по условию леммы не обращается в нуль в круге $|s-s_0|\leqslant R$. Следовательно, в этом круге можно выбрать однозначную ветвь логарифма

$$f(s)=\ln\frac{\zeta(s)}{\zeta(s_0)},$$

такую, что $f(s_0)=0$*).

Из неравенства (26) гл. 2 с $\sigma=2$ следует, что

$$\frac{1}{|\zeta(s_0)|}\leqslant(\zeta(2))^{3/4}|\zeta(2+2it)|^{1/4}\leqslant\zeta(2).$$

*) Это следует из теоремы о монодромии, доказательство которой можно прочитать, например, в книге А. И. Маркушевича «Теория аналитических функций. Т. 2», М.: Наука, 1968, с. 488.

Так как $R<2$, а $\theta\geqslant 1/2$, то по лемме 1 в круге $|s-s_0|\leqslant R$ выполняется неравенство

$$\operatorname{Re} f(s)=\ln\left|\frac{\zeta(s)}{\zeta(s_0)}\right|\leqslant \ln\left(c_1(|t|+2)^{1/2}\right)+\ln\zeta(2)<c_4\ln(|t|+2).$$

Поэтому ввиду условий (9) по лемме 2 при $|s-s_0|\leqslant r$

$$f(s)|=\left|\ln\frac{\zeta(s)}{\zeta(s_0)}\right|\leqslant \frac{2c_4\ln(|t|+2)\left(2-\theta-\frac{\varepsilon}{2}\right)}{\frac{\varepsilon}{4}}=c_5\ln(|t|+2). \tag{10}$$

Из определения чисел s_1 и r следует, что круг $|s-s_1|\leqslant\varepsilon/2$ целиком содержится как в области $\sigma>\theta$, так и в круге $|s-s_0|\leqslant r$ (см. рис. 5). Поэтому функция $f(s)$ является аналитической в круге $|s-s_1|\leqslant\varepsilon/2$, и ее производная в точке s_1 равна

$$f'(s_1)=\frac{1}{2\pi i}\int\limits_{|s-s_1|=\frac{\varepsilon}{2}}\frac{f(s)}{(s-s_1)^2}\,ds.$$

Отсюда и из оценки (10) следует, что

$$\left|\frac{\zeta'(s_1)}{\zeta(s_1)}\right|=|f'(s_1)|\leqslant\frac{1}{2\pi}\,2\pi\,\frac{\varepsilon}{2}\,\frac{c_5\ln(|t|+2)}{\left(\frac{\varepsilon}{2}\right)^2}=c_6\ln(|t|+2).$$

Лемма доказана.

Лемма 4. *При $a>0$, $b>0$, $u>0$ выполняется равенство*

$$\frac{1}{2\pi i}\int\limits_{a-iu}^{a+iu}\frac{b^s}{s}\,ds=\begin{cases}1+O\left(\dfrac{b^a}{u\ln b}\right), & \text{если } b>1\\[2ex] O\left(\dfrac{b^a}{u|\ln b|}\right), & \text{если } 0<b<1.\end{cases} \tag{11}$$

Доказательство. Интегрируя по частям *) функцию b^s/s, получаем

$$\frac{1}{2\pi i}\int\limits_{a-iu}^{a+iu}\frac{b^s}{s}\,ds=\frac{1}{2\pi i}\int\limits_{a-iu}^{a+iu}\frac{db^s}{s\ln b}=$$

$$=\frac{1}{2\pi i\ln b}\frac{b^s}{s}\Big|_{a-iu}^{a+iu}+\frac{1}{2\pi i\ln b}\int\limits_{a-iu}^{a+iu}\frac{b^s}{s^2}\,ds. \tag{12}$$

*) Возможность интегрирования по частям в комплексном интеграле легко обосновывается с помощью понятия комплексного интеграла с переменным верхним пределом.

При доказательстве леммы 9 гл. 2 фактически было установлено, что при $u>0$

$$\frac{1}{2\pi i}\int\limits_{a-iu}^{a+iu}\frac{b^s}{s^2}\,ds=\lambda+O\left(\frac{b^a}{u}\right),$$

где $\lambda=\ln b$ при $b\geqslant 1$ и $\lambda=0$ при $0<b<1$. Поэтому из равенства (12) следует утверждение леммы.

Лемма 5. *Для функции Чебышева* $\psi(x)$ *выполняется соотношение*

$$\psi(x)=\frac{1}{2\pi i}\int\limits_{3-ix^3}^{3+ix^3}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\frac{x^s}{s}\,ds+O(1), \tag{13}$$

где $x=N+\frac{1}{2}$, *а* N *— натуральное число.*

Доказательство. Так как на отрезке с концами $3-ix^3$ и $3+ix^3$ выполняется неравенство

$$\left|\frac{\Lambda(n)}{s}\left(\frac{x}{n}\right)^s\right|\leqslant\frac{x^3\ln n}{3n^3},$$

то ряд в правой части равенства (4) гл. 2 сходится на этом отрезке равномерно по s. Интегрируя почленно этот ряд, по лемме 4 получаем

$$I=\frac{1}{2\pi i}\int\limits_{3-ix^3}^{3+ix^3}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\frac{x^s}{s}\,ds=$$

$$=\sum_{n=1}^{\infty}\Lambda(n)\,\frac{1}{2\pi i}\int\limits_{3-ix^3}^{3+ix^3}\frac{1}{s}\left(\frac{x}{n}\right)^s ds=$$

$$=\psi(x)+O\left(\sum_{n=1}^{\infty}\frac{\left(\frac{x}{n}\right)^3\ln n}{x^3\left|\ln\frac{x}{n}\right|}\right). \tag{14}$$

По условию леммы $x=N+1/2$, где N — натуральное число. Поэтому

$$\left|\ln\frac{x}{n}\right|\geqslant\min\left(\left|\ln\frac{n-\frac{1}{2}}{n}\right|,\ \ln\frac{n+\frac{1}{2}}{n}\right)=\ln\left(1+\frac{1}{2n}\right)=$$

$$=\sum_{k=1}^{\infty}(-1)^{k-1}\frac{1}{k\,(2n)^k}>\frac{1}{2n}-\frac{1}{2\,(2n)^2}>\frac{1}{3n}.$$

Подставляя эту оценку в равенства (14), находим

$$I = \psi(x) + O\left(\sum_{n=1}^{\infty} \frac{3 \ln n}{n^3}\right) = \psi(x) + O(1).$$

Отсюда следует утверждение леммы.

Доказательство теоремы. Пусть ε — произвольное число, удовлетворяющее неравенству $0<\varepsilon<1-\theta$. Рассмотрим контур $\Gamma(x, \varepsilon)$, являющийся периметром прямоугольника $ABCD$ с вершинами в точках $\theta+\frac{\varepsilon}{2}-ix^3$, $3-ix^3$, $3+ix^3$, $\theta+\frac{\varepsilon}{2}+ix^3$ (рис. 6). Из условия теоремы следует, что функция $\zeta(s)$ при любом $x>0$ не обращается в нуль в этом прямоугольнике. Поэтому в нем функция

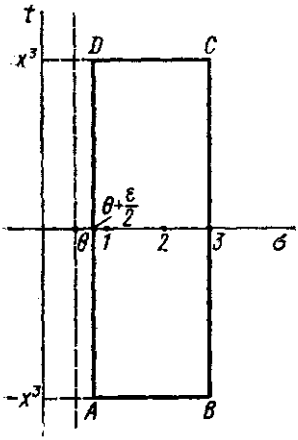

Рис. 6

$$f(s) = -\frac{\zeta'(s)}{\zeta(s)} \frac{x^s}{s} \tag{15}$$

имеет единственную особую точку — полюс первого порядка при $s=1$ с вычетом x (см. теорему 1 гл. 2). По теореме Коши о вычетах

$$\frac{1}{2\pi i} \int_{\Gamma(x,\varepsilon)} f(s)\, ds = x,$$

а тогда

$$I = \frac{1}{2\pi i} \int_{3-ix^3}^{3+ix^3} f(s)\, ds = x + \frac{1}{2\pi i} \int_L f(s)\, ds, \tag{16}$$

где L — ломаная $BADC$ (см. рис. 6).

Оценим интеграл по отрезкам ломаной L.

При $x^3 \geqslant 3$, пользуясь равенством (15) и леммой 3, получаем, что

$$\frac{1}{2\pi i} \int_{BA} f(s)\, ds = O\left(\frac{3}{2\pi} \ln (x^3+2) \frac{x^3}{x^3}\right) = O(\ln x). \tag{17}$$

Аналогичная оценка справедлива для интеграла по отрезку DC.

По следствию из леммы 3 ввиду равенства (15) находим

$$\frac{1}{2\pi i}\int\limits_{AD} f(s)\,ds = O\left(x^{\theta+\frac{\varepsilon}{2}}\ln(x^3+2)\int\limits_{-x^3}^{x^3}\frac{dt}{\left|\theta+\frac{\varepsilon}{2}+it\right|}\right) =$$

$$= O\left(x^{\theta+\frac{\varepsilon}{2}}\ln^2 x\right) = O\left(x^{\theta+\varepsilon}\right). \tag{18}$$

Из равенств (16), (17) и (18) получаем, что

$$I = \frac{1}{2\pi i}\int\limits_{3-ix^3}^{3+ix^3} f(s)\,ds = x + O\left(x^{\theta+\varepsilon}\right). \tag{19}$$

Пусть $x=N+1/2$, где N — натуральное число. Тогда из оценки (19) и леммы 5 получаем, что

$$\psi(x) = I + O(1) = x + O\left(x^{\theta+\varepsilon}\right),$$

т. е. в этом случае доказано асимптотическое равенство (1).

Для произвольного $x\geqslant 2$ аналогичное равенство тоже верно, поскольку

$$\psi(x) = \psi([x]) = \psi\left([x]+\frac{1}{2}\right).$$

Тем самым первое утверждение теоремы доказано.

Будем выводить асимптотическую формулу (2) из равенства (1). Рассмотрим функцию

$$\Pi(x) = \sum_{2\leqslant n\leqslant x}\frac{\Lambda(n)}{\ln n}. \tag{20}$$

Из определения функции $\Lambda(n)$ следует, что

$$\Pi(x) = \sum_{k=1}^{\infty}\sum_{n=p^k\leqslant x}\frac{\ln p}{\ln n} = \sum_{k=1}^{\infty}\sum_{p^k\leqslant x}\frac{1}{k} =$$

$$= \sum_{k=1}^{\infty}\frac{1}{k}\pi\left(\sqrt[k]{x}\right) = \pi(x) + O\left(\sqrt{x}\ln x\right), \tag{21}$$

поскольку $\pi\left(\sqrt[k]{x}\right) = 0$ при $k > \log_2 x$.

Применим к функции (20) лемму 4 гл. 2, полагая в этой лемме $a_n=\Lambda(n)$, $g(x)=1/\ln x$, $A(x)=\psi(x)$. Тогда равенство (10) гл. 2 примет вид

$$\Pi(x) = \frac{\psi(x)}{\ln x} + \int\limits_2^x \frac{\psi(t)\,dt}{t\ln^2 t}.$$

Подставляя в последнее равенство значение $\psi(x)$ из асимптотической формулы (1), получаем, что

$$\Pi(x) = \frac{x + O(x^{\theta+\varepsilon})}{\ln x} + \int_2^x \frac{t + O(t^{\theta+\varepsilon})}{t \ln^2 t}\, dt =$$

$$= \frac{x}{\ln x} + \int_2^x \frac{dt}{\ln^2 t} + O(x^{\theta+\varepsilon}) +$$

$$+ O\left(\int_2^x t^{\theta-1+\varepsilon}\, dt\right) = \operatorname{li} x + O(x^{\theta+\varepsilon}), \qquad (22)$$

так как

$$\operatorname{li} x = \int_2^x \frac{dt}{\ln t} = \frac{x}{\ln x} - \frac{2}{\ln 2} + \int_2^x \frac{dt}{\ln^2 t}.$$

Из равенств (21) и (22) следует асимптотическая формула (2). Теорема полностью доказана.

В заключение заметим, что

$$\int_2^x \frac{dt}{\ln^2 t} = \int_2^{\sqrt{x}} \frac{dt}{\ln^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\ln^2 t} <$$

$$< \frac{\sqrt{x}}{\ln^2 2} + \frac{x - \sqrt{x}}{\ln^2 \sqrt{x}} = O\left(\frac{x}{\ln^2 x}\right),$$

т. е. $\operatorname{li} x \sim \dfrac{x}{\ln x}$ при $x \to +\infty$.

ЗАДАЧИ

1) Доказать, что для функции (35) гл. 2 $\omega(x)$ справедлива асимптотическая формула

$$\omega(x) = x + O(xe^{-c(\ln x)^{0,1}}), \quad x \to \infty.$$

Указание. Использовать задачу 8 гл. 2. Контур интегрирования такого же вида, как на рис. 3 гл. 2.

2) Из предыдущей задачи получить, что при $x \to \infty$

$$\psi(x) = x + O(xe^{-\frac{c}{2}(\ln x)^{0,1}}),$$

$$\pi(x) = \operatorname{li} x + O(xe^{-\frac{c}{3}(\ln x)^{0,1}}).$$

3) С помощью задачи 2 доказать, что при достаточно больших x

$$|\pi(x) - \operatorname{li} x| < \left|\pi(x) - \frac{x}{\ln x}\right|.$$

ДОПОЛНЕНИЕ 2

ОЦЕНКИ МНОГОЧЛЕНОВ С ЦЕЛЫМИ КОЭФФИЦИЕНТАМИ ОТ ЧИСЛА *e*

Методы теории трансцендентных чисел позволяют не только доказывать трансцендентность различных чисел, но и получать количественные характеристики их трансцендентности. Так, теорема, доказанная в § 4, гл. 4, утверждает, что никакой отличный от нуля многочлен с целыми коэффициентами не обращается в нуль в точке e. Метод доказательства этой теоремы позволяет установить и более сильный результат, а именно найти оценку снизу для модуля многочлена с целыми коэффициентами в точке e в зависимости от величины его коэффициентов. В этом дополнении будет доказана следующая теорема.

Теорема. *Пусть H и ε — положительные числа, m — натуральное число. Для любого многочлена $P(x) \in \mathbf{Z}[x]$, $P(x) \not\equiv 0$, коэффициенты которого по абсолютной величине не превосходят H, а степень не превосходит m, выполняется неравенство*

$$|P(e)| > cH^{-m-\varepsilon},$$

где $c>0$ — некоторая постоянная, зависящая только от чисел m и ε.

Подобная теорема с худшей оценкой впервые была установлена в 1899 г. Э. Борелем (1871—1956).

Доказательство. Достаточно доказать утверждение теоремы в предположении, что многочлен $P(x)$ имеет взаимно простые коэффициенты, а число ε удовлетворяет неравенству $0<\varepsilon<1$.

Пусть многочлен $P(x)$ имеет вид

$$P(x) = a_m x^m + \ldots + a_1 x + a_0,$$

$$a_i \in \mathbf{Z},\ i=0, 1, \ldots, m,\ (a_0, a_1, \ldots, a_m) = 1.$$

В основе доказательства теоремы лежит некоторое видоизменение рассуждений, использовавшихся в § 4 гл. 4 для доказательства трансцендентности числа e.

Пусть n — натуральное число, удовлетворяющее, как и в § 4 гл. 4 условию

$$(n,\ m!) = 1. \tag{1}$$

В дальнейшем число n будет выбрано существенно меньшим, чем при доказательстве трансцендентности числа e. Поэтому необходимо изменить выбор многочлена $f(x)$.

Так как коэффициенты многочлена $P(x)$ взаимно просты, то среди них есть коэффициент a_r, не делящийся на n. Выберем многочлен $f(x)$ в виде

$$f(x) = \frac{1}{(n-1)!} \frac{(x(x-1)\cdots(x-m))^n}{x-r}.$$

Заметим, что при $r=0$ этот многочлен совпадает с многочленом, использовавшимся для доказательства трансцендентности числа e.

Определим, как и в § 4 гл. 4, многочлен $F(x)$ равенством

$$F(x)=f(x)+f'(x)+f''(x)+\ldots,$$

где сумма в правой части содержит конечное число слагаемых. Как и в § 4 гл. 4, с помощью тождества Эрмита вместо равенства (57) гл. 4 получаем равенство

$$F(0)\,P(e)-\sum_{k=0}^{m}a_kF(k)=\sum_{k=0}^{m}a_ke^k\int_0^k f(x)\,e^{-x}\,dx, \qquad (2)$$

где $F(k)$ — целые числа, делящиеся на n при $k\neq r$.

Так как

$$f^{(n-1)}(r)=(-1)^{(m-r)n}\,(r!\,(m-r)!\,)^n,$$

то

$$F(r)=\sum_{l=n-1}^{(m+1)n-1}f^{(l)}(r)=(-1)^{(m-r)n}\,(r!\,(m-r)!\,)^n+nD,\ D\in\mathbf{Z}.$$

Из условия (1) и определения числа r следует, что произведение $a_rF(r)$ не делится на n. Значит, целое число

$$\sum_{k=0}^{m}a_kF(k)$$

отлично от нуля, и

$$\Big|\sum_{k=0}^{m}a_kF(k)\Big|\geqslant 1.$$

Оценим сверху правую часть равенства (2). На отрезке $0\leqslant x\leqslant m$ для многочлена $f(x)$, как и в § 4, гл. 4, справедливо неравенство

$$|f(x)|\leqslant\frac{m^{(m+1)n-1}}{(n-1)!},\quad 0\leqslant x\leqslant m.$$

Пользуясь неравенствами

$$|a_k|\leqslant H,\ k=0,\ 1,\ \ldots,\ m,$$

находим

$$\Big|\sum_{k=0}^{m}a_ke^k\int_0^k f(x)\,e^{-x}\,dx\Big|\leqslant\frac{m^{(m+1)n-1}}{(n-1)!}\sum_{k=0}^{m}|a_k|\,e^k\int_0^k e^{-x}dx\leqslant$$

$$\leqslant H\,\frac{m^{(m+1)n}}{(n-1)!}\,e^m\leqslant He^{e_1n}n^{-n},$$

где постоянная c_1 зависит только от m. С ростом n правая часть последнего неравенства стремится к нулю.

Выберем теперь n так, чтобы выполнялись условие (1) и неравенство

$$Hn^{-n}e^{c_1 n} < \frac{1}{2}. \tag{3}$$

Из равенства (2) получаем

$$|F(0)P(e)| \geqslant \left|\sum_{k=0}^{m} a_k F(k)\right| - \left|\sum_{k=0}^{m} a_k e^k \int_0^k f(x)e^{-x}dx\right| \geqslant 1 - \frac{1}{2} = \frac{1}{2},$$

и

$$|P(e)| \geqslant \frac{1}{2}|F(0)|^{-1}. \tag{4}$$

Оценим сверху величину $|F(0)|$. Переходя в тождестве Эрмита

$$\int_0^x f(t)e^{-t}dt = F(0) - F(x)e^{-x}$$

к пределу при $x \to +\infty$ и пользуясь тем, что $F(x)$ — многочлен, находим, что

$$F(0) = \int_0^{+\infty} f(t)e^{-t}dt.$$

Поэтому

$$|F(0)| \leqslant \int_0^m |f(t)|e^{-t}dt + \int_m^{+\infty} |f(t)|e^{-t}dt <$$

$$< \frac{m^{(m+1)n}}{(n-1)!}\int_0^m e^{-t}dt + \frac{1}{(n-1)!}\int_m^{+\infty} t^{(m+1)n}e^{-t}dt <$$

$$< \frac{m^{(m+1)n}}{(n-1)!} + \frac{((m+1)n)!}{(n-1)!}. \tag{5}$$

Последняя оценка получена с помощью известного равенства

$$\int_0^{+\infty} x^k e^{-x}dx = k!, \quad k \in \mathbf{Z}, \quad k \geqslant 0.$$

Из неравенств (5) легко следует, что

$$|F(0)| \leqslant n^{mn}e^{c_2 n},$$

где постоянная c_2 зависит только от m.

Из неравенства (4) теперь находим

$$|P(e)| \geqslant \frac{1}{2} n^{-mn} e^{-c_3 n}. \tag{6}$$

Правая часть последнего неравенства с ростом n убывает. Поэтому оценка снизу для $|P(e)|$ будет тем лучше, чем меньшее удастся найти значение n, удовлетворяющее условию (1) и неравенству (3).

Положим

$$\delta = \frac{\varepsilon}{6m}.$$

Если H достаточно велико по сравнению с m и ε^{-1}, то на интервале

$$(1 + 4\delta) \frac{\ln H}{\ln \ln H} < n < (1 + 5\delta) \frac{\ln H}{\ln \ln H} \tag{7}$$

найдется $m!$ последовательных целых чисел. Выберем в качестве n, например, то из них, которое при делении на $m!$ дает в остатке 1. При таком выборе условие (1) будет выполнено.

Из неравенств (7) следует, что при достаточно большом H выполняются неравенства

$$(1-\delta) \ln \ln H < \ln n < \ln \ln H. \tag{8}$$

Так как

$$(1+4\delta)(1-\delta) = 1+3\delta-4\delta^2 > 1+2\delta,$$

то из неравенств (7) и (8) получаем, что

$$(1+2\delta) \ln H < n \ln n < (1+5\delta) \ln H. \tag{9}$$

Поскольку

$$(1+2\delta)(1-\delta) = 1+\delta-2\delta^2 \geqslant 1,$$

то из левой части неравенства (9) после умножения на $(1-\delta)$ находим

$$\ln H < (1-\delta) n \ln n, \quad H < n^{(1-\delta)n},$$

или

$$H n^{-(1-\delta)n} < 1.$$

Тогда при достаточно большом H имеем

$$H n^{-n} e^{c_3 n} = H n^{-(1-\delta)n} n^{-\delta n} e^{c_3 n} \leqslant n^{-\delta n} e^{c_3 n} < \frac{1}{2}.$$

Последнее неравенство выполняется ввиду того, что при достаточно большом H значение n тоже будет велико. Таким образом, неравенство (3) справедливо, и, значит, выполняется неравенство (6).

Пользуясь правой частью неравенства (9), находим при достаточно большом H

$$2 n^{mn} e^{c_2 n} \leqslant 2 H^{m(1+5\delta)} e^{c_2 n} \leqslant H^{m(1+6\delta)} = H^{m+\varepsilon}.$$

Теперь из неравенства (6) получаем, что

$$|P(e)| \geqslant H^{-m-\varepsilon},$$

если H больше некоторой границы, зависящей только от m и ε. Отсюда следует утверждение теоремы.

Полученная оценка достаточно точна.

Чтобы убедиться в этом, докажем с помощью принципа Дирихле следующую лемму.

Лемма. *Пусть* $\omega_0, \omega_1, \ldots, \omega_m$ — *действительные числа и* H — *натуральное число. Существуют целые числа* $a_0, a_1, \ldots, a_m$, *не все равные нулю, такие, что*

$$|a_i| \leqslant H, \quad i=0, 1, \ldots m,$$

и

$$|a_0\omega_0 + a_1\omega_1 + \ldots + a_m\omega_m| \leqslant c_0 H^{-m},$$

где

$$c_0 = 2\sum_{k=0}^{m} |\omega_k|.$$

Доказательство. Пусть переменные $x_0, \ldots, x_m$ независимо друг от друга принимают целые значения из множества

$$0, 1, \ldots, H.$$

Всего таким образом получим $(H+1)^{m+1}$ различных наборов $(x_0, x_1, \ldots, x_m)$. Каждому набору поставим в соответствие число

$$x_0\omega_0 + x_1\omega_1 + \ldots + x_m\omega_m.$$

Из неравенств

$$-\frac{c_0}{2} H \leqslant x_0\omega_1 + x_1\omega_1 + \ldots + x_m\omega_m \leqslant \frac{c_0}{2} H$$

следует, что все $(H+1)^{m+1}$ полученных таким образом чисел лежат на отрезке длиной $c_0 H$.

Разделим отрезок $-\frac{c_0}{2} H \leqslant x \leqslant \frac{c_0}{2} H$ на $(H+1)^{m+1}-1$ равных отрезков. Тогда найдутся две точки, соответствующие некоторым наборам $(x_0', x_1', \ldots, x_m')$, $(x_0'', x_1'', \ldots, x_m'')$, лежащие на одном из полученных отрезков. Это означает, что

$$\left|\sum_{i=1}^{m} (x_i' - x_i'')\,\omega_i\right| \leqslant \frac{c_0 H}{(H+1)^{m+1}-1} < c_0 H^{-m}. \tag{10}$$

Положим

$$a_i = x_i' - x_i'', \quad i=0, 1, \ldots, m.$$

Так как числа x_i' и x_i'' лежат на отрезке $0 \leqslant x \leqslant H$, то

$$|a_i| = |x_i' - x_i''| \leqslant H.$$

Из неравенств (10) теперь следует, что числа $a_0, a_1, \ldots, a_m$ удовлетворяют всем требованиям леммы.

Применив доказанную лемму в случае

$$\omega_k = e^k, \quad k = 0, 1, \ldots, m,$$

получим, что для любых натуральных m и H существует многочлен $P(x) \in \mathbf{Z}[x]$, $P(x) \not\equiv 0$, степень которого не выше m, а коэффициенты по абсолютной величине не превосходят H, удовлетворяющий неравенству

$$|P(e)| \leqslant c_0 H^{-m},$$

где $c_0 = 2(1 + e + \ldots + e^m)$.

ЛИТЕРАТУРА

1. Боревич З. И., Шафаревич И. Р. Теория чисел. М.: Наука, 1972.
2. Виноградов И. М. Основы теории чисел. М.: Наука, 1972.
3. Виноградов И. М. Избранные труды. М.: Изд-во АН СССР, 1952.
4. Гельфонд А. О. Избранные труды. М.: Наука, 1973.
5. Гекке Э. Лекции по теории алгебраических чисел. М.: ГИТТЛ, 1940.
6. Давенпорт Г. Мультипликативная теория чисел. М.: Наука, 1971.
7. Ингам А. Е. Распределение простых чисел. М.: ОНТИ, 1936.
8. Карацуба А. А. Основы аналитической теории чисел. М.: Наука, 1975.
9. Прахар К. Распределение простых чисел. М.: Мир, 1967.
10. Трост Э. Простые числа. М.: ГИФМЛ, 1959.
11. Фельдман Н. И. Приближения алгебраических чисел. М.: Изд-во Моск. ун-та, 1981.
12. Фельдман Н. И. Седьмая проблема Гильберта. М.: Изд-во Моск. ун-та, 1982.
13. Хассе Г. Лекции по теории чисел. М.: ИЛ, 1953.
14. Хинчин А. Я. Цепные дроби. М.: Наука, 1978.
15. Хуа-Ло-ген. Метод тригонометрических сумм и его приложения в теории чисел. М.: Мир, 1964.
16. Чандрасекхаран К. Введение в аналитическую теорию чисел. М.: Мир, 1974.
17. Чандрасекхаран К. Арифметические функции. М.: Наука, 1975.
18. Чудаков Н. Г. Введение в теорию L-функций Дирихле. М.: Гостехиздат, 1947.
19. Чебышев П. Л. Собрание сочинений, т. 1. М.—Л.: Изд-во АН СССР, 1946.
20. Шидловский А. Б. Диофантовы приближения и трансцендентные числа. М.: Изд-во Моск. ун-та, 1982.