Р.Вон

МЕТОД ХАРДИ — ЛИТТЛВУДА

М.: Мир, 1985. —184 с.

Книга известного английского математика, излагающая один из основных методов теории чисел — метод Харди — Литтлвуда. На примерах решения ряда конкретных проблем автор демонстрирует возможности этого метода, приводит изящные и краткие доказательства известных теорем. Приведены задачи разной степени трудности, поставлены новые проблемы.

Для математиков разных специальностей, аспирантов и студентов, специализирующихся по теории чисел.

Оглавление

Именной указатель

Предметный указатель

Предисловие редактора перевода

Книга Р. Вона посвящена изложению основ кругового метода Харди — Литтлвуда. В нашей литературе этот метод называют круговым методом Харди — Литтлвуда — Рамануджана (Х. — Л. — Р.) по причинам, изложенным в § 1.2. Круговой метод имеет своим истоком метод производящих функций Эйлера, которым Эйлер решал линейные аддитивные задачи. Рассмотрим уравнение вида

$$a_1x_1 + \ldots + a_nx_n = N, \quad a_1, \ldots, a_n > 0,$$

в целых неотрицательных числах $x_1, \ldots, x_n$. Если $J(N)$ — число решений этого уравнения, то производящая функция $\varphi(t)$ определяется так:

$$\varphi(t) = \sum_{N=0}^{\infty} J(N)\, t^N =$$

$$= \left(\sum_{x_1=0}^{\infty} t^{a_1x_1}\right) \cdots \left(\sum_{x_n=0}^{\infty} t^{a_nx_n}\right) = \frac{1}{1-t^{a_1}} \cdots \frac{1}{1-t^{a_n}}, \quad |t| < 1.$$

Следовательно,

$$N!\, J(N) = \left.\frac{d^N\varphi(t)}{dt^N}\right|_{t=0}.$$

Можно вычислить $J(N)$ по интегральной формуле Коши

$$J(N) = \frac{1}{2\pi i} \int\limits_{|t|=R<1} \varphi(t)\, t^{-N-1} dt. \qquad (*)$$

Изложенная идея Эйлера и последняя формула послужили истоком кругового метода. Кроме того, формула (*) дала название методу — «круговой». Круговым методом решаются нелинейные аддитивные задачи, такие, как проблема Варинга, проблема Гольдбаха и многие другие. Слово «решаются» означает следующее. Для числа решений $J(N)$ некоторого нелинейного уравнения выписывается точная формула в виде интеграла типа (*). Этот интеграл I разбивается на два слагаемых I_1 и I_2 по определенному правилу, предложенному Харди — Литтлвудом — Рамануджаном.

Первое слагаемое I_1 исследуется методом Х. — Л. — Р. и оно дает предполагаемый главный член асимптотической формулы для I при $N \to +\infty$. Если после этого удается доказать, что второе слагаемое I_2 есть величина меньшего порядка, чем I_1, то для I получается асимптотическая формула. Таким образом, круговой метод Х. — Л. — Р. — это метод выделения из I предполагаемого главного члена. Для полного решения задачи остается оценить предполагаемый остаток, т. е. I_2. В 1924 г. И. М. Виноградов заменил в круговом методе бесконечные ряды конечными тригонометрическими суммами. Это не только значительно упростило метод, но и открыло путь к решению новых задач аддитивной теории чисел. Создание И. М. Виноградовым в 1934 г. нового метода оценок тригонометрических сумм позволило для широкого круга задач, которые стали называться «тернарными аддитивными проблемами», оценить остаточный член I_2. Таким образом, общая схема решения тернарных аддитивных проблем круговым методом выглядит так: число решений $J(N)$ некоторого уравнения записывается в виде интеграла I от тригонометрической суммы; интеграл I разбивается на два слагаемых по правилу, предложенному Х. — Л. — Р.; интеграл I_1 исследуется методом Х. — Л. — Р. в форме тригонометрических сумм И. М. Виноградова; интеграл I_2 оценивается с помощью метода оценок тригонометрических сумм И. М. Виноградова. По такой схеме решаются основные задачи, изложенные в книге Р. Вона. Автору книги принадлежит замечательное тождество, которое позволило упростить решение И. М. Виноградова проблемы Гольдбаха (см. теорему 3.1). Отмечу также, что некоторые из теорем книги, в частности теорема о среднем И. М. Виноградова (гл. 5), асимптотическая формула для $J_s(X)$ (гл. 7) и др., в нашей литературе изложены и точнее, и лучше (см. [1]—[4]). В книге имеется ряд приложений кругового метода к задачам, которые в нашей литературе не были достаточно отражены (см. гл. 9—11). В моих примечаниях, помещенных в конце глав и обозначенных цифрой в квадратных скобках, даны дополнительные ссылки на литературу и некоторые комментарии.

В заключение мы благодарим автора, который проявил большой интерес к русскому изданию и прислал список исправлений и замечаний.

А. А. Карацуба

[1] Виноградов И. М. Метод тригонометрических сумм в теори чисел.— М.: Наука, 1980.
[2] Виноградов И. М. Особые варианты метода тригонометрических сумм. — М.: Наука, 1976.
[3] Архипов Г. И., Карацуба А. А., Чубариков В. Н. Кратные тригонометрические суммы. Труды МИАН, т. 151. — М.: Наука, 1980.
[4] Карацуба А. А, Основы аналитической теории чисел.— М.: Наука, 1983.

Предисловие

Метод Харди — Литтлвуда рассматривался ранее в двух работах Ландау (1937) и Эстермана (1952), изданных в Кембридже. Однако, несмотря на немалый вклад английских ученых в открытие и разработку данного метода, в Великобритании не был опубликован его полный обзор, тогда как за рубежом появилось много монографий.

Цель настоящей монографии состоит в том, чтобы наряду с описанием классических форм этого метода привести некоторые из недавних его усовершенствований. Сделать ударение на это представляется особенно важным, поскольку многие из более поздних приложений широко используют классический материал.

Было бы полезно уделить внимание работе Дэвенпорта о кубических формах, совместной работе Дэвенпорта и Льюиса о системах уравнений, работе Радемахера и Зигеля, в которой этот метод распространяется на алгебраические числа, а также работам различных других авторов, завершившимся недавней статьей Шмидта о границах решений однородных уравнений и неравенств. Однако это сделало бы книгу слишком громоздкой. Читатель, интересующийся этими вопросами, может обратиться к библиографии.

Предполагается, что читатель знаком с элементами теории чисел в объеме книги Харди и Райта. Кроме того, для понимания некоторых тем данной книги желательно, чтобы читатель был в курсе современного состояния дел в теории чисел. Там, где необходимо, дается ссылка на стандартный текст по соответствующей теме.

В основу содержания глав 2, 3, 4, 5, 9, 10 и 11 легли расширенные курсы, предлагаемые в «Империал Колледж» в течение ряда лет, и их можно использовать для работы аспирантов в аналитической теории чисел.

Р. Вон

Обозначения

Буквой k обозначается натуральное число, обычно $k \geqslant 2$; формулировки, в которых появляется ε, верны для каждого положительного действительного числа ε. Буквой p обозначаются простые числа.

Символы Виноградова $\ll$, $\gg$ имеют свой обычный смысл, именно для функций f и g, где g принимает неотрицательные действительные значения, $f \ll g$ означает $|f| \leqslant Cg$, где C — постоянная, а если, кроме того, f также неотрицательна, то $f \gg g$ означает $g \ll f$.

Неявные постоянные, включаемые в O, $\ll$ и $\gg$, обычно зависят от k, s и ε. Дополнительная зависимость будет упомянута особо.

Как обычно в теории чисел, функции $e(\alpha)$ и $\|\alpha\|$ означают $e^{2\pi i\alpha}$ и $\min\limits_{h \in \mathbf{Z}} |\alpha - h|$ соответственно. Иногда встречается выражение $\min(X, 1/0)$, и в этом случае надо брать X.

Соотношение $p^r \| n$ используется для обозначения того, что p^r — наивысшая степень p, делящая n.

1
Введение и исторические сведения

1.1 Проблема Варинга

В 1770 г. Варинг в своих «Алгебраических размышлениях» выдвинул гипотезу о том, что каждое четное натуральное число является суммой не более девяти кубов целых положительных чисел, суммой не более 19 биквадратов и т. д. Считается, что тем самым он предполагал следующее: для любого целого положительного числа $k \geqslant 2$ существует число s, такое, что каждое натуральное число является суммой не более s k-х степеней натуральных чисел, и наименьшее такое s, скажем $g(k)$, удовлетворяет соотношениям $g(3) = 9$, $g(4) = 19$.

Вероятно, уже Диофанту было известо, хотя и в другой форме, что каждое натуральное число есть сумма не более четырех квадратов. Впервые точно теорему о четырех квадратах сформулировал в 1621 г. Баше, а Ферма объявил, что доказал ее, однако умер, не раскрыв своего доказательства. Доказательство теоремы не было известно до 1770 г., когда Лагранжу удалось получить его на основе более ранней работы Эйлера. Теорема о четырех квадратах рассматривается в гл. 20 книги [Hardy, Wright, 1979][1]).

В XIX в. существование $g(k)$ было установлено для многих отдельных значений k, но реального прогресса на пути к решению проблемы удалось достичь только в нынешнем столетии. Гильберт [Hilbert, 1909a, b] сложным комбинаторным методом при помощи алгебраических тождеств (см. [Rieger, 1953a, b, c; Ellison, 1971]) первым доказал существование $g(k)$ для всех k. Метод Гильберта дает очень грубую оценку величины $g(k)$.

В начале 1920-х гг. Харди и Литтлвуд предложили аналитический метод, который послужил основой работ Диксона, Пиллаи и др. и привел к полному решению задачи о $g(k)$. Так как целое число

$$n = 2^k \left[\left(\tfrac{3}{2}\right)^k\right] - 1$$

меньше 3^k, то оно может быть суммой k-х степеней только 1 и 2. Ясно, что наиболее экономным является представление

[1]) См. также Венков [1], гл. V — *Прим. перев.*

посредством $\left[\left(\frac{3}{2}\right)^k\right]-1$ k-х степеней 2 и 2^k-1 k-х степеней 1. Отсюда

$$g(k) \geqslant 2^k+\left[\left(\tfrac{3}{2}\right)^k\right]-2. \tag{1.1}$$

Весьма вероятно, что это неравенство фактически является равенством. Сейчас в этом отношении известно следующее.

Предположим, что $k \neq 4$. Было показано, что если

$$2^k\left\{\left(\tfrac{3}{2}\right)^k\right\}+\left[\left(\tfrac{3}{2}\right)^k\right] \leqslant 2^k, \tag{1.2}$$

то

$$g(k)=2^k+\left[\left(\tfrac{3}{2}\right)^k\right]-2. \tag{1.3}$$

Если же

$$2^k\left\{\left(\tfrac{3}{2}\right)^k\right\}+\left[\left(\tfrac{3}{2}\right)^k\right] > 2^k,$$

то либо $\quad g(k)=2^k+\left[\left(\tfrac{3}{2}\right)^k\right]+\left[\left(\tfrac{4}{3}\right)^k\right]-2,$

либо $\quad g(k)=2^k+\left[\left(\tfrac{3}{2}\right)\right]^k]+\left[\left(\tfrac{4}{3}\right)^k\right]-3$

в зависимости от того, равно 2^k или больше 2^k число m

$$m=\left[\left(\tfrac{4}{3}\right)^k\right]\cdot\left[\left(\tfrac{3}{2}\right)^k\right]+\left[\left(\tfrac{4}{3}\right)^k\right]+\left[\left(\tfrac{3}{2}\right)^k\right].$$

Информацию о различных вкладах в доказательство этих утверждений можно найти в библиографии.

Стеммлер [Stemmler, 1964] с помощью ЭВМ проверил справедливость (1.2) (а значит, и (1.3)) для всех $k \leqslant 200\,000$, а Малер [Mahler, 1957] показал, что если существуют k, для которых неравенство (1.2) не имеет места, то количество таких k конечно. Исключения неизвестны, но, к сожалению, неизвестна и граница, за которой этих исключений нет.

Томас [Thomas, 1974] показал, что $g(4) \leqslant 22$ (значит, согласно (1.1), $g(4)=19$, 20, 21 или 22), а Баласубраманиян недавно анонсировал, что $g(4) \leqslant 21$. Томас доказал также, что n является суммой не более 19 биквадратов для $n<10^{310}$ и $n>10^{1049}$.

1.2 Метод Харди — Литтлвуда

Почти все указанные выше результаты получены на основе аналитического метода Харди и Литтлвуда, который позволяет найти число C_k, такое, что каждое натуральное число, большее C_k, есть сумма не более s_k k-х степеней натуральных чисел, причем s_k не превышает ожидаемой величины $g(k)$. Затем в некоторой степени громоздкие, но подчас очень остроумные вычисления дают возможность проверить справедливость этого утверждения для всех чисел, не превосходящих C_k.

Одна из особенностей метода Харди — Литтлвуда заключается в том, что он может применяться для рассмотрения многих других аддитивных проблем. Начало этому методу было положено работой Харди и Рамануджана (1918), касающейся главным образом функции разбиения чисел на слагаемые, но затрагивающей также представление чисел в виде сумм квадратов.

Пусть $\mathscr{A} = (a_m)$ — строго возрастающая последовательность неотрицательных целых чисел. Рассмотрим функцию

$$F(z) = \sum_{m=1}^{\infty} z^{a_m} \quad (|z| < 1)$$

и ее s-ю степень

$$F(z)^s = \sum_{m_1=1}^{\infty} \dots \sum_{m_s=1}^{\infty} z^{a_{m_1} + \dots + a_{m_s}} = \sum_{n=0}^{\infty} R_s(n) z^n,$$

где $R_s(n)$ — число представлений n в виде суммы s членов $\mathscr{A}$. Задача состоит в том, чтобы оценить $R_s(n)$ по крайней мере для больших значений n.

По интегральной формуле Коши

$$R_s(n) = \frac{1}{2\pi i} \int_{\mathscr{C}} F(z)^s z^{-n-1} dz,$$

где $\mathscr{C}$ — окружность с центром в 0 радиуса ρ, $0 < \rho < 1$.

Харди и Рамануджан разработали метод оценки этого интеграла в случае $a_m = m^2$. Пусть $\rho = 1 - 1/n$, где n велико, и пусть $e(\alpha) = e^{2\pi i \alpha}$. Тогда функция F имеет «пики» в точках $z = \rho e(\alpha)$, «близких» к $e(a/q)$, если q «не слишком большое». На самом деле в окрестности таких точек F имеет асимптотическое представление, грубо говоря, справедливое при $|\alpha - a/q| \leqslant 1/q\sqrt{n}$ и $q \leqslant \sqrt{n}$. По теореме Дирихле о диофантовом приближении, каждое $z \in \mathscr{C}$ находится в такого рода окрестности.

Упомянутое выше асимптотическое представление имеет вид

$$F\left(\rho e\left(\frac{a}{q} + \beta\right)\right) \sim \frac{C}{q} S(q, a)(1 - \rho e(\beta))^{-1/2}, \tag{1.4}$$

где
$$S(q, a) = \sum_{m=1}^{q} e(am^2/q).$$

Его можно получить путем распределения квадратов по классам вычетов модуля q в случае $\beta = 0$ с последующим применением частичного суммирования. Таким образом, можно показать, что для $s \geqslant 5$

$$R_s(n) \sim \mathfrak{S}_s(a) J_s(n), \tag{1.5}$$

где

$$\mathfrak{S}_s(n) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a, q)=1}}^{\infty} q^{-s} S(q, a)^s e(-an/q)$$

и

$$J_s(n) = C^s \int_{-1/2}^{1/2} (1 - \rho e(\beta))^{-s/2} \rho^{-n} e(-\beta n)\, d\beta.$$

Интеграл $J_s(n)$ нетрудно оценить, а ряд $\mathfrak{S}_s(n)$ отражает некоторые интересные теоретико-числовые свойства последовательности квадратов целых чисел.

Разложение (1.4) отвечает особенностям ряда для функции F в рациональных точках a/q круга его сходимости. В связи с этим Харди и Литтлвуд ввели термины *особый ряд* и *особый интеграл* для $\mathfrak{S}_s(n)$ и $J_s(n)$ соответственно.

После первой мировой войны Харди и Литтлвуд (1920, 1921) обратились к проблеме Варинга. К сожалению, в случае $a_m = m^k$ с $k \geqslant 3$ они смогли показать только, что разложение, соответствующее (1.4), справедливо при

$$q \leqslant n^{1/k-\varepsilon} \quad \text{и} \quad \left|\alpha - \frac{a}{q}\right| \leqslant q^{-1} n^{1/k-\varepsilon-1},$$

а это составляет лишь малую часть точек z на $\mathscr{C}$. Поскольку $q^{-1}S(q, a) \to 0$ при $q \to \infty$ (для $(a, q) = 1$), возникла гипотеза, что в остальных точках z функция F во всяком случае мала по сравнению с тривиальной оценкой $(1-\rho)^{-1/k} = n^{1/k}$. Эта гипотеза подкреплялась фактом равномерного распределения по модулю 1 чисел αm^k для иррациональных α. Действительно, на основе метода, берущего начало в фундаментальной работе Вейля [H. Weyl, 1916] о равномерном распределении последовательностей, Харди и Литтлвуд сумели доказать, что на остатке $\mathscr{C}$ функция F существенно меньше, чем $n^{1/k}$. Полученное утверждение о величине F часто называют неравенством Вейля. Для описания частей $\mathscr{C}$, на которых используются соответственно аналог соотношения (1.4) и неравенство Вейля, Харди и Литтлвуд ввели термины *большие дуги* и *малые дуги*.

И. М. Виноградов (1928a) внес в рассматриваемый метод ряд значительных усовершенствований [1] одним из которых явилась замена $F(z)$ конечной суммой

$$f(\alpha) = \sum_{m=1}^{N} e(\alpha m^k), \tag{1.6}$$

где

$$N = [n^{1/k}]. \tag{1.7}$$

Теперь

$$f(\alpha)^s = \sum_{m=1}^{sn} R_s(m, n)\, e(\alpha m).$$

где $R_s(m, n)$ — число представлений m суммой s k-х степеней, каждая из которых не превосходит n. Таким образом,

$$R_s(m, n) = R_s(m) \qquad (m \leqslant n).$$

Далее, специальный случай интегральной формулы Коши, именно тривиальное соотношение ортогональности

$$\int_0^1 e(\alpha h)\, d\alpha = \begin{cases} 1, & \text{если } h = 0, \\ 0, & \text{если } h \neq 0, \end{cases} \tag{1.8}$$

дает

$$\int_0^1 f(\alpha)^s e(-\alpha n)\, d\alpha = R_s(n). \tag{1.9}$$

Из предыдущих рассмотрений ясно, что величина $g(k)$ определяется согласно особым требованиям нескольких исключительных относительно малых натуральных чисел. Таким образом, более интересной проблемой является оценка числа $G(k)$, определяемого при $k \geqslant 2$ как наименьшее s, такое, что каждое достаточно большое натуральное число есть сумма не более s k-х степеней натуральных чисел. При этом оказывается, что для больших k $G(k)$ намного меньше, чем $g(k)$, что, естественно, делает его оценку намного более трудной. Фактически величина $G(k)$ известна только для $k = 2$ и $k = 4$, именно

$$G(2) = 4, \quad G(4) = 16.$$

Последним результатом мы обязаны Дэвенпорту [Davenport, 1939c]. Ю. В. Линник (1943a) показал, что $G(3) \leqslant 7$. Позднее Ватсон [Watson, 1951] дал в высшей степени элегантное доказательство этого неравенства. Для $k > 3$ все лучшие известные в настоящее время оценки $G(k)$ получены по методу Харди и Литтлвуда. Изучению $G(k)$ посвящены главы 2, 4, 5, 6, 7.

1.3 Проблемы Гольдбаха

В двух письмах к Эйлеру в 1742 г. Гольдбах высказал предположение, что каждое четное число является суммой двух простых чисел и каждое число, большее 2, есть сумма трех простых. Он включал 1 в простые числа. Современная формулировка гипотез Гольдбаха выглядит так: каждое четное число, большее 2, есть сумма двух простых, а каждое нечетное число, большее 5, является суммой трех простых.

Харди и Литтлвуд (1923a, b) обнаружили, что при условии справедливости расширенной гипотезы Римана их метод может быть с успехом применен к этим проблемам. При этом условии они смогли показать, что каждое достаточно большое нечетное число представляется в виде суммы трех простых чисел и что почти все четные числа — суммы двух простых.

В 1937 г. И. М. Виноградов сумел устранить зависимость от расширенной гипотезы Римана, дав тем самым безусловное доказательство утверждений Харди и Литтлвуда. Это направление исследований проблем Гольдбаха изучается в гл. 3. Однако природа простых чисел, и в частности проблема их распределения в арифметических прогрессиях, показывает, что дальнейшие уточнения метода (см. [Montgomery, Vaughan, 1975]) лучше прослеживаются в контексте мультипликативной теории чисел и поэтому опущены в этой книге.

Многие обобщения методов, изложенных в гл. 3, содержатся в монографии Хуа Ло-кена [Hua, 1965].

1.4 Другие проблемы

Последние тридцать лет наблюдается большое распространение и разнообразие применений метода Харди и Литтлвуда, и ряд тем в гл. 8, 9, 10, 11 выбран для иллюстрации его развития. Описанные здесь применения метода, особенно к общим формам и неравенствам в гл. 9 и 11 соответственно, охватывают лишь небольшую часть работ в этих областях и должны рассматриваться как введение к оригинальным статьям, включенным в библиографию.

1.5 Упражнения

1. Покажите, что число $\rho(n)$ решений уравнения

$$x_1 + \ldots + x_s = n$$

в неотрицательных целых $x_1, \ldots, x_s$ равно $(-1)^n \binom{-s}{n}$.

2. Покажите, что сумма делителей n, $\sigma(n) = \sum_{m|n} m$ выражается в виде

$$\sigma(n) = \frac{\pi^2}{6} n \sum_{q=1}^{\infty} q^{-2} c_q(n),$$

где $c_q(n)$ — сумма Рамануджана, т. е.

$$c_q(n) = \sum_{\substack{a=1 \\ (a,\, q)=1}}^{q} e\,(an/q).$$

3. Пусть P, Q — действительные числа, $P > 1$, $Q \geqslant 2P$. Покажите, что интервалы

$$\left\{\alpha : \left|\alpha - \frac{a}{q}\right| \leqslant q^{-1}Q^{-1}\right\}$$

при $q \leqslant P$ и $(a, q) = 1$ попарно не пересекаются.

Примечание редактора

[1] Э. Ландау (1927) в своей знаменитой книге «Vorlesungen über Zahlentheorie, Band I» посвятил этому главу под названием «Метод Виноградова»; см. также Успехи математических наук, вып. 36 : 6, 1981, с. 3—20.

2
Простейшая верхняя оценка $G(k)$

2.1 Определение больших и малых дуг

В последующие годы в метод Харди — Литтлвуда вносились различные улучшения, наиболее значительные из которых даны Хуа [Hua, 1938*b*]. Это позволило получить простое доказательство того, что $G(k) \leqslant 2^k + 1$, тем не менее иллюстрирующее замечательные свойства этого метода.

В определении больших и малых дуг много свободы, ч выбор, сделанный здесь, достаточно произволен.

Пусть n велико, N определяется формулой (1.7),

$$\nu = \frac{1}{100}, \quad P = N^{\nu}, \tag{2.1}$$

и пусть δ — достаточно малое положительное число, зависящее только от k. Для $1 \leqslant a \leqslant q \leqslant P$, $(a, q) = 1$, положим

$$\mathfrak{M}(q, a) = \{\alpha\colon\ |\alpha - a/q| \leqslant N^{\nu-k} \tag{2.2}$$

$\mathfrak{M}(q, a)$ по указанным выше историческим причинам называются *большими дугами*, хотя фактически это интервалы. Пусть $\mathfrak{M}$ означает объединение $\mathfrak{M}(q, a)$. Вместо $(0,1]$ удобнее рассматривать единичный интервал

$$\mathcal{U} = (N^{\nu-k},\ 1 + N^{\nu-k}]. \tag{2.3}$$

Это избавляет от некоторых затруднений, связанных с тем, что в промежуток $(0, 1]$ попадают не все большие дуги, тогда как $\mathfrak{M} \subset \mathcal{U}$. Множество $\mathfrak{m} = \mathcal{U}/\mathfrak{M}$ составляют *малые дуги*.

При $a/q \neq a'/q'$ и $q, q' \leqslant N^{\nu}$ имеем

$$|a/q - a'/q'| \geqslant 1/qq' > \left(\frac{1}{q} + \frac{1}{q'}\right) N^{\nu-k}.$$

Следовательно, дуги $\mathfrak{M}(q, a)$ попарно не пересекаются.

Согласно соотношению (1.9) (для краткости индекс s опущен),

$$R(n) = \int\limits_{\mathfrak{M}} f(\alpha)^s e(-\alpha n)\, d\alpha + \int\limits_{\mathfrak{m}} f(\alpha)^s e(-n\alpha)\, d\alpha, \tag{2.4}$$

где $f(\alpha)$ определяется равенством (1.6). Прежде чем перейти к оценке этих интегралов, докажем некоторые вспомогательные леммы,

2.2 Вспомогательные леммы

Метод оценки $f(\alpha)$ для $\alpha \in \mathfrak{m}$ можно описать следующим образом. При $k=1$

$$f(\alpha)=\sum_{m=1}^{N} e(\alpha m^k)$$

оценивается тривиально. В общем случае рассуждения основываются на использовании разностного оператора, позволяющего оценить $f(\alpha)$ в терминах сумм, в которых m^k заменяется полиномом степени $k-1$. Последовательное применение этих рассуждений понижает степень до 1.

Лемма 2.1 (Дирихле). *Пусть α — действительное число. Тогда для любого действительного $X \geqslant 1$ существует рациональное число a/q, такое, что $(a, q)=1$, $1 \leqslant q \leqslant X$ и*

$$|\alpha - a/q| \leqslant 1/(qX).$$

Доказательство. Достаточно получить этот результат без условия $(a, q)=1$.

Пусть $m=[X]$. Все m чисел $\beta_q=\alpha q-[\alpha q]$ $(q=1, 2, \ldots, m)$ лежат в интервале $(0, 1]$. Рассмотрим $m+1$ интервалов

$$B_r=\left[\frac{r-1}{m+1}, \frac{r}{m+1}\right) \quad (r=1,\ 2,\ \ldots,\ m+1).$$

Если в B_1 или B_{m+1} есть число β_q, то доказательство окончено. Если нет, то один из $m-1$ интервалов B_r с $2 \leqslant r \leqslant m$ содержит по крайней мере два β_q, скажем β_u, β_v, $u<v$. Полагаем $q=v-u$, $a=[\alpha v]-[\alpha u]$.

Лемма 2.2. *Пусть X, Y, α — действительные числа, $X \geqslant 1$, $Y \geqslant 1$ и $|\alpha - a/q| \leqslant q^{-2}$, $(a, q)=1$. Тогда*

$$\sum_{x \leqslant X} \min(XYx^{-1}, \|\alpha x\|^{-1}) \ll XY\left(\frac{1}{q}+\frac{1}{Y}+\frac{q}{XY}\right)\log(2Xq),$$

где $\|\beta\|=\min_{y \in \mathbb{Z}} |\beta - y|$.

Доказательство. Пусть

$$S=\sum_{x \leqslant X} \min(XYx^{-1}, \|\alpha x\|^{-1}).$$

Очевидно,

$$S \leqslant \sum_{0 \leqslant j \leqslant X/q} \sum_{r=1}^{q} \min\left(\frac{XY}{qj+r}, \|\alpha(qj+r)\|^{-1}\right).$$

Для каждого j пусть $y_j=[\alpha j q^2]$, и положим $\theta=q^2\alpha-qa$. Тогда

$$\alpha(qj+r)=(y_j+ar)/q+\{\alpha j q^2\}/q+\theta r q^{-2}.$$

При $j=0$ и $r\leqslant \frac{1}{2}q$

$$\|\alpha(qj+r)\|\geqslant\|ar/q\|-1/(2q)\geqslant\tfrac{1}{2}\|ar/q\|.$$

В противном случае для каждого j имеется не более $O(1)$ чисел r, для которых неравенство

$$\|\alpha(qj+r)\|\geqslant\tfrac{1}{2}\|(y_j+ar)/q\|$$

не имеет места и, кроме того, $qj+r\gg q(j+1)$. Поэтому

$$S\ll\sum_{1\leqslant r\leqslant q/2}\|ar/q\|^{-1}+\sum_{0\leqslant j\leqslant X/q}\left(\frac{XY}{q(j+1)}+\sum_{\substack{r=1\\ q\nmid y_j+ar}}^{q}\|(y_j+ar)/q\|^{-1}\right)\ll$$

$$\ll XYq^{-1}\sum_{0\leqslant j\leqslant X}\frac{1}{j+1}+(Xq^{-1}+1)\sum_{1\leqslant h\leqslant q/2}\frac{q}{h},$$

откуда легко следует лемма.

Пусть Δ_j означает j-е применение разностного оператора, так что для любой функции φ действительной переменной α

$$\Delta_1(\varphi(\alpha);\ \beta)=\varphi(\alpha+\beta)-\varphi(\alpha),$$

$$\Delta_{j+1}(\varphi(\alpha);\ \beta_1,\ \ldots,\ \beta_{j+1})=\Delta_1(\Delta_j(\varphi(\alpha);\ \beta_1,\ \ldots,\ \beta_j);\ \beta_{j+1}).$$

Тогда нетрудно убедиться, что

$$\Delta_j(\alpha^k;\ \beta_1,\ \ldots,\ \beta_j)=\beta_1\ldots\beta_j p_j(\alpha;\ \beta_1,\ \ldots,\ \beta_j),$$

где p_j — многочлен от α степени $k-j$ со старшим коэффициентом $k!/(k-j)!$.

Следующая лемма является промежуточным звеном в доказательствах обеих нижеследующих лемм 2.4 и 2.5.

Лемма 2.3 (Вейль). *Пусть*

$$T(\varphi)=\sum_{x=1}^{Q}e(\varphi(x)),$$

где φ — произвольная арифметическая функция. Тогда

$$|T(\varphi)|^{2^j}\leqslant(2Q)^{2^j-j-1}\sum_{|h_1|<Q}\ldots\sum_{|h_j|<Q}T_j,$$

где

$$T_j=\sum_{x\in I_j}e(\Delta_j(\varphi(x);\ h_1,\ \ldots,\ h_j)),$$

и интервалы $I_j = I_j(h_1, \ldots, h_j)$ *(возможно, пустые) удовлетворяют соотношениям:*

$$I_1(h_1) \subset [1,\ Q],\quad I_j(h_1, \ldots, h_j) \subset I_{j-1}(h_1, \ldots, h_{j-1}).$$

Доказательство. Индукция по j. Для краткости вместо $\Delta_j(\varphi(x);\ h_1, \ldots, h_j)$ пишем $\Delta_j(x)$. Очевидно,

$$|T(\varphi)|^2 = \sum_{x=1}^{Q} \sum_{h_1=1-x}^{Q-x} e(\Delta_1(x)) = \sum_{h_1=1-Q}^{Q-1} \sum_{x \in I_1} e(\Delta_1(x)),$$

где $I_1 = [1, Q] \cap [1 - h_1, Q - h_1]$.

Теперь если лемма верна для какого-либо значения j, то, согласно неравенству Коши,

$$|T(\varphi)|^{2^{j+1}} \leqslant (2Q)^{2^{j+1}-2j-2}(2Q)^j \sum_{h_1, \ldots, h_j} |T_j|^2$$

и, очевидно,

$$|T_j|^2 = \sum_{|h|<Q} \sum_{x \in I_{j+1}} e(\Delta_j(x+h) - \Delta_j(x)),$$

где
$$I_{j+1} = I_j \cap \{x:\ x + h \in I_j\}.$$

Лемма 2.4 (Неравенство Вейля). *Предположим, что* $(a, q) = 1$, $|\alpha - a/q| \leqslant q^{-2}$, $\varphi(x) = \alpha x^k + \alpha_1 x^{k-1} + \ldots + \alpha_{k-1}x + \alpha_k$ *и*

$$T(\varphi) = \sum_{x=1}^{Q} e(\varphi(x)).$$

Тогда
$$T(\varphi) \ll Q^{1+\varepsilon}(q^{-1} + Q^{-1} + qQ^{-k})^{1/K},$$

где $K = 2^{k-1}$.

Доказательство. По лемме 2.3 при $j = k - 1$ (и упражнению 2.1),

$$|T(\varphi)|^K \leqslant (2Q)^{K-k} \times$$
$$\times \sum_{h_1} \underset{|h_j| \leqslant Q}{\ldots} \sum_{h_{k-1}} \sum_{x \in I_{k-1}} e(h_1 \ldots h_{k-1} p_{k-1}(x;\ h_1, \ldots, h_{k-1})),$$

где $p_{k-1}(x;\ h_1, \ldots h_{k-1}) = k!\ \alpha\left(x + \frac{1}{2}h_1 + \ldots + \frac{1}{2}h_{k-1}\right) + (k-1)!\ \alpha_1.$

Члены с $h_1 \ldots h_{k-1} = 0$ дают вклад $\ll Q^{k-1}$. Поэтому

$$|T(\varphi)|^K \ll (2Q)^{K-k}\left(Q^{k-1} + Q^{\varepsilon} \sum_{h=1}^{k!\,Q^{k-1}} \min(Q,\ \|\alpha h\|^{-1})\right) \ll$$
$$\ll Q^{K-k+\varepsilon}\left(Q^{k-1} + \sum_{h=1}^{k!\,Q^{k-1}} \min(Q^k h^{-1},\ \|\alpha h\|^{-1})\right).$$

Согласно лемме 2.2, для $q \leqslant Q^k$ это есть

$$\ll Q^{K+2\varepsilon}(q^{-1}+Q^{-1}+qQ^{-k}).$$

Заметим, что результат тривиален при $q > Q^k$, что и завершает доказательство.

Лемма 2.5 (Лемма Хуа, 1938*b*). *Пусть* $1 \leqslant j \leqslant k$. *Тогда*

$$\int_0^1 |f(\alpha)|^{2^j}\,d\alpha \ll N^{2^j-j+\varepsilon}. \tag{2.5}$$

Доказательство. Индукция по j. Случай $j=1$ непосредственно следует из тождества Парсеваля.

Предположим теперь, что (2.5) справедливо и что $1 \leqslant \leqslant j \leqslant k-1$. По лемме 2.3 с $\varphi(x) = \alpha x^k$,

$$|f(\alpha)|^{2^j} \leqslant$$
$$\leqslant (2N)^{2^j-j-1} \sum_{h_1} \ldots \sum_{|h_j| \leqslant N} \sum_{h_j} \sum_{x \in I_j} e(\alpha h_1 \ldots h_j p_j(x;\ h_1,\ \ldots,\ h_j)),$$

где $p_j(x;\ h_1,\ \ldots,\ h_j)$ — многочлен от x степени $k-j$ с целыми коэффициентами. Следовательно,

$$|f(\alpha)|^{2^j} \ll (2N)^{2^j-j-1} \sum_h c_h e(\alpha h), \tag{2.6}$$

где c_h — число решений уравнения

$$h_1 \ldots h_j p_j(x;\ h_1,\ \ldots,\ h_j) = h$$

с $|h_i| < N$ и $x \in I_j$. Очевидно, $c_0 \ll N^j$, $c_h \ll N^\varepsilon$ $(h \neq 0)$.

Из представления

$$|f(\alpha)|^{2^j} = f(\alpha)^{2^{j-1}} f(-\alpha)^{2^{j-1}}$$

следует также, что

$$|f(\alpha)|^{2^j} = \sum_h b_h e(-\alpha h), \tag{2.7}$$

где b_h есть число решений уравнения

$$x_1^k + \ldots + x_{2^{j-1}}^k - y_1^k - \ldots - y_{2^{j-1}}^k = h$$

с $x_i,\ y_i \leqslant N$. Таким образом,

$$\sum_h b_h = f(0)^{2^j} = N^{2^j}$$

и по предположению индукции

$$b_0 = \int_0^1 |f(\alpha)|^{2^j}\,d\alpha \ll N^{2^j-j+\varepsilon}.$$

Согласно (2.6), тождеству Парсеваля и (2.7),

$$\int_0^1 |f(\alpha)|^{2^{j+1}} d\alpha \ll (2N)^{2^j-j-1} \sum_h c_h b_h.$$

Кроме того,

$$\sum_h c_h b_h \ll c_0 b_0 + N^{\varepsilon} \sum_{h \neq 0} b_h \ll N^j N^{2^j - j + \varepsilon} + N^{\varepsilon} N^{2^j},$$

что дает требуемое заключение.

Лемма 2.6. *Пусть* $c_1, c_2, \ldots$ *— произвольная последовательность комплексных чисел и* F *имеет непрерывную производную на* $[0, X]$. *Тогда*

$$\sum_{m \leqslant X} c_m F(m) = F(X) \sum_{m \leqslant X} c_m - \int_0^X F'(\gamma) \sum_{m \leqslant \gamma} c_m \, d\gamma.$$

Доказательство. Эта лемма непосредственно получается из очевидного тождества $F(m) = F(X) - \int_m^X F'(\gamma)\, d\gamma$ переменой порядка суммирования и интегрирования.

2.3 Оценка на малых дугах

Теорема 2.1. *Если* $s > 2^k$, *то*

$$\int_{\mathfrak{m}} |f(\alpha)|^s d\alpha \ll n^{s/k-1-\delta}.$$

Доказательство. Величина $n^{-1-\delta}$ представляет собой понижение по сравнению с тривиальной оценкой $n^{s/k}$. Лемма Хуа с $j = k$ понижает ее на величину $n^{\varepsilon-1}$, а неравенство Вейля дает остальное.

Очевидно,

$$\int_{\mathfrak{m}} |f(\alpha)|^s d\alpha \ll \left(\sup_{\alpha \in \mathfrak{m}} |f(\alpha)|^{s-2^k}\right) \int_0^1 |f(\alpha)|^{2^k} d\alpha. \qquad (2.8)$$

Рассмотрим произвольную точку α на $\mathfrak{m}$. По теореме Дирихле (лемма 2.1), существуют a, q, $(a, q) = 1$ и $q \leqslant N^{k-\nu}$, такие, что $|\alpha - a/q| \leqslant q^{-1} N^{\nu-k}$. Так как $\alpha \in \mathfrak{m} \subset (N^{\nu-k}, 1 - N^{\nu-k})$, то $1 \leqslant a \leqslant q$, откуда $q > N^{\nu}$ (в противном случае α принадлежало бы $\mathfrak{M}$). Поэтому. согласно неравенству Вейля,

$$f(\alpha) \ll N^{1+\varepsilon} (q^{-1} + N^{-1} + qN^{-k})^{1/K} \ll N^{1+\varepsilon-\nu/K}.$$

Это в соединении с (1.7), (2.8) и леммой Хуа доказывает теорему.

2.4 Большие дуги

Первый шаг состоит в том, чтобы получить подходящее приближение функции f на $\mathfrak{M}(q, a)$ функциями

$$v(\beta) = \sum_{m=1}^{n} \frac{1}{k} m^{1/k-1} e(\beta m), \tag{2.9}$$

$$S(q, a) = \sum_{m=1}^{q} e(am^k/q). \tag{2.10}$$

Функция v получается из f заменой характеристической функции k-х степеней вероятностью того, что m есть k-я степень. Сумма $S(q,a)$ — это дополнительный множитель, который возникает для α, близких к a/q, поскольку k-е степени в общем случае неравномерно распределены по модулю q.

Лемма 2.7. *Пусть* $1 \leqslant a \leqslant q \leqslant N^{\nu}$, $(a,q) = 1$ *и* $\alpha \in \mathfrak{M}(q,a)$. *Тогда*

$$f(\alpha) = q^{-1} S(q,a)\, v(\alpha - a/q) + O(N^{2\nu}).$$

Доказательство. Для $Y \geqslant 0$

$$\sum_{m \leqslant Y} e(am^k/q) = \sum_{r=1}^{q} e(ar^k/q) \sum_{\substack{m \leqslant Y \\ m \equiv r \pmod q}}^{q} 1 = Yq^{-1} S(q, a) + O(q)$$

и

$$\sum_{m \leqslant Y^k} \frac{1}{k} m^{1/k-1} = \int_1^{Y^k} \frac{1}{k} \alpha^{1/k-1}\, d\alpha + O(1) = Y + O(1). \tag{2.11}$$

Пусть

$$c_m = \begin{cases} e(am/q) - q^{-1} S(q, a) \frac{1}{k} m^{1/k-1}, & \text{когда } m - k\text{-я степень}, \\ -q^{-1} S(q, a) \frac{1}{k} m^{1/k-1} & \text{в противном случае} \end{cases}$$

и $Y = \gamma^{1/k}$. Тогда

$$\sum_{m \leqslant \gamma} c_m \ll q \quad (\gamma \geqslant 0).$$

Следовательно, по лемме 2.6 с $F(\gamma) = e(\beta\gamma)$,

$$\sum_{m \leqslant X} c_m e(\beta m) \ll (1 + |\beta| X)\, q.$$

Полагая $X = n$, $\beta = \alpha - a/q$, получим лемму.

Выбор функции v в лемме 2.7 не является единственно возможным. Обе функции

$$v_1(\beta) = \int_0^{n^{1/k}} e(\beta\gamma^k)\,d\gamma$$

и

$$v_2(\beta) = \sum_{h=0}^{n} \frac{\Gamma(h+1/k)}{h!\,k} e(\beta h)$$

подошли бы для этой цели. Есть аргументы за и против каждой из v, v_1, v_2. Аналитическое выражение v_1 изучать легче, чем выражения для v или v_2, а использование v_2 позволило бы избежать некоторых технических трудностей при рассмотрении определяемой ниже величины $J(n)$. Однако v_2 отчасти искусственна, а при замене v на v_1 для изучения $J(n)$ требуется формула преобразования Фурье.

То, что v и v_1 обладают во многом сходным поведением для достаточно малых β, можно вывести из (2.11) и леммы 2.6. Именно

$$v(\beta) = e(\beta n)\,n^{1/k} - 2\pi i\beta \int_0^n e(\beta\gamma)\,\gamma^{1/k}\,d\gamma + O(1 + n|\beta|) =$$

$$= \int_0^n e(\beta\gamma)\frac{1}{k}\gamma^{1/k-1}\,d\gamma + O(1+n|\beta|) = v_1(\beta) + O(1+n|\beta|).$$

Пусть

$$V(\alpha, q, a) = q^{-1}S(q, a)\,v(\alpha - a/q). \tag{2.12}$$

Тогда, по лемме 2.7, для $\alpha \in \mathfrak{M}(q, a)$

$$f(\alpha)^s - V(\alpha, q, a)^s \ll N^{s-1}\,|f(\alpha) - V(\alpha, q, a)| \ll N^{s-1+2\nu}.$$

Следовательно,

$$\sum_{q \leqslant N^\nu} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} |f(\alpha)^s - V(\alpha, q, a)^s|\,d\alpha \ll N^{s-k-1+5\nu}.$$

Таким образом, существует положительная постоянная δ, зависящая только от k, такая, что

$$\int_{\mathfrak{M}} f(\alpha)^s e(-\alpha n)\,d\alpha = R^*(n) + O(n^{s/k-1-\delta}), \tag{2.13}$$

где

$$R^*(n) = \sum_{q \leqslant N^\nu} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} V(\alpha, q, a)^s e(-\alpha n)\,d\alpha,$$

Согласно (2.2) и (2.12), $R^*(n)$ является произведением вида

$$R^*(n) = \mathfrak{S}(n, N^\nu) J^*(n), \tag{2.14}$$

где

$$\mathfrak{S}(n, Q) = \sum_{q \leqslant Q} \sum_{\substack{a=1 \\ (a, q)=1}}^{q} (q^{-1} S(q, a))^s e(-an/q)$$

и

$$J^*(n) = \int_{-N^{\gamma-k}}^{N^{\gamma-k}} v(\beta)^s e(-\beta n)\, d\beta. \tag{2.15}$$

Сумма $\mathfrak{S}(n, Q)$ и интеграл $J^*(n)$ наиболее просто изучаются путем дополнения суммы до ряда и замены интервала интегрирования единичным интервалом.

Пусть

$$S(q) = \sum_{\substack{a=1 \\ (a, q)=1}}^{q} (q^{-1} S(q, a))^s e(-an/q). \tag{2.16}$$

По неравенству Вейля, $S(q, a) \ll q^{1+\varepsilon-1/K}$ при условии, что $(a, q) = 1$. Следовательно, если $s \geqslant 2^k + 1$ и ε достаточно малое, то

$$S(q) \ll q^{(\varepsilon-1/K)s+1} \ll q^{-1-2^{-k}}, \tag{2.17}$$

поэтому ряд

$$\mathfrak{S}(n) = \sum_{q=1}^{\infty} S(q) \tag{2.18}$$

сходится абсолютно и равномерно по n и

$$\mathfrak{S}(n, N^\nu) - \mathfrak{S}(n) \ll n^{-\delta}.$$

Отсюда вследствие (2.14)

$$R^*(n) = (\mathfrak{S}(n) + O(n^{-\delta}))\, J^*(n) \quad \text{и} \quad \mathfrak{S}(n) \ll 1. \tag{2.19}$$

Для того чтобы расширить интервал интегрирования в $J^*(n)$, как сказано выше, надо оценить величину изменения $v(\beta)$ при возрастании $|\beta|$ от 0 до $\frac{1}{2}$.

Лемма 2.8. *Предположим, что* $|\beta| \leqslant \frac{1}{2}$. *Тогда*

$$v(\beta) \ll \min(n^{1/k}, |\beta|^{-1/k}).$$

Такое же заключение имеет место и для вышеупомянутых функций v_1 и v_2; доказательства аналогичны; для v_1 результат справедлив при всех действительных β.

Доказательство. Доказательство получается использованием суммирования по Абелю. Согласно (2.11), имеем

$$\sum_{r=1}^{m} \frac{1}{k} r^{1/k-1} = m^{1/k} + O(1),$$

откуда лемма следует сразу для $|\beta| \leqslant 1/n$.

Предположим теперь, что $|\beta| > 1/n$ и $M = [|\beta|^{-1}]$. Тогда члены суммы

$$v(\beta) = \sum_{m=1}^{n} \frac{1}{k} m^{1/k-1} e(\beta m)$$

с $m \leqslant M$ оцениваются величиной $\ll M^{1/k} \ll |\beta|^{-1/k}$. Чтобы оценить оставшуюся часть суммы, положим

$$S_m = \sum_{r=1}^{m} e(\beta r), \quad c_m = \frac{1}{k} m^{1/k-1}.$$

Тогда

$$\sum_{m=M+1}^{n} \frac{1}{k} m^{1/k-1} e(\beta m) = c_{n+1} S_n - c_{M+1} S_M + \sum_{m=M+1}^{n} (c_m - c_{m+1}) S_m.$$

Так как $|S_m| \leqslant 1/(2|\beta|)$ и c_m — убывающая последовательность, то

$$\sum_{m=M+1}^{n} \frac{1}{k} m^{1/k-1} e(\beta m) \ll c_{M+1} |\beta|^{-1} < |\beta|^{-1/k},$$

что и требовалось.

Пусть

$$J(n) = \int_{-1/2}^{1/2} v(\beta)^s e(-\beta n)\, d\beta. \tag{2.20}$$

Тогда, согласно (2.15) и лемме 2.8,

$$J(n) \ll \int_0^{\infty} \min(n^{s/k}, \ \beta^{-s/k})\, d\beta \ll n^{s/k-1}$$

и

$$J^*(n) - J(n) \ll \int_{N^{\nu-k}}^{\infty} \beta^{-s/k}\, d\beta \ll n^{s/k-1-\delta}$$

при условии, что $s > k$. Отсюда ввиду (2.17)

$$R^*(n) = \mathfrak{S}(n) J(n) + O(n^{s/k-1-\delta}). \tag{2.21}$$

Это в соединении с (2.4), теоремой 2.1 и (2.13) дает следующий результат.

Теорема 2.2. *Если* $s > 2^k$, *то*

$$R(n) = \mathfrak{S}(n) J(n) + O(n^{s/k-1-\delta}).$$

2.5 Особый интеграл

Особый интеграл оценивается применением индукции по s. Следующая лемма играет двоякую роль, обеспечивая начало процесса индукции и осуществление шага индукции.

Лемма 2.9. *Пусть* α, β — *действительные числа,* $\alpha \geqslant \beta > 0$, $\beta \leqslant 1$. *Тогда*

$$\sum_{m=1}^{n-1} m^{\beta-1}(n-m)^{\alpha-1} = n^{\beta+\alpha-1}\left(\frac{\Gamma(\beta)\,\Gamma(\alpha)}{\Gamma(\beta+\alpha)} + O\left(n^{-\beta}\right)\right),$$

где константа, входящая в O, *зависит только от* α *и* β.

Доказательство. Рассмотрим функцию

$$\varphi(\gamma) = \gamma^{\beta-1}(n-\gamma)^{\alpha-1}.$$

На интервале $(0, n)$ φ имеет не более одной стационарной точки. Поэтому $(0, n)$ можно разбить на два интервала $(0, X)$, (X, n) (один из которых может быть пустым), такие, что φ возрастает на одном из них и убывает на другом. Следовательно.

$$\sum_{m=1}^{n-1} \varphi(m) = \int_0^n \varphi(\gamma)\,d\gamma + O(n^{\alpha-1} + n^{\beta+\alpha-2}) =$$
$$= \frac{\Gamma(\beta)\,\Gamma(\alpha)}{\Gamma(\beta+\alpha)} n^{\beta+\alpha-1} + O(n^{\alpha-1}).$$

Теорема 2.3. *Для* $s \geqslant 2$

$$J(n) = \Gamma\left(1+\frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} n^{s/k-1}(1 + O(n^{-1/k})). \qquad (2.22)$$

Доказательство. В силу (2.9) и (2.20)

$$J(n) = J_s(n) = \sum_{m_1=1}^{n} \underset{m_1+\ldots+m_s=n}{\ldots} \sum_{m_s=1}^{n} k^{-s}(m_1 \ldots m_s)^{1/k-1}.$$

При $s=2$ теорема непосредственно следует из леммы 2.9. Предположим, что теорема имеет место для некоторого $s \geqslant 2$. Тогда

$$J_{s+1}(n)=\sum_{m=1}^{n-1}\frac{1}{k}m^{1/k-1}J_s(n-m)=$$

$$=\Gamma\left(1+\frac{1}{k}\right)^s\Gamma\left(\frac{s}{k}\right)^{-1}k^{-1}\sum_{m=1}^{n-1}m^{1/k-1}(n-m)^{s/k-1}+$$

$$+O\left(\sum_{m=1}^{n-1}m^{1/k-1}(n-m)^{(s-1)/k-1}\right).$$

Справедливость теоремы в случае $s+1$ следует теперь из леммы 2.9.

2.6 Особый ряд

Особый ряд отражает распределение вычетов k-х степеней целых чисел по модулю q. Прежде чем перейти к изучению свойств $\mathfrak{S}(n)$, оценим $S(q, a)$ и $S(q)$.

Лемма 2.10. *Если* $(a, q)=(b, r)=(q, r)=1$, *то*

$$S(qr, ar+bq)=S(q, a)S(r, b).$$

Доказательство. Согласно алгоритму Евклида, каждый класс вычетов m по модулю qr единственным образом представляется в виде $tr+uq$ с $1 \leqslant t \leqslant q$ и $1 \leqslant u \leqslant r$. Следовательно, ввиду (2.10)

$$S(qr,\ ar+bq)=\sum_{t=1}^{q}\sum_{u=1}^{r}e(at^kr^k/q+bu^kq^k/r).$$

Так как числа tr и uq пробегают полные системы вычетов по модулям q и r соответственно, то лемма доказана.

Лемма 2.11. *Функция* $S(q)$ *мультипликативна.*

Доказательство. Пусть $(q, r)=1$. Тогда, согласно (2.16) и лемме 2.10,

$$S(q,\ r)=\sum_{\substack{a=1\\(a,\ q)=1}}^{q}\ \sum_{\substack{r=1\\(r,\ b)=1}}^{b}q^{-s}r^{-s}S(qr,\ ar+bq)^s e(-(ar+$$

$$+bq)n/(qr))=S(q)\,S(r).$$

Для каждого простого p определим формально функцию $T(p)$:

$$T(p) = \sum_{h=0}^{\infty} S(p^h). \tag{2.23}$$

Теорема 2.4. *Пусть $s > 2^k$. Тогда ряд $T(p)$ и произведение $\prod_p T(p)$ абсолютно сходятся и*

$$\mathfrak{S}(n) = \prod_p T(p).$$

Более того, существует положительная постоянная C, зависящая только от k, такая, что

$$\tfrac{1}{2} < \prod_{p \geqslant C} T(p) < \tfrac{3}{2}.$$

Доказательство. Утверждения теоремы легко следуют из (2.17), леммы 2.11 и элементарной теории рядов мультипликативных функций (см. теорему 286, Харди и Райт, 1979). Заметим, что ввиду (2.16) и (2.10) замена a на $-a$ в определении $S(q)$ дает $S(q) = \bar{S}(q)$. Таким образом, $S(q)$ и $T(p)$ — действительные числа.

Остается рассмотреть $T(p)$ при $p \leqslant C$. Существует тесная связь между T и $M_n(q)$ — числом решений сравнения

$$m_1^k + \ldots + m_s^k \equiv n \pmod q$$

с $1 \leqslant m_j \leqslant q$.

Лемма 2.12. *Для любого натурального числа q*

$$\sum_{d \mid q} S(d) = q^{1-s} M_n(q).$$

Заметим, что, если $q = p^l$, сумма слева равна

$$\sum_{h=0}^{l} S(p^h)$$

и, таким образом, согласно (2.23),

$$T(p) = \lim_{l \to \infty} p^{l(1-s)} M_n(p^l)$$

всякий раз, когда существует этот предел либо предел в (2.23).

Доказательство. Из соотношения ортогональности

$$\frac{1}{q} \sum_{r=1}^{q} e(hr/q) = \begin{cases} 1, & q \mid h, \\ 0, & q \nmid h \end{cases}$$

следует, что

$$M_n(q)=\frac{1}{q}\sum_{r=1}^{q}\sum_{m_1=1}^{q}\dots\sum_{m_s=1}^{q}e\left(r\left(m_1^k+\dots+m_s^k-n\right)/q\right).$$

Теперь сумма по r разбивается на подсуммы в соответствии с величиной (r, q). Общий член в каждой подсумме является периодической функцией m_j с периодом $q/(r, q)=d$. Отсюда

$$M_n(q)=$$

$$=\frac{1}{q}\sum_{d\mid q}\sum_{\substack{a=1\\(a,\,d)=1}}^{d}\left(\frac{q}{d}\right)^s\sum_{m_1=1}^{d}\dots\sum_{m_s=1}^{d}e\left(a\left(m_1^k+\dots+m_s^k-n\right)/d\right)$$

и лемма следует из (2.10) и (2.16).

Для дальнейшего полезно привести некоторые сведения из мультипликативной теории приведенной системы вычетов по модулю p^t. Изложение этой теории см. в гл. 6 работы И. М. Виноградова (1954) или гл. 10 книги Апостола [Apostol, (1976)].

Количество различных вычетов по модулю p^t k-х степеней чисел, т. е. вычетов вида x^k с $p\nmid x$, равно $\varphi(p^t)/(k, \varphi(t))$, когда p — нечетное, или $t=1$, или k — нечетное, и равно $2^{t-2}/(k, 2^{t-2})$, когда $t\geqslant 2$ и оба числа p и k — четные. (Здесь φ обозначает функцию Эйлера.) Таким образом, когда p в высокой степени делит k, вычеты k-й степени по модулю p^t сравнительно редки, и поэтому $M_n(p^t)$ довольно трудно оценить. Удобно, следовательно, определить $\tau=\tau(p)$ как наивысшую степень p, делящую k,

$$p^\tau \| k \tag{2.24}$$

и полагать

$$\gamma=\gamma(p)=\begin{cases}\tau+1, & \text{когда } p>2 \quad \text{или } p=2 \quad \text{и } \tau=0,\\ \tau+2, & \text{когда } p=2 \quad \text{и } \tau>0.\end{cases} \tag{2.25}$$

Таким образом, количество вычетов k-х степеней по модулю p^γ равно $\varphi(p^{\tau+1})/(k, \varphi(p^{\tau+1}))$, а число решений сравнения

$$x^k\equiv a \pmod{p^\gamma}$$

для $p\nmid a$ равно 0 или $p^{\gamma-\tau-1}(k, \varphi(p^{\tau+1}))$. К тому же если a — вычет k-й степени по модулю p^γ, то он будет также вычетом k-й степени по модулю p^t для каждого t.

Пусть $M_n^*(q)$ означает число решений сравнения

$$x_1^k+\dots+x_s^k\equiv n \pmod q \tag{2.26}$$

с $(x_1, q)=1$.

Лемма 2.13. *Предположим, что* $M_n^*(p^\gamma) > 0$ *и* $t \geqslant \gamma$. *Тогда*

$$M_n(p^t) \geqslant p^{(t-\gamma)(s-1)}.$$

Доказательство. Рассмотрим какое-нибудь решение сравнения

$$x_1^k \equiv n - x_2^k - \ldots - x_s^k \pmod{p^\gamma}$$

с $p \nmid x_1$. Тогда $p^{(t-\gamma)(s-1)}$ решений сравнения

$$y_1^k \equiv n - y_2^k - \ldots - y_s^k \pmod{p^t}$$

могут быть построены выбором $y_2, \ldots, y_s$ в виде $y_i \equiv x_i \pmod{p^\gamma}$. Причем $n - y_2^k - \ldots - y_s^k$ будет вычетом k-й степени по модулю p^γ, а, значит, также и по модулю p^t.

Разрешимость сравнения (2.26) устанавливается при помощи следующей леммы.

Лемма 2.14 (Коши, 1813; Дэвенпорт, 1935; Човла [Chowla, 1935*a*]). *Пусть* $\mathscr{A}$, $\mathscr{B}$ *обозначают соответственно множества из* r *и* s *классов вычетов по модулю* q. *Предположим далее, что* $0 \in \mathscr{B}$ *и что для любого* $b \in \mathscr{B}$ $b \not\equiv 0 \pmod q$ *имеем* $(b, q) = 1$. *Пусть* $\mathscr{A} + \mathscr{B}$ *означает множество классов вычетов по модулю* q *вида* $a + b$ *с* $a \in \mathscr{A}$ *и* $b \in \mathscr{B}$. *Тогда*

$$\operatorname{card}(\mathscr{A} + \mathscr{B}) \geqslant \min(q, r + s - 1).$$

Доказательство. Можно предположить, что $r + s - 1 \leqslant q$, в противном случае достаточно просто удалить $s - (q - r + 1)$ элементов из $\mathscr{B}$. Случай $r = q$ тривиален, так что можно считать в дальнейшем, что $r < q$. Доказательство теперь проводится индукцией по s. Случай $s = 1$ тривиален. Предположим, что $s > 1$ и что утверждение леммы справедливо, если $\operatorname{card} \mathscr{B} < s$. Тогда существуют $c \in \mathscr{A}$, $b \in \mathscr{B}$, такие, что $c + b \notin \mathscr{A}$, так как иначе для каждого $b \in \mathscr{B}$, $a + b$, как и a входило бы в $\mathscr{A}$, в таком случае

$$\sum_{a \in \mathscr{A}} (a + b) \equiv \sum_{a \in \mathscr{A}} a \pmod q, \quad rb \equiv 0 \pmod q.$$

Пусть $\mathscr{C} = \{b : b \in \mathscr{B},\ c + b \notin \mathscr{A}\}$, $\mathscr{A}_1 = \mathscr{A} \cup (\{c\} + \mathscr{C})$, $\mathscr{B}_1 = \mathscr{B} \setminus \mathscr{C}$. Тогда $1 \leqslant \operatorname{card} \mathscr{B}_1 < s$, $\operatorname{card} \mathscr{A}_1 + \operatorname{card} \mathscr{B}_1 = r + s$ и

$$\mathscr{A}_1 + \mathscr{B}_1 = (\mathscr{A} + \mathscr{B}_1) \cup ((\{c\} + \mathscr{B}_1) + \mathscr{C}) \subset \mathscr{A} + \mathscr{B}.$$

Лемма 2.15. *Предположим, что* $s \geqslant \frac{p}{p-1}(k, p^\tau(p-1))$ *для* $\gamma = \tau + 1$; $s \geqslant 2^{\tau+2}$ *для* $\gamma = \tau + 2$ *и* $k > 2$, *и* $s \geqslant 5$, *когда* $p = k = 2$. *Тогда* $M_n^*(p^\gamma) > 0$ *для любого* n.

Доказательство. В случае $\gamma = \tau + 1$ лемма получается многократным применением леммы 2.14. Когда $p = 2$, результат тривиален, когда $k > 2$, имеем неравенство $s \geqslant 2^{\gamma}$, и сравнение может быть удовлетворено, если взять x_j равным 0 или 1, а когда $k = 2$, сравнение $x_1^k + \ldots + x_5^k \equiv \equiv n \pmod 8$, как легко видеть, разрешимо при $2 \nmid x_1$.

Объединение заключений теоремы 2.3 и лемм 2.12, 2.13 и 2.15 дает следующую теорему.

Теорема 2.5. *Пусть* $s > 2^k$. *Тогда*

$$\mathfrak{S}(n) \gg 1.$$

2.7 Заключение

Из (2.19) и теорем 2.2, 2.3 и 2.5 следует

Теорема 2.6. *При* $s > 2^k$ *число* $R(n)$ *представлений* n *суммой* s k*-х степеней натуральных чисел выражается в виде*

$$R(n) = \Gamma\left(1 + \frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} n^{s/k-1}\mathfrak{S}(n) + O\left(n^{s/k-1-\delta}\right), \quad (2.27)$$

где $\mathfrak{S}(n) \gg 1$.

Следствие. $G(k) \leqslant 2^k + 1$.

Асимптотическая формула (2.27), вероятно, справедлива при любом $s \geqslant k + 1$. Граница $s > 2^k$ понижена для $k > 10$, о чем см. гл. 5. Однако для $3 \leqslant k \leqslant 10$ улучшения неизвестны. Было бы действительно большим достижением получить (2.27) при $k = 3$ и $s = 8$. Это можно было бы сделать, если бы удалось показать, что

$$\int_0^1 \Big| \sum_{x=1}^{N} e(\alpha x^3) \Big|^6 d\alpha \ll N^{7/2-\delta}. \quad (2.28)$$

Существует предположение, что

$$\int_0^1 |f(\alpha)|^{2s} d\alpha \ll N^{\varepsilon} \min\left(N^s, N^{2s-k}\right), \quad (2.29)$$

вследствие которого (2.27) имело бы место для всех $s \geqslant \geqslant 2k + 1$.

Пусть $k > 2$. Харди и Литтлвуд (1922) определили $\Gamma(k)$ как наименьшее s, такое, что для каждого простого p существует положительное число $C(p)$, такое, что $T(p) \geqslant C(p)$

равномерно по n. В более поздней статье (Харди, Литтлвуд (1925)) они показали, что $\mathfrak{S}(n) \gg 1$ для всех $s \geqslant \max(\Gamma(k), 4)$.

Если определить $\Gamma_0(k)$ как наименьшее s, такое, что для каждого q и n сравнение

$$x_1^k + \ldots + x_s^k \equiv n \pmod q$$

разрешимо с $(x_1, q) = 1$, то доказательство теоремы 1 из книги Харди и Литтлвуда (1928) показывает, что $\Gamma_0(k) = \Gamma(k)$. Они предположили, что $\Gamma(k) \to \infty$ при $k \to \infty$, но до сих пор не известно даже, справедливо ли неравенство

$$\liminf_{k \to \infty} \Gamma(k) \geqslant 4.$$

2.8 Упражнения

1. Покажите, что для $1 \leqslant j \leqslant k$ j-е применение Δ_j — разностного оператора — имеет выражение

$$\Delta_j(\alpha^k;\ \beta_1, \ldots, \beta_j) = \sum_{\substack{l_0 l_1, \ldots, l_j \\ l_0 \geqslant 0,\ l_1 \geqslant 1, \ldots, l_j \geqslant 1 \\ l_0 + l_1 + \ldots + l_j = k}} \frac{k!}{l_0!\, l_1! \ldots l_j!} \alpha^{l_0} \beta_1^{l_1} \ldots \beta_j^{l_j} =$$

$$= \beta_1 \ldots \beta_k p_j(\alpha;\ \beta_1, \ldots, \beta_j),$$

где p_j — многочлен от α степени $k - j$ с коэффициентом при старшем члене $k!/(k-j)!$.

2. Покажите, что при $k > 2$ $G(k) \geqslant \max(k + 1, \Gamma_0(k))$.
3. Покажите, что каждое большое натуральное число есть сумма одного квадрата и семи кубов.
4. Покажите, что для $s \geqslant 2$

$$\int_0^1 |f(\alpha)|^s \, d\alpha \gg \max(N^{s-k}, N^{s/2}).$$

5. Покажите, что число R решений уравнения

$$x_1^2 + y_1^4 + y_2^4 = x_2^2 + y_3^4 + y_4^4$$

с $x_i \leqslant n^{1/2}$, $y_i \leqslant n^{1/4}$ оценивается в виде $R \ll n^{1+\varepsilon}$. Получите асимптотическую формулу для количества представлений числа суммой двух квадратов, четырех биквадратов и k-й степени.

6. Пусть

$$v_1(\beta) = \int\limits_0^{n^{1/k}} e(\beta\gamma^k)\,d\gamma, \qquad v_2(\beta) = \sum_{h=0}^{n} \frac{\Gamma(h+1/k)}{h!\,k}\, e(\beta h).$$

Покажите, что

$$\int\limits_{-\infty}^{\infty} v_1(\beta)^s e(-\beta n)\,d\beta \quad \text{и} \quad \int\limits_0^1 v_2(\beta)^s e(-\beta n)\,d\beta$$

асимптотически равны $\Gamma\left(1+\frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} n^{s/k-1}$ при $n \to \infty$.

3
Проблемы Гольдбаха

3.1 Тернарная проблема Гольдбаха

Полученное И. М. Виноградовым решение тернарной проблемы Гольдбаха следует схеме предыдущей главы, но на этот раз с функцией

$$f(\alpha) = \sum_{p \leqslant n} (\log p)\, e(\alpha p). \tag{3.1}$$

Недостаточность нынешних знаний распределения простых чисел в арифметических прогрессиях диктует, чтобы большие дуги были возможно более редкими. Принципиальная трудность возникает на малых дугах и заключается в получении подходящего аналога неравенства Вейля.

Пусть B — положительная постоянная. Для достаточно большого n положим

$$P = (\log n)^B \tag{3.2}$$

Когда $1 \leqslant a \leqslant q \leqslant P$ и $(a, q) = 1$, пусть

$$\mathfrak{M}(q, a) = \{\alpha\colon\ |\alpha - a/q| \leqslant Pn^{-1}\} \tag{3.3}$$

обозначают типичные большие дуги, а $\mathfrak{M}$ — их объединение. Поскольку n достаточно велико, большие дуги не пересекаются и лежат в промежутке

$$\mathcal{U} = (Pn^{-1},\ 1 + Pn^{-1}].$$

Пусть $\mathfrak{m} = \mathcal{U} \setminus \mathfrak{M}$. Тогда ввиду (3.1)

$$R(n) = \int_{\mathcal{U}} f(\alpha)^3 e(-n\alpha)\, d\alpha =$$

$$= \int_{\mathfrak{M}} f(\alpha)^3 e(-n\alpha)\, d\alpha + \int_{\mathfrak{m}} f(\alpha)^3 e(-n\alpha)\, d\alpha, \tag{3.4}$$

где
$$R(n) = \sum_{\substack{p_1,\, p_2,\, p_3 \\ p_1 + p_2 + p_3 = n}} (\log p_1)(\log p_2)(\log p_3). \tag{3.5}$$

Изучение интеграла на малых дугах принципиально основано на следующей теореме.

Теорема 3.1. *Предположим, что* $(a, q) = 1$, $q \leqslant n$ *и* $|\alpha - a/q| \leqslant q^{-2}$. *Тогда*

$$f(\alpha) \ll (\log n)^4 (nq^{-1/2} + n^{4/5} + n^{1/2} q^{1/2}).$$

Доказательство. Пусть

$$\tau_x = \sum_{\substack{d \mid x \\ d \leqslant X}} \mu(d),$$

где μ — функция Мёбиуса. Тогда выбор $X = n^{2/5}$ и $\lambda(x, y) = \Lambda(y) e(\alpha x y)$ в тождестве

$$\sum_{X < y \leqslant n} \lambda(1, y) + \sum_{X < x \leqslant n} \sum_{X < y \leqslant n/x} \tau_x \lambda(x, y) =$$
$$= \sum_{d \leqslant X} \sum_{X < y \leqslant n/d} \sum_{z \leqslant n/yd} \mu(d) \lambda(dz, y)$$

дает

$$f(\alpha) = S_1 - S_2 - S_3 + O(n^{1/2}),$$

где

$$S_1 = \sum_{x \leqslant X} \sum_{y \leqslant n/x} \mu(x) (\log y) e(\alpha x y),$$

$$S_2 = \sum_{x \leqslant X^2} \sum_{y \leqslant n/x} c_x e(\alpha x y), \quad c_x = \sum_{\substack{d \leqslant X \\ dy = x}} \sum_{y \leqslant X} \mu(d) \Lambda(y),$$

$$S_3 = \sum_{\substack{x > X \\ xy \leqslant n}} \sum_{y > X} \tau_x \Lambda(y) e(\alpha x y).$$

Здесь Λ — функция Мангольдта, а тождество получается переменной порядка суммирования, если учесть, что $\tau_x = 0$ для $1 < x \leqslant X$.

Внутренняя сумма в S_1 равна

$$\mu(x) \int_1^{n/x} \sum_{\gamma < y \leqslant n/x} e(\alpha x y) \frac{d\gamma}{\gamma}$$

и $c_x \ll \log x$. Следовательно,

$$S_1, S_2 \ll (\log n) \sum_{x \leqslant X^2} \min\left(n/x, \|\alpha x\|^{-1}\right).$$

Отсюда, по лемме 2.2,

$$S_1, S_2 \ll (\log n)^2 (nq^{-1} + n^{4/5} + q).$$

Таким образом, остается оценить S_3.

Пусть $\mathscr{A} = \{X, 2X, 4X, \ldots, 2^k X \colon 2^k X^2 < n \leqslant 2^{k+1} X^2\}$. Тогда

$$S_3 = \sum_{Y \in \mathscr{A}} S(Y),$$

где

$$S(Y) = \sum_{Y < x \leqslant 2Y} \sum_{X < y \leqslant n/x} \tau_x \Lambda(y) e(\alpha x y).$$

Согласно неравенству Коши,

$$|S(Y)|^2 \ll \Big(\sum_{x \leqslant 2Y} d(x)^2\Big) \sum_{Y < x \leqslant 2Y} \Big| \sum_{X < y \leqslant n/x} \Lambda(y) e(\alpha xy) \Big|^2.$$

Легко показать, что

$$\sum_{x \leqslant Z} d(x)^2 \ll Z (\log 2Z)^3.$$

Следовательно,

$$|S(Y)|^2 \ll Y (\log n)^5 \sum_{y \leqslant n/Y} \sum_{z \leqslant n/Y} \min\left(Y, \ \|\alpha(y-z)\|^{-1}\right).$$

Таким образом, по лемме 2.2,

$$|S(Y)|^2 \ll n (\log n)^6 (nq^{-1} + Y + n/Y + q),$$

откуда,

$$S_3 \ll \sum_{Y \in \mathscr{A}} (\log n)^3 \left(nq^{-1/2} + n^{1/2} Y^{1/2} + nY^{-1/2} + n^{1/2} q^{1/2}\right)$$
$$\ll (\log n)^4 (nq^{-1/2} + n^{4/5} + n^{1/2} q^{1/2}),$$

что и требовалось.

Теперь, чтобы оценить интеграл

$$\int_{\mathfrak{m}} f(\alpha)^3 e(-n\alpha)\, d\alpha,$$

достаточно обратить внимание на два следующих обстоятельства. Во-первых, тождество Парсеваля и элементарная теория простых чисел дают

$$\int_0^1 |f(\alpha)|^2 d\alpha = \sum_{p \leqslant n} (\log p)^2 \ll n \log n.$$

Во-вторых, согласно теореме 3.1 (ср. с выводом теоремы 2.1),

$$\sup_{\alpha \in \mathfrak{m}} |f(\alpha)| \ll n (\log n)^{4 - B/2}.$$

Таким образом, справедлива

Теорема 3.2. *Если A — положительная постоянная и $B \geqslant 2A + 10$, то*

$$\int_{\mathfrak{m}} |f(\alpha)|^3 d\alpha \ll n^2 (\log n)^{-A}.$$

Изучение интеграла на больших дугах основано на применении теории распределения простых чисел в арифметических прогрессиях.

Лемма 3.1. *Пусть*

$$v(\beta)=\sum_{m=1}^{n} e(\beta m). \tag{3.6}$$

Тогда существует положительная постоянная C, такая, что каковы бы ни были $1\leqslant a\leqslant q\leqslant P$, $(a,q)=1$, $\alpha\in\mathfrak{M}(q,a)$, имеем

$$f(\alpha)=\frac{\mu(q)}{\varphi(q)}v\left(\alpha-\frac{a}{q}\right)+O\left(n\exp\left(-C(\log n)^{1/2}\right)\right).$$

Доказательство. Пусть

$$f_X(\alpha)=\sum_{p\leqslant X}(\log p)\,e(\alpha p).$$

Тогда

$$f_X(a/q)=\sum_{\substack{r=1\\(r,\ q)=1}}^{q} e(ar/q)\,\vartheta(X,\ q,\ r)+O((\log X)(\log q)),$$

где

$$\vartheta(X,\ q,\ r)=\sum_{\substack{p\leqslant X\\ p\equiv r\ (\mathrm{mod}\ q)}}(\log p).$$

Как известно [теорема 53, Estermann, 1952], для $\sqrt{n}<X\leqslant n$ имеем

$$f_X\left(\frac{a}{q}\right)=\frac{X}{\varphi(q)}\sum_{\substack{r=1\\(r,\ q)=1}}^{q} e\left(\frac{ar}{q}\right)+O\left(n\exp\left(-C_1(\log n)^{1/2}\right)\right). \tag{3.7}$$

То же самое тривиально имеет место и для $X\leqslant\sqrt{n}$. Кроме того, [см. теорема 271, Харди, Райт, 1979][2])

$$\sum_{\substack{r=1\\(r,\ q)=1}}^{q} e\left(\frac{ar}{q}\right)=\mu(q).$$

Следовательно, из (3.1), (3.6), (3.7) и леммы 2.6 при $X=n$, $F(m)=e(\beta m)$, $\beta=\alpha-a/q$,

$$c_m=\begin{cases} e\left(\dfrac{am}{q}\right)\log m-\mu(q)/\varphi(q), & \text{если } m \text{ — простое число,}\\ -\mu(q)/\varphi(q) & \text{в противном случае}\end{cases}$$

имеем

$$f(\alpha)-\frac{\mu(q)}{\varphi(q)}v\left(\alpha-\frac{a}{q}\right)\ll\left(1+n\left|\alpha-\frac{a}{q}\right|\right)n\exp\left(-C_1(\log n)^{1/2}\right),$$

что вместе с (3.3) и (3.2) доказывает лемму.

Пусть $\alpha \in \mathfrak{M}(q, a)$, тогда вследствие леммы 3.1

$$f(\alpha)^3 - \frac{\mu(q)}{\varphi(q)^3} v\left(\alpha - \frac{a}{q}\right)^3 \ll n^3 \exp\left(-C(\log n)^{1/2}\right).$$

Теперь интегрирование по $\mathfrak{M}$ дает

$$\sum_{q \leqslant P} \sum_{\substack{a=1 \\ (a,\ q)=1}}^{q} \int\limits_{\mathfrak{M}(q,\ a)} \left(f(\alpha)^3 - \frac{\mu(q)}{\varphi(q)^3} v\left(\alpha - \frac{a}{q}\right)^3\right) e(-\alpha n)\, d\alpha \ll$$
$$\ll P^3 n^2 \exp\left(-C(\log n)^{1/2}\right).$$

Следовательно, ввиду (3.3)

$$\int\limits_{\mathfrak{M}} f(\alpha)^3 e(-\alpha n)\, d\alpha = \mathfrak{S}(n, P) \int\limits_{-P/n}^{P/n} v(\beta)^3 e(-\beta n)\, d\beta +$$
$$+ O\left(P^3 n^2 \exp\left(-C(\log n)^{1/2}\right)\right), \quad (3.8)$$

где
$$\mathfrak{S}(n, P) = \sum_{q \leqslant P} \sum_{\substack{a=1 \\ (a,\ q)=1}}^{q} \frac{\mu(q)}{\varphi(q)^3} e(-an/q). \quad (3.9)$$

Согласно (3.6), если β — нецелое число,

$$v(\beta) \ll \|\beta\|^{-1}. \quad (3.10)$$

Поэтому отрезок интегрирования $[-P/n, P/n]$ можно заменить отрезком $\left[-\frac{1}{2}, \frac{1}{2}\right]$ с точностью до величины

$$\ll \sum_{q \leqslant P} \varphi(q)^{-2} n^2 P^{-2}.$$

Следовательно, ввиду (3.2)

$$\int\limits_{\mathfrak{M}} f(\alpha)^3 e(-\alpha n)\, d\alpha = \mathfrak{S}(n, P)\, J(n) + O\left(n^2 (\log n)^{-2B}\right), \quad (3.11)$$

где
$$J(n) = \int\limits_{-1/2}^{1/2} v(\beta)^3 e(-\beta n)\, d\beta.$$

Согласно (3.6), $J(n)$ есть число решений уравнения $n = m_1 + m_2 + m_3$ в целых числах $1 \leqslant m_j \leqslant n$. Таким образом,

$$J(n) = \frac{1}{2}(n-1)(n-2). \quad (3.12)$$

Кроме того, в силу (3.9) имеем

$$\mathfrak{S}(n, P) = \mathfrak{S}(n) + O\left(\sum_{q > P} \varphi(q)^{-2}\right),$$

где
$$\mathfrak{S}(n) = \sum_{q=1}^{\infty} \frac{\mu(q)}{\varphi(q)^3} \sum_{\substack{a=1 \\ (a,\ q)=1}}^{q} e(-an/q). \quad (3.13)$$

Отсюда ввиду (3.1), (3.11) и теоремы 327 [Харди, Райт (1979)]

$$\int_{\mathfrak{M}} f(\alpha)^3 e(-\alpha n)\, d\alpha = \mathfrak{S}(n) J(n) + O\left(n^2 (\log n)^{-B/2}\right).$$

Сумма Рамануджана (см. теоремы 67 и 272 [Харди, Райт (1979)])

$$c_q(n) = \sum_{\substack{a=1 \\ (a,\ q)=1}}^{q} e(-an/q)$$

является мультипликативной функцией q и выражается в виде

$$c_q(n) = \frac{\mu(q/(q,\ n))\, \varphi(q)}{\varphi(q/(q,\ n))}. \tag{3.14}$$

Следовательно, согласно (3.13),

$$\mathfrak{S}(n) = \prod_{p \nmid n} \left(1 + (p-1)^{-3}\right) \prod_{p \mid n} \left(1 - (p-1)^{-2}\right). \tag{3.15}$$

Мы доказали следующую теорему.

Теорема 3.3. *Пусть A — положительная постоянная, $B \geqslant 2A$. Тогда*

$$\int_{\mathfrak{M}} f(\alpha)^3 e(-n\alpha)\, d\alpha = \tfrac{1}{2} n^2 \mathfrak{S}(n) + O\left(n^2 (\log n)^{-A}\right),$$

где $\mathfrak{S}(n)$ определяется равенством (3.15).

Заметим, что $\mathfrak{S}(n) \gg 1$ для нечетного числа n и $\mathfrak{S}(n) = 0$, если n — четное. В соединении с теоремой 3.2 и (3.4) теорема 3.3 дает следующий результат.

Теорема 3.4. *Пусть A — положительная постоянная, $R(n)$ и $\mathfrak{S}(n)$ определяются соответственно формулами* (3.5) *и* (3.15). *Тогда*

$$R(n) = \tfrac{1}{2} n^2 \mathfrak{S}(n) + O\left(n^2 (\log n)^{-A}\right).$$

Следствие. *Каждое достаточно большое нечетное число является суммой трех простых чисел.*

3.2 Бинарная проблема Гольдбаха

В бинарной проблеме Гольдбаха нельзя изложенным выше способом получить асимптотическую формулу. Однако может быть получена нетривиальная оценка суммы

$$\sum_{m=1}^{n} (R_1(m) - m\mathfrak{S}_1(m))^2,$$

где
$$R_1(m) = \sum_{\substack{p_1,\ p_2 \\ p_1+p_2=m}} (\log p_1)(\log p_2),$$

а $\mathfrak{S}_1(m)$ — соответствующий особый ряд. Это выражение соответствует скорее кватернарной проблеме, чем бинарной. Оно приводит к следующему менее сильному заключению: почти все четные числа — суммы двух простых чисел.

Пусть

$$R_1(m) = R_1(m,\ n) = \sum_{\substack{p_1 \leqslant n \\ p_1+p_2=m}} \sum_{p_2 \leqslant n} (\log p_1)(\log p_2). \tag{3.16}$$

Тогда
$$R_1(m) = R_2(m) + R_3(m), \tag{3.17}$$

где
$$R_2(m) = \int_{\mathfrak{M}} f(\alpha)^2 e(-\alpha m)\,d\alpha \tag{3.18}$$

и
$$R_3(m) = \int_{\mathfrak{m}} f(\alpha)^2 e(-\alpha m)\,d\alpha. \tag{3.19}$$

Здесь f, $\mathfrak{M}$, $\mathfrak{m}$ такие же, как в § 3.1.

$R_3(m)$ является коэффициентом Фурье функции, которая равна $f(\alpha)^2$ на $\mathfrak{m}$ и 0 для других значений α. Следовательно, по неравенству Бесселя,

$$\sum_{m=1}^{n} |R_3(m)|^2 \leqslant \int_{\mathfrak{m}} |f(\alpha)|^4\,d\alpha. \tag{3.20}$$

Теорема 3.5. *Пусть A — положительная постоянная, $B \geqslant A + 9$. Тогда*

$$\sum_{m=1}^{n} |R_3(m)|^2 \ll n^3 (\log n)^{-A}.$$

Эта теорема ввиду (3.20) может быть выведена таким же способом, как теорема 3.2.

Пусть

$$\mathfrak{S}_1(m,\ P) = \sum_{q \leqslant P} \sum_{\substack{a=1 \\ (a,\ q)=1}}^{q} \frac{\mu(q)^2}{\varphi(q)^2} e(-am/q). \tag{3.21}$$

Тогда тривиальными видоизменениями рассуждений, дающих оценку (3.8), получаем

$$R_2(m) = \mathfrak{S}_1(m,\ P) \int_{-P/n}^{P/n} v(\beta)^2 e(-\beta m)\, d\beta +$$
$$+ O\left(P^3 n \exp\left(-C(\log n)^{1/2}\right)\right).$$

Кроме того, согласно (3.10),

$$\int_{P/n}^{1/2} |v(\beta)|^2 d\beta \ll nP^{-1}.$$

Отсюда ввиду (3.21) и элементарной оценки $\sum_{q \leqslant P} \varphi(q)^{-1} \ll \ll \log n$ имеем

$$R_2(m) = \mathfrak{S}_1(m,\ P) J_1(m) + O\left(n(\log n)^{1-B}\right),$$

где $$J_1(m) = \int_{-1/2}^{1/2} v(\beta)^2 e(-\beta m)\, d\beta.$$

Вследствие (3.6) $J_1(m)$ есть число решений уравнения $m = m_1 + m_2$ в целых числах $1 \leqslant m_j \leqslant n$. Отсюда при $m \leqslant n$ имеем $J_1(m) = m - 1$. Поэтому ввиду (3.21)

$$R_2(m) = m\mathfrak{S}_1(m, P) + O(n(\log n)^{1-B}) \quad (1 \leqslant m \leqslant n). \tag{3.22}$$

Согласно (3.14) и элементарной оценке

$$\sum_{q > Z} \varphi(q)^{-2} \ll Z^{-1},$$

имеем

$$\sum_{X < q \leqslant Y} \frac{\mu(q)^2}{\varphi(q)^2} \sum_{\substack{a=1 \\ (a,\ q)=1}}^{q} e(-am/q) = \sum_{d \mid m} \frac{\mu(d)^2}{\varphi(d)} \sum_{\substack{X/d < q \leqslant Y/d \\ (q,\ m)=1}} \frac{\mu(q)}{\varphi(q)^2} \ll$$
$$\ll \sum_{d \mid m} \frac{\mu(d)^2}{\varphi(d)} \min\left(\frac{d}{X},\ 1\right). \tag{3.23}$$

Следовательно, ряд

$$\mathfrak{S}_1(m) = \sum_{q=1}^{\infty} \frac{\mu(q)^2}{\varphi(q)^2} \sum_{\substack{a=1 \\ (a,\ q)=1}}^{q} e(-am/q) \tag{3.24}$$

сходится,

$$\mathfrak{S}_1(m, P) - \mathfrak{S}_1(m) \ll \log m$$

и

$$\sum_{m=1}^{n} |\mathfrak{S}_1(m, P) - \mathfrak{S}_1(m)|^2 \ll (\log n) \sum_{d \leqslant n} \frac{\mu(d)^2 n}{\varphi(d) d} \min\left(\frac{d}{P}, 1\right) \ll$$
$$\ll n (\log n) P^{-1} \sum_{d \leqslant n} \frac{\mu(d)^2}{\varphi(d)} \ll nP^{-1} (\log n)^2.$$

Отсюда в силу (3.2) и (3.22)

$$\sum_{m=1}^{n} |R_2(m) - m\mathfrak{S}_1(m)|^2 \ll n^3 (\log n)^{2-B}. \tag{3.25}$$

В силу (3.14)

$$\mathfrak{S}_1(m) = \prod_{p \nmid m} \left(1 - (p-1)^{-2}\right) \prod_{p \mid m} \left(1 + (p-1)^{-1}\right). \tag{3.26}$$

Теперь, выбрав подходящую постоянную B, получаем теорему.

Теорема 3.6. *Пусть A — положительная постоянная, $B \geqslant A + 2$. Тогда*

$$\sum_{m=1}^{n} |R_2(m) - m\mathfrak{S}_1(m)|^2 \ll n^3 (\log n)^{-A},$$

где $\mathfrak{S}_1(m)$ определяется равенством (3.26).

Комбинируя равенство (3.17) и теоремы 3.5, 3.6, получаем следующую теорему.

Теорема 3.7. *Пусть A — положительная постоянная. Тогда*

$$\sum_{m=1}^{n} |R_1(m) - m\mathfrak{S}_1(m)|^2 \ll n^3 (\log n)^{-A},$$

где R_1 и $\mathfrak{S}_1$ определяются равенствами (3.16) *и* (3.26) *соответственно.*

Заметим, что $\mathfrak{S}_1(m) \gg 1$, когда m четно, и $\mathfrak{S}_1(m) = 0$ для нечетных m.

Следствие. *Число $E(n)$ четных чисел m, не превосходящих n, непредставимых в виде суммы двух простых чисел, удовлетворяет неравенству*

$$E(n) \ll n (\log n)^{-A}.$$

Доказательство. Согласно (3.16) и (3.26) для каждого m, входящего в $E(n)$,

$$m^{-2} |R_2(m) - m\mathfrak{S}_1(m)|^2 = \mathfrak{S}_1(m)^2 \gg 1,$$

Отсюда

$$E(n) \ll \sum_{m=1}^{n} m^{-2} \left| R_2(m) - m\mathfrak{S}_1(m) \right|^2.$$

Утверждение теоремы получается теперь из теоремы 3.7 частичным суммированием.

3.3 Упражнения

1. Покажите, что каждое большое натуральное число может быть представлено в виде $p_1 + p_2 + x^k$.
2. Пусть $a_1, \ldots, a_4$ — фиксированные отличные от 0 целые числа, причем a_1, a_2, a_3 не все одного знака. Покажите, что

$$R(n) = \sum_{\substack{p_1 \leqslant n \\ a_1p_1+a_2p_2+a_3p_3+a_4=0}} \sum_{p_2 \leqslant n} \sum_{p_3 \leqslant n} (\log p_1)(\log p_2)(\log p_3)$$

выражается в виде

$$R(n) = J(n)\mathfrak{S} + O(n^2(\log n)^{-A}),$$

где $J(n)$ — число решений уравнения

$$a_1m_1 + a_2m_2 + a_3m_3 + a_4 = 0$$

с $m_j \leqslant n$ и

$$\mathfrak{S} = \sum_{q=1}^{\infty} \varphi(q)^{-3} \prod_{j=1}^{4} c_q(a_j).$$

Покажите, что если $(a_1, a_2, a_3) \mid a_4$, то $J(n) \gg n^2$ для больших n.

3. В обозначениях предыдущего упражнения покажите, что достаточным условием того, что $\mathfrak{S} \gg 1$, являются следующие соотношения:

$$(a_2, a_3, a_4) = (a_1, a_3, a_4) = (a_1, a_2, a_4) = (a_1, a_2, a_3),$$

$$a_1 + a_2 + a_3 + a_4 \equiv 0 (\operatorname{mod} 2(a_1, a_2, a_3, a_4)).$$

Покажите, что эти соотношения также необходимы и что в противном случае $\mathfrak{S} = 0$.

4
Большие дуги в проблеме Варинга

4.1 Обобщенная функция

Теория больших дуг в проблеме Варинга, изложенная в гл. 2, может быть значительно усовершенствована. Наша цель здесь — получить относительно хороший остаточный член приближения $V(\alpha, q, a)$ для обобщенной функции $f(\alpha)$ на каждой большой дуге, делая эти дуги как можно более широкими и многочисленными.

Пусть

$$S(q, a, b) = \sum_{x=1}^{q} e((ax^k + bx) q^{-1}). \tag{4.1}$$

Лемма 4.1 (Хуа, 1957 *a*). *Предположим, что* $(q, a) = 1$. *Тогда*

$$S(q, a, b) \ll q^{1/2+\varepsilon}(q, b).$$

Доказательство использует глубокую теорему Вейля (Weil, см. ниже ссылку на Шмидта). Есть более элементарная теорема Дэвенпорта и Хельбронна (1936*b*, 1937*a*), в которой показатель степени $\frac{1}{2}$ заменен на $\frac{2}{3}$ для $k = 3$ и на $\frac{3}{4}$ для $k \geqslant 4$. Кроме того, теорема 7.1 вместо $\frac{1}{2}$ дает $1 - 1/k$. На самом деле рассуждения Морделла, используемые в доказательстве теоремы 7.1 в случае, когда q — простое число, можно изменить так, что вместе с рассуждениями, приведенными ниже, это даст теорему Дэвенпорта — Хельбронна.

Доказательство. Если $(q_1, q_2) = 1$, имеем (ср. с доказательством леммы 2.10)

$$S(q_1 q_2, a, b) = S(q_1, a q_2^{k-1}, b) S(q_2, a q_1^{k-1}, b).$$

Таким образом, достаточно показать, что для любой степени простого числа p^l при $p \nmid a$

$$S(p^l, a, b) \ll p^{l/2}(p^l, b). \tag{4.2}$$

При $l = 1$ оценка (4.2) сразу вытекает из следствия 2*F* гл. II книги Шмидта [Schmidt, 1976]. Поэтому можно предполагать, что $l > 1$.

Если $b=0$ или $b\neq 0$ и наивысшая степень p, p^{θ}, делящая b, удовлетворяет неравенству $\theta \geqslant l/2$, то оценка (4.2) тривиальна. Аналогично, если наивысшая степень p, p^{τ}, которая делит k, удовлетворяет неравенству $\tau \geqslant l/2$, оценка (4.2) также тривиальна. Следовательно, можно в дальнейшем считать, что

$$b\neq 0,\quad \tau<\tfrac{1}{2}l,\quad \theta<\tfrac{1}{2}l.$$

Пусть
$$\nu=\left[\tfrac{1}{2}(l+1)\right].$$

Тогда $3l-3\nu \geqslant l$. В определении $S(p^l, a, b)$ (формула (4.1)) каждое x по модулю p^l может быть записано единственным образом в виде $zp^{l-\nu}+y$ с $1\leqslant y\leqslant p^{l-\nu}$, $1\leqslant z\leqslant p^{\nu}$. Следовательно, по биномиальной теореме

$$S(p^l,\ a,\ b)=\sum_{y=1}^{p^{l-\nu}}\sum_{z=1}^{p^{\nu}} e\left((ay^k+by)p^{-l}+(kay^{k-1}+b)zp^{-\nu}+\right.$$
$$\left.+\binom{k}{2}ay^{k-2}z^2p^{l-2\nu}\right). \tag{4.3}$$

Предположим сначала, что l четно или $p\mid\binom{k}{2}$. Тогда $\binom{k}{2}p^{l-2\nu}$ — целое число, и отсюда, согласно (4.3),

$$|S(p^l, a, b)|\leqslant p^{\nu}N,$$

где N — число решений сравнения

$$kay^{k-1}+b\equiv 0 \pmod{p^{\nu}} \tag{4.4}$$

с $1\leqslant y\leqslant p^{l-\nu}$. Напомним, что $\max(\theta,\tau)<l/2\leqslant\nu$. Таким образом, это сравнение неразрешимо, если не имеет места неравенство $\theta\geqslant\tau$ и $\theta-\tau$ кратно $k-1$. Если (4.4) не имеет решений, то (4.2) следует немедленно. В противном случае пусть $\lambda=(\theta-\tau)/(k-1)$. Тогда N есть число решений сравнения

$$(kp^{-\tau})aw^{k-1}+(bp^{-\theta})\equiv 0 \pmod{p^{\nu-\theta}}$$

с $1\leqslant w\leqslant p^{l-\nu-\lambda}$. Заметим, что $\lambda\leqslant\theta\leqslant l-\nu$. Когда $l-\nu-\lambda\leqslant\nu-\theta$, имеем $N\ll 1$, так что

$$|S(p^l, a, b)|\ll p^{\nu}.$$

Если $l-\nu-\lambda>\nu-\theta$, то $N\ll p^{l+\theta-2\nu-\lambda}$, так что

$$|S(p^l, a, b)|\ll p^{l-\nu}p^{\theta}.$$

В обоих случаях

$$|S(p^l, a, b)|\ll p^{\nu}(p^l, b). \tag{4.5}$$

Когда l четное, $\nu=[(l+1)/2]=l/2$, и если $p\mid\binom{k}{2}$, то $p^{\nu}\leqslant p^{1+l/2}\ll p^{l/2}$. Таким образом, (4.2) следует из (4.5).

Остается рассмотреть случай, когда l — нечетное число и $p \nmid \binom{k}{2}$. Тогда

$$\nu = \tfrac{1}{2}(l+1), \quad \nu \geqslant 2.$$

Каждое z в (4.3) однозначно по модулю p^ν и записывается в виде $rp + w$ с $1 \leqslant r \leqslant p^{\nu-1}$, а $1 \leqslant w \leqslant p$. Более того,

$$\binom{k}{2} ay^{k-2}z^2 \equiv \binom{k}{2} ay^{k-2}w^2 \pmod p.$$

Поэтому сумма по r равна нулю, если сравнение $kay^{k-1} + b \equiv 0 \pmod{p^{\nu-1}}$ не имеет места. Отсюда

$$S(p^l, a, b) = p^{\nu-1} \sum_{y=1}^{p^{l-\nu}} e\left((ay^k + by)p^{-l}\right) \times \\ \times \sum_{w=1}^{p} e\left(\left(\binom{k}{2} ay^{k-2}w^2 + vw\right)p^{-1}\right) \quad (4.6)$$

с y и v, удовлетворяющими соотношениям

$$kay^{k-1} + b \equiv 0 \pmod{p^{\nu-1}} \text{ и } v = (kay^{k-1} + b)p^{1-\nu} \quad (4.7)$$

Сначала рассмотрим вклад S_1 членов с $p \mid y^{k-2}$. В таком случае $k > 2$ и внутренняя сумма равна нулю, если $p \nmid v$. Таким образом, по (4.7)

$$S_1 \ll p^\nu N,$$

где N — число решений сравнения

$$kap^{k-1}u^{k-1} + b \equiv 0 \pmod{p^\nu}$$

с $1 \leqslant u \leqslant p^{l-\nu-1}$. Аналогично предыдущему случаю получается $N = 0$, если $\theta \neq k - 1 + \tau + (k-1)\lambda$ с $\lambda \geqslant 0$, а в противном случае N есть число решений сравнения

$$(kp^{-\tau})ay^{k-1} + (bp^{-\theta}) \equiv 0 \pmod{p^{\nu-\theta}}$$

с $1 \leqslant y \leqslant p^{l-\nu-1-\lambda}$. Заметим, что $\theta \geqslant k-1 > 0$. Если $l - \nu - 1 - \lambda \leqslant \nu - \theta$, то $N \ll 1$ и, значит, $S_1 \ll p^\nu \leqslant p^{\nu-1+\theta} \leqslant p^{l/2}(p^l, b)$. При $l - \nu - 1 - \lambda > \nu - \theta$ имеем $N \ll p^{l-\nu-1-\lambda-(\nu-\theta)}$, так что снова

$$S_1 \ll p^{l-\nu-1-\lambda+\theta} \leqslant p^{l/2}(p^l, b).$$

Теперь остается оценить вклад S_2 членов в (4.6) с $p \nmid y^{k-2}$.

Тогда внутренняя сумма, как легко видеть, есть $\ll p^{1/2}$ (ср. со случаем $k=2$ теоремы 4.2). Таким образом,

$$S_2 \ll p^{\nu-1/2}N,$$

где N — число решений сравнения

$$kay^{k-1} + b \equiv 0 \pmod{p^{\nu-1}}$$

с $1 \leqslant y \leqslant p^{l-\nu}$. Заметим, что $\nu - \frac{1}{2} = \frac{1}{2} l$, $l - \nu = \nu - 1 = \frac{1}{2}(l - 1) \geqslant \theta$ и $l \geqslant 3$. Если $\theta = \frac{1}{2}(l-1)$, то сразу

$$S_2 \ll p^{l/2}(p^l, b).$$

Если $\theta < \frac{1}{2}(l-1)$, то, так же как и выше, или $N = 0$, или $\theta - \tau = \lambda(k-1)$, где $\lambda \geqslant 0$ и, следовательно, $N \ll \ll p^{(l-1)/2 - \lambda - ((l-1)/2 - \theta)} \leqslant p^{\theta}$. Таким образом, в этом случае также

$$S_2 \ll p^{l/2}(p^l, b).$$

Следующая лемма часто является исходной для оценки экспоненциальных сумм. Это сокращенная форма формулы суммирования Пуассона.

Лемма 4.2. *Предположим, что $X < Y$, F'' существует и непрерывна на $[X, Y]$, а F' монотонна на $[X, Y]$. Пусть H_1, H_2 — целые числа, такие, что $H_1 \leqslant F'(\alpha) \leqslant H_2$ для любого $\alpha \in \in [X, Y]$. Тогда*

$$\sum_{X < x \leqslant Y} e(F(x)) = \sum_{h=H_1}^{H_2} \int_X^Y e(F(\alpha) - \alpha h)\, d\alpha + O(\log(2 + H)),$$

где $H = \max(|H_1|, |H_2|)$.

Доказательство. Для дифференцируемой функции $\psi(\alpha)$ с непрерывной производной ψ' формула суммирования Эйлера — Маклорена дает

$$\sum_{X < x \leqslant Y} \psi(x) = \int_X^Y \psi(\alpha)\, d\alpha - \left[\psi(\alpha)\left(\alpha - [\alpha] - \tfrac{1}{2}\right)\right]_X^Y + \\ + \int_X^Y \psi'(\alpha)\left(\alpha - [\alpha] - \tfrac{1}{2}\right) d\alpha. \tag{4.8}$$

Следовательно,

$$\sum_{X < x \leqslant Y} e(F(x)) = \int_X^Y e(F(\alpha))\, d\alpha + \\ + \int_X^Y 2\pi i F'(\alpha)\, e(F(\alpha))\left(\alpha - [\alpha] - \tfrac{1}{2}\right) d\alpha + O(1).$$

Напомним теперь разложение Фурье

$$\alpha - [\alpha] - \tfrac{1}{2} = \sum_{\substack{h=-\infty \\ h \neq 0}}^{\infty} \frac{e(-\alpha h)}{2\pi i h}.$$

Этот ряд ограниченно сходится для всех действительных α. Поэтому второй интеграл записывается в виде

$$\sum_{\substack{h=-\infty \\ h \neq 0}}^{\infty} \frac{1}{h} \int_X^Y F'(\alpha)\, e(F(\alpha) - \alpha h)\, d\alpha.$$

Когда $h > H_2$ или $h < H_1$, $F'(\alpha) - h$ монотонна и не обращается в нуль на $[X, Y]$. Поэтому $F'(\alpha)/(F'(\alpha) - h)$ также монотонна на $[X, Y]$. Таким образом, интегрирование по частям дает

$$\int_X^Y F'(\alpha)\, e(F(\alpha) - h\alpha)\, d\alpha \ll \left| \frac{F'(Y)}{F'(Y) - h} \right| + \left| \frac{F'(X)}{F'(X) - h} \right|.$$

Следовательно,

$$\sum_{\substack{h=H_2+1 \\ h \neq 0}}^{\infty} \frac{1}{h} \int_X^Y F'(\alpha)\, e(F(\alpha) - h\alpha)\, d\alpha \ll$$

$$\ll \sum_{\substack{h=H_2+1 \\ h \neq 0}}^{\infty} \left(\frac{|H_2|}{|h|(h - H_2)} + \frac{|H_1|}{|h|(h - H_1)} \right) \ll 1 + \sum_{h=1}^{H+1} \frac{1}{h},$$

и аналогично получаем для суммы по $h \leqslant H_1 - 1$. Интегрирование по частям оставшихся членов дает

$$\sum_{X < x \leqslant Y} e(F(x)) = \int_X^Y e(F(\alpha))\, d\alpha + \sum_{\substack{h=H_1 \\ h \neq 0}}^{H_2} \int_X^Y e(F(\alpha) - \alpha h)\, d\alpha +$$

$$+ O(\log(2 + H)).$$

Если $H_1 \leqslant 0 \leqslant H_2$, то доказательство леммы закончено. Если же $0 < H_1$ или $H_2 < 0$, то $|F'(\alpha)| \geqslant 1$ и поэтому

$$\int_X^Y e(F(\alpha))\, d\alpha = \left[\frac{e(F(\alpha))}{2\pi i F'(\alpha)} \right]_X^Y + \int_X^Y \frac{F''(\alpha)\, e(F(\alpha))}{F'(\alpha)^2\, 2\pi i}\, d\alpha \ll 1,$$

что входит в остаточный член.

Пусть

$$f(\alpha) = \sum_{x \leqslant n^{1/k}} e(\alpha x^k), \tag{4.9}$$

$$S(q, a) = \sum_{m=1}^{q} e(am^k/q), \tag{4.10}$$

$$v(\beta)=\sum_{x\leqslant n}\frac{1}{k}x^{1/k-1}e(\beta x),\quad v_1(\beta)=\int\limits_0^{n^{1/k}}e(\beta\gamma^k)\,d\gamma,\tag{4.11}$$

$$V(\alpha,\ q,a)=q^{-1}S(q,\ a)\,v(\alpha-a/q).\tag{4.12}$$

Теорема 4.1. *Предположим, что* $(a,q)=1$ *и* $\alpha=a/q+\beta$. *Тогда*

$$f(\alpha)-V(\alpha,q,a)\ll q^{1/2+\varepsilon}(1+n|\beta|).\tag{4.13}$$

Если, кроме того, $|\beta|\leqslant(2kq)^{-1}n^{1/k-1}$, *то*

$$f(\alpha)-V(\alpha,q,a)\ll q^{1/2+\varepsilon}.\tag{4.14}$$

Те же утверждения справедливы при замене $v(\beta)$ *на* $v_1(\beta)$.

Доказательство использует лемму 4.1. Если вместо нее используются более слабые результаты, упоминавшиеся в замечании после этой леммы, то показатель степени $\frac{1}{2}$ в теореме 4.1 заменяется соответствующим большим показателем.

Доказательство. Для $X\leqslant n^{1/k}$ положим

$$f_X(\alpha)=\sum_{x\leqslant X}e(\alpha x^k).$$

Согласно (4.1) и (4.9),

$$f_X(\alpha)=\sum_{x\leqslant X}e(\beta x^k)\sum_{\substack{m=1\\ m\equiv x\ (\mathrm{mod}\ q)}}^{q}e(am^k/q)=$$

$$=q^{-1}\sum_{b=1}^{q}\Big(\sum_{x\leqslant X}e(\beta x^k-bx/q)\Big)S(q,\ a,\ b).$$

Отсюда

$$f_X(\alpha)-q^{-1}S(q,\ a)\,F(q)=q^{-1}\sum_{b=1}^{q-1}F(b)\,S(q,\ a,\ b),\tag{4.15}$$

где
$$F(b)=\sum_{x\leqslant X}e(\beta x^k-bx/q).\tag{4.16}$$

Если $\beta=0$ и $q\nmid b$, то $F(b)\ll\|b/q\|^{-1}$. Отсюда по лемме 4.1 и (4.15)

$$f_X\left(\frac{a}{q}\right)-q^{-1}S(q,\ a)\,[X]\ll q^{-1}\sum_{b=1}^{q-1}\|b/q\|^{-1}q^{1/2+\varepsilon}(q,\ b)\ll q^{1/2+2\varepsilon}.$$

Теперь (4.13) легко получается при помощи интегрирования по частям (ср. с доказательством леммы 2.7). Эквивалентность v и v_1 в (4.13) вытекает из замечания после этой леммы.

Остается доказать (4.14). Далее будем предполагать, что $X=n^{1/k}$, так что в (4.15) $f_X(\alpha)=f(\alpha)$. При $1\leqslant b\leqslant q$ выражение $\beta k\gamma^{k-1} - b/q$ — монотонная функция γ на $[0, X]$ со значениями между $-\left(b+\frac{1}{2}\right)/q$ и $-\left(b-\frac{1}{2}\right)/q$. Таким образом, может быть применена лемма 4.2 с $H_1 = -2$, $H_2 = 0$, откуда

$$F(b) = \sum_{h=-2}^{0} \int_0^X e(\beta\gamma^k - b\gamma/q - \gamma h)\, d\gamma + O(1). \qquad (4.17)$$

При $1 \leqslant b \leqslant q-1$ и $0 \leqslant \gamma \leqslant X$ имеем $|\beta k\gamma^{k-1} - b/q - h| \geqslant \geqslant \|\beta k\gamma^{k-1} - b/q\| \geqslant \frac{1}{2}\|b/q\|$. Таким образом, интегрируя по частям, получаем

$$\int_0^X e(\beta\gamma^k - b\gamma/q - \gamma h)\, d\gamma \ll \|b/q\|^{-1},$$

и поэтому, согласно (4.17), $F(b) \ll \|b/q\|^{-1}$. Следовательно, по лемме 4.1, правая часть (4.15) есть величина

$$\ll q^{-1} \sum_{b=1}^{q-1} \|b/q\|^{-1} q^{1/2+\varepsilon}(q, b) \ll q^{1/2+2\varepsilon}.$$

Рассмотрим теперь $F(q)$. При $0 \leqslant \gamma \leqslant X$ имеем $|\beta k\gamma^{k-1} \pm \pm 1| \geqslant \frac{1}{2}$. Отсюда интегрирование по частям дает

$$\int_0^X e(\beta\gamma^k \pm \gamma)\, d\gamma \ll 1.$$

Следовательно, в силу (4.11) и (4.17)

$$F(q) = v_1(\beta) + O(1). \qquad (4.18)$$

Это дает (4.14) с $v_1(\beta)$ вместо $v(\beta)$.

Пусть

$$G(Y) = \sum_{m \leqslant Y} \frac{1}{k} m^{1/k-1}.$$

Формула суммирования Эйлера — Маклорена (4.8) дает

$$G(Y) = Y^{1/k} + C_k + O(Y^{1/k-1}).$$

Следовательно, по лемме 2.6 и (4.11)

$$v(\beta) = G(X^k)\, e(\beta X^k) - 2\pi i\beta \int_1^{X^k} G(\gamma)\, e(\beta\gamma)\, d\gamma =$$

$$= (X + C_k)\, e(\beta X^k) - 2\pi i\beta \int_1^{X^k} (\gamma^{1/k} + C_k)\, e(\beta\gamma)\, d\gamma + O(X^{1-k} + |\beta| X).$$

Интегрирование по частям и замена переменных показывают, что

$$v(\beta) = v_1(\beta) + O(X^{1-k} + |\beta| X).$$

Формула (4.14) следует из этого результата, если в нем заменить $v(\beta)$ на $v_1(\beta)$, и это заканчивает доказательство теоремы.

4.2 Экспоненциальная сумма $S(q, a)$

Лемма 4.3. *Пусть $p \nmid a$. Тогда*

$$S(p, a) = \sum_{\chi \in \mathscr{A}} \bar{\chi}(a)\, \tau(\chi), \tag{4.19}$$

где $\mathscr{A}$ обозначает множество неглавных характеров χ по модулю p, для которых χ^k — главный характер, а $\tau(\chi)$ обозначает сумму Гаусса

$$\sum_{x=1}^{p} \chi(x)\, e(x/p).$$

Кроме того, $|\tau(\chi)| = p^{1/2}$ *и* $\operatorname{card} \mathscr{A} = (k, p-1) - 1$.

Доказательство. Пусть g — первообразный корень по модулю p. Тогда $\mathscr{A}$ — множество характеров χ_h вида

$$\chi_h(x) = e\left(\frac{h}{(k,\ p-1)} \operatorname{ind}_g x\right) \quad (p \nmid x)$$

с $1 \leqslant h < (k, p-1)$. Таким образом,

$$1 + \sum_{\chi \in \mathscr{A}} \chi(x)$$

есть число решений в y сравнения $y^k \equiv x \pmod p$. Откуда

$$S(p,\ a) = \sum_{x=1}^{p} e(ax/p) \left(1 + \sum_{\chi \in \mathscr{A}} \chi(x)\right),$$

что дает (4.19). Остальные утверждения леммы тривиальны.

Пусть τ и γ такие же, как в (2.24) и (2.25). Заметим, что $\gamma \leqslant k$ всегда, кроме случая $k = p = 2$, когда $\gamma = 3$. (4.20)

Лемма 4.4. *Предположим, что $p \nmid a$ и $l > \gamma$. Тогда*

$$S(p^l,\ a) = \begin{cases} p^{l-1} & \text{при} \quad l \leqslant k, \\ p^{k-1} S(p^{l-k},\ a) & \text{при} \quad l > k. \end{cases}$$

Доказательство. Напомним, что приведенный вычет по модулю p^l является вычетом k-й степени тогда и только тогда, когда он является вычетом k-й степени по модулю p^γ. Таким образом,

$$S(p^l,\ a) = \sum_{\substack{y=1 \\ p \nmid y}}^{p^\gamma} \sum_{z=1}^{p^{l-\gamma}} e\left(a\left(zp^\gamma + y^k\right) + p^{-l}\right) + \sum_{y=1}^{p^{l-1}} e\left(ap^{k-l} y^k\right).$$

Внутренняя сумма в двойной сумме равна 0, а сумма справа равна p^{l-1} при $l \leqslant k$ и $p^{k-1}S(p^{l-k}, a)$ при $l > k$.

Лемма 4.5. *Если* $(q, r) = (qr, a) = 1$, *то*

$$S(qr, a) = S(q, ar^{k-1})S(r, aq^{k-1}).$$

Доказательство см. лемму 2.10.

Теорема 4.2. *Пусть* $(q, a) = 1$. *Тогда*

$$S(q, a) \ll q^{1-1/k}.$$

Доказательство. Если $k = 2$, то

$$|S(q, a)|^2 = \sum_{x=1}^{q} \sum_{y=1}^{q} e(a(y^2 - x^2)/q) =$$

$$= \sum_{x=1}^{q} \sum_{z=1}^{q} e(a(z + 2x) z/q) = q \sum_{\substack{z=1 \\ q \setminus 2z}}^{q} e(az^2/q) \leqslant 2q.$$

Следовательно, можно предполагать, что $k > 2$. Запишем $l = uk + v$ с $1 \leqslant v \leqslant k$, $u \geqslant 0$ и предположим, что $p \nmid a$. Согласно лемме 4 4 и утверждению (4.20),

$$S(p^l, a) = p^{(k-1)u}S(p^v, a). \tag{4.21}$$

Рассмотрим сначала случай $v > 1$. Если $p > k$, то $\gamma = 1$, так что по лемме 4.4

$$S(p^v, a) = p^{v-1}.$$

Если $p \leqslant k$, то тривиально выполняется неравенство

$$|S(p^v, a)| \leqslant kp^{v-1}.$$

Следовательно, по (4.21)

$$|S(p^l, a)| \leqslant \begin{cases} p^{l-l/k} & (p > k), \\ kp^{l-l/k} & (p \leqslant k). \end{cases} \tag{4.22}$$

Рассмотрим теперь случай $v = 1$. По лемме 4.3

$$|S(p^v, a)| \leqslant kp^{1/2} \leqslant kp^{-1/6}p^{1-1/k}.$$

Таким образом, в соответствии с (4.21)

$$|S(p^l, a)| \leqslant \begin{cases} p^{l-l/k} & (p > k^6), \\ kp^{l-l/k} & (p \leqslant k^6). \end{cases} \tag{4.23}$$

Согласно (4.22), (4.23) и лемме 4.5,

$$|S(q, a)| \leqslant q^{1-1/k} \prod_{p \leqslant k^6} k,$$

откуда следует теорема.

Лемма 4.6. *Предположим, что* $(q, a) = 1$. *Тогда*

$$V\left(\frac{a}{q} + \beta,\ q,\ a\right) \ll \left(q^{-1} \min\left(n,\ \|\beta\|^{-1}\right)\right)^{1/k}.$$

Доказательство. Лемма непосредственно следует из (4.12), теоремы 4.2 и леммы 2.8.

4.3 Особый ряд

Для любого целого h положим

$$S_h(q) = \sum_{\substack{a=1 \\ (q,\ a)=1}}^{q} \left(S(q,\ a)\, q^{-1}\right)^s e(-ah/q). \tag{4.24}$$

Тогда в обозначениях (2.16) и (2.18)

$$S(q) = S_n(q), \qquad \mathfrak{S}(n) = \sum_{q=1}^{\infty} S_n(q). \tag{4.25}$$

Лемма 4.7. *Пусть* $s \geqslant 1$ *и* $l = uk + v$ *с* $1 \leqslant v \leqslant k$. *Тогда*

$$p^{us} S_h(p^l) \ll \begin{cases} p^{-s/2}\left(p^{1/2}(p^{l-1},\ h) + (p^l,\ h)\right), & \text{если} \quad l \equiv 1 \pmod k, \\ p^{-s}(p^l,\ h), & \text{если} \quad l \not\equiv 1 \pmod k. \end{cases}$$

Более того, если $\lambda = l - \max(k, \gamma)$ *удовлетворяет условиям* $\lambda > 0$ *и* $p^{\lambda} \nmid h$, *то*

$$S_h(p^l) = 0.$$

Доказательство. Пусть сначала $p > k$, так что $\gamma = 1$. Положим $l = uk + v$ с $1 \leqslant v \leqslant k$. Тогда по лемме 4.4

$$p^{ls} S_h(p^l) = \left(p^{u(k-1)}\right)^s \sum_{\substack{a=1 \\ p \nmid a}}^{p^l} S(p^v,\ a)^s e(-ahp^{-l}). \tag{4.26}$$

Каждое a может быть записано единственным образом в виде $a = xp^v + y$ с $0 \leqslant x < p^{l-v}$, $1 \leqslant y \leqslant p^v$, $p \nmid y$. Сумма по x равна 0, если $p^{l-v} \nmid h$, а в противном случае она равна p^{l-v}. В последнем случае сумма по y при $v > 1$ по лемме 4.4 равна

$$p^{s(v-1)} \sum_{\substack{y=1 \\ p \nmid y}}^{p^v} e(-yhp^{-l}),$$

и по модулю это не превышает $p^{s(v-1)}(p^v, hp^{v-l})$. Таким образом,

$$|S_h(p^l)| \leqslant p^{-us-s}(p^l,\ h) \qquad (l \not\equiv 1 \pmod k).$$

С другой стороны, когда $v=1$, сумма по y, согласно лемме 4.3, есть

$$\sum_{\chi_1 \in \mathcal{A}} \cdots \sum_{\chi_s \in \mathcal{A}} \tau(\chi_1) \ldots \tau(\chi_s) \sum_{y=1}^{p} \bar{\chi}_1 \ldots \bar{\chi}_s(y)\, e(-yhp^{-l}).$$

Когда $\chi_1 \cdots \chi_s$ — неглавный характер, предыдущая сумма по y равна

$$\chi_1 \ldots \chi_s(hp^{1-l})\, \tau(\bar{\chi}_1 \ldots \bar{\chi}_s);$$

а когда $\chi_1 \cdots \chi_s$ — главный характер, она равна -1 при $p^l \nmid h$ и $p-1$, если $p^l \mid h$. Отсюда по лемме 4.3

$$S_h(p^l) \ll p^{-us-s/2}(p^{1/2}(p^{l-1}, h) + (p^l, h)),$$

что и требовалось доказать.

Предположим теперь, что $p \leqslant k$. Когда $l \leqslant \max(\gamma, k)$, утверждение получается тривиально. Следовательно, можно считать, что $l > \max(\gamma, k)$. Запишем $l = uk + v$ с $\max(\gamma, k) - k < v \leqslant \max(\gamma, k)$. Тогда по лемме 4.4 равенство (4.26) имеет место. Более того, как и раньше, $S_h(p^l) = 0$, если $p^{l-v} \nmid h$; в противном случае

$$p^{ls} S_h(p^l) = p^{us(k-1)} p^{l-v} \sum_{\substack{y=1 \\ p \nmid y}}^{p^v} S(p^v, y)^s e(-yhp^{-l}) \ll p^{us(k-1)}(p^l, h),$$

так как $p \leqslant k$. Таким образом,

$$S_h(p^l) \ll p^{-us-vs}(p^l, h),$$

что является более сильным результатом, чем требовалось.

Теорема 4.3. *Пусть $s \geqslant 4$. Тогда ряд*

$$\mathfrak{S}(n) = \sum_{q=1}^{\infty} S_n(q)$$

абсолютно сходится и $\mathfrak{S}(n) \geqslant 0$. Кроме того, когда $s \geqslant \max(5, k+2)$, имеем $\mathfrak{S}(n) \ll 1$, а при $\max(4, k) \leqslant s < \max(5, k+2)$ имеем $\mathfrak{S}(n) \ll n^{\varepsilon}$.

Доказательство. Согласно лемме 2.11 и соотношениям (4.25), $S_n(q)$ — мультипликативная функция q. По лемме 4.7

$$\sum_{l=1}^{\infty} |S_n(p^l)| \ll np^{-(s-1)/2} \ll np^{-3/2}.$$

Отсюда

$$\sum_{q \leqslant Q} |S_n(q)| \leqslant \prod_{p \leqslant Q} (1 + C_1 p^{-3/2})^n \leqslant C_2^n,$$

где C_1 и C_2 зависят только от k и s. Это доказывает абсолютную сходимость ряда $\mathfrak{S}(n)$. Неотрицательность $\mathfrak{S}(n)$ следует из леммы 2.12.

Пусть p^θ означает наивысшую степень p, делящую n, и пусть $l = ku + v$ с $1 \leqslant v \leqslant k$. Тогда, по лемме 4.7,

$$\left.\begin{aligned} S_n(p^l) &\ll p^\omega, &&\text{если} \quad l \leqslant \theta + \max(k, \gamma), \\ S_n(p^l) &= 0, &&\text{если} \quad l > \theta + \max(k, \gamma), \end{aligned}\right\}, \tag{4.27}$$

где

$$\omega + us - \min(l, \theta) = \begin{cases} -\frac{1}{2}s, & \text{если} \quad l \leqslant \theta \text{ и } v = 1, \\ -\frac{1}{2}(s-1), & \text{если} \quad l > \theta \text{ и } v = 1, \\ -s, & \text{если} \quad v \neq 1. \end{cases} \tag{4.28}$$

Таким образом, ряд

$$\sum_{l=1}^{\infty} |S_n(p^l)|$$

есть $O(p^{-3/2})$, если $\theta = 0$ или $\theta \geqslant 1$ и $s \geqslant \max(5, k+2)$, и $O(\theta)$, когда $\theta \geqslant 1$ и $s \geqslant \max(4, k)$. Следовательно, в первом случае $\mathfrak{S}(n) \ll 1$, а в последнем — $\mathfrak{S}(n) \ll d(n)^C$, где C зависит только от s и k. Отсюда следует результат.

Лемма 4.8. *Если* $s \geqslant \max(4, k+1)$, *то*

$$\sum_{q \leqslant Q} q^{1/k} |S_n(q)| \ll (nQ)^\varepsilon.$$

Доказательство. Согласно (4.27) и (4.28), $(p^l)^{1/k} S_n(p^l)$ есть $O(\theta)$, $O(p^{-1})$ или 0 в зависимости от того, что $l \leqslant \theta$, $\theta < l \leqslant \theta + \max(k, \gamma)$ или $l > \theta + \max(k, \gamma)$. Отсюда

$$\sum_{q \leqslant Q} q^{1/k} |S_n(q)| \leqslant \prod_{p \leqslant Q} \left(1 + \sum_{l=1}^{\infty} (p^l)^{1/k} |S_n(p^l)|\right) \leqslant$$
$$\leqslant d(n)^C \prod_{p \leqslant Q} (1 + c/p),$$

где C зависит только от s и k.

4.4 Вклад больших дуг

Пусть n — большое натуральное число,

$$N = [n^{1/k}], \tag{4.29}$$

$$P = N/(2k), \tag{4.30}$$

$$\mathfrak{M}(q, a) = \{\alpha\colon\ |\alpha - a/q| \leqslant Pq^{-1}n^{-1}\}, \tag{4.31}$$

$\mathfrak{M}$ — объединение $\mathfrak{M}(q, a)$ с $1 \leqslant a \leqslant q \leqslant P$ и $(a, q) = 1$. Тогда $\mathfrak{M}(q, a)$ попарно не пересекаются и лежат в промежутке

$$\mathcal{U} = (Pn^{-1},\ 1 + Pn^{-1}]. \tag{4.32}$$

Пусть

$$R_{\mathfrak{M}}(m) = \int\limits_{\mathfrak{M}} f(\alpha)^s e(-\alpha m)\, d\alpha. \tag{4.33}$$

Лемма 4.9. *Предположим, что $t \geqslant \max(4, k)$ и что $\lambda = 0$ при $t \geqslant k + 1$ и $\lambda = 1/k$, когда $t = k$. Пусть*

$$S_t^*(q) = \sum_{\substack{a=1 \\ (a,\ q)=1}}^{q} |S(q,\ a)\, q^{-1}|^t. \tag{4.34}$$

Тогда
$$\sum_{q \leqslant Q} q^{-\lambda} S_t^*(q) \ll Q^{\varepsilon}.$$

Доказательство. Действуя так же, как для $S_n(q)$, в обозначениях леммы 4.7, можно показать, что $S_t^*(q)$ мультипликативна и $p^{ut-l} S_t^*(p^l)$ есть $O(p^{-t/2})$ при $l \equiv 1 \pmod k$ и $O(p^{-t})$ при $l \not\equiv 1 \pmod k$. Таким образом,

$$\sum_{q \leqslant Q} q^{-\lambda} S_t^*(q) \leqslant \prod_{p \leqslant Q} \left(1 + \sum_{l=1}^{\infty} p^{-\lambda l} S_t^*(p^l)\right)$$

и

$$\sum_{l=1}^{\infty} p^{-\lambda l} S_t^*(p^l) \ll \sum_{u=0}^{\infty} p^{-u\lambda k + uk - ut} \left(p^{1-\lambda-t/2} + \sum_{v=2}^{k} p^{-v\lambda - v - t}\right) \ll$$
$$\ll p^{-1}$$

при условии, что $\lambda \geqslant \max\left((1 + k - t)/k,\ 2 - \frac{1}{2} t\right)$

Теорема 4.4. *При $s \geqslant \max(5, k + 1)$ существует положительное число δ, такое, что каково бы ни было $1 \leqslant m \leqslant n$,*

$$R_{\mathfrak{M}}(m) = \Gamma\left(1 + \frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} m^{s/k - 1} \mathfrak{S}(m) + O(n^{s/k - 1 - \delta}).$$

Доказательство. Пусть $\alpha \in \mathfrak{M}(q, a)$. Тогда по теореме 4.1, (4.29), (4.30) и (4.31),

$$f(\alpha) - V(\alpha, q, a) \ll q^{1/2 + \varepsilon}.$$

Следовательно,

$$f(\alpha)^s - V(\alpha, q, a)^s \ll (q^{1/2+\varepsilon})^s + q^{1/2+\varepsilon} |V(\alpha, q, a)|^{s-1},$$

Отсюда в обозначениях (4.12), (4.31) и (4.34)

$$\sum_{\substack{a=1\\(a,\ q)=1}}^{q} \int\limits_{\mathfrak{M}(q,\ a)} (f(\alpha)^s - V(\alpha,\ q,\ a)^s)\, e(-\alpha m)\, d\alpha \ll$$

$$\ll Pn^{-1}\left(q^{1/2+\varepsilon}\right)^s + q^{1/2+\varepsilon} S^*_{s-1}(q) \int\limits_{-1/2}^{1/2} |v(\beta)|^{s-1}\, d\beta.$$

Следовательно, согласно (4.33) и лемме 2.8,

$$R_{\mathfrak{M}}(m) = \sum_{q\leqslant P} \sum_{\substack{a=1\\(a,\ q)=1}}^{q} \int\limits_{\mathfrak{M}(q,\ a)} V(\alpha,\ q,\ a)^s e(-\alpha m)\, d\alpha + E, \tag{4.35}$$

где, принимая во внимание возможность $s = k + 1$,

$$E \ll P^2 n^{-1}\left(P^{1/2+\varepsilon}\right)^s + P^{3/4+\varepsilon} \sum_{q\leqslant P} q^{-1/4} S^*_{s-1}(q)\, n^{(s-1)/k-1+\varepsilon}.$$

В силу леммы 4.9, (4.29) и (4.30)

$$E \ll n^{s/k-1-\delta} \tag{4.36}$$

для подходящего положительного числа δ.

Пусть $\mathfrak{N}(q,\ a) = \left\{\alpha\colon P/(qn) < |\alpha - a/q| \leqslant \frac{1}{2}\right\}$. Тогда из равенств (4.12), (4.24) и леммы 2.8

$$\sum_{\substack{a=1\\(a,\ q)=1}}^{q} \int\limits_{\mathfrak{N}(q,a)} V(\alpha,\ q,\ a)^s e(-\alpha m)\, d\alpha \ll |S_m(q)| \int\limits_{P/(nq)}^{\infty} \beta^{-s/k}\, d\beta \ll$$

$$\ll (nq/P)^{s/k-1} |S_m(q)|.$$

Следовательно, по лемме 4.8

$$\sum_{q\leqslant P} \sum_{\substack{a=1\\(a,\ q)=1}}^{q} \int\limits_{\mathfrak{N}(q,\ a)} V(\alpha,\ q,\ a)^s e(-\alpha m)\, d\alpha \ll n^{s/k-1-\delta}.$$

Отсюда по (4.35), (4.36) и (4.24)

$$R_{\mathfrak{M}}(m) = \mathfrak{S}(m,\ P)\, I(m) + O\left(n^{s/k-1-\delta}\right), \tag{4.37}$$

где

$$\mathfrak{S}(m,\ P) = \sum_{q\leqslant P} S_m(q), \qquad I(m) = \int\limits_{-1/2}^{1/2} v(\beta)^s e(-\beta m)\, d\beta.$$

По лемме 4.8

$$\sum_{Q<q\leqslant 2Q} |S_m(q)| \ll n^{\varepsilon} Q^{\varepsilon-1/k}.$$

Отсюда, согласно (4.29) и (4.30),

$$\sum_{q>P} |S_m(q)| \ll n^{-\delta},$$

так что по (4.25)

$$\mathfrak{S}(m, P) = \mathfrak{S}(m) + O(n^{-\delta}). \tag{4.38}$$

Наконец, из (4.11), (2.20) и теоремы 2.3 для $1 \leqslant m \leqslant n$

$$I(m) = J(m) = \Gamma\left(1 + \frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} m^{s/k-1} (1 + O(m^{-1/k})).$$

Теорема следует теперь из теоремы 4.3, (4.37) и (4.38).

4.5 Согласование условий

Пусть $M_n(q)$ и $M_n^*(q)$ такие же, как в § 2.6.

Теорема 4.5. *Предположим, что* $s \geqslant \max(4, k+1)$ *и* $M_n^*(p^\gamma) > 0$ *для каждого простого числа* p. *Тогда* $\mathfrak{S}(n) \gg 1$.

Доказательство. Согласно леммам 2.12 и 2.13,

$$\sum_{h=0}^{\infty} S_n(p^h) \geqslant p^{\gamma(1-s)},$$

причем абсолютная сходимость ряда обеспечивается абсолютной сходимостью $\mathfrak{S}(n)$ (ср. с теоремой 4.3).

Теперь достаточно показать, что при $p > k$

$$\sum_{l=1}^{\infty} S_n(p^l) \geqslant -Cp^{-3/2}. \tag{4.39}$$

Заметим, что $\gamma = 1$. Рассуждения из леммы 4.7 показывают, что если $l = uk + v$ с $2 \leqslant v \leqslant k$, то

$$p^{(u+1)s-l} S_n(p^l) = 1 - \frac{1}{p}, \quad -\frac{1}{p}, \ 0$$

$$\text{соответственно, если } p^l \mid n, \ p^{l-1} \| n, \ p^{l-1} \nmid n, \tag{4.40}$$

и что если $l \equiv 1 \pmod k$, то $S_n(p^l) = 0$ для $p^{l-1} \nmid n$; в противном случае

$$p^{-[l/k](k-s)} S_n(p^l) =$$

$$= p^{-s} \sum_{\chi_1 \in \mathcal{A}} \ldots \sum_{\chi_s \in \mathcal{A}} \tau(\chi_1) \ldots \tau(\chi_s) \sum_{a=1}^{p-1} \bar{\chi}_1 \ldots \bar{\chi}_s(a) e(-anp^{-l}). \tag{4.41}$$

Выберем θ так, чтобы $p^\theta \| n$. Тогда, по (4.40),

$$\sum_{l \not\equiv 1 \pmod K} S_n(p^l) \geqslant -p^\lambda,$$

где $\lambda = [\theta/k](k-s)+1-s$. Легко видеть, что $\lambda \leqslant -2$.

Согласно лемме 4.3, члены в (4.41) с $\chi_1 \ldots \chi_s \neq \chi_0$ оцениваются как $\ll p^{(s+1)/2}$, а если $p \nmid np^{l-1}$, то члены с $\chi_1 \ldots \chi_s = \chi_0$ дают $\ll p^{s/2}$. Следовательно,

$$\sum_{l \equiv 1 \pmod k} S_n(p^l) = \sum_{\substack{l \equiv 1 \pmod k \\ p^l \mid n}} S_n(p^l) + O(p^{-3/2}).$$

Если $s \geqslant 5$, то по лемме 4.3 и (4.41)

$$S_n(p^l) \ll p^{[l/k](k-s)-3/2},$$

так что

$$\sum_{\substack{l \equiv 1 \pmod k \\ p^l \mid n}} S_n(p^l) \ll p^{-3/2}.$$

Таким образом, остается рассмотреть $S_n(p^l)$, когда $p^l \mid n$ и $s = 4$.

Согласно (4.41),

$$p^{-[l/k](k-s)} S_n(p^l) = S_{np^{1-l}}(p) = S_p(p).$$

Следовательно, достаточно показать, что $S_p(p) \geqslant 0$.

В силу (4.24)

$$S_p(p) = \sum_{a=1}^{p-1} (S(p, a)\,p^{-1})^4.$$

Мы завершим доказательство, если покажем, что при $k=2$ или 3 и $p > k$ $S(p, a)$ является действительным или чисто мнимым числом. Заметим, что при $s = 4$ имеем $k = 2$ или 3.

При $k = 2$ лемма 4.3 дает

$$S(p, a) = \chi(a)\tau(\chi),$$

где χ — символ Лежандра. Таким образом,

$$\bar{S}(p, a) = S(p, -a) = \chi(-a)\tau(\chi) = \chi(-1) S(p, a),$$

так что $S(p, a)$ — действительное или чисто мнимое число в зависимости от того, $\chi(-1) = 1$ или $\chi(-1) = -1$.

При $k = 3$ имеем $(-x)^k = -x^k$. Отсюда

$$\bar{S}(p, a) = S(p, -a) = S(p, a),$$

так что $S(p, a)$ — действительное.

Теорема 4.6. *Предположим, что $s \geqslant 5$ при $k = 2$, $s \geqslant 4k$, если k является степенью 2 с $k > 2$, и $s \geqslant \frac{3}{2}k$ в остальных случаях. Тогда $\mathfrak{S}(n) \gg 1$.*

Доказательство. Эта теорема сразу следует из леммы 2.15 и теоремы 4.5.

4.6 Упражнения

1. Покажите, что (4.13) имеет место с заменой левой части на $q^{1/2+\varepsilon}(1+n|\beta|)^{1/2}$. Выведите частный случай $\varphi(x)=\alpha x^3$ леммы 2.4 (неравенство Вейля).
2. Рассмотрите утверждения:
   (i) $s\geqslant 4$ и $\mathfrak{S}(n)\gg 1$,
   (ii) $M_n(q)>0$ для любого n и для каждого большого q,
   (iii) $M_n^*(q)>0$ для любого n и для каждого большого q.

   Покажите, что если (i) имеет место для любого n, то (ii) справедливо, и что если $k\neq 2$ или 4, тогда из (ii) следует (iii).
3. Предположим, что $s_0(k)$ дается следующей таблицей:

k	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$s_0(k)$	4	16	5	9	4	32	13	12	11	16	6	4	15	64

Покажите, что для $s\geqslant s_0(k)$ $\mathfrak{S}(n)\gg 1$ для любого n.

5
Методы Виноградова

5.1 Теорема Виноградова о среднем

Когда k мало, т. е. меньше 11 или 12 или около того, наилучшими известными являются леммы 2.4 и 2.5, дающие основной вклад в оценки малых дуг в гл. 2. Однако для больших k можно получить весьма значительные улучшения при помощи теоремы И. М. Виноградова о среднем. Эта теорема важна также в теории дзета-функции Римана.

Для ее описания надо ввести некоторые обозначения. Пусть $\mathcal{U}_k$ означает k-мерный единичный гиперкуб $(0, 1]^k$,

$$f(\alpha) = \sum_{Y < x \leqslant Y + X} e(\alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_k x^k). \tag{5.1}$$

Для любого k-мерного вектора $\mathbf{h} = (h_1, \ldots, h_k)$ с целыми компонентами h_j пусть $J_s^{(k)}(X, Y, \mathbf{h})$ обозначает число решений системы k уравнений

$$\sum_{r=1}^{s} (x_r^j - y_r^j) = h_j \, (1 \leqslant j \leqslant k) \quad \text{с} \quad Y < x_r, \ y_r \leqslant Y + X. \tag{5.2}$$

Тогда

$$J_s^{(k)}(X, Y, \mathbf{h}) = \int_{\mathcal{U}_k} |f(\alpha)|^{2s} e(\alpha \cdot \mathbf{h}) \, d\alpha, \tag{5.3}$$

где $\alpha \cdot \mathbf{h}$ — скалярное произведение $\alpha_1 h_1 + \ldots + \alpha_k h_k$. Очевидно следующее неравенство

$$J_s^{(k)}(X, Y, \mathbf{h}) \leqslant J_s^{(k)}(X, Y, \mathbf{0}). \tag{5.4}$$

Полагая $x_r = M + u_r$, $y_r = M + v_r$ и применяя биномиальную теорему, легко видеть, что

$$J_s^{(k)}(N, M, \mathbf{0}) = J_s^{(k)}(N, 0, \mathbf{0}). \tag{5.5}$$

Для краткости пишем

$$J_s(X) = J_s^{(k)}(X) = J_s^{(k)}(X, 0, \mathbf{0}). \tag{5.6}$$

Согласно (5.2), $J_s(X)$ есть число решений системы

$$\sum_{r=1}^{s} (x_r^j - y_r^j) = 0 \ (1 \leqslant j \leqslant k) \quad \text{с} \quad 0 < x_r, \ y_r \leqslant X. \tag{5.7}$$

Нетривиальная оценка для $J_s(X)$ известна как «теорема Виноградова о среднем» [1]

Все известные методы оценки $J_s(X)$, когда k велико, основаны на редукции $J_s(X)$ к $J_{s-k}(X/p)$, где p — подходящее простое число [2]. Метод, принятый здесь, является вариантом Бомбьери метода А. А. Карацубы.

Лемма 5.1. (Линник, 1943 с). *Предположим, что p — простое число, $p > k$. Пусть $A(p, \mathfrak{h})$ означает число решений системы k сравнений*

$$\sum_{r=1}^{k} n_r^j \equiv h_j \pmod{p^j} \quad (1 \leqslant j \leqslant k)$$

с $n_r \leqslant p^k$ и n_r, несравнимыми по модулю p. Тогда [3]

$$A(p, \mathfrak{h}) \leqslant k! p^{k(k-1)/2}.$$

Доказательство. Пусть $B(\mathbf{g})$ — число решений системы

$$\sum_{r=1}^{k} n_r^j \equiv g_j \pmod{p^k} \quad (1 \leqslant j \leqslant k) \tag{5.8}$$

с $n_r \leqslant p^k$ и несравнимыми по модулю p. Тогда $A(p, \mathfrak{h})$ есть сумма всех $B(\mathbf{g})$ с $g_j \equiv h_j \pmod{p^j}$ и $1 \leqslant g_j \leqslant p^k$ $(1 \leqslant j \leqslant k)$. Общее число возможных вариантов $\mathbf{g}$ равно $p^{k(k-1)/2}$. Таким образом, достаточно показать, что

$$B(\mathbf{g}) \leqslant k!,$$

а это будет следовать из того, что каждое решение системы (5.8) является перестановкой какого-либо данного решения.

Для заданного $\mathbf{g}$ пусть $n_1, \ldots, n_k$ — решение сравнения (5.8), $n_r \leqslant p^k$ и n_r несравнимы по модулю p. Предположим, что $m_1, \ldots, m_k$ — другое такое решение, и пусть

$$P(x) = \prod_{r=1}^{k} (x - n_r). \tag{5.9}$$

Тогда из формулы Ньютона, связывающей суммы степеней корней многочлена с его коэффициентами, и условия $p > k$ следует, что

$$P(x) \equiv \prod_{r=1}^{k} (x - m_r) \pmod{p^k}.$$

Таким образом,

$$P(m_r) \equiv 0 \pmod{p^k} \quad (1 \leqslant r \leqslant k). \tag{5.10}$$

Таким образом, для каждого r найдется s, такое, что $n_s \equiv m_r \pmod{p}$. Кроме того, поскольку n_s несравнимы по модулю p, n_s единственно. Следовательно, ввиду равенств (5.9) и (5.10) $n_s \equiv m_r \pmod{p^k}$, откуда $n_s = m_r$. Таким образом, m_r являются перестановкой n_r, что и требовалось.

Пусть p — простое число, пусть $R_1(\mathbf{h})$ — число решений системы уравнений

$$\sum_{r=1}^{s} x_r^j = h_j \quad (1 \leqslant j \leqslant k),$$

где $0 < x_r \leqslant X$ и по крайней мере k из x_r несравнимы по модулю p, и пусть $R_2(\mathbf{h})$ — соответствующее число с не более чем $k-1$ из x_r несравнимыми по модулю p. Тогда

$$J_s(X) = \sum_{\mathbf{h}} (R_1(\mathbf{h}) + R_2(\mathbf{h}))^2 \leqslant 2 \sum_{\mathbf{h}} (R_1(\mathbf{h})^2 + R_2(\mathbf{h})^2).$$

Отсюда

$$J_s(X) \leqslant 2I_1(p) + 2I_2(p), \tag{5.11}$$

где $I_1(p)$ — число решений системы (5.7) с по крайней мере k из x_r несравнимыми по модулю p и по крайней мере k из y_r несравнимыми по модулю p, а $I_2(p)$ — число решений (5.7), в которых ни среди x_r, ни среди y_r нет более чем $k-1$ несравнимых по модулю p величин.

Решения системы (5.7), подсчитываемые $I_1(p)$, характеризуются тем, что в них $x_1, \ldots, x_k$ несравнимы по модулю p и $y_1, \ldots, y_k$ несравнимы по модулю p. Поэтому, обозначая I_3 число таких решений, немедленно получаем, что

$$I_1(p) \leqslant \binom{s}{k}^2 I_3. \tag{5.12}$$

Пусть

$$f(\alpha, y) = \sum_{\substack{0 < x \leqslant X \\ x \equiv y \pmod{p}}} e(\alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_k x^k),$$

и пусть $\mathscr{A}$ означает множество k-мерных векторов $\mathbf{a} = (a_1, \ldots$ $\ldots, a_k)$, где $0 < a_r \leqslant p$ и a_r несравнимы $\bmod p$. Тогда

$$I_3 = \int_{\mathscr{U}_k} \Big| \sum_{x \leqslant p} f(\alpha, x) \Big|^{2s-2k} \Big| \sum_{\mathbf{a} \in \mathscr{A}} f(\alpha, a_1) \ldots f(\alpha, a_k) \Big|^2 d\alpha.$$

По неравенству Гельдера

$$\Big| \sum_{x \leqslant p} f(\alpha, x) \Big|^{2s-2k} \leqslant p^{2s-2k-1} \sum_{x \leqslant p} |f(\alpha, x)|^{2s-2k}.$$

Следовательно,

$$I_3 \leqslant p^{2s-2k} \max_{x \leqslant p} I_4(x), \tag{5.13}$$

где $I_4(x)$ — число решений системы уравнений

$$\sum_{r=1}^{k} (m_r^j - n_r^j) = \sum_{r=1}^{s-k} ((py_r + x)^j - (pz_r + x)^j) \quad (1 \leqslant j \leqslant k)$$

с $0 < m_r,\ n_r \leqslant X,\ -x/p < y_r,\ z_r \leqslant (X-x)/p$ с $m_1, \ldots, m_k$, несравнимыми по модулю p, и с $n_1, \ldots, n_k$, несравнимыми по модулю p. Простое применение биномиальной теоремы показывает, что $I_4(x)$ является числом решений системы уравнений

$$\sum_{r=1}^{k}\left((m_r-x)^j-(n_r-x)^j\right)=\sum_{r=1}^{s-k} p^j\left(y_r^j-z_r^j\right) \quad (1 \leqslant j \leqslant k)$$

с переменными, удовлетворяющими тем же условиям, что и прежде.

Предположим теперь, что

$$p^k \geqslant X, \quad p > k. \tag{5.14}$$

Тогда, согласно лемме 5.1 и формулам (5.4), (5.5) и (5.6),

$$I_4(x) \leqslant X^k k!\, p^{k(k-1)/2} \max_h J_{s-k}^{(k)}(X/p, -x/p,\ \mathbf{h}) \leqslant$$
$$\leqslant X^k k!\, p^{k(k-1)/2} J_{s-k}(1+Xp^{-1}).$$

Это вместе с (5.11), (5.12) и (5.13) дает

$$J_s(X) \leqslant 2I_2(p)+2\binom{s}{k} k!\, p^{2s+k(k-5)/2} X^k J_{s-k}(1+Xp^{-1}). \tag{5.15}$$

Лемма 5.2. (Бомбьери). *Пусть $\lambda > 0$, и пусть, $\mathscr{B}_1, \ldots, \mathscr{B}_s$ означают s подмножеств конечного множества $\mathscr{B}$,*

$$\operatorname{card}\mathscr{B}_r \geqslant \lambda \operatorname{card}\mathscr{B} \quad (1 \leqslant r \leqslant s).$$

Тогда для любого $t < \lambda s$ существуют $r_1, \ldots, r_t$, такие, что $r_1 < r_2 < \ldots < r_t$ и

$$\operatorname{card}(\mathscr{B}_{r_1} \cap \mathscr{B}_{r_2} \cap \ldots \cap \mathscr{B}_{r_t}) \geqslant \left(\lambda-\frac{t}{s}\right)\binom{s}{t}^{-1} \operatorname{card}\mathscr{B}.$$

Доказательство. Пусть $\mathscr{C}$ обозначает множество элементов b из $\mathscr{B}$, которые принадлежат по крайней мере t из $\mathscr{B}_r$. Тогда

$$s\lambda \operatorname{card}\mathscr{B} \leqslant \sum_{r=1}^{s} \operatorname{card}\mathscr{B}_r \leqslant t \operatorname{card}\mathscr{B}+s \operatorname{card}\mathscr{C},$$

откуда

$$\operatorname{card}\mathscr{C} \geqslant \left(\lambda-\frac{t}{s}\right) \operatorname{card}\mathscr{B}.$$

Более того,

$$\operatorname{card}\mathscr{C} \leqslant \sum_{\substack{r_1, \ldots, r_t \\ r_1<r_2<\ldots<r_t}} \operatorname{card}(\mathscr{B}_{r_1} \cap \mathscr{B}_{r_2} \cap \ldots \cap \mathscr{B}_{r_t}),$$

а количество членов в кратной сумме равно $\binom{s}{k}$. Если выбрать $r_1, \ldots, r_t$, чтобы они соответствовали максимальному члену, то получим утверждение леммы.

Теорема 5.1 (теорема Виноградова о среднем). *Для любой пары натуральных чисел k, l существует положительное число $C(k, l)$, такое, что для каждого $X > 0$*

$$J_{lk}^{(k)}(X) \leqslant C(k, l) X^{2lk - k(k+1)/2+\eta},$$

где $\eta = \frac{1}{2} k^2 (1 - 1/k)^l$.

Следует отметить, что для применений в мультипликативной теории чисел существенно и поведение $C(k, l)$, когда k и l растут [4]. Здесь, однако, это менее важно. Заметим, что при $k = 1$ теорема тривиальна.

Доказательство. Индукция по l. Рассуждениями, подобными тем, что использовались при оценке $B(\mathbf{g})$ в доказательстве леммы 5.1, можно показать, что когда $s = k$, все решения (5.7) получаются с y_r, являющимися перестановками x_r [5]. Таким образом,

$$J_k(X) \leqslant k! X^k,$$

что сразу дает случай $l = 1$.

Предположим теперь, что $l > 1$ и теорема справедлива при замене l на $l - 1$. Когда $X \leqslant k^k$, искомое утверждение тривиально. Таким образом, можно считать, что $X > k^k$. Пусть p — простое число, $X^{1/k} \leqslant p \leqslant 2^{5k} X^{1/k}$, так что условия (5.14) имеют место. Тогда в силу (5.15) и предположения индукции

$$J_{kl}(X) \leqslant 2I_2(p) + C_1(k, l) p^{2kl + k(k-5)/2} (X/p)^{2kl - k(k+5)/2+\eta'} X^k,$$

где $\eta' = \frac{1}{2} k^2 (1 - 1/k)^{l-1}$. Показатель степени p здесь равен $k^2 - \eta'$, так что

$$J_{kl}(X) \leqslant 2I_2(p) + C_2(k, l) X^{2kl - k(k+1)/2+\eta}.$$

Теперь доказательство разбивается на два случая. Первый случай имеет место, когда существует по крайней мере одно простое число p в интервале $X^{1/k} \leqslant p \leqslant 2^{5k} X^{1/k}$, для которого

$$I_2(p) \leqslant \frac{1}{4} J_{kl}(X).$$

Тогда теорема следует сразу.

Второй случай — противоположность первому, — когда не существует таких простых. Тогда, согласно постулату Бертрана, имеется по крайней мере $5k$ простых $p_1, \ldots, p_{5k}$, таких, что

$$I_2(p_r) > \frac{1}{4} J_{kl}(X) \tag{5.16}$$

и

$$X^{1/k} \leqslant p_r \leqslant 2^{5k} X^{1/k}. \tag{5.17}$$

Пусть $\mathscr{B}$ означает множество решений системы (5.7) с $s = kl$. Тогда

$$\operatorname{card}\mathscr{B} = J_{kl}(X).$$

Пусть $\mathscr{B}(p)$ — подмножество $\mathscr{B}$, содержащее решения, в которых ни среди x_r, ни среди y_r нет более чем $k-1$ несравнимых по модулю p величин. Тогда

$$\operatorname{card}\mathscr{B}(p_r) = I_2(p_r).$$

Таким образом, ввиду (5.16) и леммы 5.2 с $\lambda = \frac{1}{4}$, $s = 5k$, $t = k$, имеется k различных простых $q_1, \ldots, q_k$, таких, что

$$J_{kl}(X) \leqslant 20\binom{5k}{k}\operatorname{card}(\mathscr{B}(q_1) \cap \mathscr{B}(q_2) \cap \ldots \cap \mathscr{B}(q_k)). \tag{5.18}$$

Рассмотрим теперь типичный элемент, принадлежащий $\mathscr{B}(q_1) \cap \cap \mathscr{B}(q_2) \cap \ldots \cap \mathscr{B}(q_r)$. Поскольку $x_r \leqslant X$ и $q_1 \ldots q_k \geqslant X$, каждое x_r единственным образом определяется своим классом вычетов по модулю q_1, модулю $q_2, \ldots$, модулю q_k. Более того, $x_1, \ldots, x_{kl}$ лежат, самое большее, в $k-1$ классах вычетов по модулю q_t. Таким образом, количество наборов для kl-мерного вектора $(x_1, \ldots, x_{kl})$ по модулю q_t не превышает $q_t^{k-1}(k-1)^{kl}$. Поэтому число наборов по модулю $q_1 \ldots q_k$ не больше $(q_1 \ldots q_k)^{k-1}(k-1)^{k^2 l}$. Аналогично для $(y_1, \ldots, y_{kl})$. Следовательно,

$$\operatorname{card}(\mathscr{B}(q_1) \cap \mathscr{B}(q_2) \cap \ldots \cap \mathscr{B}(q_k)) \leqslant (q_1 \ldots q_k)^{2k-2}(k-1)^{2k^2 l}.$$

Отсюда вследствие (5.18)

$$J_{kl}(X) \leqslant C_3(k, l)X^{2k-2}.$$

С другой стороны, тривиальных решений системы (5.7) с $s = kl$ при $l > 1$ в $J_{kl}(X)$ будет по крайней мере $[X]^{kl} \geqslant [X]^{2k}$. Таким образом, $X \leqslant C_4(k, l)$, что дает утверждение теоремы во втором случае.

5.2 Переход от среднего

Пусть

$$\mathbf{v}(x) = \mathbf{v}^{(k)}(x) = (x, x^2, \ldots, x^k), \tag{5.19}$$

и для $\boldsymbol{\alpha} \in \mathbb{R}^k$ положим

$$f(\boldsymbol{\alpha}) = \sum_{x=1}^{N} e(\mathbf{v}(x) \cdot \boldsymbol{\alpha}), \tag{5.20}$$

где, как обычно, для двух элементов $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ из $\mathbb{R}^k$, $\boldsymbol{\alpha} \cdot \boldsymbol{\beta}$ означает скалярное произведение $\alpha_1\beta_1 + \ldots + \alpha_k\beta_k$. Предположим, что $\mathscr{M}$ — непустое множество целых чисел,

$$\mathscr{M} \subset [1, N], \quad M = \operatorname{card}(\mathscr{M}). \tag{5.21}$$

Тогда для $m \in \mathcal{M}$

$$f(\alpha) = \sum_{x=1+m}^{N+m} e(\mathbf{v}(x-m)\cdot\alpha) =$$

$$= \int_0^1 \left(\sum_{x=1}^{2N} e(\mathbf{v}(x-m)\cdot\alpha + x\beta) \sum_{y=1+m}^{N+m} e(-y\beta)\right) d\beta.$$

Следовательно, суммированием по элементам $\mathcal{M}$ получаем

$$f(\alpha) \ll M^{-1} \int_0^1 \left(\left(\sum_{m\in\mathcal{M}} |g(m, \beta)|\right) \min(N, \|\beta\|^{-1})\right) d\beta,$$

где
$$g(m, \beta) = \sum_{x=1}^{2N} e(\mathbf{v}(x-m)\cdot\alpha + x\beta). \tag{5.22}$$

Таким образом,

$$f(\alpha) \ll M^{-1}(\log 2N) \sup_{0\leqslant\beta\leqslant1} \sum_{m\in\mathcal{M}} |g(m, \beta)|, \tag{5.23}$$

и оценка для f может быть выведена из подходящей теоремы о среднем.

Следующая лемма осуществляет связь между дискретными и соответствующими непрерывными средними величинами. Заметим, что

$$\sum_{\mathbf{n}\in\mathcal{N}} |a(\mathbf{n})|^2 = \int_{\mathcal{U}_k} |S(\boldsymbol{\beta})|^2 \, d\boldsymbol{\beta}.$$

Для получения таких связей изобретено много методов, но все они основаны на сходных идеях. Приведенный здесь метод основан на неравенстве большого решета и является его обобщением на k-мерный случай, полезный в алгебраической теории чисел (см. [Huxley, 1968] и [Wilson, 1969]).

Лемма 5.3. *Предположим, что* $\delta_j > 0$ $(j = 1, \ldots, l)$ *и что* Γ — *непустое множество точек* γ *в* $\mathbb{R}^l$, *таких, что открытые множества*

$$\mathcal{R}(\boldsymbol{\gamma}) = \{\boldsymbol{\beta}: \|\beta_j - \gamma_j\| < \delta_j, \ 0 \leqslant \beta_j < 1\}$$

попарно не пересекаются. Пусть $N_1, \ldots, N_l$ *обозначают* l *натуральных чисел, а* $\mathcal{N}$ — *множество целочисленных* l-*мерных векторов* $\mathbf{n} = (n_1, \ldots, n_l)$, $1 \leqslant n_j \leqslant N_j$. *Тогда для суммы*

$$S(\boldsymbol{\beta}) = \sum_{\mathbf{n}\in\mathcal{N}} a(\mathbf{n})\, e(\mathbf{n}\cdot\boldsymbol{\beta}),$$

где $a(\mathbf{n})$ — *комплексные числа, справедливо неравенство*

$$\sum_{\boldsymbol{\gamma}\in\Gamma} |S(\boldsymbol{\gamma})|^2 \ll \sum_{\mathbf{n}\in\mathcal{N}} |a(\mathbf{n})|^2 \prod_{j=1}^{l} (N_j + \delta_j^{-1}).$$

Доказательство. Без ограничения общности можно предполагать, что $0 \le \delta_j \le 1$. Достаточно оценить двойственную форму

$$\sum_{\mathbf{n}\in\mathcal{N}} |T(\mathbf{n})|^2,$$

где
$$T(\mathbf{n}) = \sum_{\gamma\in\Gamma} b(\gamma)\, e(\mathbf{n}\cdot\gamma).$$

Поскольку $1 - |h|/(2N) \geqslant \frac{1}{2}$ для $|h| \leqslant N$, то

$$2^{-l} \sum_{\mathbf{n}\in\mathcal{N}} |T(\mathbf{n})|^2 \leqslant \sum_{\substack{\mathbf{h} \\ |h_j| \leqslant 2N_j}} |T(\mathbf{h})|^2 \prod_{j=1}^{l} (1 - |h_j|/(2N_j)),$$

что после возведения в квадрат и изменения порядка суммирования принимает вид

$$\sum_{\gamma\in\Gamma}\sum_{\gamma'\in\Gamma} b(\gamma)\,\bar{b}(\gamma') \prod_{j=1}^{l} \left(\frac{1}{2N_j} \left| \sum_{n=1}^{2N_j} e(n(\gamma_j' - \gamma_j)) \right|^2 \right).$$

Внутренняя сумма здесь есть

$$\ll \min(N_j, \|\gamma_j' - \gamma_j\|^{-1}) \ll N_j/(1 + N_j \|\gamma_j' - \gamma_j\|).$$

Следовательно,

$$\sum_{\in\mathcal{N}} |T(\mathbf{n})|^2 \ll \sum_{\gamma\in\Gamma} |b(\gamma)|^2 \sum_{\gamma'\in\Gamma} \prod_{j=1}^{l} (N_j (1 + N_j \|\gamma_j' - \gamma_j\|)^{-2}). \quad (5.24)$$

Пусть $0 < \delta < 1$,

$$F(\beta, \delta) = N \quad \text{или} \quad N(1 + N\|\beta\|)^{-2}$$

при $\|\beta\| < \delta$ и $\|\beta\| \geqslant \delta$ соответственно и

$$I(\alpha, \delta) = \{\beta\colon \|\alpha - \beta\| < \delta,\ 0 \leqslant \beta \le 1\}.$$

Тогда достаточно доказать, что

$$F(\alpha, \delta) \ll \delta^{-1} \int_{I(\alpha,\delta)} F(\beta, \delta)\, d\beta, \qquad (5.25)$$

так как тогда из (5.24) следует, что

$$\sum_{\mathbf{n}\in\mathcal{N}} |T(\mathbf{n})|^2 \ll \sum_{\gamma\in\Gamma} |b(\gamma)|^2 \sum_{\gamma'\in\Gamma} (\delta_1 \ldots \delta_l)^{-1} \times$$
$$\times \prod_{j=1}^{l} \left(\int_{I(\gamma_j' - \gamma_j,\, \delta_j)} F(\beta, \delta_j)\, d\beta \right).$$

С помощью замены переменных произведение интегралов записывается в виде

$$\int\limits_{\mathcal{R}(\boldsymbol{\gamma}')} \prod_{j=1}^{l} F(\beta_j - \gamma_j,\ \delta_j)\, d\boldsymbol{\beta},$$

так что, согласно предположению относительно $\mathcal{R}(\boldsymbol{\gamma}')$, сумма по $\boldsymbol{\gamma}'$ не больше чем

$$(\delta_1 \ldots \delta_l)^{-1} \prod_{j=1}^{l} \left(\int\limits_0^l F(\beta - \gamma_j,\ \delta_j)\, d\beta \right).$$

Здесь j-й интеграл есть

$$\ll \int\limits_0^{\delta_j} N\, d\beta + \int\limits_{\delta_j}^{\infty} N(1 + N\beta)^{-2}\, d\beta = N\delta_j + (1 + N\delta_j)^{-1}.$$

Остается, следовательно, установить соотношение (5.25).

Если $\|\alpha\| \geqslant \delta$ и $\|\alpha - \beta\| < \delta$, то

$$1 + N\|\beta\| \leqslant 1 + N(\|\alpha\| + \delta) \leqslant 2(1 + N\|\alpha\|),$$

так что $F(\beta,\ \delta) \geqslant N(1 + N\|\beta\|)^{-2} \geqslant \frac{1}{4} F(\alpha,\ \ \delta)$, что дает (5.25) в случае $\|\alpha\| \geqslant \delta$. В противоположном случае $\|\alpha\| < \delta$ можно предполагать, что $|\alpha| < \delta$, и, более того, если необходимо, делая замену переменной, что $\alpha \geqslant 0$. Если $0 \leqslant \beta < 0$, то $-\delta < \alpha - \beta < \delta$, так что каждое такое β лежит в $I(\alpha, \delta)$ и $F(\beta, \delta) = N = F(\alpha, \delta)$. Отсюда

$$\delta^{-1} \int\limits_{I(\alpha,\ \delta)} F(\beta,\ \delta)\, d\beta \geqslant N = F(\alpha,\ \delta),$$

что снова дает (5.25).

Технический прием, применяемый здесь для оценки $f(\boldsymbol{\alpha})$, заключается в сравнении

$$\sum_{m \in \mathcal{M}} |g(m,\ \boldsymbol{\beta})|^{2s}$$

с $J_s(2N)$ посредством леммы 5.3 и подходящего выбора $\mathcal{M}$.

Пусть $\boldsymbol{\gamma}(m) = (\gamma_1(m),\ \ldots,\ \gamma_{k-1}(m))$, где

$$\gamma_j(m) = \sum_{h=j}^{k} \alpha_h \binom{h}{j} (-m)^{h-j} \quad (1 \leqslant j \leqslant k-1). \tag{5,26}$$

Тогда, согласно (5.19),

$$\mathbf{v}^{(k)}(x - m) \cdot \boldsymbol{\alpha} = \mathbf{v}^{(k-1)}(x) \cdot \boldsymbol{\gamma}(m) + x^k \alpha_k + \sum_{j=1}^{k} \alpha_j (-m)^j. \tag{5.27}$$

Таким образом, для того чтобы применить лемму к сумме g, заданной (5.22), необходимо выяснить распределение $\gamma_j(m)$ по модулю 1.

Предположим, что $1 \leqslant x,\ y \leqslant N,\ x \neq y$, и определим

$$a_{hj} = \frac{k!}{h+1}\binom{h+1}{j}\frac{(-x)^{h+1-j}-(-y)^{h+1-j}}{y-x} \qquad (1 \leqslant j \leqslant h < k), \tag{5.28}$$

$$a_{hj} = 0 \qquad (1 \leqslant h < j < k).$$

Заметим, что a_{hj} — целое число и $a_{jj} = k!$. Определим далее

$$\beta_h = \alpha_{h+1}(h+1)(y-x) \tag{5.29}$$

и $\tau_j = k!(\gamma_j(x) - \gamma_j(y))$. Тогда ввиду (5.28)

$$\tau_j = k!\,(\gamma_j(x) - \gamma_j(y)) = \sum_{h=1}^{k-1} \beta_h a_{hj}. \tag{5.30}$$

Наша следующая цель — обратить это линейное преобразование. Положим

$$\boldsymbol{A} = (a_{hj})_{h=1\ j=1}^{k-1\ k-1}$$

и $\mathbf{B} = \mathbf{A} - k!\mathbf{I}$, где $\mathbf{I}$ — единичная матрица порядка $(k-1)\times\times(k-1)$. Матрица $\mathbf{A}$ является нижней треугольной, а $\mathbf{B} = (b_{hj})$, где $b_{hj} = 0$ при $1 \leqslant h \leqslant j < k$ и $b_{hj} = a_{hj}$, когда $1 \leqslant j < h < k$. Таким образом, (5.30) можно записать в виде

$$\boldsymbol{\tau} = \boldsymbol{\beta}\mathbf{A}. \tag{5.31}$$

t-я степень $\mathbf{B}$ имеет вид

$$\mathbf{B}^t = (b_{hj}^{(t)}),$$

где
$$b_{hj}^{(t)} = \sum_{j_1=1}^{k-1} \cdots \sum_{j_{t-1}=1}^{k-1} b_{hj_1} b_{j_1 j_2} \cdots b_{j_{t-1} j}.$$

Следовательно, $b_{hj}^{(t)}$ — целое число и $b_{hj}^{(t)} = 0$, если $h < j + t$. Более того, согласно (5.28), $a_{hj} \ll N^{h-j}$ при $h > j$. Отсюда при $h \geqslant j + t$

$$b_{hj}^{(t)} \ll \sum_{j_1} \cdots \sum_{j_{t-1}} N^{h-j_1} N^{j_1-j_2} \cdots N^{j_{t-1}-j},$$
$$j < j_{t-1} < \ldots < j_2 < j_1 < h$$

так что
$$b_{hj}^{(t)} \ll N^{h-j}. \tag{5.32}$$

Очевидно, что $\mathbf{B}^{k-1}$ — нулевая матрица. Таким образом, полагая $\mathbf{J} = k!\mathbf{I}$ и

$$\mathbf{D} = \mathbf{J}^{k-2} - \mathbf{J}^{k-3}\mathbf{B} + \ldots + (-1)^{k-2}\mathbf{B}^{k-2},$$

получаем

$$\mathbf{AD} = (\mathbf{B} + \mathbf{J})\,\mathbf{D} = \mathbf{J}^{k-1} + (-1)^{k-2}\mathbf{B}^{k-1} = (k!)^{k-1}\mathbf{I}.$$

Поэтому ввиду (5.31)

$$\tau\mathbf{D} = (k!)^{k-1}\boldsymbol{\beta},$$

так что

$$(k!)^{k-1}\beta_j = (k!)^{k-2}\tau_j + \sum_{t=1}^{k-2}(-1)^t (k!)^{k-2-t} \sum_{h=j+t}^{k-1} \tau_h b_{hj}^{(t)}.$$

Таким образом, согласно (5.32),

$$\| (k!)^{k-1}\beta_j \| \ll \sum_{h=j}^{k-1} \| \tau_h \| N^{h-j}.$$

Следовательно, в соответствии с (5.29) и (5.30)

$$\| (k!)^k \alpha_j (x-y) \| \ll \sum_{h=j-1}^{k-1} \| \gamma_j(x) - \gamma_j(y) \| N^{h-j+1} \quad (2 \leqslant j \leqslant k). \tag{5.33}$$

Предположим, что для некоторого j, $2 \leqslant j \leqslant k$, существуют a, q, такие, что $(a, q) = 1$, $q \leqslant N^j$ и $|\alpha_j - a/q| \leqslant q^{-2}$. Пусть

$$L = \min(q, N). \tag{5.34}$$

Тогда для каждого $x \in [1, L]$ число $y \in [1, L]$, для которых

$$\| (k!)^k \alpha_j (x-y) \| \leqslant N^{i-j},$$

ограничивается числом $y \in [1, L]$, для которых

$$\| (k!)^k a (x-y)/q \| \leqslant N^{1-j} + (k!)^k L q^{-2},$$

что не превышает R, где

$$R = ((k!)^k L q^{-1} + 1)(2qN^{1-j} + 2(k!)^k L q^{-1} + 1). \tag{5.35}$$

Поэтому существует множество $\mathcal{M}$ целых чисел $x \in [1, L]$, такое, что $M = \operatorname{card}\mathcal{M}$ удовлетворяет неравенству $M \geqslant L/(R+1)$ и для любой пары x, y, $x \in \mathcal{M}$, $y \in \mathcal{M}$, $x \neq y$,

$$\| (k!)^k \alpha_j (x-y) \| > N^{1-j}.$$

Согласно (5.33), для каждой такой пары x, y существует h, для которого $j-1 \leqslant h \leqslant k-1$ и

$$\| \gamma_h(x) - \gamma_h(y) \| \gg N^{-h}.$$

Теперь можно применить лемму 5.3 с $k-1$ вместо k, с $N_j = sN^j$, с $\delta_j \gg N^{-j}$, с $\Gamma = \{\boldsymbol{\gamma}(m) : m \in \mathcal{M}\}$ и с

$$a(\mathbf{n}) = \sum_{x_1, \ldots, x_s} e\left((x_1^k + \ldots + x_s^k)\alpha_k + (x_1 + \ldots + x_s)\beta\right),$$

где сумма распространяется на решения $x_1, \ldots, x_s$ системы уравнений

$$x_1^h + \ldots + x_s^h = n_h \quad (1 \leqslant h \leqslant k-1)$$

с $1 \leqslant x_r \leqslant 2N$. Следовательно, в силу (5.22), (5.27) и (5.6)

$$\sum_{m \in \mathcal{M}} |g(m, \beta)|^{2s} \ll J_s^{(k-1)}(2N) N^{k(k-1)/2}.$$

Отсюда, согласно (5.23) и неравенству Гельдера,

$$f(\alpha)^{2s} \ll (R/L)(\log 2N)^{2s} J_s^{(k-1)}(2N) N^{k(k-1)/2}.$$

Отсюда и из (5.34) и (5.35) вытекает следующая теорема.

Теорема 5.2. *Предположим, что существуют числа j, a, q, такие, что $2 \leqslant j \leqslant k$, $|\alpha_j - a/q| \leqslant q^{-2}$, $(a, q) = 1$, $q \leqslant N^j$. Тогда*

$$f(\alpha) \ll \left(J_s^{(k-1)}(2N) N^{k(k-1)/2} \left(qN^{-j} + N^{-1} + q^{-1}\right)\right)^{1/2s} \log 2N.$$

Комбинируя эту теорему с теоремой 5.1 получаем следующую теорему.

Теорема 5.3. *В предположениях теоремы* 5.2

$$f(\alpha) \ll N \left(N^{\eta} (qN^{-j} + N^{-1} + q^{-1})\right)^{1/(2(k-1)l)} \log 2N,$$

где

$$\eta = \tfrac{1}{2}(k-1)^2 \left(\frac{k-2}{k-1}\right)^l.$$

В частности, если $N \ll q \ll N^{j-1}$, то

$$f(\alpha) \ll N^{1-\sigma} \log 2N,$$

где

$$\sigma = \max_l \frac{1}{2(k-1)l} \left(1 - \tfrac{1}{2}(k-1)^2 \left(\frac{k-2}{k-1}\right)^l\right). \tag{5.36}$$

Кроме того, $4\sigma k^2 \log k \sim 1$ при $k \to \infty$.

Все утверждения, кроме последней части, следуют сразу. Чтобы доказать последнюю часть, заметим, что при $k \geqslant 3$ максимум достигается при величине l, удовлетворяющей неравенству $\left| l - \lambda \left(\log \frac{k-1}{k-2}\right)^{-1} \right| < 1$, где λ — больший корень трансцендентного уравнения

$$e^{\lambda} = \tfrac{1}{2}(k-1)^2(\lambda + 1).$$

Теперь легко видеть, что $\lambda \sim 2 \log k$ и

$$\sigma = \frac{1}{2k^2} \frac{1}{\lambda + 1} \left(1 + O\left(\frac{1}{k}\right)\right).$$

Несложные вычисления показывают, что при $k \geqslant 12$ теорема 5.3 дает более сильные результаты, чем лемма 2.4.

5.3 Малые дуги в проблеме Варинга

Пусть $f(\alpha)$ задана формулой (1.6). Тогда

$$\int_0^1 |f(\alpha)|^{2s}\, d\alpha$$

есть число решений уравнения

$$x_1^k + \ldots + x_s^k = y_1^k + \ldots + y_s^k$$

с $1 \leqslant x_j, y_j \leqslant N$. Отсюда

$$\int_0^1 |f(\alpha)|^{2s}\, d\alpha \ll N^{k(k-1)/2} J_s(N). \tag{5.37}$$

Пусть $N, P, \mathfrak{M}, \mathcal{U}$ такие, как в § 4.4, и пусть $\mathfrak{m} = \mathcal{U} \setminus \mathfrak{M}$. Пусть $\alpha \in \mathfrak{m}$. Выберем a, q такими, что $(a, q) = 1$, $q \leqslant n/P$ и $|\alpha - a/q| \leqslant Pq^{-1}n^{-1}$ (лемма 2.1). Тогда $1 \leqslant a \leqslant q$, и поскольку α лежит вне больших дуг $\mathfrak{M}(a, q)$, то $q > P$. Отсюда ввиду леммы 2.4 и теоремы 5.3

$$f(\alpha) \ll N^{1-\sigma_0+\varepsilon},$$

где $\sigma_0 = \max(\sigma, 2^{1-k})$, а σ задается (5.36). Таким образом, в силу теоремы 5.1 и (5.37) с заменой s на kl существует положительное число δ, такое, что каково бы ни было

$$s > \frac{k^2}{2\sigma_0}(1 - 1/k)^l + 2kl,$$

имеем

$$\int_{\mathfrak{m}} |f(\alpha)|^{2s}\, d\alpha \ll N^{2s-k-\delta}.$$

Объединяя это с (4.33) и теоремами 4.4 и 4.6, получаем следующую теорему.

Теорема 5.4. *Пусть* $\sigma_0 = \max(\sigma, 2^{1-k})$, *и пусть* s_0 — *наименьшее целое число, такое, что*

$$s_0 > \min_l \left(\frac{k^2}{2\sigma_0}\left(1 - \frac{1}{k}\right)^l + 2kl\right). \tag{5.38}$$

Тогда асимптотическая формула (2.27) *справедлива для любого* $s \geqslant s_0$. *Кроме того,* $s_0 \sim 4k^2 \log k$ *при* $k \to \infty$.

Несложные вычисления показывают, что $s_0 < 2^k + 1$, при $k \geqslant 11$.

5.4 Верхняя граница $G(k)$

Изучение проблемы Варинга пока было сосредоточено на асимптотической формуле для числа решений уравнения

$$x_1^k+\ldots+x_s^k=n.$$

Однако Харди и Литтлвуд (1925) заметили, что величину s можно уменьшить, ограничив область изменения нескольких из переменных x_j. Этот метод был позднее значительно разработан И. М. Виноградовым и Дэвенпортом.

Виноградов показал, что $G(k)\leqslant k(\log k)(C+o(1))$ при $k\to\infty$, и в течение приблизительно 30 лет было получено снижение допустимого значения C до 2. Достаточно простыми рассуждениями можно показать, что C можно взять равным 3. Дальнейшее уменьшение от 3 до 2 см. в гл. 7.

Пусть Z велико, положим

$$Z_1=\tfrac{1}{6}Z,\quad Z_{j+1}=\tfrac{1}{2}Z_j^{1-1/k},$$

и пусть $Q_Z(m)$ — число решений уравнения

$$x_1^k+\ldots+x_t^k=m$$

с $Z_j<x_j\leqslant 2Z_j$. Тогда сумма $\sum\limits_m Q_Z(m)^2$ равна числу решений уравнения

$$x_1^k+\ldots+x_t^k=y_1^k+\ldots+y_t^k \text{ с } Z_j<x_j,\ y_j\leqslant 2Z_j. \tag{5.39}$$

Поскольку

$$|x_1^k-y_1^k|\geqslant|x_1-y_1|kZ_1^{k-1}$$

и

$$|x_2^k+\ldots+x_t^k-y_2^k-\ldots-y_t^k|<2^kZ_2^k+O(Z_3^k)<kZ_1^{k-1},$$

то (5.39) может иметь решение только при $x_1=y_1$. Повторяя это рассуждение, получаем, что $x_2=y_2$, $x_3=y_3$ и т. д. Таким образом,

$$\sum_m Q_Z(m)^2\ll Z_1\ldots Z_t\ll\Big(\sum_m Q_Z(m)\Big)^2(Z_1\ldots Z_t)^{-1}.$$

Более того, $Z_1\ldots Z_t\gg Z^{k-k(1-1/k)^t}$ и $Q_Z(m)=0$, когда

$$m>3^{-k}Z^k+O(Z^{k-1}).$$

Таким образом,

$$\sum_m Q_Z(m)^2\ll\Big(\sum_m Q_Z(m)\Big)^2Z^{-k+k(1-1/k)^t} \tag{5.40}$$

и

$$Q_Z(m)=0\quad\text{при}\quad m>\tfrac{1}{8}Z^k. \tag{5.41}$$

Приведенные выше рассуждения, кроме того, показывают, что $Q_Z(m)$ равно 0 или 1, и дают множество $\mathscr{M}$ натуральных чисел m, не превосходящих Z^k, для которого m есть сумма t k-х степеней и

$$\operatorname{card}\mathscr{M} \gg Z^{k-k(1-1/k)^t}.$$

Таким образом, для сравнительно малого t, например $Ck\log k$, мощность $\mathscr{M}$ можно сделать сравнительно близкой к Z^k. Это построение, представляющее собой незначительную модификацию построения Харди и Литтлвуда, используется на малых дугах двумя различными способами. Во-первых, аналогично лемме Хуа (лемма 2.5) для того, чтобы сэкономить почти N^k, а во-вторых (и это является вкладом Виноградова), чтобы сохранить небольшой запас для получения неравенства, подобного неравенству Вейля (лемма 2.4), но более эффективного.

Пусть

$$H(\alpha) = \sum_m Q_N(m)\, e(\alpha m), \tag{5.42}$$

Тогда, согласно тождеству Парсеваля и (5.40),

$$\int_0^1 |H(\alpha)|^2\, d\alpha \ll H(0)^2 N^{-k+k(1-1/k)^t}. \tag{5.43}$$

Следующий результат в значительной степени принадлежит И. М. Виноградову (1947).

Лемма 5.4. *Пусть*

$$V(\alpha) = \sum_{X/2<p\leqslant X} \sum_{y\leqslant Y} b_y e(\alpha p^k y),$$

где b_y — произвольные комплексные числа. Предположим, что $\alpha = a/q + \beta$, $|\beta| \leqslant \frac{1}{2} q^{-1} X^{-k}$, $q \leqslant 2X^k$, $(a, q) = 1$, что $Y \gg X^k$ и что если $q \leqslant X$, то $\|\beta\| \gg q^{-1} X^{1-k} Y^{-1}$. Тогда

$$V(\alpha) \ll \Big(XY^{1+\varepsilon} \sum_{y\leqslant Y} |b_y|^2\Big)^{1/2}.$$

Заметим, что описанные ниже рассуждения легко могут быть видоизменены, так что интервал суммирования $[0, Y]$ для y заменяется произвольным интервалом длины Y.

Доказательство. По неравенству Коши

$$V(\alpha)^2 \ll X \sum_{X/2<p\leqslant X} \Big|\sum_{y\leqslant Y} b_y e(\alpha p^k y)\Big|^2. \tag{5.44}$$

При $(h, q) = 1$ число J решений сравнения

$$x^k \equiv h \pmod q$$

оценивается в виде $J \ll q^{\varepsilon}$. Следовательно, существует $L \ll q^{\varepsilon}$, такое, что простые числа p, удовлетворяющие условию $X/2 < p \leqslant X$, можно распределить в L классов $\mathcal{P}_1, \ldots, \mathcal{P}_L$ так, что для двух различных простых p_1, p_2 в данном классе $\mathcal{P}_j$ выполнено $p_1^k \equiv p_2^k \pmod q$ тогда и только тогда, когда $p_1 \equiv p_2 \pmod q$.

Рассмотрим два таких простых числа p_1 и p_2. По предположению

$$\|\alpha(p_1^k - p_2^k)\| \geqslant \|a(p_1^k - p_2^k)/q\| - \tfrac{1}{2} q^{-1} X^{-k} X^k \geqslant \tfrac{1}{2} q^{-1}$$

при условии, что $p_1 \not\equiv p_2 \pmod q$. Когда $q > X$, элементы $\mathcal{P}_j$ несравнимы по модулю q. Поэтому для $p \in \mathcal{P}_j$ αp^k отличаются по модулю 1 друг от друга по крайней мере на $\frac{1}{2} q^{-1}$. Следовательно, в силу одномерного случая леммы 5.3 (неравенство большого решета)

$$\sum_{\substack{X/2 < p \leqslant X \\ p \in \mathcal{P}_j}} \Bigl| \sum_{y \leqslant Y} b_y e(\alpha p^k y) \Bigr|^2 \ll Y \sum_{y \leqslant Y} |b_y|^2, \tag{5.45}$$

и лемма легко следует из (5.44).

При $q \leqslant X$ рассуждения могут быть изменены следующим образом. Предположим, что $p_1 \equiv p_2 \pmod q$, но $p_1 \neq p_2$. Тогда по предположению

$$\|\alpha(p_1^k - p_2^k)\| = \|\beta(p_1^k - p_2^k)\| = |\beta|\,|p_1^k - p_2^k| \gg$$
$$\gg q^{-1} Y^{-1} |p_1 - p_2|.$$

Теперь $|p_1 - p_2| \geqslant q$, так что в комбинации с предыдущим это показывает, что αp^k по модулю 1 находятся на расстоянии $\gg Y^{-1}$. Следовательно, по лемме 5.3 сразу получается (5.45) и лемма 5.4.

Пусть $X = N^{1/2}$, $Y = X^k$ и

$$W(\alpha) = \sum_{X/2 < p \leqslant X} \sum_{y} Q_X(y) e(\alpha p^k y).$$

Примем обозначения § 5.3 и предположим, что $\alpha \in \mathfrak{m}$. Возьмем a, q такими, что $(a, q) = 1$, $q \leqslant 2X^k$, $|\alpha - a/q| \leqslant \frac{1}{2} q^{-1} \times X^{-k}$. Тогда $1 \leqslant a \leqslant q$, и, поскольку α не лежит на большой дуге, когда $q \leqslant N$, сразу имеем $|\alpha - a/q| \gg q^{-1} N^{1-k} > q^{-1} X^{1-k} Y^{-1}$. Таким образом, по лемме 5.4, (5.40) и (5.41),

$$W(\alpha) \ll W(0) \left(N^{k(1-1/k)^t - 1 + \varepsilon}\right)^{1/4}.$$

Следовательно, ввиду (5.43) и (1.6)

$$\int_{\mathfrak{m}} f(\alpha)^{4k} H(\alpha)^2 W(\alpha) e(-\alpha n)\, d\alpha \ll H(0)^2 W(0) n^{3+\varepsilon-\eta},$$

где

$$\eta = \frac{1}{4k} - \frac{5}{4}\left(1 - \frac{1}{k}\right)^t.$$

Таким образом, если t взять таким, что

$$t > (\log 5k)\Big/\left(-\log\left(1 - \frac{1}{k}\right)\right), \tag{5.46}$$

то отсюда следует, что существует положительная постоянная δ, такая, что

$$\int_{\mathfrak{m}} f(\alpha)^{4k} H(\alpha)^2 W(\alpha) e(-\alpha n)\, d\alpha \ll H(0)^2 W(0) n^{3-\delta}. \tag{5.47}$$

Теперь

$$H(\alpha)^2 W(\alpha) = \sum_m Q^*(m) e(\alpha m), \tag{5.48}$$

где

$$Q^*(m) = \sum_{\substack{m_1 \\ m_1+m_2+p^k y = m}} \sum_{m_2} \sum_{X/2 < p \leqslant X} \sum_y Q_N(m_1) Q_N(m_2) Q_X(y).$$

Согласно (5.41), $Q^*(m) = 0$, когда $m > \frac{1}{2}n$. Поэтому по теореме 4.4 и (4.6)

$$\int_{\mathfrak{M}} f(\alpha)^{4k} H(\alpha)^2 W(\alpha) e(-\alpha n)\, d\alpha =$$

$$= \sum_m Q^*(m) \int_{\mathfrak{M}} f(\alpha)^{4k} e(-(n-m)\alpha)\, d\alpha \gg n^3 \sum_m Q^*(m).$$

Следовательно, ввиду (5.47) и (5.48)

$$\int_0^1 f(\alpha)^{4k} H(\alpha)^2 W(\alpha) e(-\alpha n)\, d\alpha \gg n^3 H(0)^2 W(0) > 0.$$

С другой стороны, левая часть есть число решений уравнения

$$x_1^k + \ldots + x_{4k}^k + y_1^k + \ldots + y_t^k + z_1^k + \ldots$$

$$\ldots + z_t^k + p^k\left(w_1^k + \ldots + w_t^k\right) = n$$

с x_j, y_j, z_j, w_j, p при соответствующих ограничениях. Поэтому

$$G(k) \leqslant 4k + 3t.$$

Оптимальным вариантом t в (5.46) оказывается $t \sim k \log k$. Таким образом,

$$G(k) \leqslant k(\log k)(3 + o(1)) \text{ при } k \to \infty. \tag{5.49}$$

5.5 Упражнения

1. Покажите, что, если $\mathscr{L}$ — последовательность натуральных чисел l_k, такая, что ряд $\sum_{k=1}^{\infty} 1/l_k$ сходится, тогда для каждого ε и k_0 существует k_1, такое, что если $A(X)$ — число натуральных чисел n с $n \leqslant X$, которые могут быть записаны в форме
$$n = \sum_{k_0 < k \leqslant k_1} x_k^{l_k}$$
с неотрицательными целыми x_k, то $A(x) > X^{1-\varepsilon}(X > X_0(\varepsilon, k_0))$.
2. [Freiman's hypothesis, 1949; Scouzfield, 1960]. Пусть $\mathscr{L}$ — последовательность из натуральных чисел l_k. Покажите, что свойство: для каждого k_0 найдется k_1, такое, что любое натуральное число n может быть записано в виде
$$n = \sum_{k_0 < k \leqslant k_1} x_k^{l_k}$$
с неотрицательными x_k, имеет место тогда и только тогда, когда ряд $\sum_{k=1}^{\infty} 1/l_k$ сходится.
3. Пусть s_0 такое же, как в теореме 5.4. Покажите, что для $2s \geqslant s_0$
$$\sum_{Q < q \leqslant R} \frac{1}{q} \sum_{\substack{a=1 \\ (a,\, q)=1}}^{q} \left| f\left(\frac{a}{q}\right)\right|^{2s} \ll (N^k Q^{-1} + R) N^{2s-k}.$$

Примечания редактора

[1] Теоремой Виноградова о среднем называют теорему 5.1, которая дает точную верхнюю границу $J_s(X)$ при $s > ck^2 \log k$; нетривиальная оценка $J_s(X)$, например $J_s(X) \leqslant k! X^{2s-k}$ — первый шаг индукции на с. 65.

[2] Неточное замечание, см., например, доказательство И. М. Виноградова [1], с. 54.

[3] В оригинале формулировка леммы несколько иная.

[4] Доказательство теоремы о среднем с оценкой $c(k, l) \leqslant k^{2k^3} 2^{6k^2 l} (kl)^{2kl}$ см. в статье Архипова Г. И. Карацубы А. А. (1978) с. 762.

[5] Если решения y_r указанной системы сравнений являются перестановками x_r, то решения y_r системы уравнений тем более являются перестановками x_r.

6
Методы Дэвенпорта

6.1 Множества сумм k-х степеней

В § 5.4 было показано, что верхнюю границу $G(k)$ можно существенно уменьшить прежде всего при помощи построения множества $\mathscr{M}$ натуральных чисел, не превосходящих Z^k, являющихся суммами t k-х степеней. Это построение дает $\operatorname{card}\mathscr{M} \gg z^{k\alpha}$, где $\alpha = 1-(1-1/k)^t$, и представляет собой незначительное упрощение конструкции Харди и Литтлвуда (1925). В самом деле, они строят Z_j так же, как и выше для $j=1, \ldots, t-1$, но полагают $Z_t = Z_{t-1}$. Рассуждения проводятся, как и ранее, до $(t-1)$-го шага, когда (5.39) сводится к

$$x_{t-1}^k + x_t^k = y_{t-1}^k + y_t^k.$$

Для каждой заданной пары y_{t-1}, y_t число вариантов x_{t-1}, x_t есть $\ll Z_t^{\varepsilon}$. Следовательно,

$$\sum_m Q_Z(m)^2 \ll Z_1 \ldots Z_{t-1} Z_t^{1+\varepsilon} \ll$$
$$\ll \Bigl(\sum_m Q_Z(m)\Bigr)^2 \bigl(Z_1 \ldots Z_{t-1} Z_t^{1-\varepsilon}\bigr)\Bigr)^{-1}.$$

Кроме того,

$$Z_1 \ldots Z_t \gg Z^{k-(k-2)(1-1/k)^{t-2}}.$$

Отсюда по неравенству Коши

$$\sum_{\substack{m \\ Q_Z(m)>0}} 1 \gg Z^{k-(k-2)(1-1/k)^{t-2}-\varepsilon}.$$

Пусть $N_t(x)$ означает число натуральных чисел m, не превосходящих X, которые являются суммами не более t k-х степеней. Тогда

$$N_t(X) > X^{\alpha_t - \varepsilon} \quad (X > X_0(t, \varepsilon)) \tag{6.1}$$

с

$$\alpha_t = 1 - \Bigl(1-\frac{2}{k}\Bigr)\Bigl(1-\frac{1}{k}\Bigr)^{t-2}. \tag{6.2}$$

Заметим, что $\alpha_2 = 2/k$.

Имеется ряд усовершенствований этих рассуждений, которые эффективны при таком способе улучшения оценок сверху для $G(k)$, когда k сравнительно мало. Следующая теорема является обобщением результата Дэвенпорта и Эрдеша (1939).

Теорема 6.1. *Пусть* $t \geqslant 3$, $\theta = 1 - 1/k$, $\lambda_1 = 1$,

$$\lambda_2 = \frac{k^2 - \theta^{t-3}}{k^2 + k - k\theta^{t-3}}, \qquad \lambda_j = \frac{k^2 - k - 1}{k^2 + k - k\theta^{t-3}}\theta^{j-3} \quad (3 \leqslant j \leqslant t)$$

и $Q(m)$ *обозначает число решений уравнения*

$$x_1^k + \ldots + x_t^k = m \quad \text{с} \quad Z^{\lambda_j} < x_j < 2Z^{\lambda_j}. \tag{6.3}$$

Тогда

$$\sum_m Q(m)^2 \ll Z^{\lambda_1 + \ldots + \lambda_t + \varepsilon}.$$

Следствие. *Неравенство* (6.1) *справедливо с* $\alpha_t = 1 - \rho$, *где*

$$\rho = \frac{k^3 - 3k^2 + k + 2}{k^3 + k^2 - k^2\theta^{t-3}}\theta^{t-3}. \tag{6.4}$$

Это следствие получается использованием неравенства Коши тем же путем, что и выше.

Доказательство теоремы. Пусть M_s — число решений уравнения

$$x_1^k + \ldots + x_s^k = y_1^k + \ldots + y_s^k \tag{6.5}$$

с $Z^{\lambda_j} < x_j, y_j < 2Z^{\lambda_j}$ и $x_s \neq y_s$. Поскольку $M_1 = 0$,

$$\sum_m Q(m)^2 \ll \sum_{s=2}^{t} M_s Z^{\lambda_{s+1} + \ldots + \lambda_t} + Z^{\lambda_1 + \ldots + \lambda_t}. \tag{6.6}$$

Кроме того, M_2 — число решений уравнения

$$x_1^k - y_1^k = x_2^k - y_2^k$$

с $x_2 \neq y_2$ и $Z^j < x_j, y_j < 2Z^j$. Для каждой заданной пары x_2, y_2 $(x_2 \neq y_2)$ число возможных значений x_1, y_1 есть $\ll Z^{\varepsilon}$. Отсюда

$$M_2 \ll Z^{2\lambda_2 + \varepsilon} \ll Z^{\lambda_1 + \lambda_2}. \tag{6.7}$$

Для $s \geqslant 3$

$$M_s = M_s' + 2M_s'', \tag{6.8}$$

где M_s' — число решений (6.5) с дополнительным условием $x_1 = y_1$, а M_s'' — число решений с $x_1 > y_1$. Тогда

$$M_s' \ll Z^{\lambda_1} L_s, \tag{6.9}$$

где L_s есть число решений уравнения

$$x_2^k + \ldots + x_s^k = y_2^k + \ldots + y_s^k. \tag{6.10}$$

Для данных $x_2, \ldots, x_s$ число $y_2, \ldots, y_s$ есть $\ll 1$ (ср. с § 5.4). Таким образом,

$$L_s \ll Z^{\lambda_2+\ldots+\lambda_s}. \tag{6.11}$$

Теперь рассмотрим M_s''. Число значений x_2, y_2 есть $\ll Z^{2\lambda_2}$. Для любого такого набора уравнение (6.5) превращается в

$$x_1^k - y_1^k + A + \sum_{j=3}^{s} (x_j^k - y_j^k) = 0, \tag{6.12}$$

где A фиксировано. Пусть $h = x_1 - y_1$. Тогда $x_1^k - y_1^k > hZ^{k-1}$. К тому же

$$A + \sum_{j=3}^{s} (x_j^k - y_j^k) \ll Z^{k\lambda_2}.$$

Отсюда $0 < h \ll Z^{k\lambda_2-k+1}$ и (6.12) можно переписать в виде

$$A + (y_1 + h)^k - y_1^k \ll Z^{k\lambda_3}. \tag{6.13}$$

Для заданного h пусть y и $y+j$ — два возможных значения y_1, для которых выполняется оценка (6.13). Тогда

$$(y+j+h)^k - (y+j)^k - (y+h)^k + y^k \ll Z^{k\lambda_3},$$

откуда $hjZ^{k-2} \ll Z^{k\lambda_3}$. Таким образом, число возможных значений для y_1 есть

$$\ll 1 + Z^{k\lambda_3-k+2}h^{-1}. \tag{6.14}$$

Для данных x_1, y_1 (6.12) принимает вид

$$A_1 + \sum_{j=3}^{s} (x_j^k - y_j^k) = 0, \tag{6.15}$$

где A_1 фиксировано. Число наборов $y_3, \ldots, y_{s-1}$ есть $\ll Z^{\lambda_3+\ldots+\lambda_{s-1}}$, и для каждого такого набора число наборов $x_3, \ldots, x_{s-1}$ есть $\ll 1$ (заметим, что $x_4^k + \ldots + x_s^k \ll Z^{\lambda_3\theta}$ и что в интервале длины $Z^{\lambda_3\theta}$ имеется $\ll 1$ значений x_3^k и т. д.).

Для заданных $y_3, \ldots, y_{s-1}, x_3, \ldots, x_{s-1}$ (6.15) переписывается в виде

$$A_2 + x_s^k - y_s^k = 0,$$

где A_2 фиксировано, и, так как $x_s \neq y_s$, количество наборов x_s, y_s есть $\ll Z^{\varepsilon}$. Следовательно, в силу (6.14)

$$M_s'' \ll Z^{2\lambda_2} \sum_{0<h\leqslant Z^{k\lambda_2-k+1}} \left(1 + Z^{k\lambda_3-k+2}h^{-1}\right) Z^{\lambda_3+\ldots+\lambda_{s-1}+\varepsilon}.$$

Таким образом, ввиду (6.8), (6.9), (6.11)

$$M_s \ll Z^{\lambda_1+\ldots+\lambda_s} + Z^{2\lambda_2}\left(Z^{k\lambda_2-k+1} + Z^{k\lambda_3-k+2}\right) Z^{\lambda_3+\ldots+\lambda_{s-1}+2\varepsilon},$$

Теорема следует теперь из (6.6), если заметить, что для $s=3, \ldots, t$ $(k+1)\lambda_2 - k \ll \lambda_s$ и $\lambda_2 + k\lambda_3 - k + 1 \leqslant \lambda_s$.

Следующая теорема принадлежит Дэвенпорту (1942*a*).

Теорема 6.2. *Предположим, что* $1 \leqslant j \leqslant k-2$, $0 < \nu < 1$, $\mathscr{A}$ — *множество натуральных чисел* a, $a \leqslant Z^{\nu+k-1}$, $S = \operatorname{card} \mathscr{A}$, $Q(m)$ — *число решений уравнения*

$$x^k + a = m$$

с $Z < x < 2Z$, $a \in \mathscr{A}$ *и* $T = \sum_m Q(m)^2$. *Тогда*

$$T \ll ZS\left(1 + Z^{\nu+\varepsilon}\left(Z^{-2} + Z^{-\nu-j-1}S\right)^{2^{-j}}\right).$$

Доказательство. Пусть Δ_j такое же, как в § 2.2, и

$$\mathscr{H}_j = \{\mathbf{h}\colon h_j > 0;\ h_1 < Z^\nu;\ h_2, \ldots, h_j < Z\}.$$

Пусть $\rho_j(\mathbf{h}, m)$ обозначает число решений уравнения

$$\Delta_j(x^k; \mathbf{h}) + a = m \text{ с } Z < x < 2Z, \quad a \in \mathscr{A}, \tag{6.16}$$

и

$$M_j = \sum_{\mathbf{h} \in \mathscr{H}_j} \sum_{a \in \mathscr{A}} \rho_j(\mathbf{h}, a). \tag{6.17}$$

Очевидно,

$$T \ll ZS + M_1 \tag{6.18}$$

Согласно неравенству Коши,

$$M_j^2 < Z^{\nu+j-1} S \sum_{\mathbf{h} \in \mathscr{H}_j} \sum_{a \in \mathscr{A}} \rho_j(\mathbf{h}, a)^2.$$

Двойная сумма является числом решений уравнения

$$\Delta_j(x_1^k;\ \mathbf{h}) + a_1 = \Delta_j(x_2^k;\ \mathbf{h}) + a_2 = a$$

с $Z < x_1$, $x_2 < 2Z$, $a_1 \in \mathscr{A}$, $a_2 \in \mathscr{A}$, $a \in \mathscr{A}$, $\mathbf{h} \in \mathscr{H}_j$. Так как элементы $\mathscr{A}$ различны, эта величина $\ll M_j + M_{j+1}$. Отсюда

$$M_j \ll Z^{\nu+j-1}S + \left(Z^{\nu+j-1} S M_{j+1}\right)^{1/2}.$$

Таким образом, индукцией по j получаем

$$M_1 \ll Z^{\nu+1-2^{1-j}} S + Z^{(\nu+1)(1-2^{-j}) - j2^{-j}} S^{1-2^{-j}} M_{j+1}^{2^{-j}}. \tag{6.19}$$

По определению (6.17) M_{j+1} есть число решений уравнения

$$\Delta_{j+1}(x^k; \mathbf{h}) + a_1 = a$$

с $Z < x < 2Z$, $\mathbf{h} \in \mathscr{H}_{j+1}$, $a_1 \in \mathscr{A}$, $a \in \mathscr{A}$. Из упражнения 2.1 следует, что при $j \leqslant k-2$ для каждой пары a_1, a число наборов x, $\mathbf{h}$ оценивается как $\ll Z^\varepsilon$. Таким образом, $M_{j+1} \ll S^2 Z^\varepsilon$, Теорема следует теперь из (6.18) и (6.19).

Теорема 6.2 обычно применяется повторно для получения понижений границ $N_t(X)$ для последовательных значений t. Вообще, пусть $\mathscr{A}$ означает строго возрастающую последовательность натуральных чисел a, обладающую тем свойством, что

$$A(X) = \operatorname{card}\{a:\ a \in \mathscr{A},\ a \leqslant X\} \tag{6.20}$$

удовлетворяет неравенству

$$A(X) > X^{\alpha-\varepsilon} \quad (X > X_0(\varepsilon)), \tag{6.21}$$

где $0 < \alpha < 1$, и пусть $N(\mathscr{A}, X)$ обозначает число различных чисел вида $x^k + a$ с условиями $x^k + a \leqslant X$ и $a \in \mathscr{A}$. Пусть $Z = \frac{1}{4} X^{1/k}$. Тогда в обозначениях теоремы 6.2

$$N(\mathscr{A}, X) \geqslant \sum_{\substack{m \\ Q(m) \geqslant 0}} 1,$$

и по неравенству Коши

$$\Bigl(\sum_{\substack{m \\ Q(m) > 0}} 1\Bigr) \sum_m Q(m)^2 \geqslant \Bigl(\sum_m Q(m)\Bigr)^2 \gg Z^2 S^2,$$

где $S = A(Z^{\nu+k-1})$. Отсюда в силу теоремы 6.2

$$N(\mathscr{A}, X) \gg ZS\bigl(1 + Z^{\nu+\varepsilon}(Z^{-2} + Z^{-\nu-j-1}S)^{2^{-j}}\bigr)^{-1}.$$

Таким образом, по (6.21)

$$N(\mathscr{A}, X) > X^{\beta-\varepsilon} \quad (X > X_1(\varepsilon)), \tag{6.22}$$

где
$$\beta = \frac{1}{k}(1 + \alpha(k-1) + \tau)$$
и
$$\tau = \max_{1 \leqslant j \leqslant k-2} \sup_{0 < \nu < 1} \bigl(\min\bigl(\nu\alpha,\ 2^{1-j} - \nu(1-\alpha),$$
$$(j+1)2^{-j} - (k-1)\alpha 2^{-j} - \nu(1-\alpha)(1-2^{-j})\bigr)\bigr).$$

При $j + 1 \leqslant (k-1)\alpha$ упомянутый выше супремум неположителен, поэтому максимум достигается для значения j с условием $j + 1 > (k-1)\alpha$. Для такого j супремум имеет место, когда ν есть наименьшая из двух следующих величин:

$$\nu\alpha = 2^{1-j} - \nu(1-\alpha),$$
$$\nu\alpha = (j+1)2^{-j} - (k-1)\alpha 2^{-j} - \nu(1-\alpha)(1-2^{-j}),$$

т. е.
$$\nu = 2^{1-j}, \quad \nu = \frac{j+1-(k-1)\alpha}{2^j - 1 + \alpha}.$$

Таким образом,

$$\tau = \alpha \max_{1 \leqslant j \leqslant k-2} \min\Bigl(2^{1-j},\ \frac{j+1-(k-1)\alpha}{2^j-1+\alpha}\Bigr).$$

Рассмотрим неравенство

$$\frac{j+1-(k-1)\alpha}{2^j-1+\alpha} \geqslant \frac{j-(k-1)\alpha}{2^{j-1}-1+\alpha}.$$

Оно эквивалентно каждому из следующих неравенств:

$$2^{1-j} \geqslant \frac{j+1-(k-1)\alpha}{2^j-1+\alpha},$$

$$1+(k-1)\alpha \geqslant j+2^{1-j}(1-\alpha). \tag{6.23}$$

Правая часть (6.23) является строго возрастающей функцией j. Таким образом, если J — наибольшее значение j, при котором неравенство (6.23) выполняется, то

$$\tau = \alpha\frac{J+1-(k-1)\alpha}{2^J-1+\alpha},$$

а если таких значений j нет, т. е. если $\alpha < 1/k$, то $\tau = \alpha$. Мы доказали следующую теорему.

Теорема 6.3. *Предположим, что* $\mathscr{A}$ *удовлетворяет условиям* (6.20) *и* (6.21). *Пусть* $H = [(k-1)\alpha]$, *а* $J = H+1$, *когда*

$$2^H((k-1)\alpha - H) \geqslant 1-\alpha, \quad \text{и} \quad H+1 \leqslant k-2$$

и $J = H$ *в остальных случаях. Тогда* $N(\mathscr{A}, X)$ *удовлетворяет неравенству* (6.22) *с*

$$\beta = \frac{1}{k}\left(1+\alpha(k-1)+\alpha\frac{J+1-(k-1)\alpha}{2^J-1+\alpha}\right),$$

когда $\alpha \geqslant 1/k$, *и* $\beta = 1/k+\alpha$ *при* $\alpha < 1/k$.

В случае четвертых степеней полезно иметь небольшое улучшение этого результата. Если считать $Q(m)$ числом решений уравнения $m = x^4+a$ с $Z < x < 2Z$, $x \equiv r \pmod{16}$, $a \in \mathscr{A}$, $a \leqslant Z^{\nu+3}$, то предыдущие рассуждения изменятся незначительно. Также в сущности не меняются рассуждения, дающие (6.1) и (6.2) при ограничении каждого x_j заданным классом вычетов по модулю 16. Таким образом, справедлива

Теорема 6.4 (Дэвенпорт, 1939c). *Пусть* $N_t^{(h)}(X)$ *обозначает число натуральных* n, *не превосходящих* X *в классе вычетов* h *по модулю* 16, *которые являются суммами* t *четвертых степеней. Тогда для* $t \geqslant 2$ *и* $0 \leqslant h \leqslant \min(t, 16)$

$$N_t^{(h)}(X) > X^{\alpha_t-\varepsilon} \quad (X > X_0(\varepsilon, t)), \tag{6.24}$$

где

$$\alpha_2 = \frac{1}{2}, \quad \alpha_{t+1} = \frac{3+13\alpha_t}{12+4\alpha_t}. \tag{6.25}$$

В частности,

$$\alpha_3 = \frac{19}{28}, \qquad \alpha_4 = \frac{331}{412}, \qquad \alpha_5 = \frac{5539}{6268}. \tag{6.26}$$

Дэвенпорт (1942*a*) усовершенствовал рассуждения из теоремы 6.2, которые, в частности, эффективны при $k = 5$ или 6. Пусть в предположениях теоремы 6.2 $Q(m)$ означает число решений уравнения

$$x^k + p^k a = m \tag{6.27}$$

с $Z < x < 2Z$, $a \leqslant Z^{\nu+k-1}$, $\frac{1}{2} Z^{1-\nu} < p^k < Z^{1-\nu}$, $p \nmid x$. Пусть также $Q(m, p)$ обозначает число решений (6.27) для данного p с $Z < x < 2Z$, $a \leqslant Z^{\nu+k-1}$, $p \nmid x$. Тогда, по неравенству Коши, для

$$T = \sum_m Q(m)^2$$

справедливо неравенство

$$T \leqslant P \sum_m \sum_p Q(m, p)^2,$$

где P — число простых p, таких, что $\frac{1}{2} Z^{1-\nu} < p^k < Z^{1-\nu}$. Для заданного простого p и целого r с $p \nmid r$ число решений сравнения $x^k \equiv r \pmod{p^k}$ равно 0 или $(k, \varphi(p^k))$. Таким образом, целые x с условием $p \nmid x$ можно распределить по $q(p) = (k, \varphi(p^k))$ классам $\mathcal{R}_1, \ldots, \mathcal{R}_{q(p)}$ так, что если x и y принадлежат данному классу $\mathcal{R}_r$, то $x^k \equiv y^k \pmod{p^k}$ тогда и только тогда, когда $x \equiv y \pmod{p^k}$. Пусть $Q_r(m, p)$ означает число решений уравнения (6.27) с $Z \leqslant x \leqslant 2Z$, $a \leqslant Z^{\nu+k-1}$, $x \in \mathcal{R}_r$. Тогда по неравенству Коши

$$T \leqslant P \sum_m \sum_p \left(\sum_{\eta=1}^{q(p)} Q_r(m, p) \right)^2 \leqslant$$

$$\leqslant kP \sum_{r=1}^{k} \sum_p \sum_m Q_r(m, p)^2,$$

где $Q_r(m, p)$ полагается равным 0 при $r > q(p)$. Тройная сумма ограничена числом решений уравнения

$$x_1^k + p^k a_1 = x_2^k + p^k a_2,$$

где $x_1 \equiv x_2 \pmod{p^k}$, и x_1, x_2, a_1, a_2, p удовлетворяют тем же условиям, что и прежде.

Пусть Δ_j — такое же, как и раньше,

$$\mathcal{H}_j = \{\mathbf{h}\colon h_i > 0;\ h_1 < 2Z^\nu;\ h_2, \ldots, h_j < Z\}.$$

Пусть $\rho_j(\mathbf{h}, m, p)$ означает число решений уравнения

$$p^{-k} \Delta_j(x^k;\ p^k h_1, h_2, \ldots, h_j) + a = m$$

и

$$M_j = \sum_p \sum_{\mathbf{h} \in \mathcal{H}_j} \sum_{a \in \mathcal{A}} \rho_j(\mathbf{h}, a, p).$$

Тогда, как в доказательстве теоремы 6.2,

$$T \ll P(PZS + M_1)$$

и
$$M_j \ll Z^{\nu+j-1}PS + (Z^{\nu+j-1}PSM_{j+1})^{1/2}.$$

Таким образом, если можно показать, что

$$M_{j+1} \ll S^2 Z^{\varepsilon}, \tag{6.28}$$

то

$$T \ll P^2 ZS\left(1 + Z^{\nu+\varepsilon}\left(Z^{-2} + Z^{-\nu-j-1}P^{-1}S\right)^{2-j}\right) \tag{6.29}$$

и дополнительный сомножитель P^{-1} во внутренних скобках дает улучшение теоремы 6.2.

Вероятно, оценка (6.28) справедлива при всех $j \leqslant k-3$, но доказать это в общем виде, по-видимому, довольно трудно. Она, однако, может быть получена для некоторых значений j. Рассмотрим центральный разностный оператор ∇_j, который можно определить в терминах Δ_j как

$$\nabla_j(f(\alpha);\ \beta_1, \ldots, \beta_j) = \Delta_j\left(f\left(\alpha - \tfrac{1}{2}\beta_1 - \ldots - \tfrac{1}{2}\beta_j\right) \beta_1, \ldots, \beta_j\right).$$

Тогда

$$\nabla_j(\alpha^k;\ \beta_1, \ldots, \beta_j) =$$
$$= \sum_{\theta_1=\pm 1} \cdots \sum_{\theta_j=\pm 1} \theta_1 \ldots \theta_j \left(\alpha + \tfrac{1}{2}\theta_1\beta_1 + \ldots + \tfrac{1}{2}\theta_j\beta_j\right)^k =$$
$$= \sum_{\substack{l_0 + l_1 + \ldots + l_j = k}} \sum_{\substack{l_1 \\ 2 \nmid l_1}} \cdots \sum_{\substack{l_j \\ 2 \nmid l_j}} \frac{k!}{l_0!\, l_1! \ldots l_j!} 2^{l_0 - k + j} \alpha^{l_0} \beta_1^{l_1} \ldots \beta_j^{l_j} =$$
$$= \beta_1 \ldots \beta_j \sum_{\substack{l_0 \\ l_0 + 2(l_1 + \ldots + l_j) = k-j}} \cdots \sum_{l_j} \frac{k!\, 2^{l_0-k+j} \alpha^{l_0} \beta_1^{2l_1} \ldots \beta_j^{2l_j}}{l_0!\,(2l_1+1)! \ldots (2l_j+1)!}.$$

Если $k-j$ нечетно, то $l_0 \geqslant 1$ в каждом члене, так что

$$\nabla_j(\alpha^k;\ \beta_1, \ldots, \beta_j) = \alpha\beta_1 \ldots \beta_j p_j(\alpha;\ \beta_1, \ldots, \beta_j),$$

где

$$p_j(\alpha;\ \beta_1, \ldots, \beta_j) =$$
$$= \sum_{\substack{l_0 \\ l_0 + 2(l_1 + \ldots + l_j) = k-j-1}} \cdots \sum_{l_j} \frac{k!\, 2^{l_0+1-k+j} \alpha^{l_0} \beta_1^{2l_1} \ldots \beta_j^{2l_j}}{(l_0+1)!\,(2l_1+1)! \ldots (2l_j+1)!}.$$

Если $k-j=2$, то

$$\nabla_j(\alpha^k;\ \beta_1,\ \ldots,\ \beta_j)=\beta_1\ldots\beta_j\frac{2^jk!}{2^k3!}(12\alpha^2+\beta_1^2+\ldots+\beta_j^2).$$

Число M_{j+1} теперь можно снова интерпретировать как число решений уравнения

$$p^{-k}\nabla_{j+1}(\alpha^k;\ h_1p^k,\ h_2,\ \ldots,\ h_{j+1})+a_1=a_2$$

с $\alpha=x+\frac{1}{2}h_1p^k+\ldots+\frac{1}{2}h_{j+1}$. При нечетном и положительном $k-j-1$

$$p^{-k}\nabla_{j+1}(\alpha^k;\ h_1p^k,\ h_2,\ \ldots,\ h_{j+1})=$$
$$=\alpha h_1\ldots h_{j+1}p_{j+1}(\alpha;\ h_1p^k,\ h_2,\ \ldots,\ h_{j+1}),$$

что положительно. Для данных a_1, a_2 число наборов для α, h_1, .., h_{j+1}, т. е. для x, h_1, ..., h_{j+1} есть $\ll Z^\varepsilon$. Если, кроме того, $k-j-1\geqslant 3$, то $p_{j+1}(\alpha;\ \beta_1,\ \ldots,\ \beta_{j+1})$ — полином от β_1 степени не ниже 2. Таким образом, для заданных a_1, a_2, α, h_1, ..., h_{j+1} количество значений p есть $\ll 1$. Следовательно, в этом случае имеем (6.28).

При $k-j-1=2$

$$p^{-k}\nabla_{j+1}(\alpha^k;\ h_1p^k,\ h_2,\ \ldots,\ h_{j+1})=$$
$$=h_1\ldots h_{j+1}\frac{2^{j+1}k!}{2^k3!}(12\alpha^2+p^{2k}h_1^2+h_2^2+\ldots+h_{j+1}^2).$$

Для данных a_1, a_2 число наборов h_1, ..., h_{j+1} оценивается величиной $\ll X^\varepsilon$. Тогда при заданных a_1, a_2, h_1, ..., h_{j+1} количество наборов для α, p, т. е. для x, p, снова $\ll X^\varepsilon$, так как число решений уравнения $3u^2+v^2=m$ есть $\ll m^\varepsilon$. Таким образом, для $j=k-3$ оценка (6.28) также имеет место.

Теорема 6.5 (Дэвенпорт, 1942*a*). *Предположим, что* $1\leqslant j\leqslant k-4$ *и* $k-j$ *четно, или* $j=k-3$. *Предположим далее, что* $0<\nu<1$ *и* $\mathscr{A}$ — *множество натуральных чисел* a, $a\leqslant Z^{\nu+k-1}$. *Пусть* $Q(m)$ *обозначает число решений уравнения*

$$x^k+p^ka=m$$

с $Z<x<2Z$, $a\in\mathscr{A}$, $\frac{1}{2}Z^{1-\nu}<p^k<Z^{1-\nu}$, $p\nmid x$, *пусть* $T=\sum_m Q(m)^2$, *и пусть* $S=\operatorname{card}\mathscr{A}$. *Тогда*

$$T\ll P^2ZS\left(1+Z^{\nu+\varepsilon}\left(Z^{-2}+Z^{-\nu-j-1}P^{-1}S\right)^{2-j}\right),$$

где P — *число простых* p, *таких, что* $\frac{1}{2}Z^{1-\nu}<p^k<Z^{1-\nu}$,

Следствие. *Предположим, что неравенство* (6.1) *выполняется,* $1 \leqslant j \leqslant k-4$ *и* $k-j$ *четное или что* $j = k-3$. *Тогда*

$$N_{t+1}(X) > X^{\alpha_{t+1}-\varepsilon} \qquad (X > X_0(t+1, \varepsilon))$$

с

$$\alpha_{t+1} = \frac{1}{k}\left(1 + \alpha_t(k-1) + \tau_j\right)$$

и

$$\tau_j = \alpha_t \min\left(2^{1-j}, \frac{j+1-(k-1)\alpha_t + k^{-1}}{2^j - 1 + \alpha_t + k^{-1}}\right).$$

Это следует из теоремы 6.5 так же, как теорема 6.3 следует из теоремы 6.2.

Предположим, что $k = 5$. Тогда (6.2) дает $\alpha_2 = \frac{2}{5}$, вышеприведенное следствие дает

$$\alpha_{t+1} = \frac{16 + 85\alpha_t}{5(16 + 5\alpha_t)}, \quad \text{когда} \quad \tfrac{2}{5} \leqslant \alpha_t < \tfrac{3}{5};$$

а теорема 6.3 дает

$$\alpha_{t+1} = \frac{7 + 33\alpha_t}{5(7 + \alpha_t)} \quad \text{при} \quad \tfrac{3}{5} \leqslant \alpha_t < 1.$$

Отсюда

Теорема 6.6 (Дэвенпорт, 1942*a*). *При* $k = 5$ *неравенство* (6.1) *имеет место с*

$$\alpha_2 = \tfrac{2}{5}, \quad \alpha_3 = \tfrac{5}{9}, \quad \alpha_4 = \tfrac{569}{845}, \quad \alpha_8 = \tfrac{6\,913\,439}{7\,576\,115} \; (> 0{,}91253).$$

Пусть теперь $k = 6$. Тогда уравнение (6.12) дает $\alpha_2 = \frac{1}{3}$, следствие из теоремы 6.5 дает

$$\alpha_{t+1} = \frac{19 + 120\alpha_t}{6(19 + 6\alpha_t)} \quad \text{при} \quad \tfrac{1}{3} \leqslant \alpha_t < \tfrac{19}{42};$$

$$\alpha_{t+1} = \frac{43 + 246\alpha_t}{6(43 + 6\alpha_t)} \quad \text{при} \quad \tfrac{19}{42} \leqslant \alpha_t < \tfrac{2}{3},$$

а теорема 6.3 дает

$$\alpha_{t+1} = \frac{15 + 81\alpha_t}{6(15 + \alpha_t)}, \quad \text{если} \quad \tfrac{2}{3} \leqslant \alpha_t < 1.$$

Отсюда

Теорема 6.7 (Дэвенпорт, 1942*a*). *При* $k = 6$ *неравенство* (6.1) *справедливо с*

$$\alpha_2 = \tfrac{1}{3}, \quad \alpha_3 = \tfrac{59}{126}, \quad \alpha_4 = \tfrac{1661}{2886}, \quad \alpha_5 = \tfrac{5549}{8379}, \quad \alpha_6 = \tfrac{575\,117}{787\,182},$$

$$\alpha_{13} = \frac{24\,040\,980\,990\,984\,981}{25\,335\,323\,032\,000\,606} \; (> 0{,}94891).$$

6.2 $G(4)=16$

Здесь полезно ввести обобщенную функцию

$$h(\alpha)=\sum_{X<x\leqslant 2X} e(\alpha x^k) \tag{6.30}$$

и соответствующие вспомогательные функции

$$w(\alpha)=\sum_{X^k<x\leqslant(2X)^k}\frac{1}{k}x^{1/k-1}e(\alpha x) \tag{6.31}$$

и

$$W(\alpha,\ q,\ a)=q^{-1}S(q,\ a)\,w(\alpha-a/q), \tag{6.32}$$

где $S(q, a)$ определяется формулой (4.10). Следующая лемма является непосредственным следствием теоремы 4.1 при $n=[2X]^k$ и $n=[X]^k$.

Лемма 6.1. *Предположим, что* $(a, q)=1$ *и* $\alpha=a/q+\beta$. *Тогда*

$$h(\alpha)-W(\alpha, q, a)\ll q^{1/2+\varepsilon}(1+X^k|\beta|), \tag{6.33}$$

и если, кроме того, $|\beta|\leqslant(2kq)^{-1}(2X)^{1-k}$, *то*

$$h(\alpha)-W(\alpha, q, a)\ll q^{1/2+\varepsilon}. \tag{6.34}$$

Одна из причин такого выбора $h(\alpha)$ состоит в том, что он больше подходит в контексте § 6.1. Другая причина раскрывается следующей леммой, которая показывает, что $h(a/q+\beta)$ убывает как $\|\beta\|^{-1}$ при возрастании $\|\beta\|$, а не как $\|\beta\|^{-1/k}$, что имело место в случае $f(a/q+\beta)$ (см. лемма 4.6). Обычно это не существенно, но часто может способствовать уменьшению технических трудностей.

Лемма 6.2. *Пусть* $|\beta|\leqslant\frac{1}{2}$. *Тогда*

$$w(\beta)\ll X(1+X^k|\beta|)^{-1}.$$

Доказывается тем же способом, что и лемма 2.8. Отсюда и из теоремы 4.2 непосредственно следует

Лемма 6.3. *Предположим, что* $(q, a)=1$. *Тогда*

$$W(a/q+\beta, q, a)\ll Xq^{-1/k}(1+X^k\|\beta\|)^{-1}.$$

Следующая теорема принадлежит Дэвенпорту (1939c) и до сих пор является лучшим известным результатом для четвертых степеней. Упражнение 2.2 дает $G(4)\geqslant 16$.

Теорема 6.8. *Предположим, что* $n\not\equiv 0$ *или* $-1\,(\mathrm{mod}\,16)$ *и* n *достаточно велико. Тогда* n *является суммой четырнадцати четвертых степеней.*

Следствие. $G(4) = 16$.

Доказательство теоремы 6.8. Выберем h_1, h_2, j такими, что
$h_1 + h_2 + j \equiv n \pmod{16}$, $0 \leqslant h_1 \leqslant 4$, $0 \leqslant h_2 \leqslant 4$, $1 \leqslant j \leqslant 6$

Пусть
$$\nu = \frac{243}{1567}, \quad X = \tfrac{1}{2} n^{1/4}, \tag{6.35}$$

и пусть $\mathscr{A}(h)$ означает множество натуральных чисел a, таких, что $a \leqslant X^{3+\nu}$, $a \equiv h \pmod{16}$ и a есть сумма четырех четвертых степеней. Далее, пусть

$$V_r(\alpha) = \sum_{a \in \mathscr{A}(h_r)} e(\alpha a).$$

Тогда по теореме 6.4
$$V_r(0) > X^{\mu - \varepsilon}, \quad \mu = \frac{3972}{1567}. \tag{6.36}$$

Согласно (6.30) (с $k = 4$),

$$\int_0^1 |h(\alpha) V_r(\alpha)|^2 \, d\alpha = \sum_m Q(m)^2,$$

где $Q(m)$ — число решений уравнения

$$x^4 + a = m$$

с $X < x < 2X$ и $a \in \mathscr{A}(h_r)$. Отсюда в силу теоремы 6.2 с $k = 4$, $j = 2$

$$\int_0^1 |h(\alpha) V_r(\alpha)|^2 \, d\alpha \ll X V_r(0) \left(1 + X^{\nu+\varepsilon} \left(X^{-2} + X^{-\nu-3} V_r(0)\right)^{1/4}\right).$$

Следовательно, по (6.36) и неравенству Коши

$$\int_0^1 |h(\alpha)^2 V_1(\alpha) V_2(\alpha)| \, d\alpha \ll X^2 V_1(0) V_2(0) X^{\varepsilon - \gamma}, \quad \gamma = \frac{5539}{1567}. \tag{6.37}$$

Определим большие дуги $\mathfrak{M}(q, a)$, полагая $P = (2X)/(2k) = X/k$ и

$$\mathfrak{M}(q, a) = \{\alpha\colon |\alpha - a/q| \leqslant P q^{-1} n^{-1}\}.$$

Пусть $\mathfrak{M}$ — объединение всех $\mathfrak{M}(q, a)$ с $1 \leqslant a \leqslant q \leqslant P$ и $(a, q) = 1$. Тогда $\mathfrak{M}(q, a)$ не пересекаются и лежат в интервале $\mathscr{U} = (Pn^{-1}, 1 + Pn^{-1}]$.

Пусть $\mathfrak{m} = \mathscr{U} \setminus \mathfrak{M}$. В силу неравенства Вейля (лемма 2.4) и рассуждений, использованных при доказательстве теоремы 2.1,

$$h(\alpha) \ll X^{7/8+\varepsilon} \quad (\alpha \in \mathfrak{m}).$$

Отсюда ввиду (6.35) и (6.37)

$$\int_{\mathfrak{m}} |h(\alpha)^6 V_1(\alpha) V_2(\alpha)|\, d\alpha \ll n^{1/2-\delta} V_1(0) V_2(0), \tag{6.38}$$

где δ — подходящая положительная постоянная.

Как и в доказательстве теоремы 4.4, для $1 \leqslant m \leqslant n$ получаем

$$\int_{\mathfrak{m}} h(\alpha)^6 e(-\alpha m)\, d\alpha = I(m)\mathfrak{S}(m) + O(n^{1/2-\delta}), \tag{6.39}$$

где

$$I(m) = \sum_{\substack{X^4 < x_1 \leqslant (2X)^4 \\ x_1 + \ldots + x_6 = m}} \ldots \sum_{X^4 < x_6 \leqslant (2X)^4} 4^{-6} (x_1 \ldots x_6)^{-3/4},$$

а $\mathfrak{S}(m)$ — особый ряд, определенный в теореме 4.3. Легко проверить, рассматривая $x_1, \ldots, x_5$ с условием $X^4 < x_j \leqslant 2X^4$, что

$$I(m) \gg n^{1/2} \quad \text{при} \quad \tfrac{3}{4} n < m \leqslant n. \tag{6.40}$$

Согласно лемме 2.15, при $s = 6$ и $p > 2$ имеем $M_m^*(p^\gamma) > 0$. Кроме того, при $s = 6$, $p = 2$ и $m \equiv j \pmod{16}$ с $1 \leqslant j \leqslant 6$ из определения M_m^* в § 2.6 тривиально следует, что $M_m^*(2^\gamma) > 0$. Отсюда в силу теоремы 4.5

$$\mathfrak{S}(m) \gg 1 \quad \text{при} \quad m \equiv j \pmod{16}.$$

Если $m = n - a_1 - a_2$, $a_r \in \mathcal{A}(h_r)$, то m удовлетворяет условиям $\frac{3}{4} n < m \leqslant n$ и $m \equiv j \pmod{16}$.

Следовательно, ввиду (6.39) и (6.40)

$$\int_{\mathfrak{m}} h(\alpha)^6 V_1(\alpha) V_2(\alpha) e(-n\alpha)\, d\alpha = J(n) + O(n^{1/2-\delta} V_1(0) V_2(0)),$$

где $J(n) \gg n^{1/2} V_1(0) V_2(0)$. Поэтому, согласно (6.38), для

$$R(n) = \int_0^1 h(\alpha)^6 V_1(\alpha) V_2(\alpha) e(-\alpha n)\, d\alpha$$

имеет место неравенство

$$R(n) \gg n^{1/2} V_1(0) V_2(0) > 0.$$

Следовательно, n является суммой четырнадцати четвертых степеней, что и требовалось доказать.

6.3. Оценки Дэвенпорта $G(5)$ и $G(6)$

Теорема 6.9 (Дэвенпорт, 1942*b*). $G(5) \leqslant 23$, $G(6) \leqslant 36$.

Доказательство этого результата подобно доказательству теоремы 6.8, но несколько проще. В этом случае достаточно применять обозначения § 4.4, так что имеют место формулы (4.29), (4.32).

Пусть $r = 7$, $t = 8$ при $k = 5$ и $r = 10$, $t = 13$ при $k = 6$. Далее, пусть $\mathcal{A}$ обозначает множество натуральных чисел a, не превосходящих $\frac{1}{8}n$ и являющихся суммами t k-х степеней, и

$$V(\alpha) = \sum_{a \in \mathcal{A}} e(\alpha a).$$

В силу теорем 6.6 и 6.7

$$\int_0^1 |V(\alpha)|^2 d\alpha < V(0)^2 n^{-\mu},$$

где $\mu = 0{,}91253$ при $k = 5$ и $\mu = 0{,}94891$, если $k = 6$.

Пусть $\mathfrak{m} = \mathcal{U} \setminus \mathfrak{M}$. Тогда по неравенству Вейля (лемма 2.4)

$$\int_{\mathfrak{m}} |f(\alpha)^r V(\alpha)^2| \, d\alpha \ll n^{r/k-1-\delta} V(0)^2, \tag{6.41}$$

где δ — подходящее фиксированное положительное число.

По теореме 4.4 при $1 \leqslant m \leqslant n$

$$\int_{\mathfrak{M}} f(\alpha)^r e(-\alpha m) \, d\alpha = C m^{r/k-1} \mathfrak{S}(m) + O(n^{r/k-1-\delta}), \tag{6.42}$$

где C — положительное число, зависящее только от k и r.

Из леммы 2.15 с $s = r$, $k = 5$ или 6 и n, замененным на m, имеем $M_m^*(p^\gamma) > 0$. Отсюда по теореме 4.5 $\mathfrak{S}(m) \gg 1$. Из соотношений (6.41) и (6.42) теперь легко следует, что

$$\int_0^1 f(\alpha)^r V(\alpha)^2 e(-\alpha n) \, d\alpha \gg n^{r/k-1} V(0)^2 > 0,$$

и, следовательно, $G(k) \leqslant r + 2t$ при $k = 5$ или 6.

6.4 Упражнения

1. Покажите, что для $X > X_0$

$$N_{19}(X) > X^{0{,}9668} \text{ при } k = 7,$$

$$N_{28}(X) > X^{0{,}9838} \text{ при } k = 8,$$

Выведите, что $G(7) \leqslant 53$ [1]), $G(8) \leqslant 73$.

2. (Дэвенпорт, 1939*a*). Пусть $Q(m)$ означает число решений уравнения $m = x^3 + y^3 + z^3$ с $Z < x \leqslant 2Z$, $Z^{4/5} \leqslant y \leqslant 2Z^{4/5}$, $Z^{4/5} < z \leqslant 2Z^{4/5}$. Покажите, что
$$\sum_m Q(m)^2 \ll Z^{13/5+\varepsilon}.$$
Выведите, что (i) $G(3) \leqslant 8$ и (ii) почти каждое натуральное число есть сумма четырех положительных кубов.

3. (Дэвенпорт, 1950). Покажите, что при $k = 3$
$$N_3(X) > X^{47/54-\varepsilon} \quad (X > X_0(\varepsilon)).$$

---

[1]) Отметим, что в обосновании утверждения $G(7) \leqslant 52$ [Sambasiva Rao, 1941] допущена арифметическая ошибка.

7
Верхняя оценка $G(k)$ И. М. Виноградова

7.1 Некоторые замечания к теореме Виноградова о среднем

В этой главе сохраняются обозначения гл. 5.

По определению (5.3) $J_s^{(k)}(X, 0, \mathbf{h})$ есть число решений системы уравнений

$$\sum_{r=1}^{s} (x_r^j - y_r^j) = h_j \; (1 \leqslant j \leqslant k) \quad \text{с} \quad 0 < x_r,\ y_r \leqslant X. \tag{7.1}$$

Эта система несовместна при $|h_j| \geqslant sX^j$ для какого-либо j. Следовательно, в силу неравенства (5.4)

$$\sum_{h} J_s^{(k)}(X, 0, \mathbf{h}) \ll X^{k(k+1)/2} J_s(X). \tag{7.2}$$

С другой стороны, в левой части (7.2) подсчитываются все решения системы (7.1), где $\mathbf{h}$ рассматривается как дополнительная переменная. Таким образом,

$$J_s(X) \gg X^{2s-k(k+1)/2}.$$

Напомним, что $J_s(X)$ есть число решений системы

$$\sum_{r=1}^{s} (x_r^j - y_r^j) = 0 \;\; (1 \leqslant j \leqslant k) \quad \text{с} \quad 0 < x_r,\ y_r \leqslant X. \tag{7.3}$$

Очевидно, число $T_s(X)$ «тривиальных» решений, получаемых при выборе в качестве y_r перестановки x_r, удовлетворяет неравенствам

$$[X]^s \leqslant T_s(X) \leqslant s! X^s.$$

Таким образом,

$$J_s(X) \gg \max\left(X^{2s-k(k+1)/2},\ X^s\right), \tag{7.4}$$

что указывает, между прочим, на наличие «нетривиальных» решений системы (7.3), когда $s > \frac{1}{2}k(k+1)$ и X достаточно велико. Дальнейшие комментарии см. в § 29 Хуа (1959).

Можно предположить, что, если $k \geqslant 3$ при $X \to \infty$,

$$J_s(X) \sim C_{s,k} \max\left(X^{2s-k(k+1)/2},\ X^s\right). \tag{7.5}$$

Хотя этот результат, вероятно, лежит очень глубоко, его можно получить, во всяком случае, при достаточно большом

$s^{[1]}$. Достигается это путем применения метода Харди — Литтлвуда к k-мерному единичному гиперкубу $\mathcal{U}_k$. На малых дугах применяются теоремы 5.1 и 5.3, которые можно считать аналогами леммы Хуа и неравенства Вейля соответственно [2]. Для больших дуг необходимо получить асимптотическое приближение общей функции

$$f(\alpha) = \sum_{x \leqslant X} e(\alpha_1 x + \ldots + \alpha_k x^k) \tag{7.6}$$

и оценить соответствующие вспомогательные функции

$$I(\beta) = \int_0^X e(\beta_1 \gamma + \ldots + \beta_k \gamma^k)\, d\gamma, \tag{7.7}$$

$$S(q, \mathbf{a}) = S(q, a_1, \ldots, a_k) = \sum_{x=1}^{q} e((a_1 x + \ldots + a_k x^k)/q). \tag{7.8}$$

7.2 Предварительные оценки

Многое из материала этого параграфа принадлежит Хуа (1940*a*, 1952, 1965).

Здесь удобно напомнить определение: полиномиальное сравнение

$$\varphi(x) = b_0 + b_1 x + \ldots + b_k x^k \equiv 0 \pmod p$$

имеет корень x_0 кратности m, если $\varphi(x) = (x - x_0)^m \varphi_1(x) + p\varphi_2(x)$, где $\varphi_1(x)$ и $\varphi_2(x)$ — полиномы, такие, что $p \nmid \varphi_1(x_0)$.

Теорема 7.1. *Предположим, что* $(q, a_1, \ldots, a_k) = 1$. *Тогда*

$$S(q, \mathbf{a}) \ll q^{1-1/k+\varepsilon}.$$

Доказательство. Подобно доказательству леммы 2.10, когда $(q, r) = (qr, a_1, \ldots, a_k) = 1$, сразу имеем

$$S(qr, a_1, \ldots, a_k) = S(q, a_1, ra_2, \ldots, r^{k-1}a_k) \times \\ \times S(r, a_1, qa_2, \ldots, q^{k-1}a_k).$$

Таким образом, достаточно рассмотреть случай, когда q — степень простого числа. Предположим, что $p \nmid (a_1, \ldots, a_k)$ и p^τ является наивысшей степенью p, делящей $(a_1, 2a_2, \ldots, ka_k)$. Пусть $x_1, \ldots, x_r$ означают различные корни сравнения

$$p^{-\tau}(a_1 + 2a_2 x + \ldots + ka_k x^{k-1}) \equiv 0 \pmod p,$$

и предположим, что $m_1, \ldots, m_r$ их соответствующие кратности. Заметим, что $r \leqslant k-1$. Пусть далее $m = m_1 + \ldots$

$\ldots + m_r$. Тогда достаточно показать, что для $l = 1, 2, \ldots$

$$|S(p^l, a_1, \ldots, a_k)| \leqslant k^2 \max(1, m) p^{l-l/k}. \tag{7.9}$$

Поскольку $m \leqslant k-1$, теорема доказана.

Случай $l = 1$. Рассуждения для этого случая принадлежат Морделлу [Mordell, 1932] и дают больше, а именно

$$|S(p, a_1, \ldots, a_k)| \leqslant kp^{1-1/k}. \tag{7.10}$$

Без ограничения общности можно считать, что $p \nmid a_k$ и $p > k$. Рассмотрим

$$T = \sum_{z_1=1}^{p} \ldots \sum_{z_k=1}^{p} |S(p, z_1, \ldots, z_k)|^{2k}. \tag{7.11}$$

Тогда, раскрывая суммируемое произведение, применением (7.8) и переменой порядка суммирования получаем

$$T = p^k M, \tag{7.12}$$

где M — число решений системы сравнений

$$x_1^j + \ldots + x_k^j \equiv y_1^j + \ldots + y_k^j \pmod p \quad (1 \leqslant j \leqslant k) \tag{7.13}$$

с $1 \leqslant x_i \leqslant p$, $1 \leqslant y_i \leqslant p$. Подобно доказательству леммы 5.1, получается, что если $x_1, \ldots, x_k, y_1, \ldots, y_k$ удовлетворяют системе (7.13), то для каждого x $\prod_i (x - x_i) \equiv \prod_i (x - y_i) \pmod p$. Таким образом, $x_1, \ldots, x_k$ представляют собой перестановку $y_1, \ldots, y_k$. Отсюда $M \leqslant k! p^k$, значит, по (7.12)

$$T \leqslant k! p^{2k}. \tag{7.14}$$

При $p \nmid u$, $ux + v$ вместе с x пробегает полную систему вычетов по модулю p. Пусть

$$b_j = b_j(u, v) = \sum_{i=j}^{k} a_i \binom{i}{j} u^j v^{i-j}.$$

Тогда

$$|S(p, a_1, \ldots, a_k)| = |S(p, b_1, \ldots, b_k)|. \tag{7.15}$$

Кроме того, $b_k = a_k u^k$ и $b_{k-1} = u^{k-1}(vka_k + a_{k-1})$. Таким образом, когда u меняется, b_k принимает $(p-1)(k, p-1)^{-1}$ несравнимых по модулю p значений, а для данного u, когда меняется v, b_{k-1} принимает на p несравнимых по модулю p значений. Следовательно, ввиду (7.15) и (7.11)

$$\frac{p(p-1)}{(k, p-1)} |S(p, a_1, \ldots, a_k)|^{2k} \leqslant T.$$

Отсюда, согласно (7.14),

$$|S(p, a_1, \ldots, a_k)|^{2k} \leqslant k!\, 2kp^{2k-2} \leqslant k^{2k} p^{2k-2},$$

что дает (7.10), как и требовалось.

Случай $l > 1$. Доказывается индукцией по l. Очевидно, $p^\tau \leqslant k$. Таким образом, когда $2 \leqslant l \leqslant 2\tau + 1$, (7.9) тривиально. Следовательно, можно предполагать, что $l \geqslant 2\tau + 2$.

Для краткости положим $\varphi(x) = a_1x + \ldots + a_kx^k$. Вспоминая, что $x_1, \ldots, x_r$ — различные решения сравнения $p^{-\tau}\varphi'(x) \equiv 0 \pmod p$, получаем

$$S(p^l, a_1, \ldots, a_k) = T_0 + \sum_{j=1}^{r} T_j, \tag{7.16}$$

где

$$T_j = \sum_{\substack{x=1 \\ x \equiv x_j \pmod p}}^{p^l} e(\varphi(x)p^{-l}) \tag{7.17}$$

и

$$T_0 = \sum_{\substack{y=1 \\ p^{\tau+1} \nmid \varphi'(y)}}^{p^{l-\tau-1}} \sum_{z=1}^{p^{\tau+1}} e(\varphi(p^{l-\tau-1}z + y)p^{-l}). \tag{7.18}$$

Поскольку $l \geqslant 2\tau + 2$, имеем

$$\varphi(p^{l-\tau-1}z + y) \equiv \varphi(y) + p^{l-\tau-1}z\varphi'(y) \pmod{p^l}.$$

Следовательно, внутренняя сумма в (7.18) равна нулю. Таким образом, в (7.16) остается оценить T_j с $j \neq 0$.

При $r = 0$, т. е. $m = 0$, здесь нечего доказывать. Предположим, что $m \geqslant 1$. Когда $l \leqslant k$, тривиальная оценка $|T_j| \leqslant p^{l-1}$ в (7.16) дает

$$|S(p^l, a_1, \ldots, a_k)| \leqslant kp^{l-1} \leqslant kp^{l-l/k}.$$

Таким образом, можно предполагать, что $l > k$.

Рассмотрим полином от x:

$$\varphi(px + x_j) - \varphi(x_j) = b_1x + \ldots + b_kx^k,$$

где

$$b_i = p^i \sum_{h=i}^{k} a_h \binom{h}{i} x_j^{h-i}.$$

Пусть p^ρ означает наивысшую степень p, делящую $(b_1, b_2, \ldots, b_k)$. Очевидно, $\rho \geqslant 1$. Если $\rho > k$, то

$$p \,\Big|\, \sum_{h=i}^{k} a_h \binom{h}{i} x_j^{h-i} \quad (1 \leqslant i \leqslant k)$$

и, следовательно, $p \mid a_k$, $p \mid a_{k-1}, \ldots, p \mid a_1$ в противоречие тому, что $(p, a_1, \ldots, a_k) = 1$. Таким образом,

$$\rho \leqslant k < l. \tag{7.19}$$

Пусть $c_i = b_ip^{-\rho}$ и

$$\psi(x) = p^{-\rho}(\varphi(px + x_j) - \varphi(x_j)) = c_1x + \ldots + c_kx^k.$$

Тогда, согласно (7.17),

$$|T_j| = p^{\rho-1} |S(p^{l-\rho}, c_1, \ldots, c_k)|. \tag{7.20}$$

Так как $p^{-\tau}\varphi'(x) \equiv 0 \pmod p$ имеет корень x_j кратности m_j, $p^{-\tau}\varphi'(x)$ можно записать в виде

$$p^{-\tau}\varphi'(x) = (x - x_j)^{m_j} \varphi_1(x) + p\varphi_2(x),$$

где $p \nmid \varphi_1(x_j)$ и $\deg \varphi_2 < m_j$. Пусть теперь p^σ означает наивысшую степень p, делящую $(c_1, 2c_2, \ldots, kc_k)$. Тогда

$$p^{-\sigma}\psi'(x) = p^{1-\sigma-\rho}\varphi'(px + x_j) =$$
$$= p^{1-\sigma-\rho+\tau}\left(p^{m_j}x^{m_j}\varphi_1(px + x_j) + p\varphi_2(px + x_j)\right).$$

Все коэффициенты этого полинома целые и по крайней мере один взаимно прост с p. Так как $\deg \varphi_2 < m_j$, коэффициент при x^{m_j} равен

$$p^{1-\sigma-\rho+\tau+m_j}\varphi_1(x_j),$$

так что $\sigma + \rho \leqslant 1 + \tau + m_j$. Отсюда если $d > m_j$, то коэффициент при x^d делится на p. Поэтому

$$p^{-\sigma}\psi'(x) \equiv p^{1-\sigma-\rho+\tau}\left(p^{m_j}x^{m_j}\varphi_1(x_j) + p\varphi_2(px + x_j)\right) \pmod p.$$

Следовательно, степень $p^{-\sigma}\psi'(x)$ по модулю p не превышает m_j и число решений сравнения

$$p^{-\sigma}\psi'(x) \equiv 0 \pmod p$$

не больше m_j.

Отсюда, согласно предположению индукции (7.9) с заменой l на $l - \rho$, a_j на c_j, m на m_j, при помощи (7.19) и (7.20) получается, что

$$|T_j| \leqslant k^2 m_j p^{\rho-1} p^{(l-\rho)(1-1/k)} \leqslant k^2 m_j p^{l-l/k}.$$

Желаемое утверждение, неравенство (7.9), следует теперь из (7.16) суммированием по всем $j \geqslant 1$.

Следующая теорема дает асимптотическое представление f на больших дугах.

Теорема 7.2. *Пусть* $\alpha_j = a_j/q_j + \beta_j$ $(j = 1, \ldots, k)$, *и предположим, что* $q = [q_1, \ldots, q_k]$ *и* $A_j = a_j q q_j^{-1}$. *Тогда*

$$f(\boldsymbol{\alpha}) = q^{-1} S(q, \mathbf{A}) I(\boldsymbol{\beta}) + \Delta,$$

где $\Delta \ll q(1 + |\beta_1| X + \ldots + |\beta_k| X^k)$.

Доказательство. В силу леммы 2.6 с

$$c_x = e\left((A_1 x + \ldots + A_k x^k) q^{-1}\right)$$

и

$$F(\gamma) = e(\beta_1 \gamma + \ldots + \beta_k \gamma^k)$$

и замечания

$$\sum_{x\leqslant\gamma} c_x = \sum_{y=1}^{q} e\left(\left(A_1 y + \ldots + A_k y^k\right) q^{-1}\right) \sum_{\substack{x\leqslant\gamma \\ x\equiv y \pmod q}} 1 = \\ = \gamma q^{-1} S(q, \mathbf{A}) + O(q)$$

получается

$$f(\alpha) = q^{-1} S(q, A) \left(F(X) X - \int_0^X F'(\gamma)\gamma\, d\gamma \right) + \Delta,$$

где

$$\Delta \ll q \left(1 + \int_0^X |\beta_1 + \ldots + k\beta_k \gamma^{k-1}|\, d\gamma \right).$$

Интегрирование по частям сразу дает теорему.

Теорема 7.3. [3] *Для вспомогательной функции* $I(\beta)$ *справедлива оценка*

$$I(\beta) \ll X(1 + |\beta_1| X + \ldots + |\beta_k| X^k)^{-1/k}.$$

Доказательство. Можно предполагать, что $X = 1$, ибо общий случай следует тогда с помощью замены переменной. Далее, можно предполагать, что

$$|\beta_1| + \ldots + |\beta_k| \geqslant 1,$$

так как в противном случае результат тривиален. Пусть

$$Y_j = (|\beta_j| + \ldots + |\beta_k|)^{1/k},$$

$$p_1(\alpha) = \beta_1 + 2\beta_2\alpha + \ldots + k\beta_k\alpha^{k-1}$$

и

$$\mathscr{A} = \{\alpha\colon\ 0 \leqslant \alpha \leqslant 1,\ |p_1(\alpha)| \geqslant Y_1\}.$$

Тогда $\mathscr{A}$ можно разбить на $\ll 1$ интервалов, на каждом из которых $p_1'(\alpha)$ не меняет знак. Пусть $\mathscr{B}$ — интервал такого типа. Тогда интегрирование по частям дает

$$\int_{\mathscr{B}} e\left(\beta_1\alpha + \ldots + \beta_k\alpha^k\right) d\alpha \ll Y_1^{-1}.$$

Таким образом, остается показать, что для

$$\mathscr{C}_1 = \{\alpha\colon\ 0 \leqslant \alpha \leqslant 1,\quad |p_1(\alpha)| < Y_1\}$$

имеет место оценка

$$\operatorname{meas}(\mathscr{C}_1) \ll Y_1^{-1}. \tag{7.21}$$

Доказательство дальше ведется при помощи повторных построений последовательности следующих множеств: $\mathscr{D}_1$, $\mathscr{C}_2$, $\mathscr{D}_2$, $\mathscr{C}_3$, ... Если $\mathscr{C}_1$ пусто, то здесь больше нечего доказывать. Таким образом, можно предположить, что существует α_1, такое, что $0 \leqslant \alpha_1 \leqslant 1$ и $|p_1(\alpha_1)| < Y_1$. Теперь $|p_1(\alpha_1)| \geqslant \geqslant |\beta_1| - kY_2^k$, так что если $|\beta_1| > 2kY_2^k$, то $\frac{1}{2}|\beta_1| < (|\beta_1| + Y_2^k)^{1/k} < ((1 + 1/(2k))|\beta_1|)^{1/k}$. Откуда

$$Y_2^k \ll |\beta_1| \ll 1.$$

Следовательно, в этом случае (7.21) тривиально. Таким образом, можно предполагать, что для подходящего числа C_1, зависящего самое большее от k, имеют место неравенства $|\beta_1| \leqslant C_1 Y_2^k$ и $|p_1(\alpha)| < C_1 Y_2$ для каждого $\alpha \in \mathscr{C}_1$. Следовательно, достаточно показать, что

$$\operatorname{meas}(\mathscr{D}_1) \ll Y_2^{-1},$$

где

$$\mathscr{D}_1 = \{\alpha:\ 0 \leqslant \alpha \leqslant 1,\ |\alpha - \alpha_1| > Y_2^{-1},\ |p_1(\alpha)| < C_1 Y_2\}.$$

Пусть

$$p_2(\alpha) = \frac{p_1(\alpha) - p_1(\alpha_1)}{\alpha - \alpha_1}.$$

Тогда $\mathscr{D}_1 \subset \mathscr{C}_2$, где

$$\mathscr{C}_2 = \{\alpha:\ 0 \leqslant \alpha \leqslant 1,\ |p_2(\alpha)| < 2C_1 Y_2^2\}.$$

Продолжая таким же способом, на j-м шаге получаем константу C_{j-1}, полином $p_j(\alpha)$ степени $k-j$ и рассматриваем множество

$$\mathscr{C}_j = \{\alpha:\ 0 \leqslant \alpha \leqslant 1, \quad |p_j(\alpha)| < 2C_{j-1} Y_j^j\}.$$

Если $\mathscr{C}_j$ не пусто, то существует α_j, такое, что

$$|p_j(\alpha_j)| < 2C_{j-1} Y_j^j.$$

Определяя на каждом шаге

$$p_{j+1}(\alpha) = \frac{p_j(\alpha) - p_j(\alpha_j)}{\alpha - \alpha_j},$$

убеждаемся, что

$$p_j(\alpha) = \sum_{h=0}^{k-j} \gamma_h^{(j)} \alpha^h,$$

где

$$\gamma_h^{(j)} = \sum_{i=h}^{k-j} \gamma_{i+1}^{(j-1)} \alpha_{j-1}^{i-h}$$

и

$$\gamma_h^{(1)} = (h+1)\beta_{h+1}.$$

Таким образом,

$$\gamma_0^{(j)} = j\beta_j + O(|\beta_{j+1}| + \cdots + |\beta_k|),$$

и, следовательно, можно предполагать, что существует число C_j, зависящее, возможно, только от k, такое, что

$$|\beta_j| \leqslant C_j Y_{j+1}^k \tag{7.22}$$

и $|p_j(\alpha)| < C_j Y_{j+1}^j$ для каждого $\alpha \in \mathscr{C}_j$. Пусть

$$\mathscr{D}_j = \{\alpha\colon\ 0 \leqslant \alpha \leqslant 1,\ |\alpha - \alpha_j| > Y_{j+1}^{-1},\ |p_j(\alpha)| < C_j Y_{j+1}^j\}.$$

Тогда, согласно (7.22), требуется показать, что $\operatorname{meas}(\mathscr{D}_j) \ll \ll Y_{j+1}^{-1}$.

Процесс может прекратиться, в случае, если для некоторого $j \leqslant k-2$ множество $\mathscr{C}_j$ пусто или нарушается неравенство (7.22). В других случаях $j \leqslant k-2$ имеет место включение $\mathscr{D}_j \subset \mathscr{C}_{j+1}$, и процесс продолжается до $\mathscr{D}_{k-1}$. Теперь

$$\gamma_1^{(k-1)} = k\beta_k.$$

Таким образом,

$$\mathscr{D}_{k-1} \subset \{\alpha\colon\ |\gamma_0^{(k-1)} k^{-1} \beta_k^{-1} + \alpha| < C_{k-1} |\beta_k|^{-1/k}\},$$

так что

$$\operatorname{meas}(\mathscr{D}_{k-1}) \ll Y_k^{-1},$$

как и требовалось.

7.3 Асимптотическая формула для $J_s(X)$

Теорема 7.4. *Существуют положительная постоянная C_1 и положительные числа $\delta(k)$ и $C_2(k, s)$, такие, что для $s \geqslant \geqslant k^2(3\log k + \log\log k + C_1)$ имеем*

$$J_s(X) = C_2(k, s) X^{2s - k(k+1)/2} + O(X^{2s-k(k-1)/2-\delta(k)}).$$

Доказательство. Пусть X — большое действительное число, пусть

$$\lambda = \frac{1}{2k}, \quad Q_1 = X^{1/2}, \quad Q_j = X^{j-\lambda} \quad (2 \leqslant j \leqslant k), \tag{7.23}$$

и пусть $\mathscr{U}_k^*$ — декартово произведение интервалов $(Q_j^{-1}, 1 + Q_j^{-1}]$. Для $q_1 \leqslant \frac{1}{2} X^{1/2}$, $q_j \leqslant X^\lambda$ $(2 \leqslant j \leqslant k)$ и $1 \leqslant a_j \leqslant q_j$ с $(q_j, a_j) = 1$ пусть $\mathfrak{M}(\mathbf{q}, \mathbf{a})$ означает декартово произведение интервалов

$$\{\alpha\colon\ |\alpha - a_j/q_j| \leqslant q_j^{-1} Q_j^{-1}\}.$$

Большие дуги $\mathfrak{M}(\mathbf{q}, \mathbf{a})$ попарно не пересекаются и содержатся в $\mathscr{U}_k^*$. Пусть $\mathfrak{M}$ означает их объединение. Тогда малые дуги задаются формулой $\mathfrak{m} = \mathscr{U}_k^* \setminus \mathfrak{M}$.

Согласно лемме 2.1, для каждого $\boldsymbol{\alpha} \in \mathscr{U}_k^*$ существуют $\mathbf{q}$, $\mathbf{a}$, такие, что $(q_j, a_j) = 1$, $|\alpha_j - a_j/q_j| \leqslant q_j^{-1} Q_j^{-1}$ и $q_j \leqslant Q_j$. Пусть

$\mathfrak{n}$ означает множество $\alpha \in \mathcal{U}_k^*$, для которых к тому же $q_j > X^\lambda$ при некотором j, $2 \leqslant j \leqslant k$. Тогда по теореме 5.3 с $l = [4k \log k]$ существует положительная константа C_3, такая, что

$$f(\alpha) \ll X^{1-\rho} (\alpha \in \mathfrak{n}) \quad \text{с} \quad \rho^{-1} = C_3 k^3 \log k. \tag{7.24}$$

Пусть теперь $\mathfrak{N}$ означает множество $\alpha \in \mathcal{U}_k^*$, для которых существуют $\mathbf{q}$, $\mathbf{a}$, такие, что $(q_j, a_j) = 1$, $|\alpha_j - a_j/q_j| \leqslant q_j^{-1} Q_j^{-1}$, $q_1 \leqslant Q_1$, $q_j \leqslant X^\lambda$ $(2 \leqslant j \leqslant k)$. Таким образом, $\mathfrak{n} \cup \mathfrak{N} = \mathcal{U}_k^*$ (хотя $\mathfrak{n} \cap \mathfrak{N}$ может не быть пустым) и $\mathfrak{M} \subset \mathfrak{N}$. Пусть $\beta_j = \alpha_j - a_j/q_j$, $q = [q_1, \ldots, q_k]$, $A_j = q a_j / q_j$, так что

$$(q, A_1, \ldots, A_k) = 1. \tag{7.25}$$

По теореме 7.2 и (7.23)

$$f(\alpha) - q^{-1} S(q, \mathbf{A}) I(\beta) \ll$$
$$\ll q_1 \ldots q_k \left(1 + X^{1/2} q_1^{-1} + X^\lambda q_2^{-1} + \ldots + X^\lambda q_k^{-1}\right) \ll X^{1-\lambda}. \tag{7.26}$$

Если $\alpha \in \mathfrak{m}\mathfrak{n}$, так что $\alpha \notin \mathfrak{M}$, то $q \geqslant q_1 > \frac{1}{2} X^{1/2}$.

Следовательно, согласно теореме 7.1 и (7.7),

$$q^{-1} S(q, \mathbf{A}) I(\beta) \ll X q^{\varepsilon - 1/k} \ll X^{1-\lambda+\varepsilon}.$$

Следовательно, оценка (7.24) справедлива при замене $\mathfrak{m}$ на $\mathfrak{n}$. Пусть $m = [C_3] + 1$ и $\eta = \frac{1}{2} k^2 (1 - 1/k)^t$. Тогда, по теореме 5.1,

$$\int_{\mathfrak{m}} |f(\alpha)|^{2tk + 2mk^2} d\alpha \ll X^{2tk + 2mk^2 - k(k+1)/2 + \eta - 2mk^2\rho}.$$

Кроме того, для $t \geqslant 3k \log k + k \log\log k$ имеем

$$\eta - 2mk^2\rho < k^2 \left(1 - \frac{1}{k}\right)^t - \frac{1}{k \log k} < 0,$$

и, следовательно, при $s \geqslant tk + mk^2$, существует положительное число $\delta = \delta(k)$, такое, что

$$\int_{\mathfrak{m}} |f(\alpha)|^{2s} d\alpha \ll X^{2s - k(k+1)/2 - \delta}.$$

Остается, следовательно, рассмотреть большие дуги $\mathfrak{M}$. Для $\alpha \in \mathfrak{M}(\mathbf{q}, \mathbf{a})$ (7.26) справедливо. Определим $V(\alpha) = V(\alpha, q, a)$, если $\alpha \in \mathfrak{M}(q, a)$ и $V(\alpha) = 0$ при $\alpha \in \mathfrak{m}$. Тогда

$$\int_{\mathfrak{M}} \left| f(\alpha)^{2s} - V(\alpha)^{2s} \right| d\alpha \ll X^{2-\lambda} \int_{\mathcal{U}_k^*} \left(|f(\alpha)|^{2s-2} + |V(\alpha)|^{2s-2} \right) d\alpha. \tag{7.27}$$

По теореме 5.1, если $s-1 \geqslant kl$ с $l \geqslant 3k\log k$, то

$$\int\limits_{\mathfrak{U}_k^*} |f(\alpha)|^{2s-2}\,d\alpha \ll X^{2s-2-k(k+1)/2+\eta},$$

где $\eta = \frac{1}{2}k^2(1-1/k)^l < 1/(2k) = \lambda$. Следовательно, существует положительное число $\delta = \delta(k)$, такое, что

$$X^{2-\lambda}\int\limits_{\mathfrak{U}_k^*} |f(\alpha)|^{2s-2}\,d\alpha \ll X^{2s-k(k+1)/2-\delta}. \tag{7.28}$$

Пусть $\alpha \in \mathfrak{M}(\mathbf{q}, \mathbf{a})$. Тогда, по (7.25) и теоремам 7.1 и 7.3,

$$V(\alpha) \ll Xq^{\varepsilon-1/k}(1+|\beta_1|X+\ldots+|\beta_k|X^k)^{-1/k}.$$

Отсюда

$$\int\limits_{\mathfrak{U}_k^*} |V(\alpha)|^{2t}\,d\alpha \ll X^{2t}WZ,$$

где

$$W = \sum_{q_1=1}^{\infty}\ldots\sum_{q_k=1}^{\infty} q_1\ldots q_k[q_1,\ldots,q_k]^{2t(\varepsilon-1/k)}$$

и

$$Z = \prod_{j=1}^{k}\int\limits_0^{\infty}(1+\beta_jX^j)^{-2t/k^2}\,d\beta_j.$$

При $t > 2k^2$ имеем

$$W \ll \sum_{q_1=1}^{\infty}\ldots\sum_{q_k=1}^{\infty} q_1\ldots q_k(q_1\ldots q_k)^{-4} < \infty$$

и

$$Z \ll \prod_{j=1}^{k} X^{-j} = X^{-k(k+1)/2}.$$

Следовательно, для $s-1 > 2k^2$

$$X^{2-\lambda}\int\limits_{\mathfrak{U}_k^*} |V(\alpha)|^{2s-2}\,d\alpha \ll X^{2s-k(k+1)/2-\lambda}.$$

Эта оценка в совокупности с (7.27) и (7.28) показывает, что если s удовлетворяет предположению теоремы при подходящем выборе C_1, то

$$\int\limits_{\mathfrak{M}} |f(\alpha)|^{2s}\,d\alpha = \int\limits_{\mathfrak{M}} |V(\alpha)|^{2s}\,d\alpha + O\left(X^{2s-k(k+1)/2-\delta}\right).$$

Непосредственно из теорем 7.1 и 7.3 следует, что

$$\int\limits_{\mathfrak{M}} |V(\alpha)|^{2s}\, d\alpha = \mathfrak{S} J X^{2s-k(k+1)/2} + O\left(X^{2s-k(k+1)/2-\delta}\right),$$

где

$$\mathfrak{S} = \sum_{q_1=1}^{\infty} \dots \sum_{q_k=1}^{\infty} \sum_{\substack{a_1=1 \\ (a_1,\, q_1)=1}}^{q_1} \dots \sum_{\substack{a_k=1 \\ (a_k,\, q_k)=1}}^{q_k} |q^{-1} S(q, A_1, \dots, A_k)|^{2s}$$

и

$$J = \int\limits_{\mathbf{R}^k} \left| \int\limits_0^1 e(\beta_1\alpha + \dots + \beta_k\alpha^k)\, d\alpha \right|^{2s} d\beta.$$

Заметим, что $q^{-1}S(q, A_1, \dots, A_k) = (q_1 \dots q_k)^{-1} S(q_1 \dots q_k, a_1, \dots, a_k)$. К тому же $\mathfrak{S} < \infty$, $J < \infty$ [4], и поэтому теорема справедлива с $C_2(k, s) = \mathfrak{S}J$. Положительность $C_2(k, s)$ является следствием (7.4).

Более подробный анализ и различные приложения полученной теоремы см. Хуа (1965).

7.4 Верхняя оценка $G(k)$ И. М. Виноградова

В качестве применения теоремы 7.4 теперь можно показать, что

$$\limsup_{k\to\infty} \frac{G(k)}{k \log k} \leqslant 2.$$

Во многих отношениях доказательство опирается на идеи § 5.4.

Пусть n означает большое натуральное число и

$$N = [n^{1/k}].$$

Пусть K — натуральное число с условием

$$2K < k$$

и

$$U_1 = \left[\tfrac{1}{2} N^{1/2}\right], \quad V_1 = \left[U_1^{1/2}\right], \quad \eta = \frac{2k - 2K - 1}{2k - 1},$$

$$U_{j+1} = \left[U_j^{\eta}\right], \quad V_j = \left[U_j^{1/2}\right], \quad X = \tfrac{1}{2} N^{1/2}. \tag{7.29}$$

Теперь пусть $Q(m)$ означает число решений уравнения

$$(U_1 + x_1)^k + \dots + (U_l + x_l)^k = m$$

с $x_j \leqslant V_j$, где l — параметр, который будет определен подходящим образом в зависимости от k позднее.

Рассмотрим

$$W(\alpha)=\sum_{X/2<p\leqslant X}\sum_m Q(m)\,e(\alpha p^k m).$$

По неравенству Гёльдера для любого натурального числа r

$$W(\alpha)^{2r}\ll X^{2r-1}\sum_{X/2<p\leqslant X}\Bigl|\sum_m Q(m)\,e(\alpha p^k m)\Bigr|^{2r}=$$

$$=X^{2r-1}\sum_{X/2<p\leqslant X}\sum_h Q_1(h)\,e(\alpha p^k h),$$

где
$$Q_1(h)=\sum_{m_1,\,\ldots,\,m_{2r}}Q(m_1)\,\ldots\,Q(m_{2r})$$

и суммирование ведется по $m_1,\ldots,m_{2r}$ с условием

$$m_1+\ldots+m_r-m_{r+1}-\ldots-m_{2r}=h.$$

Следовательно, в обозначениях § 4.4 и 5.3 по лемме 5.4

$$W(\alpha)^{2r}\ll X^{2r-1}\Bigl(XU_1^{k+\varepsilon}\sum_h Q_1(h)^2\Bigr)^{1/2}\quad(\alpha\in\mathfrak{m}).\qquad(7.30)$$

Сумма $\sum_h Q_1(h)^2$ является числом решений уравнения

$$\sum_{j=1}^{l}L_j(\mathbf{x}_j)=0,\qquad(7.31)$$

где $\mathbf{x}_j\in[1,\ V_j]^{4r}$ и

$$L_j(\mathbf{y})=(U_j+y_1)^k+\ldots+(U_j+y_{2r})^k-$$
$$-(U_j+y_{2r+1})^k-\ldots-(U_j+y_{4r})^k.\qquad(7.32)$$

Оценка $Q_1(h)$ опирается на лемму, в доказательстве которой используется теорема 7.4.

Лемма 7.1. *Предположим, что $r>CK^2\log K$, где C — подходящая постоянная. Тогда число R_j различных $\mathbf{y}$ в $[1,\ V_j]^{4r}$ для которых $L_j(\mathbf{y})$ лежит в данном интервале длины $U_j^{k-K-1/2}$, удовлетворяет неравенству*

$$R_j\ll V_j^{4r}U_j^{-K}.$$

Доказательство. Для краткости параметр j будем опускать. По биномиальной теореме

$$L(\mathbf{y})=\sum_{l=1}^{k}\binom{k}{l}U^{k-l}M_l(\mathbf{y}),$$

где
$$M_l(\mathbf{y})=y_1^l+\ldots+y_{2r}^l-y_{2r+1}^l-\ldots-y_{4r}^l.$$

Так как $\mathbf{y} \in [1, V]^{4r}$ и $V = [U^{1/2}]$, имеем

$$\sum_{i=2K+1}^{k} \binom{k}{i} U^{k-i} M_i(\mathbf{y}) \ll U^{k-2K-1} V^{2K+1} \ll U^{k-K-1/2}.$$

Следовательно, достаточно показать, что число R^* различных $\mathbf{y}$ из $[1, V]^{4r}$, для которых

$$\sum_{i=1}^{2K} \binom{k}{i} U^{k-i} M_i(\mathbf{y})$$

лежит в заданном интервале длины U^{k-K}, удовлетворяет оценке

$$R^* \ll V^{4r-1} U^{1-2K}. \qquad (7.33)$$

Рассмотрим число R^{**} $2K$-мерных векторов с целыми компонентами $z_1, \ldots, z_{2K}$ с $z_i \ll V^i$, для которых

$$\sum_{i=1}^{2K} U^{k-i} z_i$$

лежат в заданном интервале длины U^{k-2K}. Этот интервал можно записать в виде

$$((u-1) U^{k-2K} + v,\ u U^{k-2K} + v),$$

где u и v — целые, $0 \leqslant v < U^{k-2K}$. Тогда

$$z_{2K} \equiv u \pmod U, \quad z_{2K+1} \equiv (u - z_{2K}) U^{-1} \pmod U$$

и т. д. Таким образом, z_{2K} определяется модулем U, z_{2K-1} определяется модулем U по z_{2K} и т. д. до z_2. Более того, поскольку $0 \leqslant v < U^{k-2K}$, z_1 единственным образом определяется по $z_{2K}, \ldots, z_2$. Следовательно, вспоминая, что $V^2 \gg U$, имеем

$$R^{**} \ll (V^{2K} U^{-1})(V^{2K-1} U^{-1}) \ldots (V^2 U^{-1}) = V^{K(2K+1)-1} U^{1-2K}. \qquad (7.34)$$

Согласно теореме 7.4, для заданных $z_1, \ldots, z_{2K}$ число решений системы

$$\binom{k}{i} M_i(\mathbf{y}) = z_i \quad (1 \leqslant i \leqslant 2K) \quad \text{с} \quad \mathbf{y} \in [1, V]^{4r}$$

есть $\ll V^{4r-K(2K+1)}$. Это совместно с (7.34) дает оценку (7.33), а следовательно, и лемму.

Здесь и далее будем предполагать, что условия леммы выполняются, и пусть $\mathbf{x}_1, \ldots, \mathbf{x}_l$ — типичное решение уравнения (7.31). По (7.32) для $\mathbf{x}_{j+1} \in [1, V_{j+1}]^{4r}$ имеем

$$L_{j+1}(\mathbf{x}_{j+1}) \ll U_{j+1}^{k-1} V_{j+1} \ll U^{k-K-1/2},$$

Отсюда по (7.29) $L_1(\mathbf{x}_1)$ лежит в интервале длины $\ll U_1^{k-K-1/2}$. Таким образом, в силу леммы 7.1 для $\mathbf{x}_1$ имеется $\ll V_1^{4r}U_1^{-K}$ значений. Тогда для данного $\mathbf{x}_1$ $L_2(\mathbf{x}_2)$ лежит в интервале длины $U_2^{k-K-1/2}$ и т. д. Следовательно, общее число значений $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_l$ есть величина

$$\ll (V_1 \ldots V_l)^{4r} (U_1 \ldots U_l)^{-K}.$$

По определению (7.29) $(U_1 \ldots U_l)^K \gg U_1^{(k-1/2)(1-\eta^l)}$. Следовательно, согласно (7.29) и (7.30), для $\alpha \in \mathfrak{m}$

$$W(\alpha) \ll XV_1 \ldots V_l \left(X^{-1}U^{k+\varepsilon-(k-1/2)(1-\eta^l)}\right)^{1/(4r)} \ll W(0)\, N^{\varepsilon-\rho},$$

где
$$\rho = \frac{1}{16r} - \frac{1}{8r}\left(k - \tfrac{1}{2}\right)\eta^l.$$

Возьмем теперь

$$K = \left[\tfrac{1}{2}\log k\right], \quad l = 3k, \quad r = 1 + [CK^2 \log K]. \tag{7.35}$$

Тогда по (7.29)

$$\eta^l = \exp\left(l \log\left(1 - \frac{K}{k - \frac{1}{2}}\right)\right) \ll \exp\left(-3\left[\tfrac{1}{2}\log k\right]\right) \ll k^{-3/2},$$

где включаемые в $\ll$ постоянные являются абсолютными. Таким образом, если k достаточно велико,

$$\rho > \frac{1}{C_1 (\log k)^3} = \sigma,$$

скажем, где C_1 — подходящая постоянная. Таким образом, в обозначениях § 5.4 (но с $W(\alpha)$, как выше)

$$\int\limits_{\mathfrak{m}} f(\alpha)^{4k} H(\alpha)^2 W(\alpha)\, e(-\alpha n)\, d\alpha \ll H(0)^2 W(0)\, n^{3+(1-1/k)^t-\sigma/k}.$$

Оптимальный выбор t, так что $(1 - 1/k)^t < \sigma/k$, дает

$$t \sim k \log k.$$

Тогда оценка на малых дугах имеет вид

$$\ll H(0)^2 W(0)\, n^{3-\delta},$$

где $\delta = \delta(k)$ — подходящее положительное число.

Большие дуги могут быть рассмотрены так же, как в § 5.4. Следовательно,

$$G(k) \leqslant 2t + 4k + l.$$

Это вместе с (7.35) показывает, что справедлива

Теорема 7.5. *При* $k \to \infty$, $G(k) \leqslant k(\log k)(2 + o(1))$. *Для больших* k *это лучшая из известных верхняя оценка* $G(k)$.

7.5 Упражнения

1. Покажите, что при $s \leqslant k$ $J_s(X) = s!X^s + O(X^{s-1})$.
2. Покажите, что при $k = 2$ $J_3(X) \ll X^3 \log X$ и что (7.5) неверно.
3. Пусть $G_1(k)$[5] означает наименьшее s, такое, что почти каждое натуральное число является суммой s k-х степеней. Покажите, что

$$\limsup_{k \to \infty} \frac{G_1(k)}{k \log k} \leqslant 1.$$

Примечания редактора

[1] Оценки $J_s(X)$ при малых s см. в статье Архипова Г. И. и Карацубы А. А. (1978).

[2] Доказательство теоремы 7.4 об асимптотической формуле для $J_s(X)$ при $s \sim 3k^2 \log k$ существенно опирается на теорему И. М. Виноградова о среднем.

[3] Эта теорема принадлежит И. М. Виноградову, см., например [1], с. 27.

[4] Сходимость (расходимость) $\mathfrak{S}$ при $2s > \frac{k^2+k}{2} + 2$ $\left(2s \leqslant \frac{k^2+k}{2} + 2\right)$ доказана Хуа (1952); сходимость (расходимость) J при $2s > \frac{k^2+k}{2} + 1$ $\left(2s \leqslant \frac{k^2+k}{2} + 1\right)$ доказана Архиповым Г. И., Карацубой А. А., Чубариковым В. Н. в работе «Тригонометрические интегралы». Изв. АН СССР, сер. матем. 1979, 43 : 5, с. 971—1003.

[5] Д. Гильберт около 1909 г. поставил задачу о представимости k натуральных чисел $N_1, N_2, \ldots, N_k$ суммами соответственно первых, вторых, ..., наконец, k-х степеней одних и тех же натуральных слагаемых (проблема Гильберта — Камке); если через $G_0(k)$ обозначить максимальное число слагаемых в таком представлении, то Архипов доказал, что $2^k - 1 \leqslant G_0(k) \leqslant 3k^3 2^k$; см., Архипов Г. И. О проблеме Гильберта — Камке. Изв. АН СССР, сер. матем., 1984, 48 : 1, с. 3—52.

8
Тернарная аддитивная проблема

8.1 Общие предположения

Предположим, что $k_1, k_2, \ldots, k_s$ — s целых чисел, таких, что

$$2 \leqslant k_1 \leqslant k_2 \leqslant \ldots \leqslant k_s \quad \text{и} \quad \sum_{j=1}^{s} k_j^{-1} > 1. \tag{8.1}$$

Тогда предыдущие рассмотрения, в частности в гл. 2 и 4, наводят на мысль, что уравнение

$$\sum_{j=1}^{s} x_j^{k_j} = n \tag{8.2}$$

разрешимо в натуральных числах $x_1, \ldots, x_s$ всякий раз, когда:

(i) для каждого простого p и большого k уравнение (8.2) разрешимо по модулю p^k с $p \nmid x_j$ для некоторого j;

(ii) n достаточно велико.

Вопросы такого рода очень тщательно разрабатывались; эта работа, в сущности, еще не завершена, потому что рассмотрение малых дуг при нынешних знаниях, вообще говоря, требует, чтобы сумма $\sum k_j^{-1}$ была значительно больше единицы.

Наименьшей величиной s, для которой условия (8.1) выполняются, является $s = 3$. Причем окончательное решение получено только при $k_1 = k_2 = k_3 = 2$ — это классическая теорема Лежандра о суммах трех квадратов. Однако во всех остальных случаях показано, что почти все числа представимы в виде (8.2). Случаи $k_1 = k_2 = 2$ и $k_1 = 2$, $k_2 = k_3 = 3$ рассмотрели Дэвенпорт и Хельбронн (1937*a*, *b*), случай $k_1 = 2$, $k_2 = 3$, $k_3 = 4$ — Рот [Roth, 1949], а случай $k_1 = 2$, $k_2 = 3$, $k_3 = 5$ — Вон [Vaughan, 1980*a*]. [1]

Последний случай — самый трудный, и ему посвящена оставшаяся часть этой главы. Изложенный здесь метод можно применять и в других случаях.

8.2 Формулировка теоремы

Пусть $E(X)$ означает количество натуральных чисел, не превосходящих X и не являющихся суммой квадрата, куба и пятой степени натуральных чисел.

Теорема 8.1. *Существует положительное число δ, такое, что $E(X) \ll X^{1-\delta}$.*

В основном рассуждения подобны изложенным в § 3.2. Важная особенность их в том, что большие дуги здесь могут быть взяты более длинными и более многочисленными, чем можно было предполагать из-за присутствия куба и пятой степени. Однако бо́льшая часть больших дуг в некотором смысле рассматривается теми же методами, что и малые дуги.

Другая особенность рассуждений — это некоторые трудности, связанные со сходимостью особого ряда. Они преодолеваются заменой особого ряда конечным произведением.

8.3 Определение больших и малых дуг

Пусть n означает большое натуральное число и

$$P_k = \left(\tfrac{1}{4} n\right)^{1/k}.$$

Далее, пусть $R(m) = R(m, n)$ обозначает число представлений m в виде

$$m = x_2^2 + x_3^3 + x_5^5$$

с $P_k < x_k \leqslant 2P_k$, и пусть

$$J(m) = \sum_{y_2} \sum_{y_3} \sum_{y_5} \frac{1}{30} y_2^{-1/2} y_3^{-2/3} y_5^{-4/5}, \tag{8.3}$$

где переменные суммирования удовлетворяют условиям $P_k^k < y_k \leqslant (2P_k)^k$ и $y_2 + y_3 + y_5 = m$.

Определим также

$$S_k = S_k(q,\ a) = \sum_{r=1}^{q} e(ar^k/q), \tag{8.4}$$

$$A(m,\ q) = \sum_{\substack{a=1 \\ (a,\ q)=1}}^{q} q^{-3} S_2 S_3 S_5 e(-am/q) \tag{8.5}$$

и

$$\mathfrak{S}(m,\ X) = \sum_{q \leqslant X} A(m,\ q). \tag{8.6}$$

Первую часть доказательства теоремы 8.1 составляет

Теорема 8.2. *Существует положительная постоянная* δ, *такая, что для каждого достаточно большого* n

$$R(m) = J(m)\mathfrak{S}(m, n^{1/2}) + O(n^{1/30-\delta})$$

для всех, за исключением $\ll n^{1-\delta}$, *значений* m, *удовлетворяющих неравенству* $n < m \leqslant 2n$.

Доказательство. Пусть

$$h_k = h_k(\alpha) = \sum_{P_k < x \leqslant 2P_k} e(\alpha x^k), \tag{8.7}$$

$$\delta = 10^{-5}, \quad P = n^{13/30+7\delta}, \quad \mathcal{U} = (P/n,\ 1 + P/n]. \tag{8.8}$$

Тогда

$$R(m) = \int_{\mathcal{U}} h_2(\alpha) h_3(\alpha) h_5(\alpha) e(-\alpha m)\, d\alpha. \tag{8.9}$$

При $1 \leqslant a \leqslant q \leqslant P$ и $(a, q) = 1$ определим большую дугу $\mathfrak{M}(q, a)$ в виде

$$\mathfrak{M}(q, a) = \{\alpha\colon |\alpha - a/q| \leqslant Pq^{-1}n^{-1}\}, \tag{8.10}$$

а $\mathfrak{M}$ — как объединение всех больших дуг. Как обычно, легко доказывается, что $\mathfrak{M}(q, a)$ не пересекаются, и малые дуги $\mathfrak{m}$ берутся как $\mathcal{U} \setminus \mathfrak{M}$.

Приведем важное в дальнейшем подразделение дуг $\mathfrak{M}$. Пусть $\mathfrak{M}_1$ означает подмножество $\mathfrak{M}$, состоящее из $\mathfrak{M}(q, a)$ с $q > n^{1/12}$, и пусть

$$\mathfrak{N}(q, a) = \{\alpha\colon |\alpha - a/q| \leqslant n^{3\delta - 14/15}\}. \tag{8.11}$$

Определим теперь $\mathfrak{M}_2$ как объединение $\mathfrak{M}(q, a) \setminus \mathfrak{N}(q, a)$ с условиями $1 \leqslant a \leqslant q \leqslant n^{1/12}$ и $(a, q) = 1$. Тогда если положить

$$\mathfrak{n} = \mathfrak{m} \cup \mathfrak{M}_1 \cup \mathfrak{M}_2 \tag{8.12}$$

и

$$R_1(m) = \int_{\mathfrak{n}} h_2(\alpha) h_3(\alpha) h_5(\alpha) e(-\alpha m)\, d\alpha,$$

то надо будет доказать неравенство

$$\sum_m |R_1(m)|^2 \ll n^{16/15 - 3\delta}$$

и соотношение

$$\sum_{q \leqslant n^{1/12}} \sum_{\substack{a=1 \\ (a, q) = 1}}^{q} \int_{\mathfrak{N}(q, a)} h_2(\alpha) h_3(\alpha) h_5(\alpha) e(-\alpha m)\, d\alpha = J(m)\mathfrak{S}(m,\ n^{1/12}) + O(1). \tag{8.13}$$

Первая из этих оценок будет следовать из тождества Парсеваля, если показать, что

$$\int_{\mathfrak{n}} |h_2(\alpha)\, h_3(\alpha)\, h_5(\alpha)|^2\, d\alpha \ll n^{16/15-3\delta}. \qquad (8.14)$$

8.4 Рассмотрение $\mathfrak{n}$

Малые дуги $\mathfrak{m}$ могут быть рассмотрены прямым путем. Интеграл

$$\int_0^1 |h_2^2(\alpha)\, h_5^4(\alpha)|\, d\alpha$$

выражает число решений уравнения

$$u^2 - v^2 + x^5 - y^5 + z^5 - t^5 = 0$$

с $P_2 < u,\ v \leqslant 2P_2,\ P_5 < x,\ y,\ z,\ t \leqslant 2P_5$. Эти решения подразделяются на три вида:

$$\begin{aligned} &\text{(i)} && u \neq v, \\ &\text{(ii)} && u = v, \quad x \neq y, \\ &\text{(iii)} && u = v, \quad x = y, \quad z = t. \end{aligned}$$

Таким образом, общее число решений есть

$$\ll P_5^{4+\varepsilon} + P_2 P_5^{2+\varepsilon} + P_2 P_5^2.$$

Следовательно, по определению (8.3)

$$\int_0^1 |h_2^2 h_5^4|\, d\alpha \ll n^{9/10+\varepsilon} \qquad (8.15)$$

Аналогично

$$\int_0^1 |h_3^4|\, d\alpha \ll n^{2/3+\varepsilon}. \qquad (8.16)$$

Из неравенства Вейля (лемма 2.4) следует, что для каждого $\alpha \in \mathfrak{m}$

$$h_2(\alpha) \ll n^{1/2+\varepsilon}(P^{-1} + n^{-1/2})^{1/2} \ll n^{\varepsilon}(n/P)^{1/2}.$$

Поэтому ввиду (8.16)

$$\int_{\mathfrak{m}} |h_2^2\, h_3^4|\, d\alpha \ll n^{5/3+3\varepsilon} P^{-1}.$$

Следовательно, по неравенству Шварца, оценке (8.15) и формулам (8.8),

$$\int\limits_{\mathfrak{m}} |h_2^2 h_3^2 h_5^2|\, d\alpha \ll n^{16/15-3\delta}. \tag{8.17}$$

Пусть

$$w_k(\beta) = \sum_x (1/k)\, x^{1/k-1} e(\beta x), \tag{8.18}$$

где переменная суммирования удовлетворяет неравенствам $P_k^k < x \leqslant (2P_k)^k$, и определим

$$W_k = W_k(\alpha,\ q,\ a) = q^{-1} S_k(q,\ a)\, w_k(\alpha - a/q). \tag{8.19}$$

Для $\alpha \in \mathfrak{M}$ определим φ_k, Δ_k полагая

$$\varphi_k = \varphi_k(\alpha) = W_k(\alpha,\ q,\ a) \quad (\alpha \in \mathfrak{M}(q,\ a)), \quad \Delta_k = \Delta_k(\alpha) = h_k - \varphi_k. \tag{8.20}$$

Первым шагом в рассмотрениях $\mathfrak{M}_1 \cup \mathfrak{M}_2$ является замена h_2 на φ_2. По теореме 4.1, $\Delta_2(\alpha) \ll P^{1/2+\varepsilon}$, если $\alpha \in \mathfrak{M}$. К тому же, так же как в доказательстве (8.16), имеем

$$\int\limits_0^1 |h_3^2 h_5^2|\, d\alpha \ll n^{8/15}.$$

Следовательно, ввиду (8.8)

$$\int\limits_{\mathfrak{m}} |\Delta_2^2 h_3^2 h_5^2|\, d\alpha \ll n. \tag{8.21}$$

Следующий шаг состоит в оценке

$$\int\limits_{\mathfrak{m}_1} |\varphi_2^2 h_3^2 h_5^2|\, d\alpha.$$

Для ее получения сначала надо рассмотреть соответствующие интегралы с подынтегральными выражениями $|\varphi_2^2 h_5^4|$ и $|\varphi_2^2 h_3^4|$.

Согласно соотношениям (8.19) и (8.20),

$$\int\limits_{\mathfrak{m}} |\varphi_2^2 h_5^4|\, d\alpha \leqslant$$

$$\leqslant \sum_{q \leqslant P} \sum_{\substack{a=1 \\ (a,\ q)=1}}^{q} q^{-2} |S_2|^2 \int\limits_{-1/2}^{1/2} |w_2(\beta)^2 h_5(\beta + a/q)^4|\, d\beta \tag{8.22}$$

и в силу (8.18)

$$|w_2(\beta)|^2 = \sum_h b(h)\, e(-\beta h),$$

где

$$b(h) = \sum_{x,\ y} \tfrac{1}{4} (xy)^{-1/2} \tag{8.23}$$

с $x-y=h$, $\frac{1}{4}n=P_2^2<x$, $y\leqslant(2P_2)^2=n$. Кроме того, по определению (8.7)

$$|h_5(\alpha)|^4=\sum_h c(h)e(\alpha h),$$

где
$$c(h)=\sum_{x,\ y,\ z,\ t}1$$

с $x^5-y^5+z^5-t^5=h$ и $P_5<x,\ y,\ z,\ t\leqslant 2P_5$. Следовательно,

$$\int_{-1/2}^{1/2}|w_2(\beta)^2h_5(\beta+a/q)^4|\,d\beta=\sum_h b(h)c(h)e(ah/q).$$

Отсюда в силу неравенства (8.22)

$$\int_{\mathfrak{m}}|\varphi_2^2h_5^4|\,d\alpha\leqslant\sum_h b(h)c(h)\sum_{q\leqslant P}\sum_{\substack{a=1\\(a,\ q)=1}}^{q}q^{-2}|S_2|^2e(ah/q).$$

Очевидно, что модуль суммы S_2, определенной в (8.4), не зависит от a и имеет оценку $|S_2|^2\ll q$. Следовательно, по формуле (3.14) для $h\neq 0$

$$\sum_{\substack{a=1\\(a,\ q)=1}}^{q}q^{-2}|S_2|^2e(ah/q)\ll q^{-1}\sum_{d|(q,\ h)}d.$$

Таким образом,

$$\int_{\mathfrak{m}}|\varphi_2^2h_5^4|\,d\alpha\ll b(0)c(0)P+\sum_{h\neq 0}b(h)c(h)\sum_{d|h}\sum_{r\leqslant P/d}\frac{1}{r}.$$

Непосредственно из (8.23) следует, что $b(h)\ll 1$. Кроме того, аналогично доказательству неравенства (8.16) имеем $c(0)\ll\ll n^{2/5+\varepsilon}$. К тому же $\sum_h c(h)\ll n^{4/5}$. Следовательно, ввиду (8.8)

$$\int_{\mathfrak{m}}|\varphi_2^2h_5^4|\,d\alpha\ll n^{5/6+8\delta}. \tag{8.24}$$

Для оценки интеграла

$$\int_{\mathfrak{m}_1}|\varphi_2^2h_3^4|\,d\alpha$$

применяются различные формы неравенства Гёльдера, и поэтому требуется оценить интеграл

$$\int_{\mathfrak{M}}|\varphi_2^4|\,d\alpha.$$

Согласно (8.20) и лемме 6.3,

$$\int\limits_{\mathfrak{m}} |\varphi_2^4|\, d\alpha \ll \sum_{q\leqslant P} q^{-1} \int\limits_0^{1/2} n^2(1+n\beta)^{-4}\, d\beta,$$

так что

$$\int\limits_{\mathfrak{m}} |\varphi_2^4|\, d\alpha \ll n^{1+\varepsilon}. \tag{8.25}$$

Следовательно, в силу неравенства Гёльдера и (8.16)

$$\int\limits_{\mathfrak{m}} |\varphi_2^2\Delta_3 h_3^3|\, d\alpha \ll (n^{1+\varepsilon})^{1/4}\, (n^{2/3+\varepsilon})^{3/4} \sup_{\mathfrak{m}} |\varphi_2\Delta_3|.$$

Ввиду лемм 6.1 и 6.3 для $\alpha \in \mathfrak{M}(q, a)$ имеем

$$\varphi_2(\alpha)\Delta_3(\alpha) \ll n^{1/2}q^{\varepsilon}.$$

Отсюда

$$\int\limits_{\mathfrak{n}} |\varphi_2^2\Delta_3 h_3^3|\, d\alpha \ll n^{5/4+2\varepsilon}. \tag{8.26}$$

По неравенству Шварца и неравенствам (8.25) и (8.16)

$$\int\limits_{\mathfrak{m}} |\varphi_2^2\varphi_3\Delta_3 h_3^2|\, d\alpha \ll (n^{1+\varepsilon})^{1/2}\, (n^{2/3+\varepsilon})^{1/2} \sup_{\mathfrak{M}} |\varphi_3\Delta_3|$$

и, согласно леммам 6.1 и 6.3, для $\alpha \in \mathfrak{M}(q, a)$

$$\varphi_3(\alpha)\Delta_3(\alpha) \ll n^{1/3}q^{1/6+\varepsilon} \ll n^{1/3}P^{1/6+}$$

Поэтому ввиду (8.8)

$$\int\limits_{\mathfrak{M}} |\varphi_2^2\varphi_3\Delta_3 h_3^2|\, d\alpha \ll n^{5/4}. \tag{8.27}$$

Из лемм 6.1 и 6.3 и (8.8) следует, что

$$\int\limits_{\mathfrak{M}} |\varphi_2^2\varphi_3^2\Delta_3^2|\, d\alpha \ll \sum_{q\leqslant P} q^{1/3+\varepsilon} \int\limits_0^{1/2} \frac{n^{5/3}}{(1+n\beta)^4}\,(1+n\beta)^2\, d\beta \ll n^{5/4}.$$

Следовательно, в силу (8.26) и (8.27)

$$\int\limits_{\mathfrak{M}_1} |\varphi_2^2 h_3^4|\, d\alpha \ll n^{5/4+\varepsilon} + \int\limits_{\mathfrak{M}_1} |\varphi_2^2\varphi_3^4|\, d\alpha. \tag{8.28}$$

Рассмотрим интеграл в правой части. Согласно соотношениям (8.20), (8.19), лемме 6.2 и теореме 4.2,

$$\int\limits_{\mathfrak{M}_1} |\varphi_2^2\varphi_3^4|\, d\alpha \ll \sum_{n^{1/12}<q\leqslant P} \ \sum_{\substack{a=1\\(a,\,q)=1}}^{q} q^{-6}|S_2^2S_3^4| \int\limits_0^{1/2} \frac{n^{7/3}}{(1+n\beta)^6}\, d\beta \ll n^{5/4}J,$$

где $J = \sum\limits_{q\leqslant P} F(q), \quad F(q) = \sum\limits_{\substack{a=1\\(a,\,q)=1}}^{q} q^{-4}|S_3^4|.$

Вследствие теоремы 4.2 $F(q) \ll q^{-1/3}$. Таким образом, $\sum_{h=3}^{\infty} F(p^h) \ll p^{-1}$. Далее по леммам 4.3 и 4.4 $|S_3(p^l, a)| \ll p^{l/2}$ при $l = 1$ или 2. Отсюда $\sum_{h=1}^{2} F(p^h) \ll p^{-1}$. Более того, в силу леммы 4.5 F — мультипликативная функция q. Следовательно, существует абсолютная постоянная C, такая, что

$$J \leqslant \prod_{p \leqslant P} (1 + Cp^{-1}).$$

Отсюда в силу (8.28) и элементарной теории простых чисел

$$\int_{\mathfrak{M}_1} |\varphi_2^2 h_3^4|\, d\alpha \ll n^{5/4+\varepsilon}.$$

Следовательно, по неравенству Шварца и неравенству (8.24)

$$\int_{\mathfrak{M}_1} |\varphi_2^2 h_3^2 h_5^2|\, d\alpha \ll n^{16/15-3\delta}.$$

Отсюда ввиду (8.21)

$$\int_{\mathfrak{M}_1} |h_2^2 h_3^2 h_5^2|\, d\alpha \ll n^{16/15-3\delta}. \tag{8.29}$$

Рассмотрим теперь $\mathfrak{M}_2$. По лемме 6.3

$$\int_{\mathfrak{M}_2} |\varphi_2^4|\, d\alpha \ll \sum_{q \leqslant P} q^{-1} \int_{n^{3\delta-14/15}}^{1/2} \frac{n^2}{(1+n\beta)^4}\, d\beta \ll n^{4/5+\varepsilon-9\delta}.$$

Согласно лемме Хуа (лемма 2.5),

$$\int_0^1 |h_3^8|\, d\alpha \ll n^{5/3+\varepsilon}, \quad \int_0^1 |h_5^8|\, d\alpha \ll n^{1+\varepsilon}.$$

Поэтому по неравенству Гёльдера

$$\int_{\mathfrak{M}_2} |\varphi_2^2 h_3^2 h_5^2|\, d\alpha \ll \left(n^{4/5+\varepsilon-9\delta}\right)^{1/2} \left(n^{5/3+\varepsilon}\right)^{1/4} \left(n^{1+\varepsilon}\right)^{1/4} \ll n^{16/15-3\delta}.$$

Следовательно, ввиду (8.21)

$$\int_{\mathfrak{M}_2} |h_2^2 h_3^2 h_5^2|\, d\alpha \ll n^{16/15-3\delta},$$

что в комбинации с (8.29) и (8.17) дает (8.14).

8.5 Большие дуги $\mathfrak{N}(q, a)$

Для завершения доказательства теоремы 8.2 остается доказать соотношение (8.13). Простые вычисления показывают, что если $k = 2$, 3 или 5, $q \leqslant n^{1/12}$ и $|\beta| \leqslant n^{3\delta - 14/15}$, то

$$q^{1/2+\varepsilon}(1 + n|\beta|) \ll (n/q)^{1/k}(1 + n|\beta|)^{-1}.$$

Отсюда по леммам 6.1 и 6.3 для $\alpha \in \mathfrak{N}(q, a)$ имеем

$$h_k(\alpha),\ W_k(\alpha) \ll (n/q)^{1/k}(1 + n|\alpha - a/q|)^{-1}$$

и

$$h_2(\alpha) h_3(\alpha) h_5(\alpha) - W_2(\alpha) W_3(\alpha) W_5(\alpha) \ll \ll (n/q)^{5/6}(1 + n|\alpha - a/q|)^{-1} q^{1/2+\varepsilon}.$$

Таким образом,

$$\sum_{q \leqslant n^{1/12}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{\mathfrak{n}(q,a)} |h_2 h_3 h_5 - W_2 W_3 W_5| \, d\alpha \ll 1.$$

Пусть $\mathfrak{P}(q, a) = \left\{\alpha : n^{3\delta - 14/15} < |\alpha - a/q| \leqslant \frac{1}{2}\right\}$. Тогда по лемме 6.3

$$\sum_{q \leqslant n^{1/12}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{\mathfrak{P}(q,a)} |W_2 W_3 W_5| \, d\alpha \ll 1.$$

Следовательно, ввиду (8.19), (8.4), (8.5) и (8.6)

$$\sum_{q \leqslant n^{1/12}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{\mathfrak{P}(q,a)} h_2 h_3 h_5 \, e(-\alpha m) \, d\alpha = I_1(m) \mathfrak{S}(m,\ n^{1/12}) + O(1),$$

где

$$I_1(m) = \int_0^1 w_2(\beta) w_3(\beta) w_5(\beta) e(-\beta m) \, d\beta.$$

Согласно (8.18) и (8.3), $I_1(m) = I(m)$, что дает требуемую формулу (8.13).

8.6 Особый ряд

Принципиальная трудность заключается в том, что ряд $\sum_{q=1}^{\infty} |A(n, q)|$, очевидно, расходится. Она преодолевается путем аппроксимации $\mathfrak{S}(m, n^{1/12})$ конечным Эйлеровым произведением.

Теорема 8.3. *Для всех, кроме* $\ll n^{1-\delta}$, *значений* m, $n < m \leqslant 2n$ *справедлива формула*

$$\mathfrak{S}(m, n^{1/12}) = \prod_{p \leqslant n} \left(\sum_{h=0}^{\infty} A(m, p^h) \right) + O(\exp(-\log n)^{\delta})). \tag{8.30}$$

Возможно, что при аналогичных условиях, используя метод, сходный с методом Миха [Miech, 1968], можно показать, что конечное произведение заменимо на бесконечное. Однако при этом возникают трудности, которые описываемым здесь методом можно обойти. Дальнейшее обсуждение этого вопроса в случае $k_1 = 2$, $k_2 = k_3 = 3$ см. в статье Дэвенпорта и Хельбронна (1937*a*). Согласно (8.4), (8.5) и теореме 4.2,

$$A(m, 1) = 1, \quad A(m, q) \ll q^{-1/30}. \tag{8.31}$$

Таким образом, каждый ряд в правой части (8.30) абсолютно сходится.

Для доказательства теоремы 8.3 требуется точная оценка $A(m, p^h)$. В основе ее получения лежат формулы для $S_k(p^h, a)$ при $p \nmid a$. Они являются следствиями лемм 4.3 и 4.4.

Если $p > 2$,

$$S_2(p^h, a) = \begin{cases} p^{h/2} & (2 \mid h), \\ \left(\frac{a}{p}\right)_L S_2(p, 1)\, p^{(h-1)/2} & (2 \nmid h), \end{cases} \tag{8.32}$$

если $p > 3$,

$$S_3(p^h, a) = \begin{cases} p^{[2h/3]} & (h \not\equiv 1 \pmod 3), \\ 0 & (h \equiv 1 \pmod 3,\ p \equiv 2 \pmod 3), \\ S_3(p, a)\, p^{2(h-1)/3} & (h \equiv p \equiv 1 \pmod 3), \end{cases} \tag{8.33}$$

если $p > 5$, то

$$S_5(p^h, a) = \begin{cases} p^{[4h/5]} & (h \not\equiv 1 \pmod 5), \\ 0 & (h \equiv 1 \pmod 5,\ p \not\equiv 1 \pmod 5), \\ S_5(p, a)\, p^{4(h-1)/5} & (h \equiv p \not\equiv 1 \pmod 5). \end{cases} \tag{8.34}$$

Далее, если $k = 3$ или 5 и $p \equiv 1 \pmod k$, то

$$S_k(p, a) = \sum_{\chi \in \mathcal{A}} \chi(a)\, \tau(\bar{\chi}), \tag{8.35}$$

где $\mathcal{A}$ означает множество из $k - 1$ неглавных характеров χ по модулю p, таких, что $\chi^k = \chi_0$. Более того,

$$|\tau(\chi)| = p^{1/2}, \quad |S_2(p, 1)| = p^{1/2} \quad (p > 2). \tag{8.36}$$

Лемма 8.1. *Предположим, что $h \geqslant 1$ и $p > 5$. Тогда*

$$A(m, p^h) = 0, \quad \text{если} \quad h > 1 \text{ и } p^{h-1} \nmid m, \tag{8.37}$$

$$|A(m, p^h)| \leqslant 8p^{-[(h-1)/30]-1} \tag{8.38}$$

и

$$A(m, p) = \sum_{\chi \in \mathscr{A}(p)} c(x)\chi(m), \tag{8.39}$$

где $\mathscr{A}(p)$ — совокупность неглавных характеров по модулю p,

$$|c(x)| \leqslant p^{-1} \quad \text{и} \quad \operatorname{card} \mathscr{A}(p) \leqslant 8. \tag{8.40}$$

Доказательство. Ввиду соотношений (8.5), (8.32), (8.33), (8.34) и (8.35)

$$A(m, p^h) = \sum_{\chi \in \mathscr{A}(p^h)} b(\chi) \sum_{a=1}^{p^h} \chi(a)e(-ap^{-h}m), \tag{8.41}$$

где $\mathscr{A}(p^h)$ есть подмножество множества характеров по модулю p, а $b(\chi)$ — подходящие комплексные числа. Если $h > 1$ и $p^{h-1} \nmid m$. то внутренняя сумма равна

$$\sum_{x=1}^{p} \chi(x)e(-xp^{-h}m) \sum_{y=1}^{p^{h-1}} e(-yp^{1-h}m) = 0.$$

Это дает (8.37).

Доказательство неравенства (8.38) подразделяется на восемь различных случаев.

(i) Предположим, что $2|h$, $h \not\equiv 1 \pmod 3$ и $h \not\equiv 1 \pmod 5$. Тогда $\mathscr{A}(p^h)$ состоит только из одного главного характера и по (8.32), (8.34) и (8.35)

$$|A(m, p^h)| \leqslant p^{\lambda},$$

где $\lambda = \frac{1}{2}h + [2h/3] + [4h/5] - 2h$. Число λ — целое и не превосходит $-h/30 \leqslant -[(h-1)/30] - 1/30$. Отсюда имеем (8.38). Во всех остальных случаях все элементы $\mathscr{A}(p^h)$ в (8.41) являются неглавными характерами по модулю p. Таким образом, если $p^h|m$, то внутренняя сумма автоматически равна 0, и неравенство (8.38) следует сразу. Кроме того, ввиду (8.37) можно предполагать, что или $h = 1$, или $h > 1$, p^{h-1}/m и $p^h \nmid m$. В любом случае внутренняя сумма в формуле (8.41) имеет вид

$$\sum_{a=1}^{p^h} \chi(a)e\left(\frac{a(-m)}{pp^{h-1}}\right) = \bar{\chi}\left(-\frac{m}{p^{h-1}}\right)p^{h-1}\tau(\chi). \tag{8.42}$$

(ii) Предположим, что $2 \nmid h$, $h \not\equiv 1 \pmod 3$ и $h \not\equiv 1 \pmod 5$. Тогда $\mathscr{A}(p^h)$ состоит из одного квадратичного характера, и

$$|b(\chi)| = p^{h/2+[2h/3]+[4h/5]-3h}.$$

Следовательно, согласно (8.42),

$$|A(m,\ p^h)| = p^\lambda \text{ с } \lambda = \tfrac{1}{2}h + [2h/3] + [4h/5] - 2h - \tfrac{1}{2}.$$

Показатель λ является целым числом, которое не превосходит $-h/30 - \frac{1}{2}$. Таким образом, справедливо неравенство (8.38).

(iii) Предположим, что $2|h, h \equiv 1 \pmod 3$ и $h \not\equiv 1 \pmod 5$. При $p \not\equiv 1 \pmod 3$ (8.33) дает $A(m, p^h) = 0$. Следовательно, можно предполагать, что $p \equiv 1 \pmod 3$. Тогда $\operatorname{card} \mathscr{A}(p^h) = 2$ и $|A(m, p^h)| \leqslant 2p^\lambda$, где $\lambda = \frac{1}{2}h + 2(h-1)/3 + \frac{1}{2} + [4h/5] - 2h - \frac{1}{2}$. Число λ — целое, не превосходящее $-h/30 - \frac{1}{2}$. Следовательно, (8.38) имеет место.

(iv) Предположим, что $2|h$, $h \not\equiv 1 \pmod 3$ и $h \equiv 1 \pmod 5$. Случай $p \not\equiv 1 \pmod 5$ снова тривиален, поэтому можно предполагать, что $p \equiv 1 \pmod 5$. Тогда

$$|A(m,\ p^h)| \leqslant 4p^\lambda \text{ с } \lambda = \tfrac{1}{2}h + [2h/3] + 4(h-1)/5 - 2h,$$

и рассуждения заканчиваются, как и выше.

(v) Предположим, что $2|h$ и $h \equiv 1 \pmod{15}$. Случай $p \not\equiv 1 \pmod{15}$ тривиален, а если $p \equiv 1 \pmod{15}$, получаем $|A(m, p^h)| \leqslant 8p^{\lambda+1/2}$ с $\lambda = \frac{1}{2}h + 2(h-1)/3 + 4(h-1)/5 - 2h$. Это снова целое число, не превосходящее $-h/30 - 22/15 < -[(h-1)/30] - 1$. Следовательно, показатель $\lambda + \frac{1}{2}$ удовлетворяет неравенству $\lambda + \frac{1}{2} \leqslant -[(h-1)/30] - \frac{3}{2}$.

(vi) Предположим, что $h \equiv 1 \pmod{10}$ и $h \not\equiv 1 \pmod 3$. При $p \not\equiv 1 \pmod 5$ неравенство (8.38) немедленно следует из (8.34); поэтому можно предполагать, что $p \equiv 1 \pmod 5$. Тогда $|A(m, p^h)| \leqslant 4p^{\lambda+1/2}$ с $\lambda = \frac{1}{2}(h-1) + [2h/3] + 4(h-1)/5 - 2h$. Как и в предыдущем случае, показатель не превосходит $-[(h-1)/30] - \frac{3}{2}$.

(vii) Предположим, что $h \equiv 1 \pmod 6$ и $h \not\equiv 1 \pmod 5$. В этом случае рассуждаем как в (vi).

(viii) Предположим, наконец, что $h \equiv 1 \pmod{30}$. Тогда $A(m, p^h) = 0$ для $p \not\equiv 1 \pmod{15}$. Остается возможность $p \equiv 1 \pmod{15}$. Тогда $|A(m, p^h)| \leqslant 8p^\lambda$ с $\lambda = \frac{1}{2}h + 2(h-1)/3 + \frac{1}{2} + 4(h-1)/5 + \frac{1}{2} - 2h - \frac{1}{2}$. Снова λ является целым, не превосходящим $-h/30 - \frac{4}{5} - \frac{1}{6} = -(h-1)/30 - 1$.

Доказательство леммы теперь заканчивает оценка (8.39) с (8.40). При $h = 1$ (8.32), (8.33), (8.34) и (8.35) дают равенство (8.41) с $b(\chi) = 0$, если $p \not\equiv 1 \pmod{15}$. Таким образом, если $p \not\equiv 1 \pmod{15}$, получается (8.39), из которого тривиально следуют неравенства (8.40).

Когда $p \equiv 1 \pmod{15}$, (8.41) справедливо с $\mathscr{A}(p)$, состоящим из характеров χ вида $\chi = \chi_2\chi_3\chi_4$ где χ_k означает неглавный характер порядка k Таким образом, все элементы $\mathscr{A}(p)$ являются неглавными и $\operatorname{card}\mathscr{A}(p) = 8$. Более того,

$$b(\chi) = S_2(p, 1)\tau(\bar{\chi}_3)\tau(\bar{\chi}_5)p^{-3}.$$

Следовательно, согласно (8.41) и (8.42),

$$A(m, p) = \sum_{\chi \in \mathscr{A}(p)} S_2(p, 1)\tau(\bar{\chi}_3)\tau(\bar{\chi}_5)p^{-3}\chi(-1)\tau(\chi)\bar{\chi}(m).$$

Если характер χ принадлежит $\mathscr{A}(p)$, то то же самое верно для $\bar{\chi}$.

Кроме того, в силу (8.36) имеем

$$|S_2(p, 1)\tau(\bar{\chi}_3)\tau(\bar{\chi}_5)p^{-3}\chi(-1)\tau(\chi)| = p^{-1}.$$

Это дает формулу (8.39) с оценками (8.40), как и требовалось.

Пусть множество $\mathscr{B}$ состоит из 1 и таких натуральных чисел q, что если $p|q$, то $p \leqslant n$ и либо $p^2|q$, либо $p \leqslant 5$. Пусть $\mathscr{C}$ означает множество бесквадратных чисел, все простые делители которых удовлетворяют неравенству $5 < p \leqslant n$. Наконец, пусть $\mathscr{D}$ — множество натуральных чисел, не имеющих простых делителей, больших n. Тогда каждое q в $\mathscr{D}$ может быть единственным образом записано в виде $q = rs$, где $r \in \mathscr{B}$, $s \in \mathscr{C}$ и $(r, s) = 1$.

Следующий этап рассуждений состоит в оценке суммы

$$\sum_{\substack{U < q \leqslant V \\ q \in \mathscr{D}}} A(m, q), \tag{8.43}$$

где

$$U = n^{1/12}, \quad V = \exp((\log n)^{1+2\delta}). \tag{8.44}$$

Согласно (8.5) и лемме 4.5, $A(m, q)$ — мультипликативная функция q. Следовательно,

$$\Big|\sum_{\substack{U < q \leqslant V \\ q \in \mathscr{D}}} A(m, q)\Big| \leqslant \sum_{\substack{r > n^{80\delta} \\ r \in \mathscr{B}}} \sum_{s \in \mathscr{C}} |A(m, r)A(m, s)| +$$

$$+ \sum_{\substack{r \leqslant n^{80\delta} \\ r \in \mathscr{B}}} |A(m, r)| \Big| \sum_{\substack{U/r < s \leqslant V/r \\ (s, r) = 1, s \in \mathscr{C}}} A(m, s)\Big|. \tag{8.45}$$

Первая двойная сумма

$$\leqslant n^{-2\delta}\Big(\sum_{r \in \mathscr{B}} r^{1/40}|A(m, r)|\Big)\Big(\sum_{s \in \mathscr{C}} |A(m, s)|\Big). \tag{8.46}$$

Первая сумма здесь равна

$$\Big(\prod_{5 < p \leqslant n}\Big(1 + \sum_{h=2}^{\infty} p^{h/40}|A(m, p^h)|\Big)\Big)\prod_{p \leqslant 5}\Big(1 + \sum_{h=1}^{\infty} p^{h/40}|A(m, p^h)|\Big),$$

и ввиду (8.31), (8.37) и (8.38) это есть величина

$$\ll \prod_{p,\,t} (1 + C(t+1)),$$

где произведение берется по всем парам p, t, для которых $p^t \parallel m$. Это произведение $\ll n^{\varepsilon}$.

Ввиду неравенства (8.38) вторая сумма в (8.46) не превосходит

$$\prod_{p\leqslant n} (1 + 8p^{-1}) \ll n^{\varepsilon}.$$

Следовательно, по (8.31) и (8.45),

$$\sum_{\substack{U<q\leqslant V\\ q\in\mathscr{D}}} A(m,\ q) \ll n^{-\delta} + F(m), \tag{8.47}$$

где

$$F(m) = \sum_{r\leqslant n^{80\delta}} \left| \sum_{\substack{U/r<s\leqslant V/r\\ (s,r)=1,\ s\in\mathscr{C}}} A(m,\ s) \right|. \tag{8.48}$$

Согласно (8.39) и (8.40) и свойству мультипликативности $A(m, s)$,

$$A(m,\ s) = \sum_{\chi_{\bmod s}}{}^{*}\ c(\chi)\,\chi(m) \quad (s\in\mathscr{C}), \tag{8.49}$$

где $\sum^*$ означает сумму по примитивным характерам,

$$|\,c(\chi)\,| \leqslant s^{-1} \tag{8.50}$$

и для $\lambda > 0$

$$\sum_{\chi \bmod s}{}^{*} |\,c(\chi)\,|^{\lambda} \leqslant 8^{\omega(s)} s^{-\lambda}. \tag{8.51}$$

Лемма 8.2. *Пусть l — натуральное число. Тогда для произвольных комплексных чисел $b(\chi)$*

$$\left(\sum_{x=1}^{N} \left| \sum_{q\leqslant Q} \sum_{\chi_{\bmod q}}{}^{*} b(\chi)\,\chi(x) \right|^{3/2}\right)^{2/3} \ll B\left(\sum_{q\leqslant Q} \sum_{\chi_{\bmod q}}{}^{*} |\,b(\chi)\,|^{2l/(2l-1)}\right)^{(2l-1)/2l},$$

где

$$B = (N^{1/2} + Q^{1/l})\, N^{1/6} (\log (N^l e))^{(l^4-1)/(6l)}$$

и входящая в $\ll$ постоянная абсолютна.

Доказательство. В случае $l = 1$ по лемме 5.3 (неравенство большого решета) для произвольных комплексных чисел $c_1, \ldots, c_N$

$$\sum_{q\leqslant Q} \sum_{\substack{a=1\\ (a,\ q)\ =\ 1}}^{q} \left| \sum_{x=1}^{N} c_x e(ax/q) \right|^2 \ll (N + Q^2) \sum_{x=1}^{N} |\,c_x\,|^2. \tag{8.52}$$

Из теории сумм Гаусса (см. § 20 [Hasse, 1964] или § 9 [Дэвенпорт, 1966]) для примитивного характера χ по модулю q,

$$\tau(\bar{\chi})^{-1}\sum_{y=1}^{q}\bar{\chi}(y)\,e\,(yx/q)=\chi\,(x),$$

где $|\tau(\bar{\chi})|^2=q$. Следовательно,

$$\sum_{x=1}^{N}c_x\chi(x)=\tau(\bar{\chi})^{-1}\sum_{y=1}^{q}\bar{\chi}(y)\sum_{x=1}^{N}c_xe\,(yx/q).$$

Отсюда

$$\sum_{\chi_{\mathrm{mod}\ q}}^{*}\left|\sum_{x=1}^{N}c_x\chi(x)\right|^2\leqslant q^{-1}\sum_{\chi_{\mathrm{mod}\ q}}\left|\sum_{y=1}^{q}\bar{\chi}(y)\sum_{x=1}^{N}c_xe\,(yx/q)\right|^2.$$

Поэтому из ортогональности характеров и (8.52)

$$\sum_{q\leqslant Q}\sum_{\chi_{\mathrm{mod}\ q}}^{*}\left|\sum_{x=1}^{N}c_x\chi(x)\right|^2\ll(N+Q^2)\sum_{x=1}^{N}|c_x|^2.$$

Применение этой оценки к l-й степени суммы $\sum\limits_{x=1}^{N}c_x\chi(x)$ дает

$$\sum_{q\leqslant Q}\sum_{\chi_{\mathrm{mod}\ q}}^{*}\left|\sum_{x=1}^{N}c_x\chi(x)\right|^{2l}\ll(N^l+Q^2)\sum_{y}|d_y|^2,$$

где

$$d_y=\sum_{x_1\ldots x_l=y}{}'\,c_{x_1}\ldots c_{x_l}$$

и $\sum'$ означает, что суммирование по x_j ограничивается условием $x_j\leqslant N$. Предположим, что $\lambda>2$. Тогда посредством двойного применения неравенства Гёльдера имеем

$$|d_y|^2\leqslant d_l(y)^{2-2/\lambda}\left(\sum_{x_1\ldots x_l=y}{}'\,|c_{x_1}\ldots c_{x_l}|^{\lambda}\right)^{2/\lambda}$$

и

$$\sum_{y}|d_y|^2\leqslant\left(\sum_{y=1}^{N^l}d_l(y)^{(2\lambda-2)/(\lambda-2)}\right)^{1-2/\lambda}\left(\sum_{x=1}^{N}|c_x|^{\lambda}\right)^{2l/\lambda},$$

где $d_l(y)$ — число решений уравнения $x_1\ldots x_l=y$ в $x_1,\ldots,x_l$. Следовательно, по теореме 288 Харди, Литтлвуда, Полиа (1951),

$$\left(\sum_{x=1}^{N}\left|\sum_{q\leqslant Q}\sum_{\chi_{\mathrm{mod}\ q}}^{*}b(\chi)\chi(x)\right|^{\lambda/(\lambda-1)}\right)^{(\lambda-1)/\lambda}\ll$$

$$\ll B_\lambda\left(\sum_{q\leqslant Q}\sum_{\chi_{\mathrm{mod}\ q}}^{*}|b(\chi)|^{2l/(2l-1)}\right)^{(2l-1)/(2l)},$$

где

$$B_\lambda=(N^l+Q^2)^{1/2l}\left(\sum_{y=1}^{N^l}d_l(y)^{(2\lambda-2)/(\lambda-2)}\right)^{(1-2/\lambda)/(2l)}.$$

Пусть $\lambda = 3$. Тогда лемма следует при условии, что для $X \geqslant 1$

$$\sum_{y \leqslant X} d_l(y)^4 \leqslant X (\log Xe)^{l^4 - 1}.$$

На самом деле при помощи индукции по r нетрудно видеть, что $d_r(xy) \leqslant d_r(x)\, d_r(y)$, а посредством индукции по s — что

$$\sum_{y \leqslant X} d_r(y)^s \leqslant X (\log Xe)^{r^s - 1}$$

и

$$\sum_{y \leqslant X} d_r(y)^s y^{-1} \leqslant (\log Xe)^{r^s}.$$

Пусть $Q_0 = Ur^{-1}$ и $Q_l = n^{l/2}$, пусть $b(\chi) = c(\chi)$, когда q-модули χ принадлежат $\mathscr{C}$, $(q, r) = 1$ и $U/r < q \leqslant V/r$, и пусть $b(\chi) = 0$ в других случаях. Тогда по (8.48) и (8.49)

$$F(m) = \sum_{r \leqslant n^{80\delta}} \left| \sum_{q} \sideset{}{^*}\sum_{\chi \bmod q} b(\chi)\, \chi(m) \right|. \tag{8.53}$$

Согласно лемме 8.2, неравенству Гельдера, неравенствам (8.50) и (8.51),

$$\sum_{m=n+1}^{2n} \left| \sum_{Q_{l-1} < q \leqslant Q_l} \sideset{}{^*}\sum_{\chi \bmod q} b(\chi)\, \chi(m) \right| \ll$$

$$\ll n\, (l \log (2ne))^{(l^4-1)/(6l)} Q_{l-1}^{-1/(2l)} \prod_{p \leqslant n} (1 + 8p^{-1})^{(2l-1)/(2l)}.$$

Последнее выражение

$$\ll n^{7/8} (l \log (2ne))^{(l^4-1)/(6l)} (\log 2n)^{(8l-4)l}$$

или

$$\ll nU^{-1/2} r^{1/2} (\log n)^4$$

в зависимости от того $l > 1$ или $l = 1$. Следовательно, суммирование по l, для которых $Q_{l-1} \leqslant V$, дает в силу (8.44) и (8.53)

$$\sum_{m=n+1}^{2n} F(m) \ll n^{47/48}.$$

Отсюда для всех, кроме $\ll n^{1-\delta}$, величин m, $n < m \leqslant 2n$, имеем $F(m) \ll n^{-\delta}$, так что по (8.47), когда m не является исключительным,

$$\sum_{\substack{U < q \leqslant V \\ q \in \mathscr{D}}} A(m, q) \ll n^{\delta}. \tag{8.54}$$

Доказательство теоремы 8.3 заканчивается рассмотрением

$$\sum_{\substack{q > V \\ q \in \mathscr{D}}} A(m, q).$$

Пусть $\lambda = 1/(\log n)$. Тогда

$$\sum_{\substack{q>V\\ q\in\mathcal{D}}} |A(m, q)| \leqslant \sum_{q\in\mathcal{D}} (q/V)^{\lambda} |A(m, q)| =$$
$$= V^{-\lambda} \prod_{p\leqslant n} \left(1 + \sum_{h=1}^{\infty} p^{h\lambda} |A(m, p^h)|\right).$$

Отсюда в силу (8.31), (8.38) и (8.44)

$$\sum_{\substack{q>V\\ q\in\mathcal{D}}} |A(m, q)| \ll \exp(-(\log n)^{2\delta}) \times$$
$$\times \prod_{5<p\leqslant n} \left(1 + 240 \sum_{k=0}^{\infty} p^{(30\lambda-1)k+30\lambda-1}\right) \ll \exp(-(\log n)^{\delta}).$$

Следовательно, по (8.54), (8.44) и (8.6) для всех, кроме $\ll n^{1-\delta}$, значений m, удовлетворяющих условию $n < m \leqslant 2n$, имеем

$$\left(\prod_{p\leqslant n} \left(\sum_{h=0}^{\infty} A(m, p^h) - \mathfrak{S}(m, n^{1/12}\right)\right) \ll \exp(-(\log n)^{\delta}),$$

что и требовалось.

8.7 Завершение доказательства теоремы 8.1

Согласно теоремам 8.2 и 8.3, для всех, кроме $\ll n^{1-\delta}$, величин m, таких, что $n < m \leqslant 2n$, имеем

$$R(m) = I(m) \left(\left(\prod_{p\leqslant n} \left(\sum_{h=0}^{\infty} A(m, p^h)\right)\right) +\right.$$
$$\left. + O(\exp(-(\log n)^{\delta}))\right) + O(n^{1/30-\delta}).$$

Рассмотрим величину $I(m)$, заданную в (8.3), когда $n < m \leqslant 2n$. Для y_3, y_5, удовлетворяющих неравенствам $\frac{1}{2}m - \frac{1}{4}n < y_3$, $y_5 < \frac{1}{2}m - \frac{1}{8}n$, имеем $\frac{1}{4}n < y_3, y_5 < n$ и $\frac{1}{4}n < m - y_3 - y_5 < n$. Следовательно, $I(m) \gg n^{1/30}$. То, что $I(m) \ll n^{1/30}$, тривиально. Таким образом, достаточно показать, что

$$\prod_{p\leqslant n} \left(\sum_{h=0}^{\infty} A(m, p^h)\right) \gg (\log n)^{-C}. \tag{8.55}$$

Согласно неравенству (8.38), существует константа C, такая, что

$$\sum_{C<p\leqslant n} \left(\sum_{h0}^{\infty} A(m, p^h)\right) \geqslant \sum_{C<p\leqslant n} (1 - Cp^{-1}) \gg (\log n)^{-C}.$$

Следовательно, надо показать только, что для каждого простого числа p имеет место неравенство

$$\sum_{h=0}^{\infty} A(m, p^h) \geqslant p^{-6}. \tag{8.56}$$

Из (8.5) легко вывести (ср. с леммой 2.12), что

$$p^{2t} \sum_{h=0}^{t} A(m, p^h) = M(m, p^t), \tag{8.57}$$

где $M(m, p^t)$ — число решений сравнения

$$x^2 + y^3 + z^5 \equiv m \pmod{p^t} \tag{8.58}$$

с $1 \leqslant x, y, z \leqslant p^t$. Пусть $\gamma(2) = 3$, $\gamma(p) = 1$. $(p > 2)$. При $p \nmid a$ сравнение $x^2 \equiv a \pmod{p^t}$ имеет решение для каждого $t \geqslant \gamma(p)$ всякий раз, когда оно имеет решение для $t = \gamma(p)$. Таким образом, если возможно показать, что (8.58) разрешимо, когда $t = \gamma(p)$ с $p \nmid x$, то $p^{2t-2\gamma(p)}$ различных решений можно получить в общем случае $t \geqslant \gamma(p)$, взяв любые y', z', такие, что $y' \equiv y \pmod{p^{\gamma(p)}}$, $z' \equiv z \pmod{p^{\gamma(p)}}$. Таким образом,

$$M(m, p^t) \geqslant p^{2t-2\gamma(p)},$$

что ввиду (8.57) дает неравенство (8.56).

То, что (8.58) разрешимо с $2 \nmid x$, когда $p = 2$ и $t = \gamma(p) = 3$, тривиально. Остается установить соответствующий результат для $p > 2$.

Число кубических или нулевых вычетов по модулю p по меньшей мере равно $(p-1)/(3, p-1) + 1$. Заключение будет следовать отсюда по принципу «ящиков», если показать, что число N вычетов по модулю p вида x^2 или $x^2 + 1$ с $1 \leqslant x \leqslant p - 1$ имеет выражение

$$N = \frac{1}{4}\left(3p + \left(\frac{-1}{p}\right)_L\right).$$

Этот результат легко получается из формулы

$$N = p - \frac{1}{2} + \frac{1}{2}\left(\frac{-1}{p}\right)_L - \sum_{x=2}^{p-1} \frac{1}{4}\left(1 - \left(\frac{x}{p}\right)_L\right)\left(1 - \left(\frac{x-1}{p}\right)_L\right).$$

8.8 Упражнения

1. Покажите, что почти каждое натуральное число имеет вид $p + x^k$.
2. Покажите, что $\operatorname{card}\{n\colon n \neq p + x^k,\ n \leqslant X\} \gg X^{1/k}$.

3. Пусть $R(n)$ означает число решений уравнения
$$x^2+y^3+z^6=n$$
с $x>0$, $y>0$, $z>0$. Покажите, что
(i) $\sum_{n\leqslant X} R(n)=X\Gamma\left(\frac{3}{2}\right)\Gamma\left(\frac{4}{3}\right)\Gamma\left(\frac{7}{6}\right)+O\left(X^{5/6}\right)$,
(ii) $\Gamma\left(\frac{2}{3}\right)\Gamma\left(\frac{4}{3}\right)\Gamma\left(\frac{7}{6}\right)=0{,}73\ \ldots$,
(iii) $x^2+y^3+z^6\equiv n \pmod q$ всегда разрешимо с $(x, q)=1$.
4. Получите асимптотическую формулу для числа представлений числа в виде суммы двух квадратов, двух кубов и двух пятых степеней.

Примечание редактора

[1] См. также замечательные работы К. Хооли: On Waring's problem for two squares and three cubes. J. Reine Angew. Mathem., 1981, 328, p. 161—207; On another sieve method and the numbers that are a sum of two h-th powers. Proc. London Math. Soc. 1981, 43 : 3, p. 73—109.

9

Однородные уравнения и теорема Бёрча

9.1 Введение

Пусть $F(x_1, \ldots, x_s)$ — однородная форма степени $k \geqslant 2$ с целыми коэффициентами. Естественно возникает вопрос, имеет ли уравнение

$$F(x_1, \ldots, x_s) = 0 \tag{9.1}$$

нетривиальное решение, т. е. решение в целых x_j, не все из которых равны нулю. Очевидно, если k четное, указанное уравнение может иметь только тривиальное решение. Однако, когда k нечетное, можно надеяться на большее. Льюис [Lewis, 19ý7], основываясь на ранней работе Брауэра [Brauer, 1945], показал, что для достаточно большого s любая кубическая форма от s переменных с целыми коэффициентами имеет нетривиальный нуль. Вскоре это утверждение было распространено Бёрчем [Birch, 1957] на формы произвольной нечетной степени. В действительности Бёрч доказал даже несколько больше. Целью настоящей главы является рассмотрение теоремы Бёрча. О более поздних работах в этом направлении и близких темах читатель может узнать из сборника работ Дэвенпорта (1977).

Доказательство теоремы Бёрча основано на частном случае, именно на разрешимости аддитивного однородного уравнения

$$c_1 x_1^k + \ldots + c_s x_s^k = 0, \tag{9.2}$$

а это может быть установлено при помощи метода Харди — Литтлвуда.

9.2 Аддитивные однородные уравнения

Для получения следующей теоремы применимы методы гл. 2, 4 и 5, поэтому ее доказательство дано лишь в общих чертах.

Теорема 9.1. *Пусть* $k \geqslant 2$ *и* s_0, *как в теореме* 5.4, *и пусть* $s \geqslant \min(s_0, 2^k + 1)$ *и* $s \geqslant 4k^2 - k + 1$. *Предположим также,* *что когда k — четное, не все целые числа $c_1, \ldots, c_s$ имеют один знак. Тогда уравнение* (9.2) *имеет нетривиальное решение в целых числах $x_1, \ldots, x_s$.*

Всюду в этом параграфе постоянные могут зависеть от $c_1, \ldots, c_s$.

Если имеется j, такое, что $c_j = 0$, утверждение теоремы тривиально. Таким образом, можно считать, что для любого j $c_j \neq 0$. Для нечетного k также можно считать (если необходимо, заменяя x_1 на $-x_1$), что не все c_j имеют один знак. Пусть $R(N)$ означает число решений уравнения (9.2) с $1 \leqslant x_j \leqslant N$. Тогда методы, развитые в гл. 2, 4 и 5, дают

$$R(N) = \mathfrak{S}J(N) + O\left(N^{s-k-\delta}\right),$$

где

$$\mathfrak{S} = \prod_p T(p), \quad T(p) = \sum_{h=0}^{\infty} S(p^h),$$

$$S(q) = \sum_{\substack{a=1 \\ (a,\, q)=1}}^{q} \prod_{j=1}^{s} \left(q^{-1} S(q,\, ac_j)\right)$$

и

$$J(N) = \sum_{\substack{m_1=1 \\ c_1m_1+\ldots+c_sm_s=0}}^{N^k} \cdots \sum_{m_s=1}^{N^k} k^{-s} (m_1 \ldots m_s)^{1/k-1}.$$

Эти методы показывают далее, что существует число C, зависящее разве что от $c_1, \ldots, c_s$, такое, что

$$\prod_{p>C} T(p) > \tfrac{1}{2}$$

и

$$J(N) \gg N^{s-k}.$$

Теперь достаточно показать, что $T(p) > 0$, и снова это будет следовать, если показать, что $M_F(q)$, число решений сравнения

$$F(x_1, \ldots, x_s) = c_1 x_1^k + \ldots + c_s x_s^k \equiv 0 \pmod q$$

с $1 \leqslant x_j \leqslant q$, удовлетворяет для достаточно большого t неравенству

$$M_F(p^t) > C(p)\, p^{t(s-1)} \tag{9.3}$$

с некоторым положительным $C(p)$, зависящим только от $c_1, \ldots, c_s$ и p.

Для того чтобы оценить M_F, необходимо преобразовать переменные так, чтобы получить новую форму H, в которой подходящее число коэффициентов взаимно просто с p. Выберем τ_j так, что $p^{\tau_j} \| c_j$, и h_j, l_j так, что $\tau_j = h_j k + l_j$ и $0 \leqslant$

$\leqslant l_j < k$. Тогда

$$F(x_1, \ldots, x_s) = G(p^{h_1}x_1, \ldots, p^{h_s}x_s),$$

где
$$G(x_1, \ldots, x_s) = d_1 p^{l_1} x_1^k + \ldots + d_s p^{l_s} x_s^k$$

и $d_j = c_j p_j^{-\tau_j}$. Пусть теперь $h = \max h_j$. Тогда

$$F(p^{h-h_1}x_1, \ldots, p^{h-h_s}x_s) = p^{hk} G(x_1, \ldots, x_s)$$

и для $t > h$

$$M_F(p^t) \geqslant \sum_{x_1=1}^{p^{t-h+h_1}} \cdots \sum_{\substack{x_s=1 \\ p^{hk}G(x_1,\ldots,x_s) \equiv 0 \pmod{p^t}}}^{p^{t-h+h_s}} 1 \geqslant M_G(p^{t-hk}) \prod_{j=1}^{s} p^{hk-h+h_j},$$

откуда
$$M_F(p^t) \geqslant M_G(p^{t-hk}). \tag{9.4}$$

Форму G можно переписать в виде

$$G = G^{(0)} + pG^{(1)} + \ldots + p^{k-1}G^{(k-1)},$$

где
$$G^{(j)} = G^{(j)}(x^{(j)}) = \sum_{\substack{i=1 \\ l_i = j}}^{s} d_i x_i^k.$$

Очевидно, существуют i и r, такие, что $r \geqslant s/k$ и $G^{(i)}$ содержит по крайней мере r переменных. Рассмотрим форму

$$H(x_1, \ldots, x_s) = \Big(\sum_{j<i} p^j G^{(j)}(px^{(j)}) + \sum_{j \geqslant i} p^j G^{(j)}(x^{(j)}) \Big) p^{-i}.$$

Теперь
$$M_G(p^t) \geqslant M_H(p^{t-i}) \tag{9.5}$$

и H имеет вид

$$H = H^{(0)} + pH^{(1)} + \ldots + p^{k-1}H^{(k-1)},$$

где $H^{(0)}$ содержит по крайней мере r переменных, $r \geqslant s/k$, и все ее коэффициенты взаимно просты с p. Можно считать, если необходимо, переименовав переменные, что

$$H^{(0)} = H^{(0)}(x_1, \ldots, x_r) = d_1 x_1^k + \ldots + d_r x_r^k.$$

Согласно неравенствам (9.5) и (9.4), для доказательства (9.3) теперь достаточно показать, что существует положительное число $C_1(p)$, такое, что для достаточно большого t

$$M_H(p^t) > C_1(p) p^{t(s-1)}. \tag{9.6}$$

Пусть τ означает наивысшую степень p, делящую k, и положим $\gamma = \tau + 1$ при $p > 2$ или $\tau = 0$ и $\gamma = \tau + 2$ при $p = 2$ и $\tau \geqslant 1$. Тогда, как в § 2.6, будем иметь (9.6), если показать, что для каждого m сравнение

$$d_1 x_1^k + \ldots + d_r x_r^k \equiv m \pmod{p^\gamma} \tag{9.7}$$

разрешимо в $x_1, \ldots, x_r$ с $p \nmid x_1$.

Пусть $K = p^{\gamma-\tau-1}(k, p^{\tau}(p-1))$. Тогда число k-х степеней вычетов по модулю p^{γ} есть $\varphi(p^{\gamma})/K$. Следовательно, по лемме 2.14 множество $\mathscr{M}_j$ вычетов m по модулю p^{γ}, которые могут быть записаны в виде

$$d_1x_1^k + \ldots + d_jx_j^k, \quad (p \nmid x_1),$$

удовлетворяет условию $\operatorname{card}\mathscr{M}_j \geqslant \min(p^{\gamma}, j\varphi(p^{\gamma})/K)$. Таким образом, если $r \geqslant 4k$, т. е. $s \geqslant 4k^2 - k$, то (9.7) имеет решение желаемого типа, и это завершает доказательство теоремы 9.1.

Предположим, что $c_1, \ldots, c_s$ — целые, такие, что для каждого q сравнение $c_1x_1^k + \ldots + c_sx_s^k \equiv 0 \pmod q$ имеет решение с $(x_j, q) = 1$ для некоторого j. Тогда, следуя Дэвенпорту и Льюису (1963), говорят, что $c_1, \ldots, c_s$ удовлетворяют *условию конгруэнтности*, $\Gamma^*(k)$ определяют как наименьшее s, такое, что каждая последовательность целых $c_1, \ldots, c_s$ удовлетворяет условию конгруэнтности, а $G^*(k)$ — как наименьшее число t, такое, что всякий раз, как $s \geqslant t$, уравнение

$$c_1x_1^k + \ldots + c_sx_s^k = 0$$

имеет нетривиальное решение в целых числах, если $c_1, \ldots, c_s$, не все одного знака при четном k и удовлетворяют условию конгруэнтности.

Предыдущие рассуждения дают $\Gamma^*(k) \leqslant 4k^2 - k + 1$ и $G^*(k) \leqslant \min(s_0, 2^k + 1)$. Дэвенпорт и Льюис показали: (i) что $\Gamma^*(k) \leqslant k^2 + 1$; (ii) что $\Gamma^*(k) = k^2 + 1$, когда $k+1$ простое, и (iii) что $G^*(k) \leqslant k^2 + 1$, когда $k \geqslant 18$ и $k \leqslant 6$. Вон (1976*b*) сократил разрыв в (iii), применив методы гл. 5, 6, 7 при $11 \leqslant k \leqslant 17$.

Для малых значений k величина $\Gamma^*(k)$ известна. (См. [Bierstedt, 1963], [Bovey, 1974], [Dodson, 1967], [Norton, 1966].) Также, на основе более ранних работ Нортона [Norton, 1966] и Човлы, Шимуры [Chowla, Shimura, 1963], Титавайненом [Tietavainen, 1971] было показано, что

$$\limsup_{k\to\infty} \frac{\Gamma^*(2k+1)}{k \log k} = \frac{2}{\log 2}.$$

9.3 Теорема Бёрча

Теорема 9.2 (Бёрч, 1957). *Пусть j, l — натуральные числа, и пусть $k_1, \ldots, k_j$ — нечетные натуральные числа. Тогда существует число $\Psi_j(k_1, \ldots, k_j, l)$ со следующим свойством. Пусть $F_1(\mathbf{x}), \ldots, F_j(\mathbf{x})$ — формы от $\mathbf{x} = (x_1, \ldots, x_s)$ степеней $k_1, \ldots, k_j$ соответственно с рациональными коэффициентами.*

Тогда, каково бы ни было

$$s \geqslant \Psi_j(k_1, \ldots, k_j, l),$$

существует l-мерное векторное пространство V в $\mathbb{Q}^s$, такое, что для каждого $\mathbf{x} \in V$

$$F_1(\mathbf{x}) = \ldots = F_j(\mathbf{x}) = 0.$$

На первом шаге доказательства устанавливается справедливость теоремы в случае, когда $j = 1$, F_1 аддитивна и $k \geqslant 3$.

Лемма 9.1. *Существует число $\Phi(k, l)$, определенное для натуральных чисел k, l с нечетным $k \geqslant 3$, такое, что если $s \geqslant \Phi(k, l)$, то для каждой формы $c_1x_1^k + \ldots + c_sx_s^k$ с рациональными $c_1, \ldots, c_s$ существует l-мерное векторное пространство V в $\mathbb{Q}^s$, такое, что для любого $\mathbf{x} \in V$*

$$c_1x_1^k + \ldots + c_sx_s^k = 0. \tag{9.8}$$

Доказательство. По теореме 9.1 найдутся $t = t(k)$ и $y_1, \ldots, y_t$, не все равные нулю, такие, что

$$c_1y_1^k + \ldots + c_ty_t^k = 0.$$

Аналогично для

$$c_{t+1}y_{t+1}^k + \ldots + c_{2t}y_{2t}^k = 0$$

и т. д. Следовательно, при $s \geqslant lt$ точка

$$(u_1y_1, \ldots, u_1y_t, u_2y_{t+1}, \ldots, u_2y_{2t}, \ldots, u_ly_{lt}, 0, \ldots, 0)$$

удовлетворяет уравнению (9.8) для всех $u_1, \ldots, u_l$.

Доказательство теоремы 9.2. Пусть $k = \max k_i$, так что k — нечетное положительное число. Доказательство проводится индукцией по нечетным k. Для $k = 1$ результат установлен. При $k \geqslant 3$ главный шаг состоит в том, чтобы показать: если теорема имеет место для систем форм, таких, что $\max k_i \leqslant k - 2$, то она справедлива для одной формы степени k. Это заключение затем легко обобщается на систему форм степени не выше k.

Для формы

$$F(\mathbf{x}) = F(x_1, \ldots, x_s) = \sum_{i_1, \ldots, i_k} c_{i_1, \ldots, i_k} x_{i_1} \ldots x_{i_k}$$

(нечетной) степени k рассмотрим

$$F(u_0\mathbf{y}^{(0)} + u_1\mathbf{y}^{(1)} + \ldots + u_{n+1}\mathbf{y}^{(n+1)}) =$$
$$= \sum_{i_1, \ldots, i_k} c_{i_1, \ldots, i_k}\left(u_0 y_{i_1}^{(0)} + \ldots + u_{n+1} y_{i_1}^{(n+1)}\right) \ldots$$
$$\ldots \left(u_0 y_{i_k}^{(0)} + \ldots + u_{n+1} y_{i_k}^{(n+1)}\right) =$$
$$= \sum_{\substack{j_1, \ldots, j_k \\ 0 \leqslant j_r \leqslant n+1}} u_{j_1} \ldots u_{j_k} \sum_{i_1, \ldots, i_k} c_{i_1, \ldots, i_k} y_{i_1}^{(j_1)} \ldots y_{i_k}^{(j_k)}.$$

Теперь определим $\mathbf{e}^{(1)} = (1, 0, 0, \ldots)$, $\mathbf{e}^{(2)} = (0, 1, 0, \ldots)$ и т. д. и возьмем $u_0 = v$, $\mathbf{y}^{(0)} = \mathbf{y}$, $\mathbf{y}^{(1)} = \mathbf{e}^{(1)}$, $\mathbf{y}^{(2)} = \mathbf{e}^{(2)}$, $\ldots$. Тогда перегруппировка членов дает

$$F(v\mathbf{y} + u_1\mathbf{e}^{(1)} + \ldots + u_{n+1}\mathbf{e}^{(n+1)}) =$$
$$= \sum_{h=0}^{k} v^h \sum_{\substack{j_1, \ldots, j_{k-h} \\ 1 \leqslant j_r \leqslant n+1}} u_{j_1} \ldots u_{j_{k-h}} F(\mathbf{y}; h, j_1, \ldots, j_{k-h}), \qquad (9.9)$$

где
$$F(\mathbf{y}; h, j_1, \ldots, j_{k-h})$$

— форма степени h от $\mathbf{y} = (y_1, \ldots, y_s)$. Общее число таких форм с нечетным h, $1 \leqslant h \leqslant k-2$ и $1 \leqslant j_r \leqslant n+1$, не превосходит $k(n+1)^k$. Следовательно, в силу предположения индукции находим, что при условии

$$s \geqslant \Psi_{k(n+1)^k}(k-2, \ldots, k-2, 1)$$

соответствующие уравнения

$$F(\mathbf{y}; h, j_1, \ldots, j_{k-h}) = 0$$

имеют нетривиальное решение $\mathbf{z}^{(0)}$ в $\mathbb{Q}^s$.

Если $\mathbf{z}^{(0)}, \mathbf{e}^{(1)}, \ldots, \mathbf{e}^{(n+1)}$ линейно зависимы в $\mathbb{Q}^s$, то исключение одного из $\mathbf{e}^{(j)}$ дает линейную независимость множества $n+1$ точек в $\mathbb{Q}^s$. Таким образом, в любом случае, беря в качестве одного из u_j в (9.9) нуль и, если необходимо, переименовывая переменные, получаем, что $\mathbf{z}^{(0)}, \mathbf{z}^{(1)}, \ldots, \mathbf{z}^{(n)}$ линейно независимы и таковы, что

$$F(v\mathbf{z}^{(0)} + u_1\mathbf{z}^{(1)} + \ldots + u_n\mathbf{z}^{(n)}) =$$
$$= cv^k + \sum_{\substack{h=2 \\ h \text{ четное}}}^{k-1} v^h G_h(\mathbf{u}) + G_0(\mathbf{u}), \qquad (9.10)$$

где $G_h(\mathbf{u})$ — форма степени $k-h$ от $\mathbf{u} = (u_1, \ldots, u_n)$.

Линейная независимость $\mathbf{z}^{(0)}, \ldots, \mathbf{z}^{(n)}$ обеспечивает то, что, если

$$\mathbf{x} = v\mathbf{z}^{(0)} + u_1\mathbf{z}^{(1)} + \ldots + u_n\mathbf{z}^{(n)},$$

нетривиальные наборы $(v, u_1, \ldots, u_n)$ дают нетривиальные значения для $\mathbf{x}$.

Рассмотрим систему форм

$$G_h(\mathbf{u}) = 0, \ h \text{ четное}, \ 2 \leqslant h \leqslant k-1. \tag{9.11}$$

Степень $k-h$ нечетна в каждом случае. Следовательно, дальнейшее применение предположения индукции показывает, что, когда $n \geqslant \Psi_k(k-2, \ldots, k-2, m)$, т. е.

$$s \geqslant s_0(k, m),$$

система (9.11) разрешима для каждого вектора $\mathbf{u}$ m-мерного векторного пространства U в $\mathbb{Q}^n$. Пусть $u^{(1)}, \ldots, u^{(m)}$ m линейно независимых точек в U и

$$\mathbf{u} = w_1\mathbf{u}^{(1)} + \ldots + w_m\mathbf{u}^{(m)}.$$

Линейная независимость снова обеспечивает то, что нетривиальность $\mathbf{w}$ в $\mathbb{Q}^m$ влечет за собой нетривиальность $\mathbf{u}$ в $\mathbb{Q}^n$. Следовательно, по формуле (9.10) для нетривиального вектора $(v, w_1, \ldots, w_m)$ существует нетривиальный вектор $\mathbf{x} = (x_1, \ldots, x_s)$, такой, что

$$F(\mathbf{x}) = cv^k + H(\mathbf{w}),$$

где H — форма от $\mathbf{w} = (w_1, \ldots, w_m)$ степени k, т. е. F представляется в виде $cv^k + H(\mathbf{w})$.

Повторение этих рассуждений показывает, что если $s \geqslant s_1(k, l)$, то F представляется диагональной формой

$$c_1v_1^k + \ldots + c_tv_t^k,$$

где $t = \Phi(k, l)$. Лемма 9.1 теперь дает случай $j = 1$, $k_1 = k$ теоремы.

Чтобы завершить рассуждения индукции, остается исследовать общий случай системы j уравнений $F_1 = \ldots = F_j = 0$ с $\max k_i = k$. Это делается в свою очередь индукцией по j. Случай $j = 1$ был только что рассмотрен. Предположим, что $j > 1$. Не ограничивая общности, можно предполагать, что $k_j = k$. Согласно утверждению в случае $j = 1$, если для данного m $s \geqslant \Psi_1(k_j, m)$, то существует m-мерное векторное пространство U в $\mathbb{Q}^s$, такое, что $F_j(\mathbf{x}) = 0$ для любого $\mathbf{x} \in U$. Точки U могут быть представлены в виде

$$y_1\mathbf{x}^{(1)} + \ldots + y_m\mathbf{x}^{(m)},$$

где $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(m)}$ — линейно независимые точки $\mathbb{Q}^s$. Для этих точек формы $F_1, \ldots, F_{j-1}$ становятся формами от $\mathbf{y} = (y_1, \ldots, y_m)$. Если

$$\max_{1 \leqslant i \leqslant j-1} k_i \leqslant k-2,$$

то используется главное предположение индукции. Если

$$\max_{1 \leqslant i \leqslant j-1} k_i = k,$$

то используется предположение индукции по j. В любом случае при условии, что $m \geqslant \Psi_{j-1}(k_1, \ldots, k_{i-1}, l)$, существует l-мерное векторное пространство V в $\mathbb{Q}^m$, на котором каждая форма F_i равна нулю. Это заканчивает доказательство теоремы. [1]

9.4. Упражнения

1. Применяя методы гл. 7, покажите, что

$$\limsup_{k \to \infty} \frac{G^*(k)}{k \log k} \leqslant 2.$$

2. Применяя методы гл. 6, покажите, что $G^*(3) \leqslant 8$, $G^*(4) \leqslant 14$, $G^*(5) \leqslant 23$, $G^*(6) \leqslant 36$.
3. Покажите, что $\Gamma^*(2) = 5$, $\Gamma^*(3) = 7$, $\Gamma^*(4) = 17$ и что $\Gamma^*(k) \leqslant \min(s_0, 2^k + 1)$.

Примечание редактора

[1] В связи с теоремой Бёрча см работы Архипова Г. И. и Карацубы А. А. О локальном представлении нуля формой. Изв. АН СССР, сер. матем., 1981, 45 : 5, с. 948—961. Об одной задаче теории сравнений. УМН, 1982, 37 : 5, с. 161—162; здесь, в частности доказана теорема: *Пусть p — простое число; для любого натурального числа r существует такое $n_1 = n_1(r; p)$, что при $n \geqslant n_1$ существует форма $F(x_1, \ldots, x_K)$ степени, не превосходящей n, с целым коэффициентами, число переменных которой K, $K \geqslant p^n$,*

$$u = \frac{n}{\log_p n \log_p \log_p n \ldots \underbrace{\log_p \ldots \log_p n}_{r} \underbrace{\log_p \ldots \log_p^3 n}_{r+1}},$$

и тривиально представляющая нуль в поле p-адических чисел.

10
Теорема Рота

10.1 Введение

В 1927 г. Ван дер Варден [Waerden, B. L. van der, 1927] доказал, что для заданных натуральных чисел l, r существует $n_0(l, r)$, такое, что если $n \geqslant n_0(l, r)$ и множество $\{1, 2, \ldots, n\}$ разбито на r подмножеств, то по крайней мере одно подмножество содержит l членов арифметической прогрессии.

Для произвольного множества натуральных чисел $\mathscr{A}$ пусть

$$A(n) = A(n, \mathscr{A}) = \sum_{a \leqslant n,\ a \in \mathscr{A}} 1, \quad D(n) = D(n, \mathscr{A}) = \frac{1}{n} A(n) \tag{10.1}$$

и $\underline{d}$ и $\bar{d}$ — соответственно нижняя и верхняя асимптотические плотности $\mathscr{A}$:

$$\underline{d} = \underline{d}(\mathscr{A}) = \liminf_{n \to \infty} D(n), \quad \bar{d} = \bar{d}(\mathscr{A}) = \limsup_{n \to \infty} D(n). \tag{10.2}$$

В случае когда $\underline{d} = \bar{d}$, пусть $d = d(\mathscr{A})$ означает их общее значение, асимптотическую плотность $\mathscr{A}$. Эрдеш и Туран [Erdos, Turan, 1936] на основе анализа известных доказательств теоремы ван дер Вардена высказали предположение, что каждое множество $\mathscr{A}$ с $\bar{d}(\mathscr{A}) > 0$ содержит арифметические прогрессии произвольной длины. Эквивалентное утверждение состоит в том, что если существует l, такое, что $\mathscr{A}$ не содержит l членов арифметической прогрессии, то $d(\mathscr{A}) = 0$.

Первый нетривиальный случай: $l = 3$. Справедливость предположения в этом случае впервые установил Рот [Roth, 1952, 1953, 1954] при помощи остроумного применения метода Харди — Литтлвуда.

Другим методом Семереди [Szemeredi, 1969] доказал предположение для $l = 4$, а Рот (1972) дал иное доказательство, используя свой предыдущий метод.

В 1975 г. Семереди установил общий случай. К сожалению, доказательство Семереди использует теорему Ван дер Вардена. Позднее Фюрстенбург [Furstenburg, 1977] доказал теорему Семереди, основываясь на идеях эргодической теории. Хотя в доказательстве не применяется теорема Ван дер

Вардена, очевидно, что оно имеет похожую структуру и, таким образом, все еще не дает желаемого результата.

Идеи, возникшие при изучении проблемы, позволили Фюрстенбургу (1977) и Шаркёзи [Sàrközy, 1978*a*, *b*] установить, что если $\bar{d}(\mathscr{A}) > 0$, то множество чисел вида $a - a'$ с $a \in \mathscr{A}$, $a' \in \mathscr{A}$ содержит бесконечно много полных квадратов.

В этой главе доказывается теорема Рота с использованием его варианта метода Харди — Литтлвуда и развивается доказательство теоремы Шаркёзи — Фюрстенбурга по Фюрстенбургу, но без эргодической теории.

На протяжении всей главы постоянные являются абсолютными.

10.2 Теорема Рота

Пусть $M^{(l)}(n)$ означает наибольшее число элементов, которые можно выбрать из множества $\{1, 2, \ldots, n\}$ так, чтобы никакие l из них не принадлежали прогрессии. Пусть

$$\mu^{(l)}(n) = n^{-1} M^{(l)}(n).$$

Тогда теорема Семереди формулируется в виде

$$\lim_{n \to \infty} \mu^{(l)}(n) = 0,$$

что, очевидно, включает в себя предположение Эрдеша — Турана. Как показывает следующая лемма, легко доказать, что такой предел существует. Другое дело — найти его значение.

Лемма 10.1. *Для любого целого числа l существует $\lim_{n \to \infty} \mu^{(l)}(n)$. Кроме того, для $m \geqslant n$ справедливо неравенство $\mu^{(l)}(m) \leqslant 2\mu^{(l)}(n)$.*

Доказательство. Из определения $M^{(l)}$ тривиально следует, что

$$M^{(l)}(m+n) \leqslant M^{(l)}(m) + M^{(l)}(n).$$

Поэтому

$$M^{(l)}(m) \leqslant \left[\frac{m}{n}\right] M^{(l)}(n) + M^{(l)}\left(m - n\left[\frac{m}{n}\right]\right) \leqslant$$

$$\leqslant \frac{m}{n} M^{(l)}(n) + n.$$

Следовательно, $\mu^{(l)}(m) \leqslant \mu^{(l)}(n) + n/m$, так что

$$\limsup_{m \to \infty} \mu^{(l)}(m) \leqslant \mu^{(l)}(n),$$

откуда

$$\limsup_{m\to\infty} \mu^{(l)}(m) \leqslant \liminf_{n\to\infty} \mu^{(l)}(n),$$

Кроме того, при $m \geqslant n$ $M^{(l)}(m) \leqslant (m/n+1) M^{(l)}(n) \leqslant \leqslant 2M^{(l)}(n) m/n$.

Следующая теорема не только показывает, что при $l=3$ рассматриваемый предел равен нулю, но и дает оценку величины $M^{(3)}(n)$.

Теорема 10.1 (Рот). *Пусть* $n \geqslant 3$. *Тогда* $\mu^{(3)}(n) \ll \ll (\log\log n)^{-1}$.

С этого момента предполагается, что $l=3$, и для удобства верхний индекс (l) опускается.

Выберем $\mathscr{M} \subset \{1, 2, \ldots, n\}$, так что $\operatorname{card} \mathscr{M} = M(n)$ и никакие 3 элемента $\mathscr{M}$ не принадлежат прогрессии. Пусть

$$f(\alpha) = \sum_{m\in\mathscr{M}} e(\alpha m).$$

Тогда
$$M(n) = \int_0^1 f(\alpha)^2 f(-2\alpha)\, d\alpha, \tag{10.3}$$

поскольку интеграл справа равен числу решений уравнения $m_1 + m_2 = 2m_3$ с $m_j \in \mathscr{M}$, а по построению $\mathscr{M}$ такие решения могут быть только при $m_1 = m_2 = m_3$.

Пусть $\varkappa(x)$ означает характеристическую функцию множества $\mathscr{M}$, так что

$$f(\alpha) = \sum_x \varkappa(x) e(\alpha x). \tag{10.4}$$

Предположим, что
$$m < n, \tag{10.5}$$
и рассмотрим
$$v(\alpha) = \mu(m) \sum_{x=1}^{n} e(\alpha x) \tag{10.6}$$
и
$$E(\alpha) = v(\alpha) - f(\alpha).$$
Тогда
$$E(\alpha) = \sum_{x=1}^{n} c(x) e(\alpha x), \tag{10.7}$$
где
$$c(x) = \mu(m) - \varkappa(x). \tag{10.8}$$

Идея доказательства состоит в том, что если $M(n)$ близко к n, то интеграл

$$\int_0^1 f(\alpha)^2 f(-2\alpha)\, d\alpha$$

должен бы быть ближе к $M(n)^2$, чем к $M(n)$ (ср. с (10.3)). Чтобы показать это, прежде всего используется беспорядочность арифметической структуры $\mathcal{M}$, чтобы заменить f на v со сравнительно малой погрешностью. Это достаточно общий принцип, возникший из применений метода, изложенного в предыдущих главах; суммы вида

$$\sum_{x \leqslant n,\ x \in \mathcal{A}} e(\alpha x)$$

стремятся иметь «пики» в точках a/q, когда элементы $\mathcal{A}$ регулярно распределены в классах вычетов по модулю q, тогда как $v(\alpha)$ имеет «пики» значений в целых точках.

Пусть

$$F(\alpha) = \sum_{z=0}^{m-1} e(\alpha z). \tag{10.9}$$

Лемма 10.2. *Пусть q — натуральное число, $q < n/m$, и для $y = 1, 2, \ldots, n - mq$ пусть*

$$\sigma(y) = \sigma(y;\ m,\ q) = \sum_{x=0}^{m-1} c(y + xq). \tag{10.10}$$

Тогда

$$\sigma(y) \geqslant 0 \quad (y = 1, 2, \ldots, n - mq) \tag{10.11}$$

и

$$F(\alpha q) E(\alpha) = \sum_{y=1}^{n-mq} \sigma(y) e(\alpha(y + mq - q)) + R(\alpha), \tag{10.12}$$

где $R(\alpha)$ удовлетворяет неравенству

$$|R(\alpha)| < 2m^2 q. \tag{10.13}$$

Доказательство. Объединяя члены произведения FE, для которых $x + zq = h + mq - q$, получаем

$$F(\alpha q) E(\alpha) = \sum_{h=1+q-mq}^{n} e(\alpha(h + mq - q)) \times \\ \times \sum_{\substack{z=0 \\ 1 \leqslant h + q(m-1-z) \leqslant n}}^{m-1} c(h + q(m - 1 - z)).$$

Внутренняя сумма по абсолютной величине не больше m, поэтому общий вклад членов с $h \leqslant 0$ и $h > n - mq$ не превышает по модулю $m(mq + (m-1)q) < 2m^2 q$. Для остальных значений h имеем $1 \leqslant h + q(m - 1 - z) \leqslant n$ для всех z в интервале $[0, m - 1]$. Это дает (10.12) и (10.13).

Согласно (10.8) и (10.10),

$$\sigma(y) = M(m) - \sum_{x=0}^{m-1} \varkappa(y + xq).$$

Пусть

$$r = \sum_{x=0}^{m-1} \varkappa(y + xq).$$

Тогда r — число элементов $\mathcal{M}$ среди y, $y+q$, ..., $y+(m-1)q$. Пусть это элементы $y+x_1 q$, ..., $y+x_r q$. Тогда никакие три из них не принадлежат прогрессии. Следовательно, никакие три из чисел x_1, ..., x_r не принадлежат прогрессии. Те же рассуждения применимы для $1+x_1$, ..., $1+x_r$. Кроме того, $1+x_j \leqslant m$. Отсюда $r \leqslant M(m)$, что дает (10.11).

Лемма 10.3. *Предположим, что $2m^2 < n$. Тогда для каждого действительного числа α*

$$|E(\alpha)| < 2n(\mu(m) - \mu(n)) + 16m^2.$$

Доказательство. По лемме 2.1 существуют a, q, такие, что $(a, q) = 1$, $1 \leqslant q \leqslant 2m$ и $|\alpha - a/q| \leqslant 1/(2qm)$. Тогда

$$F(\alpha, q) = F(\alpha q - a) = F(\beta),$$

где $|\beta| \leqslant 1/(2m)$. Следовательно, согласно (10.9),

$$|F(\alpha q)| = \left|\frac{\sin \pi m\beta}{\sin \pi\beta}\right| \geqslant \frac{2m}{\pi}.$$

Таким образом, в силу леммы 10.2

$$\frac{1}{2} m |E(\alpha)| \leqslant \frac{2}{\pi} m |E(\alpha)| \leqslant |F(\alpha q) E(\alpha)| <$$
$$< \sum_{y=1}^{n-mq} \sigma(y) + 2m^2 q < mE(0) + 8m^3.$$

Кроме того, согласно (10.7) и (10.8),

$$E(0) = \sum_{x=1}^{n} (\mu(m) - \varkappa(x)) = n(\mu(m) - \mu(n)).$$

Отсюда следует лемма.

Доказательство теоремы 10.1. Пусть

$$I = \int_0^1 f(\alpha)^2 v(-2\alpha)\, d\alpha. \tag{10.14}$$

Тогда ввиду формул (10.4) и (10.6)

$$I = \sum_{\substack{a \in \mathcal{M} \\ 2 | a+b}} \sum_{b \in \mathcal{M}} \mu(m).$$

Таким образом, если M_1 — число нечетных элементов $\mathscr{M}$, а M_2 — число четных элементов, так что $M_1 + M_2 = M(n)$, то

$$I = \mu(m)\left(M_1^2 + M_2^2\right) \geqslant \tfrac{1}{2}\mu(m)M(n)^2. \qquad (10.15)$$

Согласно (10.3) и (10.14),

$$|M(n) - I| \leqslant (\max_{\alpha}|E(\alpha)|)\int_0^1 |f(\alpha)|^2\,d\alpha.$$

Следовательно, по лемме 10.3 и равенству Парсеваля, в случае когда $2m^2 < n$, имеем

$$|M(n) - I| \leqslant (2n(\mu(m) - \mu(n)) + 16m^2)M(n).$$

Отсюда ввиду (10.15)

$$\mu(m)\mu(n) \leqslant 4(\mu(m) - \mu(n)) + 34m^2n^{-1} \quad (2m^2 < n). \qquad (10.16)$$

Переход к пределу при $n \to \infty$, а затем при $m \to \infty$ показывает, что $\tau = \lim_{n\to\infty}\mu(n)$ удовлетворяет неравенству $\tau^2 \leqslant 0$. Для того чтобы получить количественное выражение этого, положим

$$\lambda(x) = \mu(2^{3^x}).$$

Ввиду леммы 10.1 достаточно показать, что $\lambda(2x) \ll x^{-1}$.

Согласно (10.16),

$$\lambda(y)\lambda(y+1) \leqslant 4(\lambda(y) - \lambda(y+1)) + 34 \times 2^{-3^y}.$$

Деление на $\lambda(y)\lambda(y+1)$, суммирование по $y = x, x+1, \ldots, 2x-1$ и применение леммы 10.1 дают

$$x \leqslant 4\lambda(2x)^{-1} + 200x\lambda(2x)^{-2}2^{-3^x}.$$

Если $\lambda(2x) > 1/x$, второй член справа $< \frac{1}{2}x$ для достаточно больших x, так что $\lambda(2x) < 8/x$, что дает желаемое утверждение.

10.3 Теорема Фюрстенбурга и Шаркоци

Теорема 10.2. *Пусть $\mathscr{A}$ — множество натуральных чисел с $\bar{d}(\mathscr{A}) > 0$, и пусть $R(n)$ — число решений уравнения*

$$a - a' = x^2$$

в a, a', x, где $a \in \mathscr{A}$, $a' \in \mathscr{A}$, $a \leqslant n$. Тогда

$$\limsup_{n\to\infty} R(n)\,n^{-3/2} > 0.$$

Эта теорема несколько сильнее теоремы 1.2 Фюрстенбурга (1977). У Шаркоци (1978) подход другой. Он применяет методы § 10.2, чтобы показать, что если уравнение $a - a' = x^2$ имеет только тривиальные решения, то

$$A(n) \ll n(\log\log n)^{2/3}(\log n)^{-1/3}.$$

Пусть $\mathcal{N}_0$ — бесконечное множество натуральных чисел, такое, что

$$\lim_{\substack{n \to \infty \\ n \in \mathcal{N}_0}} n^{-1} A(n) = \bar{d}(\mathcal{A}),$$

пусть
$$\mathfrak{M}_n(q, a) = \{\alpha : |\alpha - a/q| \leqslant q^{-1} n^{-1/2}\}, \tag{10.17}$$
и пусть
$$f(\alpha) = \sum_{\substack{a \leqslant n \\ a \in \mathcal{A}}} e(\alpha a).$$

Необходимо показать, что f имеет довольно обычное поведение на $\mathfrak{M}_n(q, a)$. Для $n \geqslant 4$

$$\int_{\mathfrak{M}_n(q, a)} |f(\alpha)|^2 d\alpha \leqslant \int_0^1 |f(\alpha)|^2 d\alpha \leqslant n.$$

Следовательно, интеграл

$$\int_{\mathfrak{M}_n(q, a)} |f(\alpha)|^2 n^{-1} d\alpha$$

ограничен равномерно по q, a, n. Поэтому можно выбрать бесконечные множества $\mathcal{N}(q, a)$ натуральных чисел, такие, что

$$\mathcal{N}(1, 1) = \mathcal{N}(1, 0) \subset \mathcal{N}_0, \quad \mathcal{N}(q+1, 1) \subset \mathcal{N}(q, q-1),$$

$\mathcal{N}(q, a') \subset \mathcal{N}(q, a)$ при $1 \leqslant a < a' \leqslant q-1$ и $(a', q) = (a, q) = 1$, и предел

$$\rho(q, a) = \lim_{\substack{n \to \infty \\ n \in \mathcal{N}(q, a)}} \int_{\mathfrak{M}_n(q, a)} |f(\alpha)|^2 n^{-1} d\alpha$$

существует. Таким образом, при заданном Q для всех достаточно больших n $n \in \mathcal{N}(Q, Q-1)$ имеем

$$\sum_{q \leqslant Q} \sum_{\substack{a=1 \\ (a, q)=1}}^{q} \rho(q, a) < 1 + \sum_{q \leqslant Q} \sum_{\substack{a=1 \\ (a, q)=1}}^{q} \int_{\mathfrak{M}_n(q, a)} |f(\alpha)|^2 n^{-1} d\alpha$$

и $\mathfrak{M}_n(q, a)$ с $1 \leqslant a \leqslant q \leqslant Q$, $(a, q) = 1$ попарно не пересекаются. Поэтому

$$\sum_{q \leqslant Q} \sum_{\substack{a=1 \\ (a,\, q)=1}}^{q} \rho(q, a) < 1 + \int_0^1 |f(\alpha)|^2 n^{-1} d\alpha \leqslant 2.$$

Следовательно, ряд $\sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,\, q)=1}}^{q} \rho(q, a)$

сходится.

10.4 Определение больших и малых дуг

Предположим, что $0 < \eta < 1$, и выберем $Q = Q_0(\eta)$, так что

$$\sum_{q=Q+1}^{\infty} \sum_{\substack{a=1 \\ (a,\, q)=1}}^{q} \rho(q, a) < \eta, \quad Q > \frac{1}{\eta}. \tag{10.18}$$

Теперь определим

$$k = (Q!)^2, \quad P = k^{100} \tag{10.19}$$

и, начиная отсюда, будем предполагать, что

$$n \in \mathcal{N}(P, P-1).$$

Затем для заданного $X \geqslant 1$ выберем $n_0 = n_0(\eta, X) \geqslant X^2$, так что при $n > n_0$ и $1 \leqslant a \leqslant q \leqslant P$, $(a, q) = 1$, большие дуги

$$\mathfrak{M}_{n,\, X}(q, a) = \{\alpha\colon\ |\alpha - a/q| \leqslant Xq^{-1}n^{-1}\}$$

попарно не пересекаются,

$$\int_{\mathfrak{M}_n(q,\, a)} |f(\alpha)|^2 n^{-1} d\alpha < \rho(q, a) + \eta P^{-2} \tag{10.20}$$

и

$$A(n) > \tfrac{2}{3} \bar{d} n. \tag{10.21}$$

Ввиду (10.17) для $n \geqslant n_0$ $\mathfrak{M}_{n,\, X}(q, a) \subset \mathfrak{M}_n(q, a)$. Поэтому в силу (10.20)

$$\int_{\mathfrak{M}_{n,\, X}(q,\, a)} |f(\alpha)|^2 n^{-1} d\alpha < \rho(q, a) + \eta P^{-2}. \tag{10.22}$$

Обозначим через $\mathfrak{M}$ объединение больших дуг $\mathfrak{M}_{n,\, X}(q, a)$ с $1 \leqslant a \leqslant q \leqslant P$ и $(a, q) = 1$ и определим малые дуги $\mathfrak{m}$, полагая

$$\mathfrak{m} = (Xn^{-1}, 1 + Xn^{-1}] \setminus \mathfrak{M}.$$

Далее

$$g(\beta) = \sum_{x=1}^{N} e(\beta x^2), \tag{10.23}$$

где

$$N \leqslant (n/k)^{1/2}. \tag{10.24}$$

Тогда, согласно (10.19),

$$R(n) \geqslant \mathcal{R}, \text{ где } \mathcal{R} = \int_{\mathfrak{t}}^{1} g(k\alpha) \, |f(\alpha)|^2 \, d\alpha. \tag{10.25}$$

В силу теоремы 4.1 при $(a, q) = 1$

$$g(\gamma) = q^{-1} S(q, a) \, h\left(\gamma - \frac{a}{q}\right) + O\left(q^{9/16}\left(1 + N^2 \left|\gamma - \frac{a}{q}\right|\right)\right), \tag{10.26}$$

где

$$S(q, a) = \sum_{x=1}^{q} e(ax^2/q), \qquad h(\beta) = \int_0^{N_2} \tfrac{1}{2} \alpha^{-1/2} e(\beta\alpha) \, d\alpha. \tag{10.27}$$

Кроме того, по теореме 4.2 $S(q, a) \ll q^{1/2}$.

10.5 Вклад малых дуг

Предположим, что $\alpha \in \mathfrak{m}$. Выберем a, q так, что $(a, q) = 1$, $q \leqslant N^{4/3}$, $|k\alpha - a/q| \leqslant q^{-1} N^{-4/3}$. Пусть $a_1 = a/(k, a)$, $q_1 = qk/(k, a)$. Тогда $|\alpha - a_1/q_1| \leqslant q^{-1} N^{-4/3}$ и $(a_1, q_1) = 1$. Поскольку $\alpha \in \mathfrak{m}$, либо $q_1 > P$, либо $|\alpha - a_1/q_1| > Xn^{-1} q_1^{-1}$. В первом случае в силу (10.26)

$$g(k\alpha) \ll q^{-1/2} N + q^{9/16}\left(1 + N^2 \left|k\alpha - \frac{a}{q}\right|\right) \ll$$
$$\ll N k^{1/2} P^{-1/2} + N^{3/4},$$

а во втором случае $|k\alpha - a/q| > Xn^{-1} q^{-1}$, так что ввиду (10.26), (10.27) и леммы 2.8

$$g(k\alpha) \ll q^{-1/2} \left|k\alpha - \frac{a}{q}\right|^{-1/2} + N^{3/4} \ll n^{1/2} X^{-1/2} + N^{3/4}.$$

Следовательно, согласно (10.19), в любом случае

$$g(k\alpha) \ll N k^{-40} + n^{1/2} X^{-1/2} + N^{3/4}.$$

Отсюда по равенству Парсеваля

$$\int_{\mathfrak{m}} g(k\alpha) \, |f(\alpha)|^2 \, d\alpha \ll \left(N k^{-40} + n^{1/2} X^{-1/2} + N^{3/4}\right) n. \tag{10.28}$$

10.6 Вклад больших дуг

Теперь предположим, что $\alpha \in \mathfrak{M}_{n,X}(q, a)$, где $1 \leqslant a \leqslant \leqslant q \leqslant P$ и $(a, q) = 1$. Пусть $q_1 = q/(q, k)$, $a_1 = ak/(q, k)$. Тогда ввиду (10.26)

$$g(k\alpha) = q_1^{-1} S(q_1, a_1)\, h\left(k\left(\alpha - \frac{a}{q}\right)\right) + \\ + O\left(q_1^{9/16}\left(1 + N^2 k \left|\alpha - \frac{a}{q}\right|\right)\right).$$

Остаточный член этой формулы мажорируется величиной $P + N^2 k X n^{-1}$. Поэтому

$$\int\limits_{\mathfrak{M}} g(k\alpha)\, |f(\alpha)|^2\, d\alpha = \mathcal{R}_1 + O(Pn + N^2 kX), \qquad (10.29)$$

где

$$\mathcal{R}_1 = \sum_{q \leqslant P} \sum_{\substack{a=1 \\ (a,\, q)=1}}^{q} \int\limits_{\mathfrak{M}_{n,\, X}(q,\, a)} q_1^{-1} S(q_1, a_1)\, h\left(k\left(\alpha - \frac{a}{q}\right)\right) |f(\alpha)|^2\, d\alpha.$$

В силу (10.22) и (10.18) сумма членов с $q \geqslant Q + 1$ по абсолютной величине не превосходит

$$\sum_{q=Q+1}^{P} \sum_{\substack{a=1 \\ (a,\, q)=1}}^{q} Nn\left(\rho(q, a) + \eta P^{-2}\right) < 2\eta Nn.$$

При $q \leqslant Q$ ввиду (10.19) $q \mid k$, так что $q_1 = 1$. Следовательно,

$$\mathcal{R}_1 = \mathcal{R}_2 + O(\eta Nn), \qquad (10.30)$$

где

$$\mathcal{R}_2 = \sum_{q \leqslant Q} \sum_{\substack{a=1 \\ (a,\, q)=1}}^{q} \int\limits_{\mathfrak{M}_{n,\, X}(q,\, a)} h\left(k\left(\alpha - \frac{a}{q}\right)\right) |f(\alpha)|^2\, d\alpha.$$

Легко показать, что для любого положительного числа Y

$$\int\limits_0^Y \alpha^{-1/2} \cos\alpha\, d\alpha > 0.$$

Поэтому в силу (10.27)

$$\operatorname{Re} h(\beta) = |\beta|^{-1/2} \int\limits_0^{N^2|\beta|} \tfrac{1}{2}\alpha^{-1/2} \cos 2\pi\alpha\, d\alpha > 0. \qquad (10.31)$$

Следовательно, отбрасывая в $\mathcal{R}_2$ все члены, за исключением одного с $a = q = 1$, получаем

$$\operatorname{Re} \mathcal{R}_2 \geqslant \int\limits_{-1/4\pi n}^{1/4\pi n} \operatorname{Re} h(k\alpha)\, |f(\alpha)|^2\, d\alpha.$$

Кроме того, если $|\alpha| \leqslant 1/(4\pi n)$, то имеем

$$f(\alpha) - f(0) = \sum_{\substack{x=1 \\ x \in \mathscr{A}}}^{n} 2\pi i x \int_0^{\alpha} e(\beta x)\, d\beta,$$

так что

$$|f(\alpha)| \geqslant f(0)(1 - 2\pi|\alpha|n) \geqslant \tfrac{1}{2} f(0) = \tfrac{1}{2} A(n).$$

Следовательно,

$$\operatorname{Re} \mathscr{R}_2 \geqslant \tfrac{1}{4} A(n)^2 \int_0^{1/4\pi n} \operatorname{Re} h(k\alpha)\, d\alpha. \qquad (10.32)$$

10.7 Завершение доказательства теоремы 10.2

Согласно соотношениям (10.24) и (10.31), $\operatorname{Re} h(k\alpha) \geqslant \frac{1}{2} N$, как только $4\pi n|\alpha| \leqslant 1$. Поэтому в силу неравенств (10.32) и (10.21)

$$\operatorname{Re} \mathscr{R}_2 \geqslant \frac{A(n)^2 N}{32\pi n} > \frac{\bar{d}^2 n N}{250}.$$

Таким образом, в силу (10.25), (10.28) и (10.30)

$$R(n) \geqslant \mathscr{R} = \operatorname{Re} \mathscr{R} = \operatorname{Re} \mathscr{R}_2 + O\left(\left(Nk^{-40} + n^{1/2} X^{-1/2} + N^{3/4}\right)n + \eta N n\right) >$$

$$> \frac{\bar{d}^2}{250} nN - C\left(\left(Nk^{-40} + n^{1/2} X^{-1/2} + N^{3/4}\right)n + \eta N n\right) \qquad (10.33)$$

для подходящей постоянной $C \geqslant 1$.

Доказательство завершается подходящим выбором параметров. Пусть

$$\eta = 10^{-4} \bar{d}^2 C^{-1}.$$

Это фиксирует $Q = Q_0(\eta)$, а следовательно, k и P. Заметим, что ввиду (10.18) и (10.19) $k \geqslant Q > 1/\eta$.

Пусть

$$X = \eta^{-2} k,$$

и предположим, что $n \geqslant n_0(\eta, X)$, $n \in \mathscr{N}(P, P-1)$.

Наконец, пусть $N = [(n/k)^{1/2}]$, так что (10.24) выполняется. Теперь для $n \geqslant n_1(\eta)$

$$C\left(\left(Nk^{-40} + n^{1/2} X^{-1/2} + N^{3/4}\right)n + \eta N n\right) <$$

$$< C\left(\eta N n + \eta n^{3/2} k^{-1/2} + \eta N n + \eta N n\right) < 5C\eta N n = \frac{1}{2000} \bar{d}^2 N n.$$

Следовательно, ввиду (10.33)

$$\limsup_{n\to\infty} R(n)\, n^{-3/2} \geqslant \frac{1}{300}\, \bar{d}^2 k^{-1/2} > 0,$$

что и требовалось доказать.

10.8 Упражнения

1. Докажите теорему Шаркоци, сформулированную в § 10.3.
2. Покажите, что если $\bar{d}(\mathscr{A}) > 0$ и $R(n)$ означает число решений уравнения $a - a' = p - 1$ с $a \in \mathscr{A}$, $a' \in \mathscr{A}$, $a \leqslant n$, p простое, то

$$\limsup_{n\to\infty} R(n)\,(\log n)\, n^{-2} > 0.$$

11 Диофантовы неравенства

11.1 Теорема Дэвенпорта и Хельбронна

Все формы метода Харди — Литтлвуда, описанные до сих пор, были связаны с решением уравнений в целых числах. Например, в гл. 9 показано, что если s достаточно большое, то для заданных целых $c_1, \ldots, c_s$ (или, что эквивалентно, для заданных рациональных $c_1, \ldots, c_s$), не все из которых одного знака при k четном, уравнение

$$c_1x_1^k + \ldots + c_sx_s^k = 0$$

имеет нетривиальное решение в целых $x_1, \ldots, x_s$. Теперь возникает вопрос, что происходит, когда не все $c_1, \ldots, c_s$ являются рациональными числами. При этом неразумно требовать, чтобы форма представляла 0, но можно вместо этого потребовать, чтобы она принимала произвольно малые значения.

Для ответа на этот вопрос Дэвенпорт и Хельбронн (1946) ввели своеобразный вариант метода Харди — Литтлвуда. Это позволило им получить следующую теорему.

Теорема 11.1. *Предположим, что $s \geqslant 2^k + 1$ и $\lambda_1, \ldots, \lambda_s$ — отличные от нуля действительные числа, не все из которых рациональные и не все одного знака при четном k. Тогда для любого положительного числа η существуют целые $x_1, \ldots, x_s$, не все равные нулю, такие, что*

$$|\lambda_1x_1^k + \ldots + \lambda_sx_s^k| < \eta. \qquad (11.1)$$

Достаточно доказать теорему для $\eta = 1$, так как затем в ней можно заменить λ_j на λ_j/η.

Кроме того, если k нечетное, замена при необходимости x_1^k на $(-x_1)^k$ дает возможность считать и в этом случае также, что не все λ_j имеют один знак.

Введя новые обозначения, можно предполагать, что λ_1/λ_2 — иррациональное. Если $\lambda_1/\lambda_2 > 0$, рассматриваем любое j, для которого $\lambda_1/\lambda_j < 0$. Тогда если λ_1/λ_j рациональное, то λ_2/λ_j — иррациональное и отрицательное. В любом случае, снова заменив обозначения, можно предполагать, что

$$\lambda_1/\lambda_2 \text{ — иррациональное и отрицательное.} \tag{11.2}$$

Во всех формах метода Харди — Литтлвуда, рассмотренных до сих пор, основным орудием были преобразования Фурье на торе (torus), $\mathbb{T} = \mathbb{R} \setminus \mathbb{Z}$. Для решения данной проблемы удобнее работать на $\mathbb{R}$. Очевидным аналогом формулы (1.8) является тождество

$$\int_{-\infty}^{\infty} e(\alpha\beta) \frac{\sin 2\pi\alpha}{\pi\alpha}\, d\alpha = \begin{cases} 1 & (|\beta| < 1), \\ 0 & (|\beta| > 1). \end{cases}$$

Однако существуют некоторые трудности, связанные с этим преобразованием из-за того, что интеграл не сходится абсолютно. Более удобно, следовательно, вместо него использовать интеграл

$$I(\beta) = \int_{-\infty}^{\infty} e(\alpha\beta) K(\alpha)\, d\alpha, \qquad K(\alpha) = \left(\frac{\sin \pi\alpha}{\pi\alpha}\right)^2. \tag{11.3}$$

Непосредственное применение интегральной формулы Коши дает

$$I(\beta) = \max(1 - |\beta|, 0). \tag{11.4}$$

Пусть

$$f(\alpha) = \sum_{x=1}^{N} e(\alpha x^k), \qquad f_j(\alpha) = f(\lambda_j \alpha). \tag{11.5}$$

Для успешного применения метода необходимо, чтобы интеграл

$$R(N) = \int_{-\infty}^{\infty} \left(\prod_{j=1}^{s} f_j(\alpha) \right) K(\alpha)\, d\alpha \tag{11.6}$$

имел положительную нижнюю границу. Согласно (11.4) и (11.5), этот интеграл равен

$$\sum_{x_1=1}^{N} \cdots \sum_{x_s=1}^{N} \max(1 - |a_1 x_1^k + \ldots + \lambda_s x_s^k|, 0);$$

эта величина может быть положительной, только если существуют $x_1, \ldots, x_s$, для которых выполняется (11.1) с $\eta = 1$. Таким образом, теорема 11.1 вытекает из следующей теоремы.

Теорема 11.2. *Предположим, что $s > 2^k$. Тогда существуют сколь угодно большие N, для которых*

$$R(N) \gg N^{s-k}.$$

Отметим, что всюду в этой главе неявные постоянные могут зависеть от $\lambda_1, \ldots, \lambda_s$.

11.2 Определение больших и малых дуг

Используемая здесь форма метода Харди — Литтлвуда несколько проще тех, которые были описаны ранее. Наиболее важное упрощение вызвано тем, что при подходящем выборе N подынтегральное выражение имеет только один действительно большой пик в начале координат. Поэтому иррациональность λ_1/λ_2 обеспечивает относительную малость одной из функций f_1, f_2, когда α не близко к нулю.

Пусть

$$\nu = \frac{1}{100}, \quad P = N^{\nu}. \tag{11.7}$$

Тогда $\mathbb{R}$ разбивается на три части: одна большая дуга

$$\mathfrak{M} = \{\alpha\colon\ |\alpha| \leqslant PN^{-k}\}, \tag{11.8}$$

пара малых дуг

$$\mathfrak{m} = \{\alpha\colon\ PN^{-k} < |\alpha| \leqslant P\} \tag{11.9}$$

и «тривиальная» область

$$\mathfrak{t} = \{\alpha\colon\ |\alpha| > P\}. \tag{11.10}$$

Оценка интеграла по тривиальной области производится быстро. По лемме Хуа (лемма 2.5),

$$\int\limits_X^{X+1} |f_j(\alpha)|^{2^k}\, d\alpha \ll N^{2^k-k+\varepsilon},$$

так что по неравенству Гёльдера

$$\int\limits_X^{X+1} \left|\prod_{j=1}^{2^k} f_j(\alpha)\right| d\alpha \ll N^{2^k-k+\varepsilon}. \tag{11.11}$$

Таким образом, согласно (11.3),

$$\int\limits_{\mathfrak{t}} \left|\prod_{j=1}^{s} f_j(\alpha)\right| K(\alpha)\, d\alpha \leqslant \int\limits_P^{\infty} \left|\prod_{j=1}^{s} f_j(\alpha)\right| \alpha^{-2}\, d\alpha \ll$$

$$\leqslant N^{s-k+\varepsilon} \sum_{h=0}^{\infty} (h+P)^{-2}.$$

Следовательно,

$$\int\limits_{\mathfrak{t}} \left|\prod_{j=1}^{s} f_j(\alpha)\right| K(\alpha)\, d\alpha \ll N^{s-k-\delta}; \tag{11.12}$$

здесь и ниже δ — фиксированное положительное число, зависящее разве что от k, s, $\lambda_1, \ldots, \lambda_s$.

11.3 Оценка на малых дугах

Именно при оценке на $\mathfrak{m}$ используется иррациональность λ_1/λ_2 и требуется специальный выбор N.

Лемма 11.1. *Пусть a, q — произвольная пара чисел с условием $(a, q) = 1$ и*

$$\left|\frac{\lambda_1}{\lambda_2} - \frac{a}{q}\right| \leqslant q^{-2}.$$

Пусть далее $N = q^2$. Тогда

$$\sup_{\alpha \in \mathfrak{m}} \min(|f_1(\alpha)|, |f_2(\alpha)|) \ll N^{1-\delta}.$$

Существование сколь угодно большого q и, следовательно, N, удовлетворяющего лемме 11.1, обеспечивается леммой 2.1 и иррациональностью λ_1/λ_2. Такие N встречаются довольно редко, но, во всяком случае, их бесконечно много. Эта лемма неверна, если не производить такой специализации. Например, можно показать, что для подходящего λ_1/λ_2

$$\limsup_{N \to \infty} \left(\frac{1}{N} \sup_{\mathfrak{m}} \min(|f_1(\alpha)|, |f_2(\alpha)|)\right) > 0.$$

Доказательство леммы 11.1. Предположим, что $N \geqslant N_0(\lambda_1, \ldots, \lambda_s)$, $\alpha \in \mathfrak{m}$ и $Q = N^{k-\nu/2}$. Выберем q_j, a_j в соответствии с леммой 2.1 такими, что

$$(q_j, a_j) = 1, \quad q_j \leqslant Q, \quad |\lambda_j\alpha - a_j/q_j| \leqslant 1/(q_jQ).$$

Первый шаг состоит в том, чтобы показать, что по крайней мере одно из q_1, q_2 сравнительно велико. Если бы a_j равнялось 0, тогда мы имели бы

$$|\alpha| \leqslant 1/(q_jQ|\lambda_j|) < N^{\nu-k}$$

и, следовательно, α принадлежало бы $\mathfrak{M}$, а не $\mathfrak{m}$. Таким образом, $a_j \neq 0$. Кроме этого, имеем

$$\lambda_j\alpha = \frac{a_j}{q_j} + \frac{\theta_j}{q_jQ} = \frac{a_j}{q_j}\left(1 + \frac{\theta_j}{a_jQ}\right), \quad \text{где} \quad |\theta_j| \leqslant 1.$$

Поэтому

$$\frac{\lambda_1}{\lambda_2} = \frac{\lambda_1\alpha}{\lambda_2\alpha} = \frac{q_2a_1}{a_2q_1}\left(1 + \frac{\theta_1}{a_1Q}\right)\left(1 + \frac{\theta_2}{a_2Q}\right)^{-1}$$

в силу того, что N и, следовательно, Q велико, дает

$$\frac{1}{2}\left|\frac{\lambda_1}{\lambda_2}\right| < \left|\frac{q_2a_1}{a_2q_1}\right| < 2\left|\frac{\lambda_1}{\lambda_2}\right|$$

и, следовательно,

$$\frac{\lambda_1}{\lambda_2} = \frac{q_2a_1}{a_2q_1} + O(Q^{-1}).$$

Согласно предположению,

$$\frac{\lambda_1}{\lambda_2} = \frac{a}{q} + \theta q^{-2} \text{ с } |\theta| \leqslant 1.$$

Отсюда $$\frac{a}{q} - \frac{q_2 a_1}{a_2 q_1} \ll Q^{-1} + q^{-2} \ll N^{-1} = q^2,$$

так что $$|a_2 q_1 a - q_2 a_1 q| \ll |a_2 q_1|/q.$$

Если левая часть здесь не нуль, то $|a_2 q_1| \gg q$, а если нуль, то $a/q = (q_2 a_1)/(a_2 q_1)$, что снова дает $|a_2 q_1| \gg q$. Поскольку $a_2 = \lambda_2 \alpha q_2 - \theta_2 Q^{-1} \ll q_2 P$, то имеем $q_1 q_2 \gg q P^{-1}$. Следовательно, ввиду (11.7)

$$\max(q_1, q_2) > N^{1/5}. \tag{11.13}$$

Теперь, по неравенству Вейля (лемма 2.4), для $j = 1, 2$

$$f_j(\alpha) \ll N^{1+\varepsilon} \left(\frac{1}{q_j} + \frac{1}{N} + \frac{q_j}{N^k} \right)^{2^{1-k}} \ll N^{1+\varepsilon} q_j^{-2^{1-k}} + N^{1-\delta}.$$

Отсюда ввиду (11.13)

$$\min(|f_1(\alpha)|, \ |f_2(\alpha)|) \ll N^{1-\delta},$$

что и требовалось.

Для завершения доказательства теоремы 11.2 будем предполагать, что N выбрано специальным образом в соответствии с леммой 11.1. Пусть

$$\mathfrak{m}_1 = \{\alpha : \alpha \in \mathfrak{m}, \quad |f_1(\alpha)| \leqslant |f_2(\alpha)|\}, \quad \mathfrak{m}_2 = \mathfrak{m} \setminus \mathfrak{m}_1.$$

Согласно (11.3), $K(\alpha) \ll \min(1, \alpha^{-2})$. Кроме того, рассуждения, которыми мы получили оценку (11.11), показывают, что

$$\int_X^{X+1} \left| \prod_{\substack{i=1 \\ i \neq j}}^{2^k+1} f_i(\alpha) \right| d\alpha \ll N^{2^k - k + \varepsilon},$$

так что $$\int_{\mathfrak{m}} \left| \prod_{\substack{i=1 \\ i \neq j}}^{2^k+1} f_i(\alpha) \right| K(\alpha)\, d\alpha \ll N^{2^k - k + \varepsilon}.$$

Следовательно, по лемме 11.1, если $j = 1$ или 2,

$$\int_{\mathfrak{m}_j} \left| \prod_{i=1}^{2^k+1} f_i(\alpha) \right| K(\alpha)\, d\alpha \ll N^{2^k + 1 - k - \delta + \varepsilon}.$$

Таким образом, существует положительное δ, такое, что

$$\int_{\mathfrak{m}} \left| \prod_{j=1}^{s} f_j(\alpha) \right| K(\alpha)\, d\alpha \ll N^{s-k-\delta}. \tag{11.14}$$

11.4 Большая дуга

Ввиду (11.12) и (11.14) остается только показать, что для достаточно большого N

$$\int_{\mathfrak{M}}\left(\prod_{j=1}^{s} f_j(\alpha)\right)K(\alpha)\,d\alpha \gg N^{s-k}. \tag{11.15}$$

Пусть $\alpha\in\mathfrak{M}$. Ввиду (11.7), (11.8), леммы 2.7 и замечания после доказательства этой леммы имеем

$$f_j(\alpha)=v_j(\alpha)+O\left(N^{2\nu}\right),$$

где
$$v_j(\alpha)=\int_0^N e(\lambda_j\alpha\beta^k)\,d\beta. \tag{11.16}$$

Следовательно,

$$f_1\,\ldots\,f_s-v_1\,\ldots\,v_s=\sum_{j=1}^{s}(f_j-v_j)\left(\prod_{i<j}f_i\right)\left(\prod_{i>j}v_i\right)\ll N^{s-1+2\nu}.$$

Отсюда ввиду (11.8)

$$\int_{\mathfrak{M}}\left(\prod_{j=1}^{s} f_j(\alpha)-\prod_{j=1}^{s} v_j(\alpha)\right)K(\alpha)\,d\alpha \ll N^{s-k-\delta}. \tag{11.17}$$

Заменив переменные в интеграле (11.16), а также заметив, что

$$\int_0^X \frac{1}{k}\gamma^{1/k-1}e(\gamma)\,d\gamma$$

есть $\ll 1$ равномерно по $X\geqslant 0$, находим, что

$$v_j(\alpha)\ll|\alpha|^{-1/k}.$$

Отсюда по (11.7) и (11.8)

$$\int_{R\setminus\mathfrak{M}}\left(\prod_{j=1}^{s} v_j(\alpha)\right)K(\alpha)\,d\alpha \ll \int_{N^{\nu-k}}^{\infty}\alpha^{-s/k}\,d\alpha \ll N^{(s-k)(1-\nu/k)}.$$

Таким образом,

$$\int_{\mathfrak{M}}\left(\prod_{j=1}^{s} v_j(\alpha)\right)K(\alpha)\,d\alpha=\int_{-\infty}^{\infty}\left(\prod_{j=1}^{s} v_j(\alpha)\right)K(\alpha)\,d\alpha+O\left(N^{s-k-\delta}\right). \tag{11.18}$$

В силу (11.16)

$$\int_{-\infty}^{\infty}\left(\prod_{j=1}^{s} v_j(\alpha)\right)K(\alpha)\,d\alpha=$$

$$=\int_{-\infty}^{\infty} d\alpha \int_0^N d\beta_1 \ldots \int_0^N e\left(\left(\lambda_1\beta_1^k+\ldots+\lambda_s\beta_s^k\right)\alpha\right) K(\alpha)\,d\beta_s.$$

Поскольку $K(\alpha)\ll\min(1,\alpha^{-2})$ и подынтегральная функция непрерывна, порядок интегрирования можно изменить. Следовательно, согласно (11.3) и (11.4),

$$\int_{-\infty}^{\infty}\left(\prod_{j=1}^{s} v_j(\alpha)\right)K(\alpha)\,d\alpha=$$

$$=\int_0^N d\beta_1 \ldots \int_0^N \max\left(1-\left|\lambda_1\beta_1^k+\ldots+\lambda_s\beta_s^k\right|,\ 0\right)d\beta_s=$$

$$=k^{-s}\int_0^{N^k} d\alpha_1 \ldots \int_0^{N^k} (\alpha_1\ldots\alpha_s)^{1/k-1}\max\left(1-\left|\lambda_1\alpha_1+\ldots+\lambda_s\alpha_s\right|, 0\right)d\alpha_s.$$

Теперь требуется предположение, что $\lambda_1/\lambda_2<0$. Рассмотрим область

$$\mathscr{B}=\{(\alpha_2,\ \ldots,\ \alpha_s):\delta N^k\leqslant\alpha_2\leqslant2\delta N^k,\ \delta^2N^k\leqslant\alpha_j\leqslant$$
$$\leqslant 2\delta^2N^k\quad(3\leqslant j\leqslant s)\}.$$

Тогда для достаточно малого δ, каков бы ни был элемент $(\alpha_2,\ldots,\alpha_s)\in\mathscr{B}$, имеем

$$2\delta^2N^k<-\left(\lambda_2\alpha_2+\ldots+\lambda_s\alpha_s\right)\lambda_1^{-1}<\tfrac{1}{2}N^k,$$

и поэтому каждое α_1, такое, что $|\lambda_1\alpha_1+\ldots+\lambda_s\alpha_s|\leqslant\frac{1}{2}$, удовлетворяет неравенствам $\delta^2N^k<\alpha_1<N^k$. Следовательно,

$$\int_{-\infty}^{\infty}\left(\prod_{j=1}^{s} v_j(\alpha)\right)K(\alpha)\,d\alpha\gg\left(N^{1-k}\right)^s\int_{\mathscr{B}} d\alpha_2\ldots d\alpha_s\int_{\mathscr{A}(\alpha_2,\ldots,\alpha_s)} d\alpha_1,$$

где $\mathscr{A}(\alpha_2,\ \ldots,\ \alpha_s)$ означает интервал с концами в точках $\left(-\left(\lambda_2\alpha_2+\ldots+\lambda_s\alpha_s\right)\pm\frac{1}{2}\right)\lambda_1^{-1}$. Очевидно, объем $\mathscr{B}$ есть $\gg(N^k)^{s-1}$. Поэтому

$$\int_{-\infty}^{\infty}\left(\prod_{j=1}^{s} v_j(\alpha)\right)K(\alpha)\,d\alpha\gg N^{s-k},$$

что в комбинации с (11.17) и (11.18) дает оценку (11.15) и, таким образом, завершает доказательство теоремы 11.2.

11.5 Упражнения

1. (Дэвенпорт, Рот, 1955; Вон, 1974*b*.) Получите теорему 11.1 для любого $s \geqslant Ck \log k$, где C — подходящая постоянная.
2. Пусть $\lambda_1, \lambda_2, \lambda_3, \mu, \eta$ — действительные числа, $\lambda_j \neq 0$, $\eta > 0$, λ_1/λ_2 — иррациональное и $\lambda_1/\lambda_2 < 0$. Покажите, что существуют простые p_1, p_2, p_3, такие, что
$$|\lambda_1 p_1 + \lambda_2 p_2 + \lambda_3 p_3 + \mu| < \eta.$$
3. (Baker, 1967; Vaughan, 1974*a*.) Модифицируя рассуждения, использованные в вопросе 2, покажите, что существует бесконечно много троек простых чисел p_1, p_2, p_3, таких, что
$$|\lambda_1 p_1 + \lambda_2 p_2 + \lambda_3 p_3 + \mu| < (\log \max_j p_j)^{-\eta}.$$
4. (Бэйкер)[1] Пусть $F(N) \to 0$ при $N \to \infty$. Докажите, что утверждение «для любого достаточно большого N существуют простые p_1, p_2, p_3, такие, что $p_j \leqslant N$ и $|\lambda_1 p_1 + \lambda_2 p_2 + \lambda_3 p_3| > F(N)$», может быть ложным для подходящих $\lambda_1, \lambda_2, \lambda_3$, для которых $\lambda_1/\lambda_2 > 0$ и λ_1/λ_2 иррационально.

---

[1]) Сообщено в разговоре в июне 1973 г.

Библиография

Apostol, T. M. (1976). *Introduction to analytic number theory.* New York: Springer Verlag. [B].

Arhipov, G. I. & Karatsuba, A. A. (1978). A new estimate of an integral of I. M. Vinogradov. *Izv. Akad. Nauk SSSR, ser. mat.*, **42**, 751–62. [5].

Arkhangelskaya, V. M. (1957). Some calculations connected with Goldbach's problem. *Ukraine Math. J.*, **9**, 20–9. [3]

Ayoub, R. (1953*a*). On Rademacher's extension of the Goldbach–Vinogradoff theorem. *Trans. Am. Math. Soc.*, **74**, 482–91. [G].

Ayoub, R. (1953*b*). On the Waring–Siegel theorem. *Can. J. Math.*, **5**, 439–50. [G].

Babaev, G. & Subhankulov, M. A. (1963). An asymptotic formula for two additive problems. *Tadjhik. Gos. Univ. Utsen. Zap.*, **26**, 49–68. [G].

Baker, A. (1967). On some diophantine inequalities involving primes. *J. Reine Angew. Math.*, **228**, 166–81. [11].

Bambah, R. P. (1954). Four squares and a k-th power. *Q. J. Math.*, **5**, 191–202. [11].

Batchelder, P. M. (1936). Waring' problem. *Am. Math. Month.*, **43**, 21–7. [1, S].

Behrend, F. A. (1946). On sets of integers which contain no three terms in arithmetical progression. *Proc. Natn. Acad. Sci. U.S.A.*, **32**, 331–2. [10].

Bierstedt, R. G. (1963). Some problems on the distribution of kth power residues modulo a prime. Ph.D. thesis. University of Colorado, Boulder. [9].

Birch, B. J. (1957). Homogeneous forms of odd degree in a large number of variables. *Mathematika*, **4**, 102–5. [9].

Birch, B. J. (1962). Forms in many variables. *Proc. R. Soc. Lond.*, **265A**, 245–63.

Birch, B. J. (1970). Small zeros of diagonal forms of odd degree in many variables. *Proc. Lond. Math. Soc.*, (3), **21**, 12–18. [9].

Birch, B. J. & Davenport, H. (1958). On a theorem of Davenport and Heilbronn. *Acta Math.*, **100**, 259–79. [11].

Birch, B. J., Davenport, H. & Lewis, D. J. (1962). The addition of norm forms. *Mathematika*, **9**, 75–82. [G].

Bombieri, E. & Davenport, H. (1966). Small differences between prime numbers. *Proc. R. Soc. Lond.*, **293A**, 1–18. [G.].

Bovey, J. D. (1974). $\Gamma^*(8)$. *Acta Arith.*, **25**, 145–50. [9].

Brauer, R. (1945). A note on systems of homogeneous algebraic equations. *Bull. Am. Math. Soc.*, **51**, 749–55. [9].

Cassels, J. W. S. (1960). On the representation of integers as the sums of distinct summands taken from a fixed set. *Acta Sci. Math. Szeged*, **21**, 111–24. [10].

Cauchy, A. L. (1813). Recherches sur les nombres. *J. Ec. Polytech.*, **9**, 99–116. [2]

Chen, J. -R. (1958). On Waring's problem for n-th powers. *Acta Math. Sinica*, **8**, 253–7, translated in *Chin. Math. Acta*, **8** (1966), 849–53. [5].

Chen, J. -R. (1959). On the representation of a natural number as a sum of terms of the form $x(x+1)\dots(x+k-1)/k!$. *Acta Math. Sinica.*, **9**, 264–70. [G].

Chen, J. -R. (1964). Waring's problem for $g(5)=37$. *Scientia Sinica*, **13**, 335 and 1547–68. See also *Sci. Rec.*, **3** (1959), 327–30. [1].

Chen, J. -R. (1965). On large odd numbers as sums of three almost equal primes. *Scientia Sinica*, **14**, 1113–17. [3].

Chowla, I. (1935*a*). A theorem on the addition of residue classes. *Proc. Indian Acad. Sci.*, **2**, 242–3. [2].

Chowla, I. (1935*b*). A theorem on the addition of residue classes: Application to the number $\Gamma(k)$ in Waring's problem. *Proc. Indian Math. Soc.*, **2A**, 242–3, and *Q. J. Math.*, **8** (1937), 99–102. [4].

Chowla, I. (1937*a*). On $\Gamma(k)$ in Waring's problem and an analogous function. *Proc. Indian Acad. Sci.*, **5A**, 269–76. [4].

Chowla, I. (1937*b*). A new evaluation of the number $\Gamma(k)$ in Waring's problem. *Proc. Indian Acad. Sci.*, **6A**, 97–103. [4].

Chowla, S. D. (1934). A theorem on irrational indefinite quadratic forms. *J. Lond. Math. Soc.*, **9**, 162–3. [11].

Chowla, S. D. (1936). Pillai's exact formula for the number $g(n)$ in Waring's problem. *Proc. Indian Acad. Sci.*, **3A**, 339–40 and **4**, 261. [1].

Chowla, S. D. (1944). On $g(k)$ in Waring's problem. *Proc. Lahore Philos. Soc.*, **6**, 16–17. [1].

Chowla, S. D. (1960). On a conjecture of J. F. Gray, *Norske Vid. Selsk. Forh. (Trondheim)*, **33**, 58–9. [9].

Chowla, S. D. (1961). On the congruence $\Sigma_{i=1}^{s} a_i x_i^k \equiv 0 \pmod p$, *J. Indian Math. Soc.*, **25**, 47–8. [9].

Chowla, S. D. (1963). On a conjecture of Artin, I, II. *Norske Vid. Selsk. Forh. (Trondheim)*, **36**, 135–41. [9].

Chowla, S. D. & Davenport, H. (1960/1961). On Weyl's inequality and Waring's problem for cubes. *Acta Arith.*, **6**, 505–21. [9].

Chowla, S. D. & Shimura, G. (1963). On the representation of zero by a linear combination of k-th powers, *Norske Vid. Selsk. Forh. (Trondheim)*, **36**, 169–76. [9].

Chudakov, N. G. (1937). On the Goldbach problem. *C. R. Acad. Sci. URSS*, (2), **17**, 335–8.

Chudakov, N. G. (1938). On the density of the set of even numbers which are not representable as a sum of two odd primes. *Izv. Akad. Nauk SSSR Ser. Nat.*, **2**, 25–40. [3].

Chudakov, N. G. (1947). On the Goldbach–Vinogradov's theorem. *Ann. Math.*, (2), **48**, 515–45. [3].

Cook, R. J. (1971). Simultaneous quadratic equations. *J. Lond. Math. Soc.*, (2), **4**, 319–26. [G].

Cook, R. J. (*1972a*). A note on a lemma of Hua. *Q. J. Math.*, **23**, 287–8. [G].

Cook, R. J. (1972*b*). Pairs of additive equations. *Michigan Math. J.*, **19**, 325–31. [G].

Cook, R. J. (1973*a*). A note on Waring's problem. *Bull. Lond. Math. Soc.*, **5**, 11–12. [6].

Cook, R. J. (1973*b*). Simultaneous quadratic equations II. *Acta Arith.*, **25**, 1–5. [G].

Cook, R. J. (1974). Simultaneous quadratic inequalities. *Acta Arith.*, **25**, 337–46. [G].

Cook, R. J. (1975). Indefinite hermitian forms. *J. Lond. Math. Soc.*, (2), **11**, 107–12. [G].

Cook, R. J. (1977, 1979). Diophantine inequalities with mixed powers I, II. *J. Number Theor.*, **9**, 261–74; **11**, 49–68. [G].

Corput, J. G. van der (1937a). Sur le théorème de Goldbach–Vinogradov, *C. R. Acad. Sci., Paris*, **205**, 479–81. [3].

Corput, J. G. van der (1937*b*). Une nouvelle généralisation du théorème de Goldbach–Vinogradov. *C. R. Acad. Sci. Paris*, **205**, 591–2. [3].

Corput, J. G. van der (1937*c*). Sur l'hypothèse de Goldbach pour presque tous les nombres pairs. *Acta Arith.*, **2**, 266–90. [3].

Corput, J. G. van der (1937*d*, 1938*a,b,c,d*). Sur deux, trois ou quatre nombres premiers, I, II, III, IV, V. *Proc. Akad. Wet. Amsterdam*, **40**, 846–51; **41**, 25–36, 97–107, 217–26, 344–49. [G].

Corput, J. G. van der (1938*e*). Sur l'hypothèse de Goldbach. *Proc. Akad. Wet. Amsterdam*, **41**, 76–80. [3].

Corput, J. G. van der (1938*f*). Uber Summen von Primzahlen und Primzahlen quadraten. *Math. Ann.*, **116**, 1–50. [G].

Corput, J. G. van der (1938*g,h,i,j*, 1939). Contribution à la théorie additive des nombres I, II, III, IV, V. *Proc. Akad. Wet. Amsterdam*, **41**, 227–37, 350–61, 442–53, 556–67; **42**, 336–45. [G].

Corput, J. G. van der & Pisot, Ch. (1939). Sur un problème de Waring généralisé III, *Proc. Akad. Wet. Amsterdam*, **42**, 566–72. [G].

Danicic, I. (1958). The solubility of certain Diophantine inequalities. *Proc. Lond. Math. Soc.*, (3), **8**, 161–76. [11].

Danicic, I. (1966). On the integral part of a linear form with prime variables. *Can. J. Math.*, **18**, 621–28. [11].

Davenport, H. (1935). On the addition of residue classes. *J. Lond Math. Soc.*, **10**, 30–2. [2].

Davenport, H. (1938). Sur les sommes de puissances entières. *C. R. Acad. Sci., Paris*, **207**, 1366–8. [6].

Davenport, H. (1939*a*). On Waring's problem for cubes. *Acta Math.*, **71**, 123–43. [6].

Davenport, H. (1939*b*). On sums of positive integral *k*th powers. *Proc. R. Soc. Lond.*, **170A**, 293–9. [6].

Davenport, H. (1939*c*). On Waring's problem for fourth powers. *Ann. Math.*, **40**, 731–47. [6].

Davenport, H. (1942*a*). On sums of positive integral *k*th powers. *Am. J. Math.*, **64**, 189–98. [6].

Davenport, H. (1942*b*). On Waring's problem for fifth and sixth powers. *Am. J. Math.*, **64**, 199–207. [6].

Davenport, H. (1947). A historical note. *J. Lond. Math. Soc.*, **22**, 100–1. [2].

Davenport, H. (1950). Sums of three positive cubes. *J. Lond. Math. Soc.*, **25**, 339–43. [6].

Davenport, H. (1956, 1958). Indefinite quadratic forms in many variables I, II. *Mathematika*, **3**, 81–101; *Proc. Lond. Math. Soc.*, (3), **8**, 109–26. [11].

Davenport, H. (1959). Cubic forms in thirty two variables. *Philos. Trans. R. Soc. Lond.*, **261A**, 193–210. [9].

Davenport, H. (1960*a*). Über einige neuere Fortschritte der additiven Zahlentheorie. *Jahresbr. der Deutschen Math. Ver.*, **63**, 163–9. [S].

Davenport, H. (1960*b*). Some recent progress in analytic number theory. *J. Lond. Math. Soc.*, **35**, 135–42. [S].

Davenport, H. (1962*a*). Cubic forms in 29 variables. *Proc. R. Soc. Lond.*, **266A**, 287–98. [9].

Davenport, H. (1962*b*). *Analytic methods for Diophantine equations and Diophantine inequalities.* Ann Arbor: Ann Arbor Publishers. [E].

Davenport, H. (1963). Cubic forms in sixteen variables. *Proc. R. Soc. Lond.*, **272A**, 285–303. [9].

Davenport, H. (1966). *Multiplicative number theory.* 1st edn. Chicago: Markham. 2nd ed. revised by Montgomery, H. L. (1980). Graduate Texts in Mathematics, 74. Berlin: Springer–Verlag. [B].

Davenport, H. (1977). *The collected works of Harold Davenport*, vol. III, ed. B. J. Birch, H. Halberstram & C. A. Rogers. London: Academic Press. [G].

Davenport, H. & Erdős, P. (1939). On sums of positive integral kth powers. *Ann. Math.*, **40**, 533–6. [6].

Davenport, H. & Heilbronn, H. (1936*a*). On Waring's problem for fourth powers. *Proc. Lond. Math. Soc.*, (2), **41**, 143–50. [5].

Davenport, H. & Heilbronn, H. (1936*b*). On an exponential sum. *Proc. Lond. Math. Soc.*, (2), **41**, 449–53 [4].

Davenport, H. & Heilbronn, H. (1937*a*). On Waring's problem: two cubes and one square. *Proc. Lond. Math. Soc.*, (2), **43**, 73–104. [8].

Davenport, H. & Heilbronn, H. (1937*b*). Note on a result in the additive theory of numbers. *Proc. Lond. Math. Soc.*, (2), **43**, 142–51. [G].

Davenport, H. & Heilbronn, H. (1946). On indefinite quadratic forms in five variables. *J. Lond. Math. Soc.*, **21**, 185–93. [11].

Davenport, H. & Lewis, D. J. (1963). Homogeneous additive equations. *Proc. R. Soc. Lond.*, **274A**, 443–60. [9].

Davenport, H. & Lewis, D. J. (1966). Cubic equations of additive type. *Philos. Trans. R. Soc. Lond.*, **261A**, 97–136. [G].

Davenport, H. & Lewis, D. J. (1969*a*). Simultaneous equations of additive type. *Philos. Trans. R. Soc. Lond.*, **264A**, 557–95. [G].

Davenport, H. & Lewis, D. J. (1969*b*). Two additive equations. *American Mathematical Society Proceedings of Symposia in Pure Mathematics*, **12**, 74–98. [G].

Davenport, H. & Lewis, D. J. (1972). Gaps between values of positive definite quadratic forms. *Acta Arith.*, **21**, 87–105. [G].

Davenport, H. & Ridout, D. (1959). Indefinite quadratic forms. *Proc. Lond. Math. Soc.*, (3), **9**, 544–55. [G].

Davenport, H. & Roth, K. F. (1955). The solubility of certain Diophantine inequalities. *Mathematika*, **2**, 81–96. [11].

Dickson, L. E. (1933). Recent progress on Waring's theorem and its generalizations. *Bull. Am. Math. Soc.*, **39**, 701–27. [1].

Dickson, L. E. (1936*a*). *Researches on Waring's problem.* Carnegie Inst. of Washington Publ. **464**. [1].
Dickson, L. E. (1936*b*). Proof of the ideal Waring theorem for exponents 7–180. *Am. J. Math.*, **58**, 521–9. [1].
Dickson, L. E. (1936*c*). Solution of Waring's problem. *Am. J. Math.*, **58**, 530–5. [1].
Dickson, L. E. (1936*d*). The Waring problem and its generalizations. *Bull. Am. Math. Soc.*, **42**, 833–42. [1].
Dickson, L. E. (1936*e*). On Waring's problem and its generalization. *Ann. Math.*, **37**, 293–316. [1].
Dickson, L. E. (1936*f*). The ideal Waring theorem for twelfth powers. *Duke Math. J.*, **2**, 192–204. [1].
Dickson, L. E. (1936*g*). Universal Waring theorems. *Monatshefte für Mathematik und Physik*, **43**, 391–400. [1].
Dodson, M. M. (1967). Homogeneous additive congruences. *Philos. Trans. R. Soc. Lond.*, **261A**, 163–210. [9].
Ehlich, H. (1965). Zur Pillaischen Vermutung. *Arch. Math.*, **16**, 223–26. [1].
Ellison, W. J. (1971). Waring's problem. *Am. Math. Mon.*, **78**, 10–36. [1].
Emel'yanov, G. V. (1950). On a system of Diophantine equations. *Leningrad Gos. Univ. Uch. Zap.* **137**, *Ser. Mat. Nauk*, **19**, 3–39. [G].
Erdős, P. & Turán, P. (1936). On some sequences of integers. *J. Lond. Math. Soc.*, **11**, 261–4. [10].
Erdős, P. & Vaughan, R. C. (1974). Bounds for the *r*th coefficients of cyelotomic polynomials. *J. Lond. Math. Soc.*, (2), **8**, 393–400. [3].
Estermann, T. (1929). On the representation of a number as the sum of three products. *Proc. Lond. Math. Soc.*, (2), **29**, 453–78. [G].
Estermann, T. (1929). Vereinfachter Beweis eines Satzes von Kloosterman. *Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität*, **7**, 82–98. [G].
Estermann, T. (1930*a*,*b*). On the representation of a number as the sum of two products, I, II. *Proc. Lond. Math. Soc.*, (2), **31**, 123–133; *J. Lond. Math. Soc.* **5**, 131–7. [G].
Estermann, T. (1936). Proof that every large integer is a sum of seventeen biquadrates. *Proc. Lond. Math. Soc.*, (2), **41**, 126–42. [6].
Estermann, T. (1937*a*). On Waring's problem for fourth and higher powers. *Acta Arith.*, **2**, 197–211. [5].
Estermann, T. (1937*b*). Proof that every large integer is the sum of two primes and a square. *Proc. Lond. Math. Soc.*, (2), **42**, 501–16. [G].
Estermann, T. (1937*c*). A new result in the additive prime number theory. *Q. J. Math.*, **8**, 32–8. [3].
Estermann, T. (1938). On Goldbach's problem: Proof that almost all even positive integers are sums of two primes. *Proc. Lond. Math. Soc.*, (2), **44**, 307–14. [3].
Estermann, T. (1948). On Waring's problem: A simple proof of a theorem of Hua. *Sci. Rep. Natn. Tsing Hua Univ.*, **5A**, 226–39. [2].
Estermann, T. (1951). On sums of squares of square-free numbers. *Proc. Lond. Math. Soc.*, (2), **53**, 125–37. [G].
Estermann, T. (1952). *Introduction to modern prime number theory*. Cambridge University Press. [E].
Estermann, T. (1962). A new application of the Hardy–Littlewood–Kloosterman method. *Proc. Lond. Math. Soc.*, (3), **12**, 425–44. [G].

Evelyn, C. J. A. & Linfoot, E. H. (1929, 1933). On a problem in the additive theory of numbers I, VI, *Math. Z.*, **30**, 433–48; *Q. J. Math.*, **4**, 309–14. [G].
Földes, I. (1952). On the Goldbach hypothesis concerning the prime numbers of an arithmetical progression. *C. R. Prem. Cong. Mat. Hongrois*, 473–92. [3].
Fowler, J. (1962). A note on cubic equations. *Proc. Camb. Philos. Soc.*, **58**, 165–69. [9].
Freiman, G. A. (1949). Solution of Waring's problem in a new form. *Uspehi Mat. Nauk*, **4**, 193. [5,8].
Furstenburg, H. (1977). Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions. *J. d'Analyse Math.*, **31**, 204–56. [10].
Gallagher, P. X. (1975). Primes and powers of 2. *Inventiones Math.*, **29**, 125–42. [G].
Gelbcké, M. (1931). Zum Waringschen Problem. *Math. Ann.*, **105**, 637–52. [2].
Gelbcke, M. (1933). A propos de $g(k)$ dans le problème de Waring. *C. R. Acad. Sci. URSS*, (7), 631–40. [2].
Ghosh, A. (1981). The distribution of αp^2 modulo one. *Proc. Lond. Math. Soc.*, **42**, [G].
Gray, J. F. (1960). Diagonal forms of odd degree over a finite field. *Michigan Math. J.*, **7**, 297–301. [9].
Grosswald, E. (1968/9). On some conjectures of Hardy and Littlewood. *Publ. Ramanujan Inst.*, **1**, 75–89. [8].
Halberstam, H. (1950). Representation of integers as sums of a square, a positive cube, and a fourth power of a prime. *J. Lond. Math. Soc.*, **25**, 158–68. [G].
Halberstam, H. (1951*a*). Representation of integers as sums of a square of a prime, a cube of a prime, and a cube. *Proc. Lond. Math. Soc.* (2), **52**, 455–66. [G].
Halberstam, H. (1951*b*). On the representation of large numbers as sums of squares, higher powers, and primes. *Proc. Lond. Math. Soc.*, (2), **53**, 363–80. [G].
Halberstam, H. (1957). An asymptotic formula in the theory of numbers. *Trans. Am. Math. Soc.*, **84**, 338–51. [G].
Hardy, G. H. (1922). Goldbach's theorem. *Math. Tid. B*, 1–16. [1].
Hardy, G. H. (1966). *Collected papers of G. H. Hardy, including joint papers with J. E. Littlewood and others*, ed. by a committee appointed by the London Mathematical Society, vol. I. Oxford: Clarendon Press. [E].
Hardy, G. H. & Littlewood, J. E. (1919). A new solution of Waring's problem. *Q. J. Math.*, **48**, 272–93. [1,2].
Hardy, G. H. & Littlewood, J. E. (1920). Some problems of "Partitio Numerorum". I A new solution of Waring's problem. *Göttingen Nachrichten*, 33–54, [1, 2].
Hardy, G. H. & Littlewood, J. E. (1921). Some problems of "Partitio Numerorum": II Proof that every large number is the sum of at most 21 biquadrates. *Math. Z.*, **9**, 14–27. [1,6].
Hardy, G. H. & Littlewood, J. E. (1922). Some problems of "Partitio Numerorum": IV The singular series in Waring's problem. *Math. Z.*, **12**, 161–88. [4].
Hardy, G. H. & Littlewood, J. E. (1923*a*). Some problems of "Partitio Numerorum": III On the expression of a number as a sum of primes. *Acta Math.*, **44**, 1–70. [1,3].
Hardy, G. H. & Littlewood, J. E. (1923*b*). Some problems of "Partitio Numerorum": V A further contribution to the study of Goldbach's problem. *Proc. Lond. Math. Soc.*, (2), **22**, 46–56. [1,3].
Hardy, G. H. & Littlewood, J. E. (1925). Some problems of "Partitio Numerorum": VI Further researches in Waring's problem. *Math. Z.*, **23**, 1–37. [4, 6].

Hardy, G. H. & Littlewood, J. E. (1928). Some problems of "Partitio Numerorum" VIII† The number Γ(*k*) in Waring's problem. *Proc. Lond. Math. Soc.*, (2), **28**, 518–42. [4].
Hardy, G. H., Littlewood, J. E. & Pólya, G. (1951). *Inequalities*, 2nd edn. Cambridge University Press. [B].
Hardy, G. H. & Ramanujan, S. (1918). Asymptotic formulae in combinatory analysis. *Proc. Lond. Math. Soc.*, (2), **17**, 75–115. [1].
Hardy, G. H. & Wright, E. M. (1979). *An introduction to the theory of numbers*, 5th edn. Oxford: Oxford University Press. [B].
Hasse, H. (1964). *Vorlesungen über Zahlentheorie. Zweite auflage*. Berlin: Springer-Verlag. [B].
Heilbronn, H. (1936). Über das Waringsche Problem. *Acta Arith.*, **1**, 212–21. [5].
Hilbert, D. (1909*a*,*b*). Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl nter Potenzen (Waringsche Problem). Nachrichten von der Königlichen Gesellchaft der Wissenschaften zu Göttingen, mathematisch-physikalische Klasse aus den Jahren 1909, 17–36; *Math. Annalen*, **67**, 281–300. [1].
Householder, J. E. (1959). The representation of zero by odd *k*th power diagonal forms. Ph.D. Thesis. University of Colorado, Boulder. [9].
Hua, L. -K. (1935). On Waring theorems with cubic polynomial summands. *Math. Ann.*, **111**, 622–8. [G].
Hua, L. -K. (1936*a*,*b*). On Waring's problem with polynomial summands. *Am. J. Math.*, **58**, 553–62; *J. Chin. Math. Soc.*, **1**, 21–61. [G].
Hua, L. -K. (1937*a*). On a generalized Waring problem. *Proc. Lond. Math. Soc.*, (2), **43**, 161–82.
Hua, L. -K. (1937*b*). On the representation of integers as the sums of *k*th powers of primes. *C. R. Acad. Sci. URSS*, (2), **17**, 167–8. [G].
Hua, L. -K. (1938*a*). Some results on Waring's problem for smaller powers. *C. R. Acad. Sci. URSS*, (2), **18**, 527–8. [6].
Hua, L. -K. (1938*b*). On Waring's problem. *Q. J. Math.*, **9**, 199–202. [2].
Hua, L. -K. (1938*c*,*d*). Some results in the additive prime number theory. *C. R. Acad. Sci. URSS*, (2), **18**, 3; *Q. J. Math.*, **9**, 68–80. [G].
Hua, L.-K. (1939). On Waring's problem for fifth powers. *Proc. Lond. Math. Soc.*, (2), **45**, 144–60. [6].
Hua, L.-K. (1940*a*). Sur une somme exponentielle. *C. R. Acad. Sci. Paris*, **210**, 520–3. [7].
Hua, L. -K. (1940*b*). Sur le problème de Waring relatif à un polynome du troisième degré. *C. R. Acad. Sci. Paris*, **210**, 650–2. [G].
Hua, L.-K. (1940*c*). On a system of Diophantine equations. *Dokl. Akad. Nauk SSSR*, **27**, 312–13. [G].
Hua, L. -K. (1940*d*). On a generalized Waring problem II. *J. Chin. Math. Soc.*, **2**, 175–91. [G].
Hua, L. -K. (1940*e*, *f*). On Waring's problem with cubic polynomial summands. *Sci. Rep. Natn. Tsing Hua Univ.*, **4A**, 55–83; *J. Indian Math. Soc.*, **4**, 127–35. [G].
Hua, L. -K. (1947). Some results on additive theory of numbers. *Proc. Natn. Acad. Sci. U.S.A.*, **33**, 136–7. [G].

Hua, L. -K. (1949). An improvement of Vinogradov's mean value theorem and several applications. *Q. J. Math.*, **20**, 48–61. [5].

Hua, L. -K. (1952). On the number of solutions of Tarry's problem. *Acta Sci. Sinica*, **1**, 1–76. [7].

Hua, L. -K. (1957*a*). On exponential sums. *Sci. Rec.*, **1**, 1–4. [4].

Hua, L. -K. (1957*b*). On the major arcs in Waring's problem. *Sci. Rec.*, **1**, 17–18. [4].

Hua, L. -K. (1959). *Die Abschätzung von Exponentialsummen und ihre anwendung in der Zahlentheorie.* Enzyklopädie der Math. Wiss. Band I, 2. Heft 13. Teil 1. Leipzig: Teubner. [E].

Hua, L. -K. (1965). *Additive theory of prime numbers.* Providence, Rhode Island: American Mathematical Society. [E].

Humphreys, M. G. (1935). On the Waring problem with polynomial summands. *Duke Math. J.*, **1**, 361–75. [G].

Huston, R. E. (1935). Asymptotic generalizations of Waring's theorem. *Proc. Lond. Math. Soc.*, (2), **39**, 82–115. [G].

Huxley, M. N. (1968). The large sieve inequality for algebraic number fields. *Mathematika*, **15**, 178–87. [5].

Huxley, M. N. (1969). On the differences of primes in arithmetical progressions. *Acta Arith.*, **15**, 367–92. [G].

Huxley, M. N. (1973, 1977). Small differences between consecutive primes, I, II. *Mathematika*, **20**, 229–32; **24**, 142–52. [G].

Iseki, K. (1949). A remark on the Goldbach–Vinogradov theorem. *Proc. Jpn. Acad.*, **25**, 185–7. [3].

Iseki, S. (1968). A problem on partitions connected with Waring's problem. *Proc. Am. Math. Soc.*, **19**, 197–204. [2].

James, R. D. (1934*a*). The value of the number $g(k)$ in Waring's problem. *Trans. Am. Math. Soc.*, **36**, 395–444. [2].

James, R. D. (1934*b*). On Waring's problem for odd powers. *Proc. Lond. Math. Soc.*, (2), **37**, 257–91. [2].

James, R. D. & Weyl, H. (1942). Elementary note on prime number problems of Vinogradoff's type. *Am. J. Math.*, **64**, 539–52. [3].

Kalinka, V. (1963). Generalization of a lemma of L. -K. Hua for algebraic numbers. *Litovsk Mat. Sb.*, **3**, 149–55. [G].

Kamke, E. (1921). Verallgemeinerungen des Waring–Hilbertschen Satzes. *Mat. Ann.*, **83**, 85–112. [G].

Kamke, E. (1922). Bemerkung zum allgemein Waringschen Problem. *Mat. Z.*, **15**, 188–94. [G].

Karatsuba, A. A. (1965). On the estimation of the number of solutions of certain equations. *Dokl. Akad. Nauk SSSR*, **165**, 31–2, translated in *Sov. Math. Dokl.*, **6**, 1402–4. [5].

Karatsuba, A. A. (1968). A certain system of indeterminate equations. *Mat. Z.*, **4**, 125–8. [5].

Karatsuba, A. A. & Korobov, N. M. (1963). A mean value theorem. *Dokl. Akad. Nauk SSSR*, **149**, 245–8. [5].

Kestelman, H. (1937). An integral connected with Waring's problem. *J. Lond. Math. Soc.*, **12**, 232–40. [2].

Khintchine, A. (1952). *Three pearls of number theory.* Rochester, N.Y.: Graylock Press. [1].

Kloosterman, H. D. (1925*a*). Over het uitdrukken van geheele positieve getallen in den vorm $ax^2+by^2+cz^2+dt^2$. *Verslag Amsterdam*, **34**, 1011–15. [G].
Kloosterman, H. D. (1925*b*). On the representation of numbers in the form $ax^2+by^2+cz^2+dt^2$. *Acta Math.*, **49**, 407–64. [G].
Kloosterman, H. D. (1925*c*). On the representation of numbers in the form $ax^2+by^2+cz^2+dt^2$. *Proc. Lond. Math. Soc.*, (2), **25**, 143–73. [G].
Körner, O. (1960). Übertragung des Goldbach–Vinogradovschen Satzes auf reell-quadratisch Zahlkörper. *Math. Ann.*, **141**, 343–66. [G].
Körner, O. (1961*a*). Erweiterter Goldbach–Vinogradovscher Satz in beliebigen algebraischen Zahlkörpern. *Math. Ann.*, **143**, 344–78. [G].
Körner, O. (1961*b*). Zur additiven Primzahltheorie algebraischer Zahlkörper. *Math. Ann.*, **144**, 97–109. [G].
Körner, O. (1961*c*). Über das Waringsche Problem in algebraischen Zahlkörper. *Math. Ann.*, **144**, 224–38. [G].
Körner, O. (1962). Über Mittelwerte trigonometrischer Summen und ihre Anwendung in algebraischen Zahlkörpern. *Math. Ann.*, **147**, 205–39, corrections, *ibid*, **149**, (1963), 462. [G].
Körner, O. (1962/3). Ganze algebraische Zahlen als Summen von Polynomwerten. *Math. Ann.*, **149**, 97–104. [G].
Körner, O. (1964). Darstellung ganzer Grössen durch Primzahlpotenzen in algebraischen Zahlkörpern. *Math. Ann.*, **155**, 204–45. [G].
Kovacs, B. (1972). Über die Lösbarkeit diophantischer Gleichungen von additiven Typ. I. *Publ. Math.*, **19**, 259–73. [G].
Landau, E. G. H. (1922). Zur additiven Primzahltheorie. *Palermo Rend.*, **46**, 349–56. [3].
Landau, E. G. H. (1927). *Vorlesungen über Zahlentheorie*. Erster Band. Leipzig: Verlag von S. Hirzel. [E].
Landau, E. G. H. (1930). Über die neue Winogradoffsche Behandlung des Waringschen Problems. *Math. Z.*, **31**, 319–38. [2].
Landau, E. G. H. (1937). *Über einige neuere Fortschritte der additiven Zahlentheorie*. Cambridge University Press. [E].
Lau, K. W. & Liu, M.-C. (1978). Linear approximation by primes. *Bull. Aust. Math. Soc.*, **19**, 457–66. [11].
Lavrik, A. F. (1959). On a theorem in the additive theory of numbers. *Uspehi Mat. Nauk*, **14**, 197–8. [G].
Lavrik, A. F. (1960*a*). On the twin prime hypothesis of the theory of primes by the method of I. M. Vinogradov. *Dokl. Akad. Nauk SSSR*, **132**, 1013–15, translated in *Soviet Math. Dokl.*, **1** (1960), 700–2. [3].
Lavrik, A. F. (1960*b*). On the distribution of *k*-twin primes. *Dokl. Akad. Nauk SSSR*, **132**, 1258–60, translated in *Soviet Math. Dokl.*, **1** (1960), 764–6. [3].
Lavrik, A. F. (1961*a*). The number of *k*-twin primes lying in an interval of a given length. *Dokl. Akad. Nauk SSSR*, **136**, 281–3, translated in *Soviet Math. Dokl.*, **2** (1961), 52–5. [3].
Lavrik, A. F. (1961*b*). Binary problems of additive prime number theory connected with the method of trigonometric sums of I. M. Vinogradov. *Vestnik Leningrad Univ.*, **16**, 11–27. [3].
Lavrik, A. F. (1961*c*). On the theory of distribution of primes based on I. M. Vinogradov's method of trigonometric sums. *Trudy Mat. Inst. Steklov*, **64**, 90–125. [3].

Lavrik, A. F. (1961*d*). On the theory of the distribution of sets of primes with given differences between them. *Dokl. Akad. Nauk SSSR*, **138**, 1287–90, translated in *Soviet Math. Dokl.*, **2** (1961), 827–30. [3].

Lavrik, A. F. (1962). On the representation of numbers as the sum of primes by Shnirel'man's method. *Izv. Akad. Nauk UzSSR Ser. Fiz.-Mat. Nauk*, **3**, 5–10. [3]

Lewis, D. J. (1957). Cubic forms over algebraic number fields. *Mathematika*, **4**, 97–101. [9].

Lewis, D. J. (1970). *Systems of diophantine equations*. Symp. Math. IV, INDAM, Rome 1968/1969, 33–43. Academic Press. [G].

Lewis, D. J. (1973). *The distribution of the values of real quadratic forms at integer points*. American Mathematical Society Proceedings of Symposia in Pure Mathematics, **24**, 159–74. [G].

Linnik, Ju. V. (1942, 1943*a*). On the representation of large numbers as sums of seven cubes. *Doklady Akad. Nauk SSSR*, **35**, 162 and *Mat. Sbornik*, **12**, 218–24. [1].

Linnik, Ju. V. (1943*b*). An elementary solution of the problem of Waring by Schnirel'man's method. *Mat. Sb.*, **12**, 225–30, [1].

Linnik, Ju. V. (1945). On the possibility of a unique method in certain problems of "additive" and "distributive" prime number theory. *Dokl. Akad. Nauk SSSR*, **48**, 3–7. [3].

Linnik, Ju. V. (1946). A new proof of the Goldbach–Vinogradov theorem. *Mat. Sb.*, **19**(61), 3–8. [3].

Linnik, Ju. V. (1951). Prime numbers and powers of two. *Trudy Mat. Inst. Steklov*, **38**, 152–169. [G].

Linnik, Ju. V. (1951, 1952). Some conditional theorems concerning binary problems with prime numbers. *Doklady Akad. Nauk SSSR*, **77**, 15–18 and *Izv. Akad. Nauk SSSR Ser. Mat.*, **16**, 503–20. [3].

Linnik, Ju. V. (1953). Addition of prime numbers with powers of one and the same number. *Mat. Sb.*; **32**(74), 3–60. [G].

Liu, M. -C. (1974). Simultaneous approximation of two additive forms. *Proc. Camb. Philos. Soc.*, **75**, 77–82. [G].

Liu, M. -C. (1977). Diophantine approximation involving primes. *J. Reine Angew. Math.*, **289**, 199–208. [G].

Liu, M. -C. (1978). Approximation by a sum of polynomials involving primes. *J. Math. Soc. Jpn.*, **30**, 395–412. [G].

Liu, M. -C. (1979). Approximation by a sum of polynomials of different degrees involving primes. *J. Aust. Math. Soc.*, **27A**, 454–66. [G].

Liu, M. -C., Ng. S. -M. & Tsang, K. -M. (1980). An improved estimate for certain diophantine inequalities. *Proc. Am. Math. Soc.*, **78**, 457–63. [G].

Lloyd, D. P. (1975). Bounds for solutions of Diophantine equations. Ph.D. thesis. University of Adelaide. [G].

Lu, M. -G. & Chen, W. -D. (1965). On the solution of systems of linear equations with prime variables. *Acta Math. Sinica*, **15**, 731–48, translated in *Chin. Math.-Acta*, **7**, 461–79. [G].

Lucke, B. (1926). Zur Hardy–Littlewoodschen Behandlung des Goldbachschen Problems. Dissertation. Math.-naturwiss. Göttingen. [3].

Lursmanashvili, A. P. (1966). Representation of natural numbers by sums of prime numbers. *Thbilis. Sahelmc. Univ. Shrom. Mekh.-Math. Mecn. Ser.*, **117**, 63–76. [3].

Mahler, K. (1957). On the fractional parts of the powers of a rational number II. *Mathematika*, **4**, 122–4. [1].
Mahler, K. (1968). An unsolved problem on the powers of 3/2. *J. Aust. Math. Soc.*, **8**, 313–21. [1].
Malyshev, A. V. & Podsypanin, E. V. (1974). Analytic methods in the theory of systems of Diophantine equations and inequalities with a large number of unknowns. *Algebra, Topology, Geometry*, **12**, 5–50. *Akad. Nauk SSSR Vsesojuz. Inst. Nauk i Tehn. Informacii. Moscow.* [S].
Mardzhanishvili, K. K. (1936, 1937). Über die simultane Zerfällung ganzer Zahlen in m-te und n-te Potenzen. *Dokl. Akad. Nauk SSSR*, **2**, 263–4 and *Izv. Akad. Nauk SSSR, Ser. Mat.*, 609–31. [7].
Mardzhanishvili, K. K. (1939). Sur un système d'équations de Diophante. *Doklady Akad. Nauk SSSR*, **22**, 467–70. [7].
Mardzhanishvili, K. K. (1940). Sur un problème additif de la théorie des nombres. *Izv. Akad. Nauk SSSR*, **4**, 193–214. [7].
Mardzhanishvili, K. K. (1941). Sur la démonstration du théorème de Goldbach–Vinogradoff. *Dokl. Akad. Nauk SSSR*, **30**, 687–9. [3].
Mardzhanishvili, K. K. (1947). On an asymptotic formula of the additive theory of prime numbers. *Soobscheniya Akad. Nauk Gruzin. SSR*, **8**, 597–604. [G].
Mardzhanishvili, K. K. (1949). On some additive problems with prime numbers. *Uspehi Mat. Nauk*, **4**, 183–5. [G].
Mardzhanishvili, K. K. (1950*a*). On a generalization of Waring's problem. *Soobscheniya Akad. Nauk Gruzin. SSR*, **11**, 82–4. [G].
Mardzhanishvili, K. K. (1950*b*). On a system of equations in prime numbers. *Dokl. Akad. Nauk SSSR*, **70**, 381–3. [G].
Mardzhanishvili, K. K. (1950*c*). Investigations on the application of the method of trigonometric sums to additive problems. *Uspehi Mat. Nauk*, **5**, 236–40. [G].
Mardzhanishvili, K. K. (1951*a*). On the simultaneous representation of pairs of numbers by sums of primes and their squares. *Akad. Nauk Gruzin. SSR. Trudy Mat. Inst. Razmaaze*, **18**, 183–208. [G].
Mardzhanishvili, K. K. (1951*b*). On some additive problems of the theory of numbers. *Acta Math. Acad. Sci. Hungar.*, **2**, 223–7. [S].
Mardzhanishvili, K. K. (1953). On some nonlinear systems of equations in integers. *Mat. Sb.*, **33**, (75), 639–75. [7].
Miech, R. J. (1968). On the equation $n = p + x^2$. *Trans. Am. Math. Soc.*, **130**, 494–512. [G].
Mirsky, L. (1958). Additive prime number theory. *Math. Gaz.*, **42**, 7–10. [S].
Mitsui, T. (1960*a*,*b*). On the Goldbach problem in an algebraic number field I, II. *J. Math. Soc. Jpn.*, **12**, 290–324 and 325–372.
Montgomery, H. L. (1971). A lemma in additive prime number theory. In *Topics in multiplicative number theory. Lecture Notes in Mathematics*, **227**, Chapter 16. Berlin: Springer-Verlag. [3].
Montgomery, H. L. & Vaughan, R. C. (1973). Error terms in additive prime number theory. *Q. J. Math.*, (2), **24**, 207–16. [3].
Montgomery, H. L. & Vaughan, R. C. (1975). The exceptional set in Goldbach's problem. *Acta Arith.*, **27**, 353–70. [3].
Mordell, L. J. (1932). On a sum analogous to a Gauss's sum. *Q. J. Math.*, **3**, 161–7. [7].

Narasimhamurti, V. (1941). On Waring's problem for 8th, 9th and 10th powers. *J. Indian Math. Soc.*, **5**, 122. [6].

Nechaev, V. I. (1949, 1953). The representation of integers by sums of terms of the form $x(x+1)\ldots(x+n-1)/n!$. *Dokl. Akad. Nauk SSSR*, **64**, 159–62 and *Izv. Akad. Nauk SSSR Ser. Mat.*, **17**, 485–98. [G].

Nechaev, V. I. (1951). Waring's problem for polynomials. *Trudy Mat. Inst. Steklov*, **38**, 190–243. [G].

Nechaev, V. I. (1958). Multinomials with small $G(f)$. *Uch. Zap. Moscow. gor. ped. in-ta*, **71**, 291–300. [G].

Nechaev, V. I. & Telesin, Ju. Z. (1962). On the exact value of $G(f,\rho)$ for sums of multinomials of the second degree. *Uch. Zap. Moscow. gor. ped in-ta*, **188**, 131–8. [G].

Newman, D. J. (1960). A simplified proof of Waring's conjecture. *Michigan Math. J.*, **7**, 291–5. [1].

Niven, I. (1944). An unsolved case of the Waring problem. *Am. J. Math.*, **66**, 137–43. [1].

Norton, K. K. (1966). On homogeneous diagonal congruences of odd degree. Ph. D. thesis. University of Illinois. [9].

Padhy, B. (1936). Pillai's exact formula for the number $g(n)$ in Waring's problem. *Proc. Indian Acad. Sci.*, **3A**, 341–5. [1].

Pan, C. -T. (1959). Some new results in the additive prime number theory. *Acta Math. Sinica*, **9**, 315–29. [3].

Page, A. (1934*a,b*). On the representation of a number as a sum of squares and products I, III. *Proc. Lond. Math. Soc.*, (2), **36**, 241–56 and **37**, 1–16. [G].

Pillai, S. S. (1936*a,b,c,d*, 1937*a,b*, 1938*a,b,c*). On Waring's problem; I. *J. Indian Math. Soc.*, **2**, 16–44, 131: II. *J. Annamalai Univ.*, **5**, 145–66: III. *Ibid.*, **6**, 50–3: IV. *Ibid.*, **6**, 54–64: V. *J. Indian Math. Soc.*, **2**, 213–14: VI. *J. Annamalai Univ.*, **6**, 171–197 : VII. *Proc. Indian Acad. Sci.*, **9A**, 29–34 : VIII. *J. Indian Math. Soc.*, **3**, 205–20: IX. *Ibid.*, 221–5. [1].

Pillai, S. S. (1940). On Waring's problem $g(6)=73$. *Proc. Indian Acad. Sci.*, **12A**, 30–40. [1].

Pil'tai, G. Z. (1972). On the size of the difference between consecutive primes. *Issled. teor. chisel*, 73–9. [G].

Pitman, J. (1968). Cubic inequalities. *J. Lond. Math. Soc.*, **43**, 119–26. [11].

Pitman, J. (1971*a*), Bounds for the solutions of diagonal inequalities. *Acta Arith.*, **18**, 179–90. [11].

Pitman, J. (1971*b*). Bounds for solutions of diagonal equations. *Acta Arith.*, **19**, 223–47. [9, 11].

Pitman, J. & Ridout, D. (1967). Diagonal cubic equations and inequalities. *Proc. R. Soc. Lond.*, **297A**, 476–502. [11].

Pleasants, P. A. B. (1966*a*). The representation of primes by cubic polynomials. *Acta Arith.*, **12**, 23–45. [G].

Pleasants, P. A. B. (1966*b*). The representation of primes by quadratic and cubic polynomials. *Acta Arith.*, **12**, 131–63. [G].

Pleasants, P. A. B. (1967). The representation of integers by cubic forms. *Proc. Lond. Math. Soc.*, (3), **17**, 553–76. [G].

Prachar, K. (1953*a,b*). Über ein Problem vom Waring–Goldbach'schen Typ. I, II. *Monatsh. Math.*, **57**, 66–74; 113–16. [G].

Prachar, K. (1957). *Primzahlverteilung*. Berlin: Springer-Verlag. [3].
Rademacher, H. (1924*a*). Über eine Erweiterung des Goldbachshen Problems. *Math. Z.*, **25**, 627–57. [3].
Rademacher, H. (1924*b*). Zur additiven Primzahltheorie algebraischer Zahlkörper, I Über die Darstellung totalpositiver Zahlen als Summe von totalpositiven Primzahlen im reell-quadratischen Zahlkörper. *Abh. Math. Sem. Hansischen Univ.*, **3**, 109–63. [G].
Rademacher, H. (1924*c*). Zur additiven Primzahltheorie algebraischer Zahlkörper, II Über die Darstellung von Körperzahlen als Summe von Primzahlen im imaginärquadratischen Zahlkörper. *Abh. Math. Sem. Hansischen Univ.*, **3**, 331–78. [G].
Rademacher, H. (1926). Zur additiven Primzahltheorie algebraischer Zahlkörper, III Über die Darstellung totalpositiver Zahlen als Summen von totalpositiven Primzahlen in einem beliebigen Zahlkörper. *Math. Z.*, **27**, 321–426. [G].
Rademacher, H. (1942). Trends in research: the analytic number theory. *Bull. Am. Math. Soc.*, **48**, 379–401. [S].
Rademacher, H. (1950). Additive algebraic number theory. *Proc. Intern. Congr. Math.*, **1**, 356–62. [S].
Raghavan, S. (1974). On a Diophantine inequality for forms of additive type. *Acta Arith.*, **24**, 499–506. [11].
Ramachandra, K. (1973). On the sums $\sum_{j=1}^{k} \lambda_j f(p_j)$. *J. Reine Angew. Math.*, **262/263**, 158–65. [11].
Ramanujan, C. P. (1963). Cubic forms over algebraic number fields. *Proc. Camb. Philos. Soc.*, **59**, 683–705. [G].
Richert, H.-E. (1953). Aus der additiven Primzahltheorie. *J. Reine Angew. Math.*, **191**, 179–98. [3].
Ridout, D. (1958). Indefinite quadratic forms. *Mathematika*, **5**, 122–4. [11].
Rieger, G. R. (1953*a*). Über eine Verallgemeinerung des Waringschen Problems. *Math. Z.*, **58**, 281–3. [1].
Rieger, G. R. (1953*b,c*). Zur Hilbertschen Lösung des Waringschen Problems: Abschätzung von $g(n)$. *Mitt. Math. Sem. Giessen*, **44**, 1–35. and *Arch. Math.*, **4**, 275–81. [1].
Rieger, G. R. (1954). Zu Linniks Lösung des Waringschen Problems: Abschatzung von $g(n)$. *Math. Z.*, **60**, 213–34. [1].
Roth, K. F. (1949). Proof that almost all positive integers are sums of a square, a positive cube and a fourth power. *J. Lond. Math. Soc.*, **24**, 4–13. [8].
Roth, K. F. (1951). On Waring's problem for cubes. *Proc. Lond. Math. Soc.*, (2) **53**, 268–79. [[illegible]].
Roth, K. F. (19[illegible]). A problem in additive number theory. *Proc. Lond. Math. Soc.*, (2), **53**, 381–95. [8].
Roth, K. F. (1952). Sur quelques ensembles d'entiers. *C. R. Acad. Sci. Paris*, **234**, 388–90. [10].
Roth, K. F. (1953, 1954). On certain sets of integers I, II. *J. Lond. Math. Soc.*, **28**, 104–9 and **29**, 20–6. [10].
Roth, K. F. (1967*a,b*, 1970, 1972). Irregularities of sequences relative to arithmetic progressions I, II, III, IV. *Math. Ann.*, **169**, 1–25; *ibid.*, **174**, 41–52, *J. Number Theor*, **2**, 125–42; *Periodica Math. Hungar.*, **2**, 301–26. [10].
Rubugunday, R. K. (1942). On $g(k)$ in Waring's problem. *J. Indian Math. Soc.*, **6**, 192–8. [1].

Ryavec, C. (1969). Cubic forms over algebraic number fields. *Proc. Camb. Philos. Soc.*, **66**, 323–33. [G].

Salem, R. & Spencer, D. C. (1942). On sets of integers which contain no three terms in arithmetical progression. *Proc. Natn. Acad. Sci. U.S.A.*, **28**, 561–3. [10].

Salem, R. & Spencer, D. C. (1950). On sets which do not contain a given number of terms in arithmetical progression. *Niew. Arch. Wisk.*, (2), **23**, 133–43. [10].

Sambasiva Rao, K. (1941). On Waring's problem for smaller powers. *J. Indian Math. Soc.*, **5**, 117–21. [6].

Sárközy, A. (1978*a*,*b*,*c*). On difference sets of integers I, III, II. *Acta Math. Acad. Sci. Hungar.*, **31**, 125–49; *ibid.*, 355–86; *Ann. Univ. Sci. Budapest Rolando Eötvös, Sect. Math.*, **21**, 45–53. [10].

Sastry, S. & Singh, R. (1955/6). A problem in additive number theory. *J. Sci. Res. Banaras Hindu Univ.*, **6**, 251–65. [8].

Schmidt, E. (1913). Zum Hilbertschen Beweis des Waringschen Theorems. *Math. Ann.*, **74**, 271–4. [1].

Schmidt, W. M. (1976). *Equations over finite fields. An elementary approach. Lecture Notes in Mathematics*, **536**, Berlin: Springer–Verlag. [B].

Schmidt, W. M. (1979*a*,*b*). Small zeros of additive forms in many variables I, II. *Trans. Amer. Math. Soc.*, **248**, 121–33; *Acta Math.*, **143**, 219–32. [9].

Schmidt, W. M. (1980). Diophantine inequalities for forms of odd degree. *Advances in Math.*, **38**, 128–51.

Schwarz, W. (1960/1, 1961). Zur Darstellung von Zahlen durch Summen von Primzahlpotenzen I, II. *J. Reine Angew. Math.*, **205**, 21–47; **206**, 78–112. [G].

Schwarz, W. (1963). Uber die Lösbarkeit gewisser Ungleichungen durch Primzahlen. *J. Reine Angew. Math.*, **212**, 150–7. [8].

Scourfield, E. J. (1960). A generalization of Waring's problem. *J. Lond. Math. Soc.*, **35**, 98–116. [5,8].

Siegel, C. L. (1944). Generalization of Waring's problem to algebraic number fields. *Am. J. Math.*, **66**, 122–36. [G].

Siegel, C. L. (1945). Sums of *m*th powers of algebraic integers. *Ann. Math.*, (2), **46**, 313–39. [G].

Sinnadurai, J. St.-C. L. (1965). Representation of integers as sums of six cubes and one square. *Q. J. Math.*, (2), **16**, 289–96. [8].

Stanley, G. K. (1929). On the representation of a number as a sum of squares and primes. *Proc. Lond. Math. Soc.*, (2), **29**, 122–44. [G].

Stanley, G. K. (1930). The representation of a number as the sum of one square and a number of *k*-th powers. *Proc. Lond. Math. Soc.*, (2), **31**, 512–53. [G].

Statulevicius, V. (1955). On the representation of odd numbers as the sum of three almost equal prime numbers. *Vilniaus Valst. Univ. Mokslo Darbai Mat. Fiz.-Chem. Mokslu Ser.*, **3**, 5–23. [3].

Stemmler, R. M. (1964). The ideal Waring theorem for exponents 401–200 000. *Math. Comp.*, **18**, 144–6. [1].

Stridsberg, E. (1912). Sur la démonstration de M. Hilbert du théorème de Waring. *Math. Ann.*, **72**, 145–52. [1].

Subhankulov, M. A. (1960). Additive properties of certain sequences of numbers. *Issled. po mat. anal. mech. Uzb.*, 220–41. [G].

Szekeres, G. (1978). Major arcs in the four cubes problem. *J. Aust. Math. Soc.*, **25A**, 423–37. [G].

Szemerédi, E. (1969). On sets of integers containing no four elements in arithmetic progression. *Acta Math. Acad. Sci. Hungar.*, **20**, 89–104. [10].

Szemerédi, E. (1975). On sets of integers containing no *k* elements in arithmetic progression. *Acta Arith.*, **27**, 199–245. [10].

Tartakovsky, W. (1935). Über asymptotische Gesetze der allgemeinen Diophantischen Analyse mit vielen Unbekannten. *Bull. Acad. Sci. URSS*, 483–524. [9].

Tartakovsky, W. (1958*a*,*b*). The number of representations of large numbers by a form of "general type" with many variables I, II. *Vestnik Leningrad Univ.*, **13**, 131–54; **14**, 5–17. [9].

Tatuzawa, T. (1955). Additive prime number theory in an algebraic number field. *J. Math. Soc. Jpn.*, **7**, 409–23. [G].

Tatuzawa, T. (1958). On the Waring problem in an algebraic number field. *J. Math. Soc. Jpn.*, **10**, 322–41. [G].

Tatuzawa, T. (1973). On Waring's problem in algebraic number fields. *Acta Arith.*, **24**, 37–60. [G].

Telesin, Yu. Z. (1958). Waring's problem for polynomials of degree 7, 8, 9, 10. *Uch. zap. Moscow. gor. ped. in-ta*, **71**, 301–11. [G].

Thanigasalam, K. (1966). A generalization of Waring's problem for prime powers. *Proc. Lond. Math. Soc.*, (3), **16**, 193–212. [G].

Thanigasalam, K. (1967). Asymptotic formula in a generalized Waring's problem. *Proc. Camb. Philos. Soc.*, **63**, 87–98. [8].

Thanigasalam, K. (1967/1968). On additive number theory. *Acta Arith.*, **13**, 237–58. [G].

Thanigasalam, K. (1969). Note on the representation of integers as sums of certain powers. *Proc. Camb. Philos. Soc.*, **65**, 445–6. [8].

Thomas, H. E. Jr. (1974). Waring's problem for twenty two biquadrates. *Trans. Am. Math. Soc.*, **193**, 427–30. [1].

Tietäväinen, A. (1964). On the non-trivial solvability of some systems of equations in finite fields. *Ann. Univ. Turku. Ser. A.* I, No. 71. [9].

Tietäväinen, A. (1965). On the non-trivial solvability of some equations and systems of equations in finite fields. *Ann. Acad. Sci. Fenn. Ser. A.* I, No. 360. [9].

Tietäväinen, A. (1971). On a problem of Chowla and Shimura, *J. Number Theor.*, **3**, 247–52. [9].

Toliver, R. H. (1975). Bounds for solutions of two simultaneous additive equations of odd degree. Ph.D. thesis. University of Michigan. Ann. Arbor. [G].

Tong, K.-C. (1957). On Waring's problem. *Adv. Math.*, **3**, 602–7. [5].

Trost, E. (1958). Eine Bemerkung zum Waringschen Problem. *Elem. Math.*, **13**, 73–5. [1].

Uchiyama, S. (1961). Three primes in arithmetical progression. *Proc. Jpn. Acad.*, **37**, 329–30. [3].

Vaughan, R. C. (1970). On the representation of numbers as sums of powers of natural numbers. *Proc. Lond. Math. Soc.*, (3), **21**, 160–80. [8].

Vaughan, R. C. (1971). On sums of mixed powers. *J. Lond. Math. Soc.*, (2), **3**, 677–88. [6].

Vaughan, R. C. (1972). On Goldbach's problem. *Acta Arith.*, **22**, 21–48. [3].

Vaughan, R. C. (1973). A new estimate for the exceptional set in Goldbach's problem. *Am. Math. Soc. Proc. Symp. Pure Math.*, **24**, 315–20. [3].

Vaughan, R. C. (1973/1974). A survey of recent work in additive prime number theory. *Sem. Théor. Nombres*, **19**, 1–7. Bordeaux. [S].

Vaughan, R. C. (1974*a*, *b*). Diophantine approximation by prime numbers I, II. *Proc. Lond. Math. Soc.*, (3), **28**, 373–84; 385–401. [11].

Vaughan, R. C. (1975). Mean value theorems in prime number theory. *J. Lond. Math. Soc.*, (2), **10**, 153–62. [3].

Vaughan, R. C. (1977*a*). On pairs of additive cubic equations. *Proc. Lond. Math. Soc.*, (3), **34**, 354–64. [G].

Vaughan, R. C. (1977*b*). Homogeneous additive equations and Waring's problem. *Acta Arith.*, **33**, 231–53. [5, 6, 9].

Vaughan, R. C. (1977*c*). Sommes trigonométriques sur les nombres premiers. *C. R. Acad. Sci. Paris, Sér. A*, **258**, 981–3. [3].

Vaughan, R. C. (1979). A survey of some important problems in additive number theory. *Soc. Math. de France. Astérisque*, **61**, 213–22. [S].

Vaughan, R. C. (1980*a*). A ternary additive problem. *Proc. Lond. Math. Soc.*, **41**, 516–32. [8].

Vaughan, R. C. (1980*b*). *Recent work in additive prime number theory.* Proceedings of the International Congress of Mathematicians, Helsinki, 1978, 389–94. [3].

Veidinger, L. (1958). On the distribution of the solutions of diophantine equations with many unknowns. *Acta Arith.*, **5**, 15–24. [G].

Verdenius, W. (1949). On problems analogous to those of Goldbach and Waring. *Ned. Akad. Wet.*, **52** = *Indag. Math.*, **11**, 255–63. [G].

Vinogradov, A. I. (1955). On some new theorems of the additive theory of numbers. *Dokl. Akad. Nauk SSSR*, **102**, 875–76. [G].

Vinogradov, A. I. (1956). On an almost binary problem. *Izv. Akad. Nauk SSSR, Ser. Mat.*, **20**, 713–50. [G].

Vinogradov, A. I. (1963). On a problem of L. K. Hua. *Dokl. Akad. Nauk SSSR*, **151**, 255–7. [3].

Vinogradov, I. M. (1928*a*). Sur le théorème de Waring. *C. R. Acad. Sci. URSS*, 393–400. [1].

Vinogradov, I. M. (1928*b*). Sur la représentation d'un nombre entier par un polynom à plusiers variables. *C. R. Acad. Sci. URSS*, (7), **1**, 401–14. [1].

Vinogradov, I. M. (1934*a*). A new solution of Waring's problem. *C. R. Acad. Sci. URSS*, (2), **2**, 337–41. [5].

Vinogradov, I. M. (1934*b*). On the upper bound $G(n)$ in Waring's problem. *C. R. Acad. Sci. URSS*, 1455–69. [5].

Vinogradov, I. M. (1935*a*). Une nouvelle variante de la démonstration du théorème de Waring. *C. R. Acad. Sci. Paris*. **200**, 182–4. [5].

Vinogradov, I. M. (1935*b*). On Waring's problem. *Ann. Math.*, **36**, 395–405. [5].

Vinogradov, I. M. (1935*c*). A new variant of Waring's theory. *Trav. Inst. Steklov*, **9**, 5–15. [5].

Vinogradov, I. M. (1935*d*). On Weyl's sums, *Rec. Math.*, **42**, 521–30. [5].

Vinogradov, I. M. (1935*e*). An asymptotic formula for the number of representations in Waring's problem. *Rec. Math.*, **42**, 531–4. [5].

Vinogradov, I. M. (1937*a*). Representation of an odd number as a sum of three primes. *C. R. Acad. Sci. URSS*, **15**, 6–7. [3].

Vinogradov, I. M. (1937*b*). Some theorems concerning the theory of primes. *Rec. Math.*, **2**, (44), 2, 179–95. [3].

Vinogradov, I. M. (1937*c*). Some new problems of the theory of primes. *C. R. Acad. Sci. URSS*, **16**, 131–2. [G].

Vinogradov, I. M. (1937*d*). A new method in analytic number theory. *Trav. Inst. Steklov*, **10**, 1–122. [5].

Vinogradov, I. M. (1947). The method of trigonometrical sums in the theory of numbers. *Trav. Inst. Steklov*, **23**, translated from the Russian, revised and annotated by Davenport, A & Roth, K. F. (1954). New York: Interscience. [E].
Vinogradov, I. M. (1954). *Elements of number theory*, New York: Dover. Translated from the fifth Russian edition of 1949 by S. Kravetz. [B].
Vinogradov, I. M. (1959). On an upper bound for $G(n)$. *Izv. Akad. Nauk SSSR*, **23**, 637–42. [7].
Waerden, B. L. van der. (1927). Beweis einer Baudetschen Vermutung. *Niew Arch. Wisk.*, **15**, 212–16. [10].
Walfisz, A. (1941*a,b*). Zur additiven Zahlentheorie VII(1), (2). *Soobschenia Akad. Nauk Gruzinskoi SSR*, **2**, 7–14; 221–6. [3].
Watson, G. L. (1951). A proof of the seven cube theorem. *J. Lond. Math. Soc.*, **26**, 153–6. [1].
Watson, G. L. (1953). On indefinite quadratic forms in five variables. *Proc. Lond. Math. Soc.*, (3), **3**, 170–81. [11].
Watson, G. L. (1969). A cubic Diophantine equation. *J. Lond. Math. Soc.*, (2), **1**, 163–73. [G].
Weyl, H. (1916). Über die Gleichverteilung von Zahlen mod Eins. *Math. Ann.* **77**, 313–52. [2].
Whiteman, A. L. (1940). Additive prime number theory in real quadratic fields. *Duke Math. J.*, **7**, 208–32. [G].
Wilson, R. J. (1969). The large sieve in algebraic number fields. *Mathematika*, **16**, 189–204. [5].
Wright, E. M. (1933*a,b*). The representation of a number as a sum of five or more squares I, II. *Q. J. Math.*, **4**, 37–51; 228–32. [G].
Wright, E. M. (1934). Proportionality conditions in Waring's problem. *Math. Z.*, **38**, 730–46. [G].
Zuckerman, H. S. (1936). New results for the number $g(n)$ in Waring's problem. *Am. J. Math.*, **58**, 545–52. [1].
Zulauf, A. (1952*a*). Beweis einer Erweiterung des Satzes von Goldbach–Vinogradov. *J. Reine Angew. Math.*, **190**, 169–98. [3].
Zulauf, A. (1952*b*). Zur additiven Zerfallung natürlicher Zahlen in Primzahlen und Quadrate. *Arch. Math.*, **3**, 327–33. [G].
Zulauf, A. (1953*a*). Über den dritten Hardy–Littlewoodschen Satz zur Goldbachschen Vermutung. *J. Reine Angew. Math.*, **192**, 117–28. [3].
Zulauf, A. (1953*b*, 1954*a,b*). Über die Darstellung natürlicher Zahlen als Summen von Primzahlen aus gegebenen Restklassen und Quadraten mit gegebenen Koeffizienten. I, Resultate für genügend gross Zahlen; II, Die Singulare Reihe; III Resultate für "fast alle" Zahlen. *J. Reine Angew. Math.*, **192**, 210–29; **193**, 39–53; **193**, 54–64. [G].
Zulauf, A. (1961). On the number of representations of an integer as a sum of primes belonging to given arithmetical progressions. *Compos. Mat.*, **15**, 64–9. [3]

Список работ на русском языке

Архипов Г. И., Карацуба А. А. Новая оценка интеграла И. М. Виноградова. — Изв. АН СССР, сер. матем., 42 (1978), 751—762.

Архангельская В. М. Некоторые численные расчеты, связанные с проблемой Гольдбаха. — Укр. матем. журнал, 9 (1957), 20—29.

Бабаев Г., Субханкулов М. А. Асимптотическая формула для двух аддитивных задач. — Уч. зап. Тадж. ун-та, 26, сер. матем. (1963), 49—68.

Вальфиш А. Аддитивная теория чисел VII (1), (2). — Сообщ. АН Груз. ССР, 2 (1941), 7—14; 221—226.

Виноградов А. И. О некоторых новых теоремах аддитивной теории чисел. — ДАН СССР, 102 (1955), 875—876.

Виноградов А. И. Об одной «почти бинарной» задаче. — Изв. АН СССР, сер. матем., 20 (1956), 713—750.

Виноградов А. И. Об одной проблеме Хуа Ло-кена. — ДАН СССР, 151 (1963), 255—257.

Виноградов И. М. О теореме Варинга. — Изв. АН СССР, ОМЕН (1928), 393—400.

Виноградов И. М. О представлении числа целым многочленом от нескольких переменных. — Изв. АН, ОМЕН (1928), 401—414.

Виноградов И. М. Новое решение проблемы Варинга. — ДАН СССР, 2 (1934), 337—341.

Виноградов И. М. О верхней границе $G(k)$ в проблеме Варинга. — Изв. АН СССР, ОФМН (1934), 1455—1469.

Виноградов И. М. Новый вариант вывода теоремы Варинга. — Труды Физ.-матем. ин-та АН СССР, 9 (1935), 5—16.

Виноградов И. М. Представление нечетного числа суммой трех простых чисел. — ДАН СССР, 15 (1937), 6—7.

Виноградов И. М. Некоторые новые проблемы теории простых чисел. — ДАН СССР, 16 (1937), 131—132.

Виноградов И. М. Новый метод в аналитической теории чисел. — Труды Физ.-матем. ин-та АН, 10 (1937), 1—122.

Виноградов И. М. Метод тригонометрических сумм в теории чисел. — Труды Матем. ин-та АН, 23 (1947), 1—111.

Виноградов И. М. Основы теории чисел. — М.: ГИТТЛ, 1954.

Виноградов И. М. К вопросу о верхней границе для $G(n)$. — Изв. АН СССР, сер. матем., 23 (1959), 637—642.

Дэвенпорт Г. Мультипликативная теория чисел. — М.: Наука, 1971.

Емельянов Г. В. Об одной системе диофантовых уравнений. — Л.: Уч. зап. ун-та, сер. матем., 19 (1950), 3—39.

Калинка В. Обобщение леммы Хуа Ло-кена для алгебраических чисел. — Литовский матем. сб., 3 (1963), 149—155.

Карацуба А. А. Об оценке числа решений некоторых уравнений. — ДАН СССР, 165 : 1 (1965), 31—32.

Карацуба А. А. О некоторых системах неопределенных уравнений. — Матем. зам., 4 (1968), 125—128.

Карацуба А. А., Коробов Н. М. О теореме о среднем. — ДАН СССР, 149, 2 (1963), 245—248.
Лаврик А. Ф. Об одном предложении аддитивной теории чисел. — Успехи матем. наук, 14 (1959), 197—198.
Лаврик А. Ф. К бинарным гипотезам теории простых чисел по методу И. М. Виноградова. — ДАН СССР, 132, (1960), 1013—1015.
Лаврик А. Ф. К распределению простых чисел k-близнецов. — ДАН СССР, 132 (1960), 1258—1260.
Лаврик А. Ф. О числе простых чисел k-близнецов, лежащих на отрезке заданной длины. — ДАН СССР, 136 (1961), 281—283.
Лаврик А. Ф. К бинарным проблемам аддитивной теории простых чисел в связи с методом тригонометрических сумм И. М. Виноградова. — Л.: Вестн. ун-та, 16 (1961), 11—27.
Лаврик А. Ф. К теории распределения простых чисел на основе метода тригонометрических сумм И. М. Виноградова. — Труды Матем. ин-та АН СССР, 64 (1961), 90—125.
Лаврик А. Ф. К теории распределения совокупностей простых чисел с заданными разностями между ними. — ДАН СССР, 138 (1961), 1287—1290.
Лаврик А. Ф. О представлении чисел в виде суммы простых по методу Л. Г. Шнирельмана. — Изв. АН УзССР, сер. физ.-матем. н., 3 (1962), 5—10.
Линник Ю. В. О разложении больших чисел на семь кубов. ДАН СССР, 35 (1942), 179—180.
Линник Ю. В. Элементарное решение проблемы Варинга по методу Шнирельмана. — Матем. сб., 12 (1943), 225—230.
Линник Ю. В. О возможности единого метода в некоторых вопросах аддитивной и дистрибутивной теории простых чисел. — ДАН СССР, 48 (1945), 3—7.
Линник Ю. В. Новое доказательство теоремы Гольдбаха — Виноградова.— Матем. сб., 19 (61) (1946), 3—8.
Линник Ю. В. Простые числа и степени двойки. — Труды Матем. ин-та АН СССР, 38 (1951), 152—169.
Линник Ю. В. Некоторые условные теоремы, касающиеся бинарных задач с простыми числами. — ДАН СССР, 77 (1951), 15—18, и Изв. АН СССР, сер. матем. 16 (1952), 503—520.
Линник Ю. В. Складывание простых чисел со степенями одного и того же числа. — Матем. сб., 32(74) (1953), 3—60.
Лурсманашвили А. П. О представлении натуральных чисел суммами простых чисел. — Тбилиси: Труды ун-та, 117, сер. мех.-матем. 17. 5 (1966), 63—76.
Малышев А. В., Подсыпанин Е. В. Аналитические методы в теории систем диофантовых уравнений и неравенств с большим числом неизвестных. — М.: Ин-т науч.-технич. информации АН СССР, 12 (1974), 5—50.
Марджанишвили К. К. Об одновременном представлении двух чисел суммами полных m-х и n-х степеней. — ДАН СССР, 2 (1936), 263—264 и Изв. АН СССР, сер. матем. (1937), 609—631.
Марджанишвили К. К. Об одной системе диофантовых уравнений. — ДАН СССР, 22 (1939), 467—470.
Марджанишвили К. К. Об одной задаче аддитивной теории чисел. — Изв. АН СССР, 4 (1940), 193—214.
Марджанишвили К. К. К доказательству теоремы Гольдбаха — Виноградова. — ДАН СССР, 30 (1941), 687—690.
Марджанишвили К. К. Об одной асимптотической формуле аддитивной теории простых чисел. — Сообщение АН ГрузССР, 8 (1947), 597—604.
Марджанишвили К. К. О некоторых аддитивных задачах с простыми числами. — Успехи матем. н., 4 (1949), 183—185.

Марджанишвили К. К. Об одном обобщении прблемы Варинга. — Сообщение АН ГрузССР, 11 (1950), 82—84.
Марджанишвили К. К. Об одной системе уравнений в простых числах. — ДАН СССР, 70 (1950), 381—383.
Марджанишвили К. К. Исследования по применению метода тригонометрических сумм к аддитивным проблемам. — Успехи матем. н., 5 (1950), 236—240.
Марджанишвили К. К. Об одновременном представлении пары чисел суммами простых чисел и их квадратов. — Сообщения АН ГрузССР, Труды Матем. ин-та, 18 (1951), 183—208.
Марджанишвили К. К. О некоторых нелинейных системах уравнений в целых числах. — Матем. сб., 33(75) (1953), 639—675.
Монтгомери Г. Мультипликативная теория чисел. Пер. с англ. — М.: Мир, 1974.
Нечаев В. И. Представление целых чисел суммой слагаемых вида $x(x+1)\ \ldots (x+n-1)/n!$. — ДАН СССР, 64 (1949), 159—162 и Изв. АН СССР, сер. матем., 17 (1953), 485—498.
Нечаев В. И. Проблема Варинга для многочленов. — Труды Матем. ин-та АН СССР, 38 (1951), 190—243.
Нечаев В. И. Многочлены с малым $G(f)$. — Уч. зап. Москов. гор. пед. ин-та, 71 (1958), 291—300.
Нечаев В. И., Телесин Ю. З. О точном значении $G(f, a)$ для последовательности многочленов второй степени. — Уч. зап. Москов. гор. пед. ин-та, 188 (1962), 131—138.
Прахар К. Распределение простых чисел. Пер. с англ. — М.: Мир, 1967.
Статулявичус В. А. О представлении нечетных чисел суммой трех почти равных простых чисел.— Вильнюс: Ученые труды ун-та, 3 (1955), 5—23.
Субханкулов М. А. Аддитивные свойства некоторых последовательностей. — В сб. «Исследов. по матем. анализу и мех. в Узбекистане», Ташкент (1960), 220—241.
Тартаковский В. А. О количестве представлений больших чисел формами «общего вида» с большим числом переменных I, II. — Л.: Вестн. ун-та, 7, сер. матем. 2 (1958), 131—154; 2 (1959), 5—17.
Телесин Ю. З. Проблема Варинга для многочленов степени 7, 8, 9 и 10. — М.: Уч. зап. гор. пед. ин-та, 71 (1958), 301—311.
Фрейман Г. А. Решение проблемы Варинга в новой постановке. — Успехи матем. н., 4 : 1 (29) (1949), 193.
Хассе Г. Лекции по теории чисел. Пер. с англ. — М.: ИЛ, 1953.
Хуа Ло-кен. О представлении чисел суммами k-х степеней простых чисел. — ДАН СССР (2), 17 (1937), 167—168.
Хуа Ло-кен. Некоторые результаты в проблеме Варинга для малых степеней. — ДАН СССР (2), 18 (1938), 527—528.
Хуа Ло-кен. Некоторые результаты в аддитивной теории простых чисел. — ДАН СССР (2), 18 (1938), 3.
Хуа Ло-кен. О системах диофантовых уравнений.— ДАН СССР, 27 (1940), 312—313.
Хуа Ло-кен. Аддитивная теория простых чисел. — Труды Матем. ин-та АН СССР, XXII, М.-Л., 1947.
Чудаков Н. Г. О проблеме Гольдбаха. — ДАН СССР (2), 17 (1937), 335—338.
Чудаков Н. Г. О плотности совокупности четных чисел, непредставимых как суммы двух нечетных простых. — Изв. АН СССР, сер. матем., 2 (1938), 25—40.

Литература, добавленная переводчиком*

1*. Bessel-Hagen E. (1929) Bemercungen zur Behandlung des major arc bei der Anwendung der Hadry — Littlewood'schen Methode auf das Waringiche Problem. Proc. London Math. Soc. (2), 29, 328—400. [4].
2*. Baker R. C., Hartman G. (1982) Diophantine approximation by prime numbers. J. London Math. Soc. (2), 25, 201—215. [11].
3*. Balasubramanian R. Mozzochi C. J. (1984) An improved upper bound for $G(k)$ in Waring's problem for relatively small k. Acta Arith., 43, 283—285. [5].
4*. Heath-Brown D. R. (1981) Three primes and an almost prime in arit thmetic progression. J. London Math. Soc. (2), 23, 396—414. [3].
5*. Heath-Brown D. R. (1983) Cubic forms in ten variables. Proc. London Math. Soc. (3), 47, 255—257. [9].
6*. Линник Ю. В. (1943) On Weil's sum. Матем. сб. 12(54), 28—39. [5].
7*. Thanigasalam K. (1980a) On Waring's problem. Acta Arithm., 38, 141—155. [5].
8*. Thanigasalam K. (1980b, 1982b) On sums of powers and a related problem. Acta Arith., 36, 125—141. Addendum and Gorrigendum. Acta Arithm., 42, 425. [8].
9*. Thanigasalam K. (1982a) Some new estimates for G(k) in Waring's problem. Acta Arith; 42, 73—78. [5].
10*. Vaughan R. C. (В печати, a) Sums of three positive cubes. Bull. London Some remarks on weil sums, Colloquia Math. Soc. Jànos Bolyai, Budapest, 1981. [4].
11*. Vaughan R. C. (В печати, b) Sums of three positive cubes. Bull. London Math. Soc. [8].
12. Виноградов И. М. Метод тригонометрических сумм в теории чисел.— М.: Наука, 1980.
13. Виноградов И. М. Особые варианты метода тригонометрических сумм. — М.: Наука, 1976.
14. Карацуба А. А. Основы аналитической теории чисел. — М.: Наука, 1983.
15. Венков Б. А. Элементарная теория чисел. ОНТИ — НКТП, СССР, 1937.
16. Хассе Г. Лекции по теории чисел. — М.: ИЛ, 1953.

* Звездочкой отмечена литература, добавленная по просьбе автора.

Именной указатель

Предметный указатель

Оглавление