А.О. Гельфонд, Ю.В. Линник

Элементарные методы в аналитической теории чисел

А.О. Гельфонд, Ю.В. Линник

Элементарные методы в аналитической теории чисел

А.О.Гельфанд, Ю.В.Линник
ЭЛЕМЕНТАРНЫЕ МЕТОДЫ В АНАЛИТИЧЕСКОЙ ТЕОРИИ ЧИСЕЛ
М.: Физматгиз, 1962 г., 272 стр.

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Многие важные задачи современной аналитической теории чисел могут быть формулированы в терминах элементарной математики и понятия предела или даже просто понятия безгранично возрастающего параметра. Таков, например, закон простых чисел, теорема И. М. Виноградова о том, что все достаточно большие нечетные числа — суммы трех простых чисел, и количество соответствующих представлений выражается простой предельной (асимптотической) формулой, теоремы о счете целых точек внутри расширяющихся контуров, о поведении дробных частей последовательностей и многие другие. Вместе с тем решение соответствующих, сформулированных в простых терминах проблем часто требовало весьма сложных и на первый взгляд далеких от теории чисел средств. Так, до недавнего времени закон простых чисел мог быть обоснован только с помощью теории функций комплексного переменного, и появление в 1949 г. полностью элементарных доказательств А. Сельберга, и П. Эрдеша и А. Сельберга явилось крупным событием в теории чисел. Теория функций комплексного переменного существенно применялась и в аддитивных задачах (первоначальные варианты Гарди—Литтлвуда решений проблемы Варинга), различных теоремах о распределении простых чисел и их обобщений, решении А. О. Гельфонда VII проблемы Гильберта и многих других случаях. Ряды Фурье и тригонометрические суммы играют фундаментальную роль в аддитивных задачах, теория полей функций над абстрактным полем констант и алгебраическая топология получают все возрастающее значение в современной теории чисел. Все перечисленные трансцендентные методы приводят в ряде случаев к весьма сильным и точным результатам, и от них можно ожидать еще очень многого. Не может быть и речи об отказе от трансцендентных методов в современной

теории чисел. Однако естественным желанием исследователя является отыскание возможно более арифметического пути к решению элементарно формулируемой проблемы. Помимо очевидного методического значения такого пути, он важен еще тем, что часто дает простой и естественный взгляд на полученные теоремы и причины, обусловливающие их существование. Часто элементарными методами можно достигнуть результатов, недоступных пока сильным аналитическим средствам, действующим в других случаях весьма эффективно. Таково, например, положение с бинарными задачами типа проблемы Гольдбаха; наиболее важные результаты здесь выводятся с помощью элементарного метода решета Эратосфена, разработанного Вигго Бруном. В большинстве известных случаев, однако, элементарные методы, в основном давая решение проблемы, все же уступают трансцендентным методам в отношении дальнейших уточнений получаемых предельных соотношений.

В настоящее время весьма многие задачи аналитической теории могут быть решены элементарными средствами; соответствующие решения публиковались в ряде журналов и монографий. Представляется целесообразным несколько систематизировать их, внести возможные упрощения и собрать вместе. Данная книга ставит себе эту цель. Здесь собраны элементарные методы в аддитивных задачах, в задачах счета целых точек внутри контуров (асимптотическая геометрия чисел), в теории распределения простых чисел. Глава 10 содержит элементарное доказательство Ю. И. Манина римановой гипотезы для эллиптических полей функций над конечным полем (теоремы о сравнениях третьей степени). Это доказательство переработано и упрощено автором его по сравнению с первоначальным вариантом 1956 г. Глава 12 излагает впервые построенное А. О. Гельфондом элементарное доказательство его теоремы о трансцендентности чисел вида α^β (α, β — алгебраические числа, $\alpha \neq 0$ и 1; β иррациональное) для случая вещественных α и β.

Заметим, что «степень элементарности» предлагаемых в различных главах методов различная. В проблемах счета целых точек в контурах, по существу, нельзя обойтись без понятия площади кривой, касательной и радиуса кривизны, т. е. понятия определенного интеграла и производной. В соответствующих главах эти понятия в простейшей форме

применяются. В главе «Трансцендентность некоторых классов чисел» применяется понятие алгебраического числа и понятие производной. Те параграфы, где применяются понятия производной или интеграла, отмечаются звездочкой. Заметим, что таких параграфов в книге немного.

Чтение книги требует некоторых познаний в элементарной теории чисел. Достаточны сведения в объеме книги И. М. Виноградова «Основы теории чисел» и первых четырех глав книги Б. А. Венкова «Элементарная теория чисел».

Помимо А. О. Гельфонда и Ю. В. Линника, соавторами данной книги являются А. И. Виноградов и Ю. И. Манин. А. О. Гельфонд составил главы 3 и 12, Ю. В. Линник — главы 1, 2, 4, 7, 8, 9, 11, А. И. Виноградов написал главы 5, 6; Ю. И. Манин — главу 10.

ГЛАВА 1

АДДИТИВНЫЕ СВОЙСТВА ЧИСЕЛ. МЕТОД Л. Г. ШНИРЕЛЬМАНА. ТЕОРЕМА Г. МАННА. ТЕОРЕМА П. ЭРДЕША

§ 1. Аддитивные свойства последовательностей

Будем рассматривать бесконечные последовательности целых чисел, начинающиеся с нуля:

$$0,\ a_1,\ a_2,\ a_3,\ldots \qquad (1,1,1)$$

Здесь $0<a_1<a_2<\ldots$

Последовательности такого рода будем обозначать большими латинскими буквами; например, последовательность (1, 1, 1) обозначим буквой A. Иногда нам придется рассматривать различные последовательности такого вида; в подобном случае будем снабжать числа вида (1, 1, 1) двумя индексами:

$$0,\ a_{i1},\ a_{i2},\ a_{i3},\ldots \qquad (1,1,2)$$

где $i=1,\ 2,\ldots,\ N$ и образуют N последовательностей A_i.

Если даны N последовательностей A_i $(i=1,\ 2,\ldots,\ N)$ (среди которых могут быть и одинаковые), то будем называть суммой A_i новую последовательность $A_1+\ldots+A_N$ вида

$$0,\ b_1,\ b_2,\ b_3,\ldots,$$

где

$$b_j=a_{1j_1}+a_{2j_2}+\ldots+a_{Nj_N}$$

есть сумма каких-либо из N чисел наших последовательностей, взятых каждая по одному разу. При этом допускаются и слагаемые a_{i0}, под которыми мы будем понимать число 0 $(i=1,\ 2,\ldots,\ N)$; получившиеся числа b_i будут рассчиты-

ваться один и только один раз и упорядочиваться по возрастанию.

Аддитивная теория числа изучает свойства операции суммирования последовательностей; в частности описывает числа, получившиеся в результате суммирования последовательностей. При этом выделяются случаи, когда в результате суммирования ограниченного числа последовательностей, получаются все целые числа или все достаточно большие целые числа.

Если последовательность A после суммирования самой с собой k раз дает все целые числа, то она называется базисом k-го порядка. (Разумеется, она будет тогда и базисом порядка $k_1 > k$.) В элементарной теории чисел известна теорема Лагранжа о том, что всякое число есть сумма четырех квадратов. Таким образом, последовательность квадратов Q есть базис 4-го порядка. Последовательность кубов образует базис 9-го порядка (что уже трудно обосновать элементарными методами).

Иногда рассматривают базисные свойства последовательностей, принимая во внимание не все числа, а лишь достаточно большие числа. Если последовательность A после суммирования k раз дает последовательность, куда входят все достаточно большие числа, то будем называть ее базисом k-го порядка для достаточно больших чисел. Такое понятие целесообразно, так как во многих случаях основные свойства сумм последовательностей вскрываются при наблюдениях над большими числами; на структуру малых ее членов будут, естественно, влиять лишь несколько начальных членов последовательности.

Согласно известной теореме И. М. Виноградова [1], суммирование последовательности P простых чисел (со включением 0) три раза образует последовательность $P+P+P$, куда входят все достаточно большие нечетные числа. Таким образом, последовательность P образует базис 4-го порядка для достаточно больших чисел. Последовательность кубов, которую мы рассматривали ранее, образует базис 7-го порядка для достаточно больших чисел ([13], [14]). В 1930 г. Л. Г. Шнирельман [30] поставил проблему изучения суммирования последовательностей общего вида, сведения о которых касаются лишь «плотности» расположения в них членов. Понятие «плотности» последовательности A определяется по Л. Г. Шнирельману следующим образом.

Пусть $A(n)=\sum_{a_l\leqslant n} 1$ — числовая функция последовательности, количество ее членов, не превосходящих n (при подсчете $a_0=0$ опускается). Тогда

$$0\leqslant\frac{A(n)}{n}\leqslant 1.$$

Плотностью $d(A)$ последовательности A называется

$$d(A)=\inf_n\frac{A(n)}{n}. \qquad (1,1,3)$$

Заметим в виде примера, что если $1\overline{\in}A$, то $d(A)=0$. Далее, $d(A)=1$ тогда и только тогда, когда A содержит весь натуральный ряд. Плотность последовательности квадратов, кубов, простых чисел равна 0. Л. Г. Шнирельман доказал следующую важную теорему о плотности суммы последовательностей A и B.

Теорема 1.1.1 (Л. Г. Шнирельман).

$$d(A+B)\geqslant d(A)+d(B)-d(A)d(B). \qquad (1,1,4)$$

Для доказательства рассмотрим натуральные числа сегмента $[1,n]$ и введем числовые функции A и B: $A(n)$ и $B(n)$. Далее обозначим: $A+B=C$; $d(A)=\alpha$; $d(B)=\beta$; $d(C)=\gamma$. На сегменте $[1,n]$ лежит $A(n)$ чисел из A, каждое из которых входит и в C. Пусть a_k, a_{k+1} — два соседних числа такого вида. Между ними лежат числа

$$a_k+1,\ a_k+2,\ldots,\ a_k+l=a_{k+1}-1,$$

которые не принадлежат A. Некоторые из этих чисел будут входить в $C=A+B$: например, такими будут числа a_k+r, где $r\in B$. Число чисел последнего вида, очевидно, будет $B(l)$. Таким образом,

$$C(n)\geqslant A(n)+\sum_{(l)}B(l),$$

где сумма идет по отрезкам между числами вида a_k и a_{k+1}. Далее: $B(l)\geqslant\beta l$. Таким образом,

$$C(n)\geqslant A(n)+\beta\sum l=A(n)+\beta(n-A(n))=$$
$$=A(n)(1-\beta)+\beta n\geqslant\alpha(1-\beta)n+\beta n$$

для всех $n \geqslant 1$. Отсюда

$$\gamma = d(C) = \inf_n \frac{C(n)}{n} \geqslant \alpha + \beta - \alpha\beta,$$

что и доказывает (1, 1, 4).

Неравенство (1, 1, 4) удобно записать в виде

$$1 - d(A+B) \leqslant (1 - d(A))(1 - d(B)), \qquad (1, 1, 5)$$

откуда легко вывести по индукции неравенство, годное для любого числа слагаемых:

$$d(A_1 + \cdots + A_k) \geqslant 1 - \prod_{i=1}^{k} (1 - d(A_i)). \qquad (1, 1, 6)$$

Из неравенства (1, 1, 6) следует простая, но важная теорема Л. Г. Шнирельмана.

Теорема 1. 1. 2 (Л. Г. Шнирельман). *Всякая последовательность положительной плотности — базис натурального ряда.*

В самом деле, из (1, 1, 6) для одной и той же последовательности A имеем при $\underbrace{A + \cdots + A}_{k \text{ раз}} = A^{(k)}$

$$d(A^{(k)}) \geqslant 1 - (1 - \alpha)^k.$$

При достаточно большом k имеем

$$d(A^{(k)}) > \frac{1}{2}. \qquad (1, 1, 7)$$

Ввиду этого на сегменте $[1, n]$ количество чисел $A^{(k)}$ будет больше $\frac{n}{2}$. Если a_i пробегает систему чисел $A^{(k)}$, не превосходящих n, то чисел $|a_i|$ с присоединением 0 и чисел $|n - a_i|$ в совокупности будет больше $n + 1$, и они не могут быть все различны. Отсюда имеем: $n = a_{i_1} + a_{i_2}$ — сумма двух чисел $A^{(k)}$, так что A есть базис не более чем $2k$ порядка. Эта теорема найдет важные приложения в следующих главах.

§ 2. Теорема Г. Манна

Неравенство Л. Г. Шнирельмана (1, 1, 4) не является точным, и допускает замечательное усиление. Пусть, как и ранее, $C = A + B$.

Теорема 1.2.1 (Г. Манн).

$$d(C) \geqslant \min\,(d(A)+d(B),\,1)\ *). \qquad (1,2,1)$$

Мы можем считать, не нарушая общности, что $d(A)+d(B)\leqslant 1$; если это неравенство нарушается, то мы всегда можем выбросить в одной из последовательностей некоторое количество достаточно далеких чисел так, чтобы у новых последовательностей A', B' было $d(A')+d(B')<1$ и $d(A')+d(B')$ сколь угодно близко к 1. Тогда из (1, 2, 1) будет следовать, что $d(C)\geqslant d(A'+B')$ сколь угодно близко к 1, а значит, $d(C)=1$.

Итак, считаем, что $d(A)+d(B)\leqslant 1$. Надо доказать, что

$$d(C)\geqslant d(A)+d(B). \qquad (1,2,2)$$

Доказательство опирается на основную лемму.

Лемма. *При каждом* $n\geqslant 1$ *найдется* $m\in[1,\ n]$ *такое, что*

$$C(n)-C(n-m)\geqslant(\alpha+\beta)\,m, \qquad (1,2,3)$$

(*как и ранее*, $\alpha=d(A)$; $\beta=d(B)$; $\gamma=d(C)$).

Доказательство этой леммы довольно затруднительно, однако неравенство (1, 2, 2) и основная теорема (1, 2, 1) выводятся из неё без труда.

Пусть (1, 2, 3) доказано. Рассмотрим сегмент $[1,\ n-m]$. По указанной лемме там найдется сегмент $[n-m-m'+1,\ n-m]$, где количество чисел C не меньше чем $(\alpha+\beta)\,m'$. Выделим из $[1,\ n-m-m']$ крайний правый сегмент с подобным же свойством и продолжаем это рассуждение далее. В результате, очевидно, приходим к неравенству (1, 2, 2).

Теперь перейдем к доказательству нашей леммы. Будем рассматривать подмножества сегмента чисел $0, 1, \ldots, n$. Будем считать, что $n\in C$, ибо иначе для числа n лемма тривиальна: при $m=1$

$$C(n)-C(n-m)=C(n)-C(n-1)\geqslant(\alpha+\beta)\,1.$$

---

*) Эта теорема, бывшая предметом усилий многих математиков, была доказана Г. Манном в 1942 г. [42]; в 1949 г. Э. Артин и Шерк [32] дали более простое доказательство, еще более упрощенное А. Я. Хинчиным [28], изложению которого мы здесь следуем.

Систему чисел $H \subset [0, n]$ будем называть ***нормальной***, если для любых чисел $f \in [1, n]$; $f' \in [1, n]$; $f \overline{\in} (H)$; $f' \overline{\in} H$ имеем: $f + f' - n \overline{\in} H$. Если последовательность C обладает тем свойством, что отрезки ее в сегменте $[0, n]$ образуют нормальную систему, то лемма легко доказывается для $C(n)$. Именно, пусть m — наименьшее натуральное число, не входящее в C; тогда $m \leqslant n$, ибо по условию, $n \overline{\in} C$.

Пусть $s \in (n - m, n)$; тогда $0 < s + m - n < m$. Тогда $s \in C$. Будь это не так, имели бы: $s \overline{\in} C$; $m \overline{\in} C$. По свойству нормальности $s + m - n \overline{\in} C$, но $s + m - n < m$, а m — наименьшее число, не принадлежащее C. Ввиду этого все числа $s \in (n - m, n)$ входят в C. Следовательно,

$$C(n) - C(n - m) = m - 1.$$

Так как $m \overline{\in} C = A + B$, то должно быть $A(m) + B(m) \leqslant \leqslant m - 1$, как легко видеть, рассуждая, как при доказательстве теоремы 1. 2. 1. Таким образом,

$$C(n) - C(n - m) \geqslant A(m) + B(m) \geqslant (\alpha + \beta) m,$$

что доказывает (1, 2, 3).

Итак, теперь нужно допустить, что $C = A + B$ не обладает описанным выше свойством нормальности. В этом случае мы будем вводить особый метод определенного расширения множеств B и C, которое будем называть «подходящим расширением». Пусть C не обладает свойством нормальности. Тогда в интервале $(0, n)$ найдутся числа c, c' такие, что

$$c \overline{\in} C; \quad c' \overline{\in} C; \quad c + c' - n \in C.$$

Так как $C = A + B$, то отсюда

$$c + c' - n = a + b \qquad (a \in A, \ b \in B). \qquad (1, 2, 4)$$

Пусть $\beta_0 \in B$ — минимальное число, для которого выполняется (1, 2, 4). Оно будет называться базой нашего расширения. Уравнение

$$c + c' - n = a + \beta_0$$

будет иметь решение в числах c, c', a, удовлетворяющих условиям: $c \overline{\in} C$, $c' \overline{\in} C$; $a \in A$; c, c', $a \in (0, n)$. Все удовлетворяющие указанному уравнению и данным условиям числа

c, c' объединим в множество C^*. Имеем: $C \cap C^*$ — пустое множество. Объединение

$$C \cup C^* = C_1$$

и будем называть подходящим расширением множества C. Рассмотрим выражение

$$\beta_0 + n - c. \qquad (1, 2, 5)$$

Если c пробегает числа множества C^*, то значения $\beta_0 + n - c$ образуют множество B^*; в силу указанного выше уравнения числа (1, 2, 5) можно представить в виде $c' - a$, где $c' \in C^*$, $a \in A$.

Пусть b^* — любое число из B^*. Так как оно имеет вид $\beta_0 + n - c$, то $b^* \geqslant \beta_0 \geqslant 0$; так как $b^* = c' - a$, то $b^* \leqslant c' \leqslant n$, так что все числа B^* лежат в интервале $(0, n)$. Далее, так как $b^* \in B^*$, то $b^* \overline{\in} B$, ибо иначе из $b^* = c' - a$ следовало бы $c' = a + b^* \in A + B = C$, что неверно. Таким образом, $B^* \cap B$ — пустое множество; B^* лежит в отрезке $(0, n)$. Положим

$$B \cup B^* = B_1.$$

Множество B_1 будем называть подходящим расширением множества B.

Докажем теперь, что

$$A + B_1 = C_1.$$

Пусть $a \in A$, $b_1 \in B_1$; покажем, что $a + b_1 \in C_1$. Либо $b_1 \in B$, либо $b_1 \in B^*$. Если $b_1 \in B$, то $a + b_1 \in A + B = C \subset C_1$; если $b_1 \in B^*$, то $a + b_1 \in C \subset C_1$ либо $a + b_1 \overline{\in} C$. В этом случае, так как $b_1 \in B^*$, то $b_1 = \beta_0 + n - c'$; $c' \overline{\in} C$, так что

$$c'' = a + b_1 = a + \beta_0 + n - c' \overline{\in} C$$

и

$$c'' + c' - n = a + \beta_0 \in A + B = C; \quad c'' \overline{\in} C; \quad c' \overline{\in} C;$$

по определению C^* находим

$$c'' = a + b_1 \in C^* \subset C_1.$$

Итак, $A + B_1 \subset C_1$. Обратно, пусть $c \in C_1$, так что $c \in C$ либо $c \in C^*$. Если $c \in C$, то $c = a + b$; $a \in A$; $b \in B \subset B_1$.

Если же $c \in C^*$, то $b^* = c - a$ при некотором a входит в B^*. Имеем: $c = a + b^* \in A + B^* \subset A + B_1$. Таким образом,

$$C_1 = A + B_1.$$

Далее, $n \overline{\in} C_1$. В самом деле, $n \overline{\in} C$; если бы $n \in C^*$, то в соотношении $c + c' - n = a + \beta_0$ мы могли бы положить $c' = n$, и получилось бы: $c = a + \beta_0 \in A + B = C$, что невозможно, так как $c \overline{\in} C$.

Если расширенная последовательность C_1 еще не нормальна, то рассматриваем множества A, B_1, C_1; здесь $A + B_1 = C_1$; $n \overline{\in} C_1$; положение вполне аналогично предыдущему и для множеств A, B_1, C_1 можем применить предшествующие рассуждения.

Снова находим базу для расширения β_1, множества B_1^*, C_1^* и полагаем

$$B_1 \cup B_1^* = B_2; \qquad C_1 \cup C_1^* = C_2$$

и находим, что

$$A + B_2 = C_2; \qquad n \overline{\in} C_2.$$

Продолжаем этот процесс до тех пор, пока одно из расширенных множеств C_k не окажется нормальным. Такой момент непременно наступит, ибо при каждом расширении мы вводим новые числа в интервал $(0, n)$. Так находим конечный ряд множеств

$$B = B_0 \subset B_1 \subset \ldots \subset B_k,$$
$$C = C_0 \subset C_1 \subset \ldots \subset C_k.$$

При этом всякое $B_{\mu+1}$ содержит числа, не входящие в B_μ и образующие B_μ^*, так что $B_{\mu+1} = B_\mu \cup B_\mu^*$; то же касается $C_{\mu+1} = C_\mu \cup C_\mu^*$ $(0 \leqslant \mu \leqslant k-1)$.

Пусть β_μ — база расширения от B_μ и C_μ к $B_{\mu+1}$ и $C_{\mu+1}$. Имеем

$$A + B_\mu = C_\mu; \; n \overline{\in} C_\mu \qquad (0 \leqslant \mu \leqslant k).$$

Далее, C_k — нормальное множество, а C_μ при $0 \leqslant \mu \leqslant k-1$ не являются нормальными.

Для дальнейшего нам нужно будет обнаружить некоторые свойства подходящих расширений.

Мы начнем с доказательства неравенства

$$\beta_\mu > \beta_{\mu-1} \qquad (1 \leqslant \mu \leqslant k-1). \qquad (1, 2, 6)$$

Заметим, что $\beta_\mu \in B_\mu = B_{\mu-1} \cup B^*_{\mu-1}$. Если $\beta_\mu \in B^*_{\mu-1}$, то

$$\beta_\mu = \beta_{\mu-1} + n - c,$$

где $c \in C^*_{\mu-1} \subset C_\mu$, так что $c < n$ и $\beta_\mu > \beta_{\mu-1}$. Если же $\beta_\mu \in B_{\mu-1}$, то, по определению β_μ, существуют числа $a \in A$, $c \in C_\mu$, $c' \in C_\mu$ такие, что

$$c + c' - n = a + \beta_\mu \in A + B_{\mu-1} = C_{\mu-1}. \qquad (1, 2, 7)$$

Ввиду этого, по свойству минимальности $\beta_{\mu-1}$, $\beta_\mu \geqslant \beta_{\mu-1}$. Однако если бы $\beta_\mu = \beta_{\mu-1}$, то, по определению $C^*_{\mu-1}$, имели бы из (1, 2, 7)

$$c \in C^*_{\mu-1} \subset C_\mu; \qquad c' \in C^*_{\mu-1} \subset C_\mu,$$

что неверно. Итак, $\beta_\mu \neq \beta_{\mu-1}$ и $\beta_\mu > \beta_{\mu-1}$. Обозначим через m наименьшее положительное число, не входящее в C_k. Докажем следующее утверждение.

Если $c \in C^*_\mu$ $(0 \leqslant \mu \leqslant k-1)$ и $c \in (n-m, n)$, то $c \in (n-m+\beta_\mu, n)$.

Достаточно доказать, что $c + m - n > \beta_\mu$. Из $c \in (n-m, n)$ следует: $m + c - n \in (0, m)$ и, по определению m,

$$m + c - n \in C_k.$$

Ввиду того что

$$C_k = C_\mu \cup C^*_\mu \cup C^*_{\mu+1} \ldots \cup C^*_{k-1},$$

мы будем в дальнейшем различать два случая:

1) $m + c - n \in C_\mu$.

В этом случае

$$m + c - n = a + b_\mu; \quad a \in A, \quad b_\mu \in B_\mu.$$

Но $m \in C_\mu$ и $c \in C_\mu$, так как $c \in C^*_\mu$. В силу минимальности β_μ, должны иметь: $b_\mu \geqslant \beta_\mu$. Однако если $b_\mu = \beta_\mu$, то, по определению C^*_μ, имели бы $m \in C^*_\mu$, что неверно, так как $C^*_\mu \subset C_\mu \subset C_k$, а $m \notin C_k$. Поэтому $b_\mu > \beta_\mu$ и, стало быть,

$$m + c - n = a + b_\mu > b_\mu > \beta_\mu,$$

что доказывает наше утверждение.

2) Если $c'=m+c-n\in C_\nu^*$ $(\mu\leqslant\nu\leqslant k-1)$, то, по определению C_ν^*, должны иметь

$$c'-a=\beta_\nu+n-c'';\ a\in A,\ c''\in C_\nu^*,$$

откуда $c'\geqslant c'-a>\beta_\nu\geqslant\beta_\mu$ (согласно (1, 2, 6)), и наше утверждение доказано.

Докажем еще равенство

$$C_\mu^*(n)-C_\mu^*(n-m)=$$
$$=B_\mu^*(m-1)\qquad(0\leqslant\mu\leqslant k-1).\qquad(1,2,8)$$

Рассмотрим соотношение

$$b=\beta_\mu+n-c;\qquad(1,2,9)$$

по определению B_μ^* и C_μ^*, из $c\in C_\mu^*$ следует: $b\subseteq B_\mu^*$ и обратно; если $c\in(n-m+\beta_\mu,\ n)$, то $b\in(\beta_\mu,\ m)$ и обратно. В виду этого

$$C_\mu^*(n)-C_\mu^*(n-m+\beta_\mu)=B_\mu^*(m-1)-B_\mu^*(\beta_\mu).$$

Но в силу предыдущего утверждения $C_\mu^*(n-m+\beta_\mu)=C_\mu^*(n-m)$; далее, всякое $b\in B_\mu^*$ выражается в виде (1, 2, 9), где $c<n$, так что $b>\beta_\mu$ и $B_\mu^*(\beta_\mu)=0$. Отсюда $C_\mu^*(n)-C_\mu^*(n-m)=B_\mu^*(m-1)$, что совпадает с (1, 2, 8).

Мы можем теперь перейти к доказательству нашей леммы. Так как C_k нормально, то к A, B_k, C_k можно применить неравенство (1, 2, 3), как было показано выше. Имеем:

$$C_k(n)-C_k(n-m)\geqslant A(m)+B_k(m),\qquad(1,2,10)$$

где m, как и ранее, — наименьшее натуральное число, не входящее в C_k; имеем, $m\overline{\in}A$ и $m\overline{\in}B_k$, так что $A(m)=A(m-1)$; $B_k(m)=B_k(m-1)$. Ввиду определений

$$C_k=C\cup C^*\cup C_1^*\cup\ldots\cup C_{k-1}^*,$$
$$B_k=B\cup B^*\cup B_1^*\cup\ldots\cup B_{k-1}^*,$$

где множества, входящие в эти объединения, не имеют общих элементов, найдем, обозначая $C_0^*=C^*$; $B_0^*=B^*$:

$$C_k(n)-C_k(n-m)=C(n)-C(n-m)+$$
$$+\sum_{\mu=0}^{k-1}\{C_\mu^*(n)-C_\mu^*(n-m)\},$$
$$B_k(m)=B_k(m-1)=B(m-1)+\sum_{\mu=0}^{k-1}B_\mu^*(m-1).$$

Из (1, 2, 10) находим отсюда

$$C(n) - C(n-m) + \sum_{\mu=0}^{k-1} \{C_\mu^*(n) - C_\mu^*(n-m)\} \geqslant$$

$$\geqslant A(m) + B(m-1) + \sum_{\mu=0}^{k-1} B_\mu^*(m-1).$$

Из (1, 2, 8) имеем

$$C_\mu^*(n) - C_\mu^*(n-m) = B_\mu^*(m-1) \qquad (0 \leqslant \mu \leqslant k-1).$$

Отбрасывая в предыдущем неравенстве суммы равных членов, получим

$$C(n) - C(n-m) \geqslant A(m) + B(m-1) =$$

$$= A(m) + B(m) \geqslant (\alpha + \beta)\, m,$$

что доказывает нашу лемму и тем самым теорему 1. 2. 1.

§ 3. Существенные компоненты. Теорема П. Эрдеша

Из теоремы Г. Манна мы видим, что если A — последовательность положительной плотности, меньшей 1, а B — другая последовательность положительной плотности, то от сложения A с B плотность увеличивается.

Таким свойством обладают не только последовательности положительной плотности, но и некоторые последовательности нулевой плотности. Последовательности B, которые обладают свойством увеличивать плотность любой последовательности A положительной плотности < 1, если их сложить с A, называются *существенными компонентами*.

В 1936 г. П. Эрдеш [38] вывел совершенно элементарным путем одну теорему о них, которая будет здесь изложена.

Теорема 1. 3. 1 (П. Эрдеш). *Всякий базис есть существенная компонента.*

Более точно, *если B есть базис l-го порядка, а A — последовательность положительной плотности $d(A) = \delta > 0$, то при $\delta < 1$*

$$d(A+B) \geqslant \delta + \frac{\delta(1-\delta)}{2l}. \qquad (1, 3, 1)$$

Мы будем доказывать даже более общую теорему: пусть целые числа, $\leqslant n$ и не принадлежащие A, обозначаются через $b_1, b_2, \ldots$, и пусть $b_y \leqslant n < b_{y+1}$; $a_x \leqslant n < a_{x+1}$. Положим

$$E = b_1 + b_2 + \ldots + b_y - \frac{y(y+1)}{2}.$$

Очевидно, $E \geqslant 0$, ибо $b_i \geqslant i$.

Как оказывается, существует не менее $x + \frac{E}{ln}$ чисел $\leqslant n$ вида $a + b$, где $a \in A$; $b \in B$, причем нам нужно будет использовать лишь числа $b = 0$ и еще одно $b \in B$.

Сперва докажем лемму.

Лемма. *Существует целое* $l > 0$ *такое, что есть по крайней мере* $\frac{E}{n}$ *чисел* b_v *среди чисел* $\leqslant n$ *вида* $a_1 + l$, $a_2 + l, \ldots$

Доказательство. Число решений уравнения

$$a + v = b$$

в целых положительных v, a, $b \leqslant n$, есть E. Именно, для заданного $b = b_r$ есть $b_r - r$ решений, ибо число чисел $a < b_r$ есть $b_r - r$, и каждое a дает решение v. Суммируя по $r = 1, 2, \ldots, y$, находим, что полное число решений есть

$$E = \sum_{r=1}^{y} (b_r - r).$$

Но число возможных значений v не превосходит n, и найдется хотя бы одно значение v, скажем l, для которого есть не менее $\frac{E}{n}$ решений уравнения $a + l = b$; a, $b \leqslant n$.

Перейдем к доказательству теоремы.

Так как B есть базис l-го порядка, то

$$l = b^{(1)} + \ldots + b^{(l)}; \quad b^{(v)} \in B.$$

Обозначим μ_s количество чисел b в множестве $a + b^{(s)}$ $(s = 1, 2, \ldots, l)$. Покажем, что

$$\mu_1 + \mu_2 + \ldots + \mu_l \geqslant \frac{E}{n}.$$

В самом деле, в множестве чисел вида

$$a + b^{(1)} + b^{(2)}$$

не более $\mu_1+\mu_2$ чисел b. Действительно, множество $a+b^{(1)}$ содержит μ_1 чисел b и некоторые из чисел a. Если прибавить $b^{(2)}$ к числам множества $a+b^{(1)}$, то μ_1 чисел b дают не более μ_1 чисел b; числа a дают не более μ_2 чисел b. Теперь возьмем числа вида $a+b^{(1)}+b^{(2)}+b^{(3)}$. Они содержат не более $\mu_1+\mu_2+\mu_3$ чисел b, что видно, если применим то же рассуждение к сумме $a+b^{(1)}+b^{(2)}$ и $b^{(3)}$. Аналогично множество чисел $a+b^{(1)}+\ldots+b^{(l)}=a+l$ будет содержать не более $\mu_1+\ldots+\mu_l$ чисел b. Но множество $a+l$ содержит по крайней мере $\frac{E}{n}$ чисел b, так что хотя бы одно из μ_l, скажем μ_k, удовлетворяет неравенству

$$\mu_k \geqslant \frac{E}{ln},$$

так что множество $a+b^{(k)}$ содержит не менее $\frac{E}{ln}$ чисел $b \leqslant n$. Но множество $a+b^{(0)}$, где $b^{(0)}=0$, содержит ровно x чисел a. Поэтому множества $a+b^{(i)}$ (учитывая и $b^{(i)}=0$) содержат по крайней мере $x+\frac{E}{ln}$ различных целых чисел $\leqslant n$. Далее, $d(A)=\delta$; $\delta\in(0, 1)$. Имеем: если $x=f(n)$, то $f(b_r)\geqslant \delta b_r$, откуда $b_r-r=f(b_r)>\delta b_r$; $b_r\geqslant\frac{r}{1-\delta}$. Отсюда

$$E\geqslant \frac{1+2+\ldots+y}{1-\delta}-\frac{y(y+1)}{2}\geqslant\frac{\delta}{2(1-\delta)}y(y+1).$$

Таким образом, для числа N чисел $\leqslant n$ множества $a+b^{(i)}$ имеем

$$N\geqslant x+\frac{\delta}{2(1-\delta)}\frac{y^2}{ln}\qquad (y=n-x).$$

Обозначим правую часть этого неравенства через $\Psi(x)$. Легко видеть, что $\Psi(x)$ — возрастающая функция; в этом убеждаемся, подсчитывая, что $\Psi(x+1)-\Psi(x)>0$. Отсюда

$$N\geqslant\Psi(x)\geqslant\Psi(\delta n)=\delta n+\frac{\delta}{2(1-\delta)}\frac{(1-\delta)^2n^2}{ln}=$$

$$=n\left(\delta+\frac{\delta(1-\delta)}{2l}\right),$$

что и доказывает теорему.

Последовательность $\{x^m\}$ $(x = 0, 1, 2, \ldots)$ при любом $m > 0$ образует базис, как было сказано в начале этой главы и будет доказано в следующей главе. Таким образом, эта последовательность является существенной компонентой. Могут быть существенные компоненты, которые не являются базисами. Пример такой компоненты был указан Ю. В. Линником [12]; однако этот пример не элементарен. Штором и Вирзингом [50] был найден пример, требующий лишь элементарных рассуждений.

ГЛАВА 2

ЭЛЕМЕНТАРНОЕ РЕШЕНИЕ ПРОБЛЕМЫ ВАРИНГА И ПРОБЛЕМЫ ГИЛЬБЕРТА — КАМКЕ

§ 1. О проблемах Варинга и Гильберта — Камке

Проблема Варинга состоит в исследовании базисных свойств последовательности n-х степеней: $\{x^n\}$ $(x = 0,1,2,..)$, $n \geqslant 1$. Как было уже сказано в главе 1, последовательность квадратов $(n = 2)$ образует базис 4-го порядка. В 1909 г. Д. Гильберт доказал, что последовательность n-х степеней образует базис, что и составило в основном решение проблемы Варинга. Однако ряд связанных с этой проблемой вопросов был решен лишь значительно позже, а некоторые из них остались нерешенными.

Были созданы новые мощные методы Гарди — Литтлвуда и И. М. Виноградова, позволившие не только решить ряд вопросов, относящихся к проблеме Варинга, но и далеко продвинуть другие проблемы аналитической теории чисел.

Изучался вопрос о виде функции $g(n)$ — минимальном порядке базиса из степеней $\{x^n\}$ для всех чисел; этот вопрос был в основном решен индийским математиком С. Пиллэ [43] в 1936 г. с помощью указанных методов. Изучался также вопрос о поведении функции $G(n)$ — минимальном базисе из n-х степеней для больших чисел. Здесь наиболее сильный результат был получен И. М. Виноградовым [1]:

$$G(n) < n\,(3 \ln n + 11). \qquad (2, 1, 1)$$

Кроме того, изучалась асимптотическая формула для количества представлений числа N в виде суммы s n-х степеней

$$x_1^n + \ldots + x_s^n = N. \qquad (2, 1, 2)$$

Все указанные работы по проблеме Варинга были выполнены с помощью глубоких и мощных аналитических методов. Элементарными методами пока можно лишь в основном решить проблему Варинга — доказать, что n-е степени чисел образуют базис. Элементарное доказательство этой теоремы было получено Ю. В. Линником [16] в 1943 г. А. Я. Хинчин [28] дал изящное изложение этого доказательства, которому мы будем следовать.

С проблемой Варинга сходна проблема Гильберта о системе диофантовых уравнений

$$\left.\begin{aligned} x_1^n + \ldots + x_s^n &= N_n, \\ x_1^{n-1} + \ldots + x_s^{n-1} &= N_{n-1}, \\ \cdots\cdots\cdots\cdots & \\ x_1 + \ldots + x_s &= N_1, \end{aligned}\right\} \qquad (2, 1, 3)$$

где $x_i \geqslant 0$ — целые числа. Эта проблема рассматривалась Э. Камке в 1921 г.; более сильные результаты получены К. К. Марджанишвили [19], [20].

В 1950 г. Г. В. Емельянов [8] продолжил исследования К. К. Марджанишвили, а также дал элементарное решение проблемы Гильберта — Камке, которое будет изложено в этой главе.

§ 2. Основная лемма в элементарном решении проблемы Варинга

Пусть A_n — последовательность n-х степеней; $A_n^{(k)}$ — сумма k последовательностей A_n. Если мы докажем, что при достаточно большом k $A_n^{(k)}$ имеет положительную плотность, то теорема 1.2.1 показывает нам, что A_n — базис натурального ряда. Ввиду этого будем заниматься доказательством того, что $d(A_n^{(k)}) > 0$ при $k > k_0(n)$. Пусть $m > 0$.

Рассмотрим уравнение

$$x_1^n + \ldots + x_k^n = m \qquad (x_i \geqslant 0). \qquad (2, 2, 1)$$

Пусть $r_k(m)$ — число решений уравнения (2, 2, 1). В дальнейшем часто встречающиеся слова: «число решений уравнения» будем сокращенно записывать: Ч.Р.У. Число $n \geqslant 2$ будем считать фиксированным. Сформулируем теперь основную лемму.

Лемма 1. *Существует* $k=k(n)$ *такое, что при любом* $N\geqslant 1$

$$r_k(m)=BN^{\frac{k}{n}-1} \qquad (1\leqslant m\leqslant N). \qquad (2,2,2)$$

Покажем, что из леммы 1 следует, что $d(A_n^{(k)})>0$. Имеем

$$r_k(0)+r_k(1)+\ldots+r_k(N)=R_k(N)$$

есть число решений неравенства

$$x_1^n+x_2^n+\ldots+x_k^n\leqslant N. \qquad (2,2,3)$$

Если x_i удовлетворяет неравенству

$$0\leqslant x_i\leqslant\left(\frac{N}{k}\right)^{\frac{1}{n}} \qquad (i\leqslant k),$$

то система чисел $(x_1,\ldots,x_k)$ удовлетворяет неравенству (2, 2, 3). Таким образом, неравенство (2, 2, 3) имеет не менее $\left(\frac{N}{k}\right)^{\frac{k}{n}}$ решений, так что

$$R_k(N)\geqslant\left(\frac{N}{k}\right)^{\frac{k}{n}}. \qquad (2,2,4)$$

Допустим теперь, что $d(A_n^{(k)})=0$. Тогда при любом $\varepsilon>0$ и подходящем N получим

$$A_n^{(k)}(N)<\varepsilon N.$$

При этом N можно считать сколь угодно большим. Применяя оценку (2, 2, 2), найдем

$$R_k(N)=\sum_{m=0}^{N}r_k(m)=r_k(0)+\sum_{m=1}^{N}r_k(m)<1+$$
$$+BN^{\frac{k}{n}-1}A_n^{(k)}(N)<1+B\varepsilon N^{\frac{k}{n}},$$

что противоречит (2, 2, 4) при достаточно малом ε. Итак, $d(A_n^{(k)})>0$. Мы должны теперь вывести основную лемму.

§ 3. Леммы о линейных уравнениях

Все дальнейшие уравнения будут диофантовы (целочисленные).

Лемма 2. *Пусть в уравнении*

$$a_1 z_1 + a_2 z_2 = m \qquad (2, 3, 1)$$

a_1, a_2, m — *целые*; $|a_2| \leqslant |a_1| \leqslant A$; $(a_1, a_2) = 1$.
Ч. Р. У. (2,3,1) *под условием* $|z_i| \leqslant A$ $(i = 1,2)$ *не превосходит* $\frac{3A}{|a_1|}$.

Мы можем считать, что $a_1 > 0$, иначе можно в каждом решении заменить z_1 на $(-z_1)$.

Пусть (z_1, z_2), (z_1', z_2') — два различных решения уравнения (2,3,1). Из равенств

$$a_1 z_1 + a_2 z_2 = m,$$
$$a_1 z_1' + a_2 z_2' = m$$

находим

$$a_2 (z_2' - z_2) = a_1 (-z_1' + z_1).$$

Далее, $(a_1, a_2) = 1$, так что $z_2' - z_2 \equiv 0 \pmod{a_1}$ и $|z_2' - z_2| \geqslant a_1$.

Число решений (z_1, z_2) под условием $|z_i| \leqslant A$ $(i = 1,2)$ не превосходит количества чисел z_2 в этих решениях под условием $|z_2| \leqslant A$. Но разность чисел вида z_2 делится на a_1. Если их число t, то имеем

$$a_1 (t - 1) \leqslant 2A; \qquad t \leqslant \frac{2A}{a_1} + 1 \leqslant \frac{3A}{a_1},$$

что и требовалось доказать.

Лемма 3. *Пусть в уравнении*

$$a_1 z_1 + \ldots + a_l z_l = m \qquad (2, 3, 2)$$

имеем: $|a_i| \leqslant A$ $(i \leqslant l)$; $\max |a_l| = H$ $(i \leqslant l)$; $(a_1, \ldots, a_l) = 1$. *Тогда Ч. Р. У.* (2, 3, 2) *под условиями*

$$|z_i| \leqslant A \qquad (i \leqslant l)$$

не превосходит

$$B_l \frac{A^{l-1}}{H}; \qquad (2, 3, 3)$$

Мы доказали уже эту лемму при $l=2$. Допустим, что $l\geqslant 3$ и что для случая $l-1$ неизвестных лемма 3 уже установлена. Пусть $\max\limits_i |a_i| = |a_l| = H$. Будем различать два случая:

1) $a_1 = a_2 = \ldots = a_{l-1} = 0$. Так как $(a_1, a_2, \ldots, a_l) = 1$, так что $|a_l| = H = 1$, и уравнение (2, 3, 2) имеет вид $z_l = \pm m$, так что z_l принимает не более одного значения, а все остальные z_i по абсолютной величине не превосходят A, и потому принимают не более $2A+1 \leqslant 3A$ значений. Таким образом, Ч. Р. У. (2, 3, 3) в указанных условиях в нашем случае не превосходит

$$(3A)^{l-1} = B_l \frac{A^{l-1}}{H}, \qquad (2, 3, 4)$$

что доказывает нашу лемму для случая 1).

2) Пусть хотя бы одно из чисел $a_1, a_2, \ldots, a_{l-1}$ отлично от 0. Тогда существует

$$(a_1, a_2, \ldots, a_{l-1}) = \delta.$$

Положим $H' = \max \frac{|a_i|}{\delta}$ $(i \leqslant l-1)$. Пусть числа $z_1, z_2, \ldots, z_l$ удовлетворяют нашему уравнению (2, 3, 2) и неравенствам $|z_i| \leqslant A$ $(i \leqslant l)$. Положим

$$\frac{a_1}{\delta} z_1 + \ldots + \frac{a_{l-1}}{\delta} z_{l-1} = m', \qquad (2, 3, 5)$$

так что

$$a_1 z_1 + a_2 z_2 + \ldots + a_{l-1} z_{l-1} = \delta m'$$

и

$$\delta m' + a_l z_l = m. \qquad (2, 3, 6)$$

Здесь

$$|\delta m'| \leqslant \sum_{i=1}^{l-1} |a_i|\,|z_i| \leqslant l\delta H' A,$$

так что

$$|m'| \leqslant lH'A. \qquad (2, 3, 7)$$

Мы заменили, таким образом, исходное уравнение (2, 3, 2) уравнениями (2, 3, 5) и (2, 3, 6). В уравнении (2, 3, 6) $\delta \leqslant |a_l|$; $(\delta, a_l) = (a_1, \ldots, a_l) = 1$. Ч. Р. У. (2, 3, 6), для которых $|m'| \leqslant lH'A$, $|z_l| \leqslant A < lH'A$ не превосходит $\frac{3lH'A}{|a_l|}$ в силу леммы 2. При

заданном m' уравнение (2, 3, 5), в силу индуктивного предположения, имеет $C(l)\frac{A^{l-2}}{H}$ решений в целых z_i, $|z_i| \leqslant A$.

Отсюда следует, что число решений $(z_1, \ldots, z_l)$ уравнения (2, 3, 2) под условием $|z_i| \leqslant A$ $(i \leqslant l)$, не превосходит

$$\frac{3lH'A}{|a_l|} c(l) \frac{A^{l-2}}{H'} = B_l \frac{A^{l-1}}{|a_l|} = B_l \frac{A^{l-1}}{H},$$

что и доказывает лемму 3.

Теперь рассмотрим совокупность всех уравнений вида

$$a_1 z_1 + a_2 z_2 + \ldots + a_l z_l = 0, \qquad (2, 3, 8)$$

где $|a_i| \leqslant A$ $(i \leqslant l)$. Пусть A_1 — какое-либо число, связанное с A соотношениями: $1 \leqslant A \leqslant A_1 \leqslant B_l A^{l-1}$, $l > 2$. Мы хотим оценить сверху сумму Ч. Р. У. (2, 3, 8) при условии, что $|z_i| \leqslant A_1$ $(i \leqslant l)$.

Лемма 4. *Совокупное Ч. Р. У.* (2, 3, 8) *не превосходит* $B_l (AA_1)^{l-1}$.

Будем снова различать три случая:

1) $a_1 = a_2 = \ldots = a_l = 0$ (такой случай тоже нужно учитывать). Для этого случая число решений $(z_1, \ldots, z_l)$, очевидно, не превосходит

$$(2A_1 + 1)^l \leqslant (3A_1)^l = B_l A_1^l = B_l A_1^{l-1} B_l A^{l-1} = B_l (AA_1)^{l-1}.$$

2) Хотя бы один из коэффициентов a_i отличен от 0, и

$$(a_1, a_2, \ldots, a_l) = \delta = 1.$$

Пусть в этом случае

$$H = \max(|a_1|, |a_2|, \ldots, |a_l|); \quad H \in [1, A].$$

Пусть m — целое число такое, что

$$\frac{A}{2^{m+1}} < H \leqslant \frac{A}{2^m}. \qquad (2, 3, 9)$$

Для одного уравнения вида (2, 3, 8), где $\delta = 1$ и H удовлетворяет неравенствам (2, 3, 9), число решений $z_i (|z_i| \leqslant A_1)$, в силу леммы 3, не превосходит

$$B_l \frac{A_1^{l-1}}{H} = B_l \frac{A_1^{l-1}}{\frac{A}{2^{m+1}}} = B_l \frac{A_1^{l-1} 2^m}{A}.$$

Далее, из (2, 3, 9) видно, что $|a_i| \leqslant \frac{A}{2^m}$ $(i \leqslant l)$. Таким образом, число уравнений, где соблюдаются неравенства типа (2, 3, 9), не превосходит

$$\left(2\frac{A}{2^m}+1\right)^l = B_l A^l 2^{-ml}.$$

А сумма соответствующих Ч. Р. У. не превосходит

$$B_l \frac{A_1^{l-1}2^m}{A} B_l A^l 2^{-ml} = B_l (AA_1)^{l-1} 2^{-(l-1)m}.$$

Суммируя это выражение по всем $m \geqslant 0$, находим совокупную оценку

$$B_l (AA_1)^{l-1}.$$

3) Хотя бы один из коэффициентов a_i отличен от 0, и $(a_1, a_2, \ldots, a_l) = \delta > 1$.

В этом случае заменяем уравнение вида (2, 3, 8) на уравнение

$$\frac{a_1}{\delta} z_1 + \ldots + \frac{a_l}{\delta} z_l = 0; \qquad \left(\frac{a_1}{\delta}, \ldots, \frac{a_l}{\delta}\right) = 1.$$

Число A заменяется на меньшее число $\frac{A}{\delta}$. Условие $A_1 = B_l A^{l-1}$ может быть нарушенным, но оно использовалось лишь в пункте 1), а не в пункте 2), а в дальнейшем мы будем опираться на пункт 2). В силу рассуждений пункта 2), при данном δ и $|z_i| \leqslant A_1$, совокупное Ч. Р. У. не превосходит

$$B_l \left(\frac{A}{\delta} A_1\right)^{l-1} = B_l \frac{(AA_1)^{l-1}}{\delta^{l-1}}. \qquad (2, 3, 10)$$

Далее, $\delta \leqslant A$. Суммарное Ч. Р. У. при разных δ не превосходит

$$B_l (AA_1)^{l-1} \sum_{\delta=1}^{A} \frac{1}{\delta^{l-1}}. \qquad (2, 3, 11)$$

При $q \geqslant 2$ имеет место элементарно доказываемое неравенство

$$\sum_{n=1}^{A} \frac{1}{n^q} < \frac{q}{q-1}.$$

Используя это неравенство при $q=l-1\geqslant 2$, находим для (2, 3, 11) оценку

$$B_l(AA_1)^{l-1}. \qquad (2, 3, 12)$$

Оценка (2, 3, 12) вместе с результатом случая 1) доказывает лемму 4.

Будем теперь рассматривать конечные множества целых чисел, которые могут содержать и равные между собой числа; если число a встречается во множестве A ровно λ раз, то будем говорить, что его кратность в A есть $\lambda=\lambda(a)$.

Пусть c — какое-либо целое число. Рассмотрим уравнение

$$x+y=c; \quad x\in A; \quad y\in B. \qquad (2, 3, 13)$$

Лемма 5. *В уравнении* (2, 3, 13) *число решений не превосходит полусуммы Ч. Р. У.*

$$x-y=0 \qquad (x\in A,\ y\in A)$$

и

$$x-y=0 \qquad (x\in B,\ y\in B).$$

Для доказательства заметим, что каждому значению $x\in A$ в уравнении (2, 3, 13) отвечает не более одного значения $y=y_x\in B$. а считая кратность, для данного x получаем не более $\lambda(x)\mu(y_x)$, где $\lambda(x)$ — кратность $x\in A$ и $\mu(y_x)$ — кратность $y_x\in B$. Далее, очевидно, $\lambda(x)\mu(y_x)\leqslant\frac{1}{2}((\lambda(x))^2+(\mu(y_x))^2)$. Суммируя по x и учитывая, что разным значениям x должны отвечать разные значения y_x, получим, что суммарная оценка Ч. Р. У. (2, 3, 13) не превосходит

$$\frac{1}{2}\sum_{x\in A}(\lambda(x))^2+\frac{1}{2}\sum_{y\in B}(\mu(y))^2, \qquad (2, 3, 14)$$

что, очевидно, совпадает с полусуммой чисел решений указанных выше уравнений.

Непосредственным следствием леммы является такой же результат для случая $A=B$.

Лемма 6. *Ч. Р. У.* $x+y=c\,(x\in A,\ y\in A)$ *не превосходит Ч. Р. У.* $x-y=0\,(x\in A,\ y\in A)$.

Пусть теперь k и s — произвольные натуральные числа. Положим $k2^s=l$ и будем рассматривать уравнение

$$x_1+x_2+\ldots+x_l=c.$$

Пусть $A_1, A_2, \ldots, A_l$ — конечные множества чисел; пусть множество $A_i\,(1 \leqslant i \leqslant l)$ содержит различные числа $a_{i_1}, a_{i_2}, \ldots$ с кратностями $\lambda_{i_1}, \lambda_{i_2}, \ldots$ Нас будет интересовать Ч. Р. У.

$$x_1 + x_2 + \ldots + x_l = c,\ x_i \in A_i\,(1 \leqslant i \leqslant l). \quad (2, 3, 15)$$

Если положить

$$x_1 + x_2 + \ldots + x_{\frac{l}{2}} = x,\ x_{\frac{l}{2}+1} + \ldots + x_l = y$$

($\frac{l}{2}$ есть, конечно, целое число), то данное уравнение можно переписать в виде

$$x + y = c$$

и применить к нему только что доказанную лемму 5. Рассмотрим, каким множествам должны принадлежать числа x и y. Так как $x_i \in A_i\,(1 \leqslant i \leqslant l)$, то x может быть любым числом вида $z_1 + z_2 + \ldots + z_{\frac{l}{2}}$, где $z_i \in A_i\,(1 \leqslant i \leqslant \frac{l}{2})$; точно так же y может быть любым числом того же вида, где только $z_i \in A_{\frac{l}{2}+i}$ $(1 \leqslant l \leqslant \frac{l}{2})$.

В силу леммы 5 поэтому Ч. Р. У. (2, 3, 15) не превосходит полусуммы Ч. Р. У.

$$x - y = 0 \quad (2, 3, 16)$$

в следующих двух предположениях:

1)

$$x = z_1 + z_2 + \ldots + z_{\frac{l}{2}},$$

$$y = z'_1 + z'_2 + \ldots + z'_{\frac{l}{2}},$$

где

$$z_i \in A_i,\ z'_i \in A_i \left(1 \leqslant i \leqslant \frac{l}{2}\right). \quad (2, 3, 17)$$

2) x и y имеет ту же форму, но

$$z_i \in A_{\frac{l}{2}+i},\quad z'_i \in A_{\frac{l}{2}+i} \left(1 \leqslant i \leqslant \frac{l}{2}\right). \quad (2, 3, 18)$$

В обоих случаях уравнение (2, 3, 16) может быть переписано в виде

$$(z_1 - z_1') + (z_2 - z_2') + \ldots + (z_{\frac{l}{2}} - z_{\frac{l}{2}}') = 0. \quad (2, 3, 19)$$

Мы приходим таким образом к выводу, что Ч. Р. У. (2, 3, 15) не превосходит полусуммы Ч. Р. У. (2, 3, 17) в предположениях (2, 3, 17) и (2, 3, 18), т. е. не превосходит полусуммы Ч. Р. У.

$$\sum_{i=1}^{\frac{l}{2}} (z_i - z_i') = 0, \quad z_i \in A_i, \quad z_i' \in A_l \left(1 \leqslant i \leqslant \frac{l}{2} \right)$$

и

$$\sum_{i=1}^{\frac{l}{2}} (z_i - z_i') = 0, \quad z_i \in A_{\frac{l}{2}+i}, \quad z_i' \in A_{\frac{l}{2}+i} \left(1 \leqslant i \leqslant \frac{l}{2} \right).$$

Уравнение (2, 3, 19) имеет в левой части $\frac{l}{2}$ слагаемых, т. е. вдвое меньше, чем первоначальное уравнение (2, 3, 15). Полагая

$$\sum_{i=1}^{\frac{l}{4}} (z_i - z_i') = x, \qquad \sum_{i=\frac{l}{4}+1}^{\frac{l}{2}} (z_i - z_i') = y,$$

мы приводим уравнение (2, 3, 19) к виду

$$x + y = 0$$

и можем снова применить к нему лемму 5. Совершенно тем же путем, как от уравнения (2, 3, 15) мы пришли к уравнению (2. 3, 19), теперь от уравнения (2, 3, 19) мы придем, очевидно, к уравнению

$$\sum_{i=1}^{\frac{l}{4}} (u_i + u_i' - u_i'' - u_i''') = 0, \quad (2, 3, 20)$$

причем нам придется рассматривать сумму чисел решений этого уравнения в следующих (уже четырех) предположениях:

$$1)\ u_i,\ u_i',\ u_i'',\ u_i'''\in A_i,$$
$$2)\ u_i,\ u_i',\ u_i'',\ u_i'''\in A_{\frac{l}{4}+i},$$
$$3)\ u_i,\ u_i',\ u_i'',\ u_i'''\in A_{\frac{l}{2}+i},$$
$$4)\ u_i,\ u_i',\ u_i'',\ u_i'''\in A_{\frac{3l}{4}+i}$$
$$\left(1\leqslant i\leqslant\frac{l}{4}\right).$$

Так как $l=k2^s$, то мы можем повторить этот процесс s раз. В результате мы, очевидно, придем к уравнению

$$\sum_{i=1}^{k}\{y_i^{(1)}+y_i^{(2)}+\ldots+y_i^{(2^s-1)}-$$
$$-y_i^{(2^{s-1}+1)}-\ldots-y_i^{(2^s)}\}=0, \qquad (2,3,21)$$

причем нам придется рассматривать сумму чисел решений этого уравнения в 2^s различных предположениях, а именно:

$$\left.\begin{array}{l} 1)\ y_1^{(j)}\in A_1,\ y_2^{(j)}\in A_2,\ldots,\ y_k^{(j)}\in A_k,\\ 2)\ y_1^{(j)}\in A_{k+1},\ y_2^{(j)}\in A_{k+2},\ldots,\ y_k^{(j)}\in A_{2k},\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ 2^s)\ y_1^{(j)}\in A_{k2^s-k+1},\ldots,\ y_k^{(j)}\in A_{k2^s}\end{array}\right\}(1\leqslant j\leqslant 2^s).$$

Если мы положим

$$y^{(j)}=y_1^{(j)}+y_2^{(j)}+\ldots+y_k^{(j)} \qquad (1\leqslant j\leqslant 2^s),$$

то уравнение (2, 3, 21) примет простой вид

$$y^{(1)}+y^{(2)}+\ldots+y^{(2^s-1)}-$$
$$-y^{(2^{s-1}+1)}-\ldots-y^{(2^s)}=0. \qquad (2,3,22)$$

При этом речь идет о сумме чисел решений уравнения (2, 3, 22) в следующих 2^s предположениях, отличаемых друг

от друга значениями параметра m $(0 \leqslant m \leqslant 2^s - 1)$:

$$y^{(j)} = y_1^{(j)} + y_2^{(j)} + \ldots + y_k^{(j)},$$

где

$$y_1^{(j)} \in A_{mk+1},\ y_2^{(j)} \in A_{mk+2}, \ldots,\ y_k^{(j)} \in A_{(m+1)k}$$
$$(j = 1, 2, \ldots, 2^s).$$

Таким образом, мы можем формулировать окончательный результат нашего вывода в виде следующего предложения.

Лемма 7. *Ч. Р. У.*

$$x_1 + x_2 + \ldots + x_l = c \qquad (x_i \in A_i,\ 1 \leqslant i \leqslant l)$$

не превосходит суммы Ч. Р. У.

$$y^{(1)} + y^{(2)} + \ldots + y^{(2^{s-1})} - y^{(2^{s-1}+1)} - \ldots - y^{(2^s)} = 0.$$

$$\left.\begin{array}{l} y^{(j)} = y_1^{(j)} + y_2^{(j)} + \ldots + y_k^{(j)}, \\ y_1^{(j)} \in A_{mk+1},\ y_2^{(j)} \in A_{mk+2}, \ldots,\ y_k^{(j)} \in A_{(m+1)k} \end{array}\right\} (j = 1, 2, \ldots, 2^s)$$

в предположениях $m = 0, 1, \ldots, 2^s - 1$. *При этом* $l = k\,2^s$.

Мы видим, что лемма 5 есть частный случай леммы 7 при $k = s = 1$, $l = 2$.

§ 4. Доказательство основной леммы

Переходим к доказательству основной леммы 1. Мы будем доказывать ее по индукции, переходя от $n - 1$ к n. Для успешного осуществления такого перехода вместо исходного уравнения проблемы Варинга

$$x_1^n + x_2^n + \ldots + x_k^n = m \quad (m \leqslant N),$$

где $x_i \geqslant 0$, так что $x_i \leqslant m^{\frac{1}{n}} \leqslant N^{\frac{1}{n}}$ $(i \leqslant k)$, мы будем рассматривать уравнение

$$f(x_1) + f(x_2) + \ldots + f(x_k) = m \ (m \leqslant N), \qquad (2, 4, 1)$$

где $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$ — полином, который может зависеть от n и N так, что

$$|a_i| = B_n N^{\frac{i}{n}} (0 \leqslant i \leqslant n); \qquad a_0 \neq 0. \qquad (2, 4, 2)$$

Частным случаем такого полинома будет $f(x)=x^n$.

Основная лемма 1 будет следствием такой более общей леммы.

Лемма 8. *При* $|x_i|\leqslant N^{\frac{1}{n}}$ *и надлежаще выбранном* $k=k(n)$ *Ч. Р. У.* (2,4,1) *не превосходит*

$$B_n N^{\frac{k}{n}-1}. \tag{2,4,3}$$

Установим верность этого результата при $n=1$; $f(x)=a_0x+a_1$. Положим $k(1)=2$, так что уравнение (2,4,1) примет вид

$$a_0(x_1+x_2)=m-2a_1,\quad |x_i|\leqslant N\ (i=1,2). \tag{2,4,4}$$

Для каждого x_i возможно не более $2N+1\leqslant 3N$ значений, и по x_1 находим не более одного x_2, так что Ч. Р. У. (2,4,3) не превосходит $3N$, чем наша лемма доказывается при $n=1$. Пусть теперь $n>1$ и наша лемма верна для значения $n-1$. Положим $k(n-1)=k'$:

$$k=k(n)=2n\,2^{s+1},\qquad s=[4\lg_2 k']-1. \tag{2,4,5}$$

К уравнению (2,4,1) применим лемму 6. Положим

$$x=\sum_{i=1}^{\frac{k}{2}} f(x_i),\qquad y=\sum_{i=\frac{k}{2}+1}^{k} f(x_i). \tag{2,4,6}$$

В силу леммы 6 $r_k(m)$ не превосходит Ч. Р. У. $x-y=0$, где x, y задаются формулами (2,4,6); $|x_i|\leqslant N^{\frac{1}{n}}$; $|y_i|\leqslant N^{\frac{1}{n}}\left(1\leqslant l\leqslant\frac{k}{2}\right)$, т. е. Ч. Р. У.

$$\sum_{i=1}^{\frac{k}{2}}\{f(x_i)-f(y_i)\}=0 \tag{2,4,7}$$

при указанных ранее ограничениях $|x_i|$, $|y_i|$.

В уравнении (2,4,7) сделаем замену переменных: положим $x_i=y_i+h_i$ и будем рассматривать системы чисел (y_i, h_i)

$\left(l \leqslant \frac{k}{2}\right)$, причем y_l, h_l могут принимать любые значения в сегменте $[-2N^{\frac{1}{n}}, 2N^{\frac{1}{n}}]$, от чего Ч. Р. У. (2, 4,7) может только увеличиться. Каждое слагаемое в (2, 4,7) преобразуется в виде

$$f(y_l+h_l)-f(y_l)=\sum_{v=0}^{n} a_v\{(y_l+h_l)^{n-v}-y_l^{n-v}\}=$$

$$=\sum_{v=0}^{n} a_v \sum_{t=1}^{n-v} C_{n-v}^{t} h_l^t y_l^{n-v-t}.$$

Введем новую переменную, полагая

$$v+t=u,$$

так что

$$n-v-t=n-u; \qquad t=u-v.$$

После элементарных преобразований получим

$$f(y_l+h_l)-f(y_l)=h_l\varphi_l(y_l),$$

где

$$\varphi_l(y)=\sum_{u=1}^{n} a_{l,u} y^{n-u},$$

есть полином степени $(n-1)$ с коэффициентами

$$a_{l,u}=\sum_{v=0}^{n-1} a_v C_{n-v}^{u-v} h_l^{n-v-1} \qquad \left(l \leqslant \frac{k}{2}\right).$$

Мы видим, что эти коэффициенты зависят от чисел h_l. Уравнение (2, 4,7) в новых переменных (y_l, h_l) $\left(l \leqslant \frac{k}{2}\right)$ получит вид

$$h_1\varphi_1(y_1)+h_2\varphi_2(y_2)+\ldots+h_{\frac{k}{2}}\varphi_{\frac{k}{2}}(y_{\frac{k}{2}})=0. \quad (2,4,8)$$

Здесь y_l, $h_l \in [-2N^{\frac{1}{n}}, 2N^{\frac{1}{n}}]$ и коэффициенты $\varphi_l(y_l)$ зависят от чисел h_l.

Итак, $r_k(m)$ не превосходит совокупного Ч. Р. У. (2, 4,8) при указанных ограничениях на $|y_l|$, $|h_l|$.

§ 5. Дальнейшие оценки $r_k(m)$

Исследование $r_k(m)$ сведено нами на оценку Ч. Р. У. (2, 4,8). Мы будем считать $h_1, \ldots, h_{\frac{k}{2}}$ фиксированными и оценивать при этих условиях Ч. Р. У. (2, 4,8). Здесь будем применять лемму 7, где роль x_i будут играть числа $h_i \varphi_i(y_l)$, а роль числа l — число $\frac{k}{2} = 2n\,2^s$; $k_0 = 2n$.

Множества A_i состоят из чисел $x_i = h_i \varphi_i(y_l)$, где h_i заданы и $|y_i| \leqslant 2N^{\frac{1}{n}}$.

Го лемме 7, при указанных условиях Ч. Р. У. (2, 4,8) не превосходит суммы Ч. Р. У.

$$y^{(1)} + y^{(2)} + \ldots + y^{(2^{s-1})} - y^{(2^{s-1}+1)} - \ldots - y^{(2^s)} = 0 \quad (2, 5,1)$$

при 2^s возможных условиях, отвечающих значениям параметра $\mu = 0, 1, \ldots, 2^s - 1$:

$$y^{(j)} = y_1^{(j)} + \ldots + y_{k_0}^{(j)} \qquad (1 \leqslant j \leqslant 2^s),$$
$$y_i^{(j)} \in A_{\mu k_0 + i} \qquad (1 \leqslant i \leqslant k_0).$$

Для случая, например, $\mu = 0$ уравнение (2, 5,1) будет выглядеть так:

$$\{y_1^{(1)} + y_2^{(1)} + \ldots + y_{k_0}^{(1)}\} + \{y_1^{(2)} + y_2^{(2)} + \ldots + y_{k_0}^{(2)}\} + \ldots$$
$$\ldots + \left\{y_1^{(2^{s-1})} + y_2^{(2^{s-1})} + \ldots + y_{k_0}^{(2^{s-1})}\right\} -$$
$$- \left\{y_1^{(2^{s-1}+1)} + y_2^{(2^{s-1}+1)} + \ldots + y_{k_0}^{(2^{s-1}+1)}\right\} - \ldots$$
$$\ldots - \left\{y_1^{(2^s)} + y_2^{(2^s)} + \ldots + y_{k_0}^{(2^s)}\right\} = 0,$$

или, меняя порядок слагаемых,

$$\left\{y_1^{(1)} + y_1^{(2)} + \ldots + y_1^{(2^{s-1})} - y_1^{(2^{s-1}+1)} - \ldots - y_1^{(2^s)}\right\} +$$
$$+ \left\{y_2^{(1)} + y_2^{(2)} + \ldots + y_2^{(2^{s-1})} - y_2^{(2^{s-1}+1)} - \ldots - y_2^{(2^s)}\right\} + \ldots$$
$$\ldots + \left\{y_{k_0}^{(1)} + y_{k_0}^{(2)} + \ldots + y_{k_0}^{(2^{s-1})} - y_{k_0}^{(2^{s-1}+1)} - \ldots - y_{k_0}^{(2^s)}\right\} = 0;$$

каждое из чисел $y_i^{(j)}$ есть здесь число вида $h_i\varphi_i(v_i^{(j)})$, где $|v_i^{(j)}| \leqslant 2N^{\frac{1}{n}}$; поэтому последнее уравнение может быть переписано в виде

$$h_1\left\{\varphi_1(v_1^{(1)})+\varphi_1(v_1^{(2)})+\ldots+\varphi_1(v_1^{(2^{s-1})})-\right.$$
$$-\varphi_1(v_1^{(2^{s-1}+1)})-\ldots-\left.\varphi_1(v_1^{(2^s)})\right\}+$$
$$+h_2\left\{\varphi_2(v_2^{(1)})+\ldots-\varphi_2(v_2^{(2^s)})\right\}+\ldots$$
$$\ldots+h_{k_0}\left\{\varphi_{k_0}(v_{k_0}^{(1)})+\ldots-\varphi_{k_0}(v_{k_0}^{(2^s)})\right\}=0.$$

Полагая для краткости

$$\varphi_i(v_i^{(1)})+\varphi_i(v_i^{(2)})+\ldots+\varphi_i(v_i^{(2^{s-1})})-\varphi_i(v_i^{(2^{s-1}+1)})-\ldots$$
$$\ldots-\varphi_i(v_i^{(2^s)})=z_i \qquad (1\leqslant i\leqslant k_0),$$

мы можем переписать это уравнение

$$h_1z_1+h_2z_2+\ldots+h_{k_0}z_{k_0}=0. \qquad (2,5,2)$$

Уравнений такого типа мы всего будем иметь 2^s, и совокупность их можно записать в виде

$$\sum_{i=1}^{k_0}h_{mk_0+i}z_{mk_0+i}=0 \qquad (0\leqslant m\leqslant 2^s-1). \qquad (2,5,3)$$

Мы будем рассматривать лишь уравнение (2, 5,2), остальные уравнения ведут себя аналогично. Как было определено ранее,

$$\varphi_i(y)=\sum_{u=1}^{n}a_{i,u}y^{n-u},$$

где

$$a_{i,u}=\sum_{v=0}^{n-1}a_vC_{n-v}^{u-v}h_i^{u-v-i} \qquad \left(i\leqslant\frac{k}{2}\right).$$

Так как было предположено, что $|a_v| \leqslant B_n N^{\frac{v}{n}}$ и $|h_l| \leqslant 2N^{\frac{1}{n}}$, то имеем

$$|a_{i,u}| = B_n \sum_{v=0}^{n-1} N^{\frac{v}{n}} C_{n-v}^{u-v} N^{\frac{u-v-1}{n}} = B_n N^{\frac{u-1}{n}} \sum_{v=0}^{n-1} C_{n-v}^{u-v},$$

т. е. ввиду $u \leqslant n$

$$|a_{i,u}| = B_n N^{\frac{u-1}{n}}. \qquad (2,5,4)$$

Далее, так как $|v_i^{(j)}| \leqslant 2N^{\frac{1}{n}}$, имеем $|v_i^{(j)}|^{n-u} = B_n N^{\frac{n-u}{n}}$, в силу чего

$$|a_{i,u}|\,|v_i^{(j)}|^{n-u} = B_n N^{\frac{u-1}{n}} N^{\frac{n-u}{n}} = B_n N^{\frac{n-1}{n}},$$

откуда

$$|\varphi_i(v_j^{(j)})| = B_n N^{\frac{n-1}{n}} \quad (i \leqslant k_0 2^s;\ j \leqslant 2^s)$$

и

$$|z_i| \leqslant B_n N^{\frac{n-1}{n}} \quad (i \leqslant k_0 2^s). \qquad (2,5,5)$$

Таким образом, в уравнении (2, 5, 3,) каждое значение z_i может принимать только значения, ограниченные (2,5,5). При этом z_i может иметь повторения. Оценим число таких повторений, т. е. Ч. Р. У. $z_i = z$, где z — число под условиями (2, 5, 5). Имеем уравнение

$$\varphi_i(v_i^{(1)}) + \ldots + \varphi_i(v_i^{(2^{s-1})}) - \varphi_i(v_i^{(2^{s-1}+1)}) - \ldots$$
$$\ldots - \varphi_i(v_i^{(2^s)}) = z. \qquad (2,5,6)$$

Для этого применим математическую индукцию, подготовленную нами ранее.

Перепишем уравнение в виде

$$\varphi_i(v_i^{(1)}) + \varphi_i(v_i^{(2)}) + \ldots + \varphi_i(v_i^{(k')}) = z - \varphi_i(v_i^{(k'+1)}) - \ldots$$
$$\ldots + \varphi_i(v_i^{(2^{s-1}+1)}) + \ldots + \varphi_i(v_i^{(2^s)}), \quad (2,5,7)$$

что можно сделать, так как $k'=k(n-1)>1$, $k(1)=2$ и имеем $2^{s-1}>k'$, как нетрудно подсчитать.

Правую часть уравнений (2, 5, 7) обозначим через m', так что

$$\varphi_i(v_i^{(1)})+\ldots+\varphi_i(v_i^{(k')})=m'. \qquad (2,5,8)$$

Для аргументов в правой части (2, 5, 7), т. е. чисел

$$v_i^{(j)} \qquad (k'+1\leqslant j\leqslant 2^s),$$

выберем какие-либо значения в допустимом для них сегменте значений $[-2N^{\frac{1}{n}}, 2N^{\frac{1}{n}}]$; тогда и m' примет определенное значение. К уравнению (2, 5, 8) применим ранее нами высказанное предположение математической индукции. Имеем:

$$\varphi_i(y)=\sum_{u=1}^{n} a_{i,u}y^{n-u} \text{ — полином степени } n-1;$$

$$|a_{i,u}|=B_nN^{\frac{u-1}{n}}=B_n\left(N^{\frac{n-1}{n}}\right)^{\frac{u-1}{n-1}}, \qquad (2,5,9)$$

$|m'|=B_nN^{\frac{n-1}{n}}$. В силу последнего неравенства роль N может теперь играть число $c_nN^{\frac{n-1}{n}}$ ($c_n>0$ — константа), и нужные условия соблюдены. Ввиду этого мы можем утверждать, что Ч. Р. У. (2, 5, 8) при $|v_i^{(j)}|\leqslant 2N^{\frac{1}{n}}=2\left(N^{\frac{n-1}{n}}\right)^{\frac{1}{n-1}}$ имеет оценку:

$$B_n\left(N^{\frac{n-1}{n}}\right)^{\frac{k'}{n-1}-1}=B_nN^{\frac{k'-n+1}{n}}. \qquad (2,5,10)$$

При этом $v_i^{(j)}$ были фиксированы при $k'+1\leqslant j\leqslant 2^s$. Число значений этих чисел не превосходит

$$(2N^{\frac{1}{n}}+1)^{2^s-k'}=B_nN^{\frac{2^s-k'}{n}}. \qquad (2,5,11)$$

Общее Ч. Р. У. (2, 5, 7) имеет оценку, полученную перемножением (2, 5, 11) и (2, 5, 10), что дает

$$B_nN^{\frac{2^s-n+1}{n}}. \qquad (2,5,12)$$

Таким образом, в уравнении (2, 5, 2) кратность каждого z_i не превосходит (2, 5, 12).

Дальнейшее сводится к подсчету Ч. Р. У. линейных уравнений вида (2, 5, 2), причем z_i имеют кратность, не превышающую (2, 5, 12). При этом числа h_i фиксированы; мы должны перебрать все возможности для них. Мы пришли к результату: $r_k(m)$ не превосходит суммы чисел решений в целых z_i, $|z_i| \leqslant B_n N^{\frac{n-1}{n}}$ с кратностями $\lambda_i \leqslant c(n) N^{\frac{2^s - n + 1}{n}}$ уравнений вида

$$\sum_{l=1}^{k_0} h_{\mu k_0 + i} z_{\mu k_0 + i} = 0, \qquad (2,5,13)$$

где μ пробегает значения $0, 1, \ldots, 2^s - 1$, а числа h_r $(1 \leqslant r \leqslant 2^s k_0)$ независимо друг от друга пробегают все целые числа отрезка $\left(-2N^{\frac{1}{n}}, +2N^{\frac{1}{n}}\right)$.

§ 6. Окончание доказательства

Остается оценить совокупное Ч. Р. У. (2, 5, 13). Сначала фиксируем числа h_i.

Обозначим через Γ какую-нибудь определенную систему чисел $h_i \left(|h_i| \leqslant 2N^{\frac{1}{n}}, 1 \leqslant i \leqslant \frac{k}{2}\right)$ и через $U_\mu(\Gamma)$ — число решений уравнения (2, 5, 13) при этой фиксированной системе Γ и при некотором данном μ, причем имеются в виду решения z_i, удовлетворяющие неравенствам $|z_i| \leqslant B_n N^{\frac{n-1}{n}}$ и каждое z_i считается с кратностью $\lambda_i \leqslant B_n N^{\frac{2^s - n + 1}{n}}$. В силу выведенного в § 5 имеем

$$r_k(m) \leqslant \sum_{\Gamma} \left(\sum_{\mu=0}^{2^s - 1} U_\mu(\Gamma) \right),$$

где суммирование по Γ идет по всем допустимым системам чисел h_i. Следовательно,

$$r_k(m) \leqslant \sum_{\mu=0}^{2^s - 1} \left(\sum_{\Gamma} U_\mu(\Gamma) \right).$$

При различных значениях μ уравнения вида (2,5,13) ничем не отличаются одно от другого; соответствующие ограничения на величины решений также совпадают. Ввиду этого мы можем остановиться на уравнении, отвечающем $\mu = 0$, и на системе чисел $U_0(\Gamma)$. Получим

$$r_k(m) \leqslant 2^s \sum_{\Gamma} U_0(\Gamma) = B_n \sum_{\Gamma} U_0(\Gamma),$$

где $U_0(\Gamma)$ есть Ч. Р. У.

$$h_1 z_1 + h_2 z_2 + \ldots + h_{k0} z_{k0} = 0 \qquad (2,6,1)$$

при данной системе Γ чисел $h_i \left(|h_i| \leqslant 2N^{\frac{1}{n}};\ i \leqslant \frac{k}{2} \right)$. Здесь $|z_i| \leqslant$ $\leqslant B_n N^{\frac{n-1}{n}}$ и z_i имеет кратность $\lambda_i \leqslant B_n N^{\frac{2^s-n+1}{n}}$. Пусть $U_0^*(\Gamma)$ есть Ч. Р. У. (2,6,1) в предположении, что каждое значение z_i считается один раз; очевидно,

$$U_0(\Gamma) \leqslant \left(B_n N^{\frac{2^s-n+1}{n}} \right)^{k_0} U_0^*(\Gamma)$$

или, так как $k_0 = 2n$,

$$U_0(\Gamma) = B_n N^{2(2^s-n+1)}\, U_0^*(\Gamma),$$
$$r_k(m) = B_n N^{2(2^s-n+1)} \sum_{\Gamma} U_0^*(\Gamma). \qquad (2,6,2)$$

Обратимся к системам чисел Γ. Каждое Γ представляет собой некоторую допустимую систему значений всех $h_i \left(1 \leqslant i \leqslant \frac{k}{2} \right)$; между тем число $U_0^*(\Gamma)$ полностью определяется значениями первых $k_0 = 2n$ из этих чисел ($1 \leqslant i \leqslant 2n$), ибо только они входят в уравнение (2, 6, 1). Выбрав некоторую определенную систему Γ, мы тем самым однозначно определяем и некоторую систему Γ' значений чисел $h_1, h_2, \ldots, h_{2n}$. Но если, обратно, выбрана определенная система Γ' чисел $h_1, h_2, \ldots, h_{2n}$, то ей соответствует не одна система Γ, а столько, сколькими способами можно «довыбрать» остальные $h_i \left(2n < i \leqslant \frac{k}{2} \right)$; так как каждое h_i должно принадлежать отрезку $\left(-2N^{\frac{1}{n}}, +2N^{\frac{1}{n}} \right)$, то очевидно, что одной системе Γ' соответствует

не более чем

$$c(n)\left(N^{\frac{1}{n}}\right)^{\frac{k}{2}-2n} = c(n)\,N^{\frac{k}{2n}-2}$$

систем Г. Поэтому

$$\sum_{\Gamma} U_0^*(\Gamma) \leqslant c(n)\,N^{\frac{k}{2n}-2} \sum_{\Gamma'} U_0^*(\Gamma').$$

Здесь $U_0^*(\Gamma)$ есть число решений в целых z_i, $|z_i| \leqslant B_n N^{\frac{n-1}{n}}$ $(1 \leqslant i \leqslant 2n)$, уравнения (2, 6, 1) при данной системе Γ' чисел h_i, $|h_i| \leqslant 2N^{\frac{1}{n}}$ $(1 \leqslant i \leqslant 2n)$, и суммирование производится по всем таким системам. Из (2, 6, 2) мы получаем поэтому

$$r_k(m) = B_n N^{2(2^s-n+1)}\, N^{\frac{k}{2n}-2} \sum_{\Gamma'} U_0^*(\Gamma') = \\ = B_n N^{2(2^{s+1}-n)} \sum_{\Gamma'} U_0^*(\Gamma'). \qquad (2,6,3)$$

Далее применим лемму 4 (условия применимости ее выполнены). Из нее находим

$$\sum_{\Gamma'} U_0^*(\Gamma') = B_n (AB)^{2n-1} = B_n N^{2n-1}.$$

После этого оценка (2, 6, 3) дает нам

$$r_k(m) = B_n N^{2(2^{s+1}-n)}\, N^{2n-1} = B_n N^{2\cdot 2^{s+1}-1} = B_n N^{\frac{k}{n}-1},$$

что заканчивает доказательство основной леммы 1 и приводит нас к цели.

§ 7. Постановка проблемы Гильберта — Камке

Как было сказано в § 1, проблема состоит в изучении системы диофантовых уравнений

$$\left.\begin{aligned} x_1^n + x_2^n + \ldots + x_S^n &= N_n, \\ x_1^{n-1} + x_2^{n-1} + \ldots + x_S^{n-1} &= N_{n-1}, \\ \cdots\cdots\cdots\cdots\cdots\cdots & \\ x_1 + x_2 + \ldots + x_S &= N_1. \end{aligned}\right\} \qquad (2,7,1)$$

Здесь числа $x_i \geqslant 0$; правые части $N_1, N_2, \ldots, N_n$ должны быть большими числами различных порядков роста в соответствии с левыми частями. Мы предположим, что существуют системы

реальных чисел $l_1>1,\ldots,l_{n-1}>1$; $i_1<1,\ldots,i_{n-1}<1$ таких, что

$$l_k N_n^{\frac{k}{n}} \leqslant N_k \leqslant i_k s^{1-\frac{k}{n}} N_n^{\frac{k}{n}} \qquad (k=1,2,\ldots,n-1). \qquad (2,7,2)$$

Как показал К. К. Марджанишвили [19], для разрешимости системы (2, 7, 1) необходимо выполнение условий:

$$\begin{vmatrix} N_n & (n-1)^n & \ldots & 1^n \\ N_{n-1} & (n-1)^{n-1} & \ldots & 1^{n-1} \\ \cdot & \cdot & \cdot & \cdot \\ N_1 & n-1 & \ldots & 1 \end{vmatrix} \equiv 0 \pmod R;\ldots;$$

$$\begin{vmatrix} n^n & (n-1)^n & \ldots & N_n \\ n^{n-1} & (n-1)^{n-1} & \ldots & N_{n-1} \\ \cdot & \cdot & \cdot & \cdot \\ n & n-1 & \ldots & N_1 \end{vmatrix} \equiv 0 \pmod R, \qquad (2,7,3)$$

где

$$R=\begin{vmatrix} n^n & (n-1)^n & \ldots & 1^n \\ n^{n-1} & (n-1)^{n-1} & \ldots & 1^{n-1} \\ n & n-1 & \ldots & 1 \end{vmatrix}.$$

Докажем это утверждение.

Пусть имеют место равенства (2, 7, 1). Обозначим через D_n первый из детерминантов, входящих в левую часть (2, 7, 3). Применяя простейшие правила счета с детерминантами, находим последовательно

$$D_n=\begin{vmatrix} \sum x_\nu^n & (n-1)^n & \ldots & 1^n \\ \cdot & \cdot & \cdot & \cdot \\ \sum x_\nu & (n-1) & \ldots & 1 \end{vmatrix}=$$

$$=(n-1)!\begin{vmatrix} \sum x_\nu^n & (n-1)^{n-1} & \ldots & 1 \\ \cdot & \cdot & \cdot & \cdot \\ \sum x_\nu & 1 & \ldots & 1 \end{vmatrix}=(n-1)!\times$$

$$\times(n-2)!\begin{vmatrix} \sum x_\nu^{n-1}(x_\nu-1) & (n-1)^{n-2} & \ldots & 2^{n-2} \\ \cdot & \cdot & \cdot & \cdot \\ \sum x_\nu(x_\nu-1) & 1 & \ldots & 1 \end{vmatrix}=(n-1)!\times$$

$$\times(n-2)!(n-3)!\begin{vmatrix} \sum x_\nu^{n-2}(x_\nu-1)(x_\nu-2) & (n-1)^{n-3} & \ldots & 3^{n-3} \\ \cdot & \cdot & \cdot & \cdot \\ \sum x_\nu(x_\nu-1)(x_\nu-2) & 1 & \ldots & 1 \end{vmatrix}=$$

$$=\ldots=(n-1)!(n-2)!\ldots 2!\,1!\sum x_\nu(x_\nu-1)\ldots(x_\nu-n+1)\equiv$$

$$\equiv 0 \pmod R.$$

Мы будем доказывать теорему: *для достаточно большого* $S=S(n)$ *и набора чисел* $N_1, N_2, \ldots, N_n$, *удовлетворяющих условиям* (2, 7, 2) *и* (2, 7, 3), *система уравнений* (2, 7, 1) *разрешима*. Элементарное решение этой проблемы по аналогии с изложенным ранее решением проблемы Варинга построено Г. В. Емельяновым [8] в 1948 г. Здесь мы будем следовать его изложению.

§ 8. Последовательности целочисленных векторов и их плотности

Имея в виду элементарное построение решения проблемы Гильберта — Камке, мы должны перенести изложенные выше идеи плотности и сложение последовательностей целых чисел на целочисленные векторы.

В дальнейшем мы будем пользоваться следующими обозначениями: $\bar{m}, \bar{A}, \bar{B}, \ldots, \bar{T}, \bar{Z}$ — векторы с целочисленными неотрицательными координатами пространства E^n;

$\{\bar{A}\}, \{\bar{T}\}, \{\bar{m}\}$ — какие-либо множества целочисленных векторов E^n;

$\{\bar{N}\}$ — совокупность всех целочисленных векторов E^n;

$\{\bar{M}\}$ — совокупность целочисленных векторов E^n, координаты $M_1, M_2, \ldots, M_n$ которых удовлетворяют условиям (2, 7, 2) и (2, 7, 3). Если вектор $\bar{a}$ принадлежит к множеству $\{\bar{A}\}$, будем писать, как обычно, $\bar{a} \in \{\bar{A}\}$. Если все координаты двух векторов $\bar{a}$ и $\bar{b}$, т. е. a_k и b_k $(k=1, 2, \ldots, n)$, связаны соотношениями $a_k \leqslant b_k$ $(k=1, 2, \ldots, n)$, то будем писать: $\bar{a} \subseteq \bar{b}$ ($\bar{a}$ «не превосходит» $\bar{b}$). Сложение последовательностей целочисленных векторов определяется аналогично сложению числовых последовательностей в смысле Л. Г. Шнирельмана: $\{\bar{A}\}+\{\bar{B}\}=\{\bar{c}\}$, где $\{\bar{c}\}$ — совокупность векторов $\bar{c}$ вида $\bar{c}=\varepsilon_1\bar{a}+\varepsilon_2\bar{b}$; $\bar{a} \in \{\bar{A}\}$; $\bar{b} \in \{\bar{B}\}$;

$$\varepsilon_1=0;\ 1;\ \varepsilon_2=0;\ 1;\ \varepsilon_1+\varepsilon_2 \neq 0.$$

Сложение векторов понимается в обычном смысле. Сравнимость векторов по скалярному модулю $\bar{a} \equiv \bar{b} \pmod{q}$ означает: $a_k \equiv b_k \pmod{q}$ $(k=1, 2, \ldots, n)$.

Если $\overline{a}=\begin{pmatrix} a_n \\ a_{n-1} \\ \vdots \\ a_1 \end{pmatrix}$, то $(+)\,\overline{a}$ означает вектор $\begin{pmatrix} |a_n| \\ |a_{n-1}| \\ \vdots \\ |a_1| \end{pmatrix}$.

Плотность последовательности целочисленных векторов E^n определяется аналогично тому, как это делается для числовых последовательностей Л. Г. Шнирельманом:

$$D\{\overline{A}\}=\inf\frac{r_{\overline{m}}\{\overline{A}\}}{r_{\overline{m}}\{\overline{N}\}},$$

где $\overline{m}$ пробегает все $\{\overline{N}\}$, $r_{\overline{m}}\{\overline{A}\}$ — число векторов $\{\overline{A}\}$, не превосходящих $\overline{m}$, $r_{\overline{m}}\{\overline{N}\}$ — число векторов $\{\overline{N}\}$, не превосходящих $\overline{m}$; $\{\overline{A}\}$ называется базисом $\{\overline{N}\}$ порядка l, если каждый вектор $\overline{m}\in\{\overline{N}\}$ может быть представлен в виде

$$\overline{m}=\overline{a}_1+\overline{a}_2+\ldots+\overline{a}_k,$$

где $\overline{a}_i\in\{\overline{A}\}$ $(i=1, 2, \ldots, k;\ k\leqslant l)$.

§ 9. Несколько лемм

Здесь мы докажем несколько лемм, вполне аналогичных тем, которые были изложены в §§ 3 и 4.

Лемма 1. *Пусть* $F_1=\{\overline{P}_i\}$, $F_2=\{\overline{Q}_j\}$ — *две конечные системы целочисленных векторов* E^n *и каждый* $\overline{P}_j\in F_1$ *считается* $a_j\geqslant 1$ *раз, каждый вектор* $Q_j\in F_2$ — *соответственно* b_j *раз. Тогда Ч. Р. У.*

$$P_l+Q_j=Z, \tag{2,9,1}$$

где $\overline{Z}$ — *любой фиксированный целочисленный вектор не превосходит половины суммы Ч. Р. У.,*

$$\overline{P}_l-\overline{P}_j=\overline{O}\ \text{ и }\ \overline{Q}_l-\overline{Q}_j=\overline{O}, \tag{2,9,2}$$

где $\overline{O}=\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ — *нулевой вектор, который мы в дальнейшем будем обозначать просто «*O*».*

Действительно, уравнение (2,9,1) сопоставляет каждому l определенное j, т. е. каждому из a_l равных векторов $\overline{P}_l$ лю-

бой из b_j равных $\overline{Q}_j$, что дает

$$a_i b_j \leqslant \frac{a_i^2 + b_j^2}{2},$$

а так как при $i_1 \neq i_2$ вектор $\overline{P}_{i_1} \neq \overline{P}_{i_2}$, то не равны соответствующие им в силу уравнения (2,9,1) векторы $\overline{Q}_{j_1}$ и $\overline{Q}_{j_2}$ и следовательно, Ч. Р. У. $(2,9,1) \leqslant \frac{1}{2}\left(\sum a_i^2 + \sum b_j^2\right)$, где $\sum a_i^2 + \sum b_j^2$ — сумма Ч. Р. У. (2,9,2).

Лемма 2. *Пусть дано $2^s k_0$ конечных систем векторов $G_i = \{\overline{M}_{ij}\}$ $(i = 1,2,\ldots,2^s k_0)$, причем каждый вектор $\overline{M}_{ij} \in G_i$ считается $a_{ij} \geqslant 1$ раз.*

Рассмотрим Ч. Р. У.

$$\left.\begin{aligned} &\overline{M}_1 + \overline{M}_2 + \ldots + \overline{M}_{2^s k_0} = \overline{Z}; \\ &\overline{M}_i \in G_i \qquad (i = 1, 2, \ldots, 2^s k_0. \end{aligned}\right\} \tag{2,9,3}$$

Введем 2^s систем целочисленных векторов $\{\overline{Y}\}$ вида

$$\overline{Y}_j = \overline{M}_{(j-1)k_0+1} + \overline{M}_{(j-1)k_0+2} + \ldots + \overline{M}_{(j-1)k_0+k_0} \tag{2,9,4}$$
$$(j = 1, 2, \ldots, 2^s).$$

Тогда Ч. Р. У. (2,9,3) *не превосходит суммы чисел решений независимых уравнений*

$$\left.\begin{aligned} &\overline{Y}_1^{(1)} + \overline{Y}_1^{(2)} + \ldots + \overline{Y}_1^{(2^{s-1})} - \overline{Y}_1^{(2^{s-1}+1)} - \ldots - \overline{Y}_1^{(2^s)} = 0, \\ &\overline{Y}_2^{(1)} + \overline{Y}_2^{(2)} + \ldots + \overline{Y}_2^{(2^{s-1})} - \overline{Y}_1^{(2^{s-1}+1)} - \ldots - \overline{Y}_2^{(2^s)} = 0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &\overline{Y}_{2^s}^{(1)} + \overline{Y}_{2^s}^{(2)} + \ldots + \overline{Y}_{2^s}^{(2^{s-1})} - \overline{Y}_{2^s}^{(2^{s-1}+1)} - \ldots - Y_{2^s}^{(2^s)} = 0, \end{aligned}\right\} \tag{2,9,5}$$

где все переменные j-й строки пробегают независимо значения (2, 9, 4) *с соответствующим числом повторений.*

Действительно, рассматривая две системы векторов

$$\left\{\overline{M}_1 + \overline{M}_2 + \ldots + \overline{M}_{2^{s-1}k_0}\right\} \text{ и } \left\{\overline{M}_{2^{s-1}k_0+1} + \ldots + \overline{M}_{2^s k_0}\right\},$$

мы можем применить к (2, 9, 3) лемму 1 и получить два

уравнения

$$(\overline{M}_1 - \overline{M}_1') + (\overline{M}_2 - \overline{M}_2') + \ldots + (\overline{M}_2{}^{s-1}{}_{k_0} - \overline{M}_2'{}^{s-1}{}_{k_0}) = 0,$$

$$(\overline{M}_2{}^{s-1}{}_{k_0+1} - \overline{M}_2'{}^{s-1}{}_{k_0+1}) + \ldots + (\overline{M}_2{}^{s}{}_{k_0} - \overline{M}_2'{}^{s}{}_{k_0}) = 0.$$

К каждому из этих уравнений опять применяем лемму 1, и, таким образом, в s шагов мы получим утверждение леммы 2.

Лемма 3. *Ч. Р. У.*

$$h_1 \overline{z}_1 + h_2 \overline{z}_2 + \ldots + h_\nu \overline{z}_\nu = \overline{m}, \tag{2,9,6}$$

где $(+)\overline{z}_i \subseteq \overline{T}$, $|h_i| \leqslant p$, p — *некоторое фиксированное число,*

$$\overline{T} = \begin{pmatrix} T_n \\ T_{n-1} \\ \vdots \\ T_1 \end{pmatrix}, \quad T_l \geqslant 0, \quad p \leqslant T_l \ (l = 1, 2, \ldots, n), h_i \text{ фиксированы},$$

$(h_1, h_2, \ldots, h_\nu) = 1$, *не превосходит*

$$B_\nu \frac{(r_{\overline{T}}\{\overline{N}\})^{\nu-1}}{\max |h_i|^n}. \tag{2,9,7}$$

Для $\nu = 2$ имеем: $h_1\overline{z}_1 + h_2\overline{z}_2 = \overline{m}$, $|h_1| > |h_2|$, $(h_1, h_2) = 1$ и $h_2\overline{z}_2 \equiv \overline{m} \pmod{h_1}$. Вектор $\overline{z}_2$ определяется однозначно по модулю h_1 и поэтому может принимать не более $B\frac{r_{\overline{T}}\{\overline{N}\}}{|h_1|^n}$ значений. Каждому вектору $\overline{z}_2$ отвечают не более одного $\overline{z}_1$.

Пусть теперь лемма верна для $\nu - 1$ и пусть $\max|h_i| = |h_\nu|$ $(i = 1, 2, \ldots, \nu)$. Пусть $(h_1, h_2, \ldots, h_{\nu-1}) = \delta$ и

$$\max\left\{\frac{|h_1|}{\delta}, \frac{|h_2|}{\delta}, \ldots, \frac{|h_{\nu-1}|}{\delta}\right\} = H'.$$

Тогда Ч. Р. У. $h_1\overline{z}_1 + h_2\overline{z}_2 + \ldots + h_{\nu-1}\overline{z}_{\nu-1} = \delta\overline{Y}$ не превосходит $B\frac{(r_{\overline{T}}\{\overline{N}\})^{\nu-2}}{(H')^n}$, причем каждое значение $(+)\overline{Y} \subseteq \nu H'\overline{T}$. Далее, очевидно, $(\delta, h_\nu) = 1$ и Ч. Р. У.

$$\delta\overline{Y} + h_\nu z_\nu = \overline{m}$$

будет

$$B\frac{(r_{\overline{T}}\{\overline{N}\})^{\nu-2}}{(H')^n}\frac{r_{\nu H'\overline{T}}\{\overline{N}\}}{|h_\nu|^n} = B\frac{(r_{\overline{T}}\{\overline{N}\})^{\nu-1}}{|h_\nu|^n},$$

что и требовалось доказать.

Лемма 4. *Сумма Ч. Р. У.*

$$h_1z_1+h_2z_2+\ldots+h_\nu z_\nu=0, \qquad (2,9,8)$$

где $(+)\,z_i\subseteq\overline{T}$; h_i *пробегают независимо сегмент* $[-2p, 2p]$, *координаты вектора* $\overline{T}$, *т. е.* $T_k\leqslant Bp^k$, $T_k\geqslant 2p$, *будет не более*

$$B\frac{\left(r_{\overline{T}}\{\overline{N}\}\right)^{\nu-1}}{p^n}p^\nu \quad \text{для} \quad \nu=4n^2.$$

Для систем $\{h_1, h_2, \ldots, h_\nu\}$, содержащих не более двух $h_i\neq 0$, возьмем тривиальную оценку Ч.Р.У.(2, 9, 8): $B\left(r_{\overline{T}}\{\overline{N}\}\right)^{\nu-1}$, поэтому сумма чисел решений в этом случае будет не более

$$B\left(r_{\overline{T}}\{\overline{N}\}\right)^{\nu-1}p^2=\frac{B\left(r_{\overline{T}}\{N\}\right)^{\nu-1}}{p^n}p^\nu\frac{p^n}{p^{\nu-2}}=B\frac{\left(r_{\overline{T}}\{\overline{N}\}\right)^{\nu-1}}{p^n}p^\nu. \qquad (2,9,9)$$

Остающиеся системы $\{h_1, h_2, \ldots h_\nu\}$ разобьем на классы по их общему наибольшему делителю δ. Для тех систем, у которых $(h_1, h_2, \ldots, h_\nu)=1$, разделим сегмент $[1, 2p]$ на части $\left[\frac{2p}{2^{m+1}}, \frac{2p}{2^m}\right]$, число которых будет не более $B\ln p$.

Пусть $H=\max|h_i|$. Рассмотрим все системы, для которых $H\in\left[\frac{2p}{2^{m+1}}, \frac{2p}{2^m}\right]$. Сумма Ч. Р. У. (2, 9, 8) для всех таких уравнений в силу леммы 3 не превосходит

$$B\frac{\left(r_{\overline{T}}\{\overline{N}\}\right)^{\nu-1}}{H^n}\left(3\cdot\frac{2p}{2^m}\right)\left(\frac{2p}{2^m}\right)^{\nu-1}\leqslant B\frac{\left(r_{\overline{T}}\{\overline{N}\}\right)^{\nu-1}}{p^n}2^{mn}p^\nu 2^{-m\nu}=$$

$$=B_\nu\frac{\left(r_{\overline{T}}\{\overline{N}\}\right)^{\nu-1}}{p^n}p^\nu\frac{1}{2^{m(\nu-n)}}. \qquad (2,9,10)$$

Суммируя (2, 9, 10) по всем $m>0$, получим в этом случае: сумма Ч. Р. У. (2, 9, 8) не превосходит числа

$$B\frac{\left(r_{\overline{T}}\{\overline{N}\}\right)^{\nu-1}}{p^n}p^\nu. \qquad (2,9,11)$$

Рассматривая теперь системы с $(h_1, h_2, \ldots, h_\nu)=\delta$, заметим, что выражение для суммы чисел решений уравнения

(2,9,8) получится в этом случае заменой в (2,9,11) на $\frac{p}{\delta}$, в результате чего мы получим для фиксированного δ: сумма Ч. Р. У. (2,9,8) не превосходит числа

$$B\frac{\left(r_{\bar{T}}\{\bar{N}\}\right)^{\nu-1}}{p^n}\frac{p^\nu}{\delta^{\nu-n}}. \qquad (2,9,12)$$

Так как $\nu > n+2$, то при суммировании по всем значениям δ мы получим сходящийся ряд $\sum_\delta \frac{1}{\delta^{\nu-n}}$, т. е. константу, что и доказывает во всех случаях утверждение леммы.

Докажем теперь основную лемму.

Лемма 5. *Пусть вектор* $\bar{m}\in\{\bar{N}\}$, $\bar{m}\subseteq\bar{T}$, $\bar{T}\in\{\bar{N}\}$. *Рассмотрим множество векторов*

$$\bar{T}=\begin{pmatrix}T_n\\T_{n-1}\\\vdots\\T_1\end{pmatrix};\quad \{\overline{F(x)}\}=\left\{\begin{pmatrix}f_n(x)\\f_{n-1}(x)\\\vdots\\f_1(x)\end{pmatrix}\right\}, \qquad (2,9,13)$$

где $f_j(x)=a_{0j}x^j+a_{1j}x^{j-1}+\ldots+a_{jj}$ — *полином с целыми коэффициентами, причем* $a_{0j}\neq 0$ *и зависит только от* j; x *пробегает все целые числа*

$$a_{ij}=a_{ij}(j,\ T_j)(i>1),\ |a_{ij}|\leqslant B_n T_n^{\frac{1}{n}}=B_n p. \qquad (2,9,14)$$

Тогда существует $K=K(n)$ *такое, что Ч. Р. У.*

$$\overline{F(x_1)}+\overline{F(x_2)}+\ldots+\overline{F(x_k)}=\bar{m}, \qquad (2,9,15)$$

где $|x_i|\leqslant p$, *не превосходит числа*

$$B_n'\frac{p^K}{p^{n^2}}. \qquad (2,9,16)$$

§ 10. Доказательство основной леммы

Для $n=1$, т. е. для векторов пространства E^1, которые будут обыкновенными линейными полиномами $ax+b$, оно очевидно, причем $K(1)=1$.

Предположим, что утверждение леммы справедливо для всех векторов-полиномов пространства E^{n-1}, и обозначим соот-

ветствующее $K(n-1)=K'$. Положим теперь $K=2^{[4\log_2 K']}4n$ и рассмотрим уравнение

$$\overline{F(x_1)}+\overline{F(x_2)}+\ldots+\overline{F(x_K)}=\overline{m}, \qquad (2,10,1)$$

$$|x_i|\leqslant p=T_n^{\frac{1}{n}} \qquad (i=1,\ 2,\ldots,\ K);\ \overline{m}\in\{\overline{N}\}.$$

Применяя к (2, 10, 1) лемму 1, заменим уравнение (2,10,1) уравнением

$$\{\overline{F(x_1)}-\overline{F(y_1)}\}+\{\overline{F(x_2)}-\overline{F(y_2)}\}+\ldots+$$
$$+\{\overline{F(x_{\frac{K}{2}})}-\overline{F(y_{\frac{K}{2}})}\}=0, \qquad (2,10,2)$$

где x_i, y_i независимы и заключены в интервале $[-p,\ p]$. Положим $x_i=y_i+h_i$, где y_i и h_i независимо пробегают сегмент $[-2p,\ 2p]$, отчего число решений уравнения (2,10.2) только увеличится. Для каждой фиксированной системы значений $(h_1,\ h_2,\ldots,\ h_{\frac{K}{2}})$ мы получим уравнение

$$h_1\overline{\varphi_1(y_1)}+h_2\overline{\varphi_2(y_2)}+\ldots+h_{\frac{K}{2}}\overline{\varphi_{\frac{K}{2}}(y_{\frac{K}{2}})}=0, \qquad (2,10,3)$$

где $\overline{\varphi_i(y_i)}$ — вектор-полином с координатами

$$(na_{0n}y_i^{n-1}+l_{1n}^{(i)}y_i^{n-2}+\ldots+l_{n-1\,n}^{(i)};\ldots;\ a_{01}),$$

где $|l_{\gamma j}^{(i)}|\leqslant 2^{\gamma}p^{\gamma}$ $(\gamma=1,\ 2,\ldots,\ n-1)$. Эти векторы-полиномы $\overline{\varphi_i(y_i)}$ все имеют постоянную первую координату a_{01}, и поэтому, рассматривая все векторы $\overline{\varphi_i(y_i)}$ лежащими в E^{n-1}, мы получим дополнительное условие

$$h_1+h_2+\ldots+h_{\frac{K}{2}}=0. \qquad (2,10,4)$$

Будем теперь рассматривать систему векторов-полиномов $h_i\overline{\varphi_i(y_i)}$ как систему G_i из леммы 2, причем $K_0=4n$

$$2^s=2^{[4\log_2 K']-1}. \qquad (2,10,5)$$

Это дает нам 2^s уравнений вида

$$h_1\{\overline{\varphi_1(y_1^{(1)})}+\overline{\varphi_1(y_1^{(2)})}+\ldots+\overline{\varphi_1(y_1^{(2^{s-1})})}-\overline{\varphi_1(y_1^{(2^{s-1}+1)})}-\\ -\ldots-\overline{\varphi_1(y_1^{(2^s)})}\}+\ldots+h_{4n}\{\overline{\varphi_{4n}(y_{4n}^{(1)})}+\ldots-\\ -\overline{\varphi_{4n}(y_{4n}^{(2^s)})}\}=0, \qquad (2,10,6)$$

где $y_i^{(j)}$ независимо пробегают промежуток $[-2p,\ 2p]$.

Выражения, заключенные в каждой из $4n$ фигурных скобок, суть векторы $\bar{z}_i$ из E^{n-1}, удовлетворяющие условию

$$(+)\,\bar{z}\subseteq\begin{pmatrix} c_{n-1}p^{n-1}\\ \vdots\\ c_1 p\end{pmatrix},$$

и, согласно индуктивному предположению, каждый такой вектор $\bar{z}_i$ повторяется не более $B\frac{p^{2^s}}{p^{(n-1)^2}}$ раз.

Таким образом, мы придем к 2^s линейным уравнениям вида

$$\left.\begin{aligned} &h_1\bar{z}_1+h_2\bar{z}_2+\ldots+h_{4n^2}\bar{z}_{4n}=0,\\ &h_{4n+1}\bar{z}_{4n+1}+h_{4n+2}\bar{z}_{4n+2}+\ldots+h_{4n+4n}\bar{z}_{4n+4n}=0,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ &h_{\frac{K}{2}-4n+1}\bar{z}_{\frac{K}{2}-4n+1}+\ldots+h_{\frac{K}{2}}\bar{z}_{\frac{K}{2}}=0,\end{aligned}\right\} \qquad (2,10,7)$$

где

$$(+)\,\bar{z}\subseteq\begin{pmatrix} c_{n-1}p^{n-1}\\ \vdots\\ c_1 p\end{pmatrix}$$

и каждый вектор $\bar{z}_i$ повторяется не более $B\frac{p^{2^s}}{p^{(n-1)^2}}$ раз; числа же h_i удовлетворяют условию

$$\sum_{i=1}^{\frac{K}{2}}h_i=0. \qquad (2,10,8)$$

Заставляя h_i пробегать все значения, включая $(0, 0, \ldots, 0,)$, и отбрасывая условия (2, 10,8), мы лишь увеличим сумму Ч. Р. У. (2,10,7). Но тогда, применяя лемму 4, получим: сумма Ч. Р. У. (2, 10,7), где каждый вектор считается без повторений, не будет превосходить числа

$$B\frac{(r_{\overline{T}}\{\overline{N}\})^{4n-1}}{p^n}(p^{4n})^{2^s}. \qquad (2,10,9)$$

Так как каждый $\overline{z}_i$ повторяется не более $B\frac{p^{2^s}}{p^{(n-1)^2}}$ раз, то искомая сумма Ч. Р. У. (2, 10,7) с учетом повторений будет не более

$$B\frac{(r_{\overline{T}}\{\overline{N}\})^{4n-1}}{p^n}(p^{4n})^{2^s}\left(\frac{p^{2^s}}{p^{(n-1)^2}}\right)^{4n} \leqslant$$

$$\leqslant B_n\frac{p^{\frac{n(n+1)}{2}(4n-1)}p^{4n2^s}p^{4n2^s}}{p^{n^2}p^{4n(n-1)^2}} \leqslant B_n\frac{p^K}{p^{n^2}}, \qquad (2,10,10)$$

что и требовалось доказать.

Рассмотрим теперь векторы-полиномы вида

$$\overline{F_1(x_i)} = \begin{pmatrix} x_i^n \\ x_i^{n-1} \\ \vdots \\ x_i \end{pmatrix} \qquad (2,10,11)$$

и $\{\overline{F_1(x_i)}\}$ — их совокупность, где x_i пробегает все натуральные числа. Очевидно, эти векторы удовлетворяют всем условиям основной леммы. Докажем, что плотность $\{\overline{F_1(x_i)}\}$ положительна.

Действительно, фиксируя вектор $\overline{m}\in\{\overline{N}\}$ и рассматривая все целочисленные векторы E^n, среди них $\overline{F_1(x_i)}\subseteq\overline{m}$, мы можем, согласно основной лемме, найти число $K(n)$. Рассматривая далее все $\overline{F_1(x_i)}\subseteq\overline{m}$ с числами повторений a_j, удовлетворяющими условию

$$\sum_{j=1}^{r_{\overline{m}}\{\overline{F_1(x_i)}\}} a_j = B_n m_n^{\frac{K}{n}}, \qquad (2,10,12)$$

получим

$$\sum_{j=1}^{r_{\overline{m}}\{\overline{F_1(x_i)}\}} a_j \leqslant B_n \frac{m_n^n}{m_n^n} r_{\overline{m}}\{\overline{F_1(x_i)}\},$$

откуда

$$r_{\overline{m}}\{\overline{F_1(x_i)}\} \geqslant c \frac{\sum_{j=1}^{r_{\overline{m}}\{\overline{F_1(x_i)}\}} a_i m_n^n}{m_n^n} \geqslant c_n m_n^n;$$

$$\frac{r_{\overline{m}}\{\overline{F_1(x_i)}\}}{r_{\overline{m}}\{\overline{N}\}} \geqslant c_n \frac{m_n^n}{r_{\overline{m}}\{\overline{N}\}} \geqslant c_n'' > 0, \qquad (2,10,13)$$

что и требовалось доказать.

В аддитивных задачах типа проблемы Варинга идея плотности числовых последовательностей в смысле Шнирельмана, как известно, освобождает от необходимости изучать арифметическую структуру последовательности, если она имеет положительную плотность. Для целочисленных векторов E^n при $n > 1$ подобный факт не имеет места. Действительно, пусть $\{\overline{A}\}$ — какое-либо подмножество $\{\overline{N}\}$. Обозначим через $\mathfrak{A}$ арифметическую характеристику $\{\overline{A}\}$, т. е. правило, позволяющее в конечное число действий ответить на вопрос о принадлежности наперед заданного вектора $\overline{m}$ к $\{\overline{A}\}$. Пусть $\{\overline{B}\}$ — совокупность всех различных векторов, каждый из которых имеет вид

$$\overline{B} = \sum_{i=1}^{K} \overline{A}_i, \quad \overline{A}_i \in \{\overline{A}\},$$

где K пробегает все целые положительные числа. Тогда множество $\{\overline{B}\}$ имеет нетривиальную арифметическую характеристику $\mathfrak{B}$. В самом деле, пусть, например, характеристика $\mathfrak{A}$ такова, что исключает из $\{\overline{A}\}$ все векторы вида

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ m \end{pmatrix};$$

тогда, очевидно, все эти векторы не принадлежат и к $\{\overline{B}\}$, т. е. множество $\{\overline{A}\}$, если и имеет положительную плотность (что, конечно, возможно, так как оно может содержать, например, все остальные векторы, кроме указанных выше), не является базисом для $\{\overline{N}\}$. Следовательно, вопрос можно ставить лишь об отыскании свойства множества $\mathfrak{B}$, если задана совокупность векторов $\{\overline{A}\}$ со свойством $\mathfrak{A}$ и затем, является ли $\{\overline{A}\}$ базисом конечного порядка для $\{\overline{B}\}$, если $D\{\overline{A}\} > 0$. Рассмотрим лишь векторы

$$\overline{m} = \begin{pmatrix} m_n \\ m_{n-1} \\ \vdots \\ m_1 \end{pmatrix},$$

удовлетворяющие условию

$$m_1 \leqslant m_2 \leqslant \ldots \leqslant m_n. \qquad (2,10,14)$$

Определим плотность множества $\{\overline{A}\}$ по отношению к $\{\overline{B}\}$:

$$D_{\{\overline{B}\}}\{\overline{A}\} = \inf \frac{r_{\overline{m}}\{\overline{A}\}}{r_{\overline{m}}\{\overline{B}\}}, \qquad (2,10,15)$$

где $\overline{m}$ пробегает все целочисленные векторы $\{\overline{N}\}$, и докажем лемму

$$D_{\{\overline{B}\}}(\{\overline{A}\} + \{\overline{A}\}) \geqslant 2D_{\{\overline{B}\}}\{\overline{A}\} - D^2_{\{\overline{B}\}}\{\overline{A}\}. \qquad (2,10,16)$$

Пусть $\overline{m} \in \{\overline{B}\}$, упорядочим $\{\overline{A}\}$ и $\{\overline{B}\}$ так, чтобы каждый предыдущий вектор «не превосходил» последующего. Тогда, если $\{\overline{B}\} \neq \{\overline{A}\}$, то при некотором $\overline{m} \in \{\overline{B}\}$ найдутся $\overline{a}_1 \in \{\overline{A}\}$ и $\overline{a}_2 \in \{\overline{A}\}$ таких, что $\overline{a}_1 \subset \overline{m}$, $\overline{a}_2 \subseteq m$ и есть хотя бы один вектор $\overline{b} \in \{\overline{B}\}$ такой, что $a_1 \subset b \subset a_2$. Число всех таких векторов $\overline{b} \subseteq \overline{m}$ будет $r_{\overline{m}}\{\overline{B}\} - r_{\overline{m}}\{\overline{A}\}$. Пусть $D_{\{\overline{B}\}}\{\overline{A}\} = \alpha > 0$; тогда $r_{\overline{a}_2 - \overline{a}_1}\{\overline{A}\} > \alpha r_{\overline{a}_2 - \overline{a}_1}\{\overline{B}\}$, следовательно, в промежуток между векторами $\overline{a}_1$ и $\overline{a}_2$ попадет не менее $\alpha r_{\overline{a}_2 - \overline{a}_1}\{\overline{B}\}$ векторов

$$\overline{c} \in \{\overline{A}\} \perp \{\overline{A}\}.$$

Просуммировав теперь их по всем таким промежуткам, мы получим

$$r_{\overline{m}}(\{\overline{A}\}+\{\overline{A}\}) \geqslant r_{\overline{m}}\{\overline{A}\}+\alpha\sum r_{\overline{a}_l-\overline{a}_{l-1}}\{\overline{B}\}= \\ =r_{\overline{m}}\{\overline{A}\}+\alpha\left(r_{\overline{m}}\{\overline{B}\}-r_{\overline{m}}\{\overline{A}\}\right),$$

или

$$r_{\overline{m}}(\{\overline{A}\}+\{\overline{A}\}) \geqslant 2\alpha r_{\overline{m}}\{\overline{B}\}-\alpha r_{\overline{m}}\{\overline{A}\}.$$

Отсюда

$$\frac{r_{\overline{m}}(\{\overline{A}\}+\{\overline{A}\})}{r_{\overline{m}}\{\overline{B}\}} \geqslant 2\alpha-\frac{\alpha r_{\overline{m}}\{\overline{A}\}}{r_{\overline{m}}\{\overline{B}\}},$$

или

$$D_{\{\overline{B}\}}(\{\overline{A}\}+\{\overline{A}\}) \geqslant 2\alpha-\alpha^2.$$

Далее очевидно, что, взяв достаточно большое число S, мы получим $D_{\{\overline{B}\}}\left(\sum_{i=1}^{S}\{\overline{A}\}\right)>\frac{1}{2}$, откуда непосредственно вытекает, что $\{\overline{A}\}$ является базисом порядка $2S$ для множества векторов $\{\overline{B}\}$.

Применим доказанную лемму к совокупности векторов $\{\overline{F_1(x_i)}\}$. Это множество удовлетворяет условиям леммы и плотность его положительна. Далее известно, что всякий вектор

$$\begin{pmatrix} N_n \\ N_{n-1} \\ \vdots \\ N_1 \end{pmatrix},$$

представимый в виде суммы векторов из $\{\overline{F_1(x_i)}\}$, должен удовлетворять необходимым условиям (2,7,3). Это условие (2,7,3) и является свойством $\mathfrak{B}$ множества всех векторов

$$\begin{pmatrix} N_n \\ N_{n-1} \\ \vdots \\ N_n \end{pmatrix},$$

представимых в виде суммы какого бы то ни было числа слагаемых из $\{\overline{F_1(x_i)}\}$. Так как $D_{\{\overline{B}\}}\{\overline{F_1(x_i)}\} \geqslant D\{\overline{F_1(x_i)}\}>0$, то таким образом доказана основная теорема.

ГЛАВА 3

ПРОБЛЕМА РАСПРЕДЕЛЕНИЯ ПРОСТЫХ ЧИСЕЛ

§ 1. Числовые функции и связи между ними. Оценка числа простых в отрезке натурального ряда

Элементарные методы в распределении простых, опирающиеся на изучение свойств числовых функций Мангольта и Мёбиуса $\Lambda(n)$ и $\mu(n)$:

$$\Lambda(n)=\begin{cases}\ln p, & n=p^k\\ 0, & n\neq p^k\end{cases},\qquad \mu(n)=\begin{cases}+1, & n=1,\\ (-1)^k, & n=p_1\dots p_k,\\ 0, & p^2\mid n,\end{cases}$$

где p и p_k — простые, получили сильное развитие в последнее время благодаря работам А. Сельберга и других математиков, продолжавших его работы. Приведем ряд свойств этих функций, хорошо известных, которые нам понадобятся в дальнейшем.

Прежде всего,

$$\sum_{d\mid n}\mu(d)=\prod_{p\mid n}[1+\mu(p)]=\begin{cases}1, & n=1,\\ 0, & n>1,\end{cases}\qquad (3,1,1)$$

и при произвольной $U(x)$, если

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

то

$$\sum_{k\mid n}\mu(k)\,V\left(\frac{n}{k}\right)=\sum_{k\mid n}\mu(k)\sum_{d\mid k\mid n}U(d)=$$

$$=\sum_{d\mid n}U(d)\sum_{k\,\mid\,\frac{n}{d}}\mu(k)=U(n).\qquad (3,1,2)$$

Из этого последнего соотношения следует, так как

$$\ln n = \sum_{d|n} \Lambda(d),$$

что

$$\Lambda(n) = \sum_{d|n} \mu(d) \ln \frac{n}{d} = -\sum_{d|n} \mu(d) \ln d.$$

Далее, если

$$\rho(n) = \begin{cases} 1, & n \geqslant 1, \\ 0, & n < 1, \end{cases}$$

то

$$[x] = \sum_{n=1}^{\infty} \rho\left(\frac{x}{n}\right), \quad \rho(x) = \sum_{n \leqslant x} \sum_{d|n} \mu(d) =$$

$$= \sum_{d \leqslant x} \mu(d) \left[\frac{x}{d}\right]. \qquad (3,1,3)$$

Отсюда следует, что при $x \geqslant 1$

$$1 = x \sum_{n \leqslant x} \frac{\mu(n)}{n} - \sum_{n \leqslant x} \mu(n) \left\{\frac{x}{n}\right\}$$

или что

$$\left| \sum_{n \leqslant x} \frac{\mu(n)}{n} \right| \leqslant 1. \qquad (3,1,4)$$

Совершенно так же

$$\psi(x) = \sum_{n \leqslant x} \Lambda(n) = \sum_{n \leqslant x} \sum_{d|n} \mu(d) \ln \frac{x}{d} - \ln x =$$

$$= \sum_{n \leqslant x} \left[\frac{x}{n}\right] \mu(n) \ln \frac{x}{n} =$$

$$= -\sum_{n \leqslant x} \left\{\frac{x}{n}\right\} \ln \frac{x}{n} \mu(n) + x \sum_{n \leqslant x} \frac{\mu(n)}{n} \ln \frac{x}{n}.$$

Но так как при $q>0$

$$\sum_{n\leqslant x}\ln^q\frac{x}{n}=\int_1^x\ln^q\frac{x}{t}\,dt+O(\ln^q x)=$$

$$=x\int_1^x\ln^q t\,\frac{dt}{t^2}+O(\ln^q x)=O(x), \tag{3,1,5}$$

то

$$\left|\sum_{n\leqslant x}\left\{\frac{x}{n}\right\}\mu(n)\ln\frac{x}{n}\right|=O(x).$$

Далее, вследствие $\sum\limits_{k\leqslant t}\frac{1}{k}=\ln t+c+O\left(\frac{1}{t}\right)$,

$$\sum_{n\leqslant x}\frac{\mu(n)}{n}\ln\frac{x}{n}=\sum_{n\leqslant x}\frac{\mu(n)}{n}\left[\sum_{k\leqslant\frac{x}{n}}\frac{1}{k}-c+O\left(\frac{n}{x}\right)\right]=$$

$$=\sum_{n\leqslant x}\frac{1}{n}\sum_{d\mid n}\mu(d)-c\sum_{n\leqslant x}\frac{\mu(n)}{n}+O(1)=O(1).$$

Поэтому

$$\psi(x)=\sum_{n\leqslant x}\Lambda(n)=O(x). \tag{3,1,6}$$

Воспользовавшись формулой Стирлинга, мы будем иметь

$$\sum_{n\leqslant x}\ln n=x\ln x-x+O(\ln x)=\sum_{n\leqslant x}\sum_{d\mid n}\Lambda(d)=$$

$$=\sum_{d\leqslant x}\Lambda(d)\left[\frac{x}{d}\right]=x\sum_{n\leqslant x}\frac{\Lambda(n)}{n}-\sum_{d\leqslant x}\Lambda(d)\left\{\frac{x}{d}\right\}=$$

$$=x\sum_{n\leqslant x}\frac{\Lambda(n)}{n}+O(x)$$

или что

$$\sum_{n\leqslant x}\frac{\Lambda(n)}{n}=\ln x+O(1). \tag{3,1,7}$$

Эта последняя формула указывает не только на бесконечность простых чисел, но и дает представление об их количестве на отрезке $[1, x]$. Действительно,

$$\sum_{n\leqslant x}\frac{\Lambda(n)}{n}=\sum_{p\leqslant x}\frac{\ln p}{p}+\sum_{p^2\leqslant x}\frac{\ln p}{p^2}+\dots=$$
$$=\sum_{p\leqslant x}\frac{\ln p}{p}+O(1)=\ln x+O(1),$$

другими словами, число простых не только бесконечно, но и ряд с членами $\frac{\ln p}{p}$ расходится. Более точную количественную оценку для числа простых можно получить, оценив снизу $\psi(x)$. Мы будем иметь далее

$$x\ln x-x+O(\ln x)=\sum_{n\leqslant x}\Lambda(n)\left[\frac{x}{n}\right]=$$
$$=\sum_{d\leqslant x}\Lambda(d)\sum_{k\leqslant\frac{x}{d}}1=\sum_{d\leqslant x}\sum_{k\leqslant\frac{x}{d}}\Lambda(k)=\sum_{1}^{\infty}\psi\left(\frac{x}{n}\right),$$

если воспользоваться преобразованием

$$\sum_{n\leqslant x}U(n)\sum_{m\leqslant\frac{x}{n}}V(m)=\sum_{n\leqslant x}V(n)\sum_{m\leqslant\frac{x}{n}}U(m). \quad (3,1,8)$$

Отсюда, по П. Л. Чебышеву, заменяя x на $\frac{x}{2}$ и вычитая, мы будем иметь

$$\sum_{n\leqslant x}\ln n-2\sum_{n\leqslant\frac{x}{2}}\ln n=x\ln 2+O(\ln x)=\sum_{n\leqslant x}\psi\left(\frac{x}{n}\right)-$$
$$-2\sum_{n\leqslant x}\psi\left(\frac{x}{2n}\right)=\psi(x)-\psi\left(\frac{x}{2}\right)+\psi\left(\frac{x}{3}\right)-\dots<\psi(x) \quad (3,1,9)$$

вследствие монотонности $\psi(x)$. Но функция $\psi(x)$ непосредственно связана с $\pi(x)$ и $\Pi(x)$,

$$\pi(x)=\sum_{p\leqslant x}1,\qquad \Pi(x)=\sum_{p^k\leqslant x}1,$$
$$\Pi(x)=\pi(x)+\pi(\sqrt{x})+\dots=\pi(x)+O(\sqrt{x}).$$

Действительно,

$$\pi(x)=\Pi(x)+O(\sqrt{x})=\sum_{n\leqslant x}\frac{\Lambda(n)}{\ln n}+O(\sqrt{x})=$$

$$=\sum_{n\leqslant x}\frac{\psi(n)-\psi(n-1)}{\ln n}+O(\sqrt{x})=\frac{\psi(x)}{\ln x}+$$

$$+\sum_{n=1}^{[x]-1}\psi(n)\left[\frac{1}{\ln n}-\frac{1}{\ln(n-1)}\right]+O(\sqrt{x})=\frac{\psi(x)}{\ln x}+$$

$$+\sum_{n\leqslant x}\frac{\psi(n)}{n\ln^2 n}+O(\sqrt{x})=\frac{\psi(x)}{\ln x}+\int_2^x\frac{\psi(t)}{t\ln^2 t}\,dt+O(\sqrt{x})=$$

$$=\int_2^x\frac{dt}{\ln t}+\frac{\psi(x)-x}{\ln x}+\int_2^x\frac{\psi(t)}{t\ln^2 t}\,dt+O(\sqrt{x}). \quad (3,1,10)$$

Теперь из неравенства (3, 1, 9) мы будем иметь

$$\pi(x)>\frac{x}{\ln x}\ln 2+O\left(\frac{x}{\ln^2 x}\right), \quad (3,1,11)$$

то есть простейшее чебышевское неравенство снизу для $\pi(x)$. Ниже мы приведем доказательство асимптотического закона для $\pi(x)$, другими словами, оценку $\pi(x)=\frac{x}{\ln x}+o\left[\frac{x}{\ln x}\right]$, а сейчас остановимся на вопросе о числе простых чисел в арифметической прогрессии.

§ 2. Теорема Дирихле о бесконечности простых в арифметической прогрессии

Напомним основные свойства характеров модуля $D>1$. Все характеры мультипликативны, $\chi(n)\chi(m)=\chi(nm)$, и если $\chi\neq\chi_0$, другими словами, неглавный характер, то

$$\left.\begin{aligned}&\left|\sum_{k=n}^{N}\chi(k)\right|<h,\ \left|\sum_{k=n}^{N}\chi(k)\,U_k\right|<2hU_n,\\&U_n\geqslant U_{n+1}\geqslant\ldots\geqslant U_N\geqslant 0,\end{aligned}\right\} \quad (3,2,1)$$

где $h=\varphi(D)$ — функция Эйлера.

Если $\chi(n)$ — действительный характер, $\chi \neq \chi_0$, то

$$L(\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} \neq 0. \tag{3,2,2}$$

Сходимость этого ряда для любого неглавного характера обеспечивается неравенствами (3,2,1). Действительно,

$$\left| \sum_{n}^{N} \frac{\chi(k)}{k} \right| < \frac{2h}{n},$$

откуда также

$$\left| L(\chi) - \sum_{n \leqslant x} \frac{\chi(n)}{n} \right| < \frac{2h}{x}, \qquad L(\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}. \tag{3,2,3}$$

Для доказательства (3,2,2) мы рассмотрим функцию $U(x)$ $(0 < x < 1)$:

$$U(x) = \sum_{n=1}^{\infty} \frac{\chi(n)\, x^n}{1 - x^n} = \sum_{n=1}^{\infty} \left[\sum_{d \mid n} \chi(d) \right] x^n = \sum_{n=1}^{\infty} f_n x^n.$$

Прежде всего заметим, что

$$f_n = \prod_{k=1}^{s} [1 + \chi(p_k) + \ldots + \chi^{\nu_k}(p_k)] \quad (n = p_1^{\nu_1} \ldots p_s^{\nu_s}).$$

Отсюда следует, так как $\chi(p) = 1, -1, 0$, что всегда $f_n \geqslant 0$ и $f_n \geqslant 1$, если все ν_k четные, другими словами, если $n = n_0^2$. Поэтому при $1 > x > \frac{1}{2}$, $x > x_0$

$$U(x) > \sum_{n=1}^{\infty} x^{n^2} = \int_{1}^{\infty} x^{t^2}\, dt + O(1) =$$

$$= \frac{1}{\sqrt{-\ln x}} \int_{0}^{\infty} e^{-t^2}\, dt + O(1) = \frac{\sqrt{\pi}}{2\sqrt{-\ln x}} + O(1) =$$

$$= \frac{\sqrt{\pi}}{2} \frac{1}{[-\ln(1-(1-x))]^{\frac{1}{2}}} + O(1) > \frac{1}{2\sqrt{1-x}}.$$

Далее, при

$$S_n = \sum_{k=n}^{\infty} \frac{\chi(k)}{k}, \quad S_1 = L(\chi),$$

$$R_1(x) = U(x) - \frac{L(\chi)}{1-x} = \sum \chi(n) \frac{x^n}{1-x^n} - \sum_{n=1}^{\infty} \frac{\chi(n)}{n} \frac{x^n}{1-x} +$$

$$+ \sum_{n=1}^{\infty} (S_n - S_{n+1}) \frac{x^n}{1-x} - \frac{L(\chi)}{1-x} =$$

$$= \sum \chi(n) \left[\frac{x^n}{1-x^n} - \frac{x^n}{n(1-x)} \right] - \sum_{n=0}^{\infty} S_{n+1} x^n.$$

В силу (3,2,3)

$$\sum_{n=1}^{\infty} S_{n+1} x^n = O\left[\sum_{n=1}^{\infty} \frac{x^n}{n} \right] = O\left(\ln \frac{1}{1-x} \right).$$

Далее, с помощью преобразования Абеля мы будем иметь

$$R_2 = \left| \sum_{n=1}^{\infty} \chi(n) \left[\frac{x^n}{1-x^n} - \frac{x^n}{n(1-x)} \right] \right| =$$

$$= \left| \sum_{n=1}^{\infty} T(n) \left[\frac{x^n}{1-x^n} - \frac{x^n}{n(1-x)} - \frac{x^{n+1}}{1-x^{n+1}} + \frac{x^{n+1}}{(n+1)(1-x)} \right] \right| <$$

$$< \frac{h}{1-x} \sum_{n=1}^{\infty} \left| \frac{x^n}{1+x+\ldots+x^{n-1}} - \frac{x^{n+1}}{1+x+\ldots+x^n} - \right.$$

$$\left. - \frac{x^n}{n(n+1)} - \frac{(1-x)x^n}{n+1} \right| < \frac{h}{1-x} \sum_{n=1}^{\infty} \left[\frac{x^n}{1+x+\ldots+x^{n-1}} - \right.$$

$$\left. - \frac{x^{n+1}}{1+x+\ldots+x^n} - \frac{x^n}{n(n+1)} \right] + h \sum_{1}^{\infty} \frac{x^n}{n+1} =$$

$$= 2h \sum_{1}^{\infty} \frac{x^n}{n+1} = O\left(\ln \frac{1}{1-x} \right),$$

$$T(n) = \sum_{k=1}^{n} \chi(k), \quad |T_k| < h$$

Значит,

$$U(x)=O\left(\ln\frac{1}{1-x}\right), \qquad U(x)>\frac{1}{2\sqrt{1-x}},$$

если $L(\chi)=0$. Это противоречие и доказывает (3,2,2). Напомним также, что

$$\sum_{\chi}\chi(nl')=\begin{cases}h, & n\equiv l\pmod D\\ 0, & n\not\equiv l\pmod D,\end{cases} \qquad ll'\equiv 1\pmod D,$$

где сумма взята по всем χ, $(l, D)=1$.

Пусть теперь $\chi(n)$ — опять неглавный характер. Тогда

$$\sum_{n\leqslant x}\frac{\chi(n)\ln n}{n}=\sum_{n\leqslant x}\frac{\chi(n)}{n}\sum_{d\mid n}\Lambda(d)=$$

$$=\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n}\sum_{k\leqslant\frac{x}{n}}\frac{\chi(k)}{k}=L(\chi)\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n}+R(x),$$

где

$$R(x)=\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n}\sum_{k>\frac{x}{n}}\frac{\chi(k)}{k}=\sum\frac{\Lambda(n)}{n}O\left(\frac{n}{x}\right)=$$

$$=O\left[\frac{1}{x}\sum_{n\leqslant x}\Lambda(n)\right]=O(1).$$

Кроме этого, в силу (3,2,1) ряд $\sum_{n=1}^{\infty}\frac{\chi(n)\ln n}{n}$ сходящийся. Поэтому мы получаем соотношение

$$L(\chi)\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n}=O(1). \qquad (3,2,4)$$

Мы будем также иметь для неглавного характера $\chi(n)$

$$\sum_{n\leqslant x}\frac{\chi(n)}{n}\sum_{d\mid n}\mu(d)\ln\frac{x}{d}=\ln x+\sum_{n\leqslant 1}\frac{\chi(n)\Lambda(n)}{n}=$$

$$=\sum_{n\leqslant x}\frac{\chi(n)\mu(n)}{n}\ln\frac{x}{n}\sum_{k\leqslant\frac{x}{n}}\frac{\chi(k)}{k}=L(\chi)\sum_{n\leqslant x}\frac{\chi(n)\mu(n)}{n}\ln\frac{x}{n}+R(x),$$

где

$$R(x)=\sum_{n\leqslant x}\frac{1}{n}\ln\frac{x}{n}\,O\left(\frac{n}{x}\right)=O\left(\sum_{n\leqslant x}\frac{1}{x}\ln\frac{x}{n}\right)=O(1).$$

Поэтому

$$\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n}=-\ln x+L(\chi)A(x)+O(1). \qquad (3,2,5)$$

Из (3,2,4) и (3,2,5) следует, что при $\chi(n)$ неглавном характере

$$\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n}=\delta(\chi)\ln x+O(1), \qquad (3,2,6)$$

$$\delta(\chi)=\begin{cases}-1, & L(\chi)=0,\\ 0, & L(\chi)\neq 0.\end{cases}$$

Если же $\chi=\chi_0$ — главный характер, то

$$\sum_{n\leqslant x}\frac{\chi_0(n)\Lambda(n)}{n}=\sum_{n\leqslant x}\frac{\Lambda(n)}{n}+O(1)=\ln x+O(1). \qquad (3.2,7)$$

Сложим по всем χ левые и правые части (3, 2, 6) и (3,2,7). Мы будем тогда иметь

$$\ln x+\Big[\sum_{\chi\neq\chi_0}\delta(\chi)\Big]\ln x+O(1)=\sum\frac{\Lambda(n)}{n}\sum_{\chi}\chi(n)\geqslant 0. \qquad (3,2,8)$$

Допустим теперь, что $L(\chi)=0$ для характера третьего рода, не действительного характера. Тогда и $L(\bar{\chi})=0$, другими словами, в этом случае $\delta(\chi)=\delta(\bar{\chi})=-1$. Поэтому

$$(1-2)\ln x=-\ln x>O(1).$$

Это противоречие показывает, что $L(\chi)\neq 0$ для характеров третьего рода. Для характеров второго рода $\delta(\chi)=0$, так как $L(\chi)\neq 0$ в силу (3,2,2). Поэтому для всякого $\chi\neq\chi_0$

$$\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n}=O(1). \qquad (3,2,9)$$

Мы теперь можем доказать теорему, несколько более сильную, чем теорема Дирихле о прогрессиях.

Теорема 3.2.1. *Если* $D>1$, l *целые*, $(D, l)=1$, *то*

$$\sum_{\substack{p\leqslant x\\ p\equiv l \pmod D}} \frac{\ln p}{p}=\frac{1}{\varphi(D)}\ln x+O(1), \qquad (3,2,10)$$

где p *— простые числа, а* $\varphi(D)$ *— функция Эйлера.*

Пусть $l'\equiv 1 \pmod D$. Умножим левые части (3.2.6) и (3.2.7) на $\chi(l')$, соответственно, и сложим по всем χ. Мы будем иметь

$$\sum_{\chi}\chi(l')\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n}=\ln x+O(1)=$$

$$=\varphi(D)\sum_{\substack{n\leqslant x\\ n\equiv l \pmod D}}\frac{\Lambda(n)}{n}+O(1)=\varphi(D)\sum_{\substack{p\leqslant x\\ p\equiv l \pmod D}}\frac{\ln p}{p}+O(1)$$

на основании (3,2,3), (3,2,6) и (3,2,7). Это и доказывает нашу теорему.

§ 3. Основные неравенства для оценки числа простых в натуральном ряде

Переходим теперь к доказательству основных предельных теорем распределения простых чисел в натуральном ряде и прогрессиях. Мы уже знаем из (3,1,10), что

$$\pi(x)=\frac{\psi(x)}{x}+O\left[\sum_{2}^{x}\frac{1}{\ln^2 n}\right]+O(\sqrt{x})=\frac{\psi(x)}{\ln x}+O\left(\frac{x}{\ln^2 x}\right),$$

другими словами, что из $\psi(x)=x+o(x)$ следует

$$\pi(x)=\frac{x}{\ln x}+o\left(\frac{x}{\ln x}\right). \qquad (3,3,1)$$

Совершенно так же, определяя при $D>1$, $(l, D)=1$ функции

$$\pi(l, D; x)=\sum_{\substack{p\leqslant x\\ p\equiv l \pmod D}}1, \qquad \psi(l, x)=\sum_{\substack{n\leqslant x\\ n\equiv l \pmod D}}\Lambda(n),$$

мы будем иметь

$$\pi(l, D; x) = \sum_{\substack{n \leqslant x \\ n \equiv l \pmod D}} \frac{\Lambda(n)}{\ln n} + O(\sqrt{x}) = \sum_{n \leqslant x} \frac{\psi(l, n) - \psi(l, n-1)}{\ln n} +$$

$$+ O(\sqrt{x}) = \frac{\psi(l, x)}{\ln x} + \sum_{n \leqslant x} \frac{\psi(l, n)}{n \ln^2 n} + O(\sqrt{x}) =$$

$$= \frac{\psi(l, x)}{\ln x} + O\left(\frac{x}{\ln^2 x}\right).$$

Отсюда непосредственно следует, что если $\psi(l, x) = \frac{1}{h} x + o(x)$, $h = \varphi(D)$, то

$$\pi(l, D, x) = \frac{1}{h} \frac{x}{\ln x} + o\left(\frac{x}{\ln x}\right). \qquad (3,3,2)$$

Определим теперь функции

$$M(x) = \sum_{n \leqslant x} \mu(n), \qquad M(l, x) = \sum_{\substack{n \leqslant x \\ n \equiv l \pmod D}} \mu(n), \qquad (3,3,3)$$

где $(l, D) = 1$, и покажем, что вместо оценок функций $\psi(x)$ и $\psi(l, x)$ можно воспользоваться более просто получаемыми оценками функций $M(x)$ и $M(l, x)$. Предварительно докажем, что при $n > \sqrt{x}$

$$\Delta = \left[\frac{x}{n}\right] - \left[\frac{x}{n+1}\right] = \begin{cases} 1, & n = \left[\frac{x}{k}\right], \\ 0, & n \neq \left[\frac{x}{k}\right], \end{cases} \qquad (3,3,4)$$

где $k < \sqrt{x}$ — целое число. Действительно,

$$\Delta = \left[\frac{x}{n}\right] - \left[\frac{x}{n+1}\right] = \left[\frac{x}{n}\right] - \left[\left[\frac{x}{n}\right] + \left\{\frac{x}{n}\right\} - \frac{x}{n(n+1)}\right] =$$

$$= \left[\left\{\frac{x}{n}\right\} - \frac{x}{n(n+1)}\right] = 0,$$

если $\left\{\frac{x}{n}\right\} \geqslant \frac{x}{n(n+1)}$. Значит, $\Delta = 1$ тогда и только тогда, когда

выполнено обратное неравенство $\left\{\frac{x}{n}\right\} < \frac{x}{n(n+1)}$. Но в этом случае при $k = \left[\frac{x}{n}\right]$ мы будем иметь

$$\frac{n}{k}\left\{\frac{x}{n}\right\} < \frac{n}{k}\frac{x}{n(n+1)} = \frac{x}{(n+1)\frac{x}{n} - (n+1)\left\{\frac{x}{n}\right\}} < \frac{x}{(n+1)\frac{x}{n} - \frac{\lambda}{n}} = 1.$$

Следовательно, окончательно,

$$\frac{x}{k} = n + \frac{n}{k}\left\{\frac{x}{n}\right\} = n + \left\{\frac{x}{k}\right\},$$

или $n = \left[\frac{x}{k}\right]$.

Пусть $V(n)$ — число делителей числа n. Тогда вследствие (3,1,2)

$$V(n) = \sum_{d/n} 1, \quad \sum_{d/n} \mu(d)\, V\left(\frac{n}{d}\right) = 1. \tag{3,3,5}$$

Далее, мы будем иметь оценку

$$T(x) = \sum_{n \leqslant x} V(n) = \sum_{n \leqslant x}\sum_{d\ n} 1 = \sum_{n \leqslant x}\sum_{k \leqslant \frac{x}{n}} 1 = \sum_{n \leqslant x}\left[\frac{x}{n}\right] =$$

$$= \sum_{n \leqslant \sqrt{x}}\left[\frac{x}{n}\right] + \sum_{\sqrt{x} < n \leqslant x}\left[n - (n-1)\right]\left[\frac{x}{n}\right] = \sum_{n \leqslant \sqrt{x}}\left[\frac{x}{n}\right] -$$

$$- [\sqrt{x}]\left[\frac{x}{[\sqrt{x}]+1}\right] + \sum_{\sqrt{x} < n \leqslant x}\left(\left[\frac{x}{n}\right] - \left[\frac{x}{n+1}\right]\right)n =$$

$$= 2\sum_{n \leqslant \sqrt{x}}\left[\frac{x}{n}\right] + O(\sqrt{x}) - x = 2x\sum_{n \leqslant \sqrt{x}}\frac{1}{n} - x + O(\sqrt{x}) =$$

$$= x\ln x + (2C-1)x + O(\sqrt{x}) \tag{3,3,6}$$

вследствие (3,3,4) и оценки $\sum_{k \leqslant x}\frac{1}{k} = \ln x + C + O\left(\frac{1}{x}\right)$.

Это — известная оценка Дирихле. Теперь мы можем доказать лемму.

Лемма 1. *Если* $M(x)=o(x)$, *то*

$$\pi(x)=\frac{x}{\ln x}+o\left(\frac{x}{\ln x}\right). \tag{3,3,7}$$

Если же не только $M(x)=o(x)$, *но и* $M(l,\ x)=o(x)$ *для всех* $l<D$, $(l,\ D)=1$, *то и*

$$\pi(l,\ D;\ x)=\frac{1}{h}\frac{x}{\ln x}+o\left(\frac{x}{\ln x}\right), \tag{3,3,8}$$

где $(l,\ D)=1$ *и* $h=\varphi(D)$ — *функция Эйлера.*

Рассмотрим непосредственно вытекающее из (3,1,1), (3,1,3) и (3,3,5) соотношение

$$\sum_{n\leqslant x}\sum_{d/n}\mu(d)\left[\ln\frac{n}{d}-V\left(\frac{n}{d}\right)+2C\right]=\psi(x)-[x]+2C.$$

Из этого соотношения, меняя порядки суммирования, мы получаем при любом N, $N=\left[\frac{x}{t}\right]$, $t<\sqrt{x}$,

$$\psi(x)-[x]+2C=\sum_{n\leqslant x}\mu(n)\sum_{k\leqslant\frac{x}{n}}[\ln k-V(k)+2C]=$$

$$=\sum_{n\leqslant N}\mu(n)\,W\left(\frac{x}{n}\right)-M(N)\,W\left(\frac{x}{N+1}\right)+$$

$$+\sum_{n<N\leqslant x}M(n)\left[W\left(\frac{x}{n}\right)-W\left(\frac{x}{n+1}\right)\right],$$

$$W\left(\frac{x}{n}\right)=\frac{x}{n}\ln\frac{x}{n}-\frac{x}{n}+O\left(\ln\frac{x}{n}\right)-\sum_{k\leqslant\frac{x}{n}}V(k)+2C\left[\frac{x}{n}\right]=$$

$$=o\left(\sqrt{\frac{x}{n}}\right).$$

В силу (3,3,6) с помощью (3,3,4) мы окончательно получаем неравенство

$$|\psi(x)-x|<C\left[\sum_{n\leqslant N}\sqrt{\frac{x}{n}}+M\left(\frac{x}{t}\right)\sqrt{t}+\right.$$

$$\left.+\sum_{k\leqslant t}\left|\ln k-V(k)+2C\left|\max_{1\leqslant k\leqslant t}M\left(\frac{x}{k}\right)\right|\right|\right]<$$

$$<C_1\left[\frac{x}{\sqrt{t}}+2\max_{1\leqslant k\leqslant t}\left|M\left(\frac{x}{k}\right)\right|t\ln t\right],$$

где C и C_1 от χ и t не зависят. Это неравенство показывает, что $\psi(x) = x + o(x)$, так как при сколь угодно большом, но фиксированном t и условии $M(x) = o(x)$ можно выбрать x столь большим, чтобы выполнялось неравенство

$$\max_{1 \leqslant k \leqslant t} \left| M\left(\frac{x}{k}\right) \right| < \frac{x}{t^2}.$$

Но из $\psi(x) = x + o(x)$ в силу (3, 3, 1) следует (3,3,7).

Заметим теперь, что если $\chi_0(n)$ — главный характер модуля D, то

$$\sum_{n \leqslant x} \chi_0(n) \Lambda(n) = \sum_{n \leqslant x} \Lambda(n) + O(\ln x) = \\ = \psi(x) + O(\ln x), \qquad (3,3,9)$$

так как число D делится на ограниченное число простых. Далее, если $\chi(n)$ — неглавный характер модуля D, то, меняя порядок суммирования, при $N = \left[\frac{x}{t}\right]$,

$$\sum_{n \leqslant x} \chi(n) \Lambda(n) = \sum_{n \leqslant x} \chi(n) \sum_{d/n} \mu(d) \ln \frac{n}{d} = \\ = \sum_{n \leqslant x} \chi(n) \mu(n) \sum_{k \leqslant \frac{x}{n}} \chi(k) \ln k = \sum_{n \leqslant N} \chi(n) \mu(n) W\left(\frac{x}{n}\right) + \\ + \sum_{N < n \leqslant x} [M_0(\chi, n) - M_0(\chi, n-1)] W\left(\frac{x}{n}\right) = \\ = \sum_{n \leqslant N} \chi(n) \mu(n) W\left(\frac{x}{n}\right) - M_0(\chi, N) W\left(\frac{x}{N+1}\right) + \\ + \sum_{N < n \leqslant x} M_0(\chi, n) \left[W\left(\frac{x}{n}\right) - W\left(\frac{x}{n+1}\right) \right], \qquad (3,3,10)$$

$$W\left(\frac{x}{n}\right) = \sum_{k \leqslant \frac{x}{n}} \chi(k) \ln k,$$

где

$$M_0(\chi, x) = \sum_{k \leqslant x} \chi(k) \mu(k) = \sum_{l=1}^{D-1} \chi(l) M(l, x) = o(x)$$

в предположениях нашей леммы. Так как

$$W(x)=\sum_{k\leqslant x}\chi(k)\ln k=$$

$$=\sum_{k\leqslant x}\chi(k)\ln x\sum_{n\leqslant x-1}\ln\left(1+\frac{1}{n}\right)\sum_{k\leqslant n}\chi(k)=O(\ln x),$$

то в силу (3,3,4) мы получаем из (3,3,10) неравенство

$$\sum_{n\leqslant x}\chi(n)\Lambda(n)<C\Big[\sum_{n\leqslant N}\ln\frac{x}{n}+\left|M_0\left(\chi,\frac{x}{t}\right)\right|\ln t+$$

$$+\sum_{n\leqslant t}\left|M_0\left(\chi,\frac{x}{n}\right)\right|\ln n\Big]<$$

$$<C_1\Big[\frac{x}{t}\ln t+\max_{n\leqslant t}\left|M\left(\chi,\frac{x}{n}\right)\right|t\ln t\Big], \qquad (3,3,11)$$

где C и C_1 от x и t не зависят, если $x\geqslant t^2$. Это неравенство показывает, что при $\chi(n)$ неглавном характере

$$\sum\chi(n)\Lambda(n)=o(x), \qquad (3,3,12)$$

так как в правой части (3,3,11) можно t взять сколь угодно большими, а x взять столь большим, чтобы были выполнены неравенства

$$\left|M_0\left(\chi,\frac{x}{n}\right)\right|<\frac{x}{t^2}\quad(1\leqslant n\leqslant t),$$

что возможно в силу условий нашей леммы. Но тогда при $\psi(x)=o(x)+x$

$$\psi(l,x)=\frac{1}{h}\sum_{\chi}\chi(l')\sum_{n\leqslant x}\chi(n)\Lambda(n)=\frac{x}{h}+o(x),$$

где $ll'\equiv 1(\mathrm{mod}\,D)$ и $h=\varphi(D)$ — функция Эйлера. Из этой последней оценки уже следует, в силу (3,3,2), утверждение нашей леммы (3,3,8). Лемма 1 сводит оценки функций $\pi(x)$ и $\pi(l,D,x)$ на оценки функций $M(x)$ и $M(l,x)$. Для этих последних оценок нам понадобятся некоторые новые соотношения и оценки общего характера.

Прежде всего заметим, что

$$\sum_{d/n}\mu(d)\ln^2 d = \frac{d^2}{ds^2}\left[\sum_{d/n}\mu(d)\,d^s\right]\Big|_{s=0} =$$

$$= \frac{d^2}{ds^2}\left[\prod_{p/n}(1-p^s)\right]_{s=0} = \begin{cases} -\ln^2 p, & n=p^k, \\ 2\ln p\ln q, & n=p^k q^r, \\ 0, & p_1p_2p_3/n, \end{cases} \quad (3,3,13)$$

где p, q, p_1, p_2, p_3 — различные простые числа. Поэтому

$$\sum_{n\leqslant x}\sum_{d/n}\mu(d)\ln^2\frac{x}{d} = \ln^2 x + 2\ln x\sum_{n\leqslant x}\Lambda(n) +$$

$$+\sum_{nm\leqslant x}\Lambda(n)\Lambda(m) - \sum_{n\leqslant x}\Lambda(n)\ln n = 2\ln x\,\psi(x) -$$

$$-\ln x\,\psi(x) + \sum_{nm\leqslant x}\Lambda(n)\Lambda(m) + O(x) =$$

$$= \psi(x)\ln x + \sum_{n\leqslant x}\Lambda(n)\,\psi\left(\frac{x}{n}\right) + O(x) = \psi(x)\ln x +$$

$$+\sum_{nm\leqslant x}\Lambda(n)\Lambda(m) + O(x), \quad (3,3,14)$$

так как

$$\sum_{n\leqslant x}\Lambda(n)\ln n = \sum_{n\leqslant x}[\psi(n)-\psi(n-1)]\ln n = \psi(x)\ln x -$$

$$-\sum_{n\leqslant x-1}\psi(n)\ln\left(1+\frac{1}{n}\right) + O(1) = \psi(x)\ln x + O(x)$$

в силу (3,1,6). Далее,

$$\sum_{n\leqslant x}\sum_{d/n}\mu(d)\ln^2\frac{x}{d} = \sum_{n\leqslant x}\mu(n)\ln^2\frac{x}{n}\left[\frac{x}{n}\right] =$$

$$= x\sum_{n\leqslant x}\frac{\mu(n)}{n}\ln^2\frac{x}{n} - \sum_{n\leqslant x}\mu(n)\left\{\frac{x}{n}\right\}\ln^2\frac{x}{n}.$$

Воспользуемся теперь соотношением

$$\sum_{n\leqslant x}\frac{1}{n}\sum_{d/n}\mu(d)\ln\frac{x}{d}=\ln x+\sum_{n\leqslant x}\frac{\Lambda(n)}{n}=2\ln x+O(1)=$$

$$=\sum_{n\leqslant x}\frac{\mu(n)}{n}\ln\frac{x}{n}\sum_{k\leqslant\frac{x}{n}}\frac{1}{k}=\sum_{n\leqslant x}\frac{\mu(n)}{n}\ln\frac{x}{n}\left[\ln\frac{x}{n}+C+O\left(\frac{n}{x}\right)\right]=$$

$$=\sum_{n\leqslant x}\frac{\mu(n)}{n}\ln^2\frac{x}{n}+C\sum_{n\leqslant x}\frac{\mu(n)}{n}\left[\sum_{k\leqslant\frac{x}{n}}\frac{1}{k}-C+O\left(\frac{n}{x}\right)\right]+$$

$$+O\left[\frac{1}{x}\sum_{n\leqslant x}\ln\frac{x}{n}\right]=\sum_{n\leqslant x}\frac{\mu(n)}{n}\ln^2\frac{x}{n}+O(1).$$

верным в силу (3,1,2), (3,1,4), (3,1,5), (3,1,6) и неравенством

$$\left|\sum_{n\leqslant x}\mu(n)\left\{\frac{x}{n}\right\}\ln^2\frac{x}{n}\right|<\sum_{n\leqslant x}\ln^2\frac{x}{n}=O(x).$$

Мы будем тогда иметь оценку

$$\sum_{n\leqslant x}\sum_{d/n}\mu(d)\ln^2\frac{x}{d}=2x\ln x+O(x),\qquad(3,4,15)$$

откуда следует, что

$$\psi_1(x)=\sum_{nm\leqslant x}\Lambda(n)\Lambda(m)=$$

$$=2x\ln x-\psi(x)\ln x+O(x).\qquad(3,3,16)$$

Введем теперь в рассмотрение функцию $\psi_2(x)$,

$$\psi_2(x)=\sum_{nm\leqslant x}\frac{\Lambda(n)\Lambda(m)}{\ln nm}=\sum_{n\leqslant x}\frac{\psi_1(n)-\psi_1(n-1)}{\ln n}=$$

$$=\frac{\psi_1(x)}{\ln x}+\sum_{k\leqslant x-1}\psi(k)\left[\frac{1}{\ln k}-\frac{1}{\ln(k+1)}\right]+O(\ln x)=$$

$$=2x-\psi(x)+O\left(\frac{x}{\ln x}\right)+\sum_{n\leqslant x-1}\frac{2n\ln n-\psi(n)\ln n+O(n)}{n\ln^2(n+1)}=$$

$$=2x-\psi(x)+O\left(\frac{x}{\ln x}\right).\qquad(3,3,17)$$

Тогда

$$\psi_2(x)+\psi(x)=\sum_{n\leqslant x}\Lambda(n)+\sum_{nm\leqslant x}\frac{\Lambda(n)\Lambda(m)}{\ln nm}=$$

$$=2x+O\left(\frac{x}{\ln x}\right). \quad (3,3,18)$$

Рассмотрим теперь соотношение

$$R_l(x)=\sum_{\substack{n\leqslant x\\ n\equiv l\,(\mathrm{mod}\,D)}}\sum_{d/n}\mu(d)\ln^2\frac{x}{d}=2\ln x\sum_{\substack{n\leqslant x\\ n\equiv l\,(\mathrm{mod}\,D)}}\Lambda(n)-$$

$$-\sum_{\substack{n\leqslant x\\ n\equiv l\,(\mathrm{mod}\,D)}}\Lambda(n)\ln n+\sum_{\substack{nm\leqslant x\\ nm\equiv l\,(\mathrm{mod}\,D)}}\Lambda(n)\Lambda(m)+O(\ln x)=$$

$$=\psi(l,x)\ln x+\sum_{\substack{mn\leqslant x\\ mn\equiv l\,(\mathrm{mod}\,D)}}\Lambda(n)\Lambda(m)+O(x),$$

верное вследствие того, что

$$\sum_{\substack{n\leqslant x\\ n\equiv l\,(\mathrm{mod}\,D)}}\Lambda(n)\ln n=\psi(l,x)\ln x-\sum_{n\leqslant x}\frac{1}{n}\frac{\psi(l,n)}{n}+O(1)=$$

$$=\psi(l,x)\ln x+O(x).$$

Прежде всего заметим, что при $q>1$

$$\sum_{\substack{q/n\\ n\leqslant x}}\sum_{d/n}\mu(d)\ln^2\frac{x}{d}=2\ln x\sum_{\substack{n<x\\ d/n}}\Lambda(n)+O(\ln x)-$$

$$-\sum_{\substack{n\leqslant x\\ q/n}}\Lambda(n)\ln n+\sum_{\substack{mn\leqslant x\\ q/mn}}\Lambda(n)\Lambda(m)=O(\ln^2 x)+$$

$$+O\left[\sum_{n\leqslant x}\Lambda(n)\ln\frac{x}{n}\right]+O\left[\sum_{p\leqslant x}\sum_{k=2}^{\infty}\ln p\left[\frac{x}{p^k}\right]\right]=O(x),$$

$$\sum_{n<x}\Lambda(n)\sum_{\substack{mn\leqslant x\\ q/mn}}\Lambda(m)=\sum_{\substack{mn\leqslant x\\ q/mn}}\Lambda(n)\Lambda(m).$$

Поэтому, если χ_0 — главный характер модуля D, то при $D = p_1^{\alpha_1} \cdots p_\nu^{\alpha_\nu}$

$$\sum_{n \leqslant x} \chi_0(n) \sum_{d/n} \mu(d) \ln^2 \frac{x}{d} = \sum_{m/D} \mu(m) \sum_{\substack{n \leqslant x \\ m/n}} \sum_{d/n} \mu(d) \ln^2 \frac{x}{d} =$$

$$= \sum_{n \leqslant x} \sum_{d/n} \ln^2 \frac{x}{d} + O(x) = 2x \ln x + O(x)$$

в силу (3,3,15). Далее, если $\chi(n)$ — неглавный характер модуля D, то

$$\sum_{n \leqslant x} \chi(n) \sum_{d/n} \mu(d) \ln^2 \frac{x}{d} = \sum_{d \leqslant x} \mu(d) \ln^2 \frac{x}{d} \sum_{k \leqslant \frac{x}{d}} \chi(k) =$$

$$= O\left(\sum_{n \leqslant x} \ln^2 \frac{x}{n} \right) = O(x).$$

Отсюда мы уже получаем окончательно, что при $l' l \equiv 1 \pmod D$

$$R_l(x) = \frac{1}{\varphi(D)} \sum_{\chi} \chi(l') \sum_{n \leqslant x} \chi(n) \sum_{d/n} \mu(d) \ln^2 \frac{x}{d} = \frac{2x \ln x}{\varphi(D)} + O(x).$$

Значит, мы имеем

$$\sum_{\substack{nm \leqslant x \\ nm \equiv l \pmod D}} \Lambda(n) \Lambda(m) = \psi_1(l, x) = \frac{2}{h} x \ln x -$$

$$- \psi(l, x) \ln x + O(x),$$

$$h = \varphi(D). \qquad (3,3,19)$$

Воспользовавшись этим соотношением, мы получим также

$$\psi_2(l, x) = \sum_{\substack{nm \leqslant x \\ nm \equiv l \pmod D}} \frac{\Lambda(n) \Lambda(m)}{\ln nm} = \sum_{n \leqslant x} \frac{\psi_1(l, n) - \psi_1(l, n-1)}{\ln n} =$$

$$= \frac{\psi_1(l, x)}{\ln x} + \sum_{n \leqslant x} \frac{\psi_1(l, n)}{n \ln^2 n} + O(1) =$$

$$= - \psi(l, x) + \frac{2}{\varphi(D)} x + O\left(\frac{x}{\ln x} \right), \qquad (3,3,20)$$

откуда уже следует соотношение

$$\psi(l,x)+\psi_2(l,x)=\frac{2}{\varphi(D)}x+O\left(\frac{x}{\ln x}\right). \qquad (3,3,21)$$

Далее, мы будем иметь

$$\sum_{n\leqslant x}\mu(n)\ln\frac{x}{n}=O\Big(\sum_{n\leqslant x}\ln\frac{x}{n}\Big)=O(x)=M(x)\ln x-$$

$$-\sum_{n\leqslant x}\mu(n)\sum_{d/n}\Lambda(d)=M(x)\ln x-\sum_{n\leqslant x}\Lambda(n)\sum_{k\leqslant\frac{x}{n}}\mu(nk)=$$

$$=M(x)\ln x-\sum_{p\leqslant x}\ln p\sum_{k\leqslant\frac{x}{p}}\mu(p\cdot k)=$$

$$=M(x)\ln x+\sum_{p\leqslant x}\ln p\,M\left(\frac{x}{p}\right)-\sum_{p\leqslant x}\ln p\sum_{k\leqslant\frac{x}{p^2}}\mu(k)=$$

$$=M(x)\ln x+\sum_{n\leqslant x}\Lambda(n)M\left(\frac{x}{n}\right)+O(x),$$

или

$$M(x)\ln x=-\sum_{n\leqslant x}\Lambda(n)M\left(\frac{x}{n}\right)+O(x)=$$

$$=-\sum_{n\leqslant x}\mu(n)\psi\left(\frac{x}{n}\right)+O(x). \qquad (3,3,22)$$

Вставляя в правую часть (3,3,22) вместо $\psi\left(\frac{x}{n}\right)$ его выражение из (3,3,18), мы будем иметь

$$M(x)\ln x=\sum_{n\leqslant x}\mu(n)\Big[\sum_{km\leqslant\frac{x}{n}}\frac{\Lambda(k)\Lambda(m)}{\ln km}-\frac{2x}{n}+$$

$$+O\left(\frac{x}{n\left[\ln\frac{x}{n}+1\right]}\right)\Big]=-2x\sum_{n\leqslant x}\frac{\mu(n)}{n}+$$

$$+\sum_{kmn\leqslant x}\frac{\Lambda(k)\Lambda(n)\mu(m)}{\ln km}+O\left[\sum_{n\leqslant x}\frac{x}{n\left(1+\ln\frac{x}{n}\right)}\right]=$$

$$=2xO(1)+\sum_{kn\leqslant x}\frac{\Lambda(k)\Lambda(n)}{\ln kn}M\left(\frac{x}{kn}\right)+O(x\ln\ln x)=$$

$$=\sum_{kn\leqslant x}\frac{\Lambda(k)\Lambda(n)}{\ln kn}M\left(\frac{x}{kn}\right)+O(x\ln\ln x),$$

так как

$$\sum_{n\leqslant x}\frac{x}{n\left(1+\ln\frac{x}{n}\right)}=\int_1^x\frac{x\,dt}{t\left(1+\ln\frac{x}{t}\right)}+O(x)=$$

$$=x\int_1^x\frac{dt}{t(1+\ln t)}+O(x)=x\ln\ln x+O(x). \quad (3,3,23)$$

Отсюда следует неравенство

$$|M(x)|\ln x\leqslant\sum_{kn\leqslant x}\frac{\Lambda(k)\Lambda(n)}{\ln kn}\left|M\left(\frac{x}{kn}\right)\right|+O(x\ln\ln x).$$

Складывая почленно это неравенство с получаемым непосредственно из (3,3,22) неравенством

$$|M(x)|\ln x\leqslant\sum_{n\leqslant x}\Lambda(n)\left|M\left(\frac{x}{n}\right)\right|+O(x\ln\ln x),$$

мы будем иметь, в силу (3,3,18),

$$2|M(x)|\ln x\leqslant\sum_{n\leqslant x}\Lambda(n)\left|M\left(\frac{x}{n}\right)\right|+$$

$$+\sum_{mn\leqslant x}\frac{\Lambda(n)\Lambda(m)}{\ln mn}\left|M\left(\frac{x}{mn}\right)\right|+O(x\ln\ln x)=$$

$$=\sum_{n\leqslant x}[\psi(n)+\psi_2(n)-\psi(n-1)-\psi_2(n-1)]\left|M\left(\frac{x}{n}\right)\right|+$$

$$+O(x\ln\ln x)<2\sum_{n\leqslant x}n\left[\left|M\left(\frac{x}{n}\right)\right|-\left|M\left(\frac{x}{n+1}\right)\right|\right]+$$

$$+O\left[\sum_{n\leqslant x}\frac{n}{1+\ln n}\left|M\left(\frac{x}{n}\right)-M\left(\frac{x}{n+1}\right)\right|\right]+O(x\ln\ln x)=$$

$$=2\sum_{n\leqslant x}\left|M\left(\frac{x}{n}\right)\right|+O\left[\sum_{n\leqslant x}\frac{n}{1+\ln n}\frac{x}{n(n+1)}\right]+O(x\ln\ln x)=$$

$$=2\sum_{n\leqslant x}\left|M\left(\frac{x}{n}\right)\right|+O(x\ln\ln x).$$

Итак, мы получили неравенство

$$|M(x)| \ln x \leqslant \sum_{n \leqslant x} \left| M\left(\frac{x}{n}\right)\right| + O(x \ln \ln x). \quad (3,3,24)$$

Аналогичные неравенства мы получим теперь для $|M(l, x)|$.

§ 4. Основные неравенства для оценки числа простых в прогрессиях

Когда мы доказывали теорему 3. 2. 1, то мы попутно доказали, что

$$L(\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = \sum_{n=1}^{N} \frac{\chi(n)}{n} + O\left(\frac{1}{N}\right) \neq 0 \quad (3,4,1)$$

для всякого неглавного характера модуля D. Воспользовавшись этим, мы будем иметь

$$1 = \sum_{n \leqslant x} \frac{\chi(n)}{n} \sum_{d|n} \mu(d) = \sum_{n \leqslant x} \frac{\chi(n)\mu(n)}{n} \sum_{k \leqslant \frac{x}{n}} \frac{\chi(k)}{k} =$$

$$= \sum_{n \leqslant x} \frac{\chi(n)\mu(n)}{n} \left[L(\chi) + O\left(\frac{n}{x}\right)\right] + O(1) =$$

$$= L(\chi) \sum_{n \leqslant x} \frac{\chi(n)\mu(n)}{n} + O(1),$$

откуда следует, что

$$\sum_{n \leqslant x} \frac{\chi(n)\mu(n)}{n} = O(1) \quad (3,4,2)$$

для всякого неглавного характера модуля D. Если же $\chi_0(n)$ — главный характер модуля D, то

$$1 = \sum_{n \leqslant x} \chi_0(n) \sum_{d|n} \mu(d) = \sum_{n \leqslant x} \chi_0(n)\mu(n) \sum_{k \leqslant \frac{x}{n}} \chi_0(k) =$$

$$= \sum_{n \leqslant x} \chi_0(n)\mu(n) \sum_{d|D} \mu(d)\left[\frac{x}{nd}\right] =$$

$$= \sum_{d|D} \mu(d) \sum_{n \leqslant x} \chi_0(n)\mu(n)\left[\frac{x}{nd} - \left\{\frac{x}{nd}\right\}\right] =$$

$$= x \sum_{d|D} \frac{\mu(d)}{d} \sum_{n \leqslant x} \frac{\chi_0(n)\mu(n)}{n} + O(x) =$$

$$= \frac{\varphi(D)}{D} x \sum_{n \leqslant x} \frac{\chi_0(n)\mu(n)}{n} + O(x),$$

откуда следует, что

$$\sum_{n \leqslant x} \frac{\chi_0(n)\mu(n)}{n} = O(1), \qquad (3,4,3)$$

так как $\varphi(D) \neq 0$.

Далее, из (3,4,2) и (3,4,3) мы получаем также, что

$$\sum_{\substack{n \leqslant x \\ n \equiv l \pmod D}} \frac{\mu(n)}{n} = \frac{1}{\varphi(D)} \sum_{\chi} \chi(l') \sum_{n \leqslant x} \frac{\chi(n)\mu(n)}{n} = O(1), \qquad (3,4,4)$$

где $(l, D) = 1$, $ll' \equiv 1 \pmod D$ и сумма взята по всем характерам модуля D.

Рассмотрим теперь, при $(l, D) = 1$, соотношение

$$\sum_{\substack{n \equiv l \pmod D \\ n \leqslant x}} \mu(n) \ln \frac{x}{n} = M(l, x) \ln x - \sum_{\substack{n \leqslant x \\ n \equiv l \pmod D}} \mu(n) \sum_{d|n} \Lambda(d) =$$

$$= M(l, x) \ln x - \sum_{n \leqslant x} \Lambda(n) \sum_{\substack{kn \leqslant x \\ kn \equiv l \pmod D}} \mu(kn) =$$

$$= M(l, x) \ln x - \sum_{p \leqslant x} \ln p \sum_{\substack{pn \leqslant x \\ pn \equiv l \pmod D}} \mu(pn) =$$

$$= M(l, x) \ln x + \sum_{\substack{p \leqslant x \\ (p,D)=1}} \ln p\, M\left(p'l, \frac{x}{p}\right) - \sum_{\substack{p \leqslant x \\ (p,D)=1}} \times$$

$$\times \ln p \sum_{\substack{p^2 k \equiv l \pmod D \\ p^2 k \leqslant x}} \mu(pk) = M(l, x) \ln x +$$

$$+ \sum_{\substack{n \leqslant x \\ (n,D)=1}} \Lambda(n)\, M\left(n'l, \frac{x}{n}\right) + O(x)$$

$$pp' \equiv 1 \pmod D, \quad nn' \equiv 1 \pmod D,$$

откуда непосредственно следует, что

$$M(l, x)\ln x+\sum_{n\leqslant x}\chi_0(n)\Lambda(n)M\left(n'l, \frac{x}{n}\right)=$$

$$=M(l, x)\ln x+\sum_{n\leqslant x}\mu(n)\sum_{\substack{kn\leqslant x\\ kn\equiv l\,(\mathrm{mod}\,D)}}\Lambda(k)+O(x)=$$

$$=M(l, x)\ln x+\sum_{n\leqslant x}\chi_0(n)\mu(n)\,\psi\left(n'l, \frac{x}{n}\right)+O(x), \quad (3,4,5)$$

где опять $nn'\equiv 1\,(\mathrm{mod}\,D)$. Из этого соотношения следует прежде всего неравенство

$$|M(l,x)|\ln x\leqslant\sum_{n\leqslant x}\Lambda(n)\left|\mu\left(n'l, \frac{x}{n}\right)\right|+O(x), \quad (3,4,6)$$

где опять $nn'\equiv 1 \bmod D$. Вставляя теперь в правую часть (3,4,5) вместо $\psi\left(n'l, \frac{x}{n}\right)$ его выражение из (3,3,21), мы будем иметь

$$M(l,x)\ln x+\sum_{n\leqslant x}\chi_0(n)\mu(n)\left[\frac{2}{\varphi(D)}\frac{x}{n}+O\left(\frac{x}{n\left(1+\ln\frac{x}{n}\right)}\right)\right]-$$

$$-\sum_{n\leqslant x}\chi_0(n)\mu(n)\sum_{\substack{km\leqslant x\\ nkm\equiv l\,(\mathrm{mod}\,D)}}\frac{\Lambda(k)\Lambda(m)}{\ln km}+O(x)=M(l,x)\ln x-$$

$$-\sum_{\substack{kmn\leqslant x\\ kmn\equiv l\,(\mathrm{mod}\,D)}}\frac{\Lambda(k)\Lambda(m)\mu(n)}{\ln km}+\frac{2x}{\varphi(D)}\sum_{n\leqslant x}\frac{\gamma_0(n)\mu(n)}{n}+$$

$$+O(x\ln\ln x)=M(l, x)\ln x-\sum_{\substack{km\leqslant x\\ (km, D)=1}}\frac{\Lambda(k)\Lambda(m)}{\ln km}\times$$

$$\times M\left((km)'l, \frac{x}{n}\right)+O(x\ln\ln x),$$

откуда уже следует неравенство

$$|M(l,x)|\ln x\leqslant\sum_{km\leqslant x}\chi_0(km)\frac{\Lambda(k)\Lambda(m)}{\ln km}\left|M(km)'l, \frac{x}{n}\right)\Big|+$$

$$+O(x\ln\ln x), \quad (3,4,7)$$

где $(km)'\,km\equiv 1\,(\mathrm{mod}\,D)$. Складывая (3,4,7) и (3,4,5), мы

будем иметь теперь, что

$$2\,|M(l,x)|\ln x \leqslant \sum_{n\leqslant x}\chi_0(n)\Lambda(n)\left|M\left((n'l,\frac{x}{n}\right)\right|+$$

$$+\sum_{mn\leqslant x}\chi_0(mn)\frac{\Lambda(n)\Lambda(m)}{\ln mn}\left|M\left((nm)'l,\frac{x}{n}\right)\right|+O(x\ln\ln x), \quad (3,4,8)$$

где опять $nn'\equiv 1 \pmod D$, $(nm)'mn\equiv 1 \pmod D$. Далее, отсюда следует, что

$$2\,|M(l,x)|\ln x<\sum_{q=1}^{D}\chi_0(q)\sum_{\substack{n\equiv q \pmod D\\ n\leqslant x}}\Lambda(n)\left|M\left(q'l,\frac{x}{n}\right)\right|+$$

$$+\sum_{q=1}^{D}\chi_0(q)\sum_{\substack{mn\equiv q \pmod D\\ mn\leqslant x}}\frac{\Lambda(n)\Lambda(m)}{\ln nm}\left|M\left((q'l,\frac{x}{mn}\right)\right|+O(x\ln\ln x)=$$

$$=\sum_{q=1}^{D}\chi_0(q)\sum_{\substack{n\equiv q \pmod D\\ n\leqslant x}}[\psi(q,n)+\psi_2(q,n)-\psi(q,n-D)-$$

$$-\psi_2(q,n-D)]\left|M\left(q'l,\frac{x}{n}\right)\right|+O(x\ln\ln x)\leqslant\frac{2D}{\varphi(D)}\times$$

$$\times\sum_{q=1}^{D}\chi_0(q)\sum_{\substack{n\equiv q \pmod D\\ n\leqslant x}}\left|M\left(q'l,\frac{x}{n}\right)\right|+\frac{2D}{\varphi(D)}\sum_{1}^{D}\chi_0(q)\times$$

$$\times\sum_{\substack{n\equiv q \pmod D\\ n\leqslant x}}O\left(\frac{n}{1+\ln n}\right)\left|\left|M\left(q'l,\frac{x}{n}\right)\right|-\left|M\left(q'l,\frac{x}{n+D}\right)\right|\right|+$$

$$+O(x\ln\ln x)$$

в силу (3,3,21), где $qq'\equiv 1 \pmod D$. Но так как

$$\sum_{q=1}^{D}\chi_0(q)\sum_{\substack{n\equiv q \pmod D\\ n\leqslant x}}O\left(\frac{n}{1+\ln n}\right)\left|\left|M\left(q'l,\frac{x}{n}\right)\right|-\left|M\left(q'l,\frac{x}{n+D}\right)\right|\right|<$$

$$<\sum_{1}^{D}\chi_0(q)\sum_{\substack{n\equiv q \pmod D\\ n\leqslant x}}O\left(\frac{n}{1+\ln n}\right)\frac{Dx}{n(n+D)}=O\left(x\sum_{n\leqslant x}\frac{1}{n\ln n}\right)=$$

$$=O(x\ln\ln x),$$

то, следовательно,

$$|M(l,x)|\ln x \leqslant \frac{D}{\varphi(D)}\sum_{1}^{D}\chi_0(q)\sum_{\substack{n\leqslant x\\ n\equiv q \pmod D}}\left|M\left(q'l,\frac{x}{n}\right)\right| + \\ + O(x\ln\ln x).$$

Но легко видеть, что при $(l, D)=1$

$$\left|D\sum_{\substack{n\equiv l \pmod D\\ n\leqslant x}}\left|M\left(l,\frac{x}{n}\right)\right| - \sum_{n\leqslant x}\left|M\left(l,\frac{x}{n}\right)\right|\right| \leqslant \\ \leqslant \left|\sum_{\substack{n\equiv q \pmod D\\ n\leqslant x}}\sum_{k=0}^{D-1}\left[\left|M\left(l,\frac{x}{n}\right)\right| - \left|M\left(l,\frac{x}{n+k}\right)\right|\right] + O(x)\right| = \\ = O\left[\sum_{n\leqslant x}\frac{x}{n(n+1)}\right] + O(x) = O(x).$$

Поэтому окончательно для любого l, $(l, D)=1$ имеем

$$\left|M(l,x)\right|\ln x \leqslant \frac{1}{\varphi(D)}\sum_{q=1}^{D}\chi_0(q)\sum_{n\leqslant x}\left|M\left(q,\frac{x}{n}\right)\right| + \\ + O(x\ln\ln x). \qquad (3,4,9)$$

§ 5. Доказательство предельных теорем для распределения простых в натуральном ряде и прогрессиях

Неравенства (3,3,24) и (3,4,9) позволят нам доказать оценки $M(x)=o(x)$ и $M(l, x)=o(x)$ для всех l и D, если добавить к ним соображения, учитывающие колебания функций $M(x)$ и $M(l, x)$. Прежде всего из неравенства (3,1,4) следует, что

$$\left|\sum_{n\leqslant x}\frac{M(n)-M(n-1)}{n}\right| = \left|\sum_{n\leqslant x}\frac{M(n)}{n(n+1)} + \frac{M(x)}{x}\right| < 1,$$

или что

$$\left|\sum_{y\leqslant n\leqslant x}\frac{M(n)}{n(n+1)}\right| < 4. \qquad (3,5,1)$$

Совершенно так же из оценок (3,4,2) и (3,4,3) следует, что при $(l, D)=1$

$$\sum_{\substack{n\leqslant x\\ n\equiv l\,(\mathrm{mod}\,D)}}\frac{\mu(n)}{n}=\frac{1}{\varphi(D)}\sum_{\chi}\chi(l')\sum_{n\leqslant x}\frac{\chi(n)\,\mu(n)}{n}=O(1),$$

где $ll'\equiv 1\,(\mathrm{mod}\,D)$ и сумма справа взята по всем характерам модуля D. Это соотношение в свою очередь приводит к оценке

$$\left|\sum_{y\leqslant n\leqslant x}\frac{M(l,n)}{n(n+1)}\right|=\left|\frac{M(l,y)}{y}-\frac{M(l,x)}{x+1}-\sum_{\substack{n\leqslant x\\ n\equiv l\,(\mathrm{mod}\,D)}}\frac{\mu(n)}{n}+\right.$$

$$\left.+\sum_{\substack{n\leqslant y\\ n\equiv l\,(\mathrm{mod}\,D)}}\frac{\mu(n)}{n}\right|<C, \quad (3,5,2)$$

где $C=C(D)$ — постоянная, от x и l не зависящая.

Неравенства (3,5,1) и (3,5,2) приводят нас к следующей лемме.

Лемма 2. *Если* $x>t>1$, *то на интервале* $[x, tx]$ *найдется точка* q *такая, что*

$$|M(q)|<\frac{5q}{\ln t}. \quad (3,5,3)$$

Совершенно так же, если $x>t>1$, *то на интервале* $[x, tx]$ *найдется такая точка* q, *что*

$$|M(l, q)|<\frac{Cq}{\ln t},\ C=C(D), \quad (3,5,4)$$

где C *не зависит от* l, t *и* x, $(l, D)=1$.

Если $M(x)$ меняет знак на $[x, tx]$, то есть точка q такая, в которой или $M(q)=0$ или $M(q)M(q+1)<0$. Но второй случай невозможен, так как $M(q)$ отличается от $M(q+1)$ не более чем на единицу и оба целые числа. Значит, если $M(q)$ меняет знак на $[x, tx]$, то есть точка q, в которой $M(q)=0$. Если же на $[x, tx]$ $M(x)$ не меняет знака, то из (3,5,1) имеем, что

$$\min_{x\leqslant y\leqslant tx}\left|\frac{M(y)}{y}\right|\sum_{x\leqslant k\leqslant tx}\frac{1}{k}\leqslant\min_{x\leqslant y\leqslant tx}\frac{|M(y)|}{y}\left[\ln t-\frac{1}{x}\right]<4,$$

откуда и следует (3,5,3). Далее, если $M(l, x)$ меняет на $[x, tx]$ знак, то, так же как и в предшествующем случае, есть такое q на $[x, tx]$, что $M(l, q)=0$. Если же $M(l, q)$ не меняет знака на $[x, tx]$, то опять из (3,5,2)

$$\min_{x\leqslant y\leqslant tx}\frac{|M(l,y)|}{y}\sum_{x\leqslant k\leqslant tx}\frac{1}{k}<\min_{x\leqslant y\leqslant tx}\frac{|M(l,y)|}{y}\left[\ln t-\frac{1}{x}\right]<C_0,$$

где C_0 зависит только от D. Это неравенство эквивалентно (3,5,4).

Лемма 3. *Имеет место оценка* $M(x)=o(x)$.

Полагая $U(x)=\frac{1}{x}|M(x)|$, мы будем иметь из (3,4,24), разделив обе его части на $x\ln x$, что

$$U(x)\leqslant\frac{1}{\ln x}\sum_{n\leqslant x}\frac{1}{n}U\left(\frac{x}{n}\right)+O\left(\frac{\ln\ln x}{\ln x}\right). \tag{3,5,5}$$

Пусть

$$\theta=\overline{\lim_{x\to\infty}}\,U(x)>0.$$

Тогда при любом ε, $\theta>\varepsilon>0$ и $x>x_0(\varepsilon)$, $U(x)<\theta+\varepsilon$. Фуксируя ε, мы выбираем t, заставляя его только подчиняться условиям

$$t>e^6, \qquad 20<\theta\ln t. \tag{3,5,6}$$

В силу леммы 2 мы можем утверждать, что найдется такое q_k, $t^{2k}\leqslant q_k\leqslant t^{2k+1}$, для которого $|M(q_k)|<\frac{5q_k}{\ln t}$. Но тогда

$$|M(q_k+v)|<|M(q_k)|+v<\frac{5q_k}{\ln t}+v<\frac{10q_k}{\ln t},$$

если $v\ln t<5q_k$. Поэтому, если $0\leqslant v\leqslant\left[\frac{5q_k}{\ln t}\right]$, то

$$U(q_k+v)<\frac{10}{\ln t}.$$

Но числа n, удовлетворяющие неравенствам

$$q_k\leqslant\frac{x}{n}\leqslant q_k+\frac{5q_k}{\ln t}=\left(1+\frac{5}{\ln t}\right)q_k, \tag{3,5,7}$$

определяются из неравенств

$$p_k=\left[\frac{1}{1+\frac{5}{\ln t}}\frac{x}{q_k}\right]\leqslant n\leqslant\left[\frac{x}{q_k}\right]=p'_k<p_{k+1}. \quad (3,5,8)$$

Далее,

$$\sum_{p_k\leqslant n\leqslant p'_k}\frac{1}{n}=\ln\frac{p'_k}{p_k}+\alpha_k\frac{q_k}{x}=\ln\left(1+\frac{5}{\ln t}\right)+\beta_k\frac{q_k}{x},$$

$$|\beta_k|\leqslant 3. \quad (3,5,9)$$

Значит, когда n удовлетворяет неравенствам (3,5,8), то $U\left(\frac{x}{n}\right)\leqslant\frac{10}{\ln t}$. Заметив, что при $m=\left[\frac{1}{2}\frac{\ln x}{\ln t}-\frac{1}{2}\right]$

$$\sum_{k=1}^{m}\sum_{p_k\leqslant n\leqslant p'_k}\frac{1}{n}=m\ln\left(1+\frac{5}{\ln t}\right)+\sum_{1}^{m}\beta_k\frac{q_k}{x}=$$

$$=\frac{\ln x}{2\ln t}\ln\left(1+\frac{5}{\ln t}\right)+O\left(\sum_{1}^{m}|\beta_k|\frac{t^{2k}}{x}\right)+O(1)=$$

$$=\lambda\ln x+O(1)\ (\lambda>0), \quad (3,5,10)$$

мы непосредственно получаем из (3,5,5), заменяя $U\left(\frac{x}{n}\right)$ на $\frac{10}{\ln t}$ для всех n, удовлетворяющих неравенствам (3,5,8), и на $0+\varepsilon$ для остальных n, что

$$U(x)\leqslant\frac{\theta+\varepsilon}{\ln x}\left[\sum_{n\leqslant x}\frac{1}{n}-\sum_{k=1}^{m}\sum_{p_k\leqslant n\leqslant p'_k}\frac{1}{n}\right]+$$

$$+\frac{10}{\ln t\ln x}\sum_{1}^{m}\sum_{p_k\leqslant n\leqslant p'_k}\frac{1}{n}+O\left(\frac{\ln\ln x}{\ln x}\right)\leqslant$$

$$\leqslant(\theta+\varepsilon)(1-\lambda)+\frac{10\lambda}{\ln t}+O\left(\frac{\ln\ln x}{\ln x}\right).$$

Отсюда уже непосредственно следует верное при любых ε и $t>D_0$ неравенство, получаемое переходом к верхнему пределу слева,

$$\theta\leqslant(\theta+\varepsilon)(1-\lambda)+\frac{10\lambda}{\ln t},\qquad \lambda=\frac{5}{2}\frac{1}{\ln^2 t}+O\left(\frac{1}{\ln^3 t}\right).$$

Но тогда можно положить $\varepsilon \to 0$, и мы приходим к противоречивому, при достаточно больших t и $\theta > 0$, неравенству

$$\theta \leqslant \theta(1-\lambda) + \frac{10\lambda}{\ln t} < \theta\left(1 - \frac{\lambda}{2}\right), \qquad \ln t > \frac{20}{\theta}\ (t > t_0).$$

Значит, $\theta = 0$ и $M(x) = o(x)$.

Лемма 4. *Если* $(l, D) = 1$, $D > 1$, *то имеет место оценка* $M(l, x) = o(x)$.

Доказательство этой леммы ничем не отличается от доказательства леммы 3. Из неравенств (3, 4, 9), полагая $h = \varphi(D)$, $U_l(x) = \frac{1}{x}|M(l, x)|$, получаем неравенства

$$U_l(x) \leqslant \frac{1}{h \ln x} \sum_{q=1}^{D} \chi_0(q) \sum_{n \leqslant x} \frac{1}{n} U_q\left(\frac{x}{n}\right) + O\left(\frac{\ln \ln x}{\ln x}\right), \quad (3,5,11)$$

верные для любого l, $(l, D) = 1$. Опять полагаем

$$\theta = \overline{\lim_{x \to \infty}} \max_{1 \leqslant q \leqslant D} |\chi(q)\, U_q(x)|.$$

Тогда, при любом ε, $\theta > \varepsilon > 0$, $x \geqslant x_0(\varepsilon)$, $U_l(x) < \theta + \varepsilon$. $\theta - \varepsilon < \max\limits_{1 \leqslant q \leqslant D} \chi(q)\, U_q(x_k)$ для бесчисленного множества неограниченно растущих x_k.

По лемме 2 выбираем числа q_k из интервала $t^{2k} \leqslant q_k \leqslant t^{2k+1}$ такие, что

$$|M_l(q_k)| < \frac{Cq_k}{\ln t}; \quad |M_l(q_k + v)| < \frac{Cq_k}{\ln t} + v < \frac{2Cq_k}{\ln t},$$

если $v \ln t < Cq_k$. Значит, для $0 \leqslant v \leqslant \left[\frac{Cq_k}{\ln t}\right]$

$$U_l(q_k + v) < \frac{2C}{\ln t}.$$

Но для того чтобы $\frac{x}{n}$ находилось в границах

$$q_k \leqslant \frac{x}{n} \leqslant \left(1 + \frac{C}{\ln t}\right) q_k, \quad (3,5,12)$$

число n должно удовлетворять неравенствам

$$p_k = \left[\frac{1}{1 + \frac{C}{\ln t}} \frac{x}{q_k}\right] \leqslant n \leqslant \left[\frac{x}{q_k}\right] = p'_k < p_{k+1}. \quad (3,5,13)$$

Аналогично (3, 5, 9) мы будем иметь

$$S_k = \sum_{p_k \leqslant n \leqslant p_k'} \frac{1}{n} = \ln \frac{p_k'}{p_k} + \alpha_k \frac{q_k}{x} = \ln\left(1 + \frac{C}{\ln t}\right) + \beta_k \frac{t^{2k+1}}{x}, \tag{3,5,14}$$

где $\beta_k = O(1)$ по отношению к x и t. Так как при n, удовлетворяющем неравенствам (3,5,13) $U_l(x) < \frac{2C}{\ln t}$ и при

$$m = \left[\frac{1}{2}\frac{\ln x}{\ln t} - \frac{1}{2}\right]$$

$$\sum_1^m S_k = m \ln\left(1 + \frac{C}{\ln t}\right) + \sum_{k=1}^m \beta_k \frac{t^{2k+1}}{x} = m \ln\left(1 + \frac{C}{\ln t}\right) + O(1) =$$

$$= \lambda \ln x + O(1), \quad \lambda = \frac{\ln\left(1 + \frac{C}{\ln t}\right)}{2 \ln t}, \tag{3,5,15}$$

то, заменяя в (3,5,11) $U_q\left(\frac{x}{n}\right)$ на $\frac{2C}{\ln t}$, если n удовлетворяет неравенствам (3,5,13), и через $\theta + \varepsilon$ в остальных случаях, мы получаем неравенство

$$\max_{\leqslant l \leqslant D} [\chi_0(l)\, U_l(x)] < \frac{1}{h \ln x}\left[(\theta + \varepsilon)\left[\sum_{n \leqslant x} \frac{1}{n} - \sum_{k=1}^m S_k\right] + \right.$$

$$\left. + \frac{2C}{\ln t} \sum_{k=1}^m S_k\right] + O\left(\frac{\ln \ln x}{\ln x}\right) =$$

$$= \frac{1}{h}(\theta + \varepsilon)(1 - \lambda) + \frac{2C\lambda}{\ln t} + O\left(\frac{\ln \ln x}{\ln x}\right), \quad h = \varphi(D). \tag{3,5,16}$$

Переходя к верхнему пределу слева, мы получаем неравенство

$$\theta \leqslant \frac{1}{h}(\theta + \varepsilon)(1 - \lambda) + \frac{2C\lambda}{\ln t}$$

или, так как $\varepsilon > 0$ произвольно, неравенство

$$\theta \leqslant \frac{1}{h}\theta(1 - \lambda) + \frac{2C\lambda}{\ln t} \leqslant \frac{1}{h}\theta\left(1 - \frac{\lambda}{2}\right),$$

верное при $\ln t > \frac{4Ch}{\theta}$.

Это последнее неравенство и показывает, что $\theta = 0$, другими словами, доказывает нашу лемму.

Из лемм 1, 3 и 4 непосредственно следует теорема 3.5.1.

Теорема 3.5.1. *Имеют место асимптотические оценки*

$$\pi(x) = \frac{x}{\ln x} + o\left(\frac{x}{\ln x}\right) \tag{3,5,17}$$

и

$$\pi(l, D; x) = \frac{1}{\varphi(D)} \frac{x}{\ln x} + o\left(\frac{x}{\ln x}\right), \tag{3,5,18}$$

где $(D, l) = 1$, *а* $\varphi(D)$ — *функция Эйлера.*

Заметим, что, проводя в леммах 1—4 немного более точные оценки, мы могли бы заменить $o\left(\frac{x}{\ln x}\right)$ в теореме (3,5,1) по крайней мере на $O\left(\frac{x}{\ln x}\sqrt{\frac{\ln\ln x}{\ln x}}\right)$. Но, по-видимому, существенно улучшить остаточный член в формулах (3,5,17) и (3,5,18), оставаясь в рамках метода А. Сельберга, нельзя, и с очень большим трудом его можно довести до $O\left(\frac{x}{\ln^{2-\varepsilon} x}\right)$ ($\varepsilon > 0$ произвольно). Изложенный метод доказательства предельных законов распределения простых найден А. Сельбергом [46], причем идея использования в этой схеме Сельберга $M(x)$ вместо $\psi(x) - x$ для доказательства закона распределения простых в натуральном ряде принадлежит А. Г. Постникову и Н. Н. Романову [22].

Элементарное доказательство теоремы Дирихле принадлежит Г. Шапиро [47]. Для получения в формулах (3, 5, 17) и (3, 5, 18) остаточного члена типа Адамара — Валле-Пуссена, другими словами, остаточного члена вида $O(xe^{-\lambda\ln^{\gamma}x})$, где $\lambda > 0$, $1 > \gamma > 0$, постоянные, можно использовать элементарно получаемую оценку (см. [7])

$$\sum_{n\leqslant x} \frac{\chi(n)\mu(n)}{n^{1+i\tau}} = O[\ln^{7}(2 + |\tau|)],$$

где χ — любой характер модуля D — и τ произвольно, но, к сожалению, переход от этой оценки к остаточным членам в (3,5,17) и (3,5,18) пока недостаточно элементарен и требует контурного интегрирования. Поэтому мы не будем останавливаться на вопросе об остаточном члене и займемся некоторыми другими вариантами вышеизложенных элементарных идей.

§ 6. О простых числах в последовательностях, несколько более общих, чем прогрессии

Докажем элементарно одну теорему о бесконечности простых чисел в рядах, отличающихся от прогрессий.

Пусть $\tau \neq 0$ и действительно. Положим

$$\alpha(\tau) = 1 + \frac{1}{i\tau} + \frac{1}{i\tau}\sum_{2}^{\infty}\left\{\frac{1}{i\tau}\left[n^{-i\tau} - (n-1)^{-i\tau}\right] + n^{-1-i\tau}\right\}. \quad (3,6,1)$$

Этот ряд сходится, так как

$$\frac{1}{i\tau}\left[n^{-i\tau} - (n-1)^{-i\tau}\right] + n^{-1-i\tau} = O\left(\frac{1}{n^2}\right). \quad (3,6,2)$$

Отсюда непосредственно следует, что

$$\sum_{n\leqslant x}\frac{1}{n^{1+i\tau}} = \frac{i}{\tau}x^{-i\tau} + \alpha(\tau) + O\left(\frac{1}{x}\right). \quad (3,6,3)$$

Далее, мы будем иметь

$$\sum_{n\leqslant x}\frac{\ln n}{n^{1+i\tau}} = \ln[x]\sum_{n\leqslant x}\frac{1}{n^{1+i\tau}} - \sum_{n\leqslant x}\ln\left(1+\frac{1}{n}\right)\sum_{k\leqslant n}\frac{1}{k^{1+i\tau}} =$$

$$= \frac{i}{\tau}x^{-i\tau}\ln x + \alpha(\tau)\ln x - \sum_{n\leqslant x}\frac{1}{n}\left[\frac{i}{\tau}n^{-i\tau} + \alpha(\tau)\right] +$$

$$+ O(1) = \frac{i}{\tau}x^{-i\tau}\ln x + O(1). \quad (3,6,4)$$

Рассмотрим простое тождество:

$$\sum_{n\leqslant x}\frac{\ln n}{n^{1+i\tau}} = \sum_{n\leqslant x}\frac{1}{n^{1+i\tau}}\sum_{d\mid n}\Lambda(d) = \sum_{n\leqslant x}\frac{\Lambda(n)}{n^{1+i\tau}}\sum_{k\leqslant\frac{x}{n}}\frac{1}{k^{1+i\tau}} =$$

$$= \frac{i}{\tau}\sum_{k\leqslant x}\frac{\Lambda(k)}{k^{1+i\tau}}\left(\frac{x}{k}\right)^{-i\tau} + \alpha(\tau)\sum_{n\leqslant x}\frac{\Lambda(n)}{n^{1+i\tau}} + \sum_{k\leqslant x}\frac{\Lambda(k)}{k^{1+i\tau}}\,O\left(\frac{k}{x}\right) =$$

$$= \frac{i}{\tau}x^{-i\tau}\ln x + \alpha(\tau)\sum_{n\leqslant x}\frac{\Lambda(n)}{n^{1+i\tau}} + O(1), \quad (3,6,5)$$

которое получается, если воспользоваться соотношениями (3,1,6) и (3,1,7).

Сопоставляя соотношения (3,6,4) и (3,6,5), мы видим, что

$$\alpha(\tau)\sum_{n\leqslant x}\frac{\Lambda(n)}{n^{1+i\tau}}=O(1). \tag{3,6,6}$$

Рассмотрим дополнительное тождество, именно:

$$\sum_{\leqslant x}\frac{1}{n^{1+i\tau}}\sum_{d\mid n}\mu(d)\ln\frac{x}{d}=\ln x+\sum_{n\leqslant x}\frac{\Lambda(n)}{n^{1+i\tau}}=$$

$$=\sum_{n\leqslant x}\frac{\mu(n)}{n^{1+i\tau}}\ln\frac{x}{n}\sum_{k\leqslant\frac{x}{n}}\frac{1}{k^{1+i\tau}}=\frac{i}{\tau}x^{-i\tau}\sum_{n\leqslant x}\frac{\mu(n)}{n}\ln\frac{x}{n}+$$

$$+\alpha(\tau)\sum_{n\leqslant x}\frac{\mu(n)}{n^{1+i\tau}}\ln\frac{x}{n}+\sum_{n\leqslant x}\frac{\mu(n)}{n^{1+i\tau}}\ln\frac{x}{n}\,O\left(\frac{n}{x}\right)=$$

$$=\alpha(\tau)\sum_{n\leqslant x}\frac{\mu(n)}{n^{1+i\tau}}\ln\frac{x}{n}+O(1). \tag{3,6,7}$$

так как

$$\frac{1}{x}\sum_{n\leqslant x}\ln\frac{x}{n}=O(1) \tag{3,6,8}$$

и

$$\sum_{n\leqslant x}\frac{\mu(n)}{n}\ln\frac{x}{n}=\frac{1}{x}\sum_{n\leqslant x}\mu(n)\left[\frac{x}{n}\right]\ln\frac{x}{n}-\frac{1}{x}\sum_{n\leqslant x}\mu(n)\left\{\frac{x}{n}\right\}\ln\frac{x}{n}=$$

$$=\frac{1}{x}\sum_{n\leqslant x}\sum_{d\mid n}\mu(d)\ln\frac{x}{d}+O(1)=$$

$$=\frac{1}{x}\sum_{n\leqslant x}\Lambda(n)+O(1)=O(1). \tag{3,6,9}$$

Сопоставляя (3,6,6) и (3,6,7), мы видим, что

$$\varphi(\tau,\ x)=\sum_{n\leqslant x}\frac{\Lambda(n)}{n^{1+i\tau}}=\delta(\tau)\ln x+O(1), \tag{3,6,10}$$

где

$$\delta(\tau)=\begin{cases}0, & \alpha(\tau)\neq 0,\\ -1, & \alpha(\tau)=0.\end{cases} \tag{3,6,11}$$

Покажем, что при любом $\tau \neq 0$ $\delta(\tau) = 0$, другими словами, что всегда $\alpha(\tau) \neq 0$. Действительно,

$$\operatorname{Re}[3\varphi(0, x) + 4\varphi(\tau, x) + \varphi(2\tau, x)] =$$
$$= 2\sum_{n \leqslant x} \frac{\Lambda(n)}{n} [\cos(\tau \ln n) + 1]^2 =$$
$$= [3 + 4\delta(\tau) + \delta(2\tau)] \ln x + O(1), \qquad (3,6,12)$$

откуда и следует, что $\delta(\tau) \neq -1$, так как слева стоит неотрицательная величина. Поэтому $\delta(\tau) = 0$; $\tau \neq 0$ и $\alpha(\tau) \neq 0$.

Значит, если $\tau \neq 0$, то

$$\sum_{n \leqslant x} \frac{\Lambda(n)}{n^{1+i\tau}} = O(1), \ \tau \neq 0; \ \sum_{n \leqslant x} \frac{\Lambda(n)}{n} = \ln x + O(1). \qquad (3,6,13)$$

Пусть теперь a и α действительны, $a > 0$ и $P(x)$ многочлен

$$P(z) = \sum_{k=-s}^{k=s} a_k z^k, \qquad a_0 = \int_0^1 P(e^{2\pi i t})\, dt.$$

На основании (3,6,13) будем иметь

$$\sum_{n \leqslant x} P\left[\left(\frac{n}{a}\right)^{2\pi i \alpha}\right] \frac{\Lambda(n)}{n} = \sum_{k=-s}^{s} a_k a^{-2\pi i k \alpha} \sum_{n \leqslant x} \frac{\Lambda(n)}{n^{1-2\pi i k \alpha}} =$$
$$= a_0 \ln x + O(1). \qquad (3,6,14)$$

Пусть $U(z)$ — периодическая действительная функция с периодом 1, $U(z+1) = U(z)$ — непрерывная, за исключением конечного числа точек разрыва первого рода на $[0,1]$. Как известно, для такой функции можно найти при любом $\varepsilon > 0$ два многочлена $P_1(z)$ и $P_2(z)$ таких, что

$$P_1(e^{2\pi i z}) \leqslant U(z) \leqslant P_2(e^{2\pi i z}), \qquad \int_0^1 |P_1(e^{2\pi i z}) - P_2(e^{2\pi i z})|\, dz < \varepsilon.$$

Поэтому

$$\sum_{n\leqslant x} P_1\left[\left(\frac{n}{a}\right)^{2\pi i\alpha}\right]\frac{\Lambda(n)}{n} \leqslant \sum_{n\leqslant x} U\left[\alpha \ln \frac{n}{a}\right]\frac{\Lambda(n)}{n} \leqslant$$

$$\leqslant \sum_{n\leqslant x} P_2\left[\left(\frac{n}{a}\right)^{2\pi i\alpha}\right]\frac{\Lambda(n)}{n},$$

откуда на основании (3,6,14) выводим

$$\int_0^1 P_1(e^{2\pi it})\,dt \ln x + O(1) \leqslant \sum_{n\leqslant x} U\left(\alpha \ln \frac{n}{a}\right)\frac{\Lambda(n)}{n} \leqslant$$

$$\leqslant \int_0^1 P_2(e^{2\pi it})\,dt \ln x + O(1).$$

Следовательно, так как ε может быть взято сколь угодно малым, мы можем утверждать, что

$$\sum_{n\leqslant x} U\left[\alpha \ln \frac{n}{a}\right]\frac{\Lambda(n)}{n} = \sum_{p\leqslant x} U\left(\alpha \ln \frac{p}{a}\right)\frac{\ln p}{p} + O(1) =$$

$$= \int_0^1 U(t)\,dt \ln x + O(\ln x). \qquad (3,6,15)$$

Соотношение (3,6,15) может быть использовано для доказательства теоремы типа Дирихле для одного класса числовых рядов, ранее уже рассматривавшихся А. О. Гельфондом *).

Пусть $m > 1$, $r \geqslant 1$, $q \geqslant 1$ — целые числа. Рассмотрим группу подстановок

$$L_k(x) = mx + qm + k \qquad (k = 0,1,\ldots, m-1).$$

Подставим r вместо x в наши линейные формы. Мы получим m чисел первой группы. Эти m чисел подставим в наши линейные формы. Мы получим m^2 целых чисел. Этот процесс мы продолжим неограниченно и получим числовой ряд L. Все числа этого ряда, как легко видеть, будут различны, что непосредственно следует из вида любого числа N, принадлежащего к ряду L, именно

$$N = m^s r + qm\,\frac{m^s - 1}{m-1} + \sum_{i=0}^{s-1} k_i m^i \qquad (s = 1,2\ldots),$$

*) См. литературу в работе [7].

где $k_l (l = 0,1,\ldots)$ — произвольные целые, $0 \leqslant k_l \leqslant m-1$. Поэтому N принадлежит к ряду L, если

$$m^s r + qm\frac{m^s-1}{m-1} \leqslant N \leqslant$$

$$\leqslant m^s(r+1) + qm\frac{m^s-1}{m-1} - 1 \qquad (3,6,16)$$

при каком угодно $s \geqslant 1$.

Неравенства (3,6,16) являются необходимыми и достаточными условиями принадлежности числа N к ряду L. Более подробно свойства рядов типа L рассмотрены в работе [7]. Нетрудно заметить, что множество целых чисел, удовлетворяющих условиям

$$N = m^s\left(r + \frac{qm}{m-1}\right) + t \quad (0 \leqslant t \leqslant m^s, s = 1,2,\ldots), \qquad (3,6,17)$$

где t — целое число, отличается от множества чисел, определяемых неравенствами (3, 6, 16), лишь на множество плотности геометрической прогрессии. Но условия (3,6,17) могут быть переписаны в форме

$$\frac{\ln \dfrac{N}{r + \dfrac{qm}{m-1}}}{\ln m} = s + \frac{\ln\left[1 + \dfrac{t}{\left(r + \dfrac{qm}{m-1}\right)m^s}\right]}{\ln m} \quad (0 \leqslant t \leqslant m^s),$$

другими словами, в форме

$$\left\{\frac{\ln \dfrac{N}{r + \dfrac{qm}{m-1}}}{\ln m}\right\} \leqslant \frac{1}{\ln m}\left\{\ln\left(1 + \frac{1}{r + \dfrac{qm}{m-1}}\right)\right\}. \qquad (3,6,18)$$

Поставим теперь вопрос о числе простых чисел в ряде L. Так как условие принадлежности числа N к L с точностью до множества чисел, образующих геометрическую прогрессию, есть условие (3, 6, 18), то определим функцию $U(x)$, положив

$$U(x) = \begin{cases} 1, & 0 \leqslant x \leqslant \dfrac{1}{\ln m}\ln\left(1 + \dfrac{1}{r + \dfrac{qm}{m-1}}\right) = x_0, \\ 0, & x_0 < x < 1, \end{cases}$$

$$U(x+1) = U(x).$$

Тогда условие принадлежности числа N к L с точностью до очень редкого множества будет иметь вид

$$U\left[\frac{\ln\left(\frac{N}{r+\frac{qm}{m-1}}\right)}{\ln m}\right]=1.$$

Воспользовавшись соотношением (3,3,8), получаем теорему

$$\sum_{\substack{p\leqslant x\\ p\in L}}\frac{\ln p}{p}=\frac{1}{\ln m}\ln\left(1+\frac{1}{r+\frac{qm}{m-1}}\right)\ln x+o(\ln x),$$

откуда, в частности, следует бесконечность простых чисел в ряду L. Естественно, что, используя закон распределения простых чисел с хорошим остаточным членом, мы можем найти число простых чисел до x в ряду L с большой точностью. Формула (3,6,16) может быть без всяких осложнений элементарно доказана и для арифметической прогрессии. Мы будем иметь тогда соотношение

$$\sum_{\substack{p\leqslant x\\ p\equiv l\,(\mathrm{mod}\,D)}}\frac{\ln p}{p}\,U\left[\alpha\ln\frac{n}{a}\right]=\frac{1}{\varphi(D)}\int_0^1 U(t)\,dt\,\ln x+o(\ln x),$$

откуда уже будет следовать и формула

$$\sum_{\substack{p\leqslant x\\ p\equiv l\,(\mathrm{mod}\,D),\ p\in L}}\frac{\ln p}{p}=\frac{1}{\varphi(D)\ln m}\ln\left(1+\frac{1}{r+\frac{qm}{m-1}}\right)\ln x+o(\ln x). \tag{3,6,19}$$

Докажем обобщение формулы (3,6,13), из которого непосредственно будет следовать и соотношение (3, 6, 19). Действительно, если $\chi\neq\chi_0$ и $\tau\neq 0$, то очевидно, что

$$\sum_{n\leqslant x}\frac{\chi(n)}{n^{1+i\tau}}=\alpha+O\left(\frac{1}{x}\right),\qquad \alpha=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^{1+i\tau}}. \tag{3,6,20}$$

Далее, будем иметь

$$\sum_{n\leqslant x}\frac{\chi(n)\ln n}{n^{1+i\tau}}=\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n^{1+i\tau}}\sum_{k\leqslant\frac{x}{n}}\frac{\chi(k)}{k^{1+i\tau}}=$$

$$=\alpha\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n^{1+i\tau}}+O(1)=O(1) \qquad (3,6,21)$$

в силу сходимости ряда в левой части (3,6,21).

Совершенно так же мы получаем

$$\sum_{n\leqslant x}\frac{\chi(n)}{n^{1+i\tau}}\sum_{d\mid n}\mu(d)\ln\frac{x}{d}=\ln x+\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n^{1+i\tau}}=$$

$$=\sum_{n\leqslant x}\frac{\chi(n)\mu(n)}{n^{1+i\tau}}\ln\frac{x}{n}\sum_{k\leqslant\frac{x}{n}}\frac{\chi(k)}{k^{1+i\tau}}=$$

$$=\alpha\sum_{n\leqslant x}\frac{\chi(n)\mu(n)}{n^{1+i\tau}}\ln\frac{x}{n}+O(1) \qquad (3,6,22)$$

в силу (3,6,20) и того, что $\sum_{n\leqslant x}\ln\frac{x}{n}=O(x)$. Сопоставляя (3,6,21) и (3,6,22), мы видим, что всегда при $\tau\neq 0$ и $\chi\neq\chi_0$

$$\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n^{1+i\tau}}=\delta(\chi,\tau)\ln x+O(1) \qquad (3,6,23)$$

$$\delta(\chi,\tau)=\begin{cases}0, & \alpha\neq 0,\\ -1, & \alpha=0.\end{cases}$$

Заметим также, что при $\tau\neq 0$

$$\sum_{n\leqslant x}\frac{\chi_0(n)\Lambda(n)}{n^{1+i\tau}}=\sum_{n\leqslant x}\frac{\Lambda(n)}{n^{1+i\tau}}+O(1)=O(1)$$

в силу (3,6,13). Докажем, что всегда $\delta(\chi,\tau)=0$. Мы будем иметь прежде всего

$$\operatorname{Re}\left[3\sum_{n\leqslant x}\frac{\chi_0(n)\Lambda(n)}{n}+4\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n^{1+i\tau}}+\sum_{n\leqslant x}\frac{\chi^2(n)\Lambda(n)}{n^{1+2i\tau}}\right]=$$

$$=2\sum_{n\leqslant x}\frac{\chi_0(n)\Lambda(n)}{n}\left[1+\operatorname{Re}\frac{\chi(n)}{n^{i\tau}}\right]^2\geqslant 0, \qquad (3,6,24)$$

откуда следует, что

$$[3+4\delta(\chi, \tau)+\delta(\chi^2, 2\tau)]\ln x + O(1) \geqslant 0.$$

Значит, так как $\delta(\chi^2, 2\tau) = -1, 0$, то $\delta(\chi, \tau) \neq -1$, в противном случае левая часть последнего неравенства была бы отрицательной при большом x. Таким образом, всегда

$$\sum_{n\leqslant x} \frac{\chi(n)\Lambda(n)}{n^{1+i\tau}} = O(1), \tag{3,6,25}$$

если только или $\chi \neq \chi_0$, или $\tau \neq 0$. Отсюда уже непосредственно следует формула (3,6,19).

ГЛАВА 4

ЭЛЕМЕНТАРНЫЙ ВЫВОД ЗАКОНА РАСПРЕДЕЛЕНИЯ ПРОСТЫХ ГАУССОВЫХ ЧИСЕЛ. ОДНА ТЕОРЕМА О ПОЧТИ ПРОСТЫХ ГАУССОВЫХ ЧИСЛАХ

§ 1. Введение

В настоящей главе предполагается знакомство с элементами арифметики целых комплексных «гауссовых», чисел $a+bi$, где $i^2=-1$; a, b — обычные целые числа. (См. по этому поводу, например, книжку Л. Г. Шнирельмана [31].) Среди них выделяются простые гауссовы числа, такие, как $1+i$, 3, $2\pm i$ и т. д. Мы интересуемся вопросами асимптотического счета гауссовых простых чисел внутри расширяющихся контуров.

Для некоторых контуров эти вопросы сводятся к рассмотренным ранее элементарным путем законам распределения простых чисел в арифметических прогрессиях (см. гл. 3). Так, число гауссовых простых чисел ρ внутри круга $|z|<R$ асимптотически равно увосьмеренному числу простых чисел вида $x^2+y^2<R^2$. Эти простые числа совпадают с числом 2 или простыми числами вида $4n+1$. Количество таких чисел, не превосходящих R^2, имеет асимптотическое выражение

$$\frac{R^2}{\varphi(4)\ln R^2}=\frac{R^2}{4\ln R},$$

так что искомое нами количество имеет асимптотику

$$\frac{2R^2}{\ln R}.$$

Однако в случае контура общего вида вопрос не сводится к распределению обычных простых чисел в прогрессии.

Элементарное решение этого вопроса по методу Сельберга дано в 1956 г. И. В. Чулановским [25]. Мы будем здесь следовать его изложению.

Мы будем употреблять следующие обозначения. Малыми греческими буквами (кроме π) будем обозначать целые гауссовы числа, буквой ξ — любое комплексное число (не обязательно целое), буквами ρ, σ, τ — простые гауссовы числа. Символом $[\xi]$ обозначим целое гауссово число, такое, что

$$\operatorname{Re}[\xi]-\frac{1}{2}<\operatorname{Re}\xi\leqslant\operatorname{Re}[\xi]+\frac{1}{2}$$

и

$$\operatorname{Im}[\xi]-\frac{1}{2}<\operatorname{Im}\xi\leqslant\operatorname{Im}[\xi]+\frac{1}{2}.$$

D — область на плоскости комплексного переменного, $R=\max\limits_{\xi\in D}|\xi|$, M_L — множество целых гауссовых чисел λ, таких, что на линии L существует ξ с условием $[\xi]=\lambda$; $Z_L=\sum\limits_{\lambda\in M_L}1$. Наконец, знаком $\frac{D}{\nu}$ обозначаем область, определяемую так: $\xi\in\frac{D}{\nu}$ тогда и только тогда, когда $\xi\nu\in D$; аналогично знаком $\frac{L}{\nu}$ обозначаем линию такую, что $\xi\in\frac{L}{\nu}$ тогда и только тогда, когда $\xi\nu\in L$.

Буквами c_1, c_2, c_3,... будем обозначать вещественные постоянные.

Мы докажем элементарным путем следующую теорему.

Теорема 4. 1. 1 (И. В. Чулановский). *Если существует линия L, связная (или состоящая из $O(1)$ связных кусков), содержащая границу области D и такая, что $Z_L=BR$, то*

$$\sum_{\rho\in D}1=\frac{2}{\pi\ln R}\sum_{\nu\in D}1+O\left(\frac{R^2}{\ln R\sqrt[3]{\ln\ln R}}\right). \qquad (4,1,1)$$

Очевидно, что без ограничения общности можно считать область D симметричной относительно поворота на 90° (т. е. такой, что $\xi\in D$ влечет $i\xi\in D$, $-\xi\in D$, $-i\xi\in D$). Такой мы и будем считать область D для удобства рассуждений.

Следует заметить, что с помощью теории аналитических функций (а именно путем применения рядов Гекке) можно

получить закон распределения со значительно лучшим остаточным членом (см., например, Кубилюс [9]. Правда, Кубилюс доказывает свою теорему для гомотетически расширяющихся контуров, но нетрудно усмотреть, что это ограничение является несущественным и легко снимается). Доказательство при этом требует использования счетного числа рядов Гекке. Ценность же применяемого здесь метода А. Сельберга состоит в его полной элементарности.

Нам понадобится функция, которую обозначим через $q(\alpha)$ и определим так (для $\alpha \neq 0$):

$$q(\alpha)=\begin{cases} 1, \text{ если } \alpha \text{ — одна из единиц } (1,\ i,\ -1,\ -i), \\ 0, \text{ если } \alpha \text{ делится на квадрат числа с модулем} > 1, \\ (-1)^k, \text{ если } \alpha=\rho_1 \dots \rho_k \text{ и простые } \rho_1,\dots,\rho_k \text{ неассоциированные.} \end{cases} \tag{4,1,2}$$

Эта функция играет для целых гауссовых чисел роль, аналогичную роли функции Мёбиуса для целых рациональных чисел, и обладает аналогичными свойствами.

§ 2. Несколько вспомогательных формул

В процессе доказательства теоремы нам потребуется несколько вспомогательных формул, которые удобнее вывести предварительно.

Отметим сначала несколько свойств функции $q(\alpha)$. Прежде всего, очевидно, что

$$\sum_{\alpha \mid \varkappa} q(\alpha)=\begin{cases} 4, \text{ если } \varkappa \text{ — одна из единиц,} \\ 0, \text{ если } |\varkappa|>1. \end{cases} \tag{4,2,1}$$

Далее,

$$\sum_{1\leqslant|\alpha|\leqslant r}\frac{q(\alpha)}{|\alpha|^2}=\frac{1}{\pi r^2}\sum_{1\leqslant|\alpha|\leqslant r}\Bigg(\sum_{1\leqslant\beta\leqslant\frac{r}{|\alpha|}}1+O\Big(\frac{r}{|\alpha|}\Big)\Bigg)\,q(\alpha)=$$

$$=\frac{1}{\pi r^2}\sum_{1\leqslant|\nu|\leqslant r}\sum_{\alpha\mid\nu}q(\alpha)+O\Big(\frac{1}{r}\sum_{1\leqslant|\alpha|\leqslant r}\frac{1}{|\alpha|}\Big)=O(1),$$

так что

$$\sum_{1\leqslant|\alpha|\leqslant r}\frac{q(\alpha)}{|\alpha|^2}=O(1). \tag{4,2,2}$$

Очевидно также, что

$$\sum_{1\leqslant|\alpha|\leqslant r} q(\alpha)=O(r^2). \tag{4,2,3}$$

Далее, нам понадобится несколько формул с простыми числами. Прежде всего, очевидно, что

$$\ln|\nu|=\sum_{\substack{\rho,\ k\\ \rho^k|\nu}}\frac{\ln|\rho|}{4}. \tag{4,2,4}$$

А так как

$$\sum_{\substack{\rho,\ k\\ |\rho^k|\leqslant r}}\ln|\rho|=O(r^2) \tag{4,2,5}$$

(это — простое следствие известной связи между простыми гауссовыми и простыми рациональными числами, но могло бы быть доказано и без ссылки на простые рациональные числа), то легко видеть, что

$$\sum_{\substack{\rho,\ k\\ |\rho^k|\leqslant r}}\frac{\ln|\rho|}{|\rho^k|}=O(r). \tag{4,2,6}$$

Поэтому

$$\sum_{1\leqslant|\nu|\leqslant r}\ln|\nu|=\sum_{1\leqslant|\nu|\leqslant r}\sum_{\substack{\rho,\ k\\ \rho^k|\nu}}\frac{\ln|\rho|}{4}=$$

$$=\frac{1}{4}\sum_{\substack{\rho,\ k\\ |\rho^k|\leqslant r}}\ln|\rho|\sum_{\substack{1\leqslant|\nu|\leqslant r\\ \nu:\rho^k}}1=\frac{1}{4}\sum_{\substack{\rho,\ k\\ |\rho^k|\leqslant r}}\ln|\rho|\left(\frac{\pi r^2}{|\rho^k|^2}+O\left(\frac{r}{|\rho^k|}\right)\right)=$$

$$=\frac{\pi r^2}{4}\sum_{\substack{\rho,\ k\\ |\rho^k|\leqslant r}}\frac{\ln|\rho|}{|\rho^k|^2}+O\left(r\sum_{\substack{\rho,\ k\\ |\rho^k|\leqslant r}}\frac{\ln|\rho|}{|\rho^k|}\right)=$$

$$=\frac{\pi r^2}{4}\sum_{\substack{\rho,\ k\\ |\rho^k|\leqslant r}}\frac{\ln|\rho|}{|\rho^k|^2}+O(r^2).$$

Отсюда и из $\sum_{1\leqslant|\nu|\leqslant r}\ln|\nu| = \pi r^2\ln r + O(r^2)$ следует

$$\sum_{\substack{\rho,k\\ |\rho^k|\leqslant r}}\frac{\ln|\rho|}{|\rho^k|^2} = 4\ln r + O(1). \tag{4,2,7}$$

Так как $\sum_{\substack{\rho,k\\ |\rho^k|\leqslant r,\,k\geqslant 2}}\frac{\ln|\rho|}{|\rho^k|^2} = O(1)$, то также

$$\sum_{|\rho|\leqslant r}\frac{\ln|\rho|}{|\rho|^2} = 4\ln r + O(1). \tag{4,2,8}$$

Нам понадобятся также формулы

$$\sum_{1\leqslant|\nu|\leqslant r}\frac{\ln|\nu|}{|\nu|^2} = \pi\ln^2 r + c_1 + O\left(\frac{\ln r}{r}\right), \tag{4,2,9}$$

$$\sum_{1\leqslant|\nu|\leqslant r}\frac{1}{|\nu|^2} = 2\pi\ln r + c_2 + O\left(\frac{1}{r}\right). \tag{4,2,10}$$

В заключение докажем оценку

$$\sum_{\substack{\mu\\ \text{сущ. }\lambda\in M_L\\ |\mu-\lambda|\leqslant r}} 1 = Br(Z_L + r), \tag{4,2,11}$$

справедливую при $r\geqslant 1$. Именно для последней оценки существенно, чтобы линия L была связной или состояла из $O(1)$ связных кусков. Мы докажем оценку (4, 2, 11), считая линию L связной.

Доказательство крайне просто. Если μ таково, что существует $\lambda\in M_L$ с условием $|\mu-\lambda|\leqslant r$, то в силу связности линии L найдется $\geqslant\min(Z_L, r)$ чисел $\lambda'\in M_L$ таких, что $|\mu-\lambda'|\leqslant 2r$. Поэтому

$$\sum_{\substack{\mu\\ \text{сущ. }\lambda\in M_L\\ |\mu-\lambda|\leqslant r}}\ \sum_{\substack{\lambda'\in M_L\\ |\mu-\lambda'|\leqslant 2r}} 1 \geqslant \min(Z_L, r)\sum_{\substack{\mu\\ \text{сущ. }\lambda\in M_L\\ |\mu-\lambda|\leqslant r}} 1.$$

С другой стороны,

$$\sum_{\substack{\mu\\ \text{сущ. }\lambda\in M_L\\ |\mu-\lambda|\leqslant r}}\ \sum_{\substack{\lambda'\in M_L\\ |\mu-\lambda'|\leqslant 2r}} 1 \leqslant \sum_{\lambda'\in M_L}\ \sum_{\substack{\mu\\ |\mu-\lambda'|\leqslant 2r}} 1 \leqslant Z_L r^2.$$

Поэтому

$$\sum_{\substack{\text{сущ. } \lambda \in M_L \\ |\mu-\lambda|\leqslant r}} 1 \ll \frac{Z_L r^2}{\min(Z_L, r)} \ll r(Z_L + r),$$

и оценка (4,2,11) доказана. Тем же способом она доказывается и в случае, когда линия L состоит из $O(1)$ связных кусков. Приходится рассуждать о каждом куске в отдельности и потом суммировать.

Из оценки (4,2,11) очевидным образом следует (при $\nu \neq 0$)

$$\sum_{\mu \in \frac{D}{\nu}} 1 = \frac{1}{|\nu|^2} \sum_{x \in D} 1 + O\left(\frac{Z_L}{|\nu|} + 1\right), \tag{4,2,12}$$

а также

$$\sum_{\lambda \in \frac{M_L}{\nu}} 1 \ll \frac{Z_L}{\nu} + 1. \tag{4,2,13}$$

Из (4,2,13) и из $Z_L \ll R$ следует, что при $|\nu| \leqslant R$

$$\sum_{\lambda \in \frac{M_L}{\nu}} 1 \ll \frac{R}{|\nu|}. \tag{4,2,14}$$

Следовательно, условие, наложенное на D, выполняется и для $\frac{D}{\nu}$, а потому мы вправе будем применять к $\frac{D}{\nu}$ формулы, полученные для D. Этим мы впоследствии будем пользоваться.

§ 3. Доказательство формулы для $\sum_{\rho \in D} \ln^2 |\rho| + \frac{1}{4} \sum_{\substack{\rho, \sigma \\ \rho\sigma \in D}} \ln|\rho| \ln|\sigma|$

В этом параграфе мы докажем следующую лемму.

Лемма 1. *Имеет место формула*

$$\sum_{\rho \in D} \ln^2 |\rho| + \frac{1}{4} \sum_{\substack{\rho, \sigma \\ \rho\sigma \in D}} \ln|\rho| \ln|\sigma| = \frac{4 \ln R}{\pi} \sum_{x \in D} 1 + O(R^2), \tag{4,3,1}$$

которую можно написать и так

$$\sum_{\rho\in D}\ln^2|\rho|+\frac{1}{2}\sum_{|\rho|\leqslant\sqrt{R}}\ln|\rho|\sum_{\sigma\in\frac{D}{\rho}}\ln|\sigma|=$$

$$=\frac{4\ln R}{\pi}\sum_{x\in D}1+O(R^2). \qquad (4,3,2)$$

Эквивалентность (4,3,1) и (4,3,2) видна из того, что

$$\sum_{\substack{\rho,\ \sigma\\ \rho\sigma\in D}}\ln|\rho|\ln|\sigma|=\sum_{\substack{\rho,\ \sigma\\ \rho\sigma\in D\\ |\rho|\leqslant\sqrt{R}}}\ln|\rho|\ln|\sigma|+\sum_{\substack{\rho,\ \sigma\\ \rho\sigma\in D\\ |\sigma|\leqslant\sqrt{R}}}\ln|\rho|\ln|\sigma|-$$

$$-\sum_{\substack{\rho,\ \sigma\\ \rho\sigma\in D\\ |\rho|\leqslant\sqrt{R},\ |\sigma|\leqslant\sqrt{R}}}\ln|\rho|\ln|\sigma|=2\sum_{|\rho|\leqslant\sqrt{R}}\ln|\rho|\sum_{\sigma\in\frac{D}{\rho}}\ln|\sigma|+O(R^2)$$

в силу (4,3,2).

Для доказательства леммы 1 подвергнем некоторым преобразованиям сумму $\sum_{\substack{\nu\in\frac{D}{\alpha}\\ \nu\neq 0}}\ln^2|\nu|$, где $\alpha\neq 0$.

С одной стороны, в силу (4,2,4)

$$\sum_{\substack{\nu\in\frac{D}{\alpha}\\ \nu\neq 0}}\ln^2|\nu|=\sum_{\substack{\nu\in\frac{D}{\alpha}\\ \nu\neq 0}}\sum_{\rho,\sigma,k,m\ \rho^k|\nu,\sigma^m|\nu}\frac{\ln|\rho|\ln|\sigma|}{16}=$$

$$=\sum_{\rho,\sigma,k,m}\frac{\ln|\rho|\ln|\sigma|}{16}\sum_{\substack{\nu\in\frac{D}{\alpha}\\ \nu\neq 0\\ \nu:\{\rho^k,\sigma^m\}}}1=\sum_{\rho,\sigma,k,m}\frac{\ln|\rho|\ln|\sigma|}{16}\sum_{\substack{\mu\in\frac{D}{\alpha\{\rho^k,\sigma^m\}}\\ \mu\neq 0}}1$$

(где $\{\rho^k,\sigma^m\}$ означает наименьшее общее кратное чисел ρ^k, σ^m, причем ввиду симметричности области D относительно поворота

на 90° безразлично, какое из четырех наименьших общих кратных подразумевается). Поэтому благодаря (4,2,1)

$$\sum_{\substack{|\alpha|\leqslant R\\ \alpha\neq 0}} q(\alpha) \sum_{\substack{\nu\in\frac{D}{\alpha}\\ \nu\neq 0}} \ln^2|\nu| =$$

$$= \sum_{\substack{|\alpha|\leqslant R\\ \alpha\neq 0}} q(\alpha) \sum_{\rho,\sigma,k,m} \frac{\ln|\rho|\ln|\sigma|}{16} \sum_{\mu\in\frac{D}{\alpha\{\rho^k,\sigma^m\}}\atop \mu\neq 0} 1 =$$

$$= \sum_{\rho,\sigma,k,m} \frac{\ln|\rho|\ln|\sigma|}{16} \sum_{\substack{\varkappa\in\frac{D}{\{\rho^k,\sigma^m\}}\\ \varkappa\neq 0}} \sum_{\alpha\mid\varkappa} q(\alpha) = \sum_{\substack{\rho,\sigma,k,m\\ \{\rho^k,\sigma^m\}\in D}} \ln|\rho|\ln|\sigma|.$$

С другой стороны, пользуясь (4,2,11) и (4,2,9), находим

$$\sum_{\substack{\nu\in\frac{D}{\alpha}\\ \nu\neq 0}} \ln^2|\nu| = \frac{1}{|\alpha|^2} \sum_{\substack{\varkappa\\ \alpha\left[\frac{\varkappa}{\alpha}\right]\in D\\ \left[\frac{\varkappa}{\alpha}\right]\neq 0}} \ln^2\left|\left[\frac{\varkappa}{\alpha}\right]\right| = \frac{1}{|\alpha|^2} \sum_{\substack{\varkappa\in D\\ \left[\frac{\varkappa}{\alpha}\right]\neq 0}} \ln^2\left|\frac{\varkappa}{\alpha}\right| +$$

$$+\frac{1}{|\alpha|^2} \sum_{\substack{\varkappa\in D\\ \left[\frac{\varkappa}{\alpha}\right]\neq 0}} \left(\ln^2\left|\left[\frac{\varkappa}{\alpha}\right]\right| - \ln^2\left|\frac{\varkappa}{\alpha}\right|\right) +$$

$$+\frac{1}{|\alpha|^2}\left(\sum_{\substack{\varkappa\\ \alpha\left[\frac{\varkappa}{\alpha}\right]\in D\\ \left[\frac{\varkappa}{\alpha}\right]\neq 0}} \ln^2\left|\left[\frac{\varkappa}{\alpha}\right]\right| - \sum_{\substack{\varkappa\in D\\ \left[\frac{\varkappa}{\alpha}\right]\neq 0}} \ln^2\left|\left[\frac{\varkappa}{\alpha}\right]\right|\right) =$$

$$= \frac{1}{|\alpha|^2} \sum_{\substack{\varkappa\in D\\ \left[\frac{\varkappa}{\alpha}\right]\neq 0}} \left(\frac{1}{\pi} \sum_{\substack{|\nu|\leqslant\left|\frac{\varkappa}{\sigma}\right|\\ \nu\neq 0}} \frac{\ln|\nu|}{|\nu|^2} - \frac{c_1}{\pi} + O\left(\frac{|\alpha|}{|\varkappa|}\ln\left(1+\frac{|\varkappa|}{|\alpha|}\right)\right)\right) +$$

$$+O\left(\frac{1}{|\alpha|^2}\sum_{\substack{\varkappa\in D\\ \left[\frac{\varkappa}{\alpha}\right]\neq 0}} \frac{|\alpha|}{|\varkappa|}\ln\left(1+\frac{|\varkappa|}{|\alpha|}\right)\right) + O\left(\frac{|\alpha|(Z_L+|\alpha|)}{|\alpha|^2}\ln^2\frac{2R}{|\alpha|}\right) =$$

$$= \frac{1}{\pi |\alpha|^2} \sum_{\substack{x \in D \\ x \neq 0}} \sum_{\substack{|\nu| \leqslant \left|\frac{x}{\alpha}\right| \\ \nu \neq 0}} \frac{\ln |\nu|}{|\nu|^2} - \frac{c_1}{\pi |\alpha|^2} \sum_{\substack{x \in D \\ \left[\frac{x}{\alpha}\right] \neq 0}} 1 +$$

$$+ O\Big(\sum_{\substack{x \in D \\ \left[\frac{x}{\alpha}\right] \neq 0}} \frac{1}{|x\alpha|} \ln \left(1 + \frac{|x|}{|\alpha|}\right)\Big) + O\left(\left(\frac{Z_L}{|\alpha|} + 1\right) \ln^2 \frac{2R}{|\alpha|}\right).$$

Подсчитываем

$$\sum_{\substack{\alpha \\ |\alpha| \leqslant R \\ \alpha \neq 0}} \frac{q(\alpha)}{\pi |\alpha|^2} \sum_{\substack{x \in D \\ x \neq 0}} \sum_{\substack{|\nu| \leqslant \left|\frac{x}{\alpha}\right| \\ \nu \neq 0}} \frac{\ln |\nu|}{|\nu|^2} =$$

$$= \frac{1}{\pi} \sum_{\substack{x \in D \\ x \neq 0}} \sum_{\substack{\alpha \\ |\alpha| \leqslant |x| \\ \alpha \neq 0}} \frac{q(\alpha)}{|\alpha|^2} \sum_{\substack{|\nu| \leqslant \left|\frac{x}{\alpha}\right| \\ \nu \neq 0}} \frac{1}{|\nu|^2} \sum_{\substack{\rho, k \\ \rho^k \mid \nu}} \frac{\ln |\rho|}{4} =$$

$$= \frac{1}{\pi} \sum_{\substack{x \in D \\ x \neq 0}} \sum_{\substack{\rho, k \\ |\rho^k| \leqslant |x|}} \frac{\ln |\rho|}{4} \sum_{\substack{|\alpha| \leqslant \left|\frac{x}{\rho^k}\right| \\ \alpha \neq 0}} \frac{q(\alpha)}{|\alpha|^2} \sum_{\substack{|\nu| \leqslant \left|\frac{x}{\alpha}\right| \\ \nu \neq 0 \\ \nu : \rho^k}} \frac{1}{|\nu|^2} =$$

$$= \frac{1}{\pi} \sum_{\substack{x \in D \\ x \neq 0}} \sum_{\substack{\rho, k \\ |\rho^k| \leqslant |x|}} \frac{\ln |\rho|}{4 |\rho^k|^2} \sum_{\substack{|\alpha| \leqslant \left|\frac{x}{\rho^k}\right| \\ \alpha \neq 0}} \frac{q(\alpha)}{|\alpha|^2} \sum_{\substack{|\mu| \leqslant \left|\frac{x}{\alpha \rho^k}\right| \\ \mu \neq 0}} \frac{1}{|\mu|^2} =$$

$$= \frac{1}{\pi} \sum_{\substack{x \in D \\ x \neq 0}} \sum_{\substack{\rho, k \\ |\rho^k| \leqslant |x|}} \frac{\ln |\rho|}{4 |\rho^k|^2} \sum_{\substack{|\nu| \leqslant \left|\frac{x}{\rho^k}\right| \\ \nu \neq 0}} \frac{1}{|\nu|^2} \sum_{\alpha \mid \nu} q(\alpha) =$$

$$= \frac{1}{\pi} \sum_{\substack{x \in D \\ x \neq 0}} (16 \ln |x| + O(1)) = \frac{16 \ln R}{\pi} \sum_{x \in D} 1 + O(R)^2 \text{ по (4,2,4),}$$

(4,2,1) и (4,2,7);

$$\sum_{\substack{|\alpha|\leqslant R\\ \alpha\neq 0}} q(\alpha)\frac{c_1}{\pi|\alpha|^2}\sum_{\substack{x\in D\\ \left[\frac{x}{\alpha}\right]\neq 0}} 1 =$$

$$= \frac{c_1}{\pi}\sum_{\substack{|\alpha|\leqslant R\\ \alpha\neq 0}}\frac{q(\alpha)}{|\alpha|^2}\sum_{x\in D} 1 - \frac{c_1}{\pi}\sum_{\substack{|\alpha|\leqslant R\\ \alpha\neq 0}}\frac{q(\alpha)}{|\alpha|^2}\sum_{\substack{x\in D\\ \left[\frac{x}{\alpha}\right]\neq 0}} 1 =$$

$$= O(R^2) + O\Big(\sum_{\substack{|\alpha|\leqslant R\\ \alpha\neq 0}} 1\Big) = O(R^2) \quad \text{по (4,2,2) и (4,2,3);}$$

$$\sum_{\substack{|\alpha|\leqslant R\\ \alpha\neq 0}} q(\alpha)\cdot O\Big(\sum_{\substack{x\in D\\ \left[\frac{x}{\alpha}\right]\neq 0}}\frac{1}{|x\alpha|}\ln\Big(1+\Big|\frac{x}{\alpha}\Big|\Big)\Big) =$$

$$= O\Big(\sum_{\substack{|\alpha|\leqslant R\\ \alpha\neq 0}}\frac{1}{|\alpha|}\sum_{\substack{x\in D\\ \left[\frac{x}{\alpha}\right]\neq 0}}\frac{1}{|x|}\sum_{m\leqslant\frac{2|x|}{|\alpha|}}\frac{1}{m}\Big) =$$

$$= O\Big(\sum_{\substack{x\in D\\ x\neq 0}}\frac{1}{|x|}\sum_{m\leqslant 2|x|}\frac{1}{m}\sum_{|\alpha|\leqslant\frac{2|x|}{m}}\frac{1}{|\alpha|}\Big) =$$

$$= O\Big(\sum_{\substack{x\in D\\ x\neq 0}}\frac{1}{|x|}\sum_{m\leqslant 2|x|}\frac{|x|}{m^2}\Big) = O(R^2);$$

$$\sum_{\substack{|\alpha|\leqslant R\\ \alpha\neq 0}} q(\alpha)\cdot O\Big(\Big(\frac{Z_L}{|\alpha|}+1\Big)\ln^2\frac{2R}{|\alpha|}\Big) = O\Big(\sum_{\substack{|\alpha|\leqslant R\\ \alpha\neq 0}}\frac{R}{|\alpha|}\ln^2\frac{2R}{|\alpha|}\Big) =$$

$$= O\Big(\sum_{\substack{|\alpha|\leqslant R\\ \alpha\neq 0}}\sum_{m\leqslant\frac{2R}{|\alpha|}}\ln^2 m\Big) = O\Big(\sum_{m\leqslant 2R}\ln^2 m\sum_{|\alpha|\leqslant\frac{2R}{m}} 1\Big) = O(R^2).$$

В итоге получаем

$$\sum_{\substack{|\alpha|\leqslant R\\ \alpha\neq 0}} q(\alpha)\sum_{\substack{\nu\in\frac{D}{\alpha}\\ \nu\neq 0}}\ln^2|\nu| = \frac{16\ln R}{\pi}\sum_{x\in D} 1 + O(R^2)$$

и, значит,

$$\sum_{\substack{\rho,\sigma,k,m\\ \{\rho^k,\sigma^m\}\in D}} \ln|\rho|\ln|\sigma| = \frac{16\ln R}{\pi}\sum_{x\in D} 1 + O(R^2).$$

А так как

$$\sum_{\substack{\rho,\sigma,k,m\\ \{\rho^k,\sigma^m\}\in D}} \ln|\rho|\ln|\sigma| = 4\sum_{\rho\in D}\ln^2|\rho| + \sum_{\substack{\rho,\sigma \text{ неассоциированы}\\ \rho\sigma\in D}} \ln|\rho|\ln|\sigma| + O(R^2) =$$

$$= 4\sum_{\rho\in D}\ln^2|\rho| + \sum_{\substack{\rho,\sigma\\ \rho\sigma\in D}}\ln|\rho|\ln|\sigma| + O(R)$$

то лемма 1 доказана.

Заметим попутно, что, применяя рассуждения настоящего параграфа к сумме $\sum_{\nu\in\frac{D}{\alpha},\,\nu\neq 0}\ln|\nu|$ вместо $\sum_{\nu\in\frac{D}{\alpha},\,\nu\neq 0}\ln^2|\nu|$ (они соответственно упрощаются), мы могли бы получить оценку (4,2,5) без ссылки на связь с простыми рациональными числами.

§ 4. Рекуррентная оценка остаточного члена

Из (4,3,1) следует

$$\sum_{\rho\in D}\ln|\rho| + \frac{1}{4}\sum_{\substack{\rho,\sigma\\ \rho\sigma\in D}}\frac{\ln|\rho|\ln|\sigma|}{\ln|\rho\sigma|} = \frac{1}{\ln R}\sum_{\rho\in D}\ln^2|\rho| +$$

$$+\frac{1}{4\ln R}\sum_{\substack{\rho,\sigma\\ \rho\sigma\in D}}\ln|\rho|\ln|\sigma| + \frac{1}{\ln R}\sum_{\rho\in D}\ln|\rho|\ln\frac{R}{|\rho|} +$$

$$+\frac{1}{4\ln R}\sum_{\substack{\rho,\sigma\\ \rho\sigma\in D}}\frac{\ln|\rho|\ln|\sigma|}{\ln|\rho\sigma|}\ln\frac{R}{|\rho\sigma|} =$$

$$=\frac{4}{\pi}\sum_{x\in D}1+O\left(\frac{R^2}{\ln R}\right)+O\left(\frac{1}{\ln R}\sum_{\rho\in D}\ln|\rho|\sum_{m\leqslant\frac{R}{|\rho|}}\frac{1}{m}\right)+$$

$$+O\left(\frac{1}{\ln R}\sum_{\substack{\rho,\sigma\\ \rho\sigma\in D}}\frac{\ln|\rho|\ln|\sigma|}{\ln|\rho\sigma|}\sum_{m\leqslant\frac{R}{|\rho\sigma|}}\frac{1}{m}\right)=$$

$$=\frac{4}{\pi}\sum_{x\in D}1+O\left(\frac{R^2}{\ln R}\right)+O\left(\frac{1}{\ln R}\sum_{m\leqslant R}\frac{1}{m}\sum_{|\rho|\leqslant\frac{R}{m}}\ln|\rho|\right)+$$

$$+O\left(\frac{1}{\ln R}\sum_{m\leqslant R}\frac{1}{m}\sum_{\substack{\rho,\sigma\\ |\rho\sigma|\leqslant\frac{R}{m}}}\frac{\ln|\rho|\ln|\sigma|}{\ln|\rho\sigma|}\right)=$$

$$=\frac{4}{\pi}\sum_{x\in D}1+O\left(\frac{R^2}{\ln R}\right)+O\left(\frac{1}{\ln R}\sum_{m\leqslant R}\frac{R^2}{m^3}\right)+$$

$$+O\left(\frac{1}{\ln R}\sum_{m\leqslant R}\frac{1}{m}\sum_{\substack{\rho,\sigma\\ |\rho\sigma|\leqslant\frac{R}{m}\\ |\rho|\geqslant|\sigma|}}\ln|\sigma|\right)=$$

$$=\frac{4}{\pi}\sum_{x\in D}1+O\left(\frac{R^2}{\ln R}\right)+O\left(\frac{1}{\ln R}\sum_{m\leqslant R}\frac{1}{m}\sum_{|\rho|\leqslant\sqrt{\frac{R}{m}}}|\rho|^2\right)+$$

$$+O\left(\frac{1}{\ln R}\sum_{m\leqslant R}\frac{1}{m}\sum_{\sqrt{\frac{R}{m}}<|\rho|\leqslant\frac{R}{m}}\frac{R^2}{m^2|\rho|^2}\right)=\frac{4}{\pi}\sum_{x\in D}1+O\left(\frac{R^2}{\ln R}\right)+$$

$$+O\left(\frac{1}{\ln R}\sum_{m\leqslant R}\frac{R^2}{m^3}\right)+O\left(\frac{R^2}{\ln R}\sum_{m\leqslant R}\frac{1}{m^3}\cdot\frac{1}{\ln\frac{R}{m}}\sum_{\sqrt{\frac{R}{m}}<|\rho|\leqslant\frac{R}{m}}\frac{\ln|\rho|}{|\rho|^2}\right)=$$

$$=\frac{4}{\pi}\sum_{x\in D}1+O\left(\frac{R^2}{\ln R}\right)$$ (мы воспользовались (4,2,5) и (4,2,8)).

Итак,

$$\sum_{\rho\in D}\ln|\rho|+\frac{1}{4}\sum_{\substack{\rho,\sigma\\ \rho\sigma\in D}}\frac{\ln|\rho|\ln|\sigma|}{\ln|\rho\sigma|}=\frac{4}{\pi}\sum_{x\in D}1+O\left(\frac{R^2}{\ln R}\right).\qquad(4,4,1)$$

Отсюда (ввиду применимости (4,4,1) к области $\frac{D}{\sigma}$) следует:

$$\sum_{|\rho|\leqslant\sqrt{R}}\ln|\rho|\sum_{\sigma\in\frac{D}{\rho}}\ln|\sigma|+\frac{1}{4}\sum_{\substack{\rho,\tau\\|\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}\sum_{\sigma\in\frac{D}{\rho\tau}}\ln|\sigma|=$$

$$=\sum_{|\sigma|\leqslant R}\ln|\sigma|\Big(\sum_{\substack{\rho\in\frac{D}{\sigma}\\|\rho|\leqslant\sqrt{R}}}\ln|\rho|+\frac{1}{4}\sum_{\substack{\rho,\tau\\\rho\tau\in\frac{D}{\sigma}\\|\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}\Big)=$$

$$=\sum_{\sqrt{R}<|\sigma|\leqslant R}\ln|\sigma|\Big(\sum_{\rho\in\frac{D}{\sigma}}\ln|\rho|+\frac{1}{4}\sum_{\substack{\rho,\tau\\\rho\tau\in\frac{D}{\sigma}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}\Big)+$$

$$+O\Big(\sum_{|\sigma|\leqslant\sqrt{R}}\ln|\sigma|\Big(\sum_{|\rho|\leqslant\sqrt{R}}\ln|\rho|+\frac{1}{4}\sum_{\substack{\rho,\tau\\|\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}\Big)\Big)=$$

$$=\sum_{\sqrt{R}<|\sigma|\leqslant R}\left(\frac{4}{\pi}\sum_{x\in\frac{D}{\sigma}}1+O\left(\frac{R^2}{|\sigma|^2\ln\left(\frac{R}{|\sigma|}+1\right)}\right)\right)\ln|\sigma|+O(R^2)=$$

$$=\frac{4}{\pi}\sum_{\sqrt{R}<|\sigma|\leqslant R}\left(\frac{1}{|\sigma|^2}\sum_{x\in D}1+O\left(\frac{Z_L}{|\sigma|}+1\right)\right)\ln|\sigma|+$$

$$+O\Big(R^2\sum_{\sqrt{R}<|\sigma|\leqslant R}\frac{\ln|\sigma|}{|\sigma|^2}\sum_{\ln\frac{R}{|\sigma|}<m\leqslant\ln R}\frac{1}{m^2}\Big)+O(R^2)=$$

$$=\frac{8\ln R}{\pi}\sum_{x\in D}1+O\Big(R^2\sum_{m\leqslant\ln R}\frac{1}{m^2}\sum_{Re^{-m}<|\sigma|\leqslant R}\frac{\ln|\sigma|}{|\sigma|^2}\Big)+O(R^2)=$$

$$=\frac{8\ln R}{\pi}\sum_{x\in D}1+O\Big(R^2\sum_{m\leqslant\ln R}\frac{1}{m}\Big)+O(R^2)=$$

$$=\frac{8\ln R}{\pi}\sum_{x\in D}1+O(R^2\ln\ln R)$$

(мы воспользовались (4,2,5), (4,2,12), (4,2,8), (4,2,6)).

Получаем

$$\sum_{|\rho|\leqslant\sqrt{R}} \ln|\rho| \sum_{\sigma\in\frac{D}{\rho}} \ln|\sigma| + \frac{1}{4} \sum_{\substack{\rho,\tau \\ |\rho\tau|\leqslant\sqrt{R}}} \frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|} \sum_{\sigma\in\frac{D}{\rho\tau}} \ln|\sigma| =$$

$$= \frac{8\ln R}{\pi} \sum_{x\in D} 1 + O(R^2 \ln\ln R).$$

Умножая эту формулу почленно на $\frac{1}{4}$ и затем вычитая ее из (4,3,2), находим

$$\sum_{\rho\in D} \ln^2|\rho| + \frac{1}{4} \sum_{|\rho|\leqslant\sqrt{R}} \ln|\rho| \sum_{\sigma\in\frac{D}{\rho}} \ln|\sigma| - \frac{1}{16} \sum_{\substack{\rho,\tau \\ |\rho\tau|\leqslant\sqrt{R}}} \frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|} \times$$

$$\times \sum_{\sigma\in\frac{D}{\rho\tau}} \ln|\sigma| = \frac{2\ln R}{\pi} \sum_{x\in D} 1 + O(R^2 \ln\ln R). \qquad (4,4,2)$$

Существенно, что в (4, 4,2) коэффициенты при втором и третьем членах левой части находятся, с точностью до знака, в таком же отношении друг к другу, как коэффициенты при первом и втором членах левой части формулы (4,4,1).

Положим теперь

$$\sum_{\rho\in D} \ln|\rho| = \frac{2}{\pi} \sum_{x\in D} 1 + G(D), \qquad (4,4,3)$$

где $G(D)$ — остаточный член, величина которого, очевидно, зависит от области D. Подставим (4,4,3) в (4,4,2):

$$\sum_{\rho\in D} \ln^2|\rho| = \ln R \sum_{\rho\in D} \ln|\rho| - \sum_{\rho\in D} \ln|\rho| \ln\frac{R}{|\rho|} = \frac{2\ln R}{\pi} \sum_{x\in D} 1 +$$

$$+ \ln R \cdot G(D) +$$

$$+ O\Big(\sum_{\rho\in D} \ln|\rho| \sum_{m\leqslant\frac{R}{|\rho|}} \frac{1}{m}\Big) = \frac{2\ln R}{\pi} \sum_{x\in D} 1 + \ln R \cdot G(D) +$$

$$+ O\Big(\sum_{m\leqslant R} \frac{1}{m} \sum_{|\rho|\leqslant\frac{R}{m}} \ln|\rho|\Big) = \frac{2\ln R}{\pi} \sum_{x\in D} 1 + \ln R \cdot G(D) + O(R^2)$$

(мы воспользовались (4,2,5,));

$$\sum_{|\rho|\leqslant\sqrt{R}}\ln|\rho|\sum_{\sigma\in\frac{D}{\rho}}\ln|\sigma|=\frac{2}{\pi}\sum_{|\rho|\leqslant\sqrt{R}}\ln|\rho|\sum_{x\in\frac{D}{\rho}}1+$$

$$+\sum_{|\rho|\leqslant\sqrt{R}}\ln|\rho|\,G\left(\frac{D}{\rho}\right)=\frac{2}{\pi}\sum_{|\rho|\leqslant\sqrt{R}}\frac{\ln|\rho|}{|\rho|^2}\sum_{x\in D}1+$$

$$+O\left(Z_L\sum_{|\rho|\leqslant\sqrt{R}}\frac{\ln|\rho|}{|\rho|^2}\right)+O\left(\sum_{|\rho|\leqslant\sqrt{R}}\ln|\rho|\right)+$$

$$+\sum_{|\rho|\leqslant\sqrt{R}}\ln|\rho|\,G\left(\frac{D}{\rho}\right)=\frac{4\ln R}{\pi}\sum_{x\in D}1+\sum_{|\rho|\leqslant\sqrt{R}}\ln|\rho|\,G\left(\frac{D}{\rho}\right)+$$

$$+O(R^2)$$

(согласно (4,2,12), (4,4,1), (4,2,8), (4,2,5));

$$\sum_{\substack{\rho,\tau\\|\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}\sum_{\sigma\in\frac{D}{\rho\tau}}\ln|\sigma|=\frac{2}{\pi}\sum_{\substack{\rho,\tau\\|\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}\sum_{x\in\frac{D}{\rho\tau}}1+$$

$$+\sum_{\substack{\rho,\tau\\|\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}G\left(\frac{D}{\rho\tau}\right)=\frac{2}{\pi}\sum_{\substack{\rho,\tau\\|\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{|\rho\tau|^2\ln|\rho\tau|}\sum_{x\in D}1+$$

$$+O\left(Z_L\sum_{\substack{\rho,\tau\\|\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{|\rho\tau|\ln|\rho\tau|}\right)+O\left(\sum_{\substack{\rho,\tau\\|\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}\right)+$$

$$+\sum_{\substack{\rho,\tau\\|\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}G\left(\frac{D}{\rho\tau}\right)=\frac{2}{\pi R}\sum_{\substack{\rho,\tau\\|\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}\times$$

$$\times\sum_{m\leqslant\frac{R}{|\rho\tau|^2}}1\sum_{x\in D}1+O\left(\sqrt{R}\sum_{\substack{\rho,\tau\\|\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}\sum_{m\leqslant\frac{\sqrt{R}}{|\rho\tau|}}1\right)+$$

$$+O(R^2)+\sum_{\substack{\rho,\tau\\|\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}G\left(\frac{D}{\rho\tau}\right)=$$

$$= \frac{2}{\pi R} \sum_{m \leqslant R} \sum_{\substack{\rho, \tau \\ |\rho\tau| \leqslant \sqrt{\frac{R}{m}}}} \frac{\ln|\rho| \ln|\tau|}{\ln|\rho\tau|} \sum_{x \in D} 1 +$$

$$+ O\left(\sqrt{R} \sum_{m \leqslant \sqrt{R}} \sum_{\substack{\rho, \tau \\ |\rho\tau| \leqslant \frac{\sqrt{R}}{m}}} \frac{\ln|\rho| \ln|\tau|}{\ln|\rho\tau|}\right) + O(R^2) +$$

$$+ \sum_{\substack{\rho, \tau \\ |\rho\tau| \leqslant \sqrt{R}}} \frac{\ln|\rho| \ln|\tau|}{\ln|\rho\tau|} G\left(\frac{D}{\rho\tau}\right) = \frac{2}{R} \sum_{m \leqslant R} \left(\frac{16}{\pi} \sum_{|\nu| \leqslant \sqrt{\frac{R}{m}}} 1 -\right.$$

$$\left. - 4 \sum_{|\rho| \leqslant \sqrt{\frac{R}{m}}} \ln|\rho| + O\left(\frac{R}{m \ln\left(\frac{R}{m} + 1\right)}\right)\right) \sum_{x \in D} 1 +$$

$$+ O(R^2) + \sum_{\substack{\rho, \tau \\ |\rho\tau| \leqslant \sqrt{R}}} \frac{\ln|\rho| \ln|\tau|}{\ln|\rho\tau|} G\left(\frac{D}{\rho\tau}\right) =$$

$$= \frac{32 \ln R}{\pi} \sum_{x \in D} 1 - \frac{8}{\pi R} \sum_{|\rho| \leqslant \sqrt{R}} \ln|\rho| \sum_{m \leqslant \frac{R}{|\rho|^2}} 1 \sum_{x \in D} 1 +$$

$$+ O\left(R^2 \sum_{\sqrt{R} < m \leqslant R} \frac{1}{m} \sum_{\ln \frac{R}{m} < n \leqslant \ln R} \frac{1}{n^2}\right) + O(R^2) +$$

$$+ \sum_{\substack{\rho, \tau \\ |\rho\tau| \leqslant \sqrt{R}}} \frac{\ln|\rho| \ln|\tau|}{\ln|\rho\tau|} G\left(\frac{D}{\rho\tau}\right) = \frac{32 \ln R}{\pi} \sum_{x \in D} 1 - \frac{8}{\pi} \sum_{|\rho| \leqslant \sqrt{R}} \frac{\ln|\rho|}{|\rho|^2} \times$$

$$\times \sum_{x \in D} 1 + O\left(R \sum_{|\rho| \leqslant \sqrt{R}} \ln|\rho|\right) + O\left(R^2 \sum_{n \leqslant \ln R} \frac{1}{n^2} \sum_{Re^{-n} < m \leqslant R} \frac{1}{m}\right) +$$

$$+ O(R^2) + \sum_{\substack{\rho, \tau \\ |\rho\tau| \leqslant \sqrt{R}}} \frac{\ln|\rho| \ln|\tau|}{\ln|\rho\tau|} G\left(\frac{D}{\rho\tau}\right) = \frac{16 \ln R}{\pi} \sum_{x \in D} 1 +$$

$$+ O\left(R^2 \sum_{n \leqslant \ln R} \frac{1}{n}\right) + O(R^2) + \sum_{\substack{\rho, \tau \\ |\rho\tau| \leqslant \sqrt{R}}} \frac{\ln|\rho| \ln|\tau|}{\ln|\rho\tau|} G\left(\frac{D}{\rho\tau}\right) =$$

$$= \frac{16 \ln R}{\pi} \sum_{x \in D} 1 + \sum_{\substack{\rho, \tau \\ |\rho\tau| \leqslant \sqrt{R}}} \frac{\ln|\rho| \ln|\tau|}{\ln|\rho\tau|} G\left(\frac{D}{\rho\tau}\right) + O(R^2 \ln \ln R)$$

(согласно (4,2,12), (4,4,1), (4,2,8) (4,2,5)).

После подстановки полученных выражений для

$$\sum_{|\rho|\leqslant R}\ln^2|\rho|,\quad \sum_{|\rho|\leqslant\sqrt{R}}\ln|\rho|\sum_{\sigma\in\frac{D}{\rho}}\ln|\sigma|,\quad \sum_{\substack{\rho,\tau\\ |\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}\sum_{\sigma\in\frac{D}{\rho\tau}}\ln|\sigma|$$

в формулу (4,4,2) и сокращений получается

$$\ln R\cdot G(D)+\frac{1}{4}\sum_{|\rho|\leqslant\sqrt{R}}\ln|\rho|\,G\left(\frac{D}{\rho}\right)-\frac{1}{16}\sum_{\substack{\rho,\tau\\ |\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}\times$$

$$\times G\left(\frac{D}{\rho\tau}\right)=O\left(R^2\ln\ln R\right),$$

т. е.

$$G(D)=-\frac{1}{4\ln R}\sum_{|\rho|\leqslant\sqrt{R}}\ln|\rho|\,G\left(\frac{D}{\rho}\right)+$$

$$+\frac{1}{16\ln R}\sum_{\substack{\rho,\tau\\ |\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}\,G\left(\frac{D}{\rho\tau}\right)+O\left(\frac{R^2\ln\ln R}{\ln R}\right).$$

Отсюда непосредственно следует лемма.

Лемма 2. *Для $G(D)$ справедлива рекуррентная оценка*

$$|G(D)|\leqslant\frac{1}{4\ln R}\sum_{|\rho|\leqslant\sqrt{R}}\ln|\rho|\cdot\left|G\left(\frac{D}{\rho}\right)\right|+$$

$$+\frac{1}{16\ln R}\sum_{\substack{\rho,\tau\\ |\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}\left|G\left(\frac{D}{\rho\tau}\right)\right|+O\left(\frac{R^2\ln\ln R}{\ln R}\right).\qquad(4,4,4)$$

На этой рекуррентной оценке в сочетании с рассуждениями следующего параграфа и будет основано доказательство закона распределения простых гауссовых чисел.

§ 5. «Островки» с малыми значениями $\left|G\left(\frac{D}{\nu}\right)\right|$

Наша задача сейчас — убедиться, в том, что в круге $|\xi|\leqslant R$ существует достаточно большое количество достаточно больших кружков, таких, что для находящихся в них $\nu\left|G\left(\frac{D}{\nu}\right)\right|$ достаточно мал.

Для этого сначала оценим сумму $\sum_{z<|\nu|\leqslant y} G\left(\frac{D}{\nu}\right)$, где $1 \leqslant$ $\leqslant z<y \leqslant R$; начнем с суммы $\sum_{1\leqslant|\nu|\leqslant y} G\left(\frac{D}{\nu}\right)$:

$$\sum_{1\leqslant|\nu|\leqslant y} G\left(\frac{D}{\nu}\right)=\sum_{1\leqslant|\nu|\leqslant y}\left(\sum_{\rho\in\frac{D}{\nu}}\ln|\rho|-\frac{2}{\pi}\sum_{x\in\frac{D}{\nu}}1\right)=$$

$$=\sum_{|\rho|\leqslant R}\ln|\rho|\sum_{\substack{1\leqslant|\nu|\leqslant y\\ \nu\in\frac{D}{\rho}}}1-\frac{2}{\pi}\sum_{1\leqslant|\nu|\leqslant y}\left(\frac{1}{|\nu|^2}\sum_{x\in D}1+O\left(\frac{Z_L}{|\nu|}\right)+\right.$$

$$\left.+O(1)\right)=\sum_{|\rho|\leqslant\frac{R}{y}}\ln|\rho|\cdot O(y^2)+\sum_{\frac{R}{y}<|\rho|\leqslant R}\ln|\rho|\sum_{\substack{\nu\in\frac{D}{\rho}\\ \nu\neq 0}}1-$$

$$-\frac{2}{\pi}\sum_{1\leqslant|\nu|\leqslant y}\frac{1}{|\nu|^2}\sum_{x\in D}1+O(Z_L y)+O(y^2)=\sum_{\frac{R}{y}<|\rho|\leqslant R}\ln|\rho|\times$$

$$\times\left(\frac{1}{|\rho|^2}\sum_{x\in D}1+O\left(\frac{Z_L}{|\rho|}\right)+O(1)\right)-4\ln y\sum_{x\in D}1+O(R^2)=$$

$$=4\ln y\sum_{x\in D}1+O(R^2)-4\ln y\sum_{x\in D}1+O(R^2)=O(R^2)$$

(по (4,4,3), (4,2,12), (4,2,10), (4,2,5), (4,5,8) и (4,2,6)).

А тогда и

$$\sum_{z<|\nu|\leqslant y} G\left(\frac{D}{\nu}\right)=O(R^2). \qquad (4,5,1)$$

Далее нам понадобится оценка разности $G\left(\frac{D}{\nu}\right)-G\left(\frac{D}{\mu}\right)$. Пусть $|\nu|\leqslant R$, $|\mu|\leqslant R$, $\min(|\nu|,|\mu|)=h$, и пусть область $\Delta=\frac{D}{\nu}+\frac{D}{\mu}$. Условие, наложенное на D, справедливое для $\frac{D}{\nu}$ и $\frac{D}{\mu}$, будет, как легко видеть, справедливо и для

Δ. Поэтому ко всем этим трем областям применима формула (4,4,1), а также и к $\Delta - \frac{D}{\nu}$ и к $\Delta - \frac{D}{\mu}$. Из

$$\sum_{\rho \in \Delta - \frac{D}{\nu}} \ln|\rho| = \frac{4}{\pi} \sum_{x \in \Delta - \frac{D}{\nu}} 1 - \frac{1}{4} \sum_{\substack{\rho,\sigma \\ \rho\sigma \in \Delta - \frac{D}{\nu}}} \frac{\ln|\rho| \ln|\sigma|}{\ln|\rho\sigma|} + \\ + O\left(\frac{R^2}{h^2 \ln\left(\frac{R}{h}+1\right)}\right)$$

следует

$$0 \leqslant \sum_{\rho \in \Delta} \ln|\rho| - \sum_{\rho \in \frac{D}{\nu}} \ln|\rho| \leqslant \frac{4}{\pi} \sum_{\substack{x \in \Delta \\ x \overline{\in} \frac{D}{\nu}}} 1 + O\left(\frac{R^2}{h^2 \ln\left(\frac{R}{h}+1\right)}\right)$$

(левое неравенство очевидно).

Аналогично

$$0 \leqslant \sum_{\rho \in \Delta} \ln|\rho| - \sum_{\rho \in \frac{D}{\mu}} \ln|\rho| \leqslant \frac{4}{\pi} \sum_{\substack{x \in \Delta \\ x \overline{\in} \frac{D}{\mu}}} 1 + O\left(\frac{R^2}{h^2 \ln\left(\frac{R}{h}+1\right)}\right).$$

Следовательно,

$$\sum_{\rho \in \frac{D}{\nu}} \ln|\rho| - \sum_{\rho \in \frac{D}{\mu}} \ln|\rho| \begin{cases} \leqslant \frac{4}{\pi} \sum\limits_{\substack{x \in \Delta \\ x \overline{\in} \frac{D}{\mu}}} 1 + O\left(\frac{R^2}{h^2 \ln\left(\frac{R}{h}+1\right)}\right), \\ \geqslant -\frac{4}{\pi} \sum\limits_{\substack{x \in \Delta \\ x \overline{\in} \frac{D}{\nu}}} 1 + O\left(\frac{R^2}{h^2 \ln\left(\frac{R}{h}+1\right)}\right). \end{cases}$$

А тогда по (4, 4, 3)

$$\left|G\left(\frac{D}{\nu}\right) - G\left(\frac{D}{\mu}\right)\right| \leqslant \frac{2}{\pi} \sum_{\substack{x \in \Delta \\ x \overline{\in} \frac{D}{\nu}}} 1 + \frac{2}{\pi} \sum_{\substack{x \in \Delta \\ x \overline{\in} \frac{D}{\mu}}} 1 + O\left(\frac{R^2}{h^2 \ln\left(\frac{R}{h}+1\right)}\right) = \\ = \frac{2}{\pi} \sum_{\substack{x \in \frac{D}{\mu} \\ x \overline{\in} \frac{D}{\nu}}} 1 + \frac{2}{\pi} \sum_{\substack{x \in \frac{D}{\nu} \\ x \overline{\in} \frac{D}{\mu}}} 1 + O\left(\frac{R^2}{h^2 \ln\left(\frac{R}{h}+1\right)}\right).$$

Но легко видеть, что если $\xi \in \frac{D}{\mu}$ и $\xi \overline{\in} \frac{D}{\nu}$, то существует $\xi_1 \in \frac{D}{\nu}$ такое, что $|\xi - \xi_1| \leqslant R\frac{|\mu-\nu|}{|\mu\nu|}$ (достаточно взять $\xi_1 = \xi\frac{\mu}{\nu}$), а также $\xi_2 \overline{\in} \frac{D}{\mu}$ такое, что $|\xi - \xi_2| \leqslant R\frac{|\mu-\nu|}{|\mu|^2}$ (достаточно взять $\xi_2 = \xi\frac{\nu}{\mu}$). Аналогично обстоит дело при $\xi \in \frac{D}{\nu}$, $\xi \overline{\in} \frac{D}{\mu}$. Применяя оценки (4,2,11) и (4,2,13) к $\frac{L}{\mu}$, если $|\mu| \geqslant |\nu|$ и к $\frac{L}{\nu}$, если $|\nu| \geqslant |\mu|$, получим

$$\sum_{\substack{x \in \frac{D}{\mu} \\ x \overline{\in} \frac{D}{\nu}}} 1 + \sum_{\substack{x \in \frac{D}{\nu} \\ x \overline{\in} \frac{D}{\mu}}} 1 \leqslant R^2\frac{|\mu-\nu|h}{|\mu\nu|^2} + R^2\frac{|\mu-\nu|^2}{|\mu\nu|^2} + \frac{Rh}{|\mu\nu|},$$

откуда

$$\left|G\left(\frac{D}{\nu}\right) - G\left(\frac{D}{\mu}\right)\right| \leqslant R^2\frac{|\mu-\nu|h}{|\mu\nu|^2} + R^2\frac{|\mu-\nu|^2}{|\mu\nu|^2} + \frac{R^2}{h^2\ln\left(\frac{R}{h}+1\right)}. \qquad (4,5,2)$$

Если $|\mu| \asymp |\nu|$ и $|\mu-\nu| = O(1)$, то

$$\left|G\left(\frac{D}{\nu}\right) - G\left(\frac{D}{\mu}\right)\right| \leqslant \frac{R^2}{h^3} + \frac{R^2}{h^2\ln\left(\frac{R}{h}+1\right)}. \qquad (4,5,3)$$

Возьмем теперь произвольное $s > 0$ и докажем, что при некоторых условиях, налагаемых на y и z, в кольце $z < |\nu| \leqslant y$ найдется ν_0 такое, что

$$\left|G\left(\frac{D}{\nu_0}\right)\right| \leqslant \frac{sR^2}{|\nu_0|^2}.$$

Рассмотрим при этом два случая:

1) При $z < |\nu| \leqslant y$ все $G\left(\frac{D}{\nu}\right)$ имеют один знак. Тогда

$$\left|\sum_{z<|\nu|\leqslant y} G\left(\frac{D}{\nu}\right)\right| = \sum_{z<|\nu|\leqslant y}\left|G\left(\frac{D}{\nu}\right)\right|,$$

и оценка (4,5,1) дает

$$\sum_{z<|\nu|\leqslant y}\left|G\left(\frac{D}{\nu}\right)\right|=O(R^2).$$

А так как при $\ln\frac{y}{z}\geqslant\frac{c_3}{z}$ (где $c_3>0$)

$$\sum_{z<|\nu|\leqslant y}\left|G\left(\frac{D}{\nu}\right)\right|\geqslant\min_{z<|\nu|\leqslant y}\frac{|\nu|^2\left|G\left(\frac{D}{\nu}\right)\right|}{R^2}\times$$

$$\times\sum_{z<|\nu|\leqslant y}\frac{R^2}{|\nu|^2}\geqslant\min_{z<|\nu|\leqslant y}\frac{|\nu|^2\left|G\left(\frac{D}{\nu}\right)\right|}{R^2}R^2\ln\frac{y}{z},$$

то $\left(\text{при } \ln\frac{y}{z}\geqslant\frac{c_3}{z}\right)$

$$\min_{z<|\nu|\leqslant y}\frac{|\nu|^2\left|G\left(\frac{D}{\nu}\right)\right|}{R^2}<\frac{c_4}{\ln\frac{y}{z}},$$

где $c_4>0$. Значит, при дополнительном условии $\ln\frac{y}{z}\geqslant\frac{c_4}{s}$ существует ν_0 такое, что $z<|\nu_0|\leqslant y$ и $\left|G\left(\frac{D}{\nu_0}\right)\right|\leqslant\frac{sR^2}{|\nu_0|^2}$.

2) При $z<|\nu|\leqslant y$ имеются $G\left(\frac{D}{\nu}\right)$ разных знаков: $G\left(\frac{D}{\nu}\right)<0$, $G\left(\frac{D}{\nu''}\right)>0$. При $y-z\geqslant 1$ можно подобрать последовательность чисел $\nu_1=\nu', \nu_2, \nu_3, \ldots, \nu_{n-1}, \nu_n=\nu''$, удовлетворяющих условию $z<|\nu_t|\leqslant y$ и таких, что $|\nu_t-\nu_{t+1}|=O(1)$, $|\nu_t|\asymp|\nu_{t+1}|$ $(t=1, 2, \ldots, n-1)$ (число n не обязано, конечно, быть ограниченным). Найдется такое t $(1\leqslant t\leqslant n-1)$, что

$$G\left(\frac{D}{\nu_t}\right)\leqslant 0, \qquad G\left(\frac{D}{\nu_{t+1}}\right)>0.$$

Выбрав любое из ν_t, ν_{t+1} за ν_0, будем, согласно (4,5,3), иметь

$$\left|G\left(\frac{D}{\nu_0}\right)\right|\leqslant\left|G\left(\frac{D}{\nu_t}\right)-G\left(\frac{D}{\nu_{t+1}}\right)\right|\leqslant\frac{R^2}{|\nu_0|^3}+\frac{R^2}{|\nu_0|^2\ln\left(\frac{R}{|\nu_0|}+1\right)}.$$

Отсюда видно, что можно так подобрать постоянные c_5 и c_6 ($c_5 > 0$, $c_6 > 0$), что при выполнении условий $z > \frac{c_5}{s}$, $y \leqslant$ $\leqslant Re^{-\frac{c_6}{s}}$

$$\left| G\left(\frac{D}{\nu_0}\right)\right| \leqslant \frac{s R^2}{|\nu_0|^2}.$$

Итак, неравенство выполняется в обоих случаях.

Положим теперь $z = u$, $y = ue^{\frac{c_4}{s}}$. Пусть $u > \frac{c_5}{s}$, $u >$ $> \frac{c_5 + 1}{c_4} s$, $u \leqslant Re^{-\frac{c_6 + c_4}{s}}$. Тогда все условия

$$\ln \frac{y}{z} \geqslant \frac{c_5}{z},\ \ln \frac{y}{z} \geqslant \frac{c_4}{s},\ y - z \geqslant 1,\ z > \frac{c_5}{s},\ y \leqslant Re^{-\frac{c_6}{s}}$$

будут выполнены и, существуют ли в кольце $u < |\nu| \leqslant$ $\leqslant ue^{\frac{c_4}{s}}$ $G\left(\frac{D}{\nu}\right)$ разных знаков или нет, в этом кольце найдется ν_0 такое, что

$$\left| G\left(\frac{D}{\nu_0}\right)\right| \leqslant \frac{s R^2}{|\nu_0|^2}. \qquad (4,5,4)$$

Ограничим s сверху: $s \leqslant c_7$ (выбор c_7 в нашей власти). Пусть $|\nu - \nu_0| \leqslant \frac{s|\nu_0|}{c_8}$, причем $c_8 \geqslant 2c_7$. Тогда $|\nu - \nu_0| \leqslant$ $\leqslant \frac{|\nu_0|}{2}$, $|\nu| \asymp |\nu_0|$ и оценка (4,5,2) дает при $\mu = \nu_0$

$$\left| G\left(\frac{D}{\nu}\right) - G\left(\frac{D}{\nu_0}\right)\right| \leqslant R^2 \frac{|\nu - \nu_0|}{|\nu_0|^3} + R^2 \frac{|\nu - \nu_0|^2}{|\nu_0|^4} + \frac{R^2}{|\nu_0|^2 \ln\left(\frac{R}{|\nu_0|} + 1\right)}.$$

Отсюда следует, что если в неравенстве $|\nu - \nu_0| \leqslant \frac{s|\nu_0|}{c_8}$ постоянная c_8 достаточно велика, то

$$\left| G\left(\frac{D}{\nu}\right) - G\left(\frac{D}{\nu_0}\right)\right| \leqslant \frac{s R^2}{|\nu_0|^2}. \qquad (4,5,5)$$

Из (4,5,4), (4,5,5) и из $|\nu_0| \geqslant \frac{2|\nu|}{3}$ $\left(\text{ибо } |\nu - \nu_0| \leqslant \frac{|\nu_0|}{2}\right)$ следует

Лемма 3. *Если* $u > \frac{c_5}{s}$, $u > \frac{c_3+1}{c_4} s$, $u \leqslant Re^{-\frac{c_6+c_4}{s}}$, *то найдется* ν_0 $\left(u < |\nu_0| \leqslant ue^{\frac{c_4}{s}}\right)$ *такое, что при* $|\nu - \nu_0| \leqslant \frac{s|\nu_0|}{c_8}$ *будет выполнено неравенство*

$$\left|G\left(\frac{D}{\nu}\right)\right| \leqslant \frac{9s\,R^2}{2|\nu|^2}. \tag{4,5,6}$$

§ 6. Доказательство теоремы

Лемма 4.

$$G(D) = O\left(\frac{R^2}{\sqrt[3]{\ln\ln R}}\right). \tag{4,6,1}$$

Доказывать лемму будем по индукции. Пусть $R \geqslant R_0 \geqslant 300$; допустим, что при всех ν $(1 < |\nu| \leqslant \sqrt{R})$

$$\left|G\left(\frac{D}{\nu}\right)\right| \leqslant \frac{BR^2}{|\nu|^2\sqrt[3]{\ln\ln\frac{R}{|\nu|}}} \leqslant \frac{BR^2}{|\nu|^2\sqrt[3]{\ln\ln\sqrt{R}}} \tag{4,6,2}$$

(где $B \geqslant 1$).

Очевидно вообще, что $G\left(\frac{D}{\nu}\right) \leqslant \frac{R^2}{|\nu|^2}$, т. е. $\left|G\left(\frac{D}{\nu}\right)\right| \leqslant \frac{c_9 R^2}{|\nu|^2}$. Произвольную постоянную c_7 приравняем к c_9. Считая выполненным неравенство

$$\frac{B}{9\sqrt[3]{\ln\ln\sqrt{R_0}}} \leqslant c_9,$$

положим в лемме 3

$$s = \frac{B}{9\sqrt[3]{\ln\ln\sqrt{R}}}.$$

Числа u_n $\left(0 \leqslant n \leqslant \frac{s \ln R}{2c_4} - \frac{s \ln u_0}{c_4}\right)$ определим так:

$$u_0 = 9c_8 \sqrt[3]{\ln\ln \sqrt{R}} + \frac{(c_3+1)B}{9c_4 \sqrt[3]{\ln\ln \sqrt{R}}} + 1;$$

$$u_n = u_0 e^{\frac{nc_4}{s}} \left(\text{так что } u_n e^{\frac{c_4}{s}} = u_{n+1}\right).$$

При

$$0 \leqslant n \leqslant t = \frac{s \ln R}{2c_4} - \frac{s \ln u_0}{c_4} - 1$$

и при

$$18c_6 \sqrt[3]{\ln\ln \sqrt{R_0}} \leqslant \ln R_0$$

условия $u_n > \frac{c_5}{s}$, $u_n > \frac{c_3+1}{c_4} s$, $u_n \leqslant \mathrm{Re}^{-\frac{c_6+c_4}{s}}$ будут выполнены, и по лемме 3 найдется $\nu_{0,n}$ $(u_n < |\nu_{0,n}| \leqslant u_{n+1})$ такое, что для всех ν, удовлетворяющих условию $|\nu - \nu_{0,n}| \leqslant \frac{s|\nu_{0,n}|}{c_8}$, будет иметь место неравенство

$$\left|G\left(\frac{D}{\nu}\right)\right| \leqslant \frac{9sR^2}{2|\nu|^2} = \frac{BR^2}{2|\nu|^2 \sqrt[3]{\ln\ln \sqrt{R}}}. \qquad (4,6,3)$$

В силу (4,4,4), (4,6,2), (4,6,3), (4,4,1) будет:

$$|G(D)| \leqslant \frac{1}{4\ln R} \sum_{|\rho| \leqslant |\sqrt{R}} \ln|\rho| \left|G\left(\frac{D}{\rho}\right)\right| +$$

$$+ \frac{1}{16 \ln R} \sum_{\substack{\rho,\tau \\ |\rho\tau| \leqslant \sqrt{R}}} \frac{\ln|\rho| \ln|\tau|}{\ln|\rho\tau|} \left|G\left(\frac{D}{\rho\tau}\right)\right| + O\left(\frac{R^2 \ln\ln R}{\ln R}\right) \leqslant$$

$$\leqslant \frac{BR}{4\ln R \sqrt[3]{\ln\ln \sqrt{R}}} \left(\sum_{|\rho| \leqslant \sqrt{R}} \frac{R}{|\rho|^2} \ln|\rho| + \frac{1}{4} \sum_{\substack{\rho,\tau \\ |\rho\tau| \leqslant \sqrt{R}}} \frac{R \ln|\rho| \ln|\tau|}{|\rho\tau|^2 \ln|\rho\tau|} \right) -$$

$$- \frac{BR^2}{8\ln R \sqrt[3]{\ln\ln \sqrt{R}}} \sum_{0 \leqslant n \leqslant t} \left(\sum_{\substack{u_n < |\rho| \leqslant u_{n+1} \\ |\rho - \nu_{0,n}| \leqslant \frac{s|\nu_{0,n}|}{c_8}}} \frac{\ln|\rho|}{|\rho|^2} +\right.$$

$$+\frac{1}{4}\sum_{\substack{\rho,\tau\\ u_n<|\rho\tau|\leqslant u_{n+1}\\ |\rho\tau-\nu_{0,n}|\leqslant\frac{s|\nu_{0,n}|}{c_8}}}\frac{\ln|\rho|\ln|\tau|}{|\rho\tau|^2\ln|\rho\tau|}\Big)+O\left(\frac{R^2\ln\ln R}{\ln R}\right)\leqslant$$

$$\leqslant\frac{BR}{4\ln R\sqrt[3]{\ln\ln\sqrt{R}}}\Big(\sum_{|\rho|\leqslant\sqrt{R}}\ln|\rho|\sum_{m\leqslant\frac{R}{|\rho|^2}}1+$$

$$+\frac{1}{4}\sum_{\substack{\rho,\tau\\ |\rho\tau|\leqslant\sqrt{R}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}\sum_{m\leqslant\frac{R}{|\rho\tau|^2}}1\Big)-$$

$$-\frac{BR^2}{8\ln R\sqrt[3]{\ln\ln\sqrt{R}}}\sum_{0\leqslant n\leqslant t}\frac{4}{9|\nu_{0,n}|^2}\Big(\sum_{\substack{u_n<|\rho|\leqslant u_{n+1}\\ |\rho-\nu_{0,n}|\leqslant\frac{s|\nu_{0,n}|}{c_8}}}\ln|\rho|+$$

$$+\frac{1}{4}\sum_{\substack{\rho,\tau\\ u_n<|\rho\tau|\leqslant u_{n+1}\\ |\rho\tau-\nu_{0,n}|\leqslant\frac{s|\nu_{0,n}|}{c_8}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}\Big)+O\left(\frac{R^2\ln\ln R}{\ln R}\right)=$$

$$=\frac{BR}{4\ln R\sqrt[3]{\ln\ln\sqrt{R}}}\times$$

$$\times\sum_{m\leqslant R}\Big(\sum_{|\rho|\leqslant\sqrt{\frac{R}{m}}}\ln|\rho|+\frac{1}{4}\sum_{\substack{\rho,\tau\\ |\rho\tau|\leqslant\sqrt{\frac{R}{m}}}}\frac{\ln|\rho|\ln|\tau|}{\ln|\rho\tau|}\Big)-$$

$$-\frac{BR^2}{18\ln R\sqrt[3]{\ln\ln\sqrt{R}}}\sum_{0\leqslant n\leqslant t}\frac{1}{|\nu_{0,n}|^2}\times$$

$$\times\Big(\frac{4}{\pi}\sum_{\substack{u_n<|x|\leqslant u_{n+1}\\ |x-\nu_{0,n}|\leqslant\frac{s|\nu_{0,n}|}{c_8}}}1+O\Big(\frac{|\nu_{0,n}|^2}{\ln|\nu_{0,n}|}\Big)\Big)+O\left(\frac{R^2\ln\ln R}{\ln R}\right).$$

Так как $\frac{s|\nu_{0,n}|}{c_8}\leqslant\frac{|\nu_{0,n}|}{2}$, то, очевидно,

$$\sum_{\substack{u_n<|x|\leqslant u_{n+1}\\ |x-\nu_{0,n}|\leqslant\frac{s|\nu_{0,n}|}{c_8}}}1\geqslant\frac{\pi c_{10}s^2|\nu_{0,n}|^2}{c_8^2}+O(s|\nu_{0,n}|)\quad(0<c_{10}<1).$$

Продолжаем:

$$|G(D)| \leqslant \frac{BR}{4 \ln R \sqrt[3]{\ln \ln \sqrt{R}}} \times$$

$$\times \sum_{m \leqslant R} \left(\frac{4}{\pi} \sum_{|x| \leqslant \sqrt{\frac{R}{m}}} 1 + O\left(\frac{R}{m \ln \left(\frac{R}{m} + 1 \right)} \right) \right) -$$

$$- \frac{BR^2}{8 \ln R \sqrt[3]{\ln \ln \sqrt{R}}} \sum_{0 \leqslant n \leqslant t} \left(\frac{4c_{10} s^2}{c_8^2} + O\left(\frac{s}{|\nu_{0,n}|} \right) + \right.$$

$$\left. + O\left(\frac{1}{\ln |\nu_{0,n}|} \right) \right) + O\left(\frac{R^2 \ln \ln R}{\ln R} \right) = \frac{BR^2}{\sqrt[3]{\ln \ln \sqrt{R}}} -$$

$$- \frac{2c_{10} BR^2 s^2 t}{9c_8^2 \ln R \sqrt[3]{\ln \ln \sqrt{R}}} + \frac{BR^2}{18 \ln R \sqrt[3]{\ln \ln \sqrt{R}}} \times$$

$$\times O\left(\sum_{0 \leqslant n \leqslant t} \frac{1}{n+1} \right) + O\left(\frac{R^2 \ln \ln R}{\ln R} \right) = \frac{BR^2}{\sqrt[3]{\ln \ln \sqrt{R}}} -$$

$$- \frac{c_{10} B^4 R^2}{6561 c_4 c_8^2 (\ln \ln \sqrt{R})^{4/3}} + O\left(\frac{R^2 \ln u_0}{\ln R} \right) + O\left(\frac{R^2 \ln \ln R}{\ln R} \right).$$

Но из определения u_0 видно, что

$$u_0 = 9c_5 \sqrt[3]{\ln \ln \sqrt{R}} + O(1).$$

Поэтому наши вычисления дают

$$|G(D)| \leqslant \frac{BR^2}{\sqrt[3]{\ln \ln \sqrt{R}}} - \frac{c_{10} B^4 R^2}{6561 c_4 c_8^2 (\ln \ln \sqrt{R})^{\frac{4}{3}}} + O\left(\frac{R^2 \ln \ln R}{\ln R} \right).$$

При $R_0 \geqslant c_{11}$ будет, следовательно,

$$|G(D)| \leqslant \frac{BR^2}{\sqrt[3]{\ln \ln \sqrt{R}}} - \frac{c_{13} B^4 R^2}{(\ln \ln \sqrt{R})^{\frac{4}{3}}} \leqslant \frac{BR^2}{\sqrt[3]{\ln \ln R}} +$$

$$+ \frac{c_{13} BR^2}{(\ln \ln \sqrt{R})^{\frac{4}{3}}} - \frac{c_{12} B^4 R^2}{(\ln \ln \sqrt{R})^{\frac{4}{3}}} \qquad (c_{12} > 0,\ c_{13} > 0).$$

При $B^3 > \frac{c_{13}}{c_{12}}$ отсюда следует, наконец,

$$|G(D)| \leqslant \frac{BR^2}{\sqrt[3]{\ln \ln R}}.$$

Подберем теперь для B, R_0 постоянные значения так, чтобы выполнялись условия

$$B \geqslant 1,\ B^3 \geqslant \frac{c_{13}}{c_{12}},\ R_0 \geqslant 300,\ R_0 \geqslant c_{11},\ 18c_6 \sqrt[3]{\ln\ln \sqrt{R_0}} \leqslant \leqslant \ln R_0$$

$$c_9 \leqslant \frac{B}{\sqrt[3]{\ln\ln R_0}}, \frac{B}{9\sqrt[3]{\ln\ln \sqrt{R_0}}} \leqslant c_9.$$

Очевидно, что это можно сделать. При $R \leqslant R_0$ тогда будет

$$|G(D)| \leqslant c_9 R^2 \leqslant \frac{BR^2}{\sqrt[3]{\ln\ln R_0}} \leqslant \frac{BR^2}{\sqrt[3]{\ln\ln R}}.$$

Согласно нашим вычислениям, неравенство $|G(D)| \leqslant \leqslant \frac{BR^2}{\sqrt[3]{\ln\ln R}}$ будет тогда справедливо и при $R \leqslant R_0\sqrt{2}$ (ибо из $R \leqslant R_0\sqrt{2}$ и $|\nu| > 1$ следует $\frac{R}{|\nu|} \leqslant R_0$, и для $\left|G\left(\frac{D}{\nu}\right)\right|$ неравенство выполняется). А тогда оно справедливо и при $R \leqslant 2R_0$, а значит, и при $R \leqslant 2R_0\sqrt{2}$ и т. д., следовательно, при любом R. Так как B постоянное, то лемма 4 доказана.

Из леммы 4 наша теорема следует непосредственно. Действительно,

$$\sum_{\rho\in D} 1 = \frac{1}{\ln R}\sum_{\rho\in D}\ln|\rho| + \frac{1}{\ln R}\sum_{\rho\in D}\ln\frac{R}{|\rho|} = \frac{2}{\pi\ln R}\sum_{x\in D}1 + \frac{G(D)}{\ln R} + O\left(\frac{1}{\ln R}\sum_{\rho\in D}\sum_{m\leqslant\frac{R}{|\rho|}}\frac{1}{m}\right) = \frac{2}{\pi\ln R}\sum_{x\in D}1 + O\left(\frac{R^2}{\ln R\sqrt[3]{\ln\ln R}}\right) + O\left(\frac{1}{\ln R}\sum_{m\leqslant R}\frac{1}{m}\sum_{|\rho|\leqslant\frac{R}{m}}1\right) = \frac{2}{\pi\ln R}\sum_{x\in D}1 + O\left(\frac{R^2}{\ln R\sqrt[3]{\ln\ln R}}\right) + O\left(\frac{R^2}{\ln R}\sum_{m\leqslant R}\frac{1}{m^3\ln\left(\frac{R}{m}+1\right)}\right) = \frac{2}{\pi\ln R}\sum_{x\in D}1 + O\left(\frac{R^2}{\ln R\sqrt[3]{\ln\ln R}}\right),$$

и теорема доказана.

§ 7. Одна теорема о почти простых гауссовых числах

Почти простыми мы будем называть числа, имеющие лишь ограниченное число делителей. Эти числа, таким образом, приближаются по своим свойствам к простым числам. Наиболее близкими по своим свойствам к простым числам естественно считать числа вида pp', где p, p' — простые числа.

Методами гл. 5 можно вывести, что неприводимые целочисленные полиномы бесконечно много раз принимают почти простые значения; принимают ли они бесконечно много раз простые значения, до сих пор неизвестно.

В частности, неизвестно, существует ли бесконечно много простых чисел вида $p = x^2 + 1$.

Очевидно, это равносильно вопросу о том, существует ли бесконечно много гауссовых простых чисел вида $x + i$.

Приближением к этому вопросу является вопрос о существовании гауссовых простых чисел вида $x + iy$, где $|y| \leqslant \psi(x)$, и при $x \to \infty$ $\psi(x)$ — медленно возрастающая функция. Так, неэлементарными аналитическими средствами (принимая гипотезу Римана для рядов Гекке поля $k(\sqrt{-1})$) можно показать, что существует бесконечно много простых чисел указанного выше вида с $\psi(x) = O((\ln x)^{\frac{3}{2}})$. Если вместо простых гауссовых чисел рассматривать почти простые числа вида $\rho\rho'$, где ρ, ρ' — простые числа Гаусса, то можно совершенно элементарно доказать о них теорему подобного типа (см. И. П. Кубилюс. Ю. В. Линник [10]).

Теорема 4. 7. 1 (И. П. Кубилюс, Ю. В. Линник). *Существует бесконечно много пар простых чисел pp', таких, что*

$$pp' = X^2 + y^2, \tag{4,7,1}$$

где

$$y = O(\ln X). \tag{4,7,2}$$

Для доказательства рассмотрим кольцо $\sqrt{R} < |z| < R$ на комплексной плоскости гауссовых чисел. Количество простых гауссовых чисел ρ под условием $\sqrt{R} < |\rho| < R$ будет в этом круге не менее $c\frac{R^2}{\ln R}$ (см. § 1 этой главы, где дело сводится к подсчету простых чисел $p \equiv 1 \pmod 4$; $p < R^2$).

У каждого такого числа ρ_j отметим $|\rho_j| = r_l$ и $\arg \rho_j = \varphi_j$. Очевидно, найдутся по крайней мере два числа ρ_{j_1} и ρ_{j_2} в нашем круге такие, что

$$|\arg \rho_{j_2} - \arg \rho_{j_1}| = \left|\arg \frac{\rho_{j_2}}{\rho_{j_1}}\right| = B \frac{\ln R}{R^2}.$$

Составим число $\rho_{j_2} \bar{\rho}_{j_1}$. Имеем

$$\arg \rho_{j_2} \bar{\rho}_{j_1} = B \frac{\ln R}{R^2}; \qquad |\rho_{j_2} \bar{\rho}_{j_1}| = BR^2.$$

Таким образом,

$$\rho_{j_2} \bar{\rho}_{j_1} = X + iy, \qquad y = B \ln R = B \ln X,$$

что и доказывает нашу теорему.

ГЛАВА 5

РЕШЕТО ЭРАТОСФЕНА

Принцип «решета» Эратосфена был известен еще до нашей эры. Им пользовались для подсчета количества простых чисел в заданном интервале. В 1919 г. Вигго Брун [33] и в 1946 г. Атле Сельберг [45] предложили новые формы этого метода для оценки числа простых чисел в двух последовательностях сразу. Изложению этих элементарных принципов и будут посвящены гл. 5 и 6.

§ 1. «Двойное прямоугольное решето»

Прежде чем излагать идеи В. Бруна, познакомимся на конкретном примере с видом двойного решета. Слово «двойное» будет означать в дальнейшем, что метод «решета» применяется сразу к двум последовательностям. В качестве вышеупомянутого примера докажем следующую теорему.

Теорема 5. 1. 1. *Ряд, составленный из обратных величин «близнецов», сходится.*

Пусть $\pi_2(x)$ означает число пар близнецов, каждый из которых не превосходит x. Идея доказательства будет состоять в получении нетривиальной оценки сверху для $\pi_2(x)$. После этого частным суммированием легко получается теорема 5. 1. 1.

Мы начнем с доказательства теоремы 5. 1. 2.

Теорема 5. 1. 2. *Для* $\pi_2(x)$ *при* $x > x_0$ *верна оценка*

$$\pi_2(x) < c\frac{x}{\ln^2 x}(\ln\ln x)^2, \qquad (5,1,1)$$

где c, x_0 — *положительные абсолютные постоянные.*

Будем «высеивать» все числа в последовательности $a_n = n(n+2)$, которые делятся хотя бы на одно простое число

$\leqslant z$, где $z<\sqrt{x}$, $n\leqslant x$. Обозначим через R произведение всех простых чисел $\leqslant z$. Если мы в методе «решета» остановимся на четном шаге $2k$, то получим неравенство

$$\pi_2(x)\leqslant x-\sum_{p\mid R}\sum_{p\mid a_n}1+\sum_{p_1p_2\mid R}\sum_{p_1p_2\mid a_n}1-\ldots$$
$$\ldots+\sum_{p_1\ldots p_{2k}\mid R}\sum_{p_1\ldots p_{2k}\mid a_n}1. \qquad (5,1,2)$$

При этом числа z и k пока произвольные. Их величинами мы распорядимся в дальнейшем. В каждой из наружных сумм в (5,1,2) числа $p_1\ldots p_l$ $(1\leqslant l\leqslant 2k)$ считаются только один раз.

Пусть $d=p_1p_2\ldots p_l$, $\mu(d)\neq 0$, $d\equiv 1 \pmod 2$. Вычислим сумму

$$S_d=\sum_{d\mid a_n}1. \qquad (5,1,3)$$

Сумма (5,1,3) равна числу решений сравнения

$$n(n+2)\equiv 0 \pmod d, \qquad (5,1,4)$$

а число решений этого сравнения равно числу решений $\tau(d)$ систем

$$\left.\begin{aligned} n&\equiv 0 \pmod{d_1},\\ n+2&\equiv 0 \pmod{d_2},\end{aligned}\right\} \qquad (5,1,5)$$

$d_1d_2=d$. Но если $n\leqslant x$, то число решений системы (5,1,4) равно

$$\frac{x}{d}+\theta, \qquad |\theta|\leqslant 1$$

и, следовательно, число решений (5, 1, 4) равно

$$x\frac{\tau(d)}{d}+\theta\tau(d) \qquad (|\theta|\leqslant 1)$$

или

$$S_d=x\frac{\tau(d)}{d}+\theta\tau(d). \qquad (5,1,6)$$

Если же $d\equiv 0 \pmod 2$, то S_d будет равно числу решений сравнения

$$m(m+1)\equiv 0 \left(\mathrm{mod}\ \frac{d}{2}\right) \qquad \left(m\leqslant\frac{x}{2}\right),$$

и аналогично предыдущему получаем

$$S_d = x\frac{\tau\left(\frac{d}{2}\right)}{d} + \theta\tau\left(\frac{d}{2}\right). \tag{5,1,7}$$

Из равенства (5,1,6) и (5,1,7) мы можем заключить, что всегда

$$S_d = x\frac{\tau'(d)}{d} + \theta\tau'(d), \tag{5,1,8}$$

где

$$\tau'(d) = \begin{cases} \tau(d), & \text{если } d \equiv 1 \pmod 2, \\ \tau\left(\frac{d}{2}\right), & \text{если } d \equiv 0 \pmod 2. \end{cases} \tag{5,1,9}$$

Подставим оценку (5,1,8) в правую часть (5,1,2):

$$\pi_2(x) \leqslant x\Big(1 - \sum_{p \mid R}\frac{\tau'(p)}{p} + \sum_{p_1 p_2 \mid R}\frac{\tau'(p_1 p_2)}{p_1 p_2} - \dots$$

$$\dots + \sum_{p_1 \dots p_{2k} \mid R}\frac{\tau'(p_1 \dots p_{2k})}{p_1 \dots p_{2k}}\Big) + \sum_{p \mid R}\tau'(p) + \sum_{p_1 p_2 \mid R}\tau'(p_1 p_2) + \dots$$

$$\dots + \sum_{p_1 \dots p_{2k} \mid R}\tau'(p_1 \dots p_{2k}). \tag{5,1,10}$$

Но сумма $\sum\limits_{p_1 \dots p_r \mid R}\tau'(p_1 \dots p_r)$ не превосходит величины

$$2^r C^r_{\pi(z)} < 2^r\frac{\pi^r(z)}{r!}.$$

Следовательно,

$$\sum_{p \mid R}\tau'(p) + \sum_{p_1 p_2 \mid R}\tau'(p_1 p_2) + \dots$$

$$\dots + \sum_{p_1 \dots p_{2k} \mid R}\tau'(p_1 \dots p_{2k}) < \pi^{2k}(z)\sum_{r \leqslant 2k}\frac{2^r}{r!} \leqslant 9\pi^{2k}(z). \tag{5,1,11}$$

Для завершения оценки $\pi_2(x)$ мы еще должны оценить сумму

$$-\sum_{p_1\dots p_{2k+1}\mid R}\frac{\tau'(p_1\dots p_{2k+1})}{p_1\dots p_{2k+1}}+$$
$$+\sum_{p_1\dots p_{2k+2}\mid R}\frac{\tau'(p_1\dots p_{2k+2})}{p_1\dots p_{2k+2}}-\dots=T_{2k}, \qquad (5,1,12)$$

которая дополняет первый член в (5,1,10) до произведения

$$\left(1-\frac{1}{2}\right)\prod_{3\leqslant p\leqslant z}\left(1-\frac{2}{p}\right). \qquad (5,1,13)$$

Для оценки суммы (5,1,12) воспользуемся неравенством

$$\sum_{p_1\dots p_r\mid R}\frac{1}{p_1\dots p_r}\leqslant\frac{\left(\sum\limits_{p\leqslant z}\frac{1}{p}\right)^r}{r!}.$$

Оно довольно просто доказывается по индукции. Но известно, что

$$\sum_{p\leqslant z}\frac{1}{p}=\ln\ln z+c.$$

Поэтому мы можем записать

$$\sum_{p_1\dots p_r\mid R}\frac{1}{p_1\dots p_r}<\frac{(\ln\ln z+c)^r}{r!}.$$

На основании этой оценки мы заключаем, что абсолютная величина (5,1,12) не больше суммы

$$\sum_{r\geqslant 2k+1}\frac{(2\ln\ln z+2c)^r}{r!}. \qquad (5,1,14)$$

Применим к этой сумме известную оценку

$$r!>\left(\frac{r}{e}\right)^r$$

и увидим, что (5,1,14) не больше суммы

$$\sum_{r\geqslant 2k+1}\left(\frac{2e\ln\ln z+2ec}{r}\right)^r.$$

Положим теперь $k = 2e \ln\ln z + 2ec$; окончательно находим, что (5,1,12) не превосходит величины

$$2^{-2k} < \frac{1}{\ln^4 z}.$$

Учитывая эту оценку, получим, что

$$1 - \sum_{p \mid R} \frac{\tau'(p)}{p} + \sum_{p_1 p_2 \mid R} \frac{\tau'(p_1 p_2)}{p_1 p_2} - \ldots + \sum_{p_1 \ldots p_{2k} \mid R} \frac{\tau'(p_1 \ldots p_{2k})}{p_1 \ldots p_{2k}} =$$

$$= \sum_{d \mid R} \mu(d) \frac{\tau'(d)}{d} - T_{2k} \leqslant \prod_{p \leqslant z} \left(1 - \frac{\tau'(p)}{p}\right) + \frac{1}{\ln^4 z} =$$

$$= \frac{1}{2} \prod_{3 \leqslant p \leqslant z} \left(1 - \frac{2}{p}\right) + \frac{1}{\ln^4 z}.$$

Подставляя эту оценку и оценку (5,1,11) в правую часть (5,1,10), найдем

$$\pi_2(x) < \frac{x}{2} \prod_{p=3}^{z} \left(1 - \frac{2}{p}\right) + \frac{x}{\ln^4 z} + 3\pi^{2k}(z). \qquad (5,1,15)$$

Для того чтобы выполнялось неравенство

$$\pi^{2k}(z) < \frac{x}{\ln^4 z},$$

достаточно положить $z = x^{\frac{1}{2k}}$. Учитывая теперь, что

$$\prod_{3 \leqslant p \leqslant z} \left(1 - \frac{2}{p}\right) < \frac{c_0}{\ln^2 z},$$

где $c_0 > 0$ — абсолютная постоянная, мы из неравенства (5,1,15) получаем

$$\pi_2(x) < c \frac{x}{\ln^2 x} (\ln\ln x)^2.$$

Этой оценки уже достаточно для доказательства теоремы 5.1.1.

Это решето было названо «прямоугольным», потому что мы на всех $2k$ шагах пользовались неизменным количеством простых чисел для высеивания, равным $\pi(z)$. В следующем

параграфе будет изложен метод В. Бруна, который можно было бы назвать «двойным треугольным решетом», так как там с увеличением числа шагов в решете количество используемых чисел уменьшается.

§ 2. Решето Вигго Бруна

В 1919 г. Вигго Брун предложил следующий метод решета. Пусть нам дана арифметическая прогрессия

$$\Delta,\ \Delta+D,\ \Delta+2D,\ldots \quad ((D,\ \Delta)=1,\quad 0<\Delta<D) \qquad (5,2,1)$$

и последовательность различных простых чисел

$$p_1,\ p_2,\ldots,\ p_r$$

с двумя сериями их вычетов соответственно

$$a_1,\quad a_2,\quad a_3,\ldots,\quad a_r,\qquad 0\leqslant a_i\leqslant p_i.$$
$$b_1,\quad b_2,\quad b_3,\ldots,\quad b_r,\qquad 0\leqslant b_i\leqslant p_i.$$

Для простоты изложения в дальнейшем мы будем предполагать, что $a_i\neq b_i$. Надо исследовать количество чисел прогрессии (5,2,1), которые $\leqslant x$ и отличны от всех чисел вида

$$\lambda p_i+a_i,\qquad \lambda p_i+b_i.$$

Это количество В. Брун обозначает символом

$$P(\Delta,\ D,\ x;\ a_1b_1p_1;\ a_2b_2p_2;\ \ldots\ ;\ a_rb_rp_r)$$

или, так как оценки В. Бруна не зависят от Δ, a_i, b_i, то этот символ можно упростить:

$$P(D,\ x,\ p_1,\ p_2,\ldots,\ p_r).$$

Для вывода рекуррентной формулы этого количества заметим, что числа (5,2,1), попадающие в прогрессию

$$\lambda p_r+a_r,$$

снова образуют арифметическую прогрессию

$$\lambda Dp_r+\Delta_r,\qquad \Delta_r<p_rD, \qquad (5.2,2)$$

где Δ_r легко определить. Те же числа (5,2,1), которые попали в (5,2,2), но непредставимы в виде

$$\lambda p_i+a_i,\qquad \lambda p_i+b_i$$

при $1 \leqslant i \leqslant r-1$, существуют в количестве

$$P(\Delta_r,\ Dp_r,\ x;\ a_1b_1p_1;\ \ldots\ ;\ a_{r-1}b_{r-1}p_{r-1}).$$

Аналогичное рассуждение проведем для чисел из (5,2,1), представимых как

$$\lambda p_r + b_r.$$

В результате наше количество (A) будет равно

$$P(\Delta,\ D,\ x;\ a_1b_1p_1;\ \ldots\ ;\ a_{r-1}b_{r-1}p_{r-1}) -$$
$$- P(\Delta_z,\ Dp_z,\ x;\ a_1b_1p_1;\ \ldots\ ;\ a_{r-1}b_{r-1}p_{r-1}) -$$
$$- P(\Delta'_r,\ Dp_r,\ x;\ a_1b_1p_1;\ \ldots\ ;\ a_{r-1}b_{r-1}p_{r-1})$$

или, в более короткой записи,

$$P(D,\ x,\ p_1,\ p_2,\ \ldots\ ,\ p_r) =$$
$$= P(D,\ x,\ p_1, \ldots,\ p_{r-1}) - (2)\ P(Dp_r,\ x;\ p_1, \ldots,\ p_{r-1}), \quad (5,2,3)$$

где (2) при втором члене символизирует сумму двух однотипных величин. В дальнейшем мы будем пользоваться такими символическими коэффициентами для упрощения записи.

Из формулы (5,2,3) выводим

$$P(D,\ x,\ p_1,\ \ldots\ ,\ p_r) = P(D,\ x) - (2)\,P(Dp_1,\ x) -$$
$$- (2)\,P(Dp_2,\ x,\ p_1) - (2)\,P(Dp_3,\ x;\ p_1,\ p_2) - \ldots -$$
$$- (2)\,P(Dp_r,\ x;\ p_1, \ldots,\ p_{r-1}). \quad (5,2,4)$$

Ко всем членам правой части применим формулу (5,2,4):

$$P(D,\ x,\ p_1, \ldots,\ p_r) = P(D,\ x) - (2) \sum_{\alpha \leqslant r} P(Dp_\alpha,\ x) +$$
$$+ (2^2) \sum_{\alpha=1}^{r} \sum_{\beta < \alpha} P(Dp_\alpha p_\beta,\ x;\ p_1, \ldots,\ p_{\beta-1}).$$

Если выбросить часть членов из двойной суммы, то в силу их неотрицательности получим

$$P(D,\ x,\ p_1, \ldots,\ p_r) \geqslant P(D,\ x) - (2) \sum_{\alpha \leqslant r} P(Dp_\alpha,\ x) +$$
$$+ (2^2) \sum_{(\omega)} \sum P(Dp_\alpha p_\beta,\ x;\ p_1, \ldots,\ p_{\beta-1}), \quad (5,2,5)$$

где ω — некоторая область суммирования α, β, целиком входящая в $1 \leqslant \beta < \alpha \leqslant r$.

Пусть теперь $r=r_0>r_1>r_2>\ldots>r_n\geqslant 1$ — целые числа, точными значениями которых распорядимся в дальнейшем.

Тогда, повторяя процесс с применением формулы (5,2,4) и выбрасывая из каждой четной суммы часть членов, получим

$$P(D,\ x;\ p_1,\ldots,\ p_r)\geqslant P(D,\ x)-(2)\sum_{\alpha\leqslant r}P(Dp_\alpha,\ x)+$$

$$+(2^2)\sum_{\substack{\alpha\leqslant r\\ \beta>\alpha}}\sum_{\beta\leqslant r_1}P(Dp_\alpha p_\beta,\ x)-$$

$$-(2^3)\sum_{\alpha\leqslant r}\sum_{\substack{\beta\leqslant r_1\\ \alpha>\beta>\gamma}}\sum_{\gamma<r_1}P(Dp_\alpha p_\beta p_\gamma,\ x)+$$

$$+(2^4)\sum_{\alpha\leqslant r}\sum_{\substack{\beta\leqslant r_1\\ \alpha>\beta>\gamma>\delta}}\sum_{\substack{\gamma<r_1\\ \gamma>\delta}}\sum_{\delta\leqslant r_2}P(Dp_\alpha p_\beta p_\gamma p_\delta,\ x)-\ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\ldots+(2^{2n})\sum_{\substack{\alpha\leqslant r\\ \alpha>\beta>\ldots>\lambda}}\ldots\sum_{\lambda\leqslant r_n}P(Dp_\alpha p_\beta\ldots p_\lambda,\ x)-$$

$$-(2^{2n+1})\sum_{\substack{\alpha\leqslant r\\ \alpha>\beta>\ldots>\lambda>\rho}}\ldots\sum_{\rho<r_n}P(Dp_\alpha p_\beta\ldots p_\lambda p_\rho,\ x). \qquad (5,2,6)$$

$P(d,\ x)$ есть число членов арифметической прогрессии с разностью d и начальным членом $\Delta<d$, не превосходящих x. Поэтому

$$P(d,\ x)=\frac{x}{d}+\theta,\quad |\theta|\leqslant 1.$$

Если в (5,2,6) каждый из $P(d,\ x)$ заменить на $\frac{x}{d}$, то получим ошибку R, не превосходящую количества всех слагаемых с учетом коэффициентов 2^k. Поэтому

$$P(D,\ x,\ p_1,\ldots,\ p_r)>\frac{x}{D}\left(1-2\sum_{\alpha\leqslant r}\frac{1}{p_\alpha}+\right.$$

$$+2^2\sum_{\substack{\alpha_1\leqslant r\\ \alpha_1>\alpha_2}}\sum_{\alpha_2\leqslant r}\frac{1}{p_{\alpha_1}p_{\alpha_2}}-\ldots-$$

$$\left.-2^{2n+1}\sum_{\alpha_1\leqslant r_0}\ldots\sum_{\alpha_{2n+1}<r_n}\frac{1}{p_{\alpha_1}p_{\alpha_2}\ldots p_{\alpha_{2n+1}}}\right)-R. \qquad (5,2,7)$$

Очевидно, что все эти члены и только их получим среди тех членов произведения

$$\left(1-\sum_{\alpha_1\leqslant r_0}\frac{2}{p_{\alpha_1}}\right)\left(1-\sum_{\alpha_2\leqslant r_1}\frac{2}{p_{\alpha_2}}\right)\left(1-\sum_{\alpha_3\leqslant r_1}\frac{2}{p_{\alpha_3}}\right)\cdots$$
$$\cdots\left(1-\sum_{\alpha_{2n}\leqslant r_n}\frac{2}{p_{\alpha_{2n}}}\right)\left(1-\sum_{\alpha_{2n+1}\leqslant r_n}\frac{2}{p_{\alpha_{2n+1}}}\right), \qquad (5,2,8)$$

для которых

$$\alpha_1>\alpha_2>\ldots>\alpha_{2n+1}. \qquad (5,2,9)$$

Следовательно, количество их не больше чем

$$Q=(2r_0+1)(2r_1+1)^2\ldots(2r_n+1)^2, \qquad (5,2,10)$$

и, таким образом,

$$|R|\leqslant Q.$$

Пусть сумма членов (5,2,8) с условием (5,2,9) будет E. Тогда мы можем переписать (5,2,7) в виде

$$P(D,\ x,\ p_1,\ldots,\ p_r)>\frac{x}{D}E-R.$$

Соберем отдельно слагаемые E по числу множителей так, что $E^{(i)}$ будет обозначать i-кратное суммирование:

$$E=1-E^{(1)}+E^{(2)}-\ldots+E^{(2n)}-E^{(2n+1)}. \qquad (5,2,11)$$

Вычисление E производится по ступеням. Пусть E_m сумма всех членов из (5,2,8), индексы которых не только удовлетворяют условию (5,2,9), но все $>r_m$. Это возможно только для первых $2m-1$ индексов $\alpha_1, \alpha_2, \ldots, \alpha_{2m-1}$ по условиям построения: $\alpha_1\leqslant r_0$, $\alpha_2\leqslant r_1$, $\alpha_3\leqslant r_1$, $\alpha_4\leqslant r_2$, $\alpha_5\leqslant r_2, \ldots,$ $\alpha_{2m}\leqslant r_m$, $\alpha_{2m+1}\leqslant r_m$. Мы снова можем собрать их по кратности сумм и написать

$$E_m=1-E_m^{(1)}+E_m^{(2)}-\ldots+E_m^{(2m-2)}-E_m^{(2m-1)}. \qquad (5,2,12)$$

Эта сумма входит в E, и каждое из ее слагаемых $E_m^{(i)}$ есть

часть слагаемого $E^{(i)}$. Например,

$$E^{(2)} = 2^2 \sum_{\substack{\alpha_1 \leqslant r_0 \\ \alpha > \beta}} \sum_{\alpha_2 \leqslant r_1} \frac{1}{p_{\alpha_1} p_{\alpha_2}};$$

$$E_m^{(2)} = 2^2 \sum_{\substack{\alpha_1 \leqslant r_0 \\ \alpha_1 > r_m, \\ \alpha > \beta}} \sum_{\substack{\alpha_2 \leqslant r_1 \\ \alpha_2 > r_m}} \frac{1}{p_{\alpha_1} p_{\alpha_2}}.$$

В этих обозначениях $E = E_{n+1}$.

Для перехода от E_m к E_{m+1} введем элементарные симметрические функции величин

$$\frac{2}{p_{r_{m+1}+1}}, \quad \frac{2}{p_{r_{m+1}+2}}, \ldots, \quad \frac{2}{p_{r_m}} \quad (r_{m+1} < r_m) \tag{5,2,13}$$

и обозначим их через $S_{m+1}^{(1)}, S_{m+1}^{(2)}, \ldots, S_{m+1}^{(i)}$, так что $i = r_m - r_{m+1}$.

Аналогично (5,2,12) напишем

$$E_{m+1} = 1 - E_{m+1}^{(1)} + E_{m+1}^{(2)} - \ldots + E_{m+1}^{(2m)} - E_{m+1}^{(2m+1)}.$$

$E_{m+1}^{(i)}$ строится из членов, у которых первые i индексов $> r_{m+1}$. Это дает такие возможности:

1) Все i индексов не больше r_m; сумма этих членов равна $S_{m+1}^{(i)}$.

2) Только первый индекс $> r_m$; это дает величину $E_m^{(1)} S_{m+1}^{(i-1)}$. В самом деле, $E_m^{(1)}$ есть сумма всех членов с индексом $> r_m$, а $S_{m+1}^{(i-1)}$ — симметрическая функция, зачитывающая все произведения с $i-1$ сомножителями, каждый индекс которых $\leqslant r_m$.

3) Только два первых индекса $> r_m$: это дает

$$E_m^{(2)} S_{m+1}^{(i-2)}.$$

. . . .

$i+1$) Все i индексов $> r_m$: это дает

$$E_m^{(i)}.$$

В целом мы получаем

$$E_{m+1}^{(i)} = S_{m+1}^{(i)} + E_m^{(1)} S_{m+1}^{(i-1)} + E_m^{(2)} S_{m+1}^{(i-2)} + \ldots + E_m^{(i)}, \tag{5,2,14}$$

причем правая часть обрывается после $2m$-го шага, так как

у нее $\alpha_{2m} \leqslant r_m$. Поэтому

$$E_{m+1} = 1 - (S_{m+1}^{(1)} + E_m^{(1)}) + (S_{m+1}^{(2)} + E_m^{(1)} S_{m+1}^{(1)} + E_m^{(2)}) -$$
$$\cdots$$
$$\ldots - (S_{m+1}^{(2m-1)} + E_m^{(1)} S_{m+1}^{(2m-2)} + \ldots + E_m^{(2m-2)} S_{m+1}^{(1)} +$$
$$+ E_m^{(2m-1)}) + (S_{m+1}^{(2m)} + E_m^{(1)} S_{m+1}^{(2m-2)} + \ldots +$$
$$+ E_m^{(2m-2)} S_{m+1}^{(2)} + E_m^{(2m-1)} S_{m+1}^{(1)}) - (S_{m+1}^{(2m+1)} +$$
$$+ E_m^{(1)} S_{m+1}^{(2m)} + \ldots + E_m^{(2m-2)} S_{m+1}^{(3)} + E_m^{(2m-1)} S_{m+1}^{(2)}).$$

Сравним полученное выражение с произведениями:

$$E_m \prod_{\nu=r_{m+1}+1}^{r_m} \left(1 - \frac{2}{p_\nu}\right) = (1 - E_m^{(1)} + E_m^{(2)} - \ldots +$$
$$+ E_m^{(2m-2)} - E_m^{(2m-1)})(1 - S_{m+1}^{(1)} + S_{m+1}^{(2)} - \ldots \pm S_{m+1}^{(i)}) =$$
$$= 1 - (S_{m+1}^{(1)} + E_{m+1}^{(1)}) + (S_{m+1}^{(2)} + E_m^{(1)} S_{m+1}^{(1)} + E_m^{(2)}) - \ldots$$
$$\cdots$$
$$\ldots - (S_{m+1}^{(2m+1)} + E_m^{(1)} S_{m+1}^{(2m)} + \ldots + E_m^{(2m-2)} S_{m+1}^{(3)} +$$
$$+ E_m^{(2m-1)} S_{m+1}^{(2)}) + {}^{(*)} + (S_{m+1}^{(2m+2)} + E_m^{(1)} S_{m+1}^{(2m+1)} +$$
$$+ \ldots + E_m^{(2m-2)} S_{m+1}^{(4)} + E_m^{(2m-1)} S_{m+1}^{(3)}) - \ldots$$
$$\cdots$$
$$\ldots + \ldots \pm E_m^{(2m-1)} S_{m+1}^{(i)}.$$

В дальнейшем мы так распорядимся величинами $S_{m+1}^{(j)}$, что при возрастании j от 1 до i они монотонно убывают и всегда < 1. После этого замечания рассмотрим скобки, начиная со знака $^{(*)}$ и дальше. Эти скобки по абсолютной величине убывают, так как количество слагаемых в каждой из них равно $2m$ и, кроме того, они знакопеременны.

Следовательно, сумма всех скобок, которые входят в последнее произведение и не входят в E_{m+1}, меньше, чем первая из них.

Введем обозначения:

$$\pi_m = \prod_{\nu = r_m + 1}^{r_{m-1}} \left(1 - \frac{2}{p_\nu}\right) \qquad (m = 1, 2, \ldots, n),$$

$$\pi_{k+1} = \prod_{\nu = 1}^{r_k} \left(1 - \frac{2}{p_\nu}\right).$$

Тогда, используя их, можно записать неравенство

$$E_{m+1} > E_m \pi_{m+1} - (S_{m+1}^{(2m+2)} + E_m^{(1)} S_{m+1}^{(2m+1)} + \\ + \ldots + E_m^{(2m-1)} S_{m+1}^{(3)}) \qquad (5,2,15)$$

в предположении, что

$$1 > S_{m+1}^{(1)} > S_{m+1}^{(2)} > \ldots > S_{m+1}^{(i)}.$$

Для элементарных симметричных функций $S^{(1)}$, $S^{(2)}, \ldots, S^{(i)}$ от i различных положительных величин имеют место неравенства

$$\frac{S^{(1)}}{i} > \frac{2S^{(2)}}{(i-1)S^{(1)}} > \frac{3S^{(3)}}{(i-2)S^{(2)}} > \ldots > \frac{iS^{(i)}}{1 \cdot S^{(i-1)}}.$$

(Их можно получить, вводя полином $f(x) = x^i - S^{(1)}x^{i-1} + S^{(2)}x^{i-2} - \ldots \pm S^{(i)}$ и применяя к нему и его производным теорему Ролля.) Из этих неравенств следует

$$S^{(1)} > \frac{S^{(2)}}{S^{(1)}} > \frac{S^{(3)}}{S^{(2)}} > \ldots > \frac{S^{(i)}}{S^{(i-1)}}.$$

И если $S^{(1)} < 1$, то

$$1 > S^{(1)} > S^{(2)} > \ldots > S^{(i)}.$$

Кроме того, верна оценка:

$$S^{(j)} < \frac{(S^{(1)})^j}{j!}, \qquad (5,2,16)$$

ибо для $j=2$ это неравенство выполняется. Если оно верно для $j-1$, то из неравенства

$$\frac{jS^{(j)}}{(i-j+1)\,S^{(j-1)}} < \frac{S^{(1)}}{1}$$

получаем (5,2,16).

Следовательно, нам остается удовлетворить условию

$$S^{(1)} < 1.$$

Для этого надо выбрать индексы r_m так, чтобы для каждого m сумма величин (5,2,13) была <1. Мы будем выбирать простые числа $p_1, p_2, \ldots, p_r$ в порядке их естественного роста $p_1 \geqslant 3$. Дальше, пусть $h_0 > h > 1$ — два положительных числа, причем для h_0 должно выполняться условие

$$0 < 2 \ln h_0 < 1.$$

В силу того что

$$\sum_{3 \leqslant p \leqslant w} \frac{1}{p} = \ln\ln w + c_1 + O\left(\frac{1}{\ln w}\right),$$

$$\prod_{3 \leqslant p \leqslant w} \left(1 - \frac{2}{p}\right) = \frac{c_2}{\ln^2 w} + O\left(\frac{1}{\ln^3 w}\right), \qquad (5,2,17)$$

существует $w = w_0$, начиная с которого

$$0 < \sum_{w < p < w^h} \frac{1}{p} < \ln h_0$$

и

$$\prod_{w \leqslant p \leqslant w^h} \left(1 - \frac{2}{p}\right) > \frac{2}{h_0^3}. \qquad (5,2,18)$$

Теперь выберем индексы r_m так: пусть p_{r_1} — наибольшее простое число $\leqslant p_r^{\frac{1}{h}}$; p_{r_2} — наибольшее простое $\leqslant p_r^{\frac{1}{h^2}}$ и т. д., продолжаем этот процесс до p_{r_m}, причем $p_{r_m} > w_0$.

Пусть p_{r_k} — наименьшее простое число, определенное таким способом. В силу (5,2,18) получаем:

$$\left.\begin{aligned} 0 < \sigma_1 &= \sum_{\nu=r_1+1}^{r} \frac{1}{p_\nu} < \ln h_0, \\ &\cdots\cdots\cdots\cdots \\ 0 < \sigma_k &= \sum_{\nu=r_k+1}^{r_{k-1}} \frac{1}{p_\nu} < \ln h_0. \end{aligned}\right\} \qquad (5,2,19)$$

$$\left.\begin{aligned} \pi_1 &= \prod_{\nu=r_1+1}^{r} \left(1-\frac{2}{p_\nu}\right) > \frac{1}{h_0^2}, \\ &\cdots\cdots\cdots\cdots \\ \pi_k &= \prod_{\nu=r_k+1}^{r_{k-1}} \left(1-\frac{2}{p_\nu}\right) > \frac{1}{h_0^2}. \end{aligned}\right\} \qquad (5,2,20)$$

У нас было p_{r_k} наименьшее простое число при условии, что

$$w_0 < p_{r_k} \leqslant p_r^{\frac{1}{h^k}}.$$

Пусть $p_{r_{k+1}}$ — наибольшее простое число $\leqslant w_0$. Тогда

$$0 < \sigma_{k+1} = \sum_{\nu=r_{k+1}+1}^{r_k} \frac{1}{p_\nu} < \ln h_0,$$

$$\pi_{k+1} = \prod_{\nu=r_{k+1}+1}^{r_k} \left(1-\frac{2}{p_\nu}\right) > \frac{1}{h_0^2}.$$

Теперь постараемся продолжить систему индексов уже независимо от p_r. Здесь мы их должны просто подбирать так,

чтобы выполнялись неравенства:

$$0<\sigma_{k+2}=\sum_{\nu=r_{k+2}+1}^{r_{k+1}}\frac{1}{p_\nu}<\ln h_0,$$

. . . . . .

$$0<\sigma_{n+1}=\sum_{\nu=1}^{r_n}\frac{1}{p_\nu}<\ln h_0\quad(r_{k+1}=1),$$

$$\pi_{k+2}=\prod_{\nu=r_{k+2}+1}^{r_{k+1}}\left(1-\frac{2}{p_\nu}\right)>\frac{1}{h_0^2},$$

. . . . . .

$$\pi_n=\prod_{\nu=r_n+1}^{r_{n-1}}\left(1-\frac{2}{p_\nu}\right)>\frac{1}{h_0^2},$$

$$\pi_{n+1}=\prod_{\nu=1}^{r_n}\left(1-\frac{2}{p_\nu}\right)>\frac{1}{h_0^2}.$$

Чтобы эти неравенства были выполнены, достаточно взять $p_1\geqslant 3$ с условием

$$\frac{1}{p_1}<\ln h_0\qquad\left(1-\frac{2}{p_1}\right)>\frac{1}{h_0^2}\tag{5,2,21}$$

(так как в каждый интервал можно поместить по одному числу).

Пусть этот процесс уже закончен. Простые числа $p_{r_{k+1}},\ldots,p_{r_n}$ зависят не от p_r, а только от констант h и h_0. Тогда из (5,2,21) следует:

$$\begin{aligned}R&<p_r p_{r_1}^2 p_{r_2}^3\ldots p_{r_k}^2 p_{r_{k+1}}^2\ldots p_{r_n}^2\leqslant\\&\leqslant p_r p_r^{\frac{2}{h}} p_r^{\frac{2}{h^2}}\ldots p_r^{\frac{2}{h^k}} p_{r_{k+1}}^2\ldots p_{r_k}^2=\\&=c(h,h_0)\,p_r^{1+2\left(\frac{1}{h}+\frac{1}{h^2}+\ldots+\frac{1}{h^k}\right)}=\\&=c(h,h_0)\,p_r^{\frac{h+1-h^{\frac{2}{k}}}{h-1}}<c'p_r^{\frac{h+1}{h-1}},\end{aligned}\tag{5,2,22}$$

причем c' зависит только от h и h_0.

Теперь из (5,2,15) мы рекуррентным путем выведем оценку для $E_{n+1}=E$. Введем обозначение:

$$\Phi_{m+1}=S_{m+1}^{(2m+2)}+E_m^{(1)}S_{m+1}^{(2m+1)}+\ldots+E_m^{(2m-1)}E_{m+1}^{(3)}, \quad (5,2,23)$$

тогда (5,2,15) примет вид

$$E_2>E_1\pi_2-\Phi_2.$$

Но $\pi_2 h_0^2>1$, $\pi_1<1$, следовательно,

$$E_2>\pi_2(E_1-h_0^2\Phi_2)>\pi_1\pi_2(E_1-h_0^2\Phi_2).$$

Далее, $\pi_2\pi_3 h_0^4>1$,

$$E_3>\pi_3 E_2-\Phi_3>\pi_2\pi_3(E_1-h_0^2\Phi_2)-$$
$$-\pi_2\pi_3 h_0^4\Phi_3>\pi_1\pi_2\pi_3(E_1-h_0^2\Phi_2-h_0^4\Phi_3).$$

. . . . . .

И, наконец,

$$E_{n+1}>\pi_1\pi_2\ldots\pi_{n+1}(E_1-h_0^2\Phi_2-$$
$$-h_0^4\Phi_4-\ldots-h_0^{2n}\Phi_{n+1}). \quad (5,2,24)$$

Рассмотрим (5,2,23). Мы имеем

$$S_l^{(1)}=2\sigma_l<2\ln h_0<1 \qquad (l=1,2,\ldots,\ n+1)$$

и

$$S_l^{(j)}<\frac{(S_l^{(1)})^j}{j!}.$$

Полагая $\tau=2\ln h_0$, получаем

$$\Phi_{m+1}<\frac{\tau^{2m+2}}{(2m+2)!}+E_m^{(1)}\frac{\tau^{2m+1}}{(2m+1)!}+\ldots+E_m^{(2m-1)}\frac{\tau^3}{3!}. \quad (5,2,25)$$

Из (5,2,14):

$$E_{m+1}^{(i)}=S_{m+1}^{(i)}+E_m^{(1)}S_{m+1}^{(i-1)}+\ldots+E_m^{(i)}<$$
$$<\frac{\tau^i}{i!}+E_m^{(1)}\frac{\tau^{i-1}}{(i-1)!}+\ldots+E_m^{(i)}, \quad (5,2,26)$$

В частности, $E_{m+1}^{(1)}<\tau+E_m^{(1)}$, а так как $E_1^{(1)}=2\sigma_1<\tau$, то

$$E_m^{(1)}<\tau+\tau+\ldots+\tau=m\tau. \quad (5,2,27)$$

При наличии формул (5,2,25), (5,2,26), (5,2,27) можно рекуррентным способом дать числовую оценку величинам

$$E_m^{(i)} \text{ и } \Phi_m.$$

Напомним, что $E_m^{(i)}$ есть сумма произведений по i множителей, индексы которых убывают и все $> r_m$. Поэтому всего $E_m^{(1)}, E_m^{(2)}, \ldots, E_m^{(2m-1)}$ и не больше таких величин.

Будем искать оценку Φ_m для любого m. Пусть m_0 — некоторый фиксированный индекс $E_m^{(i)}$, и пусть выбраны константы c_0 и k так, что

$$E_{m_0}^{(i)} < c_0 (\tau k)^i \tag{5,2,28}$$

($k > 0$, можно выбрать произвольно, а затем задать c_0, обе константы можно произвольно увеличивать). Тогда из (5,2,26) выводим

$$E_{m_0+1}^{(i)} < \frac{\tau^i}{i!} + c_0 (\tau k)^i \left\{ \frac{\left(\frac{1}{k}\right)^{i-1}}{(i-1)!} + \frac{\left(\frac{1}{k}\right)^{i-2}}{(i-2)!} + \ldots + 1 \right\}.$$

Если $c_0 \geqslant 1$, то первый член можно внести в скобки, не нарушая неравенства. Следовательно,

$$E_{m_0+1}^{(i)} < c_0 (\tau k)^i l^{\frac{1}{k}},$$

$E_{m_0+2}^{(i)}$ получим отсюда, заменяя c_0 на $c_0 l^{\frac{1}{k}}$:

$$E_{m_0+2}^{(i)} < c_0 l^{\frac{2}{k}} (\tau k)^i$$

и т. д. В конце получим

$$E_m^{(i)} < c_0 (\tau k)^i \, l^{\frac{m-m_0}{k}} \qquad (m \geqslant m_0).$$

Подставляя эту оценку в (5,2,25), получим неравенство

$$\Phi_{m+1} < \frac{\tau^{2m+2}}{(2m+2)!} + c_0 (\tau k)^{2m+2} \, l^{\frac{m-m_0}{k}} \left\{ \frac{\left(\frac{1}{k}\right)^{2m+1}}{(2m+1)!} + \ldots + \frac{\left(\frac{1}{k}\right)^3}{3!} \right\}$$

$$(m \geqslant m_0).$$

Снова, не нарушая неравенства, первый член можно внести под скобку. В результате получим

$$\Phi_{m+1} < c_0 (\tau k)^{2m+2} l^{\frac{m-m_0}{k}} \left\{ l^{\frac{1}{k}} - \frac{\left(\frac{1}{k}\right)^2}{2!} - \frac{\frac{1}{k}}{1!} - 1 \right\}. \quad (5,2,29)$$

Подставляя эту оценку в (5,2,24), после несложных преобразований получим

$$E_{n+1} > \pi_1 \pi_2 \dots \pi_{n+1} (E_1 - h_0^2 \Phi_2 - \dots - h_0^{2m_0} \Phi_{m_0+1} - h_0^{2m_0+2} c_0 (\tau k)^{2m_0+4} l^{\frac{1}{k}} \left\{ l^{\frac{1}{k}} - \frac{1}{2k^2} - \frac{1}{k} - 1 \right\} \frac{1 - (l^{\frac{1}{k}} h_0^2 (\tau k)^2)^{n-m_0}}{1 - h_0^2 (\tau k)^2 l^{\frac{1}{k}}}. \quad (5,2,30)$$

Если $h_0^2 (\tau k)^2 l^{\frac{1}{k}} < 1$, то мы только усилим неравенство, отбросив в оценке величину $(l^{\frac{1}{k}} h_0^2 (\tau k)^2)^{n-m_0}$:

$$E_{n+1} > \pi_1 \pi_2 \dots \pi_{n+1} \left(E_1 - h_0^2 \Phi_2 - \dots - h_0^{2m_0} \Phi_{m_0+1} - \frac{h_0^{2m_0+2} c_0 (\tau k)^{2m_0+4} l^{\frac{1}{k}} \left(l^{\frac{1}{k}} - \frac{1}{2k^2} - \frac{1}{k} - 1\right)}{1 - l^{\frac{1}{k}} (\tau k)^2 h_0^2}\right). \quad (5,2,31)$$

Для того чтобы значение скобки было наибольшее, нужно взять такое k, в котором функция $k^2 l^{\frac{1}{k}}$ достигает минимума. Этим значением будет $k = \frac{1}{2}$.

Мы имеем $E_1^{(1)} < \tau$. Если взять $c_0 = 2$, $m_0 = 1$, $l = 1$, то условие (5,2,28) выполнено. Кроме того, учитывая, что $k = \frac{1}{2}$, $\tau = 2 \ln h_0$, (5,2,31) примет вид

$$E = E_{n+1} > \pi_1 \pi_2 \dots \pi_{n+1} \left(E_1 - h_0^2 \Phi_2 - \frac{h_0^4 2 (\ln h_0)^0 l^2 (l^2 - 5)}{1 - (l h_0 \ln h_0)^2}\right) \quad (5,2,32)$$

при условии, что выполняется (5,2,30) или эквивалентное ему неравенство

$$l h_0 \ln h_0 < 1.$$

Для этого оказывается достаточно положить $h_0 = 1{,}29$, откуда

$$\ln h_0 < 0{,}255. \tag{5,2,33}$$

Вычисления дают

$$lh_0 \ln h_0 < 0{,}9 < 1.$$

Далее, в силу (5,2,12) и (5,2,19)

$$E_1 = 1 - E_1^{(1)} = 1 - \sum_{\nu=r_1+1}^{r} \frac{2}{p_\nu} = 1 - 2\gamma_1 > 1 - 2\ln h_0.$$

Кроме того, из (5,2,23) и (5,2,16) вытекает оценка:

$$\Phi_2 < \frac{5}{4!}\tau^4 = \frac{5}{4!}(2\ln h_0)^4.$$

Учитывая численное значение всех нужных нам констант, без труда получаем

$$E > \frac{3}{10}\pi_1\pi_2 \ldots \pi_{n+1} = 0{,}3\prod_{\nu=1}^{r}\left(1 - \frac{2}{p_\nu}\right). \tag{5,2,34}$$

Положим $h = \frac{89}{69} < 1{,}29 = h_0$. Подставим эти значения в (5,2,11):

$$P(D, x; p_1, p_2, \ldots, p_r) > 0{,}3\frac{x}{D}\prod_{\nu=1}^{r}\left(1 - \frac{2}{p_\nu}\right) - R,$$

где

$$R < cp_r^{\frac{h+1}{h-1}} = cp_r^{7{,}9},$$

или

$$P(D, x; p_1, p_2, \ldots, p_r) > \frac{x}{D}\frac{0{,}3c}{\ln^2 p_r} - c_1 p_r^{7{,}9}.$$

При выборе h_0 были наложены условия

$$\frac{1}{p_1} < \ln h_0 \text{ и } 1 - \frac{2}{p_1} > \frac{1}{h_0^2}.$$

Для выполнения этих условий положим $p_1 = 7$. Числа 2, 3, 5, таким образом, не участвуют в «решете». Для того

чтобы они не входили в нашу последовательность, положим $D=2\cdot 3\cdot 5=30$ и будем рассматривать прогрессию

$$D\lambda+\Delta,\quad (\Delta, D)=1,\qquad 30\lambda+\Delta\leqslant x.$$

Пусть теперь $p_1, p_2, \ldots, p_r$ — все простые числа (кроме трех первых) $\leqslant x^{\frac{1}{8}}$.

p_r — наибольшее простое число, не превосходящее $x^{\frac{1}{8}}$. В таком случае

$$P(30, x, 7, 11, \ldots, p_r)>\frac{6hcx}{30(\ln x)^2}-c_1x^{\frac{7.9}{8}}.$$

Начиная с некоторого $x=x_0$, правая часть неравенства становится положительной и стремится к бесконечности, если $x\to\infty$.

В самом начале мы предположим, что для каждого числа p_i, участвующего в «решете», берется два вычета a_i и b_i, причем таких, что

$$a_i\neq b_i.$$

Это условие было наложено для того, чтобы упростить схему метода Бруна. На самом же деле в эту схему (с небольшими усложнениями) укладывается и случай, когда для некоторых чисел p_i (в количестве, скажем, не более чем $\ln x$)

$$a_i=b_i.$$

В таком случае множители

$$\left(1-\frac{2}{p_i}\right),$$

соответствующие этим числам и входящие в произведение

$$\prod_{j=1}^{r}\left(1-\frac{2}{p_j}\right), \tag{5,2,35}$$

будут заменены множителями

$$\left(1-\frac{1}{p_i}\right).$$

И если мы обозначим через N_1 произведение исключительных чисел

$$p_{i_1}p_{i_2}\dots p_{i_q}=N_1,$$

то в неравенстве (5,2,34) вместо произведения (5,2,35) появится произведение

$$\prod_{\substack{p_1\leqslant p_r\\ p_i\nmid N_1}}\left(1-\frac{2}{p_i}\right)\prod_{p_i\mid N_1}\left(1-\frac{1}{p_i}\right).$$

Его можно преобразовать к виду

$$\prod_{p_i\mid N}\left(1+\frac{1}{p_i-1}\right)\prod_{p_i\leqslant p_r}\left(1-\frac{2}{p_i}\right).$$

И, следовательно, в общем случае получим оценку

$$P(30,\ x,\ 7,\ 11,\ \dots,\ p_r)>\frac{64cx}{30(\ln x)^2}\prod_{p\mid N_1}\left(1-\frac{1}{p-1}\right)-c_1x^{\frac{7,9}{8}}. \qquad (5,2,36)$$

Заметим, что всегда выполняется неравенство

$$P(2,\ x,\ 3,\ 5,\ 7,\ \dots,\ p_r)\geqslant P(30,\ x,\ 7,\ 11,\ \dots,\ p_r).$$

Поэтому, начиная с некоторого $x\geqslant x_0$, получаем самую общую оценку снизу:

$$P(2,\ x,\ 3,\ \dots,\ p_r)>c\prod_{p\mid N_1}\left(1+\frac{1}{p-1}\right)\frac{x}{\ln^2 x}. \qquad (5,2,37)$$

Задавая вычеты $a_i=0$, $b_i=-2$, мы получаем теорему о почти простых «близнецах».

Теорема 5.2.1. *Существует бесконечно много пар чисел, q, $q+2$, таких, что каждое из них имеет не более 7 простых множителей.*

Если же мы положим $x=2N$ и зададим вычеты таблицей

$$\begin{aligned} a_i&\equiv 0\ (\mathrm{mod}\ p_i),\\ b_i&\equiv 2N\ (\mathrm{mod}\ p_i),\end{aligned}\qquad \text{если } p_i\nmid 2N,$$

и $a_i=b_i=0$, если $p_i\mid 2N$, то получим вторую теорему.

Теорема 5.2.2. *Существует такое* N_0, *что при* $N > N_0$ *всегда имеет место решение уравнения*

$$2N = q_1 + q_2,$$

где q_1 *и* q_2 *— почти простые числа, имеющие не более 7 простых множителей.*

Заметим, что константа 7 не является наилучшей. Ее можно уменьшить этим же методом, но для этого потребовалось бы значительно усложнить выкладки.

Оценка сверху для функции

$$P(D, x; p_1, \ldots, p_r)$$

производится совершенно аналогичным путем, с той только разницей, что мы начинаем выбрасывать «лишние» числа на нечетном числе. В результате получим

$$P(2, x, 3, 5, \ldots, p_r) < c \prod_{p \mid N_1} \left(1 + \frac{1}{p-1}\right) \frac{x}{\ln^2 x}.$$

Надо сказать, что константа c в этой оценке получается довольно большой.

ГЛАВА 6

МЕТОД АТЛЕ СЕЛЬБЕРГА

§ 1. Оценки А. Сельберга

В 1946 г. норвежский математик Атле Сельберг [45] предложил другую идею для получения оценок сверху методом решета. Они значительно превосходят по точности верхние оценки В. Бруна, изложенные в предыдущей главе. С изложения существа этой новой идеи на примере бинарной задачи мы и начнем эту главу.

Обозначим через $P(N)$ число решений уравнения

$$N = P_1 + P_2,$$

где N — целое четное число, P_1, P_2 — простые и каждое из них $> \sqrt{N}$. Через Q обозначим произведение всех простых $\leqslant \sqrt{N}$. В таком случае, используя известные свойства функции Мёбиуса, можем записать:

$$P(N) = \sum_{a_n} \sum_{\substack{d \mid a_n \\ d \mid Q}} \mu(d), \qquad a_n = n(N-n)\,(n \leqslant N). \quad (6,1,1)$$

(В дальнейшем для упрощения, мы будем опускать условие $d \mid Q$, подразумевая его.) К сожалению, точная формула (6,1,1) для $P(N)$ ничего не дает в таком виде.

Идея верхней оценки Сельберга заключается в том, чтобы заменить сумму $\sum_{d \mid a_n} \mu(d)$ в (6,1,1) другой суммой $\sum_{\substack{d \mid a_n \\ d \leqslant z}} \rho_d$, где $z \leqslant N^{1-\varepsilon}$, с условием, что всегда

$$\sum_{d \mid a_n} \mu(d) \leqslant \sum_{d \mid a_n} \rho_d, \quad (6,1,2)$$

и получить возможность перемены суммирования.

В нашем конкретном случае эту идею можно осуществить так. Положим:

$$\rho_1 = \lambda_1 = 1,$$

$$\rho_d = \sum_{\substack{d=\frac{d_1 d_2}{k}, \\ d_1 \leqslant \sqrt{z},\ d_2 \leqslant \sqrt{z}, \\ \rho_d = 0,\ d > z.}} \lambda_{d_1}\lambda_{d_2}, \qquad 1 < d \leqslant z, \tag{6,1,3}$$

Все делители в (6,1,3) бесквадратны.

λ_d при $d > 1$ — пока произвольные вещественные числа. Их величинами мы распорядимся в дальнейшем.

Если условия (6,1,3) выполнены, то мы получаем

$$\sum_{\substack{d \mid a_n \\ d \leqslant z}} \rho_d = \Big(\sum_{\substack{d \mid a_n \\ d \leqslant \sqrt{z}}} \lambda_d\Big)^2 \geqslant \sum_{d \mid a_n} \mu(d).$$

Таким образом, неравенство (6,1,2) действительно удовлетворено, и мы получаем оценку

$$P(N) \leqslant \sum_{a_n} \sum_{\substack{d \mid a_n \\ d \leqslant z}} \rho_d = \sum_{a_n} \Big(\sum_{\substack{d \mid a_n \\ d \leqslant \sqrt{z}}} \lambda_d\Big)^2. \tag{6,1,4}$$

Если квадрат суммы представить в виде двойной суммы и изменить порядок суммирования, то (6,1,4) примет вид

$$P(N) \leqslant \sum_{d_1 \leqslant \sqrt{z}} \sum_{d_2 \leqslant \sqrt{z}} \lambda_{d_1}\lambda_{d_2} \sum_{\substack{a_n \equiv 0 \left(\mathrm{mod}\ \frac{d_1 d_2}{k}\right) \\ k = (d_1, d_2)}} 1. \tag{6,1,5}$$

Внутренняя сумма единиц вычисляется аналогично сумме (5,1,4) и равна величине

$$N \frac{\tau_N\left(\frac{d_1 d_2}{k}\right)}{\frac{d_1 d_2}{k}} + \theta \tau_N\left(\frac{d_1 d_2}{k}\right), \tag{6,1,6}$$

где

$$\tau_N(d) = \tau\left(\frac{d}{(d, N)}\right). \tag{6,1,7}$$

Кроме того, для бесквадратных d_1 и d_2 справедливо равенство

$$\tau_N\left(\frac{d_1 d_2}{k}\right)=\frac{\tau_N(d_1)\tau_N(d_2)}{\tau_N(k)}. \qquad (6,1,8)$$

Введем обозначение

$$f(d)=\frac{d}{\tau_N(d)} \qquad (6,1,9)$$

и подставим (6,1,6) в (6,1,5) с учетом (6,1,8) и (6,1,9)

$$P(N)\leqslant N\sum_{d_1\leqslant\sqrt{z}}\sum_{d_2\leqslant\sqrt{z}}\frac{\lambda_{d_1}}{f(d_1)}\frac{\lambda_{d_2}}{f(d_2)}f(k)+$$
$$+\sum_{d_1\leqslant\sqrt{z}}\sum_{d_2\leqslant\sqrt{z}}|\lambda_{d_1}||\lambda_{d_2}|\tau_N(d_1)\tau_N(d_2). \qquad (6,1,10)$$

Кроме того, если ввести сумму

$$R=\sum_{d\leqslant\sqrt{z}}|\lambda_d|\tau(d) \qquad (6,1,11)$$

и учесть, что $\tau_N(d)\leqslant\tau(d)$, то вторая двойная сумма в (6,1,10) не превосходит величины R^2; поэтому

$$P(N)\leqslant N\sum_{d_1\leqslant\sqrt{z}}\sum_{d_2\leqslant\sqrt{z}}\frac{\lambda_{d_1}\cdot\lambda_{d_2}}{f(d_1)\cdot f(d_2)}f(k)+R^2. \qquad (6,1,12)$$

Займемся исследованием двойной суммы в (6,1,12). Введем функцию

$$f_1(r)=f(r)\prod_{p\mid r}\left(1-\frac{1}{f(p)}\right). \qquad (6,1,13)$$

Для нее выполняется равенство

$$f(k)=\sum_{d\mid k}f_1(d).$$

Следовательно,

$$\sum_{d_1 \leqslant \sqrt{z}} \sum_{d_2 \leqslant \sqrt{z}} \frac{\lambda_{d_1} \cdot \lambda_{d_2}}{f(d_1) \cdot f(d_2)} f(k) =$$

$$= \sum_{d_1 \leqslant \sqrt{z}} \sum_{d_2 \leqslant \sqrt{z}} \frac{\lambda_{d_1} \cdot \lambda_{d_2}}{f(d_1) \cdot f(d_2)} \sum_{\substack{r \mid d_1 \\ r \mid d_2}} f_1(d) =$$

$$= \sum_{r \leqslant \sqrt{z}} f_1(r) y_r^2, \quad (6,1,14)$$

где

$$y_r = \sum_{\substack{r \mid d \\ d \leqslant \sqrt{z}}} \frac{\lambda_d}{f(d)}. \quad (6,1,15)$$

Мы получили квадратичную форму. Здесь наступил момент, когда следует воспользоваться произвольностью λ_d при $d > 1$ и выбрать их так, чтобы значение квадратичной формы было минимальным при $\lambda_1 = 1$.

Для нахождения этого минимума заменим условие $\lambda_1 = 1$ другим, из него вытекающим. Умножим правую и левую части равенства (6,1,15) на $\mu(r)$ и просуммируем по всем $r \leqslant \sqrt{z}$.

В результате получим

$$\sum_{r \leqslant \sqrt{z}} \mu(r) y_r = \sum_{r \leqslant \sqrt{z}} \mu(r) \sum_{\substack{r \mid d \\ d \leqslant \sqrt{z}}} \frac{\lambda_d}{f(d)} = \sum_{d \leqslant \sqrt{z}} \frac{\lambda_d}{f(d)} \sum_{r \mid d} \mu(d) = \lambda_1 = 1,$$

т. е.

$$\sum_{r \leqslant \sqrt{z}} \mu(r) y_r = 1. \quad (6,1,16)$$

Следовательно, нам нужно найти минимум квадратичной формы (6,1,14) при дополнительном условии (6,1,16).

Применим искусственный прием. Рассмотрим новую функцию

$$F(y_1, y_2, \ldots, y_{[\sqrt{z}]}, \omega) = \sum_{r \leqslant \sqrt{z}} f_1(r) y_r^2 - 2\omega \sum_{r \leqslant \sqrt{z}} \mu(r) y_r, \quad (6,1,17)$$

где ω — пока произвольная вещественная величина. Минимум F при условии (6,1,16) связан с искомым минимумом равенством

$$\min E = \min \Big(\sum_{r \leqslant \sqrt{z}} f_1(r) y_r^2 \Big) - 2 \max \omega. \qquad (6,1,18)$$

Но функцию F мы можем преобразовать:

$$F(y_1, y_2, \ldots, y_{[\sqrt{z}]}, \omega) = \sum_{r \leqslant \sqrt{z}} f_1(r) \Big(y_r - \omega \frac{\mu(r)}{f_1(r)} \Big)^2 - \omega^2 \sum_{r \leqslant \sqrt{z}} \frac{\mu^2(r)}{f_1(r)}.$$

Из этого равенства заключаем, что в точке минимума F непременно должно выполняться равенство

$$y_r = \max \omega \frac{\mu(r)}{f_1(r)}. \qquad (6,1,19)$$

Следовательно,

$$\min F = -(\max \omega)^2 \sum_{r \leqslant \sqrt{z}} \frac{\mu^2(r)}{f_1(r)}. \qquad (6,1,20)$$

Для определения величины $\max \omega$ подставим (6,1,19) в (6,1,16) и найдем

$$\max \omega = \frac{1}{\sum\limits_{r \leqslant \sqrt{z}} \frac{\mu^2(r)}{f_1(r)}}. \qquad (6,1,21)$$

Из сопоставления равенств (6,1,18), (6,1,20) и (6,1,21) получаем

$$\min \sum_{r \leqslant \sqrt{z}} f_1(r) y_r^2 = \frac{1}{\sum\limits_{r \leqslant \sqrt{z}} \frac{\mu^2(r)}{f_1(r)}}. \qquad (6,1,22)$$

Неравенство (6,1,12) приобретает вид

$$P(N) \leqslant \frac{N}{\sum\limits_{n \leqslant \sqrt{z}} \frac{\mu^2(n)}{f_1(n)}} + R^2. \qquad (6,1,23)$$

Для завершения оценки нам нужно вычислить сумму в знаменателе правой части (6,1,23) и оценить величину R.

Начнем с оценки R. Напомним, что

$$R = \sum_{d \leqslant \sqrt{z}} |\lambda_d| \tau(d).$$

С помощью формулы обращения выразим λ_d через сумму значений φ_r. В равенстве (6,1,15) положим $r = mk$

$$y_{mk} = \sum_{\substack{mk \mid d \\ d \leqslant \sqrt{z}}} \frac{\lambda_d}{f(d)}.$$

Умножим правую и левую части этого равенства на $\mu(k)$ и просуммируем по всем $k \leqslant \frac{\sqrt{z}}{m}$, $(k, m) = 1$.

$$\sum_{\substack{k \leqslant \frac{\sqrt{z}}{m} \\ (k, m) = 1}} \mu(k) y_{mk} = \sum_{\substack{k \leqslant \frac{\sqrt{z}}{m} \\ (k, m) = 1}} \mu(k) \sum_{\substack{mk \mid d \\ d \leqslant \sqrt{z}}} \frac{\lambda_d}{f(d)} =$$

$$= \sum_{\substack{k \leqslant \frac{\sqrt{z}}{m} \\ (k, \nu) = 1}} \mu(k) \sum_{\substack{k \mid \nu \\ \nu \leqslant \frac{\sqrt{z}}{m} \\ (m, \nu) = 1}} \frac{\lambda_{m\nu}}{f(m\nu)} = \sum_{\nu \leqslant \frac{\sqrt{z}}{m}} \frac{\lambda_{m\nu}}{f(m\nu)} \sum_{k \mid \nu} \mu(k) = \frac{\lambda_m}{f(m)}.$$

Следовательно,

$$\lambda_m = f(m) \sum_{\substack{k \leqslant \frac{\sqrt{z}}{m} \\ (k, m) = 1}} \mu(k) y_{mk}. \qquad (6,1,24)$$

Подставим в равенство (6,1,19) значение $\max \omega$ из (6,1,21):

$$y_r = \frac{\mu(r)}{f_1(r)} \frac{1}{\sum\limits_{n \leqslant \sqrt{z}} \frac{\mu^2(n)}{f_1(n)}}.$$

Получив значение y_r, находим λ_m:

$$\lambda_m = \mu(m) \frac{f(m)}{f_1(m)} \frac{1}{\sum\limits_{n \leqslant \sqrt{z}} \frac{\mu^2(n)}{f_1(n)}} \sum_{\substack{k \leqslant \frac{\sqrt{z}}{m} \\ (k, m) = 1}} \frac{\mu^2(k)}{f_1(k)}.$$

Из этого равенства уже тривиально следует оценка

$$|\lambda_m| \leqslant \frac{f(m)}{f_1(m)} = \prod_{p|m} \left(1 - \frac{1}{f(p)}\right)^{-1}.$$

Рассмотрим полученное произведение. Мы имели $f(r) = 1$, $f(p) \leqslant 2$, если $p \geqslant 3$, следовательно,

$$\prod_{p|m} \left(1 - \frac{1}{f(p)}\right)^{-1} \leqslant 2 \prod_{\substack{p|m \\ p \geqslant 3}} \left(1 - \frac{2}{p}\right)^{-1} \leqslant$$

$$\leqslant 2 \prod_{3 \leqslant p \leqslant m} \left(1 - \frac{2}{p}\right)^{-1} < c (\ln m)^2.$$

Заменяя в этой оценке простые делители числа m всеми простыми до m, мы, конечно, даем очень грубую оценку этому произведению. Но это не повлияет на конечный результат. Таким образом,

$$|\lambda_m| \leqslant c (\ln m)^2.$$

Подставляя эту оценку в R, получим

$$R \leqslant c \ln^2 N \sum_{d \leqslant \sqrt{z}} \tau(d) < c \sqrt{z} \ln^3 N,$$

или

$$R^2 < c_1 z \ln^6 N. \qquad (6,1,25)$$

Для завершения оценки $P(N)$ нам осталось вычислить

$$S(N, z) = \sum_{n \leqslant \sqrt{z}} \frac{\mu^2(n)}{f_1(n)}.$$

Детального вычисления этой суммы мы не будем приводить, для того чтобы не загромождать текст длинными выкладками. Наметим только основные шаги элементарного вычисления этой суммы. Читатель, если пожелает, может сам

без труда восстановить их. Разбиваем нашу сумму по делителям числа N:

$$\sum_{n\leqslant\sqrt{z}}\frac{\mu^2(n)}{f_1(n)}=\sum_{\substack{d\mid N\\ d\leqslant\sqrt{z}}}\sum_{\substack{d\mid n\\ n\leqslant\sqrt{z}\\ (n,N)=1}}\frac{\mu^2(n)}{f(n)\prod\left(1-\frac{1}{f(p)}\right)}=$$

$$=\sum_{\substack{d\mid N\\ d\leqslant\sqrt{z}}}\frac{1}{\varphi(d)}\sum_{\substack{n\leqslant\frac{\sqrt{z}}{d}\\ (n,N)=1}}\frac{\mu^2(n)\tau(n)}{n\prod_{p\mid n}\left(1-\frac{2}{p}\right)}=\sum_{d\mid N}\frac{S_d}{\varphi(d)}=$$

$$=\sum_{\substack{d\mid N\\ d\leqslant\exp(\sqrt{\ln r})}}\frac{S_d}{\varphi(d)}+\sum_{\substack{d\mid N\\ d>\exp(\sqrt{\ln r})}}\frac{S_d}{\varphi(d)},\qquad(6,1,26)$$

где $\varphi(d)$ — функция Эйлера.

Второй шаг — оцениваем S_d для $d\leqslant\exp(\sqrt{\ln r})$

$$S_d=\sum_{\substack{n\leqslant x\\ (n,N)=1}}\frac{\mu^2(n)\tau(n)}{n}\prod_{p\mid n}\left(1+\frac{2}{p-2}\right)=$$

$$=\sum_{\substack{n\leqslant x\\ (n,N)=1}}\frac{\mu^2(n)\tau(n)}{n}\sum_{d\mid n}\frac{\tau(d)}{\varphi_1(d)}=\sum_{d\leqslant x}\frac{\mu^2(d)\tau^2(d)}{\varphi_1(d)d}\sum_{\substack{n\leqslant\frac{x}{d}\\ (n,dN)=1}}\frac{\mu^2(n)\tau(n)}{n}.$$

Внутренняя сумма уже вычисляется элементарно по схеме

$$\sum_{\substack{n\leqslant\frac{x}{d}\\ (n,Nd)=1}}\frac{\mu^2(n)\tau(n)}{n}=\sum_{n\leqslant\frac{x}{d}}\frac{\tau(n)}{n}\left(\sum_{\substack{\nu\mid Nd\\ \nu\mid n}}\mu(\nu)\right)\left(\sum_{r^2\mid n}\mu(r)\right).$$

Изменяя порядки суммирования, мы сведем все к сумме

$$\sum_{n\leqslant y}\frac{\tau(n)}{n}=\frac{1}{2}\ln^2 y+O(\ln y).$$

Подставляя значение вычисленной суммы в S_d и заменяя суммы произведениями, найдем

$$S_d = \frac{1}{2} \prod_{\substack{p \nmid N \\ p \leqslant N}} \left(1 - \frac{1}{(p-1)^2}\right)^{-1} \ln^2 \frac{\sqrt{z}}{d} + O(\ln z).$$

Из этой оценки получаем

$$\sum_{\substack{d \mid N \\ d \leqslant \exp(\sqrt{\ln z})}} \frac{S_d}{\varphi(d)} = \frac{1}{2} \prod_{p \mid N} \left(1 - \frac{1}{p}\right) \prod_{\substack{n \nmid N \\ p \leqslant N}} \left(1 - \frac{1}{(p-1)^2}\right)^{-1} \ln^2 z + O(\ln^{1,5} z \ln\ln z). \quad (6,1,27)$$

Если же $d > \exp(\sqrt{\ln z})$, то применим тривиальную оценку

$$S_d \leqslant S_1 \leqslant c \ln^2 z.$$

$$\sum_{\substack{d \mid N \\ d > \exp(\sqrt{\ln z})}} \frac{S_d}{\varphi(d)} < c \ln z \sum_{k \geqslant 1} \sum_{\substack{p_1 \dots p_k \mid N \\ p_1 \dots p_k > \exp(\sqrt{\ln z})}} \frac{1}{\varphi(p_1 \dots p_k)}.$$

Но число N может иметь не более $2 \frac{\ln N}{\ln\ln N}$ различных простых множителей.

Если $k \leqslant \frac{\sqrt{\ln z}}{\ln\ln^2 N}$, то применяем тривиальную оценку ($\omega(N)$ — число простых делителей N):

$$\sum_{\substack{p_1 \dots p_k \mid N \\ p_1 \dots p_k > \exp(\sqrt{\ln z})}} \frac{1}{\varphi(p_1 \dots p_k)} \leqslant \omega^k(N) \exp\left(-\sqrt{\ln z}\right) \prod_{p \mid N} \frac{1}{\left(1 - \frac{1}{p}\right)} \leqslant$$

$$\leqslant c\omega^k(N) \ln N \exp\left(-\sqrt{\ln z}\right) \leqslant \exp\left(-\frac{1}{2}\sqrt{\ln z}\right).$$

Если же $k > \frac{\sqrt{\ln z}}{\ln\ln^2 z}$, то

$$\sum_{\substack{p_1 \dots p_k \mid N \\ p_1 \dots p_k > \exp(\sqrt{\ln z})}} \frac{1}{\varphi(p_1 \dots p_k)} \leqslant \frac{\left(\sum\limits_{p_i \mid N} \frac{1}{p_i - 1}\right)^k}{k!} \leqslant \exp\left(-\frac{1}{2}\sqrt{\ln z}\right).$$

Соединяя эти оценки, получаем

$$\sum_{\substack{d \mid N \\ d > \exp(\sqrt{\ln z})}} \frac{S_d}{\varphi(d)} < c \ln z \exp\left(-\frac{1}{2}\sqrt{\ln z}\right) < c_1.$$

Подставляя это неравенство и (6,1,27) в (6,1,26), окончательно найдем

$$\sum_{n \leqslant \sqrt{z}} \frac{\mu^2(n)}{f_1(n)} = \frac{1}{2} \prod_{p \mid N}\left(1 - \frac{1}{p}\right) \prod_{\substack{p \nmid N \\ p \leqslant N}}\left(1 - \frac{1}{(p-1)^2}\right)^{-1} \ln^2 \sqrt{z} + \\ + O(\ln^{1,5} z \ln \ln z).$$

Подставляем это равенство и оценку (6,1,25) в (6,1,23):

$$P(N) \leqslant 8G(N) \frac{N}{\ln^2 z} + c' \frac{N}{(\ln z)^{2,5}} \ln \ln^3 N + cz \ln^6 N,$$

и если положим $z = \frac{N}{\ln^9 N}$, то

$$P(N) \leqslant 8\left(1 + c \frac{\ln \ln^2 N}{\sqrt{\ln N}}\right) G(N) \frac{N}{\ln^2 N},$$

где

$$G(N) = \prod_{p \mid N}\left(1 + \frac{1}{p-1}\right) \prod_{\substack{p \nmid N \\ p < N}}\left(1 - \frac{1}{(p-1)^2}\right).$$

Совершенно аналогично можно получить оценку сверху для количества пар «близнецов»:

$$\pi_2(x) \leqslant 8G \frac{x}{\ln^2 x}\left(1 + c \frac{\ln \ln^2 x}{\sqrt{\ln x}}\right),$$

где

$$G = 2 \prod_{N > p > 2}\left(1 - \frac{1}{(p-1)^2}\right).$$

Эти оценки отличаются от предполагаемых в 8 раз.

§ 2. Теорема Шнирельмана

Важное приложение оценок сверху для $P(N)$ дал Л. Г. Шнирельман в 1930 г. [30]. Соединив эту оценку со своим плотностным методом, он получил следующую теорему.

Теорема 6.2.1. *Каждое целое число представимо в виде суммы не более чем c_0 простых слагаемых, где c_0 — абсолютная положительная постоянная.*

Эта теорема была первым принципиальным шагом в решении аддитивных задач с простыми числами. Константа Шнирельмана c_0 имела значение $8 \cdot 10^5$. В дальнейшем она снижалась и в 1951 г. Шапиро и Варга с помощью оценок А. Сельберга получили $c_0 \leqslant 20$. Более сложными аналитическими методами И. М. Виноградовым в 1937 г. было получено $c_0 \leqslant 4$ для всех достаточно больших чисел.

Перейдем к доказательству теоремы Шнирельмана. Пусть $n' \leqslant x$ — числа, представимые в виде суммы двух простых слагаемых. Применим неравенство Шварца

$$\Big(\sum_{n \leqslant x} P(n)\Big)^2 \leqslant \Big(\sum_{n \leqslant x} P^2(n)\Big)\Big(\sum_{n' \leqslant x} 1\Big).$$

Из него вытекает оценка снизу для количества чисел $n' \leqslant x$:

$$\sum_{n' \leqslant x} 1 \geqslant \frac{\Big(\sum\limits_{n \leqslant x} P(n)\Big)^2}{\sum\limits_{n \leqslant x} P^2(n)}. \tag{6,2,1}$$

Для числителя мы должны получить оценку снизу, а для знаменателя сверху. Оценим числитель:

$$\sum_{n \leqslant x} P(n) \geqslant \sum_{\substack{P_1 + P_2 \leqslant x \\ P_1,\, P_2 \leqslant \frac{x}{2}}} 1 = \pi^2\left(\frac{x}{2}\right) \geqslant 0{,}9\,\frac{x^2}{4 \ln^2 x}.$$

Следовательно,

$$\Big(\sum_{n \leqslant x} P(n)\Big)^2 \geqslant c\,\frac{x^4}{\ln^4 x}, \tag{6,2,2}$$

где $c > 0$ — абсолютная постоянная.

Оценим знаменатель, для этого воспользуемся оценкой сверху в общем виде:

$$P(n) \leqslant c \prod_{p \mid n}\left(1 + \frac{1}{p}\right)\frac{n}{\ln^2 n},$$

$$\sum_{n \leqslant x} P^2(n) \leqslant c_1\,\frac{x^2}{\ln^4 x} \sum_{n \leqslant x} \prod_{p \mid n}\left(1 + \frac{1}{p}\right)^2. \tag{6,2,3}$$

Вычислим сумму в (6,2,3)

$$\sum_{n\leqslant x}\prod_{p\mid n}\left(1+\frac{1}{p}\right)^2=\sum_{n\leqslant x}\left(\sum_{d\mid n}\frac{1}{d}\right)^2=$$

$$=\sum_{d_1d_2\leqslant x}\sum\frac{1}{d_1d_2}\sum_{\substack{\frac{d_1d_2}{k}\mid n\\ n\leqslant x}}1\leqslant x\sum_{\substack{d_1d_2\leqslant x\\ k=(d_1,\,d_2)}}\sum\frac{k}{(d_1d_2)^2}+\sum_{d_1d_2\leqslant x}\sum\frac{1}{d_1d_2}\leqslant$$

$$\leqslant x\sum_{k\leqslant x}\frac{1}{k^3}\sum_{\substack{\nu_1\nu_2\leqslant x\\ (\nu_1,\,\nu_2)=1}}\sum\frac{1}{\nu_1^2\nu_2^2}+\sum_{n\leqslant x}\frac{\tau(n)}{n}\leqslant$$

$$\leqslant x\left(\sum_{k\leqslant x}\frac{1}{k^3}\right)\left(\sum_{\nu\leqslant x}\frac{1}{\nu^2}\right)^2+c'\ln^2 x\leqslant c''x,$$

где c'' — абсолютная постоянная.

Подставляя эту оценку в (6,2,3), получаем

$$\sum_{n\leqslant x}P^2(n)\leqslant c_2\frac{x^3}{\ln^4 x}. \tag{6,2,4}$$

Из неравенств (6,2,4), (6,2,2) и (6,2,1) находим оценку снизу

$$\sum_{n'\leqslant x}1>\alpha_0 x, \tag{6,2,5}$$

где $\alpha_0>0$ — абсолютная положительная постоянная.

Составим последовательность чисел

$$1,\ n_1',\ n_2',\ \ldots, \tag{A}$$

т. е. 1 и все числа, представимые как два простых. На основании оценки (6,2,5) мы можем сказать, что последовательность (A) имеет положительную плотность в смысле Шнирельмана. Следовательно, (A) может служить базисом натурального ряда. Или, другими словами, существует такое целое число k, зависящее только от α_0, что любое число m есть

сумма не более k слагаемых из (A):

$$m = \sum_{i \leqslant k} n_i' + \sum 1, \tag{6,2,6}$$

причем сумма единиц в (6,2,6) имеет не более k слагаемых и ее можно представить в виде суммы двоек и троек, а каждое $n_i = p_i + p_i'$. Следовательно,

$$m = \sum_{\nu \leqslant 3k} p_\nu,$$

и теорема Шнирельмана доказана.

ГЛАВА 7

О РАСПРЕДЕЛЕНИИ ДРОБНЫХ ЧАСТЕЙ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

§ 1. Постановка вопроса

Пусть дана последовательность вещественных чисел

$$\beta_1, \beta_2, \ldots, \beta_n, \ldots \tag{7,1,1}$$

Находим для каждого ее члена β_j его дробную часть $\{\beta_j\}$ (см. определение в [3]) и составим соответствующую последовательность дробных частей

$$\{\beta_1\}, \{\beta_2\}, \ldots, \{\beta_n\}, \ldots \tag{7,1,2}$$

Все числа (7,1,2) лежат на отрезке $[0, 1)$. Для многих вопросов теории чисел важно знать распределение чисел (7,1,2) на отрезке $[0, 1)$. Введем понятие о функции распределения дробных частей β_j. Для $0 \leqslant \gamma < 1$ обозначим через $\nu_n(\gamma)$ количество значений $\{\beta_j\}$ таких, что $j \leqslant n$ и $\{\beta_j\} < \gamma$. Функция

$$V_n(\gamma) = \frac{\nu_n(\gamma)}{n} \tag{7,1,3}$$

показывает распределение первых n членов последовательности (7,1,2) на сегменте $[0, 1)$. Если для всякого γ существует предел:

$$\lim_{n \to \infty} V_n(\gamma) = V(\gamma), \tag{7,1,4}$$

то $V(\gamma)$ называется функцией распределения (7,1,2). При этом $V(\gamma)$ — неубывающая функция; $V(0) = 0$; $V(1) = 1$. Особенно важен случай, когда $V(\gamma) = \gamma$; в этом случае последовательность (7,1,2) называется равномерно распределенной (или равнораспределенной) на отрезке $[0, 1)$. Если для равномерно распределенной последовательности (7,1,2) задать какой-либо сегмент

$[\alpha_1, \alpha_2] \subset [0, 1)$, то при достаточно большом n количество членов (7,1,2), лежащих в $[\alpha_1, \alpha_2]$, будет иметь вид

$$(\alpha_2 - \alpha_1)\, n + o(n). \qquad (7,1,5)$$

Весьма существенны при этом более точные оценки остаточного члена (7,1,5), т. е. получение выражений вида

$$\nu_n(\gamma) = \gamma n + O\left(\frac{n}{\rho(n)}\right), \qquad (7,1,6)$$

где $\rho(n) = n^{\alpha_0}$, $\rho(n) = (\ln n)^K$ и т. п.

В аналитической теории чисел часто возникают вопросы о распределении последовательностей вида $\{\alpha f(n)\}$, где α — заданное число, а $f(n)$ — целочисленная последовательность. Если α рационально, так что $\alpha = \frac{a}{q}$; $(a, q) = 1$, то, очевидно, $\{\alpha f(n)\}$ может принимать лишь значения $0, \frac{1}{q}, \frac{2}{q}, \ldots, \frac{q-1}{q}$, и потому равномерного распределения не может быть. Однако, если α иррационально, то равномерное распределение $\{\alpha f(n)\}$ является довольно обычным явлением. Так, если $f(n) = a_0 n^k + a_1 n^{k-1} + \ldots + a_k$ — целочисленный полином степени $k \geqslant 1$, то $\{\alpha f(n)\}$ равномерно распределена. И. М. Виноградов [1] доказал в 1937 г., что последовательность $\{\alpha p\}$, где p пробегает подряд простые числа, α иррационально, равномерно распределена. Это свойство простых чисел легло в основу данного И. М. Виноградовым решения проблемы Гольдбаха. Элементарное доказательство теоремы о равномерной распределенности полиномиальных последовательностей с соответствующими количественными оценками дано в работе И. М. Виноградова [4]. Оно представляет собой элементарный вариант метода Г. Вейля оценки тригонометрических сумм [41]. Мы изложим здесь нужную нам часть этой работы, а также работу И. М. Виноградова [5] 1953 г., где элементарными методами изучается последовательность $\{\alpha p\}$. Будет изложена также одна вспомогательная теорема о дробных частях.

§ 2. Лемма о разностях

Следуя И. М. Виноградову [4], мы докажем здесь лемму, которая будет нам нужна в дальнейшем. Пусть дана система чисел

$$\beta_1 \leqslant \beta_2 \leqslant \ldots \leqslant \beta_n \ldots, \qquad (7,2,1)$$

лежащих в отрезке (0,1]. Составим дробные части разностей

$$\{\beta - \beta'\}, \tag{7,2,2}$$

где β и β' независимо пробегают числа $\beta_1, \beta_2, \ldots, \beta_n$. Пусть для любого $\gamma \in [0, 1)$ число T_n дробных долей (7,2,2), меньших γ, выражается формулой

$$T_n = n^2\gamma + B\Delta, \tag{7,2,3}$$

где $\Delta \geqslant n$ и B не зависит от n. Тогда для последовательности (7,2,1) имеем при любом $\rho \in [0, 1)$

$$\nu_n(\rho) = n\rho + B(n\Delta)^{\frac{1}{3}}. \tag{7,2,4}$$

Заметим сперва, что, не нарушая общности выводов, можем заменить каждое из чисел β_i на ближайшую к нему слева дробь $\frac{s}{n}$, s — целое (новое число β_i). Прежде всего, от такой замены числа $\beta - \beta'$ изменяются не более чем на $\frac{2}{n}$. Количество новых чисел $\{\beta - \beta'\}$, лежащих в отрезке $[0, \gamma)$, будет отличаться от количества старых чисел $\{\beta - \beta'\}$, согласно формуле (7,2,3), не более чем на $n^2\frac{2}{n} + B\Delta = 2n + B\Delta = B\Delta$ на основании неравенства для $B\Delta$. Таким образом, вид формулы (7,2,3) не меняется. Если теперь для новых чисел β_i из (7,2,3) выводится (7,2,4), то из (7,2,4) будет следовать, что новых чисел β_i в сегменте длины $\frac{1}{n}$ будет лежать $B + B\sqrt[3]{n\Delta} = B\sqrt[3]{n\Delta}$, так что формула (7,2,4) будет верна и для старых чисел β_i.

Ввиду этого можем считать, что $\beta_i = \frac{s_i}{n}$, где $0 \leqslant s_i < n$ — целые числа.

Пусть количество чисел (7,2,1), равных $\frac{s}{n}$ $(0 \leqslant s < n)$, есть α_s. Тогда количество дробей ряда (7,2,2), равных $\frac{z}{n}$ $(0 \leqslant z < n)$, будет

$$\sum_{s=0}^{n-1} \alpha_s \alpha_{s+z}, \tag{7,2,5}$$

где $s+z$ определяется по модулю n в отрезке $[0, n)$. Рассмотрим сумму

$$\sum_{s=0}^{n-1}\sum_{z=0}^{k-1}\alpha_{s+c}\alpha_{s+z}, \tag{7,2,6}$$

где c — какой-либо вычет по модулю n.

Согласно (7,2,3), имеем для (7,2,6) выражение

$$kn+B\Delta. \tag{7,2,7}$$

Положим

$$S_{s,k}=\sum_{z=0}^{k-1}\alpha_{s+z}.$$

Суммируя (7,2,6) по $c=0,1,\ldots,k-1$, найдем

$$\sum_{s=0}^{n-1}S_{s,k}^2=k^2n+Bk\Delta. \tag{7,2,8}$$

Положим теперь

$$S_{s,k}=k+\varepsilon_{s,k}. \tag{7,2,9}$$

Нашей задачей будет получение оценки для $|\varepsilon_{s,k}|$. Имеем, очевидно, $\sum_{s=0}^{n-1}S_{s,k}=kn$; $\sum_{s=0}^{n-1}k=kn$, откуда

$$\sum_{s=0}^{n-1}\varepsilon_{s,k}=0 \tag{7,2,10}$$

для любого k. Отсюда, в силу (7,2,9) и (7,2,8),

$$\sum_{s=0}^{n-1}\varepsilon_{s,k}^2=\sum_{s=0}^{n-1}(S_{s,k}-k)^2=$$

$$=\sum_{s=0}^{n-1}S_{s,k}^2+k^2n-2k^2n=Bk\Delta. \tag{7,2,11}$$

Суммируя по $k=1,\ldots,n$, найдем

$$\sum_{k=1}^{n}\sum_{s=0}^{n-1}\varepsilon_{s,k}^2=Bn^2\Delta. \tag{7,2,12}$$

Положим $n\vartheta_i = s_i$, и изобразим (см. рис. 1) каждое s_i в виде площади прямоугольника, ограниченного прямыми $x = i$, $x = i + 1$, $y = 0$, $y = s_i$ $(i = 0, 1, \ldots, n-1)$. Пусть при этом

$$\max(s_i - i) = \sigma'', \quad \min(s_i - i - 1) = \sigma', \quad \sigma'' - \sigma' = l. \quad (7,2,13)$$

На каждой горизонтальной прямой $y = 0, 1, \ldots, n-1$ отметим точку ее пересечения с заштрихованной областью (крайнюю

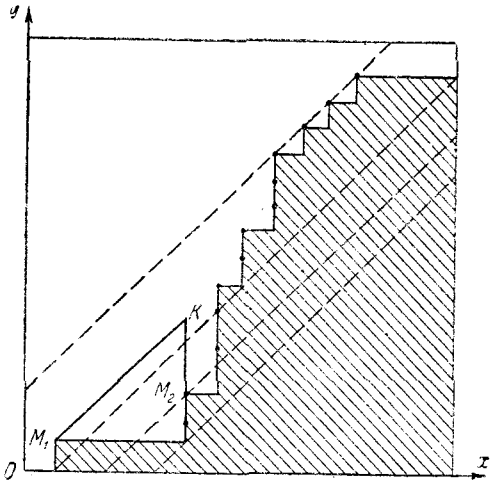

Рис. 1.

левую точку, если она не одна). Эти точки будем называть отмеченными. Пусть $M_1(x_1, s')$ и $M_2(x_2, s'')$ — две такие точки. Имеем, очевидно,

$$x_2 - x_1 = a_{s_1} + a_{s_1+1} + \ldots + a_{s_2-1} = s_2 - s_1 + \varepsilon_{s_1, s_2 - s_1},$$

где s_1, s_2 — отвечающие s', s'' точки на чертеже. Проведем прямую $y = x - x_1 + s_1$. Она пересечет прямую $x = x_2$ в некоторой точке $K(x_2, y_2)$. Имеем

$$y_2 - s_1 = x_2 - x_1 = s_2 - s_1 + \varepsilon_{s_1, s_2 - s_1} = \overline{M_2K},$$

где $\overline{M_2K}$ — расстояние между точками M_2 и K.

Таким образом, соотношение (7,2,12) дает

$$\sum_{M_2,\ K} \overline{M_2K}^2 = Bn^2\Delta, \tag{7,2,14}$$

где суммирование идет по парам M_2, K, причем то же K определяется отмеченными точками M_1 и M_2. Таким образом, для суммирования (7,2,14) нужно перебирать пары отмеченных точек M_1, M_2, находить точку K и определять $\overline{MK}^2$. Проведем прямую:

$$y = x + \frac{\sigma' + \sigma''}{2}. \tag{7,2,15}$$

Допустим, что число отмеченных точек выше этой прямой или на ней будет $\geqslant \frac{n}{2}$ (в противном случае такую оценку будет иметь число точек ниже нее или на ней, и мы рассуждали бы так же). Проведем еще прямую

$$y = x + \frac{3\sigma' + \sigma''}{4}. \tag{7,2,16}$$

Ниже нее или на ней имеется не менее

$$\left[\frac{\sigma'' - \sigma'}{4}\right] \geqslant \frac{l}{4} - 1 \tag{7,2,17}$$

отмеченных точек. Каждая из них может быть соединена с каждой из точек, лежащих на прямой (7,2,15) или выше. Соответственное значение $\overline{M_2K}$ будет $\geqslant \frac{1}{16} l^2$. Из (7,2,14) имеем

$$\frac{1}{16} l^2 \left(\frac{1}{4} l - 1\right) \frac{n}{2} = Bn^2\Delta, \quad l = B(n\Delta)^{\frac{1}{3}}. \tag{7,2,18}$$

Итак, вся ломаная линия лежит в полосе между прямыми $y = x + \sigma'$; $y = x + \sigma''$, где

$$\sigma'' - \sigma' = l = B(n\Delta)^{\frac{1}{3}} \qquad (\sigma'' \geqslant 0;\ \sigma' \leqslant 0).$$

Отсюда имеем: $\varepsilon_0 k = B(n\Delta)^{\frac{1}{3}}$, $S_{s,k} = k + B(n\Delta)^{\frac{1}{3}}$, что и доказывает лемму.

Последовательное применение этой леммы сводит вопрос о распределении последовательности $\{P_k(n)\}$, где $P_k(n)$ — по-

лином степени $k>1$ с иррациональным старшим коэффициентом, к вопросу о распределении дробных частей полинома низшей степени. Этим путем можно доказать, что для полиномов $P_k(n)$ указанного вида (где k может и равняться 1) $\{P_k(n)\}$ равномерно распределена. Мы не будем на этом останавливаться.

§ 3. Лемма о неполной системе вычетов

Пусть $p>1$ — простое число, которое будем в дальнейшем считать достаточно большим, и $f(x)$ — целочисленная функция, заданная при $x\equiv 0,\ 1,\ \ldots,\ p-1 \pmod p$. Пусть

$$s=0,\ 1,\ 2,\ \ldots,\ p-1. \tag{7,3,1}$$

Для каждого s составим новую целочисленную функцию с той же областью задания:

$$f_s(x)=f(x)+sx \tag{7,3,2}$$

и рассмотрим выражения

$$\left\{\frac{f_s(x)}{p}\right\}, \tag{7,3,3}$$

где x пробегает систему чисел $0,\ 1,\ 2,\ \ldots,\ p-1$. Пусть $\nu_{f_s}(\gamma)$ — количество дробей (7,3,3) под условием

$$0\leqslant\left\{\frac{f_s(x)}{p}\right\}<\gamma \qquad (0\leqslant\gamma<1). \tag{7,3,4}$$

Пусть известно, что при малом $s=0,\ 1,\ \ldots,\ p-1$ и любом $\gamma\in[0,\ 1)$ имеем

$$\nu_{f_s}(\gamma)=\gamma p+Bp^{1-\xi_0}. \tag{7,3,5}$$

Пусть p_1 — какое-либо число $\leqslant p$, и пусть t пробегает (вообще говоря, неполную) систему вычетов, состоящую из чисел $1,\ \ldots,\ p_1$. Нас будет интересовать функция $\mu_1(\gamma)$, показывающая, сколько раз происходит событие:

$$0\leqslant\left\{\frac{f(t)}{p}\right\}<\gamma, \tag{7,3,6}$$

когда t пробегает указанную систему вычетов. Методом тригонометрических сумм, разработанным И. М. Виноградовым, без труда можно показать, что

$$\mu_1(\gamma)=\gamma p_1+Bp^{1-\xi_0}\lg^2 p. \tag{7,3,7}$$

Мы будем исследовать тот же вопрос элементарным образом и докажем то же соотношение. Будем обозначать через (x); (t) области изменения аргументов x и t. Рассмотрим сумму

$$\sum_{s=0}^{p-1}\sum_{(x)}\sum_{(t)} V_\gamma\left(\left\{\frac{f(x)+s(x-t)}{p}\right\}\right), \tag{7,3,8}$$

где через $V_\gamma(u)$ обозначена функция, равная 1 при $0\leqslant u<\gamma$ и 0 при $\gamma\leqslant u<1$. Будем считать сперва, что γp — число не целое; как мы увидим из окончательного результата, это не нарушает общности. При $x=t$ из нашей суммы выделяется член

$$p\sum_{(t)} V_\gamma\left(\left\{\frac{f(t)}{p}\right\}\right), \tag{7,3,9}$$

который как раз нас интересует. Рассмотрим, какие члены получаются при $x\neq t$.

При данных x, t, для которых $x-t\not\equiv 0\pmod p$ выражение $s(x-t)$ при $s=0,\ 1,\ldots,\ p-1$ пробегает полную систему вычетов; то же касается выражения $f(x)+s(x-t)$. По определению функции $V_\gamma(u)$ суммирование по s в (7,3,8) при этих условиях дает величину

$$[\gamma p], \tag{7,3,10}$$

так как γp предположено нецелым. Таким образом, сумма (7,3,8) равна

$$p\sum_{(t)} V_\gamma\left(\left\{\frac{f(t)}{p}\right\}\right)+[\gamma p]p_1(p-1). \tag{7,3,11}$$

Ту же сумму (7,3,8) мы можем рассмотреть по-иному, фиксируя s и x и суммируя по t. Рассмотрим при данных s, x сумму

$$\sum_{(t)} V_\gamma\left(\left\{\frac{f(x)+sx-st}{p}\right\}\right). \tag{7,3,12}$$

При $s=0$ получаем член $V_\gamma\left(\left\{\frac{f(x)}{p}\right\}\right)\sum_{(t)}1$. Суммируя по x, получаем на основании условия (7,3,5) выражение

$$\gamma p_1 p+Bp_1 p^{1-\varepsilon_0}. \tag{7,3,13}$$

Пусть $s \neq 0$. Рассмотрим поведение суммы (7,3,12). Здесь t пробегает значения 1, 2, ..., p_1. Полагая $f(x)+sx=y_s$, рассматриваем сумму

$$\sum_{(t)} V_\tau\left(\left\{\frac{y_s - st}{p}\right\}\right). \tag{7,3,14}$$

§ 4. Сравнение двух сумм

Наряду с суммой (7,3,14) составим сумму

$$\sum_{(t)} V_\tau\left(\left\{\frac{x - st}{p}\right\}\right) \tag{7,4,1}$$

и рассмотрим разность

$$\sum_{(t)} V_\tau\left(\left\{\frac{y_s - st}{p}\right\}\right) - \sum_{(t)} V_\tau\left(\left\{\frac{x - st}{p}\right\}\right). \tag{7,4,2}$$

Представим число $\frac{s}{p}$ в виде

$$\frac{s}{p} = \frac{a_1}{q_1} + \frac{\theta_1}{q_1\tau_1}; \quad (a_1, q_1) = 1; \quad \tau_1 = p_1; \quad |\theta_1| \leqslant 1.$$

Если $q_1 \neq 1$ $a_1 \neq 0$. При этом $q_1 \leqslant p_1$. Из сегмента $[1, p_1]$ изменения t выделим, начиная с правого конца, полные системы вычетов $(\mathrm{mod}\, q_1)$; пусть таким образом выделено p_1' чисел, и остались числа 1, 2, ..., p_2, составляющие неполную систему вычетов $(\mathrm{mod}\, q_1)$. Представим $\frac{s}{p}$ в виде

$$\frac{a_2}{q_2} + \frac{\theta_2}{q_2\tau_2}; \quad \tau_2 = p_2; \quad |\theta_2| \leqslant 1; \quad (a_2, q_2) = 1.$$

Если при этом $q_2 = 1$, $a_2 = 0$, то на этом остановимся: если это не так, продолжим этот процесс далее, пока не придем к значению $q_k = 1$, $a_k = 0$. Так как $q_2 \leqslant \frac{1}{2} q_1$; $q_3 \leqslant \frac{1}{2} q_2, \ldots$, то число шагов нашего процесса будет $B \lg p$. Когда значение t пробегает полную систему вычетов $(\mathrm{mod}\, q_1)$, так же себя ведут и величины $y_s - a_1 t$ и $x - a_1 t$; при этом $\frac{\theta_1 t}{q_1\tau_1} = \frac{B}{q_1}$. Подобные же рассуждения применимы и к модулям $q_2, q_3, \ldots, q_{k-1}$ и, вводя понятным из предыдущего образом

обозначения p_2', p_3, p_3', p_4, ..., получим для (7,4,2) окончательное выражение

$$R(y_s, s) - R(x, s), \tag{7,4,3}$$

где

$$R(\xi, s) = B\left(\frac{p_1'}{q_1} + \frac{p_2'}{q_2} + \ldots + \frac{p_{k-1}'}{q_{k-1}} + p_k'\right) \tag{7,4,4}$$

для $\xi = 1, 2, \ldots, p-1$. Здесь учтено, что при $q_k = 1$, $a_k = 0$, мы можем лишь дать тривиальное значение для соответствующей суммы значений

$$V_\tau\left(\left\{\frac{y_s - st}{p}\right\}\right) - V_\tau\left(\left\{\frac{x - st}{p}\right\}\right).$$

Будем теперь суммировать выражение (7,4,2) по $x = 0, 1, \ldots, p-1$; $s = 1, 2, \ldots, p-1$. Ввиду (7,4,3) указанная сумма равна

$$\sum_{(s)}\sum_{(x)} R(y_s, s) - R(x, s). \tag{7,4,5}$$

Обозначим через $W_s(y)$ количество чисел $y_s < y$. Тогда

$$\sum_x R(y_s, s) = \sum_x R(x, s)(W_s(x+1) - W_s(x)). \tag{7,4,6}$$

В силу условия (7,3,5) имеем

$$W_s(y) = y + Bp^{1-\xi_0}. \tag{7,4,7}$$

Ввиду этого и (7,4,4) (7,4,6) получает выражение

$$\sum_x R(x, s) + B\left(\frac{p_1'}{q_1} + \frac{p_2'}{q_2} + \ldots + \frac{p_{k-1}'}{q_{k-1}} + p_k'\right)p^{1-\xi_0}, \tag{7,4,8}$$

так что (7,4,5) получает форму

$$Bp^{1-\xi_0}\sum_s\left(\frac{p_1'}{q_1} + \frac{p_2'}{q_2} + \ldots + \frac{p_{k-1}'}{q_{k-1}} + p_k'\right). \tag{7,4,9}$$

Обратимся к оценке последней суммы. Сперва оценим сумму первых членов

$$\sum_s \frac{p_1'}{q_1}. \tag{7,4,10}$$

Здесь имеем: $\frac{s}{p}=\frac{a_1}{q_1}+\frac{\theta}{q_1p_1}$. Количество чисел s, для которых q_1 будет лежать между $\frac{p_1}{2^k}$ и $\frac{p_1}{2^{k+1}}$ при $k=0, 1, 2, \ldots$; $\frac{p_1}{2^{k+1}}\geqslant\frac{1}{2}$, будет иметь оценку

$$Bp\frac{p_1}{2^kp_1}=B\frac{p}{2^k}.$$

В самом деле, из равенства $\left|\frac{s}{p}-\frac{a_1}{q_1}\right|\leqslant\frac{1}{q_1p_1}$ выводим $|q_1s-a_1p|<\frac{p}{p_1}$; при каждом заданном q_1 число соответствующих значений s будет $B\frac{p}{p_1}$; при указанных значениях q_1 соответствующее число значений s будет $B\frac{p}{p_1}\times$ $\times\frac{p_1}{2^k}=B\frac{p}{2^k}$.

Умножая на $\frac{p_1'}{q_1}=B\frac{p_1}{p_1}2^k=B2^k$ и суммируя по s, получим оценку Bp. Суммируя по различным k, находим общую оценку

$$Bp\lg p. \tag{7,4,11}$$

Таким же образом оцениваем $\sum\limits_s\frac{p_2'}{q_2}$, учитывая, что $\tau_2=p_2$; $p_2'\leqslant p_2$, затем $\sum\limits_s\frac{p_j'}{q_j}$ $(j\leqslant k-1)$. Для расчета $\sum\limits_s p_k'$ заметим, что количество чисел s, для которых $\frac{s}{p}=\frac{0}{1}+\frac{\theta}{\tau}$, где $\frac{1}{2}p_k\leqslant\tau\leqslant p_k$, будет, очевидно, $B\frac{p}{\tau}$, так что соответствующая сумма получит оценку

$$\sum_s p_k'=Bp\lg p. \tag{7,4,12}$$

Наконец, получаем оценку для любого значения s и $k=B\lg p$. Таким образом, подстановка (7,4,11) и (7,4,12) в (7,4,9) дает

$$Bp^{2-\varepsilon_0}\ln^2 p. \tag{7,4,13}$$

Возвращаясь к (7,4,2) и суммируя по (x) и $s=1, 2, \ldots, p-1$, находим

$$\sum_{s=1}^{p-1}\sum_{(x)} V_\gamma\left(\left\{\frac{y_s - st}{p}\right\}\right) = \sum_{s=1}^{p-1}\sum_{(x)} V_\gamma\left(\left\{\frac{x-st}{p}\right\}\right) + Bp^{2-\xi_0}\lg^2 p.$$

В последней сумме при данных s, t производим суммирование по x с очевидным результатом $[\gamma p]$; суммируя еще по s, t, находим

$$[\gamma p]\,p(p-1) + Bp^{2-\xi_0}\lg^2 p. \qquad (7,4,14)$$

Сравнивая (7,3,12), (7,3,14) и (7,4,14), находим

$$p\sum_{(t)} V_\gamma\left(\left\{\frac{f(t)}{p}\right\}\right) = \gamma p_1 p + Bp^{2-\xi_0}\lg^2 p, \qquad (7,4,15)$$

откуда

$$\sum_{(t)} V_\gamma\left(\left\{\frac{f(t)}{p}\right\}\right) = p_1 + Bp^{1-\xi_0}\lg^2 p, \qquad (7,4,16)$$

что и доказывает наше утверждение (7,3,7).

§ 5. Элементарный вывод И. М. Виноградова некоторых теорем о последовательности простых чисел

В 1953 г. И. М. Виноградов [5] указал элементарный путь к исследованию поведения дробных частей $\{\alpha p\}$, где α — заданное число, а p пробегает последовательность простых чисел. В данном и следующем параграфах мы воспроизведем работу [5]. Введем функцию

$$\Psi_\gamma(z) = V_\gamma(\{z\}) - \gamma, \qquad (7,5,1)$$

где $V_\gamma(u)$ — функция, введенная в § 3 $(0 \leqslant \gamma < 1)$.

Пусть $q > 1$ — целое число, $(a, q) = 1$, $0 < a \leqslant q-1$. Изучается поведение дробных частей системы чисел: $\frac{ap}{q}$, где $p \leqslant N$ $(N \to \infty)$ и $q < N$.

Теорема 7.5.1 (И. М. Виноградов).

$$\sum_{p \leqslant N} V_\gamma\left(\left\{\frac{ap}{q}\right\}\right) = \gamma\pi(N) + B_\varepsilon N^{1+\varepsilon}F, \qquad (7,5,2)$$

где $\pi(N)=\sum_{p\leqslant N}1$, $\varepsilon>0$ — *сколь угодно малая константа и*

$$F=\sqrt{\frac{1}{q}+\frac{q}{N}}+N^{-\frac{1}{6}}. \tag{7,5,3}$$

С аналитической точки зрения данная теорема уже содержит в себе основной этап решения тернарной проблемы Гольдбаха и вывода соответствующей асимптотики. Заметим, что формула (7,5,2) будет нетривиальной, если q растет вместе с N быстрее, чем N^{ε}. Доказательство теоремы 7,5,1 основывается на ряде элементарных лемм.

Пусть дано реальное число 2. Представим число α в форме

$$\alpha=\frac{A}{Q}+\frac{\theta}{Q\tau}\qquad((A, Q)=1,\quad 0<Q\leqslant\tau). \tag{7,5,4}$$

Лемма 1. *Пусть* β — *реальное число,* c — *целое число,* α — *число, заданное* (7,5,4). *Тогда*

$$\left|\sum_{x=c}^{c+Q-1}\Psi_{\gamma}(\alpha x+\beta)\right|<2. \tag{7,5,5}$$

Мы можем считать $Q>2$, ибо при $Q\leqslant 2$ лемма тривиальна. Имеем: $\alpha x+\beta=\frac{Ax+f(x)}{Q}$; $f(x)=\beta Q+\frac{\theta x}{\tau}$. Положим: $f(x)=n+\varkappa+\lambda(x)$, где n — целое число $(0\leqslant\varkappa<1,\ 0\leqslant\lambda(x)<1)$. Имеем

$$\{\alpha x+\beta\}=\left\{\frac{r+\varkappa+\rho(r)}{Q}\right\},$$

где r — наименьший неотрицательный вычет $Ax+n\pmod{}$, и $\rho(r)=\lambda(x)$. Неравенство

$$0\leqslant\{\alpha x+\beta\}<\gamma$$

может выполняться лишь при $r=Q-1;\ 0,\ 1,\ \ldots,\ [\gamma Q]$, где при целом γQ последнее значение исключается; это дает $<\gamma Q+2$ значений r. Оно наверно выполняется лишь при $r=0,\ 1,\ \ldots,\ [\gamma Q-2]$, т. е. при $>\gamma Q-2$ значениях r. Таким образом, число выполнений нашего неравенства имеет

вид $\gamma Q+\Phi$, где $|\Phi|<2$, так что сумма, входящая в левую часть (7,5,5), равна

$$(1-\gamma)(\gamma Q+\Phi)-\gamma(Q-\gamma Q-\Phi)=\Phi,$$

чем лемма доказана.

Лемма 2. *Пусть h — целое, x пробегает X_0 последовательных чисел ряда 1, 2, ..., q; y пробегает независимо от x Y_0 чисел того же ряда, взаимно простых с q. Тогда имеем*

$$\sum_x\sum_y \Psi_\gamma\left(\frac{xy+h}{q}\right)<4q(\ln q)^2. \qquad (7,5,6)$$

Легко подсчитать, что при $q\leqslant 70$ левая часть, не превосходящая $q(\varphi)(q)$, будет меньше правой. Поэтому будем считать $q>70$. При заданном y представим $\frac{y}{q}$ в форме

$$\frac{y}{q}=\frac{A_0}{Q_0}+\frac{\theta_0}{Q_0X_0},\quad (A_0,\ Q_0)=1;\quad 0<Q_0\leqslant X_0,\quad |\theta_0|\leqslant 1$$

и т. д., пока не придем к некоторому $X_{n+1}=0$. Применяя лемму 1, легко убедиться, что часть двойной суммы (7,5,6), отвечающая заданному y, по абсолютной величине не превосходит

$$2\left(\frac{X_0}{Q_0}+\frac{X_1}{Q_1}+\ldots+\frac{X_n}{Q_n}\right),$$

а вся двойная сумма имеет оценку абсолютной величины сверху

$$\sum_y\left(\frac{2X_0}{Q_0}+\frac{2X_1}{Q_1}+\ldots+\frac{2X_n}{Q_n}\right). \qquad (7,5,7)$$

Здесь числа n, Q_0, Q_1, ..., Q_n, X_0, X_1, ..., X_n зависят от y. Найдем оценку суммы (7,5,7). Выделим одно из слагаемых $\frac{2X}{Q}$. Ему отвечает система условий

$$\frac{y}{q}=\frac{A}{Q}+\frac{\theta}{QX}\qquad ((A,\ Q)=1;\quad 0<Q\leqslant X),$$

равносильная системе условий

$$yQ-Aq=t\quad\left((A,\ Q)=1;\quad 0<Q\leqslant X;\quad |t|<\frac{q}{X}\right). \qquad (7,5,8)$$

Последнее из условий (7,5,8) дает $X<\frac{q}{|t|}$, поэтому сла-

гаемое $\frac{2X}{Q}$ можно заменить слагаемым $\frac{2q}{Q|t|}$. Третье и четвертое из условий (7,5,8) заменим более грубыми

$$0<Q\leqslant q, \quad |t|\leqslant\frac{q}{Q}.$$

При $(Q, q)=\delta$ первое из условий (7,5,8) выполняется лишь при $|t|=t_1\delta$ (t_1 целое). При этом Q и $|t|$ определяют 2δ пар значений y и A, и сумма соответствующих слагаемых $\frac{2q}{Q|t|}$ будет $\leqslant 2\frac{q}{Qt_1\delta}2\delta=4\frac{q}{Qt_1}$.

Ввиду этого сумма (7,5,7) не превосходит

$$4q\sum_{0<Q\leqslant q}\frac{1}{Q}\sum_{0<t\leqslant\frac{q}{Q}}\frac{1}{t},$$

что при $q>70$, как дает простой численный подсчет, будет $<4q(\ln q)^2$. Это доказывает (7,5,6).

Лемма 3. *Пусть x пробегает X различных чисел ряда 1, 2, ..., q, а y независимо от него пробегает Y различных чисел этого же ряда, взаимно простых с q, $(a, q)=1$. Тогда для суммы*

$$S=\sum_x\sum_y\Psi_\gamma\left(\frac{axy}{q}\right)$$

имеем неравенство

$$|S|<2(XYq)^{1/2}\ln q. \tag{7,5,9}$$

Применим неравенство Коши — Буняковского к сумме S. Получим

$$|S|^2\leqslant X\sum_x\left|\sum_y\Psi_\gamma\left(\frac{axy}{q}\right)\right|^2.$$

Согласно основному принципу оценки двойных сумм по И. М. Виноградову, это неравенство лишь усилится, если в его правой части будем производить суммирование по всем значениям $x=\xi=1, 2, \ldots, q$. Пусть y_1 пробегает те же

значения, что y, независимо от y. На основании сказанного получим

$$|S|^2 \leqslant X \sum_{\xi=1}^{q} \sum_{y} \sum_{y_1} \Psi_\gamma\left(\frac{a\xi y}{q}\right) \Psi_\gamma\left(\frac{a\xi y_1}{q}\right) = X \sum_{y} S_y,$$

где

$$S_y = \sum_{y_1} \sum_{u=0}^{q-1} \Psi_\gamma\left(\frac{u}{q}\right) \Psi_\gamma\left(\frac{uy_1y'}{q}\right) = \sum_{u} \sum_{v} \Psi_\gamma\left(\frac{u}{q}\right) \Psi_\gamma\left(\frac{uv}{q}\right),$$

где $y'y \equiv 1 \pmod q$, v — наименьший неотрицательный вычет $y_1y' \pmod q$. Когда y_1 пробегает свои Y значений, v пробегает Y различных чисел ряда $1, 2, \ldots, q$, взаимно простых с q. Разобьем сумму S_y на две суммы, из которых первая содержит слагаемые с $u < \gamma q$, а вторая — слагаемые с $u \geqslant \gamma q$. В каждой из наших сумм множитель $\Psi_\gamma\left(\frac{u}{q}\right)$ будет постоянным коэффициентом при слагаемом $\Psi_\gamma\left(\frac{uv}{q}\right)$. К последним слагаемым каждой суммы в отдельности применим лемму 2; получим

$$|S_y| < 4q(\ln q)^2(1-\gamma) + 4q(\ln q)^2\gamma = 4q(\ln q)^2,$$
$$|S|^2 < 4XYq(\ln q)^2; \quad |S| < 2(XYq)^{1/2}\ln q.$$

Лемма 4. *Пусть x пробегает ряд различных чисел, содержащихся среди X последовательных целых чисел, а y пробегает независимо от x ряд различных чисел, содержащихся среди Y последовательных целых чисел взаимно простых с q. Положим*

$$S = \sum_{x} \sum_{y} \Psi_\gamma\left(\frac{axy}{q}\right).$$

Тогда имеем

$$|S| = BXYF_0; \quad F_0 = \left(\frac{1}{X} + \frac{1}{Y} + \frac{1}{q} + \frac{q}{XY}\right)^{\frac{1}{2}} \ln q. \tag{7,5,10}$$

Если $X > q$, разобьем отрезки изменения x на $B\frac{X}{q}$ отрезков, и так же поступим с отрезком изменения y. После

этого придем к суммам, рассмотренным в лемме 3. Таким образом, получим оценки:

при $X \leqslant q$, $Y \leqslant q$

$$|S| = B(XYq)^{\frac{1}{2}} \ln q = XY\left(\frac{q}{XY}\right)^{\frac{1}{2}} \ln q = BXYF_0;$$

при $X \leqslant q$, $Y > q$ или при $X > q$, $Y \leqslant q$

$$|S| = B\frac{Y}{q}(Xqq)^{\frac{1}{2}} \ln q + B\frac{X}{q}(Xqq)^{\frac{1}{2}} \ln q = BXYF_0;$$

при $X > q$, $Y > q$

$$|S| = B\frac{X}{q}\frac{Y}{q}q^{\frac{3}{2}} \ln q = BXYF_0.$$

Лемма 5. *Пусть* $1 \leqslant U < N$, $1 \leqslant \Delta \leqslant U$, $U + \Delta \leqslant N$,

$$S = \sum_x \sum_y \Psi_\tau\left(\frac{axy}{q}\right),$$

где x, y *пробегают целые числа, принадлежащие к двум возрастающим последовательностям, причем* $(y, q) = 1$;

$$U < x \leqslant U + \Delta; \quad \frac{N}{U+\Delta} < y \leqslant \frac{N}{x}, \qquad (7,5,11)$$

а в остальном x, y *независимы. Тогда имеем*

$$|S| = B\frac{N\Delta^2}{u^2}F_1,$$

$$F_1 = \left(\frac{1}{\Delta} + \frac{U^2}{N\Delta} + \frac{1}{q} + \frac{qY^2}{N\Delta^2}\right)^{\frac{1}{2}} (\ln q)^2.$$

Будем считать, что $F_1 \leqslant \xi_0$, где, как и ранее, $\xi_0 > 0$ — достаточно малая константа (в противном случае лемма тривиальна).

Пусть r_0 — наибольшее целое число под условием $2^{r_0} \leqslant F_1^{-1}$. Из области (7,5,11) (см. рис. 2) выделим «первые», «вторые», «третьи»; ..., «r-е» области, согласно схеме, указанной на чертеже. Здесь r-я область оказывается прямоугольником с основанием длины $\frac{\Delta}{2^r}$ и высотой длины, имеющей

точный порядок $\frac{N\Delta}{U^2 2^r}$ (левая и нижняя стороны прямоугольника к области не причисляются). Число r-х областей равно 2^{r-1}. Согласно лемме 4, часть суммы S, отвечающая одной из r-х областей, будем иметь оценку

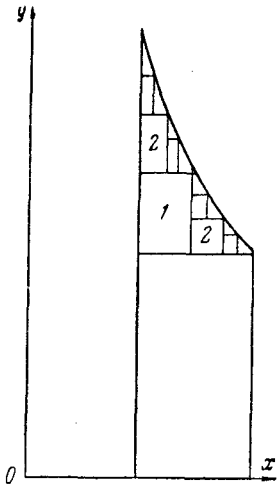

Рис. 2.

$$B\frac{\Delta}{2^r}\frac{N\Delta}{U^2 2^r}\left(\frac{2^r}{\Delta}+\frac{U^2 2^r}{N\Delta}+\frac{1}{q}+\right.$$
$$\left.+\frac{qU^2 2^{2r}}{N\Delta^2}\right)^{\frac{1}{2}}\ln q=$$
$$=B\frac{N\Delta^2}{U^2 2^r}F_1(\ln q)^{-1}.$$

Часть суммы S, отвечающая выделенным областям, будет иметь оценку

$$B\frac{N\Delta}{U^2}\frac{\Delta}{2^{r_0}}=B\frac{N\Delta^2}{U^2}F_1.$$

Поэтому

$$|S|=B\frac{N\Delta^2}{U^2}\left(\sum_{r=1}^{r_0}\frac{2^{r-1}}{2^r\ln q}+1\right)F_1=$$
$$=B\frac{N\Delta^2}{U^2}F_1,$$

чем лемма доказана.

Лемма 6. *Пусть* $1\leqslant U\leqslant N$, $0<\Delta\leqslant U$, $U+\Delta\leqslant N$,

$$S_0=\sum_x\sum_y\Psi_1\left(\frac{axy}{q}\right),$$
$$U<x\leqslant U+\Delta,\quad 0<y\leqslant\frac{N}{x},$$

а в остальном x, y *независимы, пробегают целые числа из двух возрастающих последовательностей;* $(y, q)=1$ *и значения* y *повторяются каждое не более* M *раз. Тогда имеем*

$$|S|=BNMF_2,\quad F_2=\left(\frac{1}{U}+\frac{U}{N}+\frac{1}{q}+\frac{q}{N}\right)^{\frac{1}{2}}(\ln q)^2.$$

Заметим, что достаточно рассматривать случай $M=1$ и $\Delta\geqslant 1$. Часть S суммы S_0, рассмотренная в предыдущей лемме,

будет иметь оценку BNF_2. Оставшаяся часть суммы S_0, где суммирование идет в области

$$U<x\leqslant U+\Delta,\ 0<y\leqslant\frac{N}{U+\Delta},$$

по лемме 4 будет иметь оценку

$$B\Delta\frac{N}{U}\left(\frac{1}{\Delta}+\frac{U}{N}+\frac{1}{q}+\frac{qU}{\Delta N}\right)^{\frac{1}{2}}\ln q=BNF_2.$$

Лемма 7. *Пусть x, y, m пробегают взаимно простые с q положительные числа, принадлежащие трем возрастающим последовательностям. Пусть при этом*

$$U<x\leqslant U',\quad xym\leqslant N,\quad (x,\ y)=1,$$

где

$$1<U<N,\quad U<U'\leqslant 2U,$$

а в остальном x, y, m независимы. Положим

$$S=\sum_x\sum_y\sum_m\Psi_1\left(\frac{axym}{q}\right).$$

Тогда имеем

$$|S|=B_3N^{1+\varepsilon}F_3,\quad F_3=\left(\frac{1}{U}+\frac{U}{N}+\frac{1}{q}+\frac{q}{N}\right)^{\frac{1}{2}}.$$

Снова будем считать, что $F_3\leqslant\xi_0$ (ξ_0 — достаточно малая константа), иначе лемма тривиальна. Далее имеем

$$\sum_{d/x;\ d/y}\mu(d)=\begin{cases}0, & \text{если } (x,\ y)>1,\\ 1, & \text{если } (x,\ y)=1.\end{cases}$$

Ввиду этого

$$S=\sum_d\mu(d)S_d,$$

где

$$S_d=\sum_{x'}\sum_{y'}\sum_m\Psi_1\left(\frac{ad^2x'y'm}{q}\right),$$

где x', y' пробегает числа $\frac{x}{d}$, $\frac{y}{d}$, если $(x,\ y)=d$; суммирование идет по области

$$\frac{U}{d}<x'\leqslant\frac{U'}{d};\quad x'y'm\leqslant\frac{N}{d^2}.$$

При $N_1 \leqslant N$ число пар y', m под условием $y'm = N_1$ равно $B_{\varepsilon'} N^{1+\varepsilon'}$. Поэтому при $d \leqslant F_3^{-1}$ по лемме 7 найдем

$$|S_d| = B_{\varepsilon'} \frac{N^{1+\varepsilon'}}{d^2} \left(\frac{d}{U} + \frac{Ud^2}{dN} + \frac{1}{q} + \frac{qd^2}{N} \right)^{\frac{1}{2}} (\ln q)^2 =$$
$$= B_{\varepsilon'} \frac{N^{1+\varepsilon'}}{d} F_3 (\ln q)^2,$$

а при $d > F_3^{-1}$ имеем

$$|S_d| = B_{\varepsilon'} \frac{N^{1+\varepsilon'}}{d^2} = B_{\varepsilon'} \frac{N^{1+\varepsilon'}}{d} F_3,$$

откуда легко следует лемма 7.

Лемма 8 является довольно сложно формулируемой, но элементарной леммой из известной монографии И. М. Виноградова (см. [1]).

Лемма 8. *Пусть* $0 < c \leqslant \frac{1}{6}$, $0 < \sigma \leqslant \frac{1}{3}$, $0 \leqslant p \leqslant 1 - \sigma$, P *— произведение простых чисел, не превосходящих* N^{σ}; $N > N_0$. *Положим* $r = \ln N$,

$$D = r^{\frac{\ln r}{\ln (1+c)}}$$

и рассмотрим делители d *числа* P.

Их можно распределить по $D' < D$ *системам, причем для каждой системы существует свое* φ *под условием, что значение из этой системы удовлетворяет условиям*

$$\varphi < d \leqslant \varphi^{1+c}.$$

Для некоторых систем будет $\varphi \leqslant N^p$, *а для каждой из остальных существует целое число* $\Gamma > 0$ *и две возрастающие последовательности натуральных чисел* x, y *таких, что* $x \in (\varphi_0, \varphi_0^{1+c}] \subset (N^p, N^{p+\sigma+c}]$. *При этом все числа* d *рассматриваемой системы, взятые каждое* Γ *раз, и только их получим, если из всех произведений* xy *выберем лишь такие, для которых* $(x, y) = 1$.

Для доказательства рассмотрим τ — наибольшее целое число для каждого

$$2^{(1+c)^{\tau-1}} \leqslant N^{\sigma}.$$

В силу условий на c, σ имеем

$$(1+c)^{\tau-1} \leqslant \frac{\ln N}{3\ln 2}, \quad \tau - 1 \leqslant \frac{\ln\ln N - \ln\ln 8}{\ln(1+c)},$$

$$\tau < \frac{\ln r}{\ln(1+c)} - 1.$$

Положим $b = [\ln N]$ и рассмотрим все невозрастающие системы b чисел:

$$t_1 \geqslant t_2 \geqslant \ldots \geqslant t_b, \tag{7,5,12}$$

где t_j может принимать значение τ, $\tau - 1$, ..., 1, 0. Пусть l_s — число чисел ряда (7,5,12), равных s. Числами l_τ, $l_{\tau-1}$, ..., l_1 ряд (7,5,12) определяется полностью. Отсюда следует, что число таких рядов меньше D.

При $t_j > 0$ полагаем

$$\varphi_j = 2^{(1+c)^{t_j}-1}, \qquad F_j = \varphi_j^{1+c} = 2^{(1+c)^{t_j}}.$$

При $t_j = 0$ полагаем

$$\varphi_j = F_j = 1.$$

Всякое $d \leqslant N$ является произведением $\leqslant b$ простых делителей. Будь это не так, получили бы

$$2 \cdot 3 \ldots (b+2) \leqslant N; \qquad \ln 2 + \ldots + \ln(b+2) \leqslant \ln N$$

или

$$\ln N \ln\ln N \leqslant 2\ln N - 1,$$

что невозможно при $N > N_0$. Расположим простые делители d в порядке убывания. Если число их $h < b$, положим: $p_{h+1} = \ldots = p_b = 1$. Тогда получим: $d = p_1 \ldots p_b$. Среди рядов $t_1, \ldots, t_b$ найдется единственный ряд под условием

$$\left.\begin{aligned} \varphi_j < p_j \leqslant F_j \quad &\text{при} \quad t_j > 0, \\ \varphi_j = p_j = F_j \quad &\text{при} \quad t_j = 0. \end{aligned}\right\} \tag{7,5,13}$$

Будем говорить, что рассматриваемое d связано с этим рядом $t_1, \ldots, t_b$. Полагая $\varphi = \varphi_1 \ldots \varphi_b$, получим: $\varphi < d \leqslant \varphi^{1+c}$. Пусть $\varphi > N^\rho$. Рассмотрим совокупность всех d, связанных с данным рядом $t_1, \ldots, t_b$. Пусть β — наименьшее целое число, для которого $\varphi_1 \ldots \varphi_\beta > N^\rho$ (при $\beta = 1$ полагаем $\varphi_1 \ldots \varphi_{\beta-1} = 1$).

Имеем

$$\varphi_1 \dots \varphi_{\beta-1} \leqslant N^{\rho}; \quad \varphi_\beta \leqslant N^{\sigma}; \quad \varphi_1 \dots \varphi_\beta \leqslant N^{\rho+\sigma};$$

$$(\varphi_1 \dots \varphi_\beta)^{1+c} \leqslant N^{\rho+\sigma+c}.$$

Положим $x = p_1 \dots p_\beta$; $y = p_{\beta+1} \dots p_b$; $\varphi_0 = \varphi_1 \dots \varphi_\beta$. Легко убедиться, что $x \in (\varphi_0, \varphi_0^{1+c}] \subset (N^{\rho}, N^{\rho+\sigma+c}]$. Пусть, далее, $t_{\beta-k_1+1}, \dots, t_\beta, t_{\beta+1}, \dots, t_{\beta+k_2}$ — все значения t_l равны t_β. Пусть x, y независимо пробегают все произведения с условиями (7,5,13) и условиями

$$p_1 > \dots > p_\beta; \quad p_{\beta+1} \geqslant \dots \geqslant p_b,$$

где неравенство $p_s \geqslant p_{s+1}$ надо понимать как неравенство $p_1 > p_{s+1}$, если $p_s > 1$, и как равенство $p_s = p_{s+1}$, если $p_s = 1$. В таком случае xy совпадает с одним из чисел d нашей системы, только если $(x, y) = 1$ и число повторений равенства $xy = d$ будет $C_{k_1+k_2}^{k_1}$. Принимая последнее число за Γ, приходим к доказательству леммы 7. Нам нужен будет лишь частный случай этой леммы, который мы сформулируем как следствие.

Следствие. Пусть ν — константа под условием $0 < \nu \leqslant 0{,}1$; P — произведение простых чисел, не превосходящих $N^{1/8}$; d пробегает делители P, не превосходящие N;

$$D = (\ln N)^{\frac{\ln \ln N}{\ln (1+\nu)}}.$$

Тогда все значения d могут быть распределены среди $D' < D$ членов. Часть этих классов включает только значения d под условием

$$d \leqslant N^{\frac{1}{3}+\nu}.$$

Для каждого из остальных классов существует целое $H > 0$ и две возрастающие последовательности (x) и (y) натуральных чисел под условием

$$N^{\frac{1}{3}} < x \leqslant N^{\frac{2}{3}+\nu},$$

такие, что все числа класса, взятые каждое H раз, и только эти числа получим, выбирая среди всех произведений xy лишь удовлетворяющие условиям

$$xy \leqslant N, \quad (x, y) = 1.$$

§ 6. Доказательство теоремы

Пусть $\nu < 0{,}1$ — сколь угодно малая константа. P — произведение всех $p \nmid Q$, $p \leqslant N^{\frac{1}{3}}$;

$$Q = \prod_{\substack{N^{\frac{1}{3}} < p \leqslant N \\ p \nmid q}} p,$$

$$S = \sum_{p \leqslant N} \Psi_\tau\left(\frac{ap}{q}\right). \tag{7,6,1}$$

Имеем из элементарных соображений

$$\sum_{d \mid p} \sum_{\substack{(m,\, q)=1 \\ 0<dm \leqslant N}} \mu(d)\, \Psi_\tau\left(\frac{adm}{q}\right) =$$

$$= S + \frac{1}{2} \sum_{\substack{p_1 \nmid Q \\ p_2 \nmid Q \\ p_1 p_2 \leqslant N}} \Psi_\tau\left(\frac{a p_1 p_2}{q}\right) + BN^{\frac{2}{3}}. \tag{7,6,2}$$

Здесь p_1, p_2 пробегают простые числа и связаны лишь условием $p_1,\ p_2 \leqslant N$.

В двойной сумме в правой части (7,6,2) все значения $x = p_1$ лежат в интервале $(N^{\frac{1}{3}},\ N^{\frac{2}{3}})$. Его можно разбить на $B \ln N$ отрезков, указанных в лемме 6. Ввиду этого, применяя лемму 6, найдем для этой двойной суммы оценку

$$B_\varepsilon N^{1+\varepsilon}\left(N^{-\frac{1}{3}} + \frac{N^{\frac{2}{3}}}{N} + \frac{1}{q} + \frac{q}{n}\right)^{\frac{1}{2}} = B_\varepsilon N^{1+\varepsilon} F_1.$$

Обратимся к левой части (7,6,2). Здесь все значения d разобьем на классы, как указано в следствии леммы 8. Получим $B_{\varepsilon'} N^{\varepsilon'}$ классов; для чисел одного и того же класса $\mu(d)$ постоянно.

Рассмотрим сперва класс, для которого, согласно следствию из леммы 8, можно указать $H > 0$ и две возрастающие последовательности (x), (y) натуральных чисел с условием

$$N^{\frac{1}{3}} < x \leqslant N^{\frac{2}{3}+\nu},$$

таких, что все числа класса, повторенные каждое H раз, и только эти числа получим, если из всех произведений xy выберем лишь удовлетворяющие условиям

$$xy \leqslant N; \quad (x, y) = 1.$$

Для выбранного класса соответствующая часть суммы в левой части (7,6,2) после умножения на $\mu(d) = \pm 1$ (постоянные в классе) и число H примет вид

$$\sum_x \sum_y \sum_m \Psi_\tau\left(\frac{axym}{q}\right), \tag{7,6,3}$$

где суммирование идет по области

$$N^{\frac{1}{3}} < x \leqslant N^{\frac{2}{3}+\nu}; \quad xym \leqslant N; \quad (x, y) = 1.$$

К сумме (7,6,3) применим лемму 7. Разбиваем отрезок изменения x на $B \ln N$ сегментов вида, указанного в лемме 7. После этого для (7,6,3) находим оценку

$$B_\varepsilon N^{1+\varepsilon}\left(N^{-\frac{1}{3}} + \frac{N^{\frac{2}{3}+\nu}}{N} + \frac{1}{q} + \frac{q}{N}\right)^{\frac{1}{2}} = B_{\varepsilon''} N^{1+\varepsilon''} F_4,$$

где $F_4 = F$ (см. (7,5,3)).

Далее рассмотрим указанные в следствии к лемме 8 классы, содержащие лишь значение d с условиями $d \leqslant N^{\frac{1}{3}+\nu}$. Мы рассмотрим лишь классы с $\mu(d) = +1$; случай $\mu(d) = -1$ трактуется аналогично. Часть суммы в левой части (7,6,2), *отвечающая всем таким классам, может быть записана в виде* $S' + S'' + S'''$, где

$$S' = \sum_{d > \frac{N}{q}} \sum_{m \leqslant \frac{N}{d}} \Psi_\tau\left(\frac{adm}{q}\right).$$

$$S'' = \sum_{d \leqslant \frac{N}{q}} \sum_{m \leqslant \left[\frac{N}{qd}\right] q} \Psi_\tau\left(\frac{adm}{q}\right),$$

$$S''' = \sum_{d \leqslant \frac{N}{q}} \sum_{\left[\frac{N}{dq}\right] q < m \leqslant \frac{N}{d}} \Psi_\tau\left(\frac{adm}{q}\right).$$

Сумма S' непустая, только если $\frac{N}{q} < N^{\frac{1}{3}+\nu}$.

В таком случае разобьём отрезок $\left[\frac{N}{q}, N^{\frac{1}{3}+\nu}\right]$ значений $x=d$ на $B\ln N$ отрезков вида, указанного в лемме 6. Применяя затем лемму 6 к S', получим оценку

$$B_\varepsilon N^{1+\varepsilon}\left(\frac{1}{Nq^{-1}}+\frac{N^{\frac{1}{3}+\nu}}{N}+\frac{1}{q}+\frac{q}{N}\right)^{\frac{1}{2}}=B_\varepsilon N^{1+\varepsilon}F_4.$$

Часть суммы S'', отвечающую заданному d, можно представить в виде

$$\left[\frac{N}{dq}\right]\sum_{\substack{0\leqslant p<q\\(p,\ q)=1}}\Psi_\gamma\left(\frac{p}{q}\right)=\sum_{\delta\mid q}\mu(\delta)\sum_{u=0}^{\frac{q}{\delta}-1}\Psi_\gamma\left(\frac{u}{q\delta^{-1}}\right).$$

Как известно (см. [3]), это выражение имеет оценку

$$B\tau(q)=B_{\varepsilon'}N^{\varepsilon'},$$

так что

$$|S''|=B\sum_{d<\frac{N}{q}}\frac{N^{1+\varepsilon'}}{dq}=B_\varepsilon\frac{N^{1+\varepsilon}}{q}.$$

Значения d, входящие в S''', распределяются по отрезкам

$$\left[1, \frac{N}{s_0q}\right]; \left(\frac{N}{s_0q}, \frac{N}{(s_0-1)q}\right]; \ldots; \left(\frac{N}{2q}, \frac{N}{q}\right],$$

где $s_0=\left[\sqrt{\frac{N}{q}}\right]$. Для части суммы S''', отвечающей первому отрезку, найдем оценку

$$B\frac{N}{s_0q}q=BN\sqrt{\frac{q}{N}}.$$

Рассмотрим часть $S(s)$ суммы S''', отвечающую общему виду отрезка $\left(\frac{N}{sq}, \frac{N}{(s-1)q}\right]=I_s$. Она равна

$$\sum_{d\in I_s}\sum_{(s-1)q<m\leqslant\frac{N}{d}}\Psi_\gamma\left(\frac{adm}{q}\right).$$

Применим лемму 5, беря в ней $\frac{N}{qs(s-1)}$ вместо Δ и $\frac{N}{sq}$

вместо U. Получим для $S(s)$ оценку

$$B\frac{N}{s^2}\left(\frac{qs^2}{N}+\frac{1}{q}+\frac{qs^2}{N}\right)^{\frac{1}{2}}(\ln q)^2 = B\frac{N}{s}\left(\frac{1}{q}+\frac{q}{N}\right)^{\frac{1}{2}}(\ln q)^2.$$

Таким образом,

$$\sum_{s=2}^{s_0} S(s) = B_\varepsilon N^{1+\varepsilon}\left(\frac{1}{q}+\frac{q}{N}\right)^{\frac{1}{2}}.$$

Внося это в (7, 6,2), получаем оценку

$$\sum_{p\leqslant N}\Psi_1\left(\frac{ap}{q}\right) = B_\varepsilon N^{1+\varepsilon}F, \tag{7,6,4}$$

откуда непосредственно следует теорема 7,5,1.

ГЛАВА 8

СЧЕТ ЦЕЛЫХ ТОЧЕК В КОНТУРАХ

§ 1. Постановка задачи. Характерные проблемы *

Пусть дана гладкая *) замкнутая плоская кривая C (см. рис. 3), отнесенная к системе декартовых координат xOy, и выражаемая уравнениями $y = \varphi_1(x)$ (нижняя часть) и $y = \varphi_2(x)$ (верхняя часть). Мы будем считать, что гладкость кривой такова, что существуют первые и вторые производные $\varphi_i(x)$, $\varphi_i'(x)$ внутри сегмента $[P, Q]$ (в точках P и Q это может нарушаться).

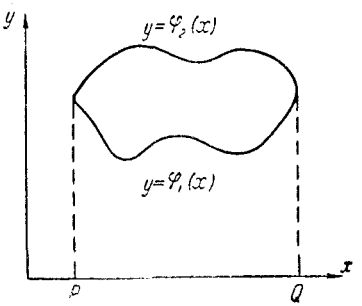

Рис. 3.

Площадь, охватываемая контуром кривой, выражается в виде

$$S = \int_P^Q (\varphi_2(x) - \varphi_1(x))\,dx. \qquad (8,1,1)$$

В той же системе координат рассматриваем решетку целых точек, т. е. совокупность точек (x, y) с целыми координатами, и отмечаем точки, лежащие внутри и на контуре кривой. Это число, очевидно, выражается в виде

$$\sum_{P \leqslant x \leqslant Q} [\varphi_2(x)] - \sum_{P \leqslant x \leqslant Q} [\varphi_1(x)], \qquad (8,1,2)$$

---

*) Настоящая глава систематически использует понятие гладкой кривой, и потому в ней применяются элементы анализа в объеме, указанном в предисловии.

где целые точки контура, имеющие абсциссы P или Q, если они существуют, не засчитываются (можно добавить их к (8,1,2), если потребуется). Сравнение (8,1,2) и (8,1,1) будет естественным, если площадь S достаточно велика и контур не слишком «извилист». Мы будем производить такое сравнение для случаев, когда $Q-P$ велико, а кривизна контура достаточным образом мала (радиус кривизны достаточно велик). Если L — периметр нашей кривой (длина ее контура), то число целых точек внутри и на контуре кривой отличается от площади кривой S не более чем на количество перерезанных ее контуром горизонтальных полосок, ограниченных горизонталями $y=y_1$, $y=y_1+1$ или вертикальных полосок, ограниченных вертикалями $x=x_1$, $x=x_1+1$. Число таких полосок имеет оценку BL. Если N — число целых точек внутри и на контуре, то имеем, таким образом,

$$N=S+BL. \tag{8,1,3}$$

Поведение остаточного члена $N-S=R$ зависит от кривой C. Исторически первыми кривыми, исследованными в этом отношении, были окружность и гипербола вместе с асимптотами.

Для окружности $x^2+y^2=R^2$ периметр $L=2\pi R$ и охватываемая площадь $S=\pi R^2$, так что имеем

$$N=\pi R^2+\rho(R);\qquad \rho(R)=BR. \tag{8,1,4}$$

Для гиперболы $xy=n$ (n — целое число) вместе с координатными осями $x=0$ и $y=0$, являющимися ее асимптотами, вопрос о счете целых точек внутри получающегося контура был поставлен еще Дирихле в связи с проблемой делителя. Пусть $\tau(m)=\sum\limits_{\delta\mid m}1$ — число делителей числа m; пусть $T(n)=\dfrac{\tau(1)+\tau(2)+\ldots+\tau(n)}{n}$ — среднее число делителей для чисел $m\leqslant n$. Можем написать

$$nT(n)=\sum_{m\leqslant n}\tau(m)=\sum_{xy\leqslant n}1=\sum_{x\leqslant n}\sum_{y\leqslant\frac{n}{x}}1=\sum_{x=1}^{n}\left[\frac{n}{x}\right]. \tag{8,1,5}$$

Количество (8,1,5) есть, очевидно, число целых точек в области $xy \leqslant n$ ($x > 0$, $y > 0$). При этом, очевидно, должно быть: $x \geqslant 1$, $y \geqslant 1$, откуда $x \leqslant n$, $y \leqslant n$. Получаем область, изображенную на рис. 4. Длина контура L здесь будет Bn, так что по формуле (8,1,3) получим

$$N = S + Bn. \qquad (8,1,6)$$

Далее, так как функция $y = \frac{n}{x}$ — убывающая функция, то

$$S = n \sum_{m \leqslant n} \frac{1}{m} + Bn, \qquad (8,1,7)$$

как легко видеть из чертежа. Возвращаясь к (8,1,5), получаем

$$T(n) = \sum_{m \leqslant n} \frac{1}{m} + B. \qquad (8,1,8)$$

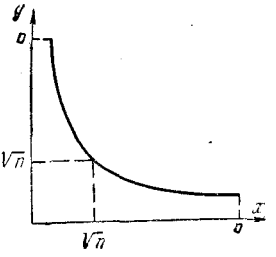

Рис. 4.

Эту же формулу мы могли бы получить непосредственно из (8,1,5), заметив что $\left[\frac{n}{x}\right] = \frac{n}{x} + \left\{\frac{n}{x}\right\}$; так как $0 \leqslant \left\{\frac{n}{x}\right\} < 1$, то из (8,1,5) следует (8,1,8). Однако геометрический подход к счету целых точек в контуре позволяет почти непосредственно улучшить оценку остаточного члена $N - S$. Именно в силу симметрии контура относительно биссектрисы $y = x$ мы непосредственно выводим из чертежа

$$N = 2N_1 - [\sqrt{n}]^2,$$

где N_1 — число целых точек в левом контуре, отсекаемом от данного вертикалью $x = \sqrt{n}$. Отсюда

$$N = nT(n) = 2 \sum_{x \leqslant \sqrt{n}} \left[\frac{n}{x}\right] - [\sqrt{n}]^2 =$$

$$= 2 \sum_{x=1}^{\sqrt{n}} \frac{n}{x} - n + B\sqrt{n} = S + B\sqrt{n},$$

по тем же соображениям, по которым мы вывели (8,1,7).

Таким образом, полагая $V = 2 \sum_{x=1}^{\sqrt{n}} \frac{n}{x} - n$, имеем

$$N = V + \rho(n); \quad \rho(n) = B\sqrt{n}. \qquad (8,1,9)$$

С начала нынешнего века, исследования многих математиков, начиная с Г. Ф. Вороного [6] и И. Серпинского [49], были направлены на отыскание «точных оценок» погрешностей $\rho(R)$ в формуле (8,1,4) и $\rho(n)$ в формуле (8,1,9). Под этим понимаем следующее.

Пусть в формуле (8,1,4) $R \to \infty$. Имеем: $\rho(R) = O(R)$. Могут существовать и (как мы увидим) в действительности существуют такие положительные α, что $\alpha < 1$, и $\rho(R) = O(R^{\alpha})$. Нижнюю грань таких чисел назовем α_0. Тогда для любого $\varepsilon > 0$ имеем

$$\rho(R) = B_{\varepsilon} R^{\alpha_0 + \varepsilon} \quad \text{(для всех } R\text{)}.$$

В то же время соотношение

$$\rho(R) = B_{\varepsilon} R^{\alpha_0 - \varepsilon} \quad \text{(для всех } R\text{)}$$

неверно ни для какого $\varepsilon > 0$.

Число α_0 и называется точным порядком погрешности в формуле (8,1,4). Аналогично вводится точный порядок погрешности в формуле (8,1,9). Отыскание таких точных порядков называется соответственно проблемой круга и проблемой делителей.

В 1914 г. Г. Гарди [39] доказал, что для проблемы круга, $\alpha_0 \geqslant \frac{1}{2}$. В работах В. Ярника [40] доказано, что $\alpha_0 < \frac{2}{3}$, однако проблема круга и проблема делителей остаются нерешенными и по сие время.

В 1917 г. И. М. Виноградов [1] предложил элементарный метод для счета целых точек в контурах общего вида, который будет здесь изложен. Для проблемы круга он дает: $\alpha_0 \leqslant \frac{2}{3}$, для проблемы делителей: $\alpha_0 \leqslant \frac{1}{3}$.

§ 2. Формулировка теоремы И. М. Виноградова *

Мы будем рассматривать число целых точек внутри и на контуре трапеции с криволинейным верхом $y = f(x)$, где $y' \geqslant 0$ — неубывающая функция, так что $y'' > 0$; пусть от P до Q имеют место неравенства $\alpha \leqslant y' < \beta$ (рис. 5). Если мы будем подобным образом увеличивать кривую, то длина PQ и все ординаты увеличатся в одинаковое число n раз; y'

не изменится, а y'' уменьшится в n раз и заменится на $\frac{y''}{n}$. Ввиду этого при увеличении контура в n раз подобным образом, $\frac{\alpha}{n} < y'' < \frac{\beta}{n}$. Но кроме подобного изменения может, очевидно, существовать и более общее изменение кривой, раздувание контура в бесконечности, такое, что при увеличении PQ в n раз будет $\frac{\alpha}{n} < y'' < \frac{\beta}{n}$. Оказывается, что для оценки остаточного члена в формуле для числа целых точек наиболее существенно как раз это условие $\frac{\alpha}{n} < y'' < \frac{\beta}{n}$, так что если оно соблюдается, то можно раздувать кривую, деформируя ее с соблюдением этого условия, и оценка остаточного члена останется достаточно точной.

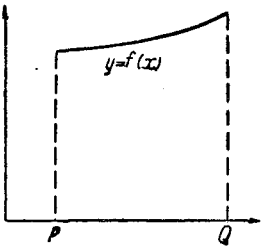

Рис. 5.

Нам нужно искать $\sum_x [f(x)] = \sum_x f(x) - \sum_x \{f(x)\}$. Главный вопрос — отыскание $\sum_x \{f(x)\}$, а это арифметический вопрос.

Пусть вид $f(x)$ и два числа Q и R определяются величиной параметра $A \to \infty$; пусть, кроме $A \to \infty$, $R - Q \to \infty$. Исследуется асимптотическое выражение для суммы

$$S = \sum_{x>Q}^{x \leqslant R} \{f(x)\} \quad \text{при} \quad A \to \infty.$$

Мы наложим ограничение на $f(x)$, считая, что существует $f'(x)$ монотонно возрастающая, и $f''(x) > 0$, причем для всех $A > A_0$, $\frac{1}{kA} \leqslant f''(x) \leqslant \frac{1}{A}$; k фиксировано; $k \geqslant 1$; x изменяется от Q до R; $Q \leqslant x \leqslant R$.

Пусть при возрастании A, $R - Q$ растет так, что

$$\lim_{A \to \infty} \frac{(A \lg A)^{\frac{2}{3}}}{R - Q} = 0. \qquad (8,2,1)$$

Теорема 8.2.1 (И. М. Виноградов). *Пусть* k, A, Q, R — *числа под условиями:* $k \geqslant 1$, $A > 25$, $Q < R$; *и для* $Q \leqslant x \leqslant R$, $f(x)$ *имеет вторую производную* $f''(x)$, *причем* $\frac{1}{kA} \leqslant f''(x) \leqslant \frac{1}{A}$. *Тогда имеет место формула*

$$\sum_{x>Q}^{x\leqslant R} \{f(x)\} = \frac{R-Q}{2} + G, \tag{8,2,2}$$

где

$$|G| \leqslant 2k\left(\frac{R-Q}{A}+1\right)(A \lg A)^{\frac{2}{3}}. \tag{8,2,3}$$

Доказательство этой теоремы начнем с нескольких лемм.

Лемма 1. *Если* a — *реальное число, то при всяком* $\tau > 1$ *можно удовлетворить неравенства*

$$-\frac{1}{\tau} < aX - Y < \frac{1}{\tau}, \quad 0 < X < \tau,$$

т. е.

$$\left|a - \frac{Y}{X}\right| < \frac{1}{X\tau}, \quad X < \tau,$$

целыми взаимно простыми числами X *и* Y.

Это известная теорема теории непрерывных дробей (см. [29]).

Лемма 2. *Пусть имеем* n *целых положительных чисел*

$$X_1, X_2, \ldots, X_n; \quad 0 < X_i \leqslant N (i = 1, 2, \ldots, n). \tag{8,2,4}$$

Тогда, не нарушая последовательности их расположения, за исключением менее чем N *из них, можно все остальные разбить на группы, удовлетворяющие такому условию: число членов* m *каждой такой группы*

$$X_{a+1}, \quad X_{a+2}, \ldots, X_{a+m}$$

равно наибольшему из участвующих здесь чисел, так что

$$X_{a+i} \leqslant m \qquad (i = 1, 2, \ldots, m).$$

Лемма тривиальна при $n < N$.

Пусть $n \geqslant N$. Рассмотрим группу из X_1 первых членов (8,2,4): $X_1, X_2, \ldots, X_{X_1}$. Пусть $X^{(2)}$ — наибольшее из встречающихся здесь чисел. Тогда либо $X^{(2)} = X_1$, либо $X^{(2)} > X_1$. Если $X^{(2)} = X_1$, то группа выделена. Если же $X^{(2)} > X_1$, то возьмем группу из $X^{(2)}$ первых членов (8,2,4): $X_1, X_2, \ldots, X_{X^{(2)}}$. Пусть $X^{(3)}$ — наибольшее из этих чисел. Либо $X^{(3)} > X^{(2)}$, либо $X^{(3)} = X^{(2)}$. Если $X^{(3)} = X^{(2)}$, то выделение закончено. Если нет, $X^{(3)} > X_2$, и берем группу из $X_1, X_2, \ldots, X_{X^{(3)}}$ и повторим то же. Число членов полученных групп все возрастает: $X_1 < X^{(2)} < X^{(3)} < \ldots$, но все члены $\leqslant N$. Значит, здесь не более чем N членов, т. е., рассмотрев не более чем N групп, совершим выделение. Если после первого выделения осталось $< N$ членов, то все доказано, иначе же опять начнем выделение с первого оставшегося члена и т. д.

Замечание. Пусть $X_{\alpha+1}, X_{\alpha+2}, \ldots, X_{\alpha+m}$ — одна из групп. Тогда $X_i \leqslant m$ $(i = \alpha+1, \alpha+2, \ldots, \alpha+m)$. Поэтому

$$1 \leqslant \sum_{i=\alpha+1}^{i=\alpha+m} \frac{1}{X_i}.$$

Складывая для всех групп, получим, что число групп не превосходит

$$\sum_{i=1}^{n} \frac{1}{X_i}, \text{ ибо число групп} = s1 \leqslant \sum_{i=1}^{n} \frac{1}{X_i}.$$

Лемма 3. *Пусть $X > 0$ — целое; Y — целое взаимно простое с X; $(Y, X) = 1$; M — целое и $P(z)$ — такая функция z, что для любых значений α и β из ряда $z = M+1, M+2, \ldots, M+X$ будет $|P(\alpha) - P(\beta)| < C$, где C — заданное число. Тогда имеют место неравенства*

$$-C - \frac{1}{2} \leqslant \sum_{z=M+1}^{M+X} \left\{\frac{Yz + P(z)}{X}\right\} - \frac{1}{2} X \leqslant C + \frac{1}{2},$$

или

$$\left| \sum_{z=M+1}^{M+X} \left\{\frac{Yz + P(z)}{X}\right\} - \frac{X}{2} \right| \leqslant C + \frac{1}{2}.$$

Обозначим $S=\sum_{z=M+1}^{M+X}\left\{\frac{Yz+P(z)}{X}\right\}$ и различим два случая:

1°. $C+\frac{1}{2}\geqslant\frac{X}{2}$ Но, очевидно, $0\leqslant S<X$, так что $-\frac{X}{2}\leqslant S-\frac{X}{2}<\frac{X}{2}$ или $-C-\frac{1}{2}\leqslant S-\frac{X}{2}<C+\frac{1}{2}$, чем лемма доказана.

2°. $C+\frac{1}{2}<\frac{X}{2}$.

Пусть P — наименьшее значение $P(z)$ при $z=M+1$, $M+2$, ..., $M+X$ и $P(z)=P+\Phi(z)$, для всех указанных значений z будет $0\leqslant\Phi(z)\leqslant C$.

Пусть $\lfloor P\rfloor=K$; $\{P\}=\varepsilon$. Тогда S можно записать так:

$$S=\sum_{z=M+1}^{M+X}\left\{\frac{Yz+K+\varepsilon+\Phi(z)}{X}\right\}.$$

Можно $Yz+K$ заменить его наименьшим вычетом по модулю X. Так как $(Y, X)=1$, то u будет пробегать в некотором порядке числа

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

когда $z=M+1,\ \ldots,\ M+X$. Сумма S приведется к виду

$$S=\sum_{u=0}^{u=X-1}\left\{\frac{u+\varepsilon+\psi(u)}{X}\right\},$$

где при всех $u=0,\ 1,\ 2,\ \ldots,\ X-1$ будет $0\leqslant\psi(u)\leqslant C$. Разобьем все члены нашего ряда на две группы. В первой группе пусть будут числа под условием $0\leqslant u<X-C-\varepsilon$, а во второй $X-C-\varepsilon\leqslant u<X$. Для чисел первой группы имеем неравенства $0\leqslant\frac{u+\varepsilon+\psi(u)}{X}<1$, а для чисел второй группы $0\leqslant\frac{u+\varepsilon+\psi(u)}{X}<2$, ибо $\frac{X}{2}>C+\frac{1}{2}$. Значит, если положим

$$\left\{\frac{u+\varepsilon+\psi(u)}{X}\right\}=\frac{u+\varepsilon+\psi(u)}{X}+h(u),$$

то для чисел первой группы $h(u)=0$, а для второй группы $h(u)=0$ или $h(u)=-1$. Во второй группе не более $C+\varepsilon$ чисел $\sum_{u=0}^{u=X-1} \frac{u+\varepsilon+\psi(u)}{X} - C - \varepsilon \leqslant S \leqslant \sum_{u=0}^{u=X-1} \frac{u+\varepsilon+\psi(u)}{X}$,

$\frac{X(X-1)}{2}\frac{1}{X} - C - \varepsilon + \varepsilon\frac{X}{X} \leqslant S$, или $\frac{X}{2} - \frac{1}{2} - C \leqslant S$.

Подобным же образом $S \leqslant \frac{1}{2}X - \frac{1}{2} + \varepsilon + C$, так что в силу $-\frac{1}{2}+\varepsilon < \frac{1}{2}$

$$\frac{1}{2}X - \frac{1}{2} - C \leqslant S \leqslant \frac{1}{2}X + \frac{1}{2} + C,$$

$$-\frac{1}{2} - C \leqslant S - \frac{1}{2}X \leqslant \frac{1}{2} + C,$$

что и требовалось доказать.

Переходим к доказательству теоремы 8.2.1. Мы разобьем его на несколько этапов.

1°. Пусть l и $l+1$ лежат в промежутке (Q, R). Тогда имеет место равенство

$$f'(l+1) - f'(l) = f''(l+\delta) \quad (0<\delta<1).$$

Поэтому в ряде чисел

$$f'([Q]+1);\ f'([Q]+2),\ \ldots,\ f'([R]) \qquad (8,2,5)$$

разность между двумя соседними $\geqslant \frac{1}{kA}$ и $\leqslant \frac{1}{A}$. Если наименьшее число из (8,2,5) обозначим K, то наибольшее из них $\leqslant K + \frac{R-Q}{A}$. Далее, число чисел ряда (8,2,5), не выходящих из пределов U и $V>U$, будет $\leqslant kA(U-V)+1$.

2°. Возьмем число τ, удовлетворяющее неравенствам: $4<\tau<\sqrt{A}$. По лемме 1 найдется одна или несколько пар X, Y под условиями $-\frac{1}{\tau} < Xf'(x) - Y < \frac{1}{\tau}$; $(X, Y) = 1$, $0<X<\tau$. Выберем одну из них, обозначая ее $X(x)$, $Y(x)$. Полагая $x=[Q]+1, [Q]+2, \ldots, [R]$, получим

$$X([Q]+1),\ X([Q]+2),\ \ldots,\ X([R]) \qquad (8,2,6)$$

целых положительных чисел, из коих каждое $\leqslant \tau$. Все эти числа, кроме, может быть, τ, из них могут быть по лемме 2 разбиты на группы леммы 2. Пусть одна такая группа будет

$$X(\alpha_s+1),\ X(\alpha_s+2),\ \ldots,\ X(\alpha_s+n_s).$$

Среди ее членов, например, $X(x_s)=n_s$. Тогда

$$-\frac{1}{\tau}<n_s f'(n_s)-Y(x_s)<\frac{1}{\tau}\ (0<n_s\leqslant\tau),$$

так что $f'(x_s)=\dfrac{Y(x_s)}{n_s}+\dfrac{\theta}{\tau n_s}$ $(-1<\theta<1)$.

Рассмотрим теперь сумму

$$\Omega_s=\sum_{x>\alpha_s+1}^{x\leqslant\alpha_s+n_s}\{f(x)\}.$$

Полагая $x=x_s+z$, найдем

$$\Omega_s=\sum_{z=\alpha_s-x_s+1}^{z=\alpha_s-x_s+n_s}\{f(x_s)+zf'(x_s)+\frac{z^2}{2}f''[x_s+z\rho(z)]\}$$
$$(-1<\rho(z)<1).$$

Но $-n_s<z<n_s$, ибо

$$z=x-x_s;\qquad \alpha_s+1\leqslant x_s\leqslant\alpha_s+n_s,$$
$$\alpha_s+1\leqslant x\leqslant\alpha_s+n_s.$$

Таким образом,

$$\Omega_s=\sum_{z=\alpha_s-x_s+1}^{z=\alpha_s-x_s+n_s}\{f(x_s)+zf'(x_s)+\frac{z^2}{2}f''[x_s+z\rho(z)]\}=$$
$$=\sum_{z=\alpha_s-x_s+1}^{z=\alpha_s-x_s+n_s}\left\{\frac{n_s f(x_s)+zY(x_s)+\dfrac{\theta}{\tau}\ z+\sigma(z)\dfrac{n_s^3}{2A}}{n_s}\right\},$$

ибо $f'(x_s)=\dfrac{Y(x_s)}{n_s}+\dfrac{\theta}{\tau n_s}$; здесь $|\theta|<1$, $|\sigma(z)|<1$ и $\sigma(z)$ сохраняет знак. Выражение $\frac{z}{2}f''(x_s+z\rho(z))$ заключено

между $\frac{1}{kA}\ \frac{z}{2}$ и $\frac{1}{A}\ \frac{z^2}{2}$, так что равно $\frac{1}{k'A}\ \frac{n_s^2}{2}\left(\frac{z}{n_s}\right)^2$ $(k' \geqslant 1)$. Обозначая $\frac{1}{k'}\left(\frac{z}{n_s}\right)^2 = \sigma(z)$, увидим, что $\sigma(z) \geqslant 0$ и $\leqslant 1$, откуда и получим нашу формулу. Здесь $z = \alpha_1 - x_s + 1, \ldots$ $\ldots, \alpha_s - x_s + n_s$.

Полагая

$$M = \alpha_s - x_s; \quad X = n_s; \quad Y = Y(x_s); \quad P(z) = n_s f(x_s) + \frac{\theta}{\tau} z + \sigma(z)\frac{n_s^2}{2A}; \quad C = \frac{n_s}{\tau} + \frac{n_s^2}{2A},$$

придем к условиям леммы 3. Применяя ее, найдем

$$\left|\Omega_s - \frac{n_s}{2}\right| < \frac{n_s}{\tau} + \frac{n_s^2}{2A} + \frac{1}{2}.$$

Напишем такие неравенства для всех групп, а для тех чисел x ряда

$$x = [Q] + 1, \quad [Q] + 2, \ \ldots, \ [R], \tag{8,2,7}$$

которые не входят ни в одну из групп, напишем неравенства $-\frac{1}{2} \leqslant \{f(x)\} - \frac{1}{2} < \frac{1}{2}$. Этих чисел $< \tau$. Сложим эти неравенства почленно, заменяя $[R] - [Q]$ на $R - Q + \theta$; $|\theta| < 1$. Тогда будет

$$\left|\sum_{x>Q}^{x\leqslant R} \{f(x)\} - \frac{1}{2}(R - Q)\right| < H,$$

где

$$H = \sum_s \left(\frac{n_s}{\tau} + \frac{n_s^2}{2A} + \frac{1}{2}\right) + \frac{1}{2}\tau + \frac{1}{2};$$

$\sum_s$ идет по всем группам. Эта сумма разбивается на две суммы

$$\sum_s \left(\frac{n_s}{\tau} + \frac{n_s^2}{2A}\right) \quad \text{и} \quad \sum_s \frac{1}{2}.$$

Первая сумма меньше (ибо $n_s < \tau$)

$$\left(\frac{1}{\tau} + \frac{\tau^2}{2A}\right)\sum_s n_s \leqslant \left(\frac{1}{\tau} + \frac{\tau^2}{2A}\right)(R - Q + 1).$$

Вторая сумма $\sum_s \frac{1}{2} = \frac{1}{2} T$, где T — число групп. Так как $\tau > 4$ и $\tau < \sqrt{A}$, то имеем

$$H < \left(\frac{1}{\tau} + \frac{\tau^2}{2A}\right)(R-Q) + \tau + \frac{T}{2}. \qquad (8,2,8)$$

3°. Для оценки T воспользуемся тем, что

$$T < \sum \frac{1}{X}, \qquad (8,2,9)$$

где X пробегает значения

$$X([Q]+1),\ X([Q]+2),\ \ldots,\ X([R]). \qquad (8,2,6)$$

Оценим, сколько раз в ряде (8,2,6) повторяется одно и то же значение X.

С каждым данным X могут быть связаны лишь такие значения Y, которые удовлетворяют неравенствам

$$-\frac{1}{\tau} < n_s f'(x_s) - Y(x_s) < \frac{1}{\tau},\quad -\frac{1}{\tau} < Xf'(x) - Y < \frac{1}{\tau}.$$

Поэтому

$$Y > -\frac{1}{\tau} + n_s f'(x_s);$$

$Y > -\frac{1}{\tau} + XK$, K — наименьшее из чисел ряда (8,2,5)

$$Y < Xf'(x) + \frac{1}{\tau} < X\left(K + \frac{R-Q}{A}\right) + \frac{1}{\tau},$$

$$XK - \frac{1}{\tau} < Y < X\left(K + \frac{R-Q}{A}\right) + \frac{1}{\tau}.$$

Число этих значений Y не превосходит

$$X\,\frac{R-Q}{A} + \frac{3}{2}.$$

Вот сколько Y может быть у одного X. С каждой данной парой X и Y могут быть связаны лишь те числа ряда (8,2,5), которые удовлетворяют неравенствам

$$\frac{Y - \frac{1}{\tau}}{X} < f'(x) < \frac{Y + \frac{1}{\tau}}{X}.$$

Число таких значений на основании сказанного в 1° $\left(f''(x)> \right.$ $\left. > \frac{1}{kA}\right)$ не больше чем

$$\frac{2kA}{\tau X}+1<3k\frac{A}{\tau X},\quad \text{ибо } \tau<\sqrt{A},\ X<\tau.$$

Значит, с данным X связано не более $\left(X\frac{R-Q}{A}+\frac{3}{2}\right)3k\frac{A}{\tau X}$ чисел ряда (8,2,5) $f'([Q]+1),\ldots,f'([R])$. А потому и в ряду (8,2,6)

$$X([Q]+1),\ldots,X([R])$$

данный X встретится не более чем столько раз. В самом деле, $X(L)$ в этом ряду есть значение X, подобранное для $f'(L)$ так, что

$$-\frac{1}{\tau}X(L)f'(L)-Y<\frac{1}{\tau}\ (0<X<\tau),$$

т. е. X связан со значением $f'(L)$, а мы подсчитали, сколько таких значений связано с X. Их, стало быть, не более чем

$$k\left(3\frac{R-Q}{\tau}+\frac{9}{2}\frac{A}{\tau X}\right).$$

А потому из (8,2,9)

$$T<k\sum_{X>0}^{X<\tau}\left(3\frac{R-Q}{\tau}\frac{1}{X}+\frac{9}{2}\frac{A}{\tau}\frac{1}{X^2}\right)<$$

$$<k\left(\frac{3}{2}\frac{R-Q}{\tau}\lg A+3\frac{R-Q}{\tau}+\frac{15}{2}\frac{A}{\tau}\right),$$

ибо $\sum\frac{1}{n^2}=\frac{\pi^2}{6}<\frac{5}{3}$. Из (8,2,8) находим

$$H<\left(\frac{1}{\tau}+\frac{\tau^2}{2A}\right)(R-Q)+\tau+\frac{1}{2}k\left(\frac{3}{2}\frac{R-Q}{\tau}\lg A+3\frac{R-Q}{\tau}+\right.$$

$$\left.+\frac{15}{2}\frac{A}{\tau}\right)<(R-Q)\left(\frac{5}{2\tau}+\frac{\tau^2}{2A}+\frac{3}{4}k\frac{\lg A}{\tau}\right)+\frac{15}{4}k\frac{A}{\tau}+\tau.$$

Пусть $\tau=\sqrt{A\lg A}$: тогда $4<\tau<\sqrt{A}$, и будет

$$H<k\frac{R-Q}{A}\left(\frac{3}{4}\frac{A\lg A}{\tau}\right)+k\frac{2A}{\tau}+$$

$$+(R-Q)\left(\frac{5}{2\tau}+\frac{\tau^2}{2A}\right)+\tau<$$

$$<2k\left(\frac{R-Q}{A}+1\right)(A\lg A)^{\frac{2}{3}}\quad (A>25).$$

Это и доказывает основную формулу.

§ 3. Применение формулы Н. Я. Сонина *

Мы получили основную оценку для суммы дробных частей

$$\sum_{x>Q}^{x\leqslant R}\{f(x)\}=\frac{R-Q}{2}+G, \tag{8,3,1}$$

где

$$|G|<2k\left(\frac{R-Q}{A}+1\right)(A\lg A)^{\frac{2}{3}}. \tag{8,3,2}$$

Отсюда

$$\sum_{x>Q}^{x\leqslant R}[f(x)]=\sum_{x>Q}^{x\leqslant R}f(x)-\frac{R-Q}{2}-G. \tag{8,3,3}$$

Для подсчета первого члена правой части применяем формулу Н. Я. Сонина (см. [23]).

Пусть $\rho(x)=[x]-x+\frac{1}{2}$; $\sigma(x)=\int\limits_0^x\rho(x)\,dx$. Тогда

$$\sum_{x>a}^{x\leqslant b}f(x)=\int\limits_a^b f(x)\,dx+\rho(b)f(b)-\rho(a)f(a)-\sigma(b)f'(b)+$$
$$+\sigma(a)f'(a)+\int\limits_a^b f''(x)\,\sigma(x)\,dx. \tag{8,3,4}$$

При этом

$$|\rho(x)|\leqslant\frac{1}{2};\quad |\sigma(x)|\leqslant\frac{1}{8}.$$

Если еще $f''(x)$ сохраняет знак, то ввиду того, что $\sigma(x)$ сохраняет знак, и если $|f'(x)|\leqslant\mu$ на сегменте $[Q, R]$, то

$$\left|\int\limits_a^b f''(x)\,\sigma(x)\,dx\right|<\frac{\mu}{4}. \tag{8,3,5}$$

Кроме того, разумеется, $|\sigma(b)f'(b)|\leqslant\frac{\mu}{8}$ и $|\sigma(a)f'(a)|\leqslant\frac{\mu}{8}$.

Поэтому (8,3,4) и (8,3,3) дают

$$\sum_{x>Q}^{x\leqslant R}[f(x)]=\int_{Q}^{R}f(x)\,dx+\rho(R)f(R)-$$

$$-\rho(Q)f(Q)-\frac{R-Q}{2}+H, \qquad (8,3,6)$$

где

$$|H|<\frac{\mu}{2}+2k\left(\frac{R-Q}{A}+1\right)(A\lg A)^{\frac{2}{3}}. \qquad (8,3,7)$$

В качестве примера применения теоремы 8.2.1 рассмотрим семейство парабол, зависящих от параметров n, a:

$$y=\frac{n+x^2}{a}, \quad n>0; \quad -a\leqslant Q<R\leqslant a.$$

Здесь имеем: $y'=\frac{2x}{a}$, $\mu=2$, $y''=\frac{2}{a}$, $k=1$, $A=\frac{a}{2}$. Для числа T целых точек внутри контура получим

$$T=\frac{1}{3a}(R^3-Q^3)+\rho(R)\frac{n+R^2}{a}-\rho(Q)\frac{n+Q^2}{a}+$$

$$+\frac{n}{a}(R-Q)-\frac{R-Q}{2}+H;$$

$$|H|\leqslant 1+10\left(\frac{a}{2}\lg\frac{a}{2}\right)^{\frac{2}{3}}<8\,(a\ln a)^{\frac{2}{3}} \quad \left(\frac{a}{2}>25\right).$$

§ 4. Обобщение теоремы 8.2.1 *

Пусть на дуге кривой отношение $\frac{r_{\max}}{r_{\min}}<\sigma$; r—радиус кривизны. Тогда $f''(x)$ сохраняет знак; $f'(x)$ монотонна. Пусть она возрастает.

1°. Пусть $|f'(x)|\leqslant 1$ на всей дуге; $f'(x)\not\equiv 0$. Имеем: $y''=\frac{(1+y'^2)^{\frac{3}{2}}}{r}$; отсюда

$$\frac{1}{r}<f''(x)<\frac{2^{\frac{3}{2}}\sigma}{r}, \quad r=r_{\max}.$$

Тогда в обозначениях § 3: полагая $\mu=1$; $A=\frac{r}{2^{\frac{3}{2}}\sigma}$; $k=2^{\frac{3}{2}}\sigma$. Далее, из $y_1'-y_0'=\int_Q^R y''dx$ выводим

$$(R-Q)\frac{1}{r}<2; \quad R-Q<2r.$$

Тогда, если T — число целых точек; S — площадь кривой, найдем

$$T=S+\rho(R)f(R)-\rho(Q)f(Q)-\frac{R-Q}{2}+H \quad (8,4,1)$$

и при $\frac{r}{2^{\frac{3}{2}}\sigma}>25$

$$|H|<\frac{1}{2}+2^{\frac{5}{2}}\sigma(2^{\frac{5}{2}}\sigma+1)\left(\frac{r}{2^{\frac{3}{2}}\sigma}\ln\frac{r}{2^{\frac{3}{2}}\sigma}\right)^{\frac{2}{3}}<19\sigma^{\frac{4}{3}}(r\ln r)^{\frac{2}{3}}. \quad (8,4,2)$$

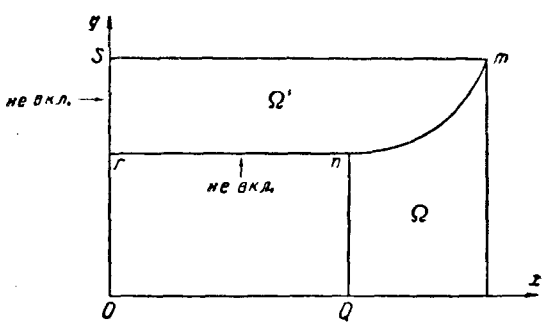

Рис. 6.

2°. Пусть $|f'(x)|\geqslant 1$ всюду на дуге (рис. 6). $Or=k$; $OS=l$; меняя роль осей, получим для области Ω' число целых точек

$$T'=S'+\rho(l)R-\rho(h)Q-\frac{1}{2}(l-h)+H'';$$

$$|H''|<19\sigma^{\frac{4}{3}}(r\ln r)^{\frac{2}{3}}.$$

Число целых точек в прямоугольнике $ORnS$ без сторон OR и OS будет: $T+T'+[Q][f(Q)]=[R][f(R)]$, так что:

$$T=[R][f(R)]-[Q][f(Q)]-T',$$
$$T'=S'+\rho(f(R))R-\rho(f(Q))Q+\frac{1}{2}(f(R)-f(Q))+H'',$$
$$S'=Rf(R)-Qf(Q)-S,$$
$$-T'=S-Rf(R)+Qf(Q)-\rho(f(R))R+\rho(f(Q))Q+$$
$$+\frac{1}{2}(f(R)-f(Q))-H''.$$

Отсюда находим

$$T=[R][f(R)]-[Q][f(Q)]+S-Rf(R)+Qf(Q)-$$
$$-\rho(f(R))R+\rho(f(Q))Q+\frac{1}{2}(f(R)-f(Q))-H''=$$
$$=S+f(R)\left([R]-R+\frac{1}{2}\right)-f(Q)\left([Q]-Q+\frac{1}{2}\right)-$$
$$-\frac{R-Q}{2}-[R]f(R)-R([f(R)]-f(R))+[R][f(R)]+$$
$$+[Q]f(Q)+Q([f(Q)]-f(Q))-[Q][f(Q)]-H''=$$
$$=S+\rho(R)f(R)-\rho(Q)f(Q)-(R-[R])(f(R)-[f(R)])+$$
$$+(Q-[Q])(f(Q)-[f(Q)])-H'=$$
$$=S+\rho(R)f(R)-\rho(Q)f(Q)+H''';$$
$$|H'''|<1+19\sigma^{\frac{4}{3}}(r\ln r)^{\frac{2}{3}}<20\sigma^{\frac{4}{3}}(r\lg r)^{\frac{2}{3}}. \qquad (8.4,3)$$

3°. Пусть в некоторых точках дуги nm $|f'(x)|\leqslant 1$, а в других >1. Дугу nm можно разбить на не более чем 3 части, в каждой из коих $|f'(x)|\leqslant 1$ либо $\geqslant 1$. Ибо на ней $f'(x)$ монотонна; скажем, если она возрастает, то если она вначале >0, то получим разбиение на 1 или 2 дуги. Если она была вначале <0 и <-1, то получим разбиение на 3, 2 или 1 дугу, если <0 и >-1, то на 2 или 1 дугу. Область Ω разобьется на $\leqslant 3$ дизъюнктных областей. В каждой области применяем (8,4,2) или (8,4,3) и складываем:

$$T=S+\rho(R)f(R)-\rho(Q)f(Q)-\frac{1}{2}(R-Q)+\Gamma; \qquad (8,4,4)$$
$$|\Gamma|<60\sigma^{\frac{4}{3}}(r\ln r)^{\frac{2}{3}}.$$

§ 5. Распространение на замкнутый контур*

Пусть Ω с площадью S ограничена контуром C (рис. 7); $\frac{r_{\max}}{r_{\min}} < \sigma$. Проводим две вертикальные касательные. Ω' — заштрихованная, Ω'' — нижняя область; γ — число точек с целыми координатами на дуге nsm. По формуле (8,4,4): если T — число точек внутри контура, то

$$T + \gamma = S + B(r \ln r)^{\frac{2}{3}}.$$

Дабы исключить γ, берем гомотетичный, но весьма близкий контур, для коего нет целых точек на верхней дуге. Отсюда

$$T = S + B(r \ln r)^{\frac{2}{3}}, \quad r = r_{\max}.$$

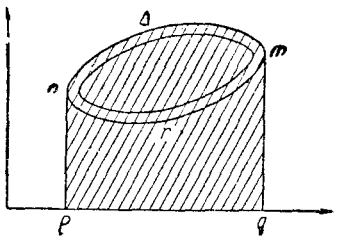

Рис. 7.

В качестве примера рассмотрим эллипс:

$$ax^2 + 2bxy + cy^2 \leqslant M,$$
$$b^2 - ac = -D < 0, \ a > 0.$$

Если исходный эллипс $ax^2 + 2bxy + cy^2 \leqslant 1$, то данный получается расширением в $\sqrt{M}$ раз; кривизна будет в $\sqrt{M}$ раз меньше, $\sigma = \frac{r_{\max}}{r_{\min}} = \text{const}, r = \rho\sqrt{M}$; площадь Ω есть $S = \frac{\pi M}{\sqrt{D}}$. Из предыдущего имеем

$$T' = \frac{\pi M}{\sqrt{D}} + BM^{\frac{1}{3}}(\ln M)^{\frac{2}{3}}.$$

Отметим, что изложенный здесь метод И. М. Виноградова, несмотря на свою элементарность, дает оценки погрешности, которые в общем случае могут быть улучшены не более чем на множитель $(\lg r)^{\frac{2}{3}}$. Такое улучшение может быть сделано применением сложных аналитических методов. Э. Ландау [41], действуя аналитическими методами, доказал следующую теорему: пусть $w > 0$ есть целое число; пусть при $\frac{1}{2} \leqslant u \leqslant w$

дано семейство функций $f(u)$, зависящих от параметра $A\to\infty$ и таких, что $f''(u)$ существует и непрерывна; $f\left(\frac{1}{2}\right)>2; 0<f'(u)<1$, $f''(u)>\frac{1}{A}$ $(A>1)$.

Тогда если S — площадь под отрезком кривой на сегменте $[1, w]$, а T — число целых точек там же, не считая оси, то

$$|T-S|<cA^{\frac{2}{3}}. \tag{8,5,1}$$

Это улучшает изложенный здесь результат И. М. Виноградова в $(\lg r)^{\frac{2}{3}}$ раз. Но дальнейшие улучшения в общем случае невозможны. Это следует из результата В. Ярника 1926 г.: существует кривая L, зависящая от параметра A и удовлетворяющая указанным ранее условиям, для которой

$$|T-S|>c_1A^{\frac{2}{3}}. \tag{8,5,2}$$

Однако для частных видов контуров, как, например, окружность или эллипс, имеют место лучшие результаты, чем (8,5,1), хотя, как уже говорилось в § 1, точный порядок $T-S$ еще не найден.

Условие § 4 для отношения радиусов кривизны не выполняется для случая гиперболы, отвечающей проблеме делителей. Однако здесь возможно видоизменение изложенного метода, состоящее в разбиении контура на куски, внутри которых относительное изменение радиуса кривизны допустимо (см. И. М. Виноградов [1]).

Таким образом, например, для проблемы делителей получается соотношение

$$\rho(n)=Bn^{\frac{1}{3}}(\lg n)^{\frac{5}{3}}$$

в формуле (8,1,9).

Изложенный здесь элементарный метод счета целых точек в контурах применим и к трехмерным проблемам, например к проблеме счета точек внутри и на сфере

$$x^2+y^2+z^2=R^2.$$

ГЛАВА 9

О РАСПРЕДЕЛЕНИИ СТЕПЕННЫХ ВЫЧЕТОВ

§ 1. Одна теорема И. М. Виноградова

В настоящей главе мы будем рассматривать распределение степенных вычетов и невычетов степени $l>1$ для большого простого модуля $p\equiv 1 \pmod l$. Мы начнем с изложения элементарного метода И. М. Виноградова (см. [4]).

Теорема 9. 1. 1 (И. М. Виноградов). *Пусть $p>2$ — простое число, $l>1$, $p\equiv 1 \pmod l$ и числа $1, 2, \ldots, p-1$ разбиты на классы $A_0, A_1, \ldots, A_{l-1}$ вычетов и невычетов l-й степени по модулю p.*

Пусть a не делится на p; b — произвольное целое число и $0<h<p$.

Количество c_i чисел i-го класса A_i $(i=0,1,\ldots, l-1)$, содержащихся в прогрессии $ax+b$ $(x=0,1,\ldots, h-1)$ имеет вид

$$c_i=\frac{h}{l}+\Delta_i, \tag{9,1,1}$$

где

$$\Delta_i^2<2T.$$

При этом

$$T=\sum_{x=1}^{h}\sum_{(y)}\left(\frac{p}{xy}+1\right) \tag{9,1,2}$$

и суммирование по y идет при данном x, по всем $y\leqslant \frac{p}{x}$; $(y, x)=1$.

Заметим, что из (9,1,2) следует

$$T=Bp(\lg p)^2, \tag{9,1,3}$$

так что

$$\Delta_1 = B\sqrt{p}\lg p. \qquad (9,1,4)$$

Доказательство теоремы 9.1.1 основывается на трех леммах, которые здесь приведем.

Лемма 1. *Пусть* A, B — *реальные числа,* $k > 0$ — *целое;*

$$A = \frac{t}{q} + \frac{\theta}{qk} \quad (0 < q \leqslant k, (t, q) = 1, |\theta| < 1);$$

c, m — *целые числа;* $0 < m \leqslant \frac{k}{q}$. *Тогда*

$$\sum_{x=c}^{c+mq-1} \{Ax + B\} = \frac{1}{2} mq + \frac{1}{2} \rho(m+1); \quad |\rho| \leqslant 1. \qquad (9,1,5)$$

Доказательство этой леммы во многом сходно с доказательством леммы главы 7.

Подставим вместо A его значение, имеем: $Ax + B = \frac{tx + f(x)}{q}$, где $f(x) = Bq + \frac{\theta x}{k}$. При этом $f(x)$ — линейная функция x, так что при $c \leqslant x \leqslant c + mq - 1$ $f(x)$ лежит между крайними значениями $f(c)$ и $f(c + mq - 1)$. Разность этих крайних значений по абсолютной величине не больше $\left|\frac{mq-1}{k}\right| \leqslant 1$. Значит, целые числа $[f(c)]$ и $[f(c + mq - 1)]$ отличаются не более чем на единицу.

Сумму в левой части (9, 1, 5) разобьем на m сумм:

$$S = S_0 + S_1 + \ldots + S_{m-1}; \quad S_i = \sum_{c+iq}^{c+iq+q-1} \{Ax + B\}.$$

Рассмотрим одну из таких сумм S_j. Если имеем равенство $[f(c + jq)] = [f(c + jq + q - 1)] = n$, то, полагая $f(x) = n + \lambda(x)$ $(0 \leqslant \lambda(x) < 1$ при $c + jq \leqslant x \leqslant c + jq + q - 1)$, имеем

$$S_j = \sum_{c+jq}^{c+jq+q-1} \left\{\frac{tx + n + \lambda(x)}{q}\right\} = \sum_{r=0}^{q-1} \frac{r + \lambda(x)}{q}, \qquad (9,1,6)$$

ибо $tx+n$ пробегает вместе с x полную систему вычетов $(\mathrm{mod}\, q)$. Из (9, 1, 6) находим

$$S_j = \frac{q}{2} + \frac{\rho_j}{2} \qquad (|\rho_j| \leqslant 1). \tag{9,1,7}$$

Если же числа $[f(c+jq)]$ и $[f(c+jq+q-1)]$ отличаются на единицу, то обозначим меньшее из них n и положим $f(x) = n + \lambda(x)$; тогда для рассматриваемых значений x имеем: $0 \leqslant \lambda(x) < 2$, причем крайние значения $\lambda(x)$ должны лежать в отрезках $[0, 1)$ и $[1, 2)$. Аналогично предыдущему находим

$$S_j = \sum_{r=0}^{q-1} \left\{\frac{r+\lambda(x)}{q}\right\}$$

при $0 \leqslant r \leqslant q-2$, $\left\{\frac{r+\lambda(x)}{q}\right\} = \frac{r+\lambda(x)}{q}$. Учитывая и $r = q-1$ и полагая $\delta = 0$ или $\delta = 1$, найдем

$$S_j = \sum_{r=0}^{q-1} \frac{r+\lambda(x)}{q} - \delta = \frac{q-1}{2} - \delta + \frac{1}{q} \sum_{c+jq}^{c+jq+q-1} \lambda(x) =$$

$$= \frac{q}{2} - \frac{1}{2} - \varepsilon + \frac{1}{2}(\lambda(c+jq) + \lambda(c+jq+q-1)), \tag{9,1,8}$$

откуда

$$S_j = \frac{q}{2} + \rho_i \qquad (|\rho_i| \leqslant 1). \tag{9,1,9}$$

Заметим теперь, что значение j, для которых $[f(c+jq)] \neq [f(c+jq+q-1)]$, может быть только одно. Складывая полученные выражения для S_j, придем к формуле (9, 1, 5).

Лемма 2. *Пусть $p > 2$ — простое число; α — одно из чисел $1, 2, \ldots, p-1$; β_α — целое число, могущее меняться с изменением α, $h \in [1, p-1]$ — целое число.*

Положим

$$S_\alpha = \sum_{x=0}^{h-1} \left\{\frac{\alpha x + \beta_\alpha}{p}\right\}, \quad L_\alpha = S_\alpha - \frac{h}{2}. \tag{9,1,10}$$

Тогда

$$\sum_{\alpha=1}^{p-1} |L_\alpha| < T,$$

где T *задается формулой* (9,1,2).

Для исследования данной суммы S_α найдем несократимую дробь $\frac{t_0}{x_0}$ под условиями $\frac{\alpha}{p} = \frac{t_0}{x_0} + \frac{\theta_0}{x_0 h}$; $x_0 \in (0,h]$; $|\theta_0| < 1$. Положим $m_0 = \left[\frac{h}{x_0}\right]$, $h_1 = h - m_0 x_0$ ($m_0 > 0$, $0 < h_1 < x_0$), и разобьем S_α на части: $S_\alpha = \sum_{x=0}^{m_0 x_0 - 1} \left\{\frac{\alpha x + \beta_\alpha}{p}\right\} + \sum_{m_0 x_0}^{h-1} \left\{\frac{\alpha x + \beta_\alpha}{p}\right\}$. К первой части S_α применим лемму 1, полагая $q = x_0$. Из формулы (9,1,5), если примем $m_0 x_0 = h - h_1$, $m_0 \leqslant \frac{h}{x_0}$, находим для суммы S_α выражение

$$S_\alpha = \frac{1}{2}(h - h_1) + \frac{1}{2}\rho_0 \left(\frac{h}{x_0} + 1\right) + S'_\alpha, \qquad |\rho_0| \leqslant 1,$$

где

$$S'_\alpha = \sum_{x=c_0}^{c_0 + h_1 - 1} \left\{\frac{\alpha x + \beta_\alpha}{p}\right\} \quad (c_0 = m_0 x_0).$$

Далее так же поступаем с новой суммой S'_α. Полагаем

$$\frac{\alpha}{p} = \frac{t_1}{x_1} + \frac{\theta_1}{x_1 h_1}; \quad 0 < x_1 \leqslant h_1; \quad (t_1, x_1) = 1, \quad |\theta_1| < 1;$$

$$m_1 = \left[\frac{h_1}{x_1}\right], \quad h_2 = h_1 - m_1 x_1, \quad 0 < h_2 < x_1,$$

и аналогично прежнему получаем выражение

$$S'_\alpha = \frac{1}{2}(h_1 - h_2) + \frac{1}{2}\rho_2 \left(\frac{h_1}{x_1} + 1\right) + S''_\alpha, \quad |\rho_2| \leqslant 1;$$

$$S''_\alpha = \sum_{x=c_1}^{c_1 + h_2 - 1} \left\{\frac{\alpha x + \beta_\alpha}{p}\right\}, \qquad c_1 = m_0 x_0 + m_1 x_1.$$

Продолжаем этот процесс далее; мы видим, что h, h_1, h_2, ... убывают, так что на некотором шаге будет $h_{n+1} = 0$, и

процесс закончится. Последнее равенство имеет вид

$$S_\alpha^{(n)} = \frac{1}{2} h_n + \frac{1}{2} \rho_n \left(\frac{h_n}{x_n} + 1 \right), \quad |\rho_n| \leqslant 1,$$

где

$$\frac{\alpha}{p} = \frac{t_n}{x_n} + \frac{\theta_n}{x_n h_n}, \qquad 0 < x_n \leqslant h_n, \qquad (t_n, x_n) = 1, \qquad |\theta_n| < 1,$$

$m_n = \left[\frac{h_n}{x_n}\right] = \frac{h_n}{x_n}$; $h_{nn} = h_n - m_n x_n = 0$. Складывая полученные выражения для S_α, $S_\alpha', \ldots, S_\alpha^{(n)}$, находим

$$S_\alpha = \frac{1}{2} h + \frac{1}{2} \rho_0 \left(\frac{h}{x_0} + 1 \right) + \frac{1}{2} \rho_1 \left(\frac{h_1}{x_1} + 1 \right) + \ldots$$
$$\ldots + \frac{1}{2} \rho_n \left(\frac{h_n}{x_n} + 1 \right),$$

откуда

$$L_\alpha = S_\alpha - \frac{h}{2} = \frac{\rho}{2} \left[\left(\frac{h}{x_0} + 1 \right) + \left(\frac{h_1}{x_1} + 1 \right) + \ldots \right.$$
$$\left. \ldots + \left(\frac{h_n}{x_n} + 1 \right) \right] (|\rho| \leqslant 1)$$

и

$$\sum_{\alpha=1}^{p-1} |L_\alpha| \leqslant \frac{1}{2} \sum_{\alpha=1}^{p-1} \left[\left(\frac{h_0}{x_0} + 1 \right) + \left(\frac{h_1}{x_1} + 1 \right) + \ldots + \right.$$
$$\left. + \left(\frac{h_n}{x_n} + 1 \right) \right]. \quad (9,1,11)$$

В последней сумме числа x_i, h_i зависят от α и определяются этим числом.

Для оценки суммы соберем в ней все слагаемые вида $\frac{h_l}{x_l} + 1$, где x имеет одно и то же значение. Равенство

$$\frac{\alpha}{p} = \frac{t_i}{x_i} + \frac{\theta_i}{x_i h_i}$$

запишем в виде

$$\alpha x_i = p t_i + y_i, \quad y_i = \frac{p \theta_i}{h_i}.$$

Отсюда видим, что y_i — целое число; $(y_i, x_i) = 1$ и $\alpha x_i \equiv y_i \pmod p$

$\left(0<|y_i|<\frac{p}{h_i}\right)$. Если x_i, y_i заданы и удовлетворяют данным условиям, то (при фиксированных α, h_i) определяется t_i.

Для оценки сверху тех членов $\frac{h_i}{x_i}+1$, где x_i равны заданному числу x $(0<x\leqslant h)$, рассмотрим соответствующие значения α; y_i. Так как $|y_i|\in\left(0, \frac{p_i}{h_i}\right)$, то y_i может принимать лишь значения $\pm 1, \pm 2, \ldots, \pm\left[\frac{p}{x}\right]$ взаимно простые с x. При выбранном y_i число α определяется из сравнения $\alpha x_i \equiv y_i \pmod p$. Далее, $\frac{h_i}{x_i}<\frac{p}{x_i|y_i|}$, и поэтому сумма указанных членов $\frac{h_i}{x_i}+1$ не превосходит $2\sum\left(\frac{p}{xy}+1\right)$, где сумма берется по всем $y=1,2,\ldots,\left[\frac{p}{x}\right]$, взаимно простым с x. Это доказывает лемму 2.

Лемма 3. *Пусть числа* p, α, β_α *определяются, как в предыдущей лемме;* h, γ — *целые числа* $\in(0, p)$. *Пусть* R_α — *количество тех чисел* $\alpha x+\beta_\alpha$ $(x=0,1,2,\ldots,h-1)$, *для которых*

$$0<\left\{\frac{\alpha x+\beta_\alpha}{p}\right\}<\frac{\gamma}{p}.$$

Положим

$$H(\alpha, \beta_\alpha, h, \gamma)=R_\alpha-\frac{h\gamma}{p}. \qquad (9,1,12)$$

Тогда

$$\sum_{\alpha=1}^{p-1}|H(\alpha, \beta_\alpha, h, \gamma)|<2T. \qquad (9,1,13)$$

Эта лемма легко выводится из леммы 2. Заметим, что

$$\left\{\frac{\alpha x+\beta_\alpha-\gamma}{p}\right\}-\left\{\frac{\alpha x+\beta_\alpha}{p}\right\}=1-\frac{\gamma}{p},$$

если наименьший вычет $\alpha x+\beta_\alpha$ по модулю p лежит в отрезке $(0, \gamma]$, и $-\frac{\gamma}{p}$, если он лежит в отрезке $[\gamma, p)$. Ввиду этого

получим

$$S'_\alpha - S_\alpha = \sum_{x=0}^{h-1} \left\{\frac{\alpha x + \beta_\alpha - \gamma}{p}\right\} - \sum_{x=0}^{h-1} \left\{\frac{\alpha x + \beta_\alpha}{p}\right\} = H(\alpha, \beta_\alpha, h, \gamma).$$

По лемме 2 имеем

$$\sum_{\alpha=1}^{p-1} \left| S'_\alpha - \frac{h}{2} \right| < T; \quad \sum_{\alpha=1}^{p-1} \left| S_\alpha - \frac{h}{2} \right| < T,$$

откуда

$$\sum_{\alpha=1}^{p-1} |S'_\alpha - S_\alpha| = \sum_{\alpha=1}^{p-1} |H(\alpha, \beta_\alpha, h, \gamma)| < 2T,$$

что и доказывает лемму 3.

§ 2. Доказательство теоремы 9.1.1

Перейдем к доказательству теоремы 9.1.1. Пусть j — одно из чисел $0, 1, 2, \ldots, l-1$. Составим $(p-1)h : l$ произведений

$$\alpha(ax + b), \tag{9,2,1}$$

где α пробегает все числа класса A_j, и независимо от α $x = 0, 1, 2, \ldots, h-1$. Для каждого из этих произведений определим число u сравнением:

$$au + b \equiv \alpha(ax + b) \pmod p \quad (0 \leqslant u < p). \tag{9,2,2}$$

Обозначим через D число произведений (9, 2, 1), для которых соответствующие значения u меньше h. Это количество D мы будем вычислять двумя разными способами; сравнение их и даст нам нужное доказательство. Рассмотрим сначала те произведения (9, 2, 1), которые отвечают одному и тому же значению α. Пусть $aa' \equiv 1 \pmod p$, тогда сравнение (9, 2, 2) можно заменить сравнением $u \equiv \alpha x + \beta_\alpha$, $\beta_\alpha = \alpha ba' - ba'$ и не зависит от x. Применяя лемму 3 для заданного значения α и суммируя по всем значениям α, находим

$$D = \frac{p-1}{l} \frac{h^2}{p} + \sum_\alpha H(\alpha, \beta_\alpha, h, h). \tag{9,2,3}$$

Теперь подсчитаем D другим способом, оставляя в произведениях (9, 2, 1) x постоянным. Если при этом $ax + b \equiv$

$\equiv 0 \pmod p$, то все $\frac{p-1}{l}$ соответствующих произведений должны быть причислены к D. Если $ax+b\equiv 0 \pmod p$, то это число есть одно из c_j чисел класса A_j, содержащихся в нашей прогрессии. В этом случае, в силу (9, 2. 2), $au+b$ принадлежит классу A_{i+j} (число $i+j$ надо брать по модулю l). Из всех чисел α существует, ввиду этого, c_{i+j} таких, для которых $u\in(0, h)$. Отсюда

$$D=c_0 c_i+c_1 c_{i+1}+\ldots+c_{l-1} c_{i+l-1}+\eta, \qquad (9,2,4)$$

где $\eta=\frac{p-1}{l}$, если сравнение $ax+b\equiv 0 \pmod p$ $(0\leqslant x\leqslant h-1)$ разрешимо, и $\eta=0$ в противном случае.

Сравнивая (9, 2, 3) и (9, 2, 4), получим при всяком i

$$c_0 c_i+c_1 c_{i+1}+\ldots+c_{l-1} c_{i+l-1}+\eta= \\ =\frac{p-1}{l}\frac{h^2}{p}+\sum_{\alpha} H(\alpha, \beta_\alpha, h, h), \qquad (9,2,5)$$

где справа суммирование по $\alpha\in A_i$. Положим в (9, 2, 5) $i=0$, и из полученной формулы вычтем почленно (9, 2, 5). Так как числа $c_i, c_{i+1}, \ldots, c_{i+l-1}$ лишь порядком отличаются от $c_0, c_1, \ldots, c_{l-1}$, получим

$$(c_0-c_i)^2+(c_1-c_{i+1})^2+\ldots+(c_{l-1}-c_{i+l-1})^2= \\ =2\sum_{\alpha'} H(\alpha', \beta_{\alpha'}, h, h)-2\sum_{\alpha} H(\alpha, \beta_\alpha, h, h), \qquad (9,2,6)$$

причем в правой части α, α' пробегает все числа классов A_i и A_0. По лемме 3 правая часть нашего равенства не превышает $4T$; поэтому при любом r

$$(c_r-c_{r+i})^2+(c_r-c_{r-i})^2<4T. \qquad (9,2,7)$$

Отсюда

$$2\sum_{i=0}^{l-1}(c_r-c_i)^2<4T(l-1). \qquad (9,2,8)$$

Положим теперь

$$\frac{c_0+c_1+\ldots+c_{l-1}}{l}=\bar{c},\ c_i=\bar{c}+\delta_i,$$

тогда имеем

$$\sum_{l=0}^{l-1}(\delta_r-\delta_l)^2<2T(l-1),$$

так как $\sum_{l=0}^{l-1}\delta_l=0$, то

$$l\delta_r^2+\sum_{l=0}^{l-1}\delta_l^2<2T(l-1),$$

откуда

$$\delta_r^2<2T\frac{l-1}{l+1}. \tag{9,2,9}$$

Если данная прогрессия $ax+b$ $(x=0,1,\ldots,h-1)$ не содержит нуль, то, очевидно, $\bar{c}=\frac{h}{l}$; $\delta_r=\Delta_r$, $\Delta_r^2<2T\frac{l-1}{l+1}<$ $<2T$. Если же она содержит нуль по модулю p, то $\bar{c}=\frac{h-1}{l}$; $\Delta_r=\delta_r-\frac{1}{l}$; $\Delta_r^2<2T\frac{l-1}{l+1}+\frac{2|\delta_r|}{l}$; далее, $\delta_i=c_i-\bar{c}$, так что $|\delta_i|<\frac{p}{2}<\frac{T}{2}$ и

$$\Delta_r^2<2T\left(\frac{l-1}{l+1}+\frac{1}{2l}\right)<2T,$$

что и завершает доказательство теоремы.

§ 3. Другие элементарные теоремы о распределении характеров. Нерешенные проблемы

На языке арифметической теории характеров (см., например, [3]), теорема 9.1.1 имеет простую формулировку. Пусть $p\equiv 1\pmod{l}$ — простое число, а $\chi(m)$ — неглавный характер l-й степени по модулю p. Тогда имеем

$$\left|\sum_{x=0}^{h-1}\chi(ax+b)\right|<2lT. \tag{9,3,1}$$

Менее точная формулировка (при использовании (9,1,4)) будет

$$\left|\sum_{x=0}^{h-1}\chi(ax+b)\right|=Blp^{\frac{1}{2}}\lg p. \tag{9,3,2}$$

Заметим, что случай распределения характеров в прогрессии $ax+b$ легко сводится на случай распределения их в ряду последовательных чисел $x=1,2,\ldots,H$ $(H\leqslant p-1)$. В самом деле, так как a выбирается $\not\equiv 0 \pmod p$ то $\chi(ax+b)=\chi(a)\chi(x+ba')$, где $aa'\equiv 1 \pmod p$. Если известно, что

$$\left|\sum_{y=1}^{Y}\chi(y)\right| = Blp^{\frac{1}{2}}\lg p, \tag{9.3.3}$$

то имеем также

$$\left|\sum_{x=0}^{h-1}\chi(x+ba')\right| = Blp^{\frac{1}{2}}\lg p, \tag{9.3.4}$$

откуда следует (9. 3, 2).

Мы будем далее заниматься неглавными характерами второй степени (квадратичными характерами), ка имеющими наиболее простую структуру. Как известно, по всякому простому числу $p>2$ такие характеры $\chi_p(m)$ совпадают с символами Лежандра $\left(\frac{m}{p}\right)$. Они характеризуются свойствами:

1) $\chi_p(n)$ задано на целых числах 0, ± 1, $\pm 2,\ldots$ и принимает на них значения 0, $+1$ или -1;

2) $\chi_p(n)$ периодично: $\chi_p(n+p)=\chi_p(n)$;

3) $\chi_p(n)$ мультипликативно: $\chi_p(mn)=\chi_p(m)\chi_p(n)$;

4) $\chi_p(n)$ хотя бы при одном n принимает значение -1.

Четыре таких свойства определяют функцию $\chi_p(n)$ как значение символа Лежандра $\left(\frac{m}{p}\right)$. Структура функции $\chi_p(n)$ представляется несложной. Эта функция имеет большое значение в аналитической и алгебраической теории чисел, и потому изучается многими авторами на протяжении более 160 лет. Первые результаты об ее аналитическом поведении при $p\to\infty$ были получены еще К. Ф. Гауссом в 1796 г. С тех пор мы узнали сравнительно немного об аналитических свойствах $\chi_p(n)$. Здесь имеется ряд нерешенных проблем представляющихся весьма трудными. Рассмотрим ряд чисел:

$$\chi_p(1),\ \chi_p(2),\ldots,\chi_p(p-1). \tag{9.3.5}$$

Очевидно, $\chi_p(1)=1$, а далее в этом ряду следуют числа $+1$ или -1. Если $\chi_p(m)=+1$, то, как известно m называется квадратичным вычетом (mod p); если $\chi_p(m)=-1$,

то m — квадратичный невычет (mod p). Если $m = \mu^2 < p$ (m — квадрат), то, очевидно, m — квадратичный вычет. Расстояние между соседними квадратами $\mu^2 < p$ и $(\mu+1^2) < p$ не превосходит $2\sqrt{p}+1$; стало быть, в ряду чисел (9, 3, 5) расстояние между соседними квадратичными вычетами также не превосходит $2\sqrt{p}+1$. Вопрос о расстоянии между соседними квадратичными невычетами весьма труден. И. М. Виноградовым еще более сорока лет назад высказан ряд гипотез о распределении квадратичных характеров, которые мы здесь приведем.

Гипотеза I. *Расстояние между соседними квадратичными невычетами в ряду чисел* (9, 3, 5) *есть* $B_\varepsilon p^\varepsilon$ *при любом* $\varepsilon > 0$ *и* $p \to \infty$.

Другими словами, если $d(p)$ — максимальное расстояние между соседними невычетами в ряду (9,3,5), то при любом заданном $\varepsilon > 0$

$$\lim_{p\to\infty} \frac{d(p)}{p^\varepsilon} = 0. \tag{9,3,6}$$

Особенно интересен для аналитической теории чисел частный случай этой гипотезы — гипотеза о поведении наименьшего квадратичного невычета $N(p)$ в ряду (9, 3, 5)

Гипотеза I'.

$$\lim_{p\to\infty} \frac{N(p)}{p^\varepsilon} = 0 \tag{9,3,7}$$

при любом заданном $\varepsilon > 0$.

Вопрос о наименьшем квадратичном вычете решается тривиально: число 4 есть квадратичный вычет; если 2 и 3 — квадратичные невычеты, то $6 = 2 \cdot 3$ есть квадратичный вычет и т. п. Однако, если мы поставим вопрос о наименьшем простом квадратичном вычете $P(p)$, то такой вопрос весьма труден.

Гипотеза II.

$$\lim_{p\to\infty} \frac{P(p)}{p^\varepsilon} = 0 \tag{9,3,8}$$

при любом заданном $\varepsilon > 0$.

В настоящее время мы еще очень далеки от доказательства этих гипотез; особенно трудной представляется гипотеза I. Одной из основных гипотез современной аналитической тео-

рии чисел является расширенная гипотеза Римана для L-рядов Дирихле. Если эта гипотеза верна, то верны (9, 3, 7) и (9, 3, 8) даже в более сильной форме: $N(p) = B(\lg p)^2$; $P(p) = B(\lg p)^2$, но для гипотезы I существенных продвижений не получается.

Различные теоремы о связи указанных гипотез между собой и с другими гипотезами имеются в работе Ю. В. Линника и А. Реньи [17]. В данном параграфе мы изложим также результаты, полученные для сформулированных гипотез элементарными методами.

Теорема 9. 3. 1.

$$N(p) < \frac{1}{2} + \sqrt{p + \frac{1}{4}}. \tag{9,3,9}$$

Пусть $N(p) = n$. Заметим кстати, что n — простое число: если $n = n_1 n_2$, то $\chi_p(n_1) = -1$, либо $\chi_p(n_2) = -1$; если $n_i \neq n$ или $n_i \neq 1$ $(i = 1, 2)$, получается противоречие. Найдем число $\xi \in (0, n)$ такое, что $p + \xi \equiv 0 \pmod n$. Так как $\xi < n$, то $\chi_p(\xi) = \chi_p(p + \xi) = +1$, так что $\chi_p\left(\frac{p+\xi}{n}\right) = -1$. Но тогда $\frac{p+\xi}{n} \geqslant n$; и подавно $\frac{p}{n} + 1 > n$. Отсюда $n < \frac{1}{2} + \sqrt{p + \frac{1}{4}}$, что и требовалось вывести.

Теорема 9. 3. 2.

$$d(p) < 2\sqrt{p}. \tag{9,3,10}$$

Пусть в ряде (9, 3, 5) между знаками (-1) где-либо имеется просвет длины больше $2\sqrt{p}$.

Пусть u — простое левое число просвета в соответствующем ряду чисел

$$1, 2, \ldots, p - 1. \tag{9,3,11}$$

Тогда имеем: $\chi_p(u + \xi) = +1$ $(\xi = 0, 1, \ldots, H)$, где $H > 2\sqrt{p}$. Рассмотрим числа $N(p)(u + \xi) = nu + n\xi$, где $n = N(p)$ — наименьший квадратичный невычет $\bmod p$. Имеем: $\chi_p(nu + n\xi) = -1$ $(\xi = 0, 1, \ldots, H)$; по теореме (9, 3, 1) $n < 2\sqrt{p}$ $(p > 3)$. Расстояние между соседними числами $nu + n\xi \pmod p$ будет, очевидно, меньше $2\sqrt{p}$, если $H > 2\sqrt{p}$ то в ряду чисел (9. 3, 11) найдутся, таким образом, квадра

тичные невычеты на расстоянии, меньшем $2\sqrt{p}$, что противоречиво. Этим (9, 3, 10) доказано.

Дальнейшее изучение оценки $N(p)$ элементарными средствами требует применения элементов теории распределения простых чисел. В 1926 г. И. М. Виноградов [1] доказал следующую теорему.

Теорема 9. 3. 3 (И. М. Виноградов).

$$N(p) = Bp^{\frac{1}{2\sqrt{e}}} (\lg p)^2, \tag{9,3,12}$$

где e — неперово число.

Для доказательства рассмотрим числа ряда: $1, 2, \ldots, p_1$, где $p_1 = \sqrt{p}\,(\lg p)^2$. Согласно оценке (9,3,2), имеем:

$$\sum_{m \leqslant p_1} \chi_p(m) = B\sqrt{p} \lg p = B\frac{p_1}{\lg p}. \tag{9,3,13}$$

Если $N(p) \leqslant p_1^{\frac{1}{2}}$, то, очевидно, (9,3,12) верно, ибо $p_1^{\frac{1}{2}} = Bp^{\frac{1}{2\sqrt{e}}} (\lg p)^2$. Поэтому можем предполагать, что $N(p) > p_1^{\frac{1}{2}}$. Пусть $m \leqslant p_1$; $\chi_p(m) = -1$. Тогда среди простых делителей m может быть лишь один квадратичный невычет; если бы их было больше, неравенство $N(p) > p_1^{\frac{1}{2}}$ не могло бы выполняться. Итак, если $\chi_p(m) = -1$, то число m имеет вид: $m = p\xi$, где $\chi_p(q) = -1$; $q \geqslant N(p) > p_1^{\frac{1}{2}}$, и $\chi_p(\xi) = +1$. Рассмотрим сумму

$$S = \sum_{\substack{\chi_p(m) = -1 \\ m \leqslant p_1}} 1. \tag{9,3,14}$$

В силу (9,3,13) имеем

$$S = \frac{p_1}{2} + B\frac{p_1}{\lg p}. \tag{9,3,15}$$

С другой стороны, из сказанного выше очевидно, что

$$S \leqslant S_1 = \sum_{\substack{m = q\xi \leqslant p_1 \\ N(p) \leqslant q \leqslant p_1}} 1, \tag{9,3,16}$$

где суммирование идет по простым числам q и положительным числам ξ. Имеем

$$S_1 = \sum_{N(p) \leqslant q \leqslant p_1} \left[\frac{p_1}{q}\right]. \tag{9,3,17}$$

Если мы опустим квадратные скобки в (9,3,17), то общая погрешность не будет превышать $\sum_{q \leqslant p_1} 1$. Согласно сказанному в гл. III, эта погрешность будет иметь оценку $B \frac{p_1}{\lg p_1}$. Таким образом,

$$S_1 = \sum_{N(p) \leqslant q \leqslant p_1} \frac{p_1}{q} + B \frac{p_1}{\lg p_1}. \tag{9,3,18}$$

Далее имеем

$$\sum_{q \leqslant x} \frac{1}{q} = \lg \lg x + C + \frac{B}{\lg x}, \tag{9,3,19}$$

где C — константа. Отсюда

$$S_1 = p_1 \lg \frac{\lg p_1}{\lg N(p)} + \frac{Bp_1}{\lg p}. \tag{9,3,20}$$

Сравнивая с (9,3,15), находим

$$\lg \frac{\lg p_1}{\lg N(p)} \geqslant \frac{1}{2} + \frac{B}{\lg p_1}, \tag{9,3,21}$$

$$\frac{\lg p_1}{\lg N(p)} \geqslant e^{\frac{1}{2}} + \frac{B}{\lg p_1}, \tag{9,3,22}$$

$$\lg N(p) \leqslant \frac{\lg p_1}{\sqrt{e}} + B. \tag{9,3,23}$$

Отсюда, согласно определению числа p_1, вытекает (9,3,12). Сделаем еще замечание, важное для дальнейшего. Если внимательно проследить за доказательством теоремы 9. 3. 3, то видно, что здесь существенно не то, что $p_1 = \sqrt{p}\ (\lg p)^2$, а лишь то, что $\sum_{m \leqslant p_1} \gamma_p(m) = B \frac{p_1}{\lg p}$. Если такая оценка верна для какого-либо значения $p_1 = p_1(p)$, то предыдущие рассуждения показывают, что верна и оценка (9, 3, 23).

Применение современной теории простых чисел, в частности теоремы о наименьшем простом числе в прогрессии, данной одним из авторов, позволяет дать сведения о возможных больших значениях $N(p)$. Так Г. Салие [44] и В. Р. Фридлендер [24] доказали, что существует бесконечно много простых чисел p, для которых $N(p) > C_0 \lg p$. С другой стороны, числа, где $N(p) > p^{\varepsilon}$ при данном $\varepsilon > 0$, если и существуют, то редки. Назовем ε-исключительными простые числа p, для которых $N(p) > p^{\varepsilon}$. Ю. В. Линник [11] доказал, что при достаточно большом N на сегменте $[N^{\varepsilon}, N]$ число таких чисел не превосходит константы: $C(\varepsilon) = 320\pi (g + 2)^g g!$, где $g = \left[\frac{2}{\varepsilon^2} + 1\right]$. В. Р. Фридлендер [24] улучшил эту оценку.

Отметим еще любопытный факт: для доказательства гипотезы I' $N(p) = B_\varepsilon p^{\varepsilon}$ достаточно доказать, что $\sum\limits_{xy \leqslant N} \chi_p(xy) = B_\varepsilon p^{\frac{1}{2}+\varepsilon}$, если N — любое число сегмента $\left[\frac{p}{\lg^2 p}, p \lg^2 p\right]$.

§ 4. Элементарные выводы из неэлементарной теоремы

Вернемся к ряду чисел (9,3,5). Они образуют последовательность знаков $+$ и $-$. Пусть s — заданное число, а $p \to \infty$. Можно образовать 2^s различных последовательностей знаков $+$ или $-$ длины s, и поставить вопрос, все ли такие последовательности будут встречаться в ряду (9,3,5) при $p \to \infty$, и как часто это будет происходить. Этот вопрос изучался Г. Дэйвенпортом [36], [37] в начале тридцатых годов. Г. Дэйвенпорт разработал аналитический метод для решения данного вопроса. При этом возник ряд вопросов алгебраической теории чисел. Изучение этих вопросов в руках Г. Хассе дало новое направление алгебраической и аналитической теории чисел — изучение гипотез Римана для дзета-функций над конечными полями. Это направление бурно развивается в настоящее время, и в 1958 г. впервые привело к продвижению в гипотезах I и I'. Прежде чем затронуть эти вопросы, приведем одно элементарное рассуждение об указанных ранее последовательностях длины s, принадлежащее А. Брауэру.

Ван дер Варден доказал элементарными средствами следующую теорему (см. [28]).

Теорема 9.4.1 (Ван дер Варден). *Пусть ряд последовательных чисел, например ряд* (9,3,11) *разбит на два непересекающихся множества. Если* r *— заданное число, и* $p > p_0(r)$, *то хотя бы в одном из этих множеств можно выделить числа, лежащие в арифметической прогрессии длины* r: $a\xi + b$; $\xi = 0,1,\ldots,r-1$.

Мы не будем приводить здесь доказательства этой теоремы, отсылая читателя к простому доказательству М. А. Лукомской [28], и выведем здесь лишь следствие ее, указанное А. Брауэром. Пусть задано число s; выберем $p > p_0(s)$ так, чтобы была применима теорема Ван дер Вардена, и в качестве разбиения ряда (9, 3, 11) рассмотрим его разбиение на квадратичные вычеты и невычеты соответственно ряду (9,3,5). Возьмем прогрессию $a\xi + b$ ($\xi = 0,1,\ldots,s-1$) теоремы 9.4.1. Имеем

$$\chi_p(a\xi + b) = \eta_0 \qquad (\xi = 0,1,\ldots,s-1),$$

где η_0 — одно и то же число $+1$ или -1.

Отсюда имеем

$$\chi_p(\xi + ba') = \eta_0\,\chi_p(a) \qquad (\xi = 0,1,\ldots,s-1;\ aa' \equiv 1 \pmod p).$$

Здесь число справа равно $+1$ или -1 для всех значений ξ. Таким образом, справедлива

Теорема 9.4.2. *При заданном* s *и* $p > p_0(s)$ *в ряду чисел* (9, 3, 11) *всегда найдется последовательность из не менее* s *рядом стоящих квадратичных вычетов или невычетов.*

Мы сформулируем теперь неэлементарную теорему, приводящую к гораздо более сильным результатам.

Пусть $P_r(x) = x^r + a_1x^{r-1} + \ldots + a_r$ — целочисленный полином, коэффициенты которого берутся по модулю p. Рассмотрим «кривую по модулю p»:

$$y^2 - P_r(x) \equiv 0 \pmod p. \qquad (9,4,1)$$

Допустим, что эта кривая неприводима по модулю p, т. е. $P_r(x) \not\equiv (Q(x))^2 \pmod p$. Будем рассматривать целые точки по модулю p, лежащие на кривой (9,4,1), т. е. такие пары целых чисел (x, y), для которых (9,4,1) превращается в тождество. Различными среди них будем считать, разумеется, несравнимые между собой (mod p).

В 1941 г. А. Вейль [51], развивая идеи Г. Хассе и М. Дейринга, путем весьма глубоких и неэлементарных алгебраических соображений пришел к доказательству «гипотезы Римана для кривых по модулю p». Для неприводимой кривой вида (9,4,1) (такая кривая называется эллиптической при $3 \leqslant r \leqslant 4$ и гиперэллиптической при $r > 4$) из результатов А. Вейля следует теорема.

Теорема 9.4.3 (А. Вейль). *Число различных целых точек по модулю p на неприводимой* (mod p) *кривой*(9,4,1) *равно*

$$p + 1 + R(p), \tag{9,4,2}$$

где

$$|R(p)| < r\sqrt{p}. \tag{9,4,3}$$

Мы приведем здесь элементарно выводимые интересные следствия из неэлементарной теоремы 9. 4. 3.

Пусть точка (x, y), рассматриваемая по модулю p, лежит на кривой (9, 4, 1). Тогда либо $P_r(x) \equiv 0 \pmod p$, $y \equiv 0 \pmod p$, либо $P_r(x) \not\equiv 0 \pmod p$; $\chi_p(P_r(x)) = +1$. Решений (x, y) первого типа будет не более r, так как по теореме Лагранжа сравнение $P_r(x) \equiv 0 \pmod p$ имеет не более r корней. Для каждого x такого, что $\chi_p(P_r(x)) = +1$, найдутся два решения: $+y$ и $-y$ (mod p). Обозначим

$$S_+ = \sum_{\chi_p(P_r(x))=+1} 1, \qquad S_- = \sum_{\chi_p(P_r(x))=-1} 1.$$

Тогда

$$S_+ - S_- = \sum_{x=0}^{p-1} \chi_p(P_r(x)),$$

$$S_+ + S_- = p + \theta r \qquad (|\theta| \leqslant 1).$$

Отсюда

$$S_+ = \frac{p}{2} + \frac{1}{2} \sum_{x=0}^{p-1} \chi_p(P_r(x)) + \theta \frac{r}{2}. \tag{9,4,4}$$

Ввиду сказанного выше, сравнивая (9,4,4) с (9,4,2) и (9,4,3), находим

$$\left|\sum_{x=0}^{p-1} \chi_p(P_r(x))\right| \leqslant 2r\sqrt{p}. \tag{9,4,5}$$

Эта глубокая оценка, как уже было сказано, выводится неэлементарными средствами. Только для случая $r=3$ (эллиптические кривые) подобную оценку в 1956 г. удалось вывести элементарными средствами Ю. И. Манину [18] (см. гл. 10).

Обратимся к следствиям оценки (9, 4, 5). Прежде всего, следуя Г. Дэйвенпорту [36], [37], применим оценку (9, 4, 5) к вопросу о распределении предписанных последовательностей квадратичных вычетов длины s *).

Пусть $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_s$ — заданная последовательность знаков ± 1. Составим выражение

$$\Pi_s(x) = \frac{1}{2^s}(1+\varepsilon_1\chi_p(x))(1+\varepsilon_1\chi_p(x+1))\ldots \\ \ldots(1+\varepsilon_s\chi_p(x+s-1)).$$

Очевидно, $\Pi_s(x)=1$, если числа $\chi_p(x), \chi_p(x+1), \ldots, \chi_p(x+s)$ образуют нужную нам последовательность $\varepsilon_1, \ldots, \varepsilon_s$; $\Pi_s(x)=0$, если это не так. Таким образом,

$$N_s = \sum_{x=0}^{p-1} \Pi_s(x) \qquad (9,4,6)$$

доставляет число последовательностей $\varepsilon_1, \ldots, \varepsilon_s$ на сегменте $[0, p-1]$ с погрешностью, не превышающей числа s; при этом, как видно из формулы (9, 4, 6), допускаются частичные налегания одной последовательности на другую.

Выражение $\Pi_s(x)$ состоит из числа $\frac{1}{2^s}$ и 2^s-1 выражений вида $\frac{1}{2^s}\varepsilon_{\alpha_1}\ldots\varepsilon_{\alpha_t}\chi_p(\Phi(x))$, где $\Phi(x)=(x+\alpha_1)\ldots(x+\alpha_t)$. При достаточно большом p кривые $y^2=\Phi(x)$ будут все неприводимы (mod p), так что в силу (9,4,5) получим

$$|\sum\chi_p(\Phi(x))| \leqslant 2s\sqrt{p}. \qquad (9,4,7)$$

Учитывая это, получаем из (9, 4, 6)

$$N_s = \frac{p}{2^s} + 2\theta\, s\sqrt{p} \qquad (|\theta|\leqslant 1). \qquad (9,4,8)$$

---

*) Работы Г. Дэйвенпорт [36], [37] относились к тому времени, когда оценки А. Вейля еще не были получены. Здесь мы следуем дипломной работе студ. ЛГУ Б. З. Мороз [21].

Пусть

$$2^s \leqslant \frac{\sqrt{p}}{\lg^2 p}. \qquad (9,4,9)$$

Тогда (9, 4, 8) дает

$$N_s = \frac{p}{2^s} + 2\theta \frac{1}{\lg p} \frac{p}{2^s} \qquad (p > p_0). \qquad (9,4,10)$$

Отсюда получаем теорему

Теорема 9.4.4. *Если* $2^s \leqslant \frac{\sqrt{p}}{\lg^2 p}$ $(p > p_0)$, *то всегда найдется предписанная последовательность* $\varepsilon_1, \ldots, \varepsilon_s$ *знаков* $+1$ *или* -1, *отвечающая вычетам или невычетам* mod p *среди чисел* $1, 2, \ldots, p-1$. *Число таких последовательностей, считаемое, как было указано ранее, выражается асимптотической формулой* (9,4,10).

Эта теорема, как мы видим, значительно сильнее теоремы 9.4.2, но последняя допускает элементарное доказательство.

Весьма замечательные следствия из оценки (9,4,7) были получены в 1958 г. Д. Берджессом [34]. Они явились первым заметным сдвигом в исследовании гипотез I и I′ § 3 со времени работы И. М. Виноградова 1926 г. о наименьшем квадратичном невычете, о которой говорилось в § 3. Сформулируем две теоремы Д. Берджесса.

Теорема 9.4.5 (Д. Берджесс). *Для сколь угодно малой константы* $\delta > 0$ $d(p) = B_\delta p^{\frac{1}{4}+\delta}$. Точнее: *если* $\delta > 0$, $\varepsilon > 0$ — *заданные сколь угодно малые константы, то при* $p > p_0$ (ε, δ) *и любом* N *имеем неравенство*

$$\left| \sum_{n=N+1}^{N+H} \left(\frac{n}{p}\right) \right| < \varepsilon H, \qquad (9,4,11)$$

если $H > p^{\frac{1}{4}+\delta}$.

Отсюда легко выводится теорема.

Теорема 9.4.6 (Д. Берджесс). *При любом фиксированном* $\delta > 0$

$$N(p) = B_\delta p^{\frac{1}{4\sqrt{e}}+\delta}. \qquad (9,4,12)$$

Мы видим, что (9,4,12) есть значительное усиление оценки (9,3,9), грубо говоря, из этой оценки извлекается квадратный корень.

Переходим к выводу теоремы 9.4.5 из оценки (9,4,5). Он основан на нескольких несложных леммах.

Лемма 1. *Пусть r — натуральное число, p — простое число; h — целое число из интервала $(0, p)$. Положим*

$$S_h(x) = \sum_{m=1}^{h} \left(\frac{x+m}{p} \right) \tag{9,4,13}$$

(мы полагаем $\left(\frac{s}{p}\right) = 0$, если $s \equiv 0 \pmod p$). Тогда

$$\sum_{x=0}^{p-1} (S_h(x))^{2r} < (2r)^r p h^r + 4r \sqrt{p}\, h^{2r}. \tag{9,4,14}$$

Имеем

$$\sum_{x=0}^{p-1} (S_h(x))^{2r} = \sum_{m_1,\dots,m_{2r}=1}^{h} \sum_{x=0}^{p-1} \left(\frac{(x+m_1)\dots(x+m_{2r})}{p} \right).$$

Системы величин $m_1, \dots, m_{2r}$ разобьем на два класса. Первый класс будет состоять из систем величин, где не более r различных величин, и каждая встречается четное число раз; остальные системы величин составят второй класс. Число систем первого класса, очевидно, не превосходит $(2r)^r h^r$, и для каждой системы внутренняя сумма по x не превосходит p, так что полная сумма для таких систем не превосходит $(2r)^r p h^r$. Число систем второго класса, очевидно, не превосходит h^{2r}, для каждой из них внутренняя сумма имеет вид

$$\sum_{x=0}^{p-1} \left(\frac{(x+n_1)^{e_1} \dots (x+n_s)^{e_s}}{p} \right),$$

где $s \leqslant 2r$; $n_1, n_2, \dots, n_s$ попарно несравнимые (mod p); $e_1, e_2, \dots, e_s$ не все четные. Можно выбросить те множители, для которых e_j четно и $x + n_j \not\equiv 0 \pmod p$; число значений x, где $x + n_j \equiv 0 \pmod p$, не превосходит $2r$, так что наша сумма отличается не более чем на $2r$ от суммы

$$S = \sum_{x} \left(\frac{(x+u_1)\dots(x+u_k)}{p} \right),$$

где $1 \leqslant K \leqslant 2r$, $u_1, \ldots, u_k$ попарно несравнимы (mod p). Кривая $y^2 = (x+u_1)\ldots(x+u_k)$ неприводима (mod p), если k нечетно; в этом случае, согласно оценке (9,4,5),

$$|S| < 2u\sqrt{p} < 4r\sqrt{p}.$$

Эта оценка справедлива и в том случае, когда k четно. Именно, определим y из условия

$$(x+u_1)y \equiv 1 \pmod{p}.$$

Тогда сумма S преобразуется в аналогичную сумму $k-1$ переменной вместо k, из которой нужно вычесть 1, так как $y \equiv 0$ не соответствует ни одно значение x. Ввиду этого при четном k имеем

$$|S| \leqslant 1 + 2(k-1)\sqrt{p} < 4r\sqrt{p}.$$

Из этих результатов выводим (9,4,14).

Пусть даны целые числа $H > 0$, $q > 0$, t, N. Определим отрезок $I(q, t)$:

$$\frac{N+tp}{q} < z \leqslant \frac{N+H+tp}{q}. \tag{9,4,15}$$

Лемма 2. *Пусть q пробегает ряд различных положительных целых чисел в количестве Q, таких, что каждое из них лежит в интервале*

$$(q_1, q_2) \tag{9,4,16}$$

и все они взаимно просты. Пусть

$$2Hq_2 < p. \tag{9,4,17}$$

Тогда (при данных p, N, H) можно для каждого q построить ряд $T(q)$ целых чисел t $(0 \leqslant t < q)$ в количестве $q = Q$ и таким образом, что интервалы $I(q, t)$ для всех q и всех t в $T(q)$ не пересекаются.

Для доказательства заметим, что два интервала (9,4,15) с одинаковыми q и разными t всегда различны, ибо $0 < H < p$. Пусть интервалы $I(q, t)$ и $I(q', t')$ имеют общую точку и $q > q'$. Тогда

$$\frac{N+tp}{q} < \frac{N+H+t'p}{q'} \quad \text{и} \quad \frac{N+t'p}{q} < \frac{N+H+tp}{q}$$

и

$$p(tq' - t'q) + N(q' - q) < Hq,$$
$$p(tq' - t'q) + N(q' - q) > -Hq'.$$

Используя (9,4,17) находим

$$|p(tq'-t'q)+N(q'-q)|<Hq<\frac{p}{2}.$$

Отсюда непосредственно следует, что существует не больше одной пары t, t' для пересекающихся интервалов. Ряд $T(q)$ можно теперь построить для каждого q путем исключения из ряда $0\leqslant t<q$ всех тех величин t, которые входят хотя бы в одну пару t, t', соответствующую $q\neq q'$. Количество величин t, исключенных таким образом, не превосходит $Q-1$, следовательно, мы можем построить ряды $T(q)$ такие, что каждый из них включает $q-Q$ чисел t.

Переходим к доказательству теоремы 9.4.5. Достаточно рассмотреть значение H под условиями

$$p^{\frac{1}{4}+\delta}<H<p^{\frac{1}{2}+\delta}, \tag{9,4,18}$$

ибо при $H>p^{\frac{1}{2}+\delta}$ требуемое неравенство следует из (9,3,1). Допустим, что для некоторого N, и H под условиями (9,4,18) имеем

$$\left|\sum_{n=N+1}^{N+H}\left(\frac{n}{p}\right)\right|\geqslant \varepsilon H. \tag{9,4,19}$$

Покажем, что это предположение приводит к противоречию для достаточно большого p. Для какого-либо положительного $q<p$ имеем

$$\sum_{n=N+1}^{N+H}\left(\frac{n}{p}\right)=\sum_{z=0}^{q-1}\sum_{\substack{n=N+1\\ n\equiv -tp \pmod q}}^{N+H}\left(\frac{n}{p}\right).$$

Полагая во внутренней сумме $n\equiv -tp+qz$, замечаем, что z изменяется в сегменте

$$\left[\frac{N+1+tp}{q},\ \frac{N+H+tp}{q}\right]$$

и пробегает целые числа отрезка (9,4,15). Далее,

$$\left(\frac{n}{p}\right)=\left(\frac{qz}{p}\right)=\left(\frac{q}{p}\right)\left(\frac{z}{p}\right),$$

так что из (9,4,19) выводим

$$\sum_{t=0}^{q-1}\left|\sum_{z\in I(q,\,t)}\left(\frac{z}{p}\right)\right|\geqslant \varepsilon H. \tag{9,4,20}$$

Применим лемму 2, причем q будут пробегать простые числа интервала $\left(\frac{1}{2}p^{\frac{1}{4}}, p^{\frac{1}{4}}\right)$. Условие (9, 4, 17) выполнится в силу (9,4,18). Число целых q, обозначенное через Q, равно

$$Q=\pi(p^{\frac{1}{4}})-\pi\left(\frac{1}{2}p^{\frac{1}{4}}\right). \tag{9,4,21}$$

Суммируя (9,4,20) по всем простым q, найдем

$$\varepsilon HQ\leqslant\sum_{q}\sum_{t=0}^{q-1}\left|\sum_{z\in I(q,\,t)}\left(\frac{z}{p}\right)\right|\leqslant$$

$$\leqslant\sum_{q}\sum_{t\in T(q)}\left|\sum_{z\in I(q,\,t)}\left(\frac{z}{p}\right)\right|+\sum_{q}Q\,2H\,q^{-1},$$

так как число целых z в $I(q, t)$ меньше $2Hq^{-1}$, и все величины t, кроме Q, принадлежат $T(q)$. Далее, $\sum q^{-1}<$ $<2p^{-\frac{1}{4}}Q$ в силу неравенств для q. Поэтому мы имеем

$$\sum_{q}\sum_{t\in T(q)}\left|\sum_{z\in I(q,\,t)}\left(\frac{z}{p}\right)\right|>HQ(\varepsilon-4p^{-1/4}Q)>\frac{\varepsilon HQ}{2}$$

при достаточно больших q (имеем $Q=o(p^{\frac{1}{4}})$ (см. гл. 3). Пусть I означает какой-либо из наших интервалов $I(q, t)$. Все такие интервалы не пересекаются по лемме 2; число их не превосходит

$$\sum_{q}(q-Q)<p^{\frac{1}{4}}Q. \tag{9,4,22}$$

Ранее сформулированный результат перепишем в виде

$$\sum_{I}\left|\sum_{z\in I}\left(\frac{z}{p}\right)\right|>\frac{\varepsilon HQ}{2}. \tag{9,4,23}$$

Для любого целого $h>0$ имеем

$$\sum_{z\in I}\left(\frac{z}{p}\right)=h^{-1}\sum_{m=1}^{h}\sum_{n\in I}\left(\frac{n}{p}\right)=$$

$$=h^{-1}\sum_{m=1}^{h}\left\{\sum_{n\in I}\left(\frac{n+m}{p}\right)+\varphi_m\right\}\quad(|\varphi_m|\leqslant 2m).$$

Отсюда

$$\sum_{z\in I}\sum_{m=1}^{h}\left(\frac{n+m}{p}\right)=h\sum_{z\in I}\left(\frac{z}{p}\right)-\sum_{m=1}^{h}\varphi_m.$$

Следовательно,

$$\sum_{n\in I}|S_h(n)|\geqslant h\left|\sum_{z\in I}\left(\frac{z}{p}\right)\right|-2h^2.$$

Теперь суммируем по всем I и используем оценку (9,4,22) для числа интервалов I. Тогда из (9,4,23) получим

$$\sum_{I}\sum_{n\in I}|S_h(n)|>\frac{\varepsilon HQh}{2}-2p^{\frac{1}{4}}Qh^2.$$

Положим

$$h=\left[\frac{1}{8}\varepsilon Hp^{-\frac{1}{4}}\right].\qquad(9,4,24)$$

Тогда получим неравенство

$$\sum_{I}\sum_{n\in I}|S_h(n)|>\frac{1}{4}\varepsilon HQh.$$

Применим неравенство Гельдера (см. [2]). Получим

$$\sum_{I}\sum_{n\in I}|S_h(n)|\leqslant\left\{\sum_{I}\sum_{n\in I}1\right\}^{1-\frac{1}{2r}}\left\{\sum_{I}\sum_{n\in I}|S_h(n)|^{2r}\right\}^{\frac{1}{2r}}$$

и, следовательно,

$$\sum_{I}\sum_{n\in I}|S_h(n)|^{2r}>\left(\frac{\varepsilon HQh}{4}\right)^{2r}(p^{\frac{1}{4}}Q3p^{-\frac{1}{4}}H)^{1-2r}$$

(при этом учтено, что количество целых чисел в интервале I не превосходит $3p^{-\frac{1}{4}}H$). Так как наши интервалы не пересекаются, можем написать

$$\sum_{x} |S_h(x)|^{2r} > \left(\frac{1}{12}\varepsilon\right)^{2r} HQh^{2r}.$$

Сопоставляя с результатом леммы 1, находим

$$\left(\frac{1}{12}\varepsilon\right)^{2r} HQh^{2r} < (2r)^r ph^r + 4r\sqrt{p}\, h^{2r}. \qquad (9.4.25)$$

По закону простых чисел (см. гл. 3) имеем

$$Q > c_1 \frac{p^{\frac{1}{4}}}{\lg p}.$$

Положим теперь $r > \frac{1}{\delta}$; мы имеем: $h > \frac{1}{9}\varepsilon p^{\delta}$. Далее $H > p^{\frac{1}{4}+\delta}$. Ввиду этого, при достаточно большом p левая часть (9,4,25) становится больше правой, и мы имеем противоречие. Это доказывает теорему 9.4.5. Нетрудно видеть, что, помимо основной оценки (9,4,5), здесь используется в усиленной форме рассуждение, приведшее к теореме 9.4.2.

Теорема 9. 4. 6 о наименьшем квадратичном невычете выводится из нее на основании таких же рассуждений, как теорема 9.3.3 выводится из оценки (9,3,13) (см. замечания после вывода формулы (9,3,23)).

ГЛАВА 10

ЭЛЕМЕНТАРНОЕ ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ ХАССЕ

§ 1. Постановка задачи

Пусть $p > 3$ — любое простое число, a, b — целые числа. Обозначим буквой N количество решений сравнения

$$y^2 \equiv x^3 + ax + b \pmod{p} \qquad (10,1,1)$$

(считая два целочисленных решения (x_1, y_1) и (x_2, y_2) одинаковыми, если $x_1 \equiv x_2 \pmod{p}$, $y_1 \equiv y_2 \pmod{p}$). Отметим прежде всего, что к сравнению (10,1,1) легко сводится общее сравнение вида

$$v^2 \equiv a_3u^3 + a_2u^2 + a_1u + a_0 \pmod{p}, \qquad (10,1,2)$$

где $a_3 \not\equiv 0 \pmod{p}$. В самом деле, умножим обе части сравнения (10,1,2) на a_3^2 и положим $y = a_3v$, $x = a_3u + a'$, где $3a' \equiv a_2 \pmod{p}$. Новые неизвестные x, y окажутся связанными сравнением вида (10,1,1).

Если дискриминант $4a^3 + 27b^2$ многочлена $x^3 + ax + b$ делится на p, то подсчитать число N нетрудно. В самом деле, тогда сравнение $x^3 + ax + b \equiv 0 \pmod{p}$ имеет по крайней мере двукратный корень, так что существуют такие целые числа x_0 и x_1, что $x^3 + ax + b \equiv (x - x_0)^2(x - x_1) \pmod{p}$. Отсюда следует, что при $x \not\equiv x_0 \pmod{p}$ сравнение (10,1,1) равносильно сравнению $y^2 \equiv x - x_1 \pmod{p}$, которое, очевидно, имеет (за исключением $x \equiv x_0 \pmod{p}$) p решений, если $\left(\frac{x_0 - x_1}{p}\right) = -1$; $p - 2$ решения, если $\left(\frac{x_0 - x_1}{p}\right) = 1$, и, наконец, $p - 1$ решение, если $x_0 \equiv x_1 \pmod{p}$. Соответственно этим трем возможностям получаем $N = p + 1$, $p - 1$ или p.

Остается, следовательно, разобрать случай, когда $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$. Этот случай гораздо труднее и вместо

точного результата мы сможем получить два числа N лишь асимптотическую оценку с главным членом p и остаточным членом порядка $\sqrt{p}$. Точная формулировка такова:

Теорема 10.1.1. *Число решений N сравнения* (10,1,1) *при условии, что* $4a^3+27b^2\not\equiv 0 \pmod p$, *удовлетворяет неравенству*

$$|N-p|<2\sqrt{p}. \tag{10,1,3}$$

(Разумеется, случай $4a^3+27b^2\equiv 0 \pmod p$ можно было бы не исключать, так как согласно проведенному подсчету, тогда $|N-p|=0$ или 1 и, очевидно, $1<2\sqrt{p}$ при любом p.)

Неравенство (10,1,3) представляет собой впервые доказанный Хассе [35] частный случай общего результата А. Вейля относительно числа решений сравнения $F(x, y)\equiv 0 \pmod p$, где F — любой многочлен от двух неизвестных с целыми коэффициентами.

Отметим еще, что оценка (10,1,3) является наилучшей возможной: можно доказать, что при $a=-1$, $b=0$ и $p\to\infty$ отношение $\frac{|N-p|}{2\sqrt{p}}$ подходит сколь угодно близко к единице (см. [27]).

§ 2. Сложение решений

Прежде чем доказывать теорему, нам придется проделать некоторую подготовительную работу. Мы будем рассматривать многочлены и рациональные функции от некоторой фиксированной раз навсегда неизвестной x, причем в качестве коэффициентов этих многочленов будут фигурировать классы вычетов по модулю p. В соответствии с этим соглашением ниже мы будем всюду писать равенства вместо сравнений. В частности, равенство двух многочленов $P_1(x)$ и $P_2(x)$ означает, что коэффициенты при одних и тех же степенях неизвестной x в этих многочленах представляют собой один и тот же класс вычетов $(\mathrm{mod}\, p)$, а равенство двух рациональных функций $\frac{P_1(x)}{Q_1(x)}$ и $\frac{P_2(x)}{Q_2(x)}$ означает равенство многочленов $P_1(x)Q_2(x)$ и $P_2(x)Q_1(x)$. Буквами a, b (в отличие от соглашения, принятого в предыдущем пункте) мы обозначаем теперь некоторые классы вычетов $(\mathrm{mod}\, p)$, удовлетворяющие соотношению $4a^3+27b^2\neq 0$.

Наша цель по-прежнему состоит в оценке числа решений N уравнения (10,1,1), но в ходе доказательства важнейшую роль будет играть несколько видоизмененное уравнение

$$Y^2 = \frac{X^3 + aX + b}{x^3 + ax + b}. \qquad (10,2,1)$$

решения которого (X, Y) мы ищем в области рациональных функций от неизвестной x (с коэффициентами описанного вида).

Займемся уравнением (10,2,1) внимательнее. Прежде всего, оно имеет очевидное решение $X = x$, $Y = \pm 1$. Менее очевидно и весьма важно для дальнейшего другое решение: $X = x^p$, $Y = \pm (x^3 + ax + b)^{\frac{p-1}{2}}$ (достаточно заметить, что $(x^3 + ax + b)^p = x^{3p} + ax^p + b$, потому что биномиальные коэффициенты $\frac{p!}{i!j!k!}$ $(i + j + k = p)$ при $ijk \not\equiv 0 \pmod p$ делятся на p).

Существует простой способ находить некоторое третье решение уравнения (10,2,1), если два решения уже известны. Этот способ удобно описывать геометрическим языком, рассматривая уравнение (10,2,1) как «кривую» с текущими координатами X, Y (неизвестная x играет роль параметра, от которого зависят коэффициенты уравнения кривой). Рассмотрим пару точек на этой кривой (X_1, Y_1) и (X_2, Y_2) и проведем через эту пару точек прямую с текущими координатами X, Y:

$$\frac{X - X_1}{X_2 - X_1} = \frac{Y - Y_1}{Y_2 - Y_1}. \qquad (10,2,2)$$

Для того чтобы уравнение (10,2,2) имело смысл, предположим временно, что $X_2 \neq X_1$ (то есть что выбранные точки не совпадают). Прямая (10, 2, 2) пересекается с кривой (10,2,1) в трех точках, две из которых — (X_1, Y_1) и (X_2, Y_2) — известны. Для отыскания третьей точки выразим Y через X из уравнения (10,2,2) и подставим результат в уравнение (10,2,1):

$$X^3 + aX + b - \left(\frac{Y_2 - Y_1}{X_2 - X_1}(X - X_1) + Y_1\right)^2 (x^3 + ax + b) = 0.$$

Два корня X_1 и X_2 этого кубического относительно X уравнения известны; коэффициент при X^2 в левой части, преди-

ставляющий собой сумму всех трех корней с обратным знаком, равен

$$-\left(\frac{Y_2-Y_1}{X_2-X_1}\right)^2 (x^3+ax+b).$$

Отсюда находится третий корень:

$$X_3=-X_1-X_2+\left(\frac{Y_2-Y_1}{X_2-X_1}\right)^2 (x^3+ax+b). \quad (10,2,3)$$

Подставляя это значение в уравнение прямой (10,2,2), найдем вторую координату искомой точки пересечения:

$$Y_3=\frac{Y_2-Y_1}{X_2-X_1}(X_3-X_1)+Y_1. \quad (10,2,4)$$

Вместе с точкой (X_3, Y_3) на кривой (10,2,1) лежит и симметричная ей точка $(X_3, -Y_3)$; именно ее мы и будем считать окончательным результатом описанной операции над точками (X_1, Y_1) и (X_2, Y_2).

Эта операция обозначается символом $+$ и называется «сложением» точек кривой (10,2,1) или, что все равно, решений уравнения (10,2,1). Таким образом, мы пишем

$$(X_1, Y_1)+(X_2, Y_2)=(X_3, -Y_3), \quad (10,2,5)$$

если величины X_3, Y_3 выражаются через координаты заданных двух точек по формулам (10, 2, 3), (10, 2, 4).

Остается еще разобрать случай вырождения: $X_1=X_2$. Если при этом $Y_1\neq Y_2$, то проходящая через точки (X_1, Y_1) и $(X_1, -Y_1)$ прямая $X-X_1=0$ пересекается с кривой (10,2,1) еще в несобственной, бесконечно удаленной точке, которая совпадает с симметричной к ней. Мы не станем придавать этой фразе точный смысл и в дальнейшем обойдем возможность появления в нашей конструкции такого «решения» уравнения (10,2,1) с помощью некоторого формального приема.

Наконец, если $X_1=X_2$, $Y_1=Y_2$, то, как подсказывает геометрическое истолкование формул (10, 2, 3) и (10, 2, 4), вместо уравнения (10,2,2,) следует написать уравнение «касательной» к кривой (10,2,1) в точке (X_1, Y_1)

$$Y-Y_1=\frac{3X_1^2+a}{2Y_1(x^3+ax+b)}(X-X_1), \quad (10,2,6)$$

а затем решить это уравнение совместно с уравнением (10,2,1). Окончательно получаем

$$X_3 = -2X_1 + \frac{(3X_1^2 + a)^2}{4(X_1^3 + aX_1 + b)}. \qquad (10,2,7)$$

Вторая координата Y_3 точки пересечения получится, если подставить это значение вместо X в формулу (10,2,1); напомним еще раз, что для получения удвоенной точки (X_1, Y_1) следует вместо точки (X_2, Y_2) взять симметричную к ней точку $(X_2, -Y_2)$.

Определенное формулами (10,2,3); (10,2,4); (10,2,6); (10,2,7) сложение точек кривой (10,2,1) в действительности удовлетворяет всем аксиомам групповой операции. Оно коммутативно: это следует прямо из определения. Оно также обладает нулем — им служит бесконечно удаленная точка. Наконец, оно ассоциативно. Но *два последние свойства* нам ни разу не понадобятся, и мы не станем их проверять, тем более, что непосредственная проверка ассоциативности по формулам сложения приводит к довольно громоздким выкладкам. В дальнейшем нам придется пользоваться только следующим фактом: равенство (10,2,5) равносильно равенству

$$(X_1, Y_1) + (X_3, Y_3) = (X_2, -Y_2). \qquad (10,2,8)$$

Геометрическое истолкование подсказывает, как проверить это утверждение без всяких выкладок: через точки (X_3, Y_3) и $(X_3, -Y_3)$ проходит та же прямая, что и через точки (X_1, Y_1) и (X_2, Y_2), а роль третьей точки пересечения теперь играет точка (X_2, Y_2).

§ 3. Основная конструкция

Мы прекращаем теперь говорить о точках кривой и снова будем называть пару (X, Y) рациональных функций от неизвестной x, удовлетворяющих уравнению (10,2,1), решением этого уравнения. Два частных решения мы указали в начале предыдущего пункта. Теперь с помощью только что определенной операции сложения мы построим из этих двух решений бесконечную в обе стороны последовательность

решений, которая представляет собой как бы арифметическую прогрессию с разностью $(x, 1)$ и начальным членом $(x^p, (x^3+ax+b)^{\frac{p-1}{2}})$. Именно, мы положим

$$(X_0, Y_0)=(x^p, (x^3+ax+b)^{\frac{p-1}{2}}) \qquad (10,3,1)$$

и если решение (X_n, Y_n) уже определено,

$$(X_{n+1}, Y_{n+1})=(X_n, Y_n)+(x, 1), \qquad (10,3,2)$$

$$(X_{n-1}, Y_{n-1})=(X_n, Y_n)+(x, -1). \qquad (10,3,3)$$

(Ясно, что формулой (10,3,2) следует пользоваться для продолжения последовательности вправо с любого места, а формулой (10,3,3) — для продолжения влево.) Если для какого-то номера n в ходе построения последовательности окажется, что $(X_n, Y_n)=(x, -1)$, то вместо решения (X_{n+1}, Y_{n+1}) оставим в последовательности пробел и положим $(X_{n+2}, Y_{n+2})=(x, 1)$. Подобным же образом, если при продолжении влево мы дойдем до решения $(X_n, Y_n)=(x, 1)$, то вместо решения (X_{n-1}, Y_{n-1}) оставим пробел и положим $(X_{n-2}, Y_{n-2})=(x, -1)$. Очевидно, эти соглашения однозначно определяют некоторую последовательность решений уравнения (10,2,1), возможно, с пробелами.

Для всякого номера n, для которого решение (X_n, Y_n) определено, представим X_n в виде несократимого отношения $\frac{P_n}{Q_n}$ двух многочленов от неизвестной x. Мы определим это отношение однозначно, потребовав, чтобы старший коэффициент многочлена P_n был равен единице.

Введем, наконец, бесконечную в обе стороны последовательность неотрицательных целых чисел, полагая

$$d_n=\begin{cases}0, \text{ если функция } X_n \text{ не определена,}\\ \text{степени многочлена } P_n \text{ в остальных случаях.}\end{cases}$$

Теперь мы уже в состоянии выяснить связь описанной конструкции с поставленной первоначально задачей оценки числа N решений сравнения (10,1,1). Первый шаг в этом направлении составляет следующая

Лемма 1.

$$d_{-1}-d_0-1=N_p-p.$$

Согласно формуле (10,2,3), имеем

$$X_{-1} = -x - x^p + \frac{[1 + (x^3 + ax + b)^{\frac{p-1}{2}}]^2 (x^3 + ax + b)}{(x - x^p)^2}$$

Заметим, что степень числителя P_{-1} на единицу больше степени знаменателя Q_{-1}. В самом деле, легко видеть, что

$$X_{-1} = \frac{x^{2p+1} + R(x)}{(x - x^p)^2},$$

где $R(x)$ — многочлен степени, не превосходящей $2p$.

Вычислим степень знаменателя Q_{-1} по проведении необходимых сокращений. С одной стороны, $(x - x^p)^2 = [x(x-1)\dots(x-p+1)]^2$, с другой стороны, как известно,

$$(x^3 + ax + b)^{\frac{p-1}{2}} \equiv \left(\frac{x^3 + ax + b}{p}\right).$$

Поэтому при сокращении из знаменателя выпадут лишь множители вида $(x-k)^2$ с $\left(\frac{k^3 + ak + b}{p}\right) = -1$ и множители вида $x - l$ с $l^3 + al + b = 0$. Пусть m — число множителей первого, а n — второго вида. Тогда $d_{-1} = 2p - 2m - n + 1$, $d_{-1} - d_0 - 1 = p - 2m - n$, потому что $d_0 = p$. Число же N равно $2(p-m) - n$, потому что каждому классу вычетов k с $\left(\frac{k^3 + ak + b}{p}\right) = 1$ соответствует два решения сравнения (10, 1, 1), а каждому классу вычетов l, для которого $l^3 + al + b = 0$, соответствует лишь одно решение $(l, 0)$. Это доказывает требуемое.

Основные трудности доказательства оценки (10,1,3) сконцентрированы в доказательстве следующего факта.

Основная лемма.

$$d_{n-1} + d_{n+1} = 2d_n + 2.$$

§ 4. Вывод теоремы из основной леммы

Покажем, как из основной леммы выводится оценка (10,1,3).

Лемма 2.

$$d_n = n^2 - (d_{-1} - d_0 - 1)n + d_0.$$

По основной лемме, $d_{n+2} = 2d_{n+1} - d_n + 2$.

Очевидно, для $n = -1$ и $n = 0$ лемма верна; пусть она верна для индексов n и $n+1$, $n \geqslant 0$. Тогда

$$d_{n+2} = 2d_{n+1} - d_n + 2 = 2[(n+1)^2 - (d_{-1} - d_0 - 1)(n+1) + d_0] - n^2 + (d_{-1} - d_0 - 1)n - d_0 + 2 =$$
$$= (n+2)^2 - (d_{-1} - d_0 - 1)(n+2) + d_0.$$

Подобным же образом проходит индукция для $n < 0$.

Доказательство оценки (10,1,3). Согласно леммам 1 и 2, $d_n = n^2 - (N-p)n + p$. Этот квадратный трехчлен принимает для всех целых n неотрицательные значения, причем по определению чисел d_n он не может иметь двух последовательных целых нулей. Покажем, что дискриминант такого трехчлена неположителен. В самом деле, иначе трехчлен имел бы два корня α и β в промежутке между двумя последовательными целыми числами: $n \leqslant \alpha < \beta \leqslant n+1$, причем оба знака равенства одновременно не могут иметь места. Но тогда числа $\alpha\beta$ и $\alpha + \beta$ не могли бы быть одновременно целыми. Следовательно,

$$(N-p)^2 - 4p \leqslant 0,$$

так что

$$|N-p| < 2\sqrt{p}.$$

Теорема доказана.

§ 5. Доказательство основной леммы

Приступим к доказательству основной леммы. Для любого многочлена P от неизвестной x символом ст. P будем обозначать его степень. Нам понадобится следующий вспомогательный факт.

Лемма 3. *Для всех n, для которых функция X_n определена, имеет место неравенство*

$$\text{ст. } P_n > \text{ст. } Q_n.$$

Мы докажем это неравенство, формально найдя значение функции X_n при $x = \infty$. Пусть m есть нуль или первый номер после очередного пробела, $m \geqslant 0$. По построению, $X_m|_\infty = \infty$, $Y_m|_\infty \neq 0$. Предполагая, что эти соотношения

справедливы для некоторого индекса n, вслед за которым идет не пробел, докажем, что они выполнены для индекса $n+1$. Этого достаточно для справедливости утверждения о степенях числителя и знаменателя функции X_{n+1}. Как показывает равенство (10,2,1), достаточно проверить лишь, что $Y_{n+1}|_\infty \neq 0$. Допустим обратное. Ввиду того, что дробь $\dfrac{X_{n+1}^3 + aX_{n+1} + b}{x^3 + ax + b}$ должна быть квадратом, разность степеней числителя и знаменателя функции X_{n+1} должна быть числом нечетным, что вместе с $Y_{n+1}|_\infty = 0$ дает $X_{n+1}|_\infty = 0$. Из формул (10,2,4) и (10,3,2) следует, что

$$Y_{n+1} = \frac{1 - Y_n}{x - X_n}(x - X_{n+1}) - 1.$$

Отсюда находим

$$\frac{1 - Y_n}{x - X_n}(x - X_{n+1})\Big|_\infty = 1 \text{ или } \frac{1 - Y_n}{1 - \dfrac{X_n}{x}}\Big|_\infty = 1,$$

то есть

$$\frac{Y_n x}{X_n}\Big|_\infty = 1, \qquad \frac{Y_n^2 x^2}{X_n^2}\Big|_\infty = \frac{(X_n^3 + aX_n + b)x^2}{(x^3 + ax + b)X_n^2}\Big|_\infty = 1.$$

Поскольку $X_n|_\infty = x|_\infty = \infty$, отсюда следует, что $\dfrac{X_n}{x}|_\infty = 1$

С другой стороны, из формул (10, 2, 3) и (10, 3, 2) вытекает, что

$$X_{n+1} = -x - X_n + \frac{(1 - Y_n)^2}{(x - X_n)^2}(x^3 + ax + b). \quad (10,5,1)$$

Отсюда находим

$$\frac{X_{n+1}}{x} = -1 - \frac{X_n}{x} + \frac{(1 - Y_n)^2}{\left(1 - \dfrac{X_n}{x}\right)^2}\left(1 + \frac{a}{x^2} + \frac{b}{x^3}\right),$$

так что

$$\frac{X_{n+1}}{x}\Big|_\infty = -1.$$

Но из этого равенства в силу формулы (10,2,1) следует, что $Y_{n+1}^2|_\infty = -1$, а это противоречит сделанному предположению $Y_{n+1}|_\infty = 0$.

Подобным же образом проходит индукция влево.

Лемма доказана.

В доказательстве основной леммы будем различать два случая.

а) Не все функции X_{n-1}, X_n, X_{n+1} определены. Ясно, что из последовательной тройки функций может не быть определена лишь одна. Если не определена средняя функция, то

$$X_{n-1} = x, \quad X_{n+1} = x, \quad d_{n-1} = 1, \quad d_n = 0, \quad d_{n+1} = 1,$$

что удовлетворяет доказываемому равенству. Если же не определена одна из крайних функций, скажем, правая, то в силу формулы (10,2,7)

$$X_n = x, \qquad X_{n+1} = \frac{(x^2 - a)^2 - 8bx}{4(x^3 + ax + b)},$$

то есть $d_n = 1$, $d_{n+1} = 4$, что вместе с $d_{n-1} = 0$ снова дает утверждение основной леммы. Подобным же образом проверяется случай, когда не определена левая функция.

б) Все функции X_{n-1}, X_n, X_{n+1} определены.

Приводя к общему знаменателю и собирая подобные члены в формуле (10,2,8) находим

$$X_{n-1} = \frac{-(xQ_n + P_n)(xQ_n - P_n)^2 + (1 + Y_n)^2 (x^3 + ax + b) Q_n^2}{(xQ_n - P_n)^2} =$$

$$= \frac{(xQ_n + P_n)(xP_n + aQ_n) + 2bQ_n^2 - 2Y_n (x^3 + ax + b) Q_n^2}{(xQ_n - P_n)^2} =$$

$$= \frac{R}{(xQ_n - P_n)^2}. \qquad (10,5,2)$$

Подобным же образом

$$X_{n+1} = \frac{-(xQ_n + P_n)(xQ_n - P_n)^2 + (1 - Y_n)^2 (x^3 + ax + b) Q_n^2}{(xQ_n - P_n)^2} =$$

$$= \frac{(xQ_n + P_n)(xP_n + aQ_n) + 2bQ_n^2 + 2Y_n (x^3 + ax + b) Q_n^2}{(xQ_n - P_n)^2} =$$

$$= \frac{S}{(xQ_n - P_n)^2}. \qquad (10,5,3)$$

Перемножая почленно формулы (10,5,2) и (10,5,3) и произведя сокращения, получим (мы позволим себе опустить подробности выкладки)

$$X_{n-1} X_{n+1} = \frac{P_{n-1}}{Q_{n-1}} \frac{P_{n+1}}{Q_{n+1}} =$$

$$= \frac{(xP_n - aQ_n)^2 - 4bQ_n (xQ_n + P_n)}{(xQ_n - P_n)^2}. \qquad (10,5,4)$$

Цель последующих рассуждений — показать, что

$$Q_{n-1}\,Q_{n+1} = (xQ_n - P_n)^2. \qquad (10,5,5)$$

Из этого равенства основная лемма получится немедленно. В самом деле, из формулы (10,5,5) тогда следует, что

$$P_{n-1}\,P_{n+1} = (xP_n - aQ_n)^2 - 4bQ_n(xQ_n + P_n)$$

и, значит,

$$d_{n-1} + d_{n+1} = \text{ст.}\,(P_{n-1}\,P_{n+1}) = \text{ст.}\,(x^2\,P_n^2) = 2d_n + 2,$$

потому что в силу леммы 3 старший член многочлена $P_{n-1}\,P_{n+1}$ совпадает со старшим членом многочлена $x^2\,P_n^2$.

Остается установить равенство (10,5,5).

Напомним, что в области многочленов имеет место однозначное расположение на неприводимые множители. Пусть E — неприводимый многочлен, $e > 0$ — любое целое число. Мы будем говорить, что многочлен E^e строго делит некоторую несократимую рациональную функцию, если ее числитель делится на E^e, но не делится на E^{e+1}.

Для доказательства равенства (10,5,5) достаточно установить, что если многочлен E^e строго делит $(xQ_n - P_n)^2$, то он строго делит также $Q_{n-1}\,Q_{n+1}$. В самом деле, тогда частное $\frac{Q_{n-1}\,Q_{n+1}}{(xQ_n - P)^2}$ представляет собой многочлен, который взаимно прост с многочленом $(xQ_n - P_n)^2$. Но поскольку из равенства (10,2,1) следует, что функция $Y_n(x^3 + ax + b)\,Q_n^2$ является многочленом, из равенств (10,5,2) и (10,5,3) без труда получается, что знаменатели Q_{n-1} и Q_{n+1} делят многочлен $(xQ_n - P_n)^4$. Тем самым, частное $\frac{Q_{n-1}\,Q_{n+1}}{(xQ_n - P_n)^2}$ может быть только константой, и эта константа равна единице в силу принятой нами нормировки старших членов числителей P_n.

Разобьем все неприводимые делители E многочлена $(xQ_n - P_n)^2$ на три группы. (Отметим, что все такие многочлены E делят RS.)

К первой группе отнесем те многочлены E, которые делят R, но не делят S. Из формул (10,5,2) — (10,5,4) сразу же вытекает, что если многочлен E^e строго делит $(xQ_n - P_n)^2$, то он строго делит знаменатель Q_{n+1} и взаимно прост со знаменателем Q_{n-1}.

Ко второй группе отнесем те многочлены E, которые делят S, но не делят R. Точно так же получается, что если многочлен E^e строго делит $(xQ_n - P_n)^2$, то он строго делит Q_{n-1} и взаимно прост с Q_{n+1}.

Наконец, к третьей группе отнесем те многочлены E, которые делят и R, и S. Поскольку

$$P_n \equiv xQ_n \pmod{E},$$

из формул (10,5,2) и (10,5,3) следует, что

$$R \equiv 2\,Q_n^2 (1 - Y_n)(x^3 + ax + b) \pmod{E},$$
$$S \equiv 2\,Q_n^2 (1 + Y_n)(x^3 + ax + b) \pmod{E}. \qquad (10,5,6)$$

Многочлен E, деля многочлен $(x\,Q_n - P_n)^2$, не может делить Q_n, поскольку P_n и Q_n взаимно просты. Из формулы (10,5,6) вытекает, что $S + R \equiv 4\,Q_n^2 (x^3 + ax + b) \bmod E$, так что если E делит R и S, то E строго делит многочлен $x^3 + ax + b$ (по предположению, этот многочлен не имеет кратных корней).

Итак, пусть E — некоторый неприводимый делитель многочлена $x^3 + ax + b$. Предположим сначала, что $Y_n \not\equiv \pm 1 \pmod{E}$ (эта запись по определению означает, что числитель несократимого представления функции $Y_n \pm 1$ не делится на E). Тогда из формулы (10,5,2) следует, что E строго делит R, потому что многочлен $(x\,Q_n - P_n)^2$ делится по крайней мере на E^2. Подобным же образом получается, что E строго делит S, но тогда из формул (10,5,2) — (10,5,4) вытекает, что E^2 строго делит $(x\,Q_n - P_n)^2$.

Таким образом, остается проверить случаи $Y_n \equiv \pm 1 \pmod{E}$. Пусть, например, $Y_n \equiv -1 \pmod{E}$ (вторая возможность разбирается аналогично). Тогда E строго делит S. Пусть E^{2e} строго делит $(x\,Q_n - P_n)^2$, а E^{2f+1} строго делит $(1 + Y_n)^2 (x^3 + ax + b)\,Q_n^2$. Очевидно, E^{2f} строго делит также функцию $(1 + Y_n)^2 (1 - Y_n)^2 = (1 - Y_n^2)^2$. Но

$$(1 - Y_n^2)^2 = \frac{(x^3 + ax - X_n^3 - a\,X_n)^2}{(x^3 + ax + b)^2} =$$
$$= \frac{(x - X_n)^2 (x^2 + xX_n + X_n^2 + a)^2}{(x^3 + ax + b)^2}.$$

Кроме того, $x \equiv X_n \pmod{E}$ и $x^2 + xX_n + X_n^2 + a \equiv 3x^2 + a \not\equiv 0 \pmod{E}$, так что $2f = 2e - 2$ и, следовательно, число $2f + 1 = 2e - 1$ меньше степени, в которой E строго делит $(xQ_n + P_n)(xQ_n - P_n)^2$. Поэтому E^{2e-1} строго делит R, а E^{2e} строго делит RS. Из формул (10,5,2) — (10,5,4) снова вытекает тогда, что E^{2e} строго делит $Q_{n-1}Q_{n+1}$.

Этим завершается доказательство основной леммы и оценки (10,1,3).

ГЛАВА II

ЭЛЕМЕНТАРНОЕ ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ К. Л. ЗИГЕЛЯ

§ 1. Формулировка теоремы. Средства доказательства

Теорема Зигеля о числе классов $h(\Delta)$ бинарных квадратичных форм фундаментального дискриминанта Δ утверждает, что если $\Delta = -D < 0$, то

$$\lim_{D\to\infty} \frac{\ln h(-D)}{\ln D} = \frac{1}{2}. \qquad (11,1,1)$$

Эта теорема, доказанная К. Л. Зигелем в 1935 г. [48] аналитическими средствами, играет фундаментальную роль в современной аналитической теории чисел. Здесь мы изложим доказательство этой теоремы сравнительно элементарными средствами, данное Ю. В. Линником [15] как приложение одной идеи И. М. Виноградова.

В 1918 г. И. М. Виноградовым была высказана мысль о примечательном сходстве между поведением примитивных реальных характеров $\chi(n)$ по большому модулю D на интервале $[1, D-1]$ и поведением функции Лиувилля $\lambda(n) = (-1)^{\nu(n)}$ ($\nu(n)$ — число всех простых делителей n) на том же интервале. Основой такого сходства является полная мультипликативность обоих видов функций. Однако в то время как для сумм характеров $\chi(n)$ существует оценка И. М. Виноградова [см. [3]]

$$\sum_{n\leqslant x} \chi(n) = B\sqrt{D}\ln D \qquad (11,1,2)$$

для любого $x \in [1, D-1]$, существование оценки типа

$$\sum_{n\leqslant x} \lambda(n) = Bx^{1-c_0} \qquad (c_0 > 0 \text{ — константа}) \qquad (11,1,3)$$

для функции Лиувилля $\lambda(n)$ является неразрешенной проблемой, совпадающей со «слабой гипотезой Римана» для ζ-функции Римана.

Для выяснения связи между оценками (11,1,1) и (11,1,2) И. М. Виноградов указал на полезность изучения степени порчи функции Лиувилля $\lambda(n)$ при замене ее на характер $\chi(n)$. При построении элементарного доказательства теоремы К. Л. Зигеля на основе указанной идеи мы будем применять следующие средства:

а) элементы арифметической теории бинарных квадратичных форм и реальных характеров, включая оценку И. М. Виноградова (11,1,2) *);

б) элементарные свойства простых чисел и функции Мёбиуса;

в) определение и свойства неперова числа;

г) элементарная алгебра;

д) понятие о пределе (этого можно и избежать, но тогда нужно очевидным образом изменить формулировку теоремы), и элементарное свойство непрерывной функции.

К сожалению, доказательство будет столь же неэффективным, как и другие известные доказательства.

Формула (11,1,1) не позволяет эффективных вычислений.

§ 2. Леммы

$C_0, C_1, \ldots$; $c_0, c_1, \ldots$; $\varepsilon_0, \varepsilon_1, \ldots$; $\eta_0, \eta_1, \ldots$, как и в других главах обозначают положительные константы; в двух последних рядах будут всегда малые $\left(\text{меньше } \frac{1}{4}\right)$ константы.

Пусть дан реальный примитивный характер $\chi_k(n)$ по модулю $k > 2$ и число $\beta > \frac{1}{2}$, не превосходящее 1.

Мы будем говорить, что $\chi_k(n)$ обладает свойством $\mathfrak{A}(\beta)$, если существует такая константа $C_0(\chi_k)$, что при любом $N > C_0(\chi_k)$ в сегменте $[\sqrt{N}, N]$ найдется такое $N_1 \in [\sqrt{N}, N]$, что

$$\left|\sum_{n \leqslant N_1} \chi_k(n)\mu(n)\right| > N_1^{\beta}. \qquad (11,2,1)$$

Со свойством $\mathfrak{A}(\beta)$ связана следующая лемма.

*) Впрочем, ее можно заменить и тривиальной оценкой: D вместо $\sqrt{D}\ln D$.

I основная лемма. *Если существует какой-либо характер* $\chi_k(n)$, *обладающий свойством* $\mathfrak{A}(\beta)$, *где* $\beta \geqslant \frac{3}{4}$, *то при* $D \geqslant C_1(\chi_k, \eta_0)$ *будем иметь*

$$h(-D) > D^{\frac{1}{2} - \eta(\beta)}, \tag{11,2,2}$$

где

$$\eta(\beta) = 10{,}5(1-\beta) + \eta_0 \tag{11,2,3}$$

и η_0 — *сколь угодно малое положительное фиксированное число.*

Доказательство этого предложения будет опираться на несколько лемм.

Лемма 1. *Если* $\rho > 1$, $q_1 > q_0 > 1$, *то*

$$\sum_{q=q_0}^{q_1} \frac{1}{q^\rho} < \frac{2}{1 - \frac{1}{2^\rho}} \frac{1}{q_0^{\rho-1}}. \tag{11,2,4}$$

Для доказательства заменяем все числа q между q_0 и $2q_0$ на q_0, все числа q между $2q_0+1$ и $4q_0$ на $2q_0$ и т. д. и оцениваем далее сумму геометрической прогрессии со знаменателем $\frac{1}{2^\rho}$.

Лемма 2. *Если имеет место неравенство*

$$\left| \sum_{n \leqslant N_1} \chi_k(n) \mu(n) \right| > N_1^\beta \left(\beta > \frac{1}{2}\right) \tag{11,2,5}$$

и ε — *любое число под условием* $0 < \varepsilon < \beta - \frac{1}{2}$, *то при* $N_1 > C_0(\beta, \varepsilon, \chi_k)$ *в сегменте* $[N_1^{2\beta-1-2\varepsilon}, N_1]$ *найдется целое число* $N_2 \in [N_1^{2\beta-1-2\varepsilon}, N_1]$ *такое, что*

$$\left| \sum_{n \leqslant N_2} \chi_k(n) \lambda(n) \right| > N_2^{\beta-\varepsilon}. \tag{11,2,6}$$

По соображениям «решета», имеем

$$\sum_{n \leqslant N_1} \chi_k(n) \mu(n) = \sum_{q \leqslant \sqrt{N_1}} \mu(q) \sum_{m \leqslant \frac{N_1}{q^2}} \chi_k(m) \lambda(m). \tag{11,2,7}$$

Отберем те значения q, для которых $q \geqslant N_1^{1-\beta+\varepsilon}$. Для них, согласно (11,2,4), получим

$$\left| \sum_{N_1^{1-\beta+\varepsilon} \leqslant q \leqslant \sqrt{N_1}} \mu(q) \sum_{m \leqslant \frac{N_1}{q^2}} \chi_k(m) \lambda(m) \right| \leqslant$$

$$\leqslant \sum_{N_1^{1-\beta+\varepsilon} \leqslant q \leqslant \sqrt{N_1}} \frac{N_1}{q^2} < \frac{4N_1}{N_1^{1-\beta+\varepsilon}}.$$

Это последнее число не превосходит $4N_1^{\beta-\varepsilon}$, так что

$$\sum_{n \leqslant N_1} \chi_k(n) \mu(n) = \sum_{q < N_1^{1-\beta+\varepsilon}} \mu(q) \sum_{m \leqslant \frac{N_1}{q^2}} \chi_k(m) \lambda(m) + R_{N_1}, \quad (11,2,8)$$

где $|R_{N_1}| < 4N_1^{\beta-\varepsilon}$.

Допустим теперь, что при $q < N_1^{1-\beta+\varepsilon}$ имеем всегда

$$\left| \sum_{n \leqslant \frac{N_1}{q^2}} \chi_k(m) \lambda(m) \right| < \left(\frac{N_1}{q^2}\right)^{\beta-\varepsilon},$$

и приведем предположение к противоречию. На основании (11,2,4) мы получим из предположения

$$\left| \sum_{q < N_1^{1-\beta+\varepsilon}} \mu(q) \sum_{m \leqslant \frac{N_1}{q^2}} \chi_k(m) \lambda(m) \right| <$$

$$< N_1^{\beta-\varepsilon} \sum_{1 \leqslant q \leqslant N_1^{1-\beta+\varepsilon}} \frac{1}{q^{2\beta-2\varepsilon}} < C(\beta, \varepsilon) N_1^{\beta-\varepsilon}.$$

Подставляя в (11,2,8), находим

$$\left| \sum_{n \leqslant N_1} \chi_k(n) \mu(n) \right| < (C(\beta, \varepsilon) + 4) N_1^{\beta-\varepsilon},$$

что противоречит (11,2,5). Отсюда следует, что при достаточно большом N_1 найдется q такое, что

$$\left| \sum_{m \leqslant \frac{N_1}{q^2}} \chi_k(m) \lambda(m) \right| \geqslant \left(\frac{N_1}{q^2}\right)^{\beta-\varepsilon}, \quad q < N_1^{1-\beta+\varepsilon}.$$

Полагая $N_2 = \frac{N_1}{q^2}$, мы видим, что $N_2 \leqslant N_1$ и $N_2 > N^{2\beta-1-2\varepsilon}$. Это и доказывает лемму 2.

Лемма 3. *Для любого характера* $\chi(n)$, *примитивного* (mod D), *имеем*

$$\sum_{n \leqslant x} \chi(n) = B\sqrt{D}\ln D, \tag{11,2,9}$$

где x — *любое число.*

Далее, если $\nu(n)$ — *число простых делителей* n, $\tau(n)$ — *число всех его делителей, то*

$$2^{\nu(n)} = B_\varepsilon n^\varepsilon; \qquad \tau(n) = B_\varepsilon n^\varepsilon$$

при любом фиксированном ε *и* $n \to \infty$.

Эти три соотношения, из которых (11,2,9) есть известная оценка И. М. Виноградова, доказываются элементарно.

Лемма 4. *Если* $Q(x, y) = ax^2 + bxy + cy^2$ — *приведенная положительная коренная форма дискриминанта* — D, *то*

$$\sum_{m \leqslant M} r(m) < c_1 \frac{M}{\sqrt{D}},$$

где $r(m)$ — *число решений уравнения* $Q(x, y) = m$, а $M \geqslant D^2$.

Для подсчета достаточно грубо оценить число целых точек в области $Q(x, y) \leqslant M$.

§ 3. Доказательство I основной леммы

Пусть дан реальный характер $\chi_k(n)$ обладающий свойством $\mathfrak{A}(\beta)$ с $\beta \geqslant \frac{3}{4}$, и указана соответствующая константа $C_0(\chi_k)$. Тогда, по определению свойства $\mathfrak{A}(\beta)$ и по лемме 2, при любом положительном $\varepsilon < \beta - \frac{1}{2}$ и $N > C_1(\beta, \varepsilon, \chi_k)$ в сегменте $[N^{\beta-\frac{1}{2}-\varepsilon}, N]$ найдется число N_2 такое, что

$$\left|\sum_{n \leqslant N_2} \chi_k(n)\lambda(n)\right| > N_2^{\beta-\varepsilon}. \tag{11,3,1}$$

Положим здесь

$$\varepsilon = \varepsilon_0 = 0{,}01(1-\beta). \tag{11,3,2}$$

Пусть существует бесконечная последовательность фундаментальных дискриминантов $-D_j$ $(j=1, 2, \ldots)$ под условием

$$h(-D_j) \leqslant D_j^{\frac{1}{2}-\eta(\beta)}; \quad \eta(\beta) = 10{,}5(1-\beta)+\eta_0, \quad (11{,}3{,}3)$$

где η_0 — сколь угодно малое положительное фиксированное число. Нам нужно привести это предположение к противоречию. Возьмем столь большое $D_j = D$, что $D_j > C_1(\beta, \varepsilon, \chi_k)$, и выберем

$$N = [2D^{\frac{4}{\beta-\frac{1}{2}-\varepsilon_0}}] = N_3.$$

Тогда найдется $N_2 \in [D^4, N_3]$, $N_3 > D^8$ такое, что

$$\Big|\sum_{n\leqslant N_2} \chi_k(n)\lambda(n)\Big| > N_2^{\beta-\varepsilon_0}. \quad (11{,}3{,}4)$$

Положим $\chi(n) = \left(\frac{-D}{n}\right)$ и введем сумму

$$\sum_{n\leqslant N_2} \chi_k(n)\chi(n).$$

Согласно лемме 3 и основным свойствам характеров, имеем

$$\sum_{n\leqslant N_2} \chi_k(n)\chi(n) \leqslant \sqrt{kD}\ln(kD). \quad (11{,}3{,}5)$$

Сравним суммы (11,3,4) и (11,3,5), исследуя возможные различия в поведении $\lambda(n)$ и $\chi(n)$.

Пусть сперва $p_1, p_2, \ldots, p_s$ — различные простые числа, для которых $\chi(p_j) = 0$. Тогда $p_1 p_2 \ldots p_s \leqslant D$.

Введем мультипликативную функцию $\chi'(n)$, которая отличается от $\chi(n)$ тем и только тем, что $\chi'(p_j) = -1$ $(j = 1, 2, \ldots, s)$. Тогда получим

$$\sum_{n\leqslant N_2} \chi_k(n)\chi'(n) = \sum_{n\leqslant N_2} \chi_k(n)\chi(n) - \sum_{p_j}\sum_{n\leqslant \frac{N_2}{p_j}} \chi_k(n)\chi(n) + \ldots$$

$$\ldots + (-1)^{s-1} \sum_{n\leqslant \frac{N_2}{p_1\ldots p_s}} \chi_k(n)\chi(n).$$

Число наших сумм не превосходит $2^s \leqslant \tau(D) \leqslant B_{\varepsilon'} D^{\varepsilon'}$ при любом фиксированном $\varepsilon' > 0$. Каждая из сумм, по лемме 3, не превосходит $C_1 \sqrt{Dk} \ln(kD)$, и поэтому

$$\sum_{n \leqslant N_2} \chi_k(n) \chi'(n) \leqslant B_{\varepsilon'} N_2^{\varepsilon'} \sqrt{kD} \ln(kD). \qquad (11,3,6)$$

Произведем в этой сумме замену всех $\chi'(n)$ на $\lambda(n)$, что равносильно замене значений $\chi'(p) = 1$ для $p \mid n$ на $\lambda(p) = -1$ $(p \mid n)$.

Обозначим через $\mathfrak{A}_D$ множество всех таких чисел n', каждый простой делитель которых $p \mid n'$ будет иметь $\chi(p) = +1$.

Из элементарной теории квадратичных форм хорошо известно, что $\mathfrak{A}_D$ совпадает с множеством всех чисел, примитивно представляемых формами дискриминанта — D. Следовательно,

$$\sum_{n \leqslant N_2} \chi_k(n) \lambda(n) \leqslant \sum_{n \leqslant N_0} \chi_k(n) \chi'(n) - 2 \sum_{p_j \in \mathfrak{A}_D} \sum_{n \leqslant \frac{N_2}{p_j}} \chi_k(n) \chi'(n) +$$

$$+ 4 \sum_{p_i p_j \in \mathfrak{A}_D} \sum_{n \leqslant \frac{N_2}{p_i p_j}} \chi_k(n) \chi'(n) + \ldots$$

$$\ldots + (-1)^m 2^m \sum_{p_i p_j \ldots p_\rho \in \mathfrak{A}_D} \sum_{n \leqslant \frac{N_2}{p_i p_j \ldots p_\rho}} \chi_k(n) \chi'(n) + \ldots \qquad (11,3,7)$$

Разобьем суммы на два типа:

1) те, в которых $p_i p_j \ldots p_\rho \geqslant \frac{N_2}{D^2}$,

2) остальные.

Суммы первого типа в совокупности не превосходят

$$N_2 \sum_{\frac{N_2}{D^2} \leqslant n' \leqslant N_2} \frac{2^{\nu(n')}}{n'},$$

где n' — свободное от квадратов число, принадлежащее $\mathfrak{A}_D$. Из элементарной теории квадратичных форм следует, что

эта сумма не превосходит

$$N_2 \sum_{Q} \sum_{\frac{N_2}{D^2} \leqslant Q(x,\,y) \leqslant N_2} \frac{1}{Q(x, y)},$$

где $Q(x, y)$ пробегает проведенные формы дискриминанта $-D$.

Из леммы 4 легко выводим

$$\sum_{\frac{N_2}{D^2} \leqslant Q(x,\,y) \leqslant N_2} \frac{1}{Q(x, y)} < C_2 \frac{\log_2 D}{\sqrt{D}}.$$

Суммирование на все $\leqslant 2h(-D)$ форм $Q(x, y)$ дает

$$N_2 \sum_{Q} \sum_{\frac{N_2}{D^2} \leqslant Q(x,\,y) \leqslant N_2} \frac{1}{Q(x, y)} < 2N_2 h(-D) \frac{C_2 \log_2 D}{\sqrt{D}}. \quad (11,3,8)$$

Но, согласно (11, 3, 3),

$$h(-D) \leqslant D^{\frac{1}{2}-\eta(\beta)},$$

так что получаем

$$N_2 \sum_{\frac{N_2}{D^2} \leqslant n' \leqslant N_2} \frac{2^{\nu(n')}}{n'} < 2C_2 N_2 \log_2 D \cdot D^{\frac{1}{2}-\eta(\beta)} \cdot \frac{1}{\sqrt{D}} =$$

$$= B_0 N_2 \log_2 D \cdot D^{-\eta(\beta)}. \quad (11,3,9)$$

Для сумм второго типа, где $p_i p_j \ldots p_\rho < \frac{N_2}{D^2}$, имеем

$$\left|2^m \sum_{n \leqslant \frac{N_2}{p_i \ldots p_\rho}} \chi_k(n) \chi'(n)\right| < N_2^{\varepsilon'} 2\sqrt{kD} \ln(kD), \quad (11,3,10)$$

на основании очевидной модификации оценки (11,3,6).

Далее, $2^m \ll N_2^{\varepsilon'}$ по лемме 3. Количество же сумм второго типа равно количеству $p_i p_j \ldots p_\rho < \frac{N_2}{D^2}$, так что общая их оценка не превосходит

$$C_8 N_2^{2\varepsilon'} \frac{\sqrt{kD} \ln(kD)}{D^2} N^2. \quad (11,3,11)$$

§ 4. Продолжение доказательства. Другие леммы

Оценки (11,3,9) и (11,3,11) дают в соединении с (11,3,7)

$$\left|\sum_{n\leqslant N_2}\chi_k(n)\lambda(n)\right|\leqslant N_2 D^{-0,9\eta(\beta)}, \qquad (11,4,1)$$

в то время как, согласно (11, 3, 4),

$$\left|\sum_{n\leqslant N_2}\chi_k(n)\lambda(n)\right|>N_2^{\beta-\varepsilon_0}=N_2^{\beta-0,01(1-\beta)}. \qquad (11,4,2)$$

По выбору N_2 имеем $N_2\leqslant 2D^{\beta-\frac{1}{2}-\varepsilon_0}<D^{\frac{4}{9}}$, откуда

$$D^{0,9\eta(\beta)}>N_2^{0,1\eta(\beta)}.$$

Вспоминая, что $\eta(\beta)=10{,}5(1-\beta)+0{,}1\eta_0$, получим, сравнивая (11,4,1) и (11,4,2)

$$N_2^{1-1,01\eta(\beta)}\leqslant N_2^{1-0,1\eta(\beta)}=N_2^{1-1,05(1-\beta)-0,1\eta_0}. \qquad (11,4,3)$$

При $D>C_0(\beta,\eta_0,k)$ получим очевидное противоречие, доказывающее I основную лемму.

Лемма 5. *При* $h\to 0$ *имеем*

$$\ln(1+h)=1+O(h),\quad (1+h)^\beta=1+O(h), \qquad (11,4,4)$$

где $\beta>0$ *— фиксированное число.*

Эта лемма доказывается на основании определения числа e и натуральных логарифмов, а также свойств обыкновенного бинома Ньютона.

Пусть $(-k)$ — фундаментальный дискриминант, а $\chi_k(n)=\left(\frac{-k}{n}\right)$ — соответствующий характер. Пусть ε_1 — какое-либо число, фиксированное под условиями

$$0<\varepsilon_1<0{,}01. \qquad (11,4,5)$$

Предположим, что

$$h(-k)<k^{\frac{1}{2}-\varepsilon_1}, \qquad (11,4,6)$$

и, считая в дальнейшем k достаточно большим сравнительно $\frac{1}{\varepsilon_1}$, выведем из (11,4,6) некоторые следствия.

Пусть a_1 — положительное число под условиями

$$0{,}01\,\varepsilon_1 \leqslant a_1 \leqslant \frac{3}{2}. \tag{11,4,7}$$

Мы будем рассматривать выражение

$$L(a_1) = \sum_{n \leqslant k^3} \chi_k(n)\, n^{-a_1} \tag{11,4,8}$$

и в нем, как это делалось ранее, постараемся заменить $\chi_k(n)$ на $\lambda(n)$, а затем отсеять числа, делящиеся на квадраты. Таким образом, мы будем сравнивать (11,4,8) с

$$L_1(a_1) = \sum_{n \leqslant k^3} \chi_k(n)\, n^{-a_1}. \tag{11,4,9}$$

Пусть

$$A = \frac{4}{\varepsilon_1}, \qquad (\ln k)^A = \Delta, \qquad k_1 = k^3. \tag{11,4,10}$$

Посмотрим, что получится, если отсеять из (11,4,8) числа n, содержащие простые множители, не превосходящие Δ. Если обозначить

$$\prod_1(a_1) = \prod_{p \leqslant \Delta} \left(1 - \frac{\chi_k(p)}{p^{a_1}}\right) = \sum_q \frac{b_q}{q^{a_1}},$$

то получим

$$L_2(a_1) = \sum_{q \leqslant k_1} \frac{b_q}{q^{a_1}} \sum_{m \leqslant \frac{k_1}{q}} \chi_k(m)\, m^{-a_1}, \tag{11,4,11}$$

где $L_2(a_1)$ — результат высеивания из $L(a_1)$ указанных выше чисел.

Докажем следующую оценку: для любого $N \geqslant k$ имеем

$$\sum_{N \leqslant q \leqslant 2N} |b_q| q^{-a_1} \ll N^{-0{,}18\varepsilon_1}. \tag{11,4,12}$$

В самом деле, пусть (11,4,12) не выполняется для какого-либо $N \geqslant k$. Пусть $a_1' = 1 - 0{,}2\varepsilon_1$. Тогда имеем

$$\sum_{N \leqslant q \leqslant 2N} |b_q| q^{-a_1'} > N^{a_1 - a_1'} \sum_{N \leqslant q \leqslant 2N} |b_q| q^{-a_1} \geqslant N^{-0{,}18\varepsilon_1 + 0{,}19\varepsilon_1} = N^{0{,}01\varepsilon_1}. \tag{11,4,13}$$

С другой стороны,

$$\sum_{N\leqslant q\leqslant 2N}\frac{|b_q|}{q^{a_1'}}<\prod_{p\leqslant\Delta}\left(1+\frac{1}{p^{a_1}}\right)$$

и

$$\ln\prod_{p\leqslant\Delta}\left(1+\frac{1}{p^{a_1'}}\right)=B\sum_{n\leqslant\Delta}\frac{1}{n^{a_1'}}=B\,\Delta^{1-a_1'}$$

по леммам 1 и 5.

Далее,

$$\Delta^{1-a_1'}=(\ln k)^{A0{,}2\varepsilon_1}=(\ln k)^{0,8}\leqslant(\ln N)^{0,8}. \qquad (11{,}4{,}14)$$

Это явно противоречит (11,4,13) и доказывает лемму.

Полагая

$$\prod\nolimits_2(a_1)=\prod_{\substack{\Delta<p<k_1\\ \chi_k(p)=+1}}\frac{1-\frac{1}{p^{a_1}}}{1+\frac{1}{p^{a_1}}}=1+\sum_{q>\Delta}\frac{d_q}{q^{a_1}}, \qquad (11{,}4{,}15)$$

докажем следующую лемму.

Лемма 6. *Для любого* $N\in[\Delta,\ k^{\frac{1}{4}}]$ *число простых чисел под условием* $\chi_k(p)=+1$, $N\leqslant p\leqslant 2N$, *будет*

$$N_1\leqslant N^{-0{,}015\varepsilon_1}. \qquad (11{,}4{,}16)$$

Пусть это не так для данного N. Найдем целое число r, для которого $(2N)^r=k^\gamma\,(2\leqslant\gamma<3)$, и будем рассматривать $C_{N_1}^r$ всевозможных различных произведений по r из наших простых чисел. Имеем

$$C_{N_1}^r>\frac{N_1^r\,2^{-r}}{r!}>N_1^r e^{-r(1+\ln r)}$$

(очевидно, $r!\leqslant e^{r\ln r}$),

$$r\leqslant\frac{3\ln k}{\ln\Delta}=\frac{3}{4}\varepsilon_1\frac{\ln k}{\ln\ln k},\quad \ln r\leqslant\ln\ln k.$$

Отсюда при большом k имеем

$$C_{N_1}^r>N_1^r\,k^{-0{,}76\varepsilon_1}.$$

Если $N_1>N^{1-0{,}015\varepsilon_1}$, то

$$C_{N_1}^r>k^\gamma\,k^{-0{,}76\varepsilon_1}.$$

Все построенные произведения лежат между $k^{\frac{1}{2}}$ и $k^{\frac{1}{2}}2^{-r}$, $r \leqslant \frac{3}{4}\varepsilon_1 \frac{\ln k}{\ln\ln k}$. Все эти произведения представимы квадратичными формами $Q(x, y)$ дискриминанта $(-k)$ и лемма 4 в этом случае непосредственно дает

$$h(-k) > k^{\frac{1}{2}-0{,}82\varepsilon_1},$$

что противоречит (11, 4, 6) при большом k. Лемма доказана.

Обозначая

$$\overline{\prod}_2(a_1) = \prod_{\substack{\Delta < p \leqslant k_1 \\ \chi_k(p) = +1}} \frac{1+\frac{1}{p^{a_1}}}{1-\frac{1}{p^{a_1}}},$$

мы с помощью этой леммы получаем произведение, мажорирующее $\Pi_2(a_1)$ по лемме 5

$$\ln \overline{\prod}_2(a) \leqslant \sum_{\substack{\Delta < p \leqslant k \\ \chi_k(p) = +1}} \frac{1}{p^{a_1}} \leqslant \frac{1}{\Delta^{a_1}} \sum_{i=1}^{\infty} \frac{1}{2^{ia_1}} \times$$

$$\times\ \Delta^{i})^{1-0{,}015\varepsilon_1} \leqslant (\ln k)^{-0{,}02}. \quad (11{,}4{,}17)$$

Отсюда следует

Лемма 6а. *При* $N \geqslant k$, $a_2 \geqslant 1 - 0{,}005\,\varepsilon_1$ *имеем*

$$\sum_{N \leqslant q \leqslant 2N} |d_q|\, q^{-a_2} \leqslant N^{-0{,}004\varepsilon_1}. \quad (11{,}4{,}18)$$

Доказательство с помощью (11,4,17) полностью аналогично доказательству оценки (11,4,12).

Будем считать a_3 фиксированным и принадлежащим сегменту $\left[1 - 0{,}001\varepsilon_1, \frac{3}{2}\right]$. Полагая

$$\prod(a_3) = \prod_{2 \leqslant p \leqslant \Delta} \frac{1-\frac{\chi_k(p)}{p^{a_3}}}{1+\frac{1}{p^{a_3}}} \prod_{\substack{\Delta < p \leqslant k_1 \\ \chi_k(p) = +1}} \frac{1-\frac{1}{p^{a_3}}}{1+\frac{1}{p^{a_3}}} \prod_{2 \leqslant p \leqslant k_1} \left(1 - \frac{1}{p^{2a_3}}\right) =$$

$$= \sum_q \frac{c_q}{q^{a_3}},$$

находим, объединяя предыдущие оценки,

$$\ln \prod(a_3) = B(\ln k)^{0,8}, \tag{11,4,19}$$

$$\sum_{N \leqslant q \leqslant 2N} |e_q| q^{-a_3} = BN^{-0,003\varepsilon_1} \text{ при } N \geqslant k. \tag{11,4,20}$$

Далее, имеем

$$L_1(a_3) = \sum_{n \leqslant k_1} \frac{\mu(n)}{n^{a_3}} \sum_{q \leqslant k_1} \frac{l_q}{q^{a_3}} \sum_{m \leqslant \frac{k_1}{q}} \frac{\chi_k(m)}{m^{a_3}}. \tag{11,4,21}$$

Но абелево суммирование и оценка вида (11,1,2) дают

$$\sum_{m \leqslant \frac{k_1}{q}} \frac{\chi_k(m)}{m^{a_1}} = \begin{cases} L(a_1) + Bk^{-\frac{1}{2}} & \text{при } q \leqslant k^{1,5}, \\ B_k^{0,0015\varepsilon_1} & \text{при } q > k^{1,5}. \end{cases} \tag{11,4,22}$$

Подставим результат (11,4,20) и (11,4,22) в (11,4,21); тогда получим

$$L_1(a_3) = \sum_{q \leqslant \frac{k_1}{k^2}} \frac{l_q}{q^{a_1}} \left(L(a_3) + Bk^{-\frac{1}{2}}\right) + R_{a_1}, \tag{11,4,23}$$

где

$$R_{a_1} \leqslant k^{0,0015\varepsilon_1} \sum_{u^2 \leqslant q \leqslant k^3} \frac{|l_q|}{q^{a_3}} \leqslant k^{0,0015\varepsilon_1 - 0,003\varepsilon_1} \leqslant k^{-0,0015\varepsilon_1}. \tag{11,4,24}$$

Далее, (11,4,20) дает

$$\sum_{q \leqslant \frac{k_1}{k^2}} \frac{l_q}{q^{a_3}} = \prod(a_3) + Bk^{-0,003\varepsilon_1}. \tag{11,4,25}$$

Наконец, известная арифметическая оценка

$$\tau(n) = O(n^{\eta})$$

при любом фиксированном $\eta > 0$ дает

$$\sum_{q \leqslant \frac{k_1}{k^2}} \frac{|l_q|}{q^{a_1}} \leqslant k^{0,0015\varepsilon_1}.$$

Следовательно, (11,4,24) и (11,4,25) дают

$$L_1(a_3) = \Pi(a_3)\, L(a_3) + Bk^{-0{,}0015\varepsilon_1}. \qquad (11,4,26)$$

Учитывая (11,4,19), найдем отсюда

$$L(a_3) = L_1(a_3)\,(\Pi(a_3))^{-1} + Bk^{-0{,}001\varepsilon_1}. \qquad (11,4,27)$$

Положим $a_3 = \beta$, так что $\beta \in [1 - 0{,}001\,\varepsilon_1, \frac{3}{2}]$.

Лемма 7. *Для любого* $n \in [k^2, k^4]$

$$\sum_{n \leqslant N} \mu(n) \ll n^{1 - 0{,}01\varepsilon_1}. \qquad (11,4,28)$$

Эта лемма доказывается с помощью тривиальной модификации доказательства I основной леммы: нарушение (11, 4, 28) привело бы к противоречию с гипотезой

$$h(-k) < k^{\frac{1}{2} - \varepsilon_1}. \qquad (11,4,6)$$

(По существу, лемма 7 — частный случай несколько видоизмененной I основной леммы.)

$$F(\beta, k_2) = \sum_{n \leqslant k_2} a_n n^{-\beta},$$

где

$$a_n = (-1)^{n-1}, \qquad k_2 = k_1 k = k^4.$$

В таком случае имеем равенство

$$\sum_{n \leqslant k_2} n^{-\beta} \sum_{\delta \mid n} a_\delta \mu\left(\frac{n}{\delta}\right) = 1 - 2^{1-\beta}; \qquad (11,4,29)$$

его можно переписать в виде

$$\sum_{q \leqslant k_1 k} \frac{\mu(q)}{q^\beta} \sum_{m \leqslant \frac{k_1 k}{q}} \frac{a^m}{m^\beta} = 1 - 2^{1-\beta}. \qquad (11,4,30)$$

Здесь мы можем выделить $q > k_1$ и применить (11,4,28) и очевидную оценку $\left|\sum_{m \leqslant a} a_m\right| \leqslant 1$, рассуждая, как ранее. Тогда получим

$$L(\beta) F(\beta, k_2) = 1 - 2^{1-\beta} + Bk^{-0{,}005\varepsilon_1} \qquad (11,4,31)$$

или, учитывая (11,4,27),

$$L(\beta)F(\beta, k_2) = (1 - 2^{1-\beta})\left(\prod(\beta)\right) + Bk^{-0{,}001\varepsilon_1}, \quad (11,4,32)$$

$$\ln \prod(\beta) \ll (\ln k)^{0,8}. \quad (11,4,33)$$

Отсюда находим

$$\left.\begin{aligned} L(\beta)F(\beta, k_2) &> c'_{\varepsilon_1} e^{-c_1(\ln k)^{0,8}} \text{ при } \beta = 1 + 0{,}001\,\varepsilon_1, \\ L(\beta)F(\beta, k_2) &< -c''_{\varepsilon_1} - c_1(\ln k)^{0,8} \text{ при } \beta = 1 - 0{,}001\,\varepsilon_1. \end{aligned}\right\} \quad (11,4,34)$$

Но

$$F(\beta, k_2) = 1 - \frac{1}{2^\beta} + \frac{1}{3^\beta} - \ldots \pm \frac{1}{k_2^\beta} > 1 - \frac{1}{2^\beta} + \frac{B}{k_2^{\frac{1}{2}}} > \frac{1}{4}.$$

Таким образом, мы получаем весьма важные неравенства:

$$\left.\begin{aligned} L(\beta) &> c_{\varepsilon_1} e^{-c_1(\ln k)^{0,8}} \quad \text{при } \beta = 1 + 0{,}001\,\varepsilon_1, \\ L(\beta) &< -c_{\varepsilon_1} e^{-c_1(\ln k)^{0,8}} \text{при } \beta = 1 - 0{,}001\,\varepsilon_1. \end{aligned}\right\} \quad (11,4,35)$$

§ 5. II основная лемма. Завершение доказательства

Характер $\chi_k(n)$, *для которого имеем*

$$h(-k) < k^{\frac{1}{2}-\varepsilon_1}, \quad (11,4,6)$$

должен обладать свойством $\mathfrak{A}(\beta_1)$ *при* $\beta_1 = 1 - 0{,}08\,\varepsilon_1$.

Для доказательства *а* леммы предположим, что это не так. Тогда найдется $N \geqslant k^{100}$ такое, что для любого $x \in [\sqrt{N}, N]$ будем иметь

$$\left|\sum_{n \leqslant x} \chi_k(n)\mu(n)\right| \leqslant x^{1-0{,}08\varepsilon_1}. \quad (11,5,1)$$

Положим $x = N$. Способ «решета» приводит к равенству:

$$\sum_{q \leqslant N} \chi_k(q)\mu(q)q^{-\beta} \sum_{m \leqslant \frac{N}{q}} \chi_k(m)m^{-\beta} = 1. \quad (11,5,2)$$

Примем во внимание (11,4,22) и оценки

$$\sum_{N_1 \leqslant m \leqslant N_2} \chi_k(m)\, m^{-\beta} < \frac{k}{N_1^{\beta}}$$

для любого N_1. Тогда (11,5,1) и (11,5,2) дадут нам, по тому же способу, что § 4:

$$M(\beta) \sum_{m \leqslant \sqrt{N}} \frac{\chi_k(m)}{m^{\beta}} = 1 + BN^{-0.05\varepsilon_1}, \qquad (11,5,3)$$

где

$$M(\beta) = \sum_{q \leqslant \sqrt{N}} \chi_k(q)\, \mu(q)\, q^{-\beta}.$$

Далее, имеем

$$\sum_{k_1 \leqslant m \leqslant \sqrt{N}} \chi_k(m)\, m^{-\beta} = Bk^{-1},$$

так что

$$Q(\beta) = \sum_{m \leqslant \sqrt{N}} \frac{\chi_k(m)}{m^{\beta}} = L(\beta) + Bk^{-1}.$$

Отсюда, используя (11,4,35), получаем

$$\left.\begin{aligned} Q(\beta) &> \tfrac{1}{2}\, c_{\varepsilon_1}\, e^{-c_1 (\ln k)^{0,08}} \text{ при } \beta = 1 + 0{,}01\,\varepsilon_1, \\ Q(\beta) &< -\tfrac{1}{2}\, c_{\varepsilon_1}\, e^{-c_1 (\ln k)^{0,08}} \text{ при } \beta = 1 - 0{,}01\,\varepsilon_1. \end{aligned}\right\} \qquad (11,5,4)$$

Так как $Q(\beta)$ — непрерывная функция, то существует точка в интервале $[1 - 0{,}001\,\varepsilon_1,\ 1 + 0{,}001\,\varepsilon_1]$, где $Q(\beta) = 0$. Полагая в неравенстве (11,5,3) $\beta = \beta_0$, мы придем к абсурдному для больших k равенству, которое и доказывает II основную лемму.

Теперь можно доказать теорему Зигеля. Возьмем $\varepsilon_1 \in (0;\ 0{,}01)$. Если существует достаточно большое k, для которого

$$h(-k) < k^{\frac{1}{2} - \varepsilon_1},$$

то характер $\chi_k(n)$ по II основной лемме обладает свойством $\mathfrak{A}(1-0{,}08\,\varepsilon_1)$. Но тогда по I основной лемме имеем для достаточно больших D

$$h(-D) > D^{\frac{1}{2}-\eta(\beta)},$$

где

$$\eta(\beta) = 10{,}5 \cdot 0{,}08\,\varepsilon_1 + \eta_0 = 0{,}84\,\varepsilon_1 + \eta_0 < 0{,}85\,\varepsilon_1,$$

ибо η_0 может быть выбрано сколь угодно малым.

Итак, указанных k лишь конечное число, что требовалось доказать.

ГЛАВА 12

ТРАНСЦЕНДЕНТНОСТЬ НЕКОТОРЫХ КЛАССОВ ЧИСЕЛ

§ 1. Вспомогательные предложения*

Трансцендентность чисел вида e^{ω} при ω алгебраическом, $\omega \neq 0$, и чисел вида a^b, где $a \neq 0,1$ алгебраическое, b алгебраическое иррациональное, доказывается с помощью аналитических средств. Для чисел вида e^{ω} используются свойства интеграла от функций вида $z^k e^{\omega z}$, а для чисел вида a^b еще более тонкие аналитические свойства функции a^{bz}.

Мы приведем здесь доказательство трансцендентности чисел вида e^{ω} и a^b в случае, когда ω действительно и соответственно действительны $a > 0$ и b при прежних условиях их алгебраичности, использующее в своей аналитической части только теорему Ролля. Нам в дальнейшем понадобятся две хорошо известные леммы из анализа, доказательства которых мы ввиду их краткости приведем.

Лемма 1. *Если все числа $a_{k,s}$ действительны, отличны от нуля в совокупности, числа $\alpha_0, \ldots, \alpha_n$ действительны и различны, то число действительных нулей функции $f_n(x)$,*

$$f_n(x) = \sum_{k=0}^{n} e^{\alpha_k x} \sum_{s=0}^{p_k - 1} a_{k,s} x^s, \quad a_{k,p_k-1} \neq 0 \ (0 \leqslant k \leqslant n), \quad (12,1,1)$$

не превышает $N_n = \sum_{k=0}^{n} p_k - 1$.

Действительно, допустим, что лемма верна для $n < q - 1$. Допустим, что число нулей некоторой функции $f_q(x)$ превы-

шает число N_q нашей леммы. Тогда число нулей функции

$$\frac{d^{p_0}}{dx^{p_0}} e^{-\alpha_0 x} f_q(x) = \sum_{k=1}^{q} e^{(\alpha_k - \alpha_0)x} \sum_{s=0}^{p_k - 1} b_{k,s} x^s = f_{q-1}(x)$$

превышает число $N_{q-1} = \sum_{1}^{q} p_k - 1$ по известной теореме Ролля. Мы приходим к противоречию с нашим предположением, которое при $q = 0$ есть очевидное следствие основной теоремы алгебры. Лемма доказана.

Лемма 2. *Если число нулей действительной функции $f(x)$ не меньше q на интервале $[a, b]$ и $f(x)$ непрерывна вместе со всеми своими производными до q-й включительно, то при $a \leqslant x \leqslant b$ имеют место неравенства*

$$|f^{(\nu)}(x)| \leqslant \frac{(b-a)^{q-\nu}}{(q-\nu)!} \max_{a \leqslant y \leqslant b} |f^{(q)}(y)| \quad (\nu < q). \quad (12,1,2)$$

Действительно, если $f(x)$ имеет q нулей на (a, b), то $f^{(\nu)}(x)$ имеет по крайней мере $q - \nu$ нулей на (a, b). Допустим, что это будут нули $x_1, \ldots, x_{q-\nu}$, причем каждый нуль повторяется столько раз, какова его кратность. Тогда рассмотрим функцию

$$F(y) = f^{(\nu)}(y) - \lambda \prod_{k=1}^{q-\nu} (y - x_k), \qquad \lambda = \frac{f^{(\nu)}(x)}{(x - x_1) \ldots (x - x_{q-\nu})},$$

$$x = x_k \quad (a \leqslant x \leqslant b).$$

Эта функция имеет на (a, b) уже $q - \nu + 1$ нуль. Значит, по теореме Ролля, существует такое ξ $(a \leqslant \xi \leqslant b)$, что $F^{(q-\nu)}(y)$ имеет при этом ξ нуль на (a, b); другими словами, что

$$F^{(q-\nu)}(\xi) = 0 = f^{(q)}(\xi) - \lambda (q - \nu)!,$$

откуда

$$|f^{(\nu)}(x)| = \frac{|f^{(q)}(\xi)|}{(q-\nu)!} (b-a)^{q-\nu} \leqslant \frac{(b-a)^{q-\nu}}{(q-\nu)!} \max_{a \leqslant y \leqslant b} |f^{(q)}(\xi)|.$$

Прямым следствием леммы 2 является следующая лемма.

Лемма 3. *Если p и q — достаточно большие целые числа, $f(x)$ удовлетворяет условиям*

$$\left.\begin{aligned} f(x) &= \sum_{k=0}^{n} e^{\alpha_k x} \sum_{s=0}^{p_k-1} a_{k,s} x^s, \quad n \leqslant p^2, \quad p_k \leqslant p, \\ |a_{k,s}| &\leqslant e^{\theta_0 p}, \quad |\alpha_n| \leqslant \theta_0 p, \quad 0 \leqslant k \leqslant n, \quad 0 \leqslant s \leqslant p, \end{aligned}\right\} \quad (12,1,3)$$

где θ_0 не зависит от p, и если $f(x)$ имеет на интервале $(0, \sqrt{p})$ не менее $q > \theta p^2$ нулей, $\theta > 0$ не зависит от p и q, то должны выполняться неравенства

$$|f^{(\nu)}(x)| < e^{-\frac{1}{2} q \ln p + \gamma_0 q}, \quad \nu < \frac{q}{\ln p}, \quad 0 \leqslant x \leqslant \sqrt{p}, \quad (12,1,4)$$

где γ_0 от p и q не зависит.

Действительно, по лемме 2 имеем, что

$$|f^{(\nu)}(x)| < \frac{p^{\frac{q-\nu}{2}}}{(q-\nu)!} \max |f^{(q)}(x)| <$$

$$< e^{\frac{1}{2} q \ln p - 2 q \ln p + O(q)} \cdot p^3 e^{\theta q} p^q < e^{-\frac{1}{2} q \ln p + \gamma_0 q},$$

$$\nu < \frac{q}{\ln p}, \quad 0 \leqslant x \leqslant \sqrt{p},$$

где γ_0 от p и q не зависит.

Приведем теперь хорошо известную лемму из теории алгебраических чисел.

Лемма 4. *Если α_1, α_2, α_3 — алгебраические числа, A_{k_1, k_2, k_3} — целые, $|A_{k_1, k_2, k_3}| < e^{\gamma_1 p^2}$, где γ_1 от p не зависит, то или*

$$|N| = \left| \sum_{k_1=1}^{p^2} \sum_{k_2=1}^{p^2} \sum_{k_3=1}^{p^2} A_{k_1, k_2, k_3} \alpha_1^{k_1} \alpha_2^{k_2} \alpha_3^{k_3} \right| > e^{-\gamma_2 p^2}, \quad (12,1,5)$$

где γ_2 от p не зависит, или $N = 0$.

Действительно, если α_1, α_2, α_3 — алгебраические, то существует такое целое a, что $a\alpha_1$, $a\alpha_2$, $a\alpha_3$ будут целыми алгебраическими числами приведенного поля R степени ν. Тогда $N_1 = a^{3p^2} N$ будет целым числом этого поля. Если N_1 — не нуль, то все его сопряженные $N_1^{(k)}$ удовлетворяют неравенствам $|N_1^{(k)}| < e^{\gamma' p^2}$, где γ' от p не зависит, а число

$\prod_1^{\circ} N_1^{(k)}$ будет целым рациональным, отличным от нуля. Отсюда и следует неравенство нашей леммы.

Лемма 5. *Если* $a_{k,n}\,(1 \leqslant k \leqslant q,\ 1 \leqslant n \leqslant p,\ q \geqslant 2p)$ — *целые рациональные,* $|a_{k,n}| \leqslant a$, *то можно найти целые рациональные числа* $x_1, \ldots, x_q$, *в совокупности отличные от нуля, такие, что*

$$\sum_{k=1}^{q} a_{k,n} x_k = 0 \ (n = 1, \ldots, p), \qquad (12,1,6)$$

причем $|x_k|\,(1 \leqslant k \leqslant q)$ *ограничены неравенствами*

$$|x_k| \leqslant x = 3aq. \qquad (12,1,7)$$

Действительно, рассмотрим линейные формы от q переменных x_k

$$L_n = \sum_1^q a_{k,n} x_k \qquad (1 \leqslant n \leqslant p).$$

В p-мерном евклидовом пространстве на осях декартовой системы координат мы будем откладывать значения наших форм $L_1, \ldots, L_p$ при x_k, пробегающих независимо друг от друга целые значения из интервала $[0, 3qa]$. Все полученные таким образом $(3aq+1)^q$ точки $L_1, \ldots, L_p$ попадут в p-мерный куб $-3a^2q^2 \leqslant y_k \leqslant 3a^2q^2$ объема $(6q^2a^2)^p$. Но при условии $q \geqslant 2p$

$$(6a^2q^2)^p < (3qa)^q.$$

Значит, число полученных нами точек с целочисленными координатами $(L_1, \ldots, L_p)$ больше объема p-мерного куба, в котором они должны лежать. Другими словами, существуют два различных набора целых чисел $x_1, \ldots, x_q$ и $x_1', \ldots, x_q'$ таких, что

$$\sum_{k=1}^{q} a_{k,n} x_k = \sum_{k=1}^{q} a_{k,n} x_k'; \qquad \sum_{k=1}^{q} a_{k,n} (x_k - x_k') = 0 \ (1 \leqslant n \leqslant p).$$

Так как $|x_k - x_k'| < 3aq$, то наша лемма доказана ввиду того, что числа $x_k - x_k'$ в совокупности отличны от нуля.

§ 2. Общие теоремы о трансцендентности e^{ω} и α^{β} при алгебраических и действительных ω, α, β

Наши леммы позволяют доказать следующие теоремы.

Теорема 12. 2. 1. *Если* $\omega \neq 0$ *— действительное и алгебраическое, то число* e^{ω} *не алгебраическое.*

Рассмотрим функцию

$$f(x)=\sum_{n=0}^{p}\sum_{k=0}^{p} C_{k,n}x^k e^{\omega n x}$$

и допустим, что $e^{\omega}=\omega_1$ — алгебраическое, вместе с ω, число. Возьмем производную порядка ν от $f(x)$, $\nu \leqslant \frac{p^2}{\ln p}$ в точке $x=s\,(0 \leqslant s \leqslant \ln^2 p)$. Тогда

$$f^{(\nu)}(s)=\sum_{n=0}^{p}\sum_{k=0}^{p} C_{k,n}\sum_{m=0}^{\nu}\frac{\nu!\,k!\,n^{\nu-m}s^{k-m}}{m!\,(\nu-m)!\,(k-m)!}\,\omega^{\nu-m}e^{\omega n s}.$$

Далее, если α — целое алгебраическое число степени r, то

$$\alpha^r=\sum_{k=1}^{r} b_k\alpha^{r-k},\quad \alpha^N=\sum_{k=1}^{r} B_{k,N}\alpha^{r-k}, \tag{12,2,1}$$

где b_k и $B_{k,N}$ — целые числа.

Для определения и оценки чисел $B_{k,N}$ воспользуемся тем, что уравнение степени r для α неприводимо, откуда следует, что все числа $\alpha_2, \alpha_3, \ldots, \alpha_r$ сопряженные $\alpha=\alpha_1$ между собой различны и для определения $B_{k,N}$ имеется система уравнений

$$\sum_{k=1}^{r} B_{k,N}\alpha_s^{r-k}=\alpha_s^N\ (s=1,\ldots,r).$$

Детерминант этой системы Δ есть детерминант Вандермонда, отличный от нуля. Поэтому

$$|B_{k,N}|<\Big|\sum_{s=1}^{r} C_s\alpha_s^N\Big|\,e^{\gamma N},\ \gamma>0, \tag{12,2,2}$$

где γ зависит только от α.

Так как числа ω и $\omega_1=e^{\omega}$ алгебраические, то найдется целое число d такое, что числа $d\omega$ и $d\omega_1$ будут целыми

алгебраическими соответственно степеней r_1 и r_2. Поэтому имеют место соотношения

$$(d\omega)^N = \sum_{\nu=1}^{r_1} B_{\nu,N}(d\omega)^{r_1-\nu},$$

$$(d\omega_1)^N = \sum_{\nu=1}^{r_2} B'_{\nu,N}(d\omega_1)^{r_2-\nu}, \qquad (12,2.3)$$

где $B_{\nu,N}$ и $B'_{\nu,N}$ — целые и удовлетворяют неравенствам (12, 2, 2) со своими постоянными γ — γ_1 и γ_2 соответственно. Учитывая наибольшие возможные значения ν и s и пользуясь равенствами (12,2,3), мы получаем, что

$$d^{p^2}f^{(\nu)}(s) = \sum_{\nu_1=0}^{r_1-1}\sum_{\nu_2=0}^{r_2-1}\left[\sum_{k=0}^{p}\sum_{n=0}^{p} C_{k,n} D^{(\nu,s)}_{k,n,\nu_1,\nu_2}\right](d\omega)^{\nu_1}(d\omega_1)^{\nu_2},$$

$$|D^{(\nu,s)}_{k,n,\nu_1,\nu_2}| < e^{\theta p^2}, \qquad (12,2,4)$$

где $D^{(\nu,s)}_{k,n,\nu_1,\nu_2}$ — целые рациональные, а θ от p не зависит при $\nu \leqslant \frac{p^2}{\ln p}$, $s < \ln^2 p$.

С помощью леммы 5 числа C_{kn} можно выбрать целыми, отличными от нуля в совокупности, так, чтобы удовлетворялись уравнения

$$\sum_{k=0}^{p}\sum_{n=0}^{p} C_{k,n}D^{(\nu,s)}_{k,n,\nu_1,\nu_2} = 0, \quad 0 \leqslant \nu_1 \leqslant r_1 - 1, \quad 0 \leqslant \nu_2 \leqslant r_2 - 1,$$

$$0 \leqslant \nu \leqslant \left[\frac{p^2}{\ln p}\right], \qquad 0 \leqslant s \leqslant \left[\frac{\ln p}{2\nu_1\nu_2}\right], \qquad p > p_0,$$

причем $C_{k,n}$ будут также удовлетворять неравенствам

$$|C_{k,n}| < e^{\theta_0 p^2}, \qquad (12,2,5)$$

где θ — постоянная, взятая из неравенств (12,2,4). Выбрав таким образом целые числа $C_{k,n}$, мы получаем, что $f(x)$ удовлетворяет условиям

$$f(x) = \sum_{k=0}^{p}\sum_{n=0}^{p} C_{k,n}\, x^k\, e^{\omega n x}, \quad f^{(\nu)}(s) = 0,$$

$$|C_{k,n}| \leqslant e^{\theta p^2}, \quad 0 \leqslant \nu \leqslant \frac{p^2}{\ln p}, \quad 0 \leqslant s \leqslant \frac{\ln p}{2\nu_1\nu_2},$$

где $C_{k,n}$ — целые, отличные от нуля в совокупности, а θ от p не зависит. Значит, $f(x)$ имеет на интервале $0 \leqslant x \leqslant \ln^2 p$ не менее $\left[\frac{p^2}{2\nu_1\nu_2}\right]$ нулей. Поэтому $f(x)$ удовлетворяет всем условиям леммы 3. Следовательно,

$$\left|f^{(\nu)}(x)\right| < e^{-\frac{p^2 \ln p}{5\nu_1\nu_2} + \gamma_0 p^2}, \quad 0 \leqslant \nu \leqslant \frac{p^2}{\ln p}, \quad 0 \leqslant x \leqslant \ln^2 p. \quad (12,2,6)$$

Но числа

$$f^{(\nu)}(s), \quad 0 \leqslant \nu \leqslant \left[\frac{p^2}{\ln p}\right], \quad 0 \leqslant s \leqslant [\ln^2 p]$$

будут алгебраическими. По лемме 4 или $f^{(\nu)}(s) = 0$ или

$$f^{(\nu)}(s) > e^{-\gamma_2 p^2}, \quad (12,2,7)$$

где γ_2 от p не зависит, так как в нашем случае условия леммы 4 выполнены. Но при $p > p_1$ неравенства (12, 2, 6) придут в противоречие с неравенствами (12,2,7) и, значит, $f^{(\nu)}(s) = 0$ $\left(0 \leqslant \nu \leqslant \left[\frac{p^2}{\ln p}\right], \ 0 \leqslant s \leqslant \ln^2 p\right)$. Поэтому число действительных нулей $f(x)$ заведомо превышает $4p^2$, в то время как по лемме 1 оно не может быть больше $(p+1)^2$, $p > 2$. Это противоречие и доказывает невозможность одновременной алгебраичности чисел ω и e^{ω}.

Теорема 12.2.2. *Если $a \neq 1$ и $b \neq 1$ — действительные, положительные алгебраические числа, то число $\omega = \frac{\ln a}{\ln b}$, где берутся действительные ветви логарифмов, будет или рациональным, или трансцендентным числом.*

Следствия из теоремы 12.2.2. Положив $b = 10$, мы получаем, что десятичные логарифмы всех алгебраических чисел или рациональны, или трансцендентны. Если мы предположим, что $b^{\omega} = a$ при алгебраическом, действительном и иррациональном ω и алгебраическом положительном $b \neq 0,1$ будет алгебраическим числом, то придем к противоречию с утверждением нашей теоремы. Значит при выше сформулированных условиях b^{ω} всегда трансцендентно.

Доказательство теоремы 12.2.2. Схема доказательства этой теоремы ничем не отличается от схемы доказательства предшествующей.

Рассмотрим опять функцию

$$f(x)=\sum_{k=0}^{p}\sum_{n=0}^{p}C_{k,n}\,a^{kx}\,b^{nx},$$

где a и b удовлетворяют условиям нашей теоремы. Положим $\omega=\frac{\ln a}{\ln b}$ и допустим, что ω — алгебраическое иррациональное число. Пусть также d — целое, такое, что $d\omega$, da, db — целые алгебраические числа степеней r_1, r_2, r_3 соответственно. Тогда, в силу представлений (12, 2, 1) и неравенств (12, 2, 2), мы, будем иметь, что

$$\ln^{-\nu} bd^{p^2} f^{(\nu)}(s)=d^{p^2}\sum_{k=0}^{p}\sum_{n=0}^{p}C_{k,n}\,(k+n\omega)^{\nu}\,a^{ks}\,b^{ns}=$$

$$=\sum_{\nu_1=0}^{r_1-1}\sum_{\nu_2=0}^{r_2-1}\sum_{\nu_3=0}^{r_3-1}\left(\sum_{k=0}^{p}\sum_{n=0}^{p}C_{k,n}\,D^{(\nu,s)}_{k,n,\nu_1,\,\nu_2,\,\nu_3}\right)(d\omega)^{\nu_1}(da)^{\nu_2}(db)^{\nu_3},$$

$$\left|D^{(\nu,s)}_{k,n,\nu_1,\,\nu_2,\,\nu_3}\right|<e^{\theta p^2},\ 0\leqslant\nu\leqslant\frac{p^2}{\ln p},\ 0\leqslant s\leqslant\ln^2 p,\quad(12,2,8)$$

причем все числа $D^{(\nu,s)}_{k,n,\nu_1,\,\nu_2,\,\nu_3}$ — целые рациональные, а θ от p не зависит.

По лемме 5 числа $C_{k,n}$ можно выбрать целыми рациональными, отличными от нуля в совокупности и такими, что

$$\sum_{k=0}^{p}\sum_{n=0}^{p}C_{k,n}\,D^{(\nu,s)}_{k,n,\nu_1,\,\nu_2,\,\nu_3}=0,\quad|C_{k,n}|<e^{\vartheta\theta p^2},$$

$$0\leqslant n\leqslant p,\quad 0\leqslant k\leqslant p,\quad 0\leqslant\nu_1\leqslant r_1-1,$$

$$0\leqslant\nu_2\leqslant r_2-1,\quad 0\leqslant\nu_3\leqslant r_3-1,$$

$$0\leqslant s\leqslant\left[\frac{p^2}{\ln p}\right],\quad 0\leqslant s\leqslant\left[\frac{\ln p}{2r_1r_2r_3}\right],\quad p>p_1,$$

где θ от p не зависит и взята из неравенств (12, 2, 8). Выбрав таким образом $C_{k,n}$, мы видим, что для функции $f(x)$ выполняются условия

$$f^{(\nu)}(s)=0;\ 0\leqslant\nu\leqslant\left[\frac{p^2}{\ln p}\right],\quad 0\leqslant s\leqslant\left[\frac{\ln p}{2r_1r_2r_3}\right],\quad p>p_1.$$

По лемме 3, условия которой для нашей функции выполняются, мы будем иметь, так как в нашем случае $q > \frac{p^2}{2r_1r_2r_3}$, что

$$|f^{(\nu)}(s)| < e^{-\frac{1}{5r_1r_2r_3}p^2\ln p}, 0 \leqslant \nu \leqslant \frac{p^2}{\ln p}, \quad 0 \leqslant s \leqslant \ln^2 p, \quad p > p_1. \qquad (12,2,9)$$

Но по лемме 4, условия которой в нашем случае также выполняются, или $f^{(\nu)}(s) = 0$ (s — целое), или

$$|f^{(\nu)}(s)| > e^{-\gamma p^2}, \quad 0 \leqslant \nu \leqslant \left[\frac{p^2}{\ln p}\right], \quad 0 \leqslant s \leqslant [\ln^2 p]. \qquad (12,2,10)$$

Но при $p > p_2$ условия (12, 2, 9) и (12, 2, 10) противоречат друг другу и, следовательно,

$$f^{(\nu)}(s) = 0, \quad \nu = 0,1,\ldots, \left[\frac{p^2}{\ln p}\right], \quad s = 0,1,\ldots,[\ln^2 p].$$

Значит, число действительных нулей $f(x)$ превышает $2p^2$, в то время как по лемме 1 оно не может быть больше $(p+1)^2$. Это противоречие и доказывает нашу теорему. В случае, когда ω и соответственно a и b — комплексные алгебраические числа, наиболее простыми будут доказательства, опирающиеся на теорию функций комплексного переменного. Добавляя еще одну интерполяционную лемму в действительной области, можно было бы дать, например, оценку отклонения $\frac{\ln a}{\ln b}$ от рациональной дроби $\frac{p}{q}$.

Но на этом мы не будем останавливаться.

ЛИТЕРАТУРА

1. Виноградов И. М., Избранные труды, Изд. АН СССР, М., 1952.
2. Виноградов И. М., Метод тригонометрических сумм в теории чисел, Тр. МИАН **23** (1947), 1 — 111.
3. Виноградов И. М., Основы теории чисел, Гостехиздат М.—Л., 1954, 1 — 180.
4. Виноградов И. М., Элементарное доказательство одной общей теоремы аналитической теории чисел, ИАН (6) **19** (1925), 785—796.
5. Виноградов И. М., Элементарное доказательство одной теоремы теории простых чисел, ИАН, сер. матем., **17** (1953), 3—12.
6. Вороной Г. Ф., Собрание сочинений, т. II, Изд. АН УССР, Киев, 1952.
7. Гельфонд А. О., Об арифметическом эквиваленте аналитичности L-ряда Дирихле на прямой $Rs = 1$, ИАН, сер. матем., **20** (1956), 145—166.
8. Емельянов Г. В., Об одной системе диофантовых уравнений, Учен. зап. ЛГУ, сер. матем., **19** (1950), 3—39.
9. Кубилюс И. П., Распределение простых чисел гауссова поля в секторах и контурах, Учен. зап. ЛГУ, сер. матем., **19** (1950), 40—52.
10. Кубилюс И. П., Линник Ю. В., Одна элементарная теорема теории простых чисел, УМН **11**:**2** (68), (1956), 191—192.
11. Линник Ю. В., Замечание о наименьшем квадратичном невычете, ДАН **36** (1942), 131—132.
12. Линник Ю. В., On Erdös's theorem on the addition of numerical sequlnces. Матем. сб. **10** (52), (1942), 67—78.
13. Линник Ю. В., О представлении больших чисел суммою семи кубов, Матем. сб. **12** (54), (1943), 220—224.
14. Линник Ю. В., О разложении больших чисел на семь кубов, ДАН **36** (1942), 179—180.
15. Линник Ю. В., Элементарное доказательство теоремы Зигеля на основе способа И. М. Виноградова, ИАН, сер. матем., **14** (1950), 327—342.
16. Линник Ю. В., Элементарное решение проблемы Варинга по методу Шнирельмана, Матем. сб. **12** (54), (1943), 225—230.
17. Линник Ю. В., Реньи А., О некоторых гипотезах теории характеров Дирихле, ИАН **11** (1947), 539—546.

18. Манин Ю. И., О сравнениях третьей степени по простому модулю, ИАН, сер. матем., **20** (1956), 673—678.
19. Марджанишвили К. К., Об одновременном представлении n чисел суммами полных первых, вторых... n-х степеней, ИАН, сер. матем. (1937), 609—631.
20. Марджанишвили К. К., Об одной задаче аддитивной теории чисел, ИАН, сер. матем., **4** (1940), 193—214.
21. Мороз Б. З., О распределении степенных вычетов и невычетов, Вестник ЛГУ, сер. матем., **19** (1961), 164—169.
22. Постников А. Г., Романов Н. П., Упрощение элементарного доказательства А. Сельберга асимптотического закона распределения простых чисел, УМН **X**, 4 (66), (1955), 75—87.
23. Сонин Н. Я., Об одном определенном интеграле, содержащем числовую функцию $[x]$, Варш. универс. изв. (1885).
24. Фридлендер В. Р., О наименьших степенных невычетах по простым модулям, Елабуга, Учен. зап. пед. ин-та **1** (1956), 5—55.
25. Чудановский И. В. Элементарное доказательство закона распределения простых чисел гауссова поля, Вестник ЛГУ **13** (1956), 43—62.
26. Харди Г. Г., Литтльвуд Дж., Полиа Г., Неравенства, ИЛ, 1948.
27. Хассе Г., Лекции по теории чисел, ИЛ, 1953.
28. Хинчин А. Я., Три жемчужины теории чисел, Физматгиз, 1948.
29. Хинчин А. Я., Цепные дроби, Физматгиз, 1949.
30. Шнирельман Л. Г., Об аддитивных свойствах чисел, Ростов н/Д, Изв. донец. политехн. ин-та **14**, 2—3 (1930), 3—28.
31. Шнирельман Л. Г., Простые числа, Гостехиздат, М.—Л. (1940), 1—59.
32. Artin E., Scherk P., On the sum of two sets of integers, Ann. of Math. (2), **44** (1943), 138—142.
33. Brun V., Le cridle d' Eratosphene et le thèoreme de Goldbach, Videnskaps-selskapet Skr. Mat., naturw. I, № 3 (1920).
34. Burgess D., The distribution of quadratic residues and non-residues, Mathematika, **4**, p. 2, № 8 (1957), 106—112.
35. Hasse H., Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, Abh. Math. Sem. Hamburg, **10** (1934), 325—348.
36. Davenport H., On the distribution of l-th power residues, Journ. of London Math. Soc. **7**, p. 2, № 26 (1932), 117—121.
37. Davenport H., On the distribution of quadratic residues (mod. p.), Journ. of London Math. Soc., **8** (1933), 46—52.
38. Erdös P., On the arithmetical density of the sum of two sequences one of which forms a basis for the integers, Acta Arithm., Warszawa, I (1936), 197—200.
39. Hardy G., On the expression of a number as the sum of two squares, Quarterly Journ. of Math. **46** (1915), 263—283.
40. Jarnik V., Über Gitterpunkte in mehrdimensionalen Ellipsoiden, Math. Zeitschr. **21** (1927), 154—160.
41. Landau E., Vorlesungen über der Zahlentheorie, Leipz. 1927.

42. Mann H. B., A proof of the fundamental theorem on the density of sums of sets of positive integers, Annals of Math. (2), **43** (1942), 523—527.
43. Pillai S., On Waring's problem. Journ. Indian Math. Soc. (2), **2** (1937), 213—214.
44. Salié H., Über den kleinsten positiven Nichtrest nach einer Primzahl, Math. Nachr., **3** (1949), 7—8.
45. Selberg A., On an elementary method in the theory of primes, Norske Vid. Selsk. Trondhejm **19**, № 18 (1947), 64—67.
46. Selberg A., In Elementary Proof of the Prime Number Theorem, Ann. Math. **50** (1949), 305—313.
47. Shapiro H. N., On Primes in Arithmetic Progressions. II, Ann. Math. **52** (1950), 231—243.
48. Siegel C. L., Über die Classenzahl quadratischen Körper, Acta Arithm. I (1936), 83—86.
49. Sierpinski I., Sur un problème du calcul des fonctions asymptotiques, Prace mat.-fis. **17** (1906).
50. Stöhr A., Wirsing E., Beispiele von wesentlichen Komponenten, die keine Basen sind, Journ. für die reine und ang. Math. **196** (1956), 96—98.
51. Weil A., Riemann hypothesis in function fields, Proc. Mat. Acad. of Sc. of USA **27** (1941), 345—347.