
ИЗДАТЕЛЬСТВО
МИР

DIE GRUNDLEHREN
DER MATHEMATISCHEN WISSENSCHAFTEN

Band 148

K. CHANDRASEKHARAN

INTRODUCTION TO ANALYTIC NUMBER THEORY

SPRINGER-VERLAG

Berlin Heidelberg New York 1968

К. ЧАНДРАСЕКХАРАН

ВВЕДЕНИЕ В АНАЛИТИЧЕСКУЮ ТЕОРИЮ ЧИСЕЛ

Перевод с английского
С. А. СТЕПАНОВА

Под редакцией
А. И. ВИНОГРАДОВА

ИЗДАТЕЛЬСТВО «МИР»
МОСКВА 1974

УДК 511

Книга известного индийского математика, президента Международного математического союза К. Чандрасекхарана посвящена систематическому изложению классических результатов аналитической теории чисел. Она не требует больших предварительных знаний и вводит читателя в широкий круг основных теоретико-числовых вопросов.

Книга написана с большим педагогическим мастерством, четко и сжато. Она будет полезна математикам различных специальностей, а также студентам университетов и пединститутов.

Редакция литературы по математическим наукам

Ч $\frac{20203-013}{041(01)-74}$ 13-74

ПРЕДИСЛОВИЕ К РУССКОМУ ИЗДАНИЮ

Эта книга предназначается для студентов старших курсов и призвана служить введением в ту простейшую область аналитической теории чисел, которая в основном восходит к знаменитой теореме Дирихле 1837 года о бесконечности множества простых чисел в арифметической прогрессии. Никакого предварительного знакомства с элементарной теорией чисел не предполагается.

Автор испытает чувство глубокого удовлетворения, если это русское издание, любезно подготовленное А. И. Виноградовым и С. А. Степановым, заинтересует студентов в Советском Союзе, который является родиной выдающихся специалистов по теории чисел.

21 марта 1973 г. *К. Чандрасекхаран*

ПРЕДИСЛОВИЕ

Эта книга возникла на основе курса лекций, прочитанных мною в Высшей технической школе в Цюрихе. Записи лекций, подготовленные в основном моими ассистентами, были опубликованы. Настоящая книга следует тому же общему плану, что и эти записи, однако и по стилю изложения (см., например, гл. III, V и VIII), и по степени подробностей они сильно различаются. Цель книги — познакомить неспециалистов с некоторыми основными результатами теории чисел, показать, как в теории чисел используются аналитические методы, и подготовить почву для последующего изучения более тонких вопросов. Книга опубликована в серии «Die Grundlehren der mathematischen Wissenschaften» благодаря интересу, проявленному к ней профессором Бено Экманом.

Я считаю своим долгом выразить признательность профессору Карлу Людвигу Зигелю, который прочитал рукопись и корректуру и сделал много ценных замечаний и предложений. Профессор Рагхаван Нарасимхан неоднократно помогал мне сделать изложение более ясным и доступным. Доктор Гарольд Даймонд прочитал корректуру и помог устранить некоторые неточности. Я считаю себя обязанным выразить им свою благодарность.

К. Ч.

ГЛАВА I

ТЕОРЕМА ЕДИНСТВЕННОСТИ РАЗЛОЖЕНИЯ НА ПРОСТЫЕ СОМНОЖИТЕЛИ

§ 1. Простые числа. Мы предполагаем известными *положительные целые числа* 1, 2, 3, ..., *отрицательные целые числа* —1, —2, —3, ... и *нуль*, который мы будем считать целым числом. Под *неотрицательными целыми числами* подразумеваются положительные целые вместе с нулем. Мы предполагаем известными также элементарные арифметические операции над целыми числами.

Мы говорим, что целое число a *делится* на целое $b \neq 0$, если существует такое целое c, что $a = bc$. При этом мы будем говорить, что b *делит* a, или b есть *делитель* a, и записывать это так: $b \mid a$. Мы будем также называть a *целым кратным* или просто *кратным* числа b. В случае когда b не делит a, мы будем писать $b \nmid a$. Легко проверить следующие свойства:

если $b \mid a$ и $a > 0$, $b > 0$, то $1 \leqslant b \leqslant a$;

если $b \mid a$ и $c \mid b$, то $c \mid a$;

если $b \mid a$ и $c \neq 0$, то $bc \mid ac$;

если $c \mid a$ и $c \mid b$, то $c \mid (ma + nb)$ при всех целых m и n.

Если заданы целые числа a и b, $b \neq 0$, то однозначно определяются такие целые числа q и r, что $a = bq + r$ и $0 \leqslant r < |b|$. Назовем q *частным*, а r *остатком* при делении a на b. Ясно, что если $b \mid a$, то $r = 0$.

Целое число $p > 1$ называется *простым*, если все его положительные делители исчерпываются числами 1 и p. Целые числа, бóльшие 1 и не являющиеся простыми, называются *составными*.

В этой главе мы докажем, что каждое целое число, большее 1, можно разложить в произведение простых чисел и что такое разложение *единственно* с точностью до порядка следования сомножителей. Кроме того, мы докажем, что существует бесконечно много простых чисел.

§ 2. Теорема единственности разложения на простые сомножители.

Теорема 1. *Каждое целое число n, большее единицы, разлагается в произведение простых чисел.*

Доказательство. Число n является или простым, или составным. В первом случае утверждение теоремы очевидно. Если n составное, то по определению существует такое целое число d, что $1<d<n$ и $d|n$. Пусть m — наименьшее из таких делителей. Покажем, что m должно быть простым числом. Если бы m не являлось простым, то можно было найти такое целое число k, что $1<k<m$ и $k|m$. Отсюда следовало бы, что $1<k<m$ и $k|n$, а это противоречит выбору m. Полученное противоречие показывает, что m действительно является простым числом, и мы обозначим его через p_1. Таким образом, мы можем считать, что $n=p_1r$, где $1<r<n$. Применяя те же рассуждения к числу r, мы получим, что $n=p_1p_2s$, где $p_2\geqslant p_1$ и $1\leqslant s<r<n$. Этот процесс оборвется после конечного числа шагов, так как между 1 и n имеется только конечное число целых чисел. В результате мы получим разложение

$$n=p_1p_2\ldots p_t, \text{ где } p_1\leqslant p_2\leqslant\ldots\leqslant p_t, \qquad (1)$$

и тем самым завершим доказательство теоремы.

Заметим сразу же, что если $n=ab$, то a и b не могут быть одновременно больше, чем $\sqrt{n}$. Отсюда следует, что любое составное целое n имеет простой делитель p, не превосходящий $\sqrt{n}$.

Объединяя в представлении (1) равные простые числа и меняя, если это необходимо, нумерацию, мы можем переписать равенство (1) в виде

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}, \qquad (2)$$

где $p_1<p_2<\ldots<p_k$ и $\alpha_i>0$ для $i=1, 2, \ldots, k$. Представление числа n в виде (2) мы назовем его *каноническим разложением.*

Теперь мы в состоянии доказать теорему единственности разложения на простые сомножители, которая называется также основной теоремой арифметики:

Теорема 2. *Каноническое разложение целого числа n, большего единицы, единственно.*

Мы дадим три доказательства этой теоремы. Первое доказательство использует только теорему 1. Второе связано с решением в целых числах линейных уравнений, а третье использует теорию *последовательностей Фарея.*

Первое доказательство теоремы 2. Каноническое разложение простого числа, очевидно, единственно.

Пусть некоторые положительные целые числа, бо́льшие 1, имеют два различных канонических разложения, и пусть N — *наименьшее* из таких чисел, причем

$$N=p_1p_2...p_k=q_1q_2...q_m.$$

Каждое p отличается от каждого q, так как любое простое, общее для обоих представлений, при делении N на него давало бы целое число $N'<N$, которое обладает тем же свойством, что и N, а это невозможно в силу выбора N. Мы можем предположить, что

$$p_1\leqslant p_2\leqslant...\leqslant p_k \text{ и } q_1\leqslant q_2\leqslant...\leqslant q_m.$$

Кроме того, поскольку $p_1\neq q_1$, мы можем считать, что $p_1<q_1$. Определим число

$$P=p_1q_2...q_m.$$

Из условий $p_1|P$ и $p_1|N$ следует, что $p_1|(N-P)$, где $N-P=(q_1-p_1)\,q_2...q_m>1$. Поэтому мы можем записать

$$N-P=p_1t_1...t_h, \tag{3}$$

где t_i, $i=1, 2, ..., h$, — простые числа. Если $q_1-p_1>1$, то мы можем также записать q_1-p_1 в виде произведения простых чисел:

$$q_1-p_1=r_1r_2...r_s.$$

Тогда мы получим другое представление $N-P$ в виде произведения простых чисел, а именно

$$N-P=r_1r_2...r_sq_2...q_m. \tag{4}$$

Мы видели, что ни одно p не равно какому-либо q. В частности, p_1 не равно никакому q. Далее, ясно, что $p_1\nmid(q_1-p_1)$, и тогда p_1 не равно никакому r, так что q_1-p_1 в разложении на простые сомножители не может содержать p_1. Таким образом, число $N-P$ имеет два различных разложения (3) и (4) на простые сомножите-

ли. То же самое справедливо и в случае, когда $q_1 - p_1 = 1$. Но $1 < N - P < N$, а это противоречит минимальности N. Следовательно, не существует целых чисел $n > 1$, имеющих более одного канонического разложения.

§ 3. Второе доказательство теоремы 2. Доказательство основывается на решении в целых числах некоторых линейных уравнений. Введем некоторые новые понятия.

Пусть a и b — целые числа, не равные одновременно нулю. Их *наибольший общий делитель*, который обозначается через (a, b), определяется как наибольшее положительное целое число, которое делит одновременно a и b. Если $(a, b) = 1$, то мы будем говорить, что a и b — *взаимно простые* целые числа. Мы покажем, что если $(a, b) = d$, то уравнение $ax + by = d$ разрешимо в целых числах x и y. Отсюда следует, что если p простое и $p \mid ab$, то $p \mid a$ или $p \mid b$. Из последнего факта в свою очередь вытекает теорема единственности разложения на простые сомножители.

Непустое множество целых чисел S, обладающее свойством

$$m \in S \text{ и } n \in S \Rightarrow m - n \in S,$$

называется *модулем*. Из определения следует, что если $m, n \in S$, то

$$0 = m - m \in S, \quad -n = 0 - n \in S, \quad m + n = m - (-n) \in S.$$

Другими словами, если $a \in S$, $b \in S$, то $ax + by \in S$ при любых целых x и y. Если модуль состоит только из нуля, мы будем называть его *тривиальным модулем*. Нетривиальный модуль содержит, очевидно, бесконечно много положительных и отрицательных целых чисел. Мы можем сказать даже несколько больше:

Теорема 3. *Каждый нетривиальный модуль S состоит из всех целых кратных некоторого положительного целого числа.*

Доказательство. Так как S — нетривиальный модуль, он содержит некоторые положительные целые числа. Пусть d — наименьшее такое целое число. Тогда S содержит все целые кратные числа d. Для того чтобы

показать, что ими исчерпываются все элементы S, возьмем любое $n \in S$. Мы можем представить n в виде $n = dk + c$, где k и c — целые и $0 \leqslant c < d$. Так как $d \in S$, то и $dk \in S$. Далее, поскольку $n \in S$, мы имеем $n - dk \in S$, так что $c \in S$. Но $c < d$, а d — наименьшее положительное целое в модуле S. Следовательно, $c = 0$ и n есть целое кратное числа d.

Отсюда мы получаем следующую теорему:

Теорема 4. *Для данных целых a и b модуль $S = \{ax + by\}$, где x и y — целые числа, представляет собой множество всех целых кратных числа $d = (a, b)$.*

Доказательство. Легко видеть, что множество S является модулем. Из теоремы 3 следует, что S есть множество всех целых кратных некоторого положительного числа e. Следовательно, e делит все элементы множества S; в частности, $e \mid a$ и $e \mid b$. Так как d есть *наибольший* общий делитель чисел a и b, то $e \leqslant d$. С другой стороны, $d \mid (ax + by)$ при всех x, y, так что d делит каждый элемент из S. В частности, $d \mid e$. Следовательно, $d \leqslant e$. Таким образом, $e = d$, что и доказывает теорему.

Ясно, кроме того, что справедлива следующая теорема:

Теорема 5. *Уравнение $ax + by = n$ разрешимо в целых числах x и y тогда и только тогда, когда $(a, b) \mid n$.*

Следствие 1. *Если $(a, b) = d$, то уравнение $ax + by = d$ разрешимо в целых числах x и y. Другими словами, наибольший общий делитель целых чисел a и b является их линейной комбинацией с целыми коэффициентами.*

Следствие 2. *Любой общий делитель целых чисел a и b делит (a, b).*

Из этих результатов теперь легко выводится

Теорема 6 (Евклид). *Если $a \mid bc$ и $(a, b) = 1$, то $a \mid c$.*

Доказательство. Так как $(a, b) = 1$, то существуют такие целые числа x и y, что $ax + by = 1$. Если мы умножим последнее равенство на c, то получим $acx + bcy =$

$=c$, и так как $a \mid bc$, то $a \mid (acx+bcy)$. Следовательно, $a \mid c$.

Следствие. *Если p — простое число и $p \mid \prod_{i=1}^{r} p_i$, где каждое p_i, $i=1, 2, \ldots, r$, также простое число, то $p=p_i$ по меньшей мере для одного i.*

Мы можем теперь дать

Второе доказательство теоремы 2. Предположим, что целое число N имеет два различных канонических разложения

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \ldots q_r^{\beta_r}.$$

Тогда $p_1 \mid q_1^{\beta_1} q_2^{\beta_2} \ldots q_r^{\beta_r}$ и, следовательно, в силу следствия теоремы 6 $p_1 = q_i$ для некоторого i, $1 \leqslant i \leqslant r$. Аналогично мы получаем, что каждое p равно некоторому q и каждое q равно некоторому p. Таким образом, $k=r$ и, так как оба разложения упорядочены по возрастанию сомножителей, мы имеем

$$p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k},$$

где $p_1 < p_2 < \ldots < p_k$. Покажем, что $\alpha_i = \beta_i$ для всех $i = 1, 2, \ldots, k$. Если бы мы имели, например, $\alpha_i > \beta_i$ для некоторого i, мы получили бы после деления на $p_i^{\beta_i}$ равенство

$$p_1^{\alpha_1} \ldots p_i^{\alpha_i - \beta_i} \ldots p_k^{\alpha_k} = p_1^{\beta_1} \ldots p_{i-1}^{\beta_{i-1}} p_{i+1}^{\beta_{i+1}} \ldots p_k^{\beta_k},$$

в котором левая часть делится на p_i, а правая нет, что невозможно. Аналогично невозможен и случай $\alpha_i < \beta_i$. Следовательно, $\alpha_i = \beta_i$ для всех i, и потому каноническое разложение единственно.

§ 4. Наибольший общий делитель и наименьшее общее кратное. С понятием наибольшего общего делителя целых чисел a и b, данным в § 3, тесно связано понятие наименьшего общего кратного.

Определение. *Наименьшее общее кратное* $\{a, b\}$ двух целых чисел a и b, где $ab \neq 0$, есть наименьшее положи-

тельное целое число, которое делится одновременно на a и b.

Соотношение между (a, b) и $\{a, b\}$, где $ab>0$, выражается тождеством

$$ab=(a, b)\cdot\{a, b\}. \tag{5}$$

Для доказательства рассмотрим целое число $\mu=ab/(a, b)$. Так как $(a, b)\mid b$, то μ есть целое кратное a. Подобным же образом μ есть целое кратное b. Тогда μ будет общим кратным a и b. Пусть ν — какое-либо другое общее целое кратное a и b. Рассмотрим число

$$\frac{\nu}{\mu}=\frac{\nu\cdot(a, b)}{ab}$$

Мы знаем, что $(a, b)=ax+by$ при некоторых целых x и y. В таком случае

$$\frac{\nu}{\mu}=\frac{\nu\cdot(ax+by)}{ab}=\frac{\nu x}{b}+\frac{\nu y}{a}.$$

Но ν/a и ν/b являются целыми числами и, следовательно, ν/μ также будет целым числом. Таким образом, любое общее целое кратное чисел a и b есть целое кратное числа μ. Значит, μ будет их наименьшим общим кратным и

$$\mu=\frac{ab}{(a, b)}=\{a, b\}.$$

Попутно мы показали, что наименьшее общее кратное a и b делит любое общее кратное этих чисел.

Если a — положительное целое, то мы можем записать, что

$$a=\prod p^{\alpha},\quad \alpha\geqslant 0,$$

где произведение распространяется на все простые числа, а α есть неотрицательные целые числа, которые, за исключением конечного числа значений p, равны нулю. Если простое число p *не* делит a, то соответствующий показатель α есть нуль. Подобным же образом мы имеем

$$b=\prod p^{\beta},\quad \beta\geqslant 0.$$

Легко видеть, что

$$(a, b)=\prod p^{\min[\alpha, \beta]},\quad \{a, b\}=\prod p^{\max[\alpha, \beta]}. \tag{6}$$

§ 5. Последовательности Фарея. Если h и k — целые числа и $k>0$, мы назовем h/k *дробью* с *числителем* h и *знаменателем* k. Дробь h/k называется *несократимой*, или *сокращенной*, если $(h, k)=1$. Дробь h/k называется *правильной*, если $0\leqslant h/k\leqslant 1$.

Последовательность Фарея порядка n, где n — положительное целое, — это последовательность F_n всех несократимых правильных дробей h/k, у которых $1\leqslant k\leqslant n$, расположенных в неубывающем порядке. Например, F_5 есть последовательность

$$\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}.$$

Члены последовательности Фарея какого-либо порядка называются *дробями Фарея*. Заметим, что каждое рациональное число m/n, такое, что $0\leqslant m/n\leqslant 1$, *равно* некоторой дроби Фарея.

Из теоремы единственности разложения на простые сомножители (теорема 2) следует, что несократимая дробь единственна. Другими словами, две равные между собой несократимые дроби должны совпадать. Однако мы *не* хотим использовать теорему 2 и поэтому должны допустить возможность того, что две дроби Фарея *могут* быть равны между собой, но не совпадают. В этом случае мы упорядочим их по возрастанию числителей. Следующая теорема фактически исключает такую возможность и подготавливает почву для третьего доказательства теоремы 2:

Теорема 7 (Фарей — Коши). *Если l/m непосредственно следует за h/k в последовательности Фарея F_N, то* $kl-hm=1$.

Доказательство. Непосредственной проверкой можно убедиться, что результат справедлив для F_N при $1\leqslant N\leqslant 5$. *Предположим*, что результат справедлив для F_N, и докажем его для F_{N+1}.

Пусть a/b — несократимая правильная дробь, *не* принадлежащая F_N. Тогда $b\geqslant N+1$ и дробь a/b должна лежать между некоторыми двумя последовательными дробями h/k и l/m в последовательности Фарея F_N,

скажем

$$\frac{h}{k} \leqslant \frac{a}{b} \leqslant \frac{l}{m},$$

где знак равенства допускается ввиду того, что единственность несократимой дроби *не* предполагается. Определим целые числа λ и μ следующим образом:

$$\lambda = ka - hb, \quad \mu = bl - am.$$

Тогда $\lambda \geqslant 0$, $\mu \geqslant 0$ и $\lambda + \mu > 0$, так как мы предположили, что теорема справедлива для последовательности F_N, которой принадлежат дроби h/k и l/m. Далее, по предположению индукции $kl - hm = 1$, и тогда

$$\lambda l + \mu h = kal - ham = a(kl - hm) = a.$$

Аналогично,

$$\lambda m + \mu k = b, \tag{7}$$

и поскольку $(a, b) = 1$, мы имеем $(\lambda, \mu) = 1$. Таким образом, если $h/k \leqslant a/b \leqslant l/m$, $(a, b) = 1$, то

$$\frac{a}{b} = \frac{\lambda l + \mu h}{\lambda m + \mu k}, \quad \lambda \geqslant 0, \ \mu \geqslant 0, \ \lambda + \mu > 0, \ (\lambda, \mu) = 1.$$

Обратно, если λ и μ — целые числа, такие, что $\lambda \geqslant 0$, $\mu \geqslant 0$, $\lambda + \mu > 0$, $(\lambda, \mu) = 1$, и мы *определим* a и b равенствами $a = \lambda l + \mu h$, $b = \lambda m + \mu k$, то *однозначно* $\lambda = ka - hb$, $\mu = bl - am$ и $(a, b) = 1$, так что дробь a/b несократима. Кроме того, из равенства $kl - hm = 1$ следует, что $h/k \leqslant a/b \leqslant l/m$. Таким образом, a/b принадлежит F_M для некоторого M.

Так как $k > 0$, $m > 0$, $(\lambda, \mu) = 1$, то мы видим также, что $b \leqslant m + k$ только в трех случаях $\lambda, \mu = 0, 1$; $1, 1$; $1, 0$, которые приводят соответственно к значениям $a, b = h, k$; $l + h, m + k$; l, m. Далее, $\lambda \neq 0$. Действительно, если бы $\lambda = 0$, то дробь $a/b = (\mu h)/(\mu k)$ *не* была бы несократимой, за исключением случая $\mu = 1$. В последнем же случае, согласно равенству (7), мы имели бы $b = k$, что противоречит предположению о том, что $b \geqslant N + 1 > k$. Подобным же образом $\mu \neq 0$. Следовательно, $b \leqslant m + k$, только если $\lambda = \mu = 1$. Мы имеем $b \geqslant N + 1$, и если

$(a/b)\in F_{N+1}$, то $b=N+1$. Далее, поскольку h/k и l/m являются последовательными членами в F_N,

$$\frac{l+h}{m+k}\notin F_N,$$

и потому $m+k\geqslant N+1$. Отсюда вытекает, что если $b=N+1$, то $\lambda=1$ и $\mu=1$. Следовательно,

$$\frac{a}{b}\in F_{N+1}\Rightarrow a=h+l,\ b=k+m,\ \frac{a}{b}=\frac{h+l}{k+m}$$

и дробь a/b, очевидно, удовлетворяет теореме относительно соседних дробей h/k и l/m, так как по предположению индукции для F_N мы имеем $kl-hm=1$. Таким образом, если теорема справедлива для F_N, то она справедлива и для F_{N+1}, и поскольку теорема справедлива для F_1, то она справедлива для всех F_n.

Из теоремы 7 следует, что несократимая дробь единственна.

Определение. Дробь $(h+l)/(k+m)$ называется *медиантой* дробей h/k и l/m.

При доказательстве теоремы 7 мы показали неявным образом, что медианта двух дробей Фарея снова является дробью Фарея, а также доказали следующий результат:

Теорема 8. *Дроби, принадлежащие F_{N+1}, но не принадлежащие F_N, являются медиантами соседних дробей из F_N.*

Из теоремы 7 вытекают также следующие утверждения:

Теорема 9. *Если h/k, h''/k'', h'/k' — последовательные дроби некоторой последовательности Фарея, то $h''/k''=(h+h')/(k+k')$.*

Доказательство. По теореме 7 мы имеем $kh''-hk''=1$ и $k''h'-h''k'=1$; вычитая одно равенство из другого, мы получаем требуемое утверждение.

Теорема 10. *Если h/k и l/m — две последовательные дроби в последовательности Фарея F_N, то $k+m\geqslant N+1$.*

Доказательство. Так как

$$\frac{h}{k} < \frac{h+l}{k+m} < \frac{l}{m},$$

то медианта h/k и l/m не принадлежит F_N. Следовательно, $k+m>N$.

Наконец, мы докажем следующую теорему:

Теорема 11. *Если $N>1$, то в F_N нет двух последовательных дробей с одним и тем же знаменателем.*

Доказательство. Пусть $k>1$. Если h'/k непосредственно следует за h/k в F_N, то $h+1\leqslant h'<k$, и мы имели бы

$$\frac{h}{k} < \frac{h}{k-1} < \frac{h+1}{k} \leqslant \frac{h'}{k}.$$

Таким образом, $h/(k-1)$ будет лежать между h/k и h'/k в последовательности F_N, что противоречит нашему предположению о дробях h/k и h'/k.

Третье доказательство теоремы 2. Мы можем использовать теперь наши знания о последовательностях Фарея для доказательства того, что уравнение $ax+by=1$, где $(a, b)=1$, разрешимо в целых числах x, y. Как мы уже видели, отсюда следует справедливость теоремы 2.

Так как утверждение очевидно, если $ab=0$ или $a=b$, предположим, что $b>a>0$ и $(a, b)=1$. Рассмотрим дробь a/b. Мы можем считать ее членом некоторой последовательности Фарея, например F_b. Пусть дробь a/b непосредственно следует за h/k в этой последовательности. Тогда по теореме 7 имеем $ka-hb=1$, так что $x=k$ и $y=-h$ дают решение уравнения $ax+by=1$.

§ 6. Бесконечность множества простых чисел. Мы получили три различных доказательства теоремы единственности разложения на простые сомножители. Докажем теперь, что простых чисел бесконечно много.

Теорема 12 (Евклид). *Существует бесконечно много простых чисел.*

Мы дадим два различных доказательства этой теоремы. Первое доказательство принадлежит Евклиду, а второе — Г. Пойа. Третье доказательство, принадлежащее Эйлеру, будет дано в гл. VII, § 1.

Первое доказательство теоремы 12 (Евклид). Допустим, что $2, 3, 5, \ldots, p$—множество всех простых чисел и p—наибольшее из них. Рассмотрим целое число

$$q = (2 \cdot 3 \cdot 5 \ldots p) + 1.$$

Это число не делится ни на одно простое до p включительно. Но $q > 1$ и тогда q или само простое, бóльшее p, или оно делится на простое число, бóльшее p. В обоих случаях существует простое, бóльшее p. Следовательно, простых чисел бесконечно много.

Если через p_n мы обозначим n-е простое число, то из сказанного следует, что

$$p_m \Big| \prod_{i=1}^{n} p_i + 1$$

для некоторого $m > n$. Следовательно, $p_{n+1} \leqslant p_m \leqslant \prod_{i=1}^{n} p_i + 1 < p_n^n + 1$ при $n > 1$.

На самом деле с помощью подобных рассуждений мы можем доказать несколько больше, а именно что

$$p_n \leqslant 2^{2^{n-1}}, \quad n \geqslant 1,$$

причем $p_n < 2^{2^{n-1}}$ при $n > 1$. В самом деле, предположим, что

$$p_1 \leqslant 2, \quad p_2 \leqslant 2^2, \quad p_3 \leqslant 2^4, \ldots, p_n \leqslant 2^{2^{n-1}}.$$

Тогда

$$p_{n+1} \leqslant p_1 p_2 \ldots p_n + 1 \leqslant 2^{1+2+4+\ldots+2^{n-1}} + 1 < 2^{2^n},$$

и мы получаем требуемый результат с помощью индукции.

Доказательство Пойа теоремы 12 использует свойства *чисел Ферма*. Число Ферма f_n есть целое число вида

$f_n=2^{2^n}+1$, $n\geqslant 1$. Мы покажем, что теорема 12 является следствием следующей теоремы:

Теорема 13. (Пойа). *Любые два различных числа Ферма взаимно просты.*

Доказательство. Пусть f_n и $f_{n+k}(k>0)$ — два любых числа Ферма. Предположим, что m — такое положительное целое число, что $m|f_n$ и $m|f_{n+k}$. Полагая $x=2^{2^n}$, мы получаем

$$\frac{f_{n+k}-2}{f_n}=\frac{x^{2^k}-1}{x+1}=x^{2^k-1}-x^{2^k-2}+\ldots-1,$$

так что $f_n|(f_{n+k}-2)$. Отсюда следует, что $m|(f_{n+k}-2)$, и так как $m|f_{n+k}$, то $m|2$. Но числа Ферма нечетны. Следовательно, $m=1$ и доказательство теоремы 13 закончено.

Второе доказательство теоремы 12 (Пойа). Из теоремы 13 следует, что каждое из чисел Ферма $f_1, f_2, \ldots, f_n$ делится на нечетное простое число, которое не делит любое другое число Ферма. Следовательно, имеется по меньшей мере n нечетных простых чисел, не превосходящих f_n. Следовательно, простых чисел бесконечно много.

Далее, если мы рассмотрим $f_0=3$ при $n=0$, то, поскольку $p_1=2$ и поскольку имеется по меньшей мере n *нечетных* простых чисел, не превосходящих f_n для $n\geqslant 1$, мы получим, что $p_{n+2}\leqslant f_n$, где p_n означает n-е простое. Тогда

$$p_{n+2}\leqslant 2^{2^n}+1,$$

причем эта оценка лучше полученной ранее.

Ферма заметил, что числа

$$f_1=5,\ f_2=17,\ f_3=257,\ f_4=65537$$

являются простыми, и предположил, что все f_n также являются простыми. Однако это предположение было опровергнуто Эйлером, который показал, что f_5 делится на 641. Простое доказательство последнего факта, предложенное Г. Т. Беннетом, сводится к следующему:

$$f_5=2^{2^5}+1=2^{32}+1=(2\cdot 2^7)^4+1.$$

Положим $2^7=a$ и $5=b$. Тогда $f_5=(2a)^4+1=2^4a^4+1$. Далее, $2^4=1+3b$ или $2^4=1+b(a-b^3)$. Значит,

$$f_5=(1+ab-b^4)a^4+1=(1+ab)[a^4+(1-ab)(1+a^2b^2)]$$

и, следовательно, $1+ab\,(=641)$ делит f_5.

По-видимому, неизвестно, являются ли простыми какие-либо другие числа Ферма, за исключением первых четырех.

СРАВНЕНИЯ

§ 1. Классы вычетов. Пусть a, b, m — целые числа и $m>0$. Мы говорим, что *a сравнимо с b по модулю m*, если $m \mid (a-b)$. Это соотношение между a, b и m мы будем называть *сравнением* и обозначать символом $a \equiv b \pmod{m}$. Если $m \nmid (a-b)$, мы говорим, что a и b *не сравнимы по модулю m*, и записываем это следующим образом: $a \not\equiv b \pmod{m}$.

Отношение сравнимости является отношением эквивалентности. Действительно, оно рефлексивно, так как $a \equiv a \pmod{m}$; симметрично, поскольку из $a \equiv b \pmod{m}$ следует $b \equiv a \pmod{m}$, и транзитивно, так как из $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$ следует $a \equiv c \pmod{m}$.

Таким образом, отношение «$\equiv \pmod{m}$» разбивает множество целых чисел на непересекающиеся классы эквивалентности A, B, C, ..., причем два целых числа сравнимы друг с другом по модулю m тогда и только тогда, когда они лежат в одном и том же классе. Эти классы называются *классами вычетов* по модулю m.

Очевидно, что целые числа 0, 1, ..., $m-1$ лежат в разных классах вычетов. Так как каждое целое число n может быть записано в виде $n=qm+r$, $0 \leqslant r \leqslant m-1$, то каждое целое сравнимо по модулю m с одним из чисел 0, 1, ..., $m-1$. Следовательно, имеется точно m классов вычетов по модулю m и числа 0, 1, ..., $m-1$ образуют множество представителей этих классов.

Подобно обычным равенствам, сравнения можно складывать, вычитать и умножать. Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то мы имеем $a+c \equiv b+d \pmod{m}$, $a-c \equiv b-d \pmod{m}$ и $ac \equiv bd \pmod{m}$. Действительно, если $m \mid (a-b)$ и $m \mid (c-d)$, то $m \mid \{(a-b) \pm (c-d)\}$. Далее, $m \mid (a-b)c$, так что $ac \equiv bc \pmod{m}$ и $m \mid (c-d)b$, так что $bc \equiv bd \pmod{m}$, откуда по свойству транзитивности $ac \equiv bd \pmod{m}$.

В общем случае делить сравнения нельзя. Мы имеем $2 \equiv 12 \pmod{10}$, но $1 \not\equiv 6 \pmod{10}$.

Пусть A и B — два класса вычетов. Если a — произвольный элемент из A и b — произвольный элемент из B, то $a+b$ всегда лежит в одном и том же классе вычетов, который мы назовем *суммой* $A+B$. В таком же смысле мы будем использовать обозначения $A-B$ и $A\cdot B$ и говорить о *разности* и *произведении* двух классов вычетов.

Легко видеть, что классы вычетов по модулю m образуют относительно сложения абелеву группу. Нулевым элементом этой группы является класс, состоящий из всех целых кратных m, а обратным к классу A является класс A', состоящий из всех элементов класса A, взятых со знаком минус.

Сравнение

$$ax\equiv c\pmod m$$

эквивалентно линейному уравнению

$$ax-my=c,$$

которое по теореме 5 гл. I, если $(a, m)=1$, разрешимо в целых числах x, y. Решение указанного сравнения единственно, так как если

$$ax_1\equiv c\pmod m \quad\text{и}\quad ax_2\equiv c\pmod m,$$

то $a(x_1-x_2)\equiv 0\pmod m$, или $m\mid a(x_1-x_2)$. Но из условия $(a, m)=1$ следует, что $m\mid(x_1-x_2)$, или $x_1\equiv x_2\pmod m$.

Следовательно, если x_0, y_0 — частное решение линейного уравнения

$$ax+by=n,\quad (a, b)=1,$$

то общим решением будет $x=x_0-bt$, $y=y_0+at$, где t — любое целое число.

Только что полученный результат можно выразить иначе: если A, C и X — классы вычетов по модулю m, то уравнение $AX=C$ имеет единственное решение X при условии, что элементы класса A взаимно просты с m.

Классы вычетов по модулю m, элементы которых взаимно просты с m, мы назовем *приведенными классами вычетов* [1]. Они образуют абелеву группу относитель-

[1] В русской литературе приведены классы вычетов принято называть классами приведенной системы вычетов. — *Прим. перев.*

но умножения, единичным элементом которой будет класс, содержащий целое число 1. Каждый приведенный класс вычетов имеет обратный, так как если $(a, m)=1$, то существует целое a', такое, что $aa' \equiv 1 \pmod{m}$.

Рассмотрим аддитивную группу всех классов вычетов *по простому модулю p*. За исключением нулевого класса, все остальные классы вычетов в этом случае будут приведенными классами вычетов и, следовательно, образуют также мультипликативную абелеву группу. Дистрибутивный закон $A \cdot (B+C)=A \cdot B+A \cdot C$ непосредственно следует из дистрибутивного закона для целых чисел. Следовательно, справедлива следующая теорема:

Теорема 1. *Классы вычетов по простому модулю p образуют поле из p элементов.*

Системы вычетов. Из всех m классов вычетов по модулю m мы выделили *приведенные классы вычетов* по модулю m. *Полная система вычетов* по модулю m состоит из m представителей, взятых по одному из каждого класса. Следовательно, множество из m целых чисел образует полную систему вычетов по модулю m, если только его элементы попарно не сравнимы друг с другом по модулю m. С другой стороны, *полная приведенная система вычетов* по модулю m состоит из представителей, взятых по одному из каждого приведенного класса по модулю m.

Например, числа 0, 1, ..., 7 образуют полную систему вычетов (mod 8), в то время как 1, 3, 5, 7 образуют полную приведенную систему вычетов (mod 8).

Функция Эйлера φ. *Функция Эйлера* φ определяется для всех положительных целых чисел n следующим образом: значение $\varphi(n)$ равно количеству положительных целых чисел $\leqslant n$, которые взаимно просты с n.

Из определения следует, что значение $\varphi(n)$ равно также числу приведенных классов вычетов по модулю n.

§ 2. Теоремы Эйлера и Ферма. Если $a_1, a_2, \ldots, a_m$ составляют полную систему вычетов по модулю m и если k взаимно просто с m, то множество $ka_1, ka_2, \ldots, ka_m$ также будет полной системой вычетов по модулю m. Это

сразу же следует из того, что ka_1, ka_2, ..., ka_m попарно не сравнимы по модулю m.

Более общо, если $(k, m)=1$ и h — некоторое целое число, то множество ka_i+h, $i=1, 2, ..., m$, составляет полную систему вычетов по модулю m.

С другой стороны, если r_1, r_2, ..., $r_{\varphi(m)}$ есть приведенная система вычетов по модулю m и если $(a, m)=1$, то числа ar_1, ar_2, ..., $ar_{\varphi(m)}$ также образуют приведенную систему вычетов. Следовательно,

$$r_1 \cdot r_2 ... r_{\varphi(m)} \equiv ar_1 \cdot ar_2 ... ar_{\varphi(m)} \pmod m,$$

или

$$(a^{\varphi(m)}-1) r_1 \cdot r_2 ... r_{\varphi(m)} \equiv 0 \pmod m.$$

Так как r_1, r_2, ..., $r_{\varphi(m)}$ взаимно просты с m, то тем самым нами доказана

Теорема 2 (Эйлер). *Если* $(a, m)=1$, *то* $a^{\varphi(m)} \equiv 1 \pmod m$.

Частный случай этой теоремы, когда m простое, был открыт Ферма:

Теорема 3 (Ферма). *Если* p — *простое число и* $(a, p)=1$, *то* $a^{p-1} \equiv 1 \pmod p$.

Чтобы доказать важное свойство функции Эйлера, нам потребуется следующая теорема:

Теорема 4. *Пусть* $(m, m')=1$. *Если* a *пробегает полную систему вычетов по* $\bmod m$ *и* a' *пробегает полную систему вычетов по* $\bmod m'$, *то* $am'+a'm$ *пробегает полную систему вычетов по* $\bmod mm'$.

Доказательство. Мы имеем mm' целых чисел $am'+a'm$. Покажем, что они попарно не сравнимы по $\bmod mm'$. Пусть

$$a_1' m+a_1 m' \equiv a_2' m+a_2 m' \pmod{mm'}.$$

Тогда

$$a_1 m' = a_2 m' \pmod m,$$

откуда следует, поскольку $(m, m')=1$, что $a_1 \equiv a_2 \pmod m$. Аналогично, $a_1' \equiv a_2' \pmod{m'}$.

Определение. Комплекснозначная функция, определенная на множестве положительных целых чисел, называется *арифметической функцией.*

Арифметическая функция f называется *мультипликативной*, если

(i) f не равна тождественно нулю;

(ii) из $(m, n)=1$ следует, что $f(mn)=f(m)\cdot f(n)$.

Используя теорему 4, мы можем теперь доказать следующий результат:

Теорема 5. *Функция Эйлера* $\varphi(n)$ *мультипликативна.*

Доказательство. Так как $\varphi(1)=1$, то $\varphi(n)$ не равна тождественно нулю. Пусть $(m, m')=1$, и пусть a и a' пробегают полные системы вычетов по модулям m и m' соответственно. Тогда по теореме 4 $am'+a'm$ пробегает полную систему вычетов по $\bmod mm'$. Следовательно, $\varphi(mm')$ равна числу целых чисел вида $am'+a'm$, удовлетворяющих условию $(am'+a'm, mm')=1$. Но последнее условие эквивалентно следующим двум условиям:

$$(am'+a'm, m)=1 \quad \text{и} \quad (am'+a'm, m')=1,$$

или

$$(am', m)=1 \quad \text{и} \quad (a'm, m')=1,$$

или

$$(a, m)=1 \quad \text{и} \quad (a', m')=1.$$

Так как имеется $\varphi(m)$ значений a, для которых $(a, m)=1$, и $\varphi(m')$ значений a', для которых $(a', m')=1$, то имеется $\varphi(m)\varphi(m')$ значений $am'+a'm$, которые взаимно просты с mm'. Следовательно,

$$\varphi(mm')=\varphi(m)\cdot\varphi(m').$$

Из доказательства теоремы 5 вытекает следующее утверждение:

Теорема 5′. *Пусть* $(m, m')=1$. *Если* a *пробегает полную приведенную систему вычетов по* $\bmod m$ *и* a' *пробегает полную приведенную систему вычетов по* $\bmod m'$, *то* $am'+a'm$ *пробегает полную приведенную систему вычетов по* $\bmod mm'$.

Теорема 5 может быть использована для вычисления $\varphi(n)$. Каждое целое $n>1$ может быть записано в виде

$$n=\prod_{i=1}^{r} p_i^{\alpha_i},$$

так что

$$\varphi(n)=\prod_{i=1}^{r} \varphi\left(p_i^{\alpha_i}\right).$$

Следовательно, чтобы вычислить $\varphi(n)$, достаточно знать значения $\varphi(p^{\alpha})$ для всех простых чисел p. Очевидно, $\varphi(p)=p-1$. Если $\alpha>1$, рассмотрим полную систему вычетов по модулю p^{α}, а именно 1, 2, ..., p^{α}. Из этих чисел точно $p^{\alpha-1}$ не будут взаимно простыми с p^{α}, а именно кратные p числа p, $2p$, $3p$, ..., p^{α}. Следовательно,

$$\varphi(p^{\alpha})=p^{\alpha}-p^{\alpha-1}=p^{\alpha}\left(1-\frac{1}{p}\right).$$

Таким образом,

$$\varphi(n)=\prod_{i=1}^{r} \varphi\left(p_i^{\alpha_i}\right)=\prod_{i=1}^{r} p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right),$$

или

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

Другое важное свойство функции φ сформулировано в следующей теореме:

Теорема 6. $\sum\limits_{d\mid m}\varphi(d)=m.$

Доказательство. Пусть $m=\prod\limits_{i=1}^{r} p_i^{\alpha_i}$. Делители числа m имеют вид $\prod\limits_{i=1}^{r} p_i^{\beta_i}$, где $0\leqslant\beta_i\leqslant\alpha_i$. Следовательно, по теореме 5

$$\sum_{d|m} \varphi(d) = \sum_{\substack{(\beta_1,\ldots,\beta_r)\\ 0\leqslant\beta_k\leqslant\alpha_k}} \varphi\Big(\prod_{i=1}^{r} p_i^{\beta_i}\Big) = \sum_{\substack{(\beta_1,\ldots,\beta_r)\\ 0\leqslant\beta_k\leqslant\alpha_k}} \prod_{i=1}^{r} \varphi\big(p_i^{\beta_i}\big).$$

Отсюда после перегруппировки членов мы получаем

$$\sum_{d|n} \varphi(d) = \prod_{i=1}^{r} \sum_{\beta_i=0}^{\alpha_i} \varphi\big(p_i^{\beta_i}\big) =$$

$$= \prod_{i=1}^{r} \left[\varphi(1)+\varphi(p_i)+\ldots+\varphi\left(p_i^{\alpha_i}\right)\right] =$$

$$= \prod_{i=1}^{r} \left[1+(p_i-1)+p_i(p_i-1)+\ldots+p_i^{\alpha_i-1}(p_i-1)\right] =$$

$$= \prod_{i=1}^{r} p_i^{\alpha_i} = m.$$

§ 3. Число решений сравнения. Мы уже видели в этой главе, что если $(a, m)=1$, то линейное сравнение $ax\equiv c \pmod m$ разрешимо и имеет единственное решение. Поставим теперь вопрос о числе решений полиномиального сравнения

$$a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod p,$$

где a_0, a_1, ..., a_n — целые числа, $n>1$ и p — простое число.

Если x — какое-либо решение этого сравнения, то любое целое число, сравнимое с x по модулю p, также будет его решением. По этой причине, когда мы говорим о числе решений сравнения, мы имеем в виду число классов вычетов, элементы которых удовлетворяют данному сравнению. Следовательно, число решений равно числу удовлетворяющих сравнению представителей полной системы вычетов по mod p.

Полиномиальные сравнения могут иметь решения, а могут их не иметь. Например, сравнение $x^2\equiv 3 \pmod 7$ не имеет решений.

С другой стороны, по теореме Ферма (теорема 3) сравнение

$$x^{p-1} \equiv 1 \pmod{p}$$

имеет $p-1$ решений $x=1, 2, \ldots, p-1$.

Так как $x^{p-1} \equiv 1 \pmod{p}$, если $p \nmid x$, то мы имеем $x^p \equiv x \pmod{p}$ для *всех* x, $x^{p+1} \equiv x^2 \pmod{p}$ и т. д. Следовательно, любая степень, большая $p-1$, может быть редуцирована и можно считать, что $n < p$. Далее мы предположим, что $(a_0, p) = 1$. Это условие гарантирует, что степень сравнения в точности равна n.

Ответ на вопрос, поставленный в начале этого параграфа, дает

Теорема 7 (Лагранж). *Сравнение*

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 \pmod{p}, \quad (a_0, p) = 1, \qquad (2)$$

имеет не более n решений.

Доказательство. Докажем теорему индукцией по n. Для $n=1$ утверждение теоремы справедливо, поскольку $(a_0, p) = 1$. Предположим теперь, что теорема справедлива для $n-1$, и докажем ее справедливость для n. Если сравнение (2) не имеет решений, то доказывать нечего. Если же оно имеет решение, скажем x_1, то

$$a_0 x_1^n + a_1 x_1^{n-1} + \ldots + a_n \equiv 0 \pmod{p}. \qquad (3)$$

Вычитая из (2) сравнение (3), мы получим сравнение

$$a_0 (x^n - x_1^n) + a_1 (x^{n-1} - x_1^{n-1}) + \ldots + a_{n-1} (x - x_1) \equiv 0 \pmod{p}, \qquad (4)$$

которому, очевидно, удовлетворяет каждое решение сравнения (2). Далее, мы можем переписать (4) в виде

$$(x - x_1)(a_0 x^{n-1} + b_1 x^{n-2} + \ldots + b_{n-1}) \equiv 0 \pmod{p},$$

где $b_1, b_2, \ldots, b_{n-1}$ — целые числа, зависящие только от x_1 и $a_0, a_1, \ldots, a_{n-1}$. Следовательно, каждое решение сравнения (2) должно удовлетворять или сравнению

$$x - x_1 \equiv 0 \pmod{p},$$

которое дает исходное решение $x=x_1$, или сравнению

$$a_0x^{n-1}+b_1x^{n-2}+\ldots+b_{n-1}\equiv 0 \pmod{p}, \quad (a_0, p)=1,$$

которое имеет степень n—1 и по предположению индукции не более n—1 решений. В таком случае сравнение (2) может иметь самое большее n решений, что и требовалось доказать.

АППРОКСИМАЦИЯ ИРРАЦИОНАЛЬНЫХ ЧИСЕЛ РАЦИОНАЛЬНЫМИ И ТЕОРЕМА ГУРВИЦА

§ 1. Аппроксимация иррациональных чисел. Пусть ξ — действительное иррациональное число. Так как множество рациональных чисел плотно в множестве всех действительных чисел, то для данного $\varepsilon>0$ найдется такое рациональное число h/k, что $|\xi-h/k|<\varepsilon$. Наша задача состоит в изучении разности $|\xi-h/k|$ как функции от k.

Будем предполагать в дальнейшем, что $0<\xi<1$, дробь h/k несократима и $k>0$.

Теорема 1. *Если ξ — иррациональное число и N — положительное целое число, то существует рациональное число h/k со знаменателем $k\leqslant N$, такое, что*

$$\left|\xi-\frac{h}{k}\right|<\frac{1}{kN}.$$

Доказательство. Для любого действительного числа x обозначим через $[x]$ *целую часть* числа x, т. е. такое целое число m, что $m\leqslant x<m+1$. Из иррациональности ξ следует, что $0<n\xi-[n\xi]<1$. Пусть n принимает значения 1, 2, ..., N. Тогда мы получим N различных чисел $n\xi-[n\xi]$, каждое из которых лежит в открытом интервале $(0, 1)$. Рассмотрим N подинтервалов $\left(0, \frac{1}{N}\right)$, $\left(\frac{1}{N}, \frac{2}{N}\right), \ldots, \left(\frac{N-1}{N}, 1\right)$. Каждый из этих подинтервалов или содержит внутри себя точно одно из чисел $n\xi-[n\xi]$, или же существует подинтервал, содержащий более одного из этих чисел. В первом случае интервал $\left(0, \frac{1}{N}\right)$ содержит число $m\xi-[m\xi]$ при некотором целом m, таком, что $1\leqslant m\leqslant N$, и, следовательно, $0<m\xi-[m\xi]<\frac{1}{N}$. Таким образом, $0<\xi-\frac{[m\xi]}{m}<\frac{1}{mN}$,

и тем самым мы нашли рациональное число h/k, обладающее требуемым свойством.

Если подинтервал $\left(0, \frac{1}{N}\right)$ не содержит ни одно из чисел $n\xi-[n\xi]$, $1\leqslant n\leqslant N$, то существует другой подинтервал, содержащий по меньшей мере два таких числа, скажем $n\xi-[n\xi]$ и $m\xi-[m\xi]$. Тогда мы имеем два целых числа m и n, $0<m<n\leqslant N$, таких, что

$$|(n\xi-[n\xi])-(m\xi-[m\xi])|<\frac{1}{N},$$

или

$$|(n-m)\xi-([n\xi]-[m\xi])|<\frac{1}{N}.$$

Если мы положим $n-m=k$ и $[n\xi]-[m\xi]=h$, то снова получим

$$\left|\xi-\frac{h}{k}\right|<\frac{1}{kN},$$

где $k<N$.

Несколько более сильный результат дает

Теорема 2. *Если ξ — иррациональное число и N — положительное целое число, то существует рациональное число h/k со знаменателем $k\leqslant N$, такое, что*

$$\left|\xi-\frac{h}{k}\right|<\frac{1}{k(N+1)}.$$

Доказательство. Теорема может быть доказана таким же способом, что и теорема 1. Пусть $x_0=0$, x_1, ..., x_N, $x_{N+1}=1$ — набор различных чисел, состоящий из 0, 1 и чисел $n\xi-[n\xi]$, $n=1, 2, \ldots, N$, упорядоченных по возрастанию. Разности $x_{n+1}-x_n>0$ при $n=0, 1, \ldots, N$ иррациональны, и их сумма равна 1. Следовательно, хотя бы для одного значения n мы будем иметь $x_{n+1}-x_n<1/(N+1)$. Тогда существует рациональное число h/k, такое, что

$$\left|\xi-\frac{h}{k}\right|<\frac{1}{k(N+1)},$$

где $k\leqslant N$.

Другое доказательство теоремы 2 использует последовательности Фарея. Если F_N — последовательность Фарея порядка N, то, поскольку ξ иррационально, мы имеем $\xi \notin F_N$ при любом N. Но ξ лежит между двумя последовательными дробями a/b и c/d, принадлежащими F_N. Пусть $a/b<\xi<c/d$. Рассмотрим медианту $(a+c)/(b+d)$. Из гл. I мы знаем, что $a/b<(a+c)/(b+d)<c/d$. Следовательно, или $a/b<\xi<(a+c)/(b+d)$, или $(a+c)/(b+d)<\xi<c/d$. Так как a/b и c/d — последовательные члены в F_N, то $(a+c)/(b+d)\notin F_N$. Значит, $b+d\geqslant N+1$. Поэтому или

$$0<\xi-\frac{a}{b}<\frac{a+c}{b+d}-\frac{a}{b}=\frac{bc-ad}{b(b+d)}=\frac{1}{b(b+d)}\leqslant\frac{1}{b(N+1)},$$

или

$$0<\frac{c}{d}-\xi<\frac{c}{d}-\frac{a+c}{b+d}=\frac{bc-ad}{d(b+d)}=\frac{1}{d(b+d)}\leqslant\frac{1}{d(N+1)}.$$

Поскольку a/b и c/d принадлежат F_N, они несократимы и $b\leqslant N$, $d\leqslant N$. Тем самым мы получили требуемое рациональное приближение h/k (равное a/b или c/d).

Проверим теперь справедливость теоремы 2 в случае, когда ξ рационально, скажем, $\xi=l/m$, $(l, m)=1$ и $m>N$. Тогда $\xi\notin F_N$ и мы можем следовать данному выше доказательству, за исключением случая, когда $\xi=(a+c)/(b+d)$. В последнем случае мы не можем поставить в теореме знак строгого неравенства и, таким образом, получаем следующий результат:

Теорема 3. *Если ξ — рациональное число, N — положительное целое число и $\xi=l/m$, $(l, m)=1$, где $m>N$, то существует неприводимая дробь h/k со знаменателем $k\leqslant N$ такая, что*

$$\left|\frac{l}{m}-\frac{h}{k}\right|\leqslant\frac{1}{k(N+1)}.$$

Так как $N\geqslant k$, из теоремы 1 вытекает

Теорема 4. *Если ξ — иррациональное число, то существует бесконечно много рациональных чисел h/k, таких, что*

$$\left|\xi-\frac{h}{k}\right|<\frac{1}{k^2}.$$

Иногда мы будем выражать этот результат другими словами, говоря, что иррациональное число ξ аппроксимируется рациональными числами h/k с точностью до $1/k^2$.

Так как $\xi - h/k$ можно записать в виде $(\xi+n) - (h+kn)/k$, где n — целое число, то теоремы 1, 2, 3 и 4 будут справедливыми и без предположения $0<\xi<1$.

§ 2. Суммы двух квадратов. Теорему 3 можно использовать для доказательства того факта, что целые числа определенного вида представимы в виде суммы двух квадратов.

Теорема 5. *Пусть n и A — положительные целые числа и $n \mid (A^2+1)$. Тогда существуют такие целые числа s и t, что $n=s^2+t^2$.*

Доказательство. Случай $n=1$ тривиален. Предположим, что $n \geqslant 2$, и пусть $N=[\sqrt{n}]$. Ясно, что в этом случае $n>N$. Из условия $n \mid (A^2+1)$ следует, что $(n, A)=1$. Следовательно, A/n есть несократимая дробь со знаменателем $n>N$, и тогда по теореме 3 существует несократимая дробь r/s, такая, что

$$\left|\frac{A}{n}-\frac{r}{s}\right| \leqslant \frac{1}{s(N+1)}, \quad 0<s \leqslant N,$$

т. е.

$$|As-rn| \leqslant \frac{n}{N+1} = \frac{n}{[\sqrt{n}]+1} < \sqrt{n}.$$

Пусть $As-rn=t$. Тогда t является целым числом и $s^2+t^2=s^2+(As-rn)^2=s^2(A^2+1)-2Asrn+r^2n^2$. Поскольку n делит правую часть последнего равенства, мы имеем $n \mid (s^2+t^2)$. Кроме того, $0<s \leqslant N \leqslant \sqrt{n}$, $|t|<\sqrt{n}$, откуда $0<s^2+t^2<2n$. Следовательно, $n=s^2+t^2$, так что n действительно является суммой двух квадратов.

Легко видеть, кроме того, что $(s, t)=1$. Действительно, мы имеем $(s, t)=(s, As-rn)=(s, rn)$. Но дробь r/s несократима и, следовательно, $(r, s)=1$. Таким образом,

$(s, t) = (s, n)$. Кроме того, $n = s^2 + t^2$ и тогда

$$1 = \frac{s^2(A^2+1)}{n} - 2Asr + r^2 n.$$

Поскольку по предположению $(A^2+1)/n$ есть целое, любой общий делитель s и n должен делить 1. Следовательно, $(s, n) = 1 = (s, t)$.

Следствие. *Пусть n является положительным целым и $n \mid (A^2+B^2)$, где $(A, B) = 1$. Тогда существуют такие целые числа s и t, что $n = s^2 + t^2$.*

Доказательство. Воспользуемся тождеством

$$(A^2+B^2)(C^2+D^2) = (AD+BC)^2 + (AC-BD)^2.$$

Из гл. I нам известно, что для данных A и B с условием $(A, B) = 1$ можно найти такие целые числа C и D, что $AC - BD = 1$. Тогда мы получим

$$(A^2+B^2)(C^2+D^2) = (AD+BC)^2 + 1,$$

так что если $n \mid (A^2+B^2)$, то $n \mid \{(AD+BC)^2+1\}$. По теореме 5 мы получаем отсюда, что $n = s^2 + t^2$.

§ 3. Простые числа вида $4k \pm 1$. В гл. I мы привели доказательство Евклида бесконечности множества простых чисел. Каждое простое число, отличное от 2, нечетно, а любое нечетное число представляется или в виде $4k-1$, или в виде $4k+1$ с целым k. С помощью рассуждений, аналогичных рассуждениям Евклида, мы покажем, что каждая из этих последовательностей содержит бесконечно много простых чисел.

Теорема 6. *Существует бесконечно много простых чисел вида $4k-1$.*

Доказательство. Пусть $q_1, q_2, \ldots, q_r$ — первые r простых чисел вида $4k-1$. Положим $N = 4q_1 q_2 \ldots q_r - 1$ и заметим, что N есть нечетное число. Следовательно, все его делители имеют вид $4k-1$ или $4k+1$. Но N не может иметь в качестве делителей только числа вида $4k+1$, так как произведение двух чисел такого вида снова является числом того же вида, в то время как N имеет

вид $4k-1$. Следовательно, число N имеет простой делитель вида $4k-1$. Ясно, что N не делится на $q_1, q_2, \ldots, q_r$, и тогда указанный простой делитель должен быть больше q_r.

Теорема 7. *Существует бесконечно много простых чисел вида* $4k+1$.

Доказательство. Предположим, напротив, что простых чисел вида $4k+1$ конечное число и что $5, 13, \ldots, p$ — все эти простые числа, причем p — наибольшее из них. Положим

$$N=(2\cdot 5\cdot 13\ldots p)^2+1.$$

Число N нечетное и, следовательно, все его делители также будут нечетными. По теореме 5 каждый простой делитель q числа N представляется в виде $q=s^2+t^2$. Поскольку q нечетное, одно из чисел s и t должно быть четным, а другое нечетным. Тогда $q=s^2+t^2\equiv 1 \pmod 4$ и, следовательно, каждый простой делитель числа N должен иметь вид $4k+1$. Это приводит, однако, к противоречию, так как $N>1$ и не делится на любое из простых чисел $5, 13, \ldots, p$, которые по предположению исчерпывают все простые вида $4k+1$.

§ 4. Теорема Гурвица. Мы начнем с уточнения теоремы 4.

Теорема 8. *Если* ξ *— иррациональное число, то существует бесконечно много несократимых дробей* h/k, *таких, что*

$$\left|\xi-\frac{h}{k}\right|<\frac{1}{2k^2}.$$

Доказательство. Пусть F_N — последовательность Фарея порядка $N>1$. Тогда ξ лежит между некоторыми двумя последовательными дробями a/b и c/d этой последовательности, так что

$$\frac{a}{b}<\xi<\frac{c}{d}.$$

Мы докажем теорему, если покажем, что выполняется по крайней мере одно из неравенств

$$\xi - \frac{a}{b} < \frac{1}{2b^2}, \quad \frac{c}{d} - \xi < \frac{1}{2d^2}. \tag{1}$$

Предположим, что неравенства (1) не выполняются. Тогда, поскольку ξ иррационально,

$$\xi - \frac{a}{b} > \frac{1}{2b^2}, \quad \frac{c}{d} - \xi > \frac{1}{2d^2}. \tag{2}$$

Отсюда и из условия $bc-ad=1$ мы получаем $(b-d)^2<0$. Следовательно, или

$$\xi - \frac{a}{b} < \frac{1}{2b^2}, \text{ или } \frac{c}{d} - \xi < \frac{1}{2d^2}.$$

Таким образом, существует рациональная дробь h/k в F_N (равная a/b или c/d), такая, что

$$\left|\xi - \frac{h}{k}\right| < \frac{1}{2k^2}.$$

Поскольку $(c/d)-(a/b)=1/(bd)$, в силу выбора h/k мы имеем

$$\left|\xi - \frac{h}{k}\right| < \frac{1}{bd} \leqslant \frac{1}{b+d-1},$$

и так как по теореме 10 гл. I $b+d \geqslant N+1$, то

$$\left|\xi - \frac{h}{k}\right| \leqslant \frac{1}{N}.$$

Так как величину N можно менять по нашему усмотрению, мы заключаем отсюда, что имеется бесконечно много таких дробей h/k. Тем самым теорема доказана.

В теореме 4 мы показали, что любое иррациональное число с точностью до $1/k^2$ аппроксимируется бесконечным множеством рациональных чисел h/k. В теореме 8 эта аппроксимация была улучшена до $1/2k^2$. Естественным образом возникает вопрос о возможности дальнейшего улучшения последнего результата. А именно, существует ли число $c>2$, такое, что ξ можно с точностью до $1/ck^2$ аппроксимировать бесконечным множеством рациональных чисел h/k? Ответ на этот вопрос дает следующая теорема Гурвица:

Теорема 9 (Гурвиц). *Если ξ — иррациональное число и $c \leqslant \sqrt{5}$ — любое положительное действительное число, то существует бесконечно много рациональных чисел h/k, таких, что*

$$\left|\xi - \frac{h}{k}\right| < \frac{1}{ck^2}.$$

Если же $c > \sqrt{5}$, то существуют иррациональные числа ξ, для которых указанное неравенство выполняется только для конечного множества рациональных чисел h/k.

Доказательство (Хинчин). Пусть F_N — последовательность Фарея порядка $N > 1$ и h/k, h'/k' — соседние члены этой последовательности, такие, что $h/k < \xi < h'/k'$. Мы можем считать, что или

$$k' > \frac{\sqrt{5}+1}{2}k, \quad \text{или} \quad k' < \frac{\sqrt{5}-1}{2}k.$$

В самом деле, если

$$\frac{\sqrt{5}-1}{2}k < k' < \frac{\sqrt{5}+1}{2}k,$$

то

$$k + k' > \frac{\sqrt{5}+1}{2}\max(k, k')$$

и мы можем заменить F_N на F_M, $M = k+k'$, а одно из чисел h/k, h'/k' их медиантой $(h+h')/(k+k')$, так как $k(h+h') - h(k+k') = (k+k')h' - (h+h')k' = 1$ (см. теорему 7 гл. I).

Таким образом, если $k'/k = \omega$, то $\omega > (\sqrt{5}+1)/2$ или $\omega < (\sqrt{5}-1)/2$. В любом из этих случаев мы имеем $1 + \omega^{-2} > \sqrt{5}\,\omega^{-1}$, поскольку

$$\frac{1}{\sqrt{5}}\left(1 + \frac{1}{\omega^2}\right) - \frac{1}{\omega} =$$

$$= \frac{1}{\sqrt{5}\,\omega^2}\left(\omega - \frac{\sqrt{5}+1}{2}\right)\left(\omega - \frac{\sqrt{5}-1}{2}\right) > 0.$$

Следовательно,

$$\frac{1}{\sqrt{5}}\left(\frac{1}{k^2}+\frac{1}{k'^2}\right)=\frac{1}{\sqrt{5}k^2}\left(1+\frac{1}{\omega^2}\right)>\frac{1}{\omega k^2},$$

так что

$$\frac{h'}{k'}-\frac{h}{k}=\frac{1}{kk'}=\frac{1}{k^2\,\omega}<\frac{1}{\sqrt{5}}\left(\frac{1}{k^2}+\frac{1}{k'^2}\right),$$

откуда

$$\frac{h}{k}+\frac{1}{\sqrt{5}k^2}>\frac{h'}{k'}-\frac{1}{\sqrt{5}k'^2}.$$

Значит, один из открытых интервалов

$$\left(\frac{h}{k},\ \frac{h}{k}+\frac{1}{\sqrt{5}k^2}\right)\quad\text{или}\quad\left(\frac{h'}{k'}-\frac{1}{\sqrt{5}k'^2},\ \frac{h'}{k'}\right)$$

будет содержать точку ξ. Рассуждая так же, как в заключительной части доказательства теоремы 8, мы видим, что существует бесконечно много таких рациональных приближений. Этим первая часть теоремы доказана.

Для доказательства второй части предположим, что $c>\sqrt{5}$, и рассмотрим иррациональное число $\xi=\frac{1}{2}(1+\sqrt{5})$. Покажем, что для этого ξ имеется только конечное число дробей h/k, удовлетворяющих неравенству

$$\left|\xi-\frac{h}{k}\right|<\frac{1}{ck^2}. \tag{3}$$

Пусть $c=\sqrt{5}/\alpha$, где $0<\alpha<1$. Предположим, что

$$\left|\frac{h}{k}-\frac{\sqrt{5}+1}{2}\right|<\frac{\alpha}{\sqrt{5}k^2}.$$

Последнее неравенство мы можем записать в виде равенства

$$\frac{\theta}{\sqrt{5}k^2}=\frac{h}{k}-\frac{\sqrt{5}+1}{2},$$

где $|\theta|<\alpha$. Отсюда мы получаем, что

$$h-\frac{k}{2}=\frac{\sqrt{5}\,k}{2}+\frac{\theta}{\sqrt{5}\,k},$$

или, после возведения в квадрат обеих частей последнего равенства,

$$h^2-hk-k^2=\theta+\frac{\theta^2}{5k^2}.$$

Поскольку h и k — целые, h^2-hk-k^2 не может обращаться в нуль, за исключением случая $h=k=0$. Но $k\neq 0$ и, следовательно, $|h^2-hk-k^2|\geqslant 1$. Так как $|\theta|<\alpha<1$, мы имеем

$$1\leqslant\left|\theta+\frac{\theta^2}{5k^2}\right|\leqslant|\theta|+\frac{|\theta|^2}{5k^2}<\alpha+\frac{\alpha^2}{5k^2},$$

или

$$k^2<\frac{\alpha^2}{5(1-\alpha)}. \tag{4}$$

Таким образом, знаменатель k дроби h/k, удовлетворяющей неравенству (3), должен удовлетворять неравенству (4). Но α фиксировано и потому k может принимать лишь конечное число значений. Из (3) следует, что h также может принимать только конечное число значений. Следовательно, если $c>\sqrt{5}$, то неравенство (3) справедливо лишь для конечного числа дробей h/k. Тем самым теорема 9 полностью доказана.

Отметим, наконец, что теоремы 4, 8 и 9 останутся справедливыми, если опустить условие $0<\xi<1$.

КВАДРАТИЧНЫЕ ВЫЧЕТЫ И ПРЕДСТАВЛЕНИЕ ЧИСЕЛ В ВИДЕ СУММЫ ЧЕТЫРЕХ КВАДРАТОВ

§ 1. Символ Лежандра. Теория квадратичных вычетов является одним из основных разделов теории чисел. С ее помощью, например, можно доказать такие элегантные результаты, как теорему Эйлера о том, что каждое простое число вида $4k+1$ представляется в виде суммы двух квадратов, и теорему Лагранжа о том, что каждое положительное целое число представляется в виде суммы четырех квадратов.

Пусть p — нечетное простое число и a — целое число, причем $(a, p)=1$. Если существует такое целое число x, что $x^2 \equiv a \pmod p$, то a называется *квадратичным вычетом по модулю p*. Если такого x не существует, то a называется *квадратичным невычетом по модулю p*.

Мы иногда будем использовать запись aRp для обозначения того, что a — квадратичный вычет по модулю p, и aNp для обозначения того, что a — квадратичный невычет по модулю p. Чтобы выяснить, сколько чисел из набора 1, 2, ..., $p-1$ являются квадратичными вычетами по модулю p, мы должны знать, сколько сравнений

$$x^2 \equiv a \pmod p \tag{1}$$

разрешимо, когда a пробегает значения 1, 2, ..., $p-1$.

Рассмотрим целые числа

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

Все они попарно не сравнимы по $\bmod p$. Действительно, если мы возьмем любые два из этих чисел, скажем r^2 и s^2, $r \neq s$, то из $r^2 \equiv s^2 \pmod p$ будет следовать, что $r \equiv s \pmod p$ или $r \equiv -s \pmod p$. Но обе эти альтернативы исключены, так как $1 \leqslant r,\ s \leqslant (p-1)/2$. Далее, $r^2 \equiv (p-r)^2 \pmod p$. Из этих двух замечаний следует, что целое число a принимает в сравнении (1) в точности $(p-1)/2$ различных значений, когда x пробегает множе-

ство 1, 2, 3, ..., $p-1$. *Следовательно, имеется в точности* $(p-1)/2$ *квадратичных вычетов и* $(p-1)/2$ *квадратичных невычетов по модулю* p.

Символ Лежандра. Пусть p — нечетное простое число и m — целое число, такие, что $(m, p)=1$. Определим символ Лежандра $\left(\frac{m}{p}\right)$ следующим образом:

$$\left(\frac{m}{p}\right)=\begin{cases}+1, & \text{если } mRp,\\ -1, & \text{если } mNp.\end{cases} \tag{2}$$

Удобно расширить определение символа Лежандра, положив

$$\left(\frac{m}{p}\right)=0, \text{ если } p\mid m.$$

Поскольку имеется столько же квадратичных невычетов, сколько и квадратичных вычетов, мы имеем

$$\sum_{m=0}^{p-1}\left(\frac{m}{p}\right)=0.$$

Далее, если $m_1\equiv m_2 \pmod p$, то

$$\left(\frac{m_1}{p}\right)=\left(\frac{m_2}{p}\right).$$

§ 2. Теорема Вильсона и критерий Эйлера. Следующий результат, известный под названием теоремы Вильсона, но впервые доказанный Лагранжем, выражает характеристическое свойство простых чисел:

Теорема 1. *Если* p *— простое число, то* $(p-1)!\equiv -1 \pmod p$.

Доказательство. При $p=2$ утверждение теоремы очевидно. Пусть $p>2$. Из рассуждений § 1 гл. II следует, что для любого x из множества 1, 2, ..., $p-1$ существует, и притом единственный, элемент x' из того же самого множества, такой, что

$$xx'\equiv 1 \pmod p. \tag{3}$$

Далее, $x=x'$ тогда и только тогда, когда $x=1$ или $x=$

$=p-1$. Действительно, сравнение $x^2\equiv 1 \pmod p$ эквивалентно сравнению $(x-1)(x+1)\equiv 0 \pmod p$, так что или $x\equiv 1 \pmod p$, откуда $x=1$, или $x\equiv -1 \pmod p$, откуда $x=p-1$.

Из (3) следует тогда, что

$$2\cdot 3\ldots(p-2)\equiv 1 \pmod p,$$

и если мы умножим это сравнение на сравнение

$$1\cdot(p-1)\equiv -1 \pmod p,$$

то получим

$$1\cdot 2\cdot 3\ldots(p-1)\equiv -1 \pmod p. \qquad (4)$$

Тем самым теорема Вильсона доказана.

Предположим теперь, что число p *составное*. Тогда его можно представить в виде $p=qr$, $1<q<p$. Следовательно, q будет входить в качестве сомножителя в произведение $1\cdot 2\cdot 3\ldots(p-1)$, и сравнение

$$(p-1)!+1\equiv 0 \pmod q$$

в этом случае не разрешимо. Тем более не будет разрешимым и сравнение $(p-1)!+1\equiv 0 \pmod p$. Таким образом, теорема Вильсона устанавливает характеристическое свойство простых чисел.

Пусть теперь p — нечетное простое число и $(a, p)=1$. Покажем, что если a — квадратичный вычет по модулю p, то

$$a^{(p-1)/2}\equiv 1 \pmod p.$$

Действительно, сравнение $x^2\equiv a \pmod p$ в этом случае разрешимо и $(x, p)=1$, ввиду того что $(a, p)=1$. Если мы возведем обе части этого сравнения в степень $(p-1)/2$, которая, поскольку p нечетно, будет целым числом, то получим

$$x^{p-1}\equiv a^{(p-1)/2} \pmod p.$$

Но по теореме Ферма (теорема 3 гл. II) мы знаем, что $x^{p-1}\equiv 1 \pmod p$. Следовательно, $a^{(p-1)/2}\equiv 1 \pmod p$.

С другой стороны, по теореме Лагранжа (теорема 7 гл. II) сравнение

$$x^{(p-1)/2}\equiv 1 \pmod p$$

может иметь не более чем $(p-1)/2$ решений. Но в § 1 мы показали, что имеется в точности $(p-1)/2$ квадратичных вычетов и каждый из них удовлетворяет последнему сравнению. Следовательно, это сравнение не может иметь других решений. Таким образом, нами доказана

Теорема 2 (критерий Эйлера). *Пусть p — нечетное простое число и a — любое целое. Сравнение*

$$a^{(p-1)/2} \equiv 1 \pmod{p}$$

справедливо тогда и только тогда, когда a является квадратичным вычетом по модулю p.

Далее, если p — нечетное простое число и $(x, p) = 1$, то по теореме Ферма

$$x^{p-1} - 1 = (x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1) \equiv 0 \pmod{p}.$$

Следовательно, *или*

$$x^{(p-1)/2} \equiv 1 \pmod{p}, \tag{5}$$

или

$$x^{(p-1)/2} \equiv -1 \pmod{p}, \tag{6}$$

и так как по теореме 2 квадратичные невычеты не удовлетворяют сравнению (5), они должны удовлетворять сравнению (6). Вспоминая определение символа Лежандра, мы получаем отсюда следующую теорему:

Теорема 3. *Если p — нечетное простое число, то*

$$m^{(p-1)/2} \equiv \left(\frac{m}{p}\right) \pmod{p}.$$

Следствие. *Имеет место равенство*

$$\left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = \left(\frac{mn}{p}\right),$$

которое означает, что произведение двух квадратичных вычетов или невычетов по модулю p является квадратичным вычетом, а произведение квадратичного вычета и квадратичного невычета по модулю p есть квадратичный невычет по модулю p.

§ 3. Суммы двух квадратов. Пусть p — нечетное простое число, и пусть $m=p-1$. Так как $p-1\equiv -1 \pmod p$, то мы получим по теореме 3

$$\left(\frac{-1}{p}\right)\equiv(-1)^{(p-1)/2} \pmod p.$$

Но $\left(\frac{-1}{p}\right)=\pm 1$, $(-1)^{(p-1)/2}=\pm 1$ и $p\geqslant 3$. Следовательно,

$$\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2},$$

откуда следует, что -1 есть *квадратичный вычет по* $\bmod p$ *для всех простых* $p\equiv 1 \pmod 4$ *и квадратичный невычет по* $\bmod p$ *для всех простых* $p\equiv 3 \pmod 4$. Это приводит нас к следующей теореме:

Теорема 4 (Эйлер). *Каждое простое число вида* $4k+1$ *можно представить в виде суммы двух квадратов.*

Доказательство. Если p — простое число вида $4k+1$, то -1 является квадратичным вычетом по модулю p, т. е. сравнение $x^2\equiv -1 \pmod p$ разрешимо. Следовательно, существует целое число A, такое, что $p\mid (A^2+1)$. По теореме 5 гл. III отсюда следует, что p является суммой двух квадратов.

Результат о том, что для простого числа p вида $4k+1$ мы имеем $p\mid (A^2+1)$ при некотором A, может быть уточнен следующим образом:

Теорема 5. *Если* p *— простое число и* $p\equiv 1 \pmod 4$, *то существует такое целое число* x, *что*

$$x^2+1=mp, \text{ где } 0<m<p.$$

Доказательство. Так как -1 является квадратичным вычетом по $\bmod p$, существует целое x из набора $1, 2, \ldots, (p-1)/2$, которое удовлетворяет сравнению

$$x^2\equiv -1 \pmod p.$$

Тогда $x^2+1=mp$ для некоторого целого m. Но $x<p/2$ и, следовательно, $x^2+1<(p/2)^2+1<p^2$. Таким образом, $x^2+1=mp$, где $0<m<p$.

Следующий результат аналогичен результату теоремы 5.

Теорема 6. *Если p — нечетное простое число, то существуют целые x и y, такие, что*

$$1 + x^2 + y^2 = mp, \text{ где } 0 < m < p.$$

Доказательство. Целые x^2, $0 \leqslant x \leqslant (p-1)/2$, попарно не сравнимы по $\bmod p$. То же самое справедливо для целых $-1-y^2$, $0 \leqslant y \leqslant (p-1)/2$. Но эти два множества вместе содержат $p+1$ целых чисел, и так как имеется только p классов вычетов по $\bmod p$, некоторый член x^2 первого множества должен быть сравним с некоторым членом $-1-y^2$ второго множества. Таким образом,

$$x^2 \equiv -1-y^2 \pmod{p},$$

или

$$1+x^2+y^2 = mp.$$

Но $0 \leqslant x, y \leqslant (p-1)/2$. Следовательно,

$$1+x^2+y^2 < 1+2\left(\frac{1}{2}p\right)^2 < p^2,$$

и тогда

$$1+x^2+y^2 = mp, \quad 0 < m < p.$$

Теорема доказана.

Мы видели, что каждое простое число вида $4k+1$ представимо в виде суммы двух квадратов. Но другие числа также обладают этим свойством, например $10 = 1^2+3^2$. Следующая теорема дает необходимое и достаточное условие представимости положительного целого числа в виде суммы двух квадратов:

Теорема 7. *Положительное целое число n можно представить в виде суммы двух квадратов тогда и только тогда, когда все простые сомножители вида $4k+3$ входят в каноническое разложение этого числа с четными показателями.*

Докажем предварительно две леммы. Мы назовем представление $n = x^2+y^2$ *примитивным*, если $(x, y) = 1$, и *непримитивным* в противном случае.

Лемма 1. *Если n делится на простое число p, где $p\equiv 3 \pmod 4$, то n не имеет примитивных представлений.*

Доказательство. Если n имеет примитивное представление, скажем

$$n=x^2+y^2, \quad (x, y)=1,$$

то $p \mid (x^2+y^2)$, но $p \nmid x$ и $p \nmid y$. Так как $(p, x)=1$, то уравнение $mx-tp=c$ разрешимо в целых числах m и t при всех целых c и, в частности, при $c=y$. Следовательно, существует такое целое число m, что

$$mx\equiv y \pmod p,$$

откуда

$$x^2+(mx)^2\equiv x^2+y^2\equiv 0 \pmod p.$$

Тогда $p \mid x^2(m^2+1)$, и так как $p \nmid x$, то $p \mid (m^2+1)$. Таким образом, $m^2\equiv -1 \pmod p$. Другими словами, -1 есть квадратичный вычет по простому модулю p вида $4k+3$, но, как было выяснено в начале § 3, это невозможно. Тем самым лемма доказана.

Лемма 2. *Если p — простое число, $p\equiv 3 \pmod 4$, и c — нечетное целое, такое, что $p^c \mid n$, но $p^{c+1} \nmid n$, то n не может быть представлено в виде суммы двух квадратов.*

Доказательство. Предположим обратное, т. е. что $n=x^2+y^2$, где $(x, y)=d$. Тогда $x=dX$, $y=dY$, $(X, Y)=1$, и $n=d^2(X^2+Y^2)=d^2N$ при некотором N.

Пусть p^r — наивысшая степень p, которая делит d. Тогда p^{c-2r} будет наивысшей степенью p, делящей N. Из нечетности c следует, что $c-2r>0$. Таким образом, мы имеем, что $N=X^2+Y^2$, $(X, Y)=1$, и $p \mid N$, где $p\equiv 3 \pmod 4$. Но это противоречит утверждению леммы 1 и доказывает лемму 2.

Доказательство теоремы 7. Условия теоремы необходимы. Действительно, из леммы 2 следует, что если n представимо в виде суммы двух квадратов, то каждый простой делитель числа n вида $4k+3$ должен иметь четный показатель степени в каноническом разложении n.

Условия теоремы являются также и достаточными. Действительно, если n — положительное целое, такое,

что каждое простое вида $4k+3$ входит в каноническое разложение этого числа с четным показателем, то n можно записать в виде $n=n_1^2 n_2$, где n_2 не имеет простых делителей вида $4k+3$. Следовательно, простыми делителями числа n_2 являются только простые числа вида $4k+1$ или число 2. Но 2 представимо в виде суммы двух квадратов: 1^2+1^2, и каждое простое вида $4k+1$ также можно представить в таком виде. Далее, из тождества

$$(x_1^2+y_1^2)(x_2^2+y_2^2)=(x_1x_2+y_1y_2)^2+(x_1y_2-x_2y_1)^2$$

следует, что произведение двух чисел, представимых в виде суммы двух квадратов, также имеет такое представление. Таким образом, $n_2=a^2+b^2$, откуда $n=(n_1a)^2+(n_1b)^2$.

§ 4. Суммы четырех квадратов. В заключении этой главы мы докажем хорошо известный и элегантный результат:

Теорема 8 (Лагранж). *Каждое положительное целое число n является суммой четырех квадратов.*

Доказательство. Мы имеем $1^2=1^2+0^2+0^2+0^2$ и потому можем предполагать, что $n>1$. Из тождества

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)=$$
$$=z_1^2+z_2^2+z_3^2+z_4^2, \quad (7)$$

где

$$z_1=x_1y_1+x_2y_2+x_3y_3+x_4y_4,$$
$$z_2=x_1y_2-x_2y_1+x_3y_4-x_4y_3,$$
$$z_3=x_1y_3-x_3y_1+x_4y_2-x_2y_4,$$
$$z_4=x_1y_4-x_4y_1+x_2y_3-x_3y_2,$$

следует, что произведение двух целых чисел, представимых суммой четырех квадратов, также можно представить в таком виде. Каждое целое число $n>1$ является произведением нечетных простых и, возможно, числа $2=1^2+1^2+0^2+0^2$. Следовательно, достаточно доказать, что каждое нечетное простое представляется в виде суммы четырех квадратов.

Из теоремы 6 следует, что если p — нечетное простое число, то существует целое $m<p$, такое, что

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$

где не каждое x_1, x_2, x_3, x_4 делится на p.

Для данного нечетного простого числа p обозначим через m_0 наименьшее положительное целое число, такое, что

$$m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2, \quad m_0 < p. \tag{8}$$

Если $m_0 = 1$, то доказывать больше нечего.

Предположим, что $m_0 > 1$. Покажем сначала, что m_0 должно быть *нечетным*. Действительно, если m_0 четное, то x_1, x_2, x_3, x_4 или все четные, или все нечетные, или два из них четные и два нечетные (например, x_1, x_2 четные, а x_3, x_4 нечетные). Так как

$$\frac{1}{2} m_0 p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2,$$

мы видим, что $(m_0 p)/2$ является суммой четырех *целых* квадратов, не все из которых делятся на p. Но это противоречит минимальности m_0.

В таком случае $m_0 \geqslant 3$ и мы можем записать, что

$$x_i = b_i m_0 + y_i \quad (i = 1, 2, 3, 4), \tag{9}$$

причем целые b_i можно выбрать таким образом, чтобы $|y_i| < m_0/2$. Действительно, если при делении x_i на нечетное число m_0 мы получим $x_i = b_i' m_0 + y_i'$, где $y_i' > m_0/2$, то мы можем записать, что

$$x_i = (b_i' + 1) m_0 + (y_i' - m_0) = b_i m_0 + y_i,$$

где $-m_0/2 < y_i < 0$.

Далее, не все x_1, x_2, x_3, x_4 делятся на m_0. Действительно, если бы все x_1, x_2, x_3, x_4 делились на m_0, то мы имели бы $m_0 \mid p$, что невозможно, так как $1 < m_0 < p$. Следовательно,

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 > 0.$$

и мы имеем

$$0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4\left(\frac{1}{2}m_0\right)^2 = m_0^2.$$

Но из (8) и (9) следует, что

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \pmod{m_0}.$$

Итак, мы имеем целые числа x_i, y_i $(i=1, 2, 3, 4)$, для которых

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p, \quad m_0 < p,$$

и

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_1 m_0, \quad 0 < m_1 < m_0.$$

Тождество (7) дает нам четыре целых числа z_1, z_2, z_3, z_4, такие, что

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = m_0^2 m_1 p. \tag{10}$$

Далее,

$$z_1 = \sum_{i=1}^{4} x_i y_i = \sum_{i=1}^{4} x_i (x_i - b_i m_0) \equiv \sum_{i=1}^{4} x_i^2 \pmod{m_0} \equiv$$

$$\equiv 0 \pmod{m_0},$$

и, аналогично,

$$z_2 \equiv z_3 \equiv z_4 \equiv 0 \pmod{m_0}.$$

Следовательно, $z_i = m_0 t_i$, где t_i — целые числа при $i = 1, 2, 3, 4$. Подставляя эти значения z_i в равенство (10), мы получаем

$$m_1 p = t_1^2 + t_2^2 + t_3^2 + t_4^2,$$

где $0 < m_1 < m_0$, что противоречит минимальности m_0. Следовательно, $m_0 = 1$ и теорема 8 доказана.

КВАДРАТИЧНЫЙ ЗАКОН ВЗАИМНОСТИ

§ 1. Квадратичная взаимность. Пусть p и q — различные нечетные простые числа. Тогда определены символы Лежандра $\left(\frac{p}{q}\right)$ и $\left(\frac{q}{p}\right)$. Можно ли указать значение $\left(\frac{q}{p}\right)$, если известно значение $\left(\frac{p}{q}\right)$? Квадратичный закон взаимности Гаусса показывает, что это действительно возможно.

Теорема 1 (Гаусс). *Если p и q — различные нечетные простые числа, то*

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Так как $\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)$ есть нечетное число тогда и только тогда, когда $p\equiv q\equiv 3 \pmod 4$, теорему 1 можно сформулировать следующим образом:

$$\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right), \text{ если } p\equiv q\equiv 3 \pmod 4,$$

и

$$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right) \text{ в противном случае.}$$

Мы выведем квадратичный закон взаимности из формулы взаимности для некоторых тригонометрических сумм.

§ 2. Формула взаимности для обобщенных сумм Гаусса. Пусть m и n — ненулевые целые числа. Определим *обобщенную сумму Гаусса* следующим образом:

$$g(m,n)=\sum_{k=1}^{|n|} e^{\pi i\frac{m}{n}k^2+\pi imk}. \qquad (1)$$

Когда m четное, эта сумма представляет собой *сумму Гаусса*. Теорема 1 может быть выведена из формулы, связывающей $g(m, n)$ и $g(-n, m)$, которая устанавливается в следующей теореме:

Теорема 2. *Если m и n — ненулевые целые числа, то*

$$\frac{1}{\sqrt{|n|}} g(m, n) = e^{\frac{\pi i}{4}(1-|mn|)\operatorname{sgn}(mn)} \frac{1}{\sqrt{|m|}} g(-n, m), \qquad (2)$$

где

$$\operatorname{sgn} r = \begin{cases} r/|r| & \text{при } r \neq 0, \\ 0 & \text{при } r = 0. \end{cases}$$

Доказательство. В доказательстве мы будем пользоваться интегрированием в комплексной плоскости. Рассмотрим интеграл

$$f(X) = f(X, \tau) = \int_C \Phi(u)\, du, \qquad (3)$$

где

$$\Phi(u) = \Phi(u, X) = \Phi(u, X, \tau) = \frac{e^{\pi i \tau u^2 + 2\pi i X u}}{e^{2\pi i u} - 1}. \qquad (4)$$

Здесь u — комплексная переменная, X — произвольное комплексное число, τ — комплексное число с положительной действительной частью, а C — прямая в комплексной u-плоскости, проходящая через точку $u = 1/2$ и составляющая с положительным направлением действительной оси угол $\pi/4$. Покажем сначала, что интеграл сходится. Для этого мы оценим функцию Φ в любой полосе (конечной ширины), которая ограничена двумя прямыми, параллельными C Если мы положим

$$u = c + e^{\frac{\pi i}{4}},$$

где c и r — действительные переменные величины, причем величина c ограничена, и

$$\tau = \operatorname{Re}\tau + i \operatorname{Im}\tau,$$

то

$$\left| e^{\pi i \tau u^2 + 2\pi i X u} \right| = e^{-\pi \operatorname{Im}(\tau u^2 + 2Xu)}$$

и

$$\tau u^2 + 2Xu = i\tau r^2 + 2e^{\frac{\pi i}{4}}(\tau c + X) r + (\tau c + 2X) c,$$

так что

$$\operatorname{Im}(\tau u^2+2Xu) \geqslant \operatorname{Re}\tau \cdot r^2 - 2|\tau c+X|\cdot|r| - |(\tau c+2X)c|.$$

Следовательно,

$$|e^{\pi i\tau u^2+2\pi i Xu}| \leqslant e^{-\pi r^2 \operatorname{Re}\tau + \pi|\tau|\cdot(c^2+2|cr|)+2\pi|X|\cdot(|c|+|r|)} \leqslant$$

$$\leqslant Ae^{-\pi r^2 \operatorname{Re}\tau + B|r|}, \qquad (5)$$

где A и B — постоянные, не зависящие от r.

Далее,

$$|e^{2\pi iu}-1| \geqslant |1-|e^{2\pi iu}|| = |1-e^{-\sqrt{2}\pi r}|,$$

и если в указанной полосе $|u|\to\infty$, то $r\to\pm\infty$, так что при достаточно больших значениях $|u|$ мы будем иметь

$$|e^{2\pi i u}-1| \geqslant \frac{1}{2} > 0. \qquad (6)$$

Тогда из (5) и (6) мы имеем в указанной полосе при всех достаточно больших значениях $|u|$

$$|\Phi(u)| \leqslant A_1 e^{-\pi r^2 \operatorname{Re}\tau + B|r|}. \qquad (7)$$

Следовательно, интеграл $\int\limits_C \Phi(u)\,du$ сходится.

Покажем теперь, что $g(m, n)$ при $n>0$ является значением интеграла $\int\limits_\gamma \Phi(u)\,du$ при подходящем выборе контура γ.

Пусть γ — параллелограмм, образованный прямой C, прямой C_n, параллельной C и пересекающей действительную ось в точке $n+1/2$, $n>0$, и прямыми L_1 и L_2, лежащими в верхней и нижней полуплоскостях соответственно, параллельными действительной оси и отстоящими от нее на положительном расстоянии (рис. 1).

Функция $\Phi(u)$ является мероморфной функцией переменного u, и, если контур γ обходится в положительном направлении, мы имеем по теореме Коши о вычетах

$$\int\limits_\gamma \Phi(u)\,du = \sum_{k=1}^{n} e^{\pi i\tau k^2 + 2\pi i Xk}. \qquad (8)$$

Из (7) следует, что $\Phi(u)\to 0$ равномерно в полосе между параллельными прямыми C и C_n при $|u|\to\infty$. Следова-

тельно, при удалении прямых L_1 и L_2 от действительной оси к бесконечности интеграл по сторонам L_1 и L_2 параллелограмма γ будет стремиться к нулю, и тогда

$$\int_{C_n} \Phi(u)\,du - \int_{C} \Phi(u)\,du = \sum_{k=1}^{n} e^{\pi i \tau k^2 + 2\pi i X k}. \tag{9}$$

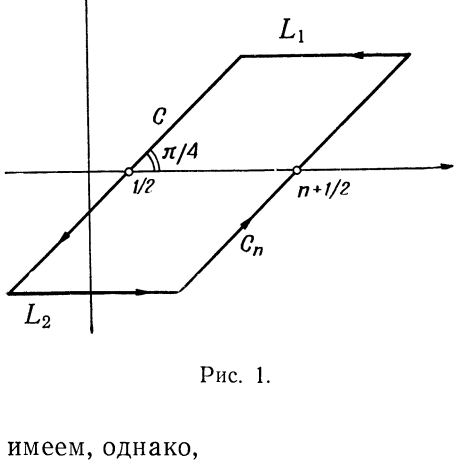

Рис. 1.

Из (4) мы имеем, однако,

$$\Phi(u+n, X) = e^{\pi i \tau n^2 + 2\pi i X n}\,\Phi(u, X+\tau n),$$

так что

$$\int_{C_n} \Phi(u)\,du = e^{\pi i \tau n^2 + 2\pi i X n} f(X+\tau n),$$

где f определена по формуле (3). Следовательно, соотношение (9) переходит в

$$e^{\pi i \tau n^2 + 2\pi i X n} f(X+\tau n) - f(X) = \sum_{k=1}^{n} e^{\pi i \tau k^2 + 2\pi i X k}, \tag{10}$$

что дает соотношение между $f(X)$ и $f(X+\tau n)$. Найдем теперь другое такое соотношение и сравним их между собой.

Начнем с тождества

$$f(X+1)-f(X)=\int\limits_C \frac{e^{\pi i\tau u^2}}{e^{2\pi i u}-1}\left\{e^{2\pi i(X+1)u}-e^{2\pi i X u}\right\}du=$$

$$=\int\limits_C e^{\pi i\tau u^2+2\pi i X u}\,du=e^{-\pi i\frac{X^2}{\tau}}\int\limits_C e^{\pi i\tau\left(u+\frac{X}{\tau}\right)^2}du.$$

Пусть теперь C' — прямая, полученная из C с помощью параллельного переноса $u\to u+X/\tau$. Тогда

$$f(X+1)-f(X)=e^{-\pi i\frac{X^2}{\tau}}\int\limits_{C'} e^{\pi i\tau u^2}du.$$

Из оценки (5) ясно, что этот интеграл сходится. Интегрируя, как и раньше, по параллелограмму и используя оценку (5) при $X=0$, мы видим, что

$$\int\limits_{C'} e^{\pi i\tau u^2}du=\int\limits_{C_0} e^{\pi i\tau u^2}du,$$

где C_0 — прямая, параллельная C' и проходящая через начало координат. На прямой C_0 мы имеем $u=re^{\pi i/4}$ при действительном r. Следовательно,

$$\int\limits_{C_0} e^{\pi i\tau u^2}du=e^{\frac{\pi i}{4}}\int\limits_{-\infty}^{\infty} e^{-\pi\tau r^2}dr=e^{\frac{\pi i}{4}}I_\tau,$$

и тогда

$$f(X+1)-f(X)=e^{\pi i\left(\frac{1}{4}-\frac{X^2}{\tau}\right)}I_\tau.$$

Итерируя эту формулу m раз, получаем

$$f(X+m)-f(X)=I_\tau\cdot\sum_{\nu=0}^{m-1} e^{\pi i\left(\frac{1}{4}-\frac{(X+\nu)^2}{\tau}\right)},$$

где m — положительное целое. Отсюда, заменяя X на $X+\tau n-m$, мы получим второе соотношение

$$f(X+\tau n)-f(X+\tau n-m)=$$

$$=I_\tau\cdot\sum_{\nu=0}^{m-1} e^{\pi i\left(\frac{1}{4}-\frac{(X+\tau n-m+\nu)^2}{\tau}\right)}. \quad (11)$$

Из (11) и (10) мы выводим, что

$$e^{\pi i\tau n^2+2\pi iXn}f(X+\tau n-m)-f(X)=$$

$$=\sum_{k=1}^{n}e^{\pi i\tau k^2+2\pi iXk}-I_\tau e^{\pi i\tau n^2+2\pi iXn}\sum_{\nu=1}^{m}e^{\pi i\left[\frac{1}{4}-\frac{(X+\tau n-\nu)^2}{\tau}\right]}=$$

$$=\sum_{k=1}^{n}e^{\pi i\tau k^2+2\pi iXk}-I_\tau\sum_{\nu=1}^{m}e^{\pi i\left[\frac{1}{4}-\frac{(X-\nu)^2}{\tau}\right]}. \qquad (12)$$

Положим в этом равенстве $X=m/2$ и $\tau=m/n$, $m>0$, $n>0$. Тогда

$$\sum_{k=1}^{n}e^{\pi ik^2\frac{m}{n}+\pi imk}=I_{m/n}e^{\frac{\pi i}{4}(1-mn)}\sum_{\nu=1}^{m}e^{\pi i\nu n-\nu^2\pi i\frac{n}{m}}. \qquad (12')$$

Далее, если мы положим $m=n=1$, то получим отсюда $I_1=1$, т. е.

$$\int_{-\infty}^{\infty}e^{-\pi t^2}dt=1,$$

и, используя подстановку $t\to t\sqrt{\tau}$, где τ — положительное действительное число, приходим к соотношению

$$I_\tau=\int_{-\infty}^{\infty}e^{-\pi\tau t^2}dt=\frac{1}{\sqrt{\tau}}. \qquad (13)$$

В таком случае из (13) при $\tau=m/n$ и (12′) мы имеем

$$\frac{1}{\sqrt{n}}\sum_{k=1}^{n}e^{\pi ik^2\frac{m}{n}+\pi imk}=$$

$$=\frac{1}{\sqrt{m}}e^{\frac{\pi i}{4}(1-mn)}\sum_{\nu=1}^{m}e^{\pi i\nu n-\nu^2\pi i\frac{n}{m}}=$$

$$=\frac{1}{\sqrt{m}}e^{\frac{\pi i}{4}(1-mn)}\sum_{\nu=1}^{m}e^{-\pi i\nu n-\nu^2\pi i\frac{n}{m}},$$

а это по определению $g(m, n)$ означает, что

$$\frac{1}{\sqrt{n}} g(m, n) = \frac{1}{\sqrt{m}} e^{\frac{\pi i}{4}(1-mn)} g(-n, m). \qquad (14)$$

Тем самым при $m>0$, $n>0$ теорема доказана.

Если $m>0$ и $n<0$, то $-n$, $m>0$ и из (14) следует, что

$$\frac{1}{\sqrt{m}} g(-n, m) = \frac{1}{\sqrt{-n}} e^{\frac{\pi i}{4}(1+mn)} g(-m, -n),$$

или

$$\frac{1}{\sqrt{|n|}} g(-m, -n) = e^{-\frac{\pi i}{4}(1-|mn|)} \frac{1}{\sqrt{m}} g(-n, m).$$

Но, по определению, $g(-m, -n) = g(m, n)$ и, следовательно,

$$\frac{1}{\sqrt{|n|}} g(m, n) = e^{\frac{\pi i}{4}(1-|mn|)\operatorname{sgn}(mn)} \frac{1}{\sqrt{m}} g(-n, m),$$

так что теорема справедлива и в этом случае.

Если $m<0$ и $n<0$, то формула (2) также остается справедливой, так как $g(-m, -n) = g(m, n)$, $g(n, -m) = g(-n, m)$ и $(1-|mn|)\operatorname{sgn}(mn)$ не меняется при замене m и n соответственно на $-m$ и $-n$. Теперь доказательство теоремы 2 закончено.

Следует отметить, что в доказательстве равенство

$$\int_{-\infty}^{\infty} e^{-\pi t^2} dt = 1$$

не предполагалось известным и было получено в качестве побочного результата.

§ 3. Доказательство квадратичного закона взаимности. Квадратичный закон взаимности, сформулирован-

ный в теореме 1, теперь нетрудно вывести из формулы взаимности для обобщенных сумм Гаусса, которая доказана в теореме 2.

Так как $k^2 \equiv k \pmod 2$, мы можем заменить k на k^2 в определении (1) суммы $g(m, n)$ и записать

$$g(m, n) = \sum_{k=1}^{|n|} e^{\pi i k^2 \frac{m}{n}(n+1)}.$$

Пусть теперь n — нечетное простое число и m — некоторое целое, взаимно простое с n. Тогда мы имеем

$$g(m, n) = 1 + \sum_{k=1}^{n-1} e^{\pi i k^2 \frac{m}{n}(n+1)}.$$

Если $k^2 \equiv \rho \pmod n$, то легко видеть, что

$$e^{\pi i k^2 \frac{m}{n}(n+1)} = e^{\pi i \rho \frac{m}{n}(n+1)}.$$

Но если $k^2 \equiv \rho \pmod n$ и $1 \leqslant k \leqslant n-1$, то ρ — квадратичный вычет по модулю n и $(n-k)^2 \equiv k^2 \equiv \rho \pmod n$. Следовательно, если k пробегает целые 1, 2, ..., $n-1$, то k^2 (взятое по модулю n) *дважды* пробегает множество квадратичных вычетов по модулю n. Значит,

$$g(m, n) = 1 + 2 \sum_{\rho} e^{\pi i \rho \frac{m}{n}(n+1)}, \tag{15}$$

где ρ пробегает множество квадратичных вычетов по модулю нечетного простого n.

Рассмотрим теперь сумму

$$\sum_{\nu} e^{\pi i \nu \frac{m}{n}(n+1)},$$

где ν пробегает множество квадратичных *невычетов* по модулю n. Мы имеем, очевидно,

$$1 + \sum_{\rho} e^{\pi i \rho \frac{m}{n}(n+1)} + \sum_{\nu} e^{\pi i \nu \frac{m}{n}(n+1)} = \sum_{k=0}^{n-1} e^{\pi i k \frac{m}{n}(n+1)}.$$

Но $n+1$ есть четное число и, следовательно, $e^{\pi i k \frac{m}{n}(n+1)}$ есть k-я степень корня n-й степени из единицы, скажем η, причем $\eta \neq 1$, так как $n \nmid m$. Таким образом,

$$1 + \sum_{\rho} e^{\pi i \rho \frac{m}{n}(n+1)} + \sum_{\nu} e^{\pi i \nu \frac{m}{n}(n+1)} =$$

$$= 1 + \sum_{\rho} \eta^{\rho} + \sum_{\nu} \eta^{\nu} = \sum_{p=0}^{n-1} \eta^{p} = \frac{1-\eta^{n}}{1-\eta} = 0. \quad (16)$$

Из (15) и (16) мы получаем, что

$$g(m,n) = \sum_{\rho} e^{\pi i \rho \frac{m}{n}(n+1)} - \sum_{\nu} e^{\pi i \nu \frac{m}{n}(n+1)}. \quad (17)$$

Рассмотрим теперь два возможных случая $\left(\frac{m}{n}\right) = +1$ и $\left(\frac{m}{n}\right) = -1$.

(а) Если m — квадратичный вычет по модулю n и ρ пробегает все квадратичные вычеты по тому же модулю, то, согласно следствию теоремы 3 гл. IV, ρm также пробегает все квадратичные вычеты. Если же ν пробегает все квадратичные невычеты, то νm также пробегает квадратичные невычеты по модулю n. Следовательно, в силу (17)

$$g(m,n) = \sum_{\rho} e^{\pi i \rho \left(\frac{n+1}{n}\right)} - \sum_{\nu} e^{\pi i \nu \left(\frac{n+1}{n}\right)} =$$

$$= g(1,n) = \left(\frac{m}{n}\right) g(1,n).$$

(б) Если m — квадратичный *невычет* по модулю n, то с помощью рассуждений, аналогичных рассуждениям пункта (а), мы имеем

$$g(m, n) = \sum_{\nu} e^{\pi i \nu \left(\frac{n+1}{n}\right)} - \sum_{\rho} e^{\pi i \rho \left(\frac{n+1}{n}\right)} =$$

$$= -g(1, n) = \left(\frac{m}{n}\right) g(1, n).$$

Таким образом, мы показали, что если n — нечетное простое число и $(m, n) = 1$, то

$$g(m, n) = \left(\frac{m}{n}\right) g(1, n). \tag{18}$$

С другой стороны, из теоремы 2 следует, что

$$\frac{1}{\sqrt{n}} g(1, n) = e^{\frac{\pi i}{4}(1-n)} g(-n, 1),$$

и так как, по определению, $g(-n, 1) = 1$, мы имеем

$$g(1, n) = \sqrt{n}\, e^{\frac{\pi i}{4}(1-n)}. \tag{19}$$

Из (18) и (19) мы получаем важную формулу:

$$\left(\frac{m}{n}\right) = \frac{1}{\sqrt{n}} e^{\frac{\pi i}{4}(n-1)} g(m, n). \tag{20}$$

где n — нечетное простое число и $(m, n) = 1$.

Если $m = -1$, то из (20) следует, что

$$\left(\frac{-1}{n}\right) = \frac{1}{\sqrt{n}} e^{\frac{\pi i}{4}(n-1)} g(-1, n).$$

Но, согласно соотношению (2), мы имеем

$$\frac{1}{\sqrt{n}} g(-1, n) = e^{\frac{\pi i}{4}(n-1)} g(-n, -1) = e^{\frac{\pi i}{4}(n-1)},$$

поскольку $g(-n, -1) = 1$. Следовательно,

$$\left(\frac{-1}{n}\right) = e^{\frac{\pi i}{2}(n-1)} = (-1)^{\frac{n-1}{2}}. \tag{21}$$

До сих пор мы предполагали, что n — нечетное простое число. *Пусть теперь m также будет нечетным простым.*

Тогда из (20) и (2) следует, что

$$\left(\frac{m}{n}\right) = e^{\frac{\pi i}{4}(n-1)} e^{\frac{\pi i}{4}(1-mn)} \frac{1}{\sqrt{m}} g(-n, m),$$

и, снова используя (20), мы получаем

$$\left(\frac{m}{n}\right) = e^{\frac{\pi i}{4}(n-1)} e^{\frac{\pi i}{4}(1-mn)} e^{-\frac{\pi i}{4}(m-1)} \left(\frac{-n}{m}\right).$$

Но, согласно (21),

$$\left(\frac{-n}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}} \left(\frac{n}{m}\right) = e^{\frac{2\pi i}{4}(m-1)} \left(\frac{n}{m}\right).$$

Следовательно,

$$\left(\frac{m}{n}\right) = e^{-\frac{\pi i}{4}(n-1)(m-1)} \left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}} \left(\frac{n}{m}\right),$$

и так как $\left(\frac{n}{m}\right)^2 = 1$, то

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}.$$

Тем самым доказательство теоремы 1 завершено.

§ 4. Некоторые приложения. Теорема 1 касалась величины $\left(\frac{p}{q}\right)$, где p и q — различные нечетные простые числа. Для того чтобы определить, будет ли данное *четное* число квадратичным вычетом или невычетом по модулю нечетного простого числа, мы должны научиться вычислять символ Лежандра $\left(\frac{2}{p}\right)$. Это можно сделать, используя формулы (2) и (20).

Теорема 3. *Если p — нечетное простое число, то*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}. \tag{22}$$

Другими словами,

$$\left(\frac{2}{p}\right) = \begin{cases} +1, & \text{если } p \equiv \pm 1 \pmod 8, \\ -1, & \text{если } p \equiv \pm 3 \pmod 8. \end{cases} \tag{23}$$

Доказательство. Согласно формуле (20), мы имеем

$$\left(\frac{2}{p}\right)=\frac{1}{\sqrt{p}}\,e^{\frac{\pi i}{4}(p-1)}\,g(2,p)$$

и в силу формулы (2)

$$\frac{1}{\sqrt{p}}\,g(2,p)=e^{\frac{\pi i}{4}(1-2p)}\,\frac{1}{\sqrt{2}}\,g(-p,2).$$

Далее, из определения $g(m, n)$ следует, что

$$g(-p,2)=1+e^{\frac{\pi i p}{2}}.$$

Таким образом,

$$\left(\frac{2}{p}\right)=\frac{e^{-\frac{\pi i p}{4}}}{\sqrt{2}}\left(1+e^{\frac{\pi i p}{2}}\right)=\frac{1}{\sqrt{2}}\left(e^{-\frac{\pi i p}{4}}+e^{\frac{\pi i p}{4}}\right)=(-1)^{\frac{p^2-1}{8}}.$$

Пример. Вычислим, используя теоремы 1 и 3,

$$\left(\frac{12703}{16361}\right).$$

Здесь оба числа 12703 и 16361 простые. По теореме 1 мы имеем

$$\left(\frac{12703}{16361}\right)=\left(\frac{16361}{12703}\right),$$

и так как $16361\equiv 3658 \pmod{12703}$, то

$$\left(\frac{16361}{12703}\right)=\left(\frac{3658}{12703}\right).$$

Далее, поскольку $\left(\frac{mn}{p}\right)=\left(\frac{m}{p}\right)\cdot\left(\frac{n}{p}\right)$, то, согласно теоремам 3 и 1,

$$\left(\frac{3658}{12703}\right)=\left(\frac{2}{12703}\right)\left(\frac{31}{12703}\right)\left(\frac{59}{12703}\right)=\left(\frac{31}{12703}\right)\left(\frac{59}{12703}\right)=$$

$$=\left\{-\left(\frac{12703}{31}\right)\right\}\cdot\left\{-\left(\frac{12703}{59}\right)\right\}=\left(\frac{24}{31}\right)\left(\frac{18}{59}\right)=$$

$$=\left(\frac{2^3}{31}\right)\left(\frac{3}{31}\right)\left(\frac{2}{59}\right)\left(\frac{3^2}{59}\right).$$

Наконец, ввиду того что $\left(\frac{2^2}{31}\right)=\left(\frac{2}{31}\right)^2=1$ и $\left(\frac{3^2}{59}\right)=1$, мы получаем

$$\left(\frac{12703}{16361}\right)=\left(\frac{2}{31}\right)\left(\frac{3}{31}\right)\left(\frac{2}{59}\right)=1\cdot\left(\frac{3}{31}\right)\cdot(-1)=$$
$$=\left(\frac{31}{3}\right)=\left(\frac{1}{3}\right)=1.$$

Замечание. Как мы видели в гл. IV, если p — нечетное простое число, то $\left(\frac{m}{p}\right)=\left(\frac{m'}{p}\right)$ для всех целых $m'\equiv m\pmod p$.

С другой стороны, из теоремы 3 мы знаем, что $\left(\frac{2}{p}\right)$ имеет одно и то же значение для всех простых p, принадлежащих арифметическим прогрессиям $8m\pm1$ или $8m\pm3$.

Теорема 1 может быть использована для доказательства более общего результата: если q — фиксированное нечетное простое число, то

$$\left(\frac{q}{p}\right)=\left(\frac{q}{p'}\right), \tag{24}$$

где p' такое простое, что $p'\equiv p\pmod{4q}$.

Действительно, так как $p'\equiv p\pmod{4q}$, то $p'\equiv p\pmod 4$ и тогда $\frac{1}{2}(p'-1)\equiv\frac{1}{2}(p-1)\pmod 2$. По теореме 1 мы имеем

$$\left(\frac{p'}{q}\right)\left(\frac{q}{p'}\right)=(-1)^{\frac{p'-1}{2}\cdot\frac{q-1}{2}}=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}=\left(\frac{p}{q}\right)\left(\frac{q}{p}\right).$$

Далее, так как $p'\equiv p\pmod{4q}$, то $p'\equiv p\pmod q$, откуда $\left(\frac{p'}{q}\right)=\left(\frac{p}{q}\right)$. Таким образом, $\left(\frac{q}{p}\right)=\left(\frac{q}{p'}\right)$ и тем самым равенство (24) доказано.

ГЛАВА VI

АРИФМЕТИЧЕСКИЕ ФУНКЦИИ И ЦЕЛЫЕ ТОЧКИ

§ 1. Общие замечания. Напомним, что арифметическая функция — это комплекснозначная функция, определенная на множестве положительных целых чисел. Многие из арифметических функций, которые будут нами рассмотрены, являются целозначными.

Арифметическая функция f называется *мультипликативной*, если (i) f не равняется тождественно нулю и (ii) $f(mn)=f(m)\cdot f(n)$ при $(m, n)=1$. Условие (i) можно сформулировать иначе, а именно $f(1)=1$.

В качестве примера такой функции можно привести функцию Эйлера φ, введенную в гл. II. Мы показали, что она мультипликативна и что $\varphi(p^\alpha)=p^\alpha(1-1/p)$ для любого простого p и положительного целого числа α.

Многие арифметические функции ведут себя крайне нерегулярно, и поэтому часто более интересным представляется изучение *сумматорной функции* арифметической функции f, а именно

$$F(N)=\sum_{n=1}^{N} f(n),$$

а не самой функции $f(n)$.

Некоторые из рассматриваемых нами арифметических функций имеют простую геометрическую интерпретацию. С их помощью можно подсчитать число *целых точек* в некоторых областях, т. е. число точек n-мерного евклидова пространства, $n\geqslant 1$, имеющих целые координаты.

§ 2. Функция $r(n)$. Арифметическая функция $r(n)$ определяется как число представлений целого $n\geqslant 1$ в виде суммы двух квадратов; другими словами, значение $r(n)$ равно числу решений уравнения $x^2+y^2=n$ в целых числах x и y. Решения, отличающиеся друг от друга знаком или порядком, считаются различными. Так, $r(1)=4$

ввиду того, что $1=(\pm 1)^2+0^2=0^2+(\pm 1)^2$. Следовательно, $r(n)$ *не* мультипликативна.

Мы видели в теореме 7 гл. IV, что $r(n)=0$, если n — простое число вида $4k+3$. С другой стороны, из теоремы 6 гл. III следует, что таких простых бесконечно много. Таким образом, $r(n)=0$ для бесконечного множества значений n, и так как $r(n)\geqslant 0$, то

$$\overline{\lim_{n\to\infty}}\, r(n)=0.$$

Можно оценить порядок роста $r(n)$ и доказать, что $r(n)=O(n^{\varepsilon})$ для любого $\varepsilon>0$, т. е. $|r(n)|n^{-\varepsilon}<K$, где K — положительная постоянная, не зависящая от n. Однако более интересным представляется изучение (несколько измененной) сумматорной функции

$$R(N)=\sum_{n=0}^{N} r(n), \quad r(0)=1.$$

Геометрически $R(N)$ представляет собой число целых точек внутри и на границе круга $x^2+y^2\leqslant N$. Ясно, что величина $R(N)$ *приближенно* равна площади этого круга.

Теорема 1. (Гаусс). $R(N)=\pi N+O(\sqrt{N})$.

Доказательство. Целые точки на плоскости являются вершинами квадратов единичной площади. Каждой точке с целыми координатами, лежащей внутри или на границе круга $x^2+y^2\leqslant N$, мы можем поставить в соответствие некоторый такой квадрат, взяв, например, за указанную точку его «юго-западный» угол. Тогда $R(N)$ будет равно сумме площадей этих квадратов.

Некоторые из квадратов не полностью лежат внутри круга; с другой стороны, некоторая часть круга не покрывается этими квадратами (рис. 2).

Однако, так как диагональ каждого квадрата равна $\sqrt{2}$, все квадраты содержатся внутри круга $x^2+y^2\leqslant (\sqrt{N}+\sqrt{2})^2$, так что

$$R(N)<\pi(\sqrt{N}+\sqrt{2})^2.$$

Подобным же образом эти квадраты полностью покрывают меньший круг радиуса $\sqrt{N}-\sqrt{2}$, так что

$$R(N)>\pi\left(\sqrt{N}-\sqrt{2}\right)^2, \quad N\geqslant 2.$$

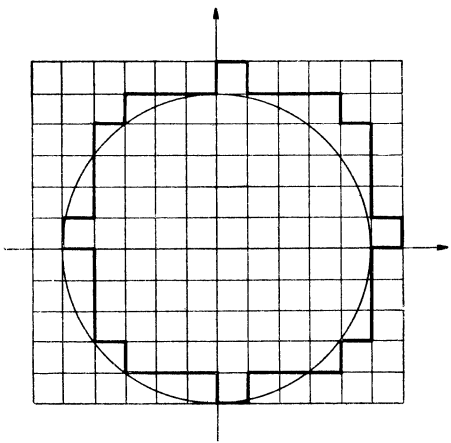

Рис. 2.

Таким образом,

$$\pi\left(N-2\sqrt{2N}+2\right)<R(N)<\pi\left(N+2\sqrt{2N}+2\right)$$

и, следовательно,

$$R(N)=\pi N+O(\sqrt{N}).$$

§ 3. Функция $d(n)$. Арифметическая функция $d(n)$ определяется как число положительных делителей положительного целого числа n.

Теорема 2. *Функция* $d(n)$ *мультипликативна.*

Доказательство. Очевидно, $d(1)=1$, и если $(m, n)=1$, то каждый делитель произведения mn может быть единственным образом представлен в виде произведения делителя m и делителя n. Обратно, каждое такое про-

изведение является делителем произведения mn. Следовательно, $d(mn)=d(m)d(n)$.

Теорема 3. *Если* $n=\prod_{i=1}^{r} p_i^{\alpha_i}$ *— каноническое разложение числа* $n>1$, *то* $d(n)=\prod_{i=1}^{r}(\alpha_i+1)$.

Доказательство. Поскольку $d(n)$ мультипликативна, мы имеем

$$d(n)=\prod_{i=1}^{r} d\left(p_i^{\alpha_i}\right).$$

Но положительными делителями числа $p_i^{\alpha_i}$ являются только α_i+1 целых чисел $1, p_i, p_i^2, \ldots, p_i^{\alpha_i}$. Следовательно,

$$d(n)=\prod_{i=1}^{r}(\alpha_i+1).$$

Функция $d(n)$ также допускает геометрическую интерпретацию. Число положительных делителей числа n равно числу решений уравнения $xy=n$ в положительных целых числах x, y. Следовательно, $d(n)$ равна числу целых точек (x, y) «верхнего правого квадранта» (x, y)-плоскости, которые лежат на гиперболе $xy=n$.

Порядок роста $d(n)$. Из теоремы 3 следует, что $d(n)$ может принимать сколь угодно большие значения. С другой стороны, $d(n)=2$, если n простое. Следовательно,

$$\lim_{n\to\infty} d(n)=2.$$

Теорема 4. *Для каждого* $\Delta>0$ *существует последовательность целых чисел* n_i, *для которых*

$$\frac{d(n_i)}{(\log n_i)^{\Delta}}\to\infty \qquad (1)$$

при $i\to\infty$.

Доказательство. Определим целое число k следующим образом: $k \leqslant \Delta < k+1$, если $\Delta > 0$. Пусть p_{k+1} будет $(k+1)$-м простым числом, и пусть

$$n = (2 \cdot 3 \cdot 5 \ldots p_{k+1})^m,$$

где m — положительное целое число. По теореме 3 мы имеем

$$d(n) = (m+1)^{k+1} > m^{k+1}.$$

Но

$$m^{k+1} = \left\{ \frac{\log n}{\log (2 \cdot 3 \cdot 5 \ldots p_{k+1})} \right\}^{k+1} > c (\log n)^{k+1} \qquad (2)$$

где константа c не зависит от n.

Положив $m = 1, 2, 3, \ldots$, мы получим бесконечную последовательность положительных целых чисел n, для которых

$$d(n) > c (\log n)^{k+1},$$

и, обозначив $k+1 = \Delta + \delta$ $(\delta > 0)$, мы будем иметь для этой последовательности

$$\frac{d(n)}{(\log n)^{\Delta}} > c (\log n)^{\delta} \to \infty \text{ при } n \to \infty.$$

Тем самым теорема доказана.

С другой стороны, справедлива

Теорема 5. *$d(n) = o(n^{\delta})$ для любого $\delta > 0$.*

Другими словами, $d(n)/n^{\delta} \to 0$ при $n \to \infty$. Для доказательства этой теоремы нам потребуется следующее утверждение:

Теорема 6. *Если f — мультипликативная арифметическая функция и*

$$f(p^m) \to 0 \text{ при } p^m \to \infty,$$

где p — простое число и m — положительное целое (т. е. $f(n) \to 0$, когда n пробегает множество степеней простых чисел), то $f(n) \to 0$ при $n \to \infty$.

Доказательство. Так как $f(p^m)\to 0$ при $p^m\to\infty$, то f удовлетворяет следующим условиям:

(i) существует положительная константа A, такая, что

$$|f(p^m)|<A$$

для всех m и p;

(ii) существует константа B, такая, что если $p^m>B$, то $|f(p^m)|<1$;

(iii) для данного $\varepsilon>0$ существует такое $N(\varepsilon)$, что если $p^m>N(\varepsilon)$, то $|f(p^m)|<\varepsilon$.

Ясно, что A и B не зависят от ε, m и p, а $N(\varepsilon)$ зависит лишь от ε.

Пусть

$$n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\dots p_r^{\alpha_r} \tag{3}$$

— каноническое разложение числа $n>1$. Поскольку f мультипликативна, мы имеем

$$f(n)=f\left(p_1^{\alpha_1}\right)\cdot f\left(p_2^{\alpha_2}\right)\dots f\left(p_r^{\alpha_r}\right). \tag{4}$$

Рассмотрим все степени простых p^α, и пусть C — число таких степеней, которые не превосходят B. Тогда C не зависит от n и ε. Для множителей $f(p_i^{\alpha_i})$ в разложении (4), соответствующих этим степеням, мы можем применить неравенство (i); следовательно, их произведение по абсолютной величине будет меньше чем A^C. Оставшиеся множители $f(n)$ в силу (ii) по абсолютной величине меньше 1.

Далее, имеется только конечное множество целых чисел вида p^α, которые не превосходят $N(\varepsilon)$. Следовательно, существует только конечное число целых, каноническое разложение которых состоит только из множителей вида p^α, где $p^\alpha\leqslant N(\varepsilon)$. Пусть $P(\varepsilon)$ — верхняя граница таких целых чисел.

Если мы возьмем $n>P(\varepsilon)$, то каноническое разложение числа n должно содержать по меньшей мере один сомножитель $p^\alpha>N(\varepsilon)$ и мы можем применить тогда неравенство (iii), а именно $|f(p^\alpha)|<\varepsilon$.

Следовательно, если $n>P(\varepsilon)$, то мы имеем

$$|f(n)|<A^c\cdot\varepsilon,$$

так что $f(n)\to 0$ при $n\to\infty$.

Доказательство теоремы 5. Функция $f(n)=d(n)/n^\delta$ мультипликативна и

$$f(p^m)=\frac{m+1}{p^{m\delta}}\leqslant\frac{2m}{p^{m\delta}}=\frac{2}{p^{m\delta}}\cdot\frac{\log p^m}{\log p}.$$

Так как $\log p\geqslant\log 2$, то отсюда для каждого $\delta>0$

$$f(p^m)\leqslant\frac{2}{\log 2}\cdot\frac{\log p^m}{p^{m\delta}}\to 0 \text{ при } p^m\to\infty.$$

Следовательно, по теореме 6

$$\frac{d(n)}{n^\delta}\to 0 \text{ при } n\to\infty$$

для каждого $\delta>0$; тем самым теорема 5 доказана.

Можно показать, что для данного $\varepsilon>0$ существует такое число $N(\varepsilon)$, что

$$d(n)<2^{(1+\varepsilon)\frac{\log n}{\log\log n}}$$

при $n>N(\varepsilon)$ и, кроме того, что существует бесконечно много целых чисел n, для которых

$$d(n)>2^{(1-\varepsilon)\frac{\log n}{\log\log n}}.$$

Порядок роста $d(n)$ в среднем. Рассмотрим сумматорную функцию

$$D(N)=\sum_{n=1}^{N}d(n).$$

Так как $d(n)=\sum_{t|n}1=\sum_{xy=n}1$, мы имеем

$$D(N)=\sum_{n=1}^{N}d(n)=\sum_{1\leqslant n\leqslant N}\sum_{xy=n}1,$$

или

$$D(N)=\sum_{1\leqslant xy\leqslant N}1.$$

Ясно, что $D(N)$ представляет собой число целых точек «первого» квадранта (т. е. верхнего правого квадранта), лежащих на или ниже гиперболы $xy=N$, при этом целые точки, лежащие на осях координат, исключаются, так как для них $xy=0$.

Чтобы оценить порядок роста $D(N)$, нам потребуется следующая теорема:

Теорема 7. *Пусть g — монотонно убывающая функция действительного переменного t, определенная при $t\geqslant 0$, причем $g(t)>0$ при $t\geqslant 1$. Тогда*

$$\sum_{1\leqslant n\leqslant X} g(n) = \int_1^X g(t)\,dt + A + O(g(X)),$$

где n — целое положительное число, $X\geqslant 1$ и A — постоянная, зависящая только от g.

Доказательство. Рассмотрим замкнутый интервал $[n, n+1]$. Так как g — убывающая функция, то

$$g(n+1) \leqslant \int_n^{n+1} g(t)\,dt \leqslant g(n).$$

Следовательно,

$$0 \leqslant A_n = g(n) - \int_n^{n+1} g(t)\,dt \leqslant g(n) - g(n+1).$$

Пусть M и N — произвольные положительные целые числа и $M<N$. Тогда

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

и из условия $g(t)>0$ при $t\geqslant 1$ мы получаем

$$\sum_{n=M}^{N} A_n \leqslant g(M) \text{ для всех } N > M. \tag{5}$$

В частности, $\sum\limits_{n=1}^{\infty} A_n \leqslant g(1)$, так что ряд $\sum\limits_{n=1}^{\infty} A_n$ сходится.

Положим

$$\sum_{n=1}^{\infty} A_n = A.$$

Тогда в силу (5) мы имеем

$$A = \sum_{n=1}^{N} A_n + \sum_{n=N+1}^{\infty} A_n = \sum_{n=1}^{N} A_n + O(g(N+1))$$

или

$$A = \sum_{n=1}^{N} \left\{ g(n) - \int_{n}^{n+1} g(t)\,dt \right\} + O(g(N+1)),$$

откуда следует, что

$$\sum_{n=1}^{N} g(n) = \int_{1}^{N+1} g(t)\,dt + A + O(g(N+1)).$$

Положим $N = [X]$. Тогда последнее равенство перепишется в виде

$$\sum_{1 \leqslant n \leqslant X} g(n) = \int_{1}^{[X]+1} g(t)\,dt + A + O(g([X]+1)),$$

где n пробегает только целые значения.

Но функция g положительная и убывающая, так что

$$\int_{X}^{[X]+1} g(t)\,dt \leqslant g(X), \qquad 0 < g([X]+1) \leqslant g(X),$$

откуда

$$\sum_{1 \leqslant n \leqslant X} g(n) = \int_{1}^{X} g(t)\,dt + A + O(g(X)),$$

что и требовалось доказать.

Следствие 1. *Существует постоянная* γ (*постоянная Эйлера*), *такая, что*

$$\sum_{1 \leqslant n \leqslant X} \frac{1}{n} = \log X + \gamma + O\left(\frac{1}{X}\right).$$

Следствие 2. *Так как*

$$\int_2^X \frac{dt}{t \log t} = \log\log X - \log\log 2,$$

то

$$\sum_{2 \leqslant n \leqslant X} \frac{1}{n \log n} = \log\log X + B + O\left(\frac{1}{X \log X}\right),$$

где B — константа.

Мы можем теперь доказать следующую теорему:

Теорема 8. $D(N) = N \log N + O(N)$.

Доказательство. Как уже отмечалось, $D(N)$ представляет собой число целых точек в правом верхнем квадранте (x, y)-плоскости, которые лежат на или ниже гиперболы $xy = N$, но не лежат на координатных осях. Очевидно, эти точки лежат левее прямой $x = N$ и ниже прямой $y = N$ (рис. 3). Сосчитаем число целых точек на каждой

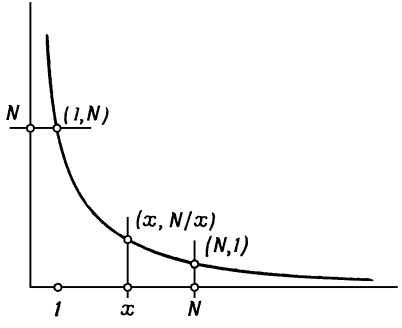

Рис. 3.

из вертикальных прямых, пересекающих ось абсцисс в целых точках. Число целых точек на вертикальной прямой, ординаты которых не превосходят величины N/x, равно $[N/x]$, так что

$$D(N) = \sum_{x=1}^{N} \left[\frac{N}{x}\right].$$

Положим $[N/x]=N/x-\theta_x$, где $0\leqslant\theta_x<1$. Тогда

$$D(N)=N\sum_{x=1}^{N}\frac{1}{x}-\sum_{x=1}^{N}\theta_x=N\sum_{x=1}^{N}\frac{1}{x}+O(N),$$

поскольку $\sum\limits_{x=1}^{N}\theta_x<N$, и по следствию 1 теоремы 7

$$D(N)=N\log N+O(N).$$

Теорема доказана.

Теорема 8 может быть значительно усилена. В качестве первого шага мы докажем следующий результат:

Теорема 9 (Дирихле). $D(N)=N\log N+(2\gamma-1)N+O(\sqrt{N})$, *где* γ *— постоянная Эйлера.*

Доказательство. Гипербола $xy=N$ симметрична относительно прямой $x=y$. Следовательно, области $ABGEO$ и $CDOFG$ (рис. 4) содержат одно и то же число

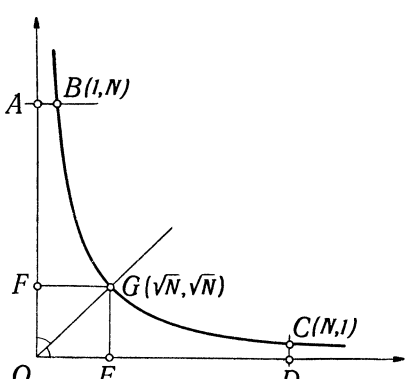

Рис. 4.

целых точек. Общее число целых точек в первом квадранте, которые лежат на или ниже гиперболы (но не лежат на осях координат), равно поэтому удвоенному числу целых точек в области $ABGEO$ минус число целых то-

чек в квадрате $OFGE$. Таким образом,

$$D(N)=2\sum_{\substack{1\leqslant x\leqslant\sqrt{N}\\ 1\leqslant xy\leqslant N}}1-[\sqrt{N}]^2=2\sum_{1\leqslant x\leqslant\sqrt{N}}\sum_{1\leqslant y\leqslant N/x}1-[\sqrt{N}]^2=$$

$$=2\sum_{1\leqslant x<\sqrt{N}}\left[\frac{N}{x}\right]-[\sqrt{N}]^2.$$

Пусть $[N/x]=N/x-\theta_x$, $0\leqslant\theta_x<1$, и $[\sqrt{N}]=\sqrt{N}-\theta$, $0\leqslant\theta<1$. Тогда мы получим

$$D(N)=2N\sum_{1\leqslant x\leqslant\sqrt{N}}\frac{1}{x}-2\sum_{1\leqslant x<\sqrt{N}}\theta_x-(\sqrt{N}-\theta)^2=$$

$$=2N\sum_{1\leqslant x\leqslant\sqrt{N}}\frac{1}{x}-N-2\sum_{1\leqslant x<\sqrt{N}}\theta_x+2\theta\sqrt{N}-\theta^2.$$

Но

$$\sum_{1\leqslant x<\sqrt{N}}\theta_x=O(\sqrt{N}),\quad \theta^2=O(1);$$

следовательно,

$$D(N)=2N\sum_{1\leqslant x\leqslant\sqrt{N}}\frac{1}{x}-N+O(\sqrt{N}).$$

В силу следствия 1 теоремы 7

$$D(N)=N\log N+(2\gamma-1)N+O(\sqrt{N}),$$

что и требовалось доказать.

Остаточный член $O(\sqrt{N})$ в теореме 9 был улучшен Г. Вороным и доведен до $O(N^{1/3}\log N)$. Существует гипотеза, что остаточный член на самом деле есть $O(N^{1/4+\varepsilon})$. С другой стороны, известно, что остаточный член в теореме 9 не может быть доведен до $O(N^{1/4})$.

§ 4. Функция $\sigma(n)$. Связанная с функцией $d(n)$ арифметическая функция $\sigma(n)$ определяется как сумма положительных делителей числа n. В общем случае мы можем определить

$$\sigma_k(n) = \sum_{d|n} d^k, \quad k = 0, 1, 2, \ldots,$$

так что $\sigma_0(n) = d(n)$ и $\sigma(n) = \sigma_1(n)$.

Теорема 10. *Арифметическая функция* $\sigma_k(n)$ *мультипликативна.*

Доказательство. Рассуждения, аналогичные рассуждениям теоремы 2, показывают, что если $(m, n) = 1$, то

$$\sum_{d|m} d \sum_{d'|n} d' = \sum_{d^*|mn} d^*.$$

Отсюда следует мультипликативность $\sigma(n)$. Подобным же образом доказывается и мультипликативность $\sigma_k(n)$.

Теорема 11. *Пусть* $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ *— каноническое разложение числа* $n > 1$. *Тогда*

$$\sigma_k(n) = \prod_{i=1}^{r} \frac{p_i^{(\alpha_i+1)k} - 1}{p_i^k - 1}. \tag{6}$$

Доказательство. Поскольку функция $\sigma_k(n)$ мультипликативна, мы имеем

$$\sigma_k(n) = \prod_{i=1}^{r} \sigma_k(p_i^{\alpha_i}) = \prod_{i=1}^{r} (1 + p_i^k + p_i^{2k} + \ldots + p_i^{\alpha_i k}) =$$

$$= \prod_{i=1}^{r} \frac{p_i^{(\alpha_i+1)k} - 1}{p_i^k - 1}$$

и, в частности, при $k = 1$

$$\sigma_1(n) = \sigma(n) = \prod_{i=1}^{r} \frac{p_i^{(\alpha_i+1)} - 1}{p_i - 1}. \tag{7}$$

С функцией $\sigma(n)$ связана старая проблема совершенных чисел. Положительное число N называется *совер-*

шенным, если $\sigma(N)=2N$, т. е. N равно сумме всех его положительных делителей, меньших N. Например, 6 и 28 являются совершенными числами.

Целые числа вида 2^n-1 называются *числами Мерсенна*, а простые числа такого вида называются *простыми числами Мерсенна*.

Связь между простыми числами Мерсенна и совершенными числами устанавливается следующей теоремой:

Теорема 12. *Если $2^{n+1}-1$ является простым числом, то $2^n(2^{n+1}-1)$ есть совершенное число.*

Доказательство. Пусть $N=2^n(2^{n+1}-1)=2^np$, где p простое. Тогда, согласно (7),

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

Следовательно, N — совершенное число.

Эйлер заметил, что этот результат можно частично обратить, а именно, справедлива следующая теорема:

Теорема 13 (Эйлер). *Каждое четное совершенное число имеет вид 2^np, где $p=2^{n+1}-1$ есть простое число Мерсенна.*

Доказательство. Пусть $N=2^nN'$ — совершенное число, где $n\geqslant 1$, и N' — нечетное число. Тогда

$$\sigma(N)=2N=2^{n+1}N'.$$

В силу мультипликативности σ мы имеем

$$\sigma(N)=\sigma(2^n)\sigma(N'),$$

и так как, согласно (7), $\sigma(2^n)=2^{n+1}-1$, то

$$(2^{n+1}-1)\sigma(N')=2^{n+1}N'.$$

Следовательно, $(2^{n+1}-1)\mid N'$. Если мы положим $N'=(2^{n+1}-1)N''$, то $\sigma(N')=2^{n+1}N''$, где $N''<N'$. Но $N'+N''=2^{n+1}N''=\sigma(N')$. Таким образом, и N', и N'' делят N' и их сумма равна $\sigma(N')$. Значит, число N' не может иметь других делителей и потому оно является простым. Но $N'=(2^{n+1}-1)N''$. Следовательно, $N'=2^{n+1}-1$, $N''=1$. Тем самым теорема 13 доказана.

Неизвестно, будет ли бесконечным множество *четных* совершенных чисел (т. е. неизвестно, будет ли бесконеч-

ным множество простых вида 2^n-1). Неизвестно также, существуют ли *нечетные* совершенные числа.

Простые числа Мерсенна — это простые числа вида 2^n-1. Легко видеть, что если $n>1$, a — положительное целое число и a^n-1 является простым числом, то $a=2$ и n также должно быть простым числом. Действительно, если $a>2$, то $(a-1)\mid(a^n-1)$. Если же $a=2$ и $n=kl$, $1<k\leqslant l$, то $(2^k-1)\mid(2^n-1)$.

§ 5. Функция Мёбиуса $\mu(n)$. Функция Мёбиуса $\mu(n)$ — это арифметическая функция, которая определяется следующим образом:

(i) $\mu(1)=1$;

(ii) $\mu(n)=(-1)^k$, если n есть произведение k различных простых чисел;

(iii) $\mu(n)=0$ в противном случае, т. е. если n делится на квадрат целого числа, отличного от единицы.

Из определения сразу же вытекает

Теорема 14. *Функция Мёбиуса* $\mu(n)$ *мультипликативна.*

Теорема 15. *Справедливо соотношение*

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

Доказательство. Пусть $n=\prod_{i=1}^{m}p_i^{\alpha_i}$ — каноническое разложение числа $n>1$. Делители d числа n, для которых $\mu(d)\neq 0$, имеют вид

$$1,\ p_1, p_2, \ldots, p_m,\quad p_ip_j\,(i\neq j),\quad p_ip_jp_k\,(i\neq j\neq k),\ \ldots,\ p_1p_2\ldots p_m.$$

Тогда

$$\sum_{d\mid n}\mu(d)=\mu(1)+\sum_{i}\mu(p_i)+\sum_{i<j}\mu(p_ip_j)+\ldots+\mu(p_1p_2\ldots p_m)$$

и, следовательно,

$$\sum_{d\mid n}\mu(d)=1-\binom{m}{1}+\binom{m}{2}-\binom{m}{3}+\ldots=(1-1)^m=0.$$

Заметим, что функцию Мёбиуса можно определить, используя теорему 15, и вывести из нее свойства (i), (ii), (iii).

Наиболее важные приложения этой функции основаны на так называемых формулах обращения Мёбиуса.

Теорема 16 (первая формула обращения Мёбиуса). *Пусть f — арифметическая функция и*

$$g(n) = \sum_{d|n} f(d).$$

Тогда

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

Доказательство. Мы имеем

$$\sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{d' \left| \frac{n}{d}\right.} f(d') =$$

$$= \sum_{dd'|n} \mu(d)\, f(d') = \sum_{d'|n} f(d') \sum_{d \left| \frac{n}{d'}\right.} \mu(d)$$

и, следовательно, по теореме 15

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

Справедливо и обратное утверждение:

Теорема 17. *Если*

$$h(n) = \sum_{d|n} \mu(d)\, f\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d),$$

то

$$f(n) = \sum_{d|n} h(d).$$

Доказательство. Мы имеем по теореме 15

$$\sum_{d|n} h(d) = \sum_{d|n} h\left(\frac{n}{d}\right) = \sum_{d|n} \sum_{d'\left|\frac{n}{d}\right.} \mu\left(\frac{n}{dd'}\right) f(d') =$$

$$= \sum_{dd'|n} \mu\left(\frac{n}{dd'}\right) f(d') =$$

$$= \sum_{d'|n} f(d') \sum_{d\left|\frac{n}{d'}\right.} \mu\left(\frac{n}{dd'}\right) = f(n).$$

В качестве приложения теоремы 16 рассмотрим соотношение

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

которое было доказано в теореме 6 гл. II. Из теоремы 16 следует, что

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d}. \tag{8}$$

Другое приложение этой теоремы связано с *функцией Мангольдта* Λ, которая определяется следующим образом:

$$\Lambda(n) = \begin{cases} \log p, & \text{если } n = p^m, \ p \text{ простое}, \ m > 0, \\ 0, & \text{если } n \neq p^m. \end{cases}$$

Теорема 18. $\sum_{d|n} \Lambda(d) = \log n.$

Доказательство. Пусть $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ — каноническое разложение числа $n > 1$. Тогда по определению Λ мы имеем

$$\sum_{d|n} \Lambda(d) = \sum_{i=1}^{r} \sum_{\alpha=1}^{\alpha_i} \Lambda(p_i^{\alpha}) = \sum_{i=1}^{r} \alpha_i \log p_i = \log n.$$

Тем самым теорема доказана.

Объединяя первую формулу обращения Мёбиуса и теорему 18, получаем

$$\Lambda(n)=\sum_{d|n}\mu(d)\log\frac{n}{d},$$

и так как по теореме 15 $\sum_{d|n}\mu(d)=0$ при $n>1$ и $\log 1=0$, то отсюда следует, что

$$\Lambda(n)=-\sum_{d|n}\mu(d)\log d. \tag{9}$$

Теорема 19 (вторая формула обращения Мёбиуса). *Пусть функция f определена при $x\geqslant 1$ и*

$$g(x)=\sum_{n\leqslant x}f\left(\frac{x}{n}\right).$$

Тогда при $x\geqslant 1$

$$f(x)=\sum_{n\leqslant x}\mu(n)\,g\left(\frac{x}{n}\right),$$

и обратно.

Сумма $\sum_{n\leqslant x}$ интерпретируется как $\sum_{n=1}^{[x]}$, а сумма, не содержащая членов, полагается равной нулю.

Доказательство. Из определения функции g мы имеем при $x\geqslant 1$

$$\sum_{n\leqslant x}\mu(n)\,g\left(\frac{x}{n}\right)=\sum_{n\leqslant x}\mu(n)\sum_{m\leqslant\frac{x}{n}}f\left(\frac{x}{mn}\right)=\sum_{\substack{m,n\\ 1\leqslant mn\leqslant x}}\mu(n)f\left(\frac{x}{mn}\right).$$

Группируя в последней сумме члены, для которых $mn=r$, $1\leqslant r\leqslant x$, получаем

$$\sum_{\substack{m,n\\ 1\leqslant mn\leqslant x}}\mu(n)f\left(\frac{x}{mn}\right)=\sum_{1\leqslant r\leqslant x}f\left(\frac{x}{r}\right)\sum_{n|r}\mu(n)=f(x).$$

Итак, первая часть теоремы доказана.

Чтобы доказать обратное утверждение, положим при $x \geqslant 1$

$$f(x) = \sum_{n \leqslant x} \mu(n)\, g\left(\frac{x}{n}\right).$$

Тогда

$$\sum_{m \leqslant x} f\left(\frac{x}{m}\right) = \sum_{m \leqslant x} \sum_{n \leqslant \frac{x}{m}} \mu(n) g\left(\frac{x}{mn}\right) = \sum_{\substack{m,n \\ 1 \leqslant mn \leqslant x}} \mu(n) g\left(\frac{x}{mn}\right)$$

и так же, как выше, последняя сумма может быть записана в виде

$$\sum_{1 \leqslant r \leqslant x} g\left(\frac{x}{r}\right) \sum_{n \mid r} \mu(n) = g(x).$$

§ 6. Функция Эйлера $\varphi(n)$. Вернемся к функции Эйлера φ. Мы знаем, что $\varphi(n) < n$ при $n > 1$. С другой стороны, если $n = p^m$, где p — простое число, $p > 1/\varepsilon$, $0 < \varepsilon < 1$, и $m \geqslant 1$, то [см. гл. II]

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

Из этих неравенств следует

Теорема 20. $\overline{\lim\limits_{n \to \infty}} \dfrac{\varphi(n)}{n} = 1.$

Другой результат о порядке роста $\varphi(n)$ дает

Теорема 21. *Для каждого* $\delta > 0$ *мы имеем*

$$\frac{\varphi(n)}{n^{1-\delta}} \to \infty \quad \textit{при} \quad n \to \infty.$$

Доказательство. Результат очевиден, если $\delta > 1$. Пусть $\delta \leqslant 1$ и

$$f(n) = \frac{n^{1-\delta}}{\varphi(n)}.$$

Тогда f мультипликативна, и в силу теоремы 6 достаточ-

но показать, что $f(p^m)\to 0$ при $p^m\to\infty$. В самом деле, для каждого $\delta>0$ мы имеем

$$\frac{1}{f(p^m)}=\frac{\varphi(p^m)}{p^{m(1-\delta)}}=p^{m\delta}\left(1-\frac{1}{p}\right)\geqslant\frac{1}{2}p^{m\delta}\to\infty$$

при $p^m\to\infty$.

Из теоремы 20 или теоремы 21 следует, что утверждение $\varphi(n)=O(n^{\Delta})$ неверно, если $\Delta<1$.

Порядок роста $\varphi(n)$ в среднем. Изучим поведение сумматорной функции для функции φ, а именно

$$\Phi(t)=\sum_{1\leqslant n\leqslant t}\varphi(n).$$

Заметим, что значение $\Phi(N)$ равно числу членов в последовательности Фарея порядка N.

Теорема 22 (Мертенс). $\Phi(t)=\dfrac{3t^2}{\pi^2}+O(t\log t)$.

Доказательство. Мы имеем

$$\Phi(t)=\sum_{1\leqslant n\leqslant t}\ \sum_{\substack{1\leqslant m\leqslant n\\(m,n)=1}}1=\sum_{\substack{1\leqslant m\leqslant n\leqslant t\\(m,n)=1}}1,$$

и, следовательно, $\Phi(t)$ равна числу целых точек с взаимно простыми координатами, которые лежат в прямоугольном треугольнике $0<y\leqslant x\leqslant t$.

Рассмотрим квадрат $0<x\leqslant t$, $0<y\leqslant t$. Прямая $x=y$ делит этот квадрат на два прямоугольных треугольника, каждый из которых содержит одно и то же число целых точек с взаимно простыми координатами. Один из этих треугольников является данным треугольником $0<y\leqslant x\leqslant t$. Заметим, что на прямой $x=y$ лежит единственная точка $x=y=1$ с взаимно простыми координатами.

Обозначим через $\Psi(t)$ число целых точек с взаимно простыми координатами в упомянутом выше квадрате. Тогда

$$\Psi(t)=2\Phi(t)-1, \tag{10}$$

так как точка $x=y=1$ содержится в обоих треугольниках.

Общее число целых точек в квадрате $0<x\leqslant t$, $0<y\leqslant t$ равно $[t]^2$, так что

$$[t]^2=\sum_{\substack{0<m\leqslant t\\ 0<n\leqslant t}} 1.$$

Отсюда мы получаем

$$[t]^2=\sum_{1\leqslant d\leqslant t}\ \sum_{\substack{0<m\leqslant t\\ 0<n\leqslant t\\ (m,n)=d}} 1. \tag{11}$$

Далее, $(m, n)=d$ тогда и только тогда, когда $(m/d, n/d)=1$. Следовательно, существует взаимно однозначное соответствие между целыми точками с координатами m, n, где $0<m\leqslant t$, $0<n\leqslant t$, $(m, n)=d$, и парами целых чисел m', n', такими, что

$$0<m'\leqslant\frac{t}{d},\quad 0<n'\leqslant\frac{t}{d},\quad (m', n')=1.$$

Но по определению Ψ имеется в точности $\Psi(t/d)$ таких пар m', n'. Таким образом, равенство (11) может быть переписано в виде

$$[t]^2=\sum_{1\leqslant d\leqslant t}\Psi\left(\frac{t}{d}\right), \tag{12}$$

и, применяя к равенству (12) вторую формулу обращения Мёбиуса, мы получаем при $t\geqslant 1$

$$\Psi(t)=\sum_{1\leqslant d\leqslant t}\mu(d)\left[\frac{t}{d}\right]^2.$$

Пусть $t/d=[t/d]+\theta$, где $0\leqslant\theta<1$. Тогда

$$\Psi(t)=\sum_{1\leqslant d\leqslant t}\mu(d)\left\{\frac{t}{d}+O(1)\right\}^2=$$

$$=t^2\sum_{1\leqslant d\leqslant t}\frac{\mu(d)}{d^2}+2t\cdot O\left(\sum_{1\leqslant d\leqslant t}\frac{1}{d}\right)+O\left(\sum_{1\leqslant d\leqslant t}1\right),$$

так как $|\mu(n)|\leqslant 1$. В силу следствия 1 теоремы 7 мы знаем, что

$$2t\cdot O\Big(\sum_{1\leqslant d\leqslant t}\frac{1}{d}\Big)=2t\cdot O\Big(\log t+\gamma+O\Big(\frac{1}{t}\Big)\Big)=O(t\log t)$$

и $O(\sum\limits_{1\leqslant d\leqslant t}1)=O(t)$. Следовательно,

$$\Psi(t)=t^2\sum_{1\leqslant d\leqslant t}\frac{\mu(d)}{d^2}+O(t\log t). \tag{13}$$

Чтобы оценить сумму в формуле (13), заметим, что

$$\sum_{1\leqslant d\leqslant t}\frac{\mu(d)}{d^2}=\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}-\sum_{d=[t]+1}^{\infty}\frac{\mu(d)}{d^2}$$

и

$$\Big|\sum_{d=[t]+1}^{\infty}\frac{\mu(d)}{d^2}\Big|<\sum_{d=[t]+1}^{\infty}\frac{1}{d^2}<\int_{[t]}^{\infty}\frac{du}{u^2}=\frac{1}{[t]}=O\Big(\frac{1}{t}\Big).$$

Тогда из (13) следует, что

$$\Psi(t)=t^2\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}+O(t\log t). \tag{14}$$

Ряд $\sum\limits_{d=1}^{\infty}\frac{\mu(d)}{d^2}$ можно вычислить следующим образом. Поскольку оба ряда $\sum\limits_{n=1}^{\infty}\frac{1}{n^2}$ и $\sum\limits_{m=1}^{\infty}\frac{\mu(m)}{m^2}$ сходятся абсолютно, то, перемножив их, мы получим

$$\sum_{n=1}^{\infty}\frac{1}{n^2}\cdot\sum_{m=1}^{\infty}\frac{\mu(m)}{m^2}=\sum_{\nu=1}^{\infty}\frac{c_\nu}{\nu^2},$$

где

$$c_\nu=\sum_{k|\nu}\mu(k).$$

Но $\sum\limits_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}$ и $c_1=1$, $c_n=0$ при $n>1$ по теореме 15.

Следовательно,

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \left(\sum_{n=1}^{\infty} \frac{1}{n^2}\right)^{-1} = \frac{6}{\pi^2},$$

и, подставляя это значение в (14), мы получим

$$\Psi(t) = \frac{6t^2}{\pi^2} + O(t \log t).$$

Отсюда и из (10) следует, что

$$\Phi(t) = \frac{3t^2}{\pi^2} + O(t \log t), \tag{15}$$

как и утверждалось.

Соотношение между φ и σ. Интересно отметить, что из результатов о поведении функции φ следуют результаты о поведении функции σ, и наоборот. Это вытекает из следующей теоремы:

Теорема 23. *Существует положительная константа C, такая, что*

$$C < \frac{\sigma(n)\,\varphi(n)}{n^2} < 1 \quad \textit{при всех} \quad n \geqslant 2. \tag{16}$$

Доказательство. Пусть $n = \prod_{p \mid n} p^{\alpha}$. Тогда, изменив очевидным образом обозначения, мы имеем, согласно (7),

$$\sigma(n) = \prod_{p \mid n} \frac{p^{\alpha+1} - 1}{p - 1} = n \prod_{p \mid n} \frac{1 - p^{-\alpha-1}}{1 - p^{-1}}.$$

Поскольку

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

мы имеем

$$\frac{\sigma(n)\,\varphi(n)}{n^2} = \prod_{p \mid n} \left(1 - \frac{1}{p^{\alpha+1}}\right) < 1.$$

Тем самым доказано второе неравенство в (16).

С другой стороны,

$$\prod_{p|n}\left(1-\frac{1}{p^{\alpha+1}}\right)\geqslant\prod_{p|n}\left(1-\frac{1}{p^2}\right)>\prod_{p}\left(1-\frac{1}{p^2}\right),$$

причем $1-1/p^2<1$ и произведение в правой части распространяется на *все* простые числа p. Тем самым доказано и первое неравенство в (16).

ТЕОРЕМА ЧЕБЫШЕВА О РАСПРЕДЕЛЕНИИ ПРОСТЫХ ЧИСЕЛ

§ 1. Функции Чебышева. В гл. I мы установили, что существует бесконечно много простых чисел. Следовательно, если мы обозначим через $\pi(x)$ количество простых чисел, не превосходящих x, то $\pi(x)\to\infty$ при $x\to\infty$. Асимптотический закон распределения простых чисел, который мы докажем в гл. XI, даст нам много больше, а именно

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

В этой главе мы докажем несколько интересных промежуточных результатов. Начнем с результата Эйлера о том, что сумма $\sum 1/p$, где суммирование распространяется на все простые числа, расходится, откуда следует, что простых чисел бесконечно много.

Теорема 1 (Эйлер). *Пусть p пробегает множество всех простых чисел. Тогда сумма $\sum 1/p$ и произведение $\prod(1-1/p)^{-1}$ расходятся.*

Доказательство. Докажем сначала, что произведение $\prod(1-1/p)^{-1}$ расходится, и выведем отсюда утверждение о расходимости ряда $\sum 1/p$. Пусть

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

Для действительного числа u, $0<u<1$, и положительного целого m мы имеем

$$\frac{1}{1-u}>\frac{1-u^{m+1}}{1-u}=1+u+\cdots+u^m.$$

Положим $u=1/p$, где p — простое число. Тогда из последнего неравенства следует, что для всех простых $p\leqslant x$

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

Выберем теперь m так, чтобы выполнялось неравенство $2^m \geqslant x$. Тогда

$$\prod_{p \leqslant x} \left(1 + \frac{1}{p} + \ldots + \frac{1}{p^m}\right) \geqslant \sum_{n=1}^{[x]} \frac{1}{n}.$$

Действительно, каждое целое число n, $1 < n \leqslant [x]$, имеет в качестве простых сомножителей только простые числа $p \leqslant x$, а неравенство $2^m \geqslant x$ гарантирует, что после разложения левой части последнего неравенства в сумму каждое слагаемое правой части встретится среди слагаемых левой части. Таким образом,

$$P(x) > \sum_{n=1}^{[x]} \frac{1}{n} > \int_1^{[x]+1} \frac{du}{u} > \log x$$

и, следовательно, произведение $\prod (1-1/p)^{-1}$ расходится.

Чтобы доказать расходимость ряда $\sum \frac{1}{p}$, рассмотрим разложение

$$\log\left(\frac{1}{1-u}\right) = u + \frac{u^2}{2} + \frac{u^3}{3} + \cdots, \quad -1 \leqslant u < 1.$$

Для $u > 0$ мы имеем

$$\log\left(\frac{1}{1-u}\right) - u < \frac{1}{2}(u^2 + u^3 + u^4 + \ldots).$$

Геометрический ряд в правой части последнего неравенства сходится при $|u| < 1$, так что

$$\log\left(\frac{1}{1-u}\right) - u < \frac{u^2}{2(1-u)}, \quad 0 < u < 1.$$

Положим теперь $u = 1/p$ и просуммируем неравенства

$$\log\left(\frac{1}{1-1/p}\right) - \frac{1}{p} < \frac{1}{2p(p-1)}$$

по всем $p \leqslant x$. Мы получим

$$\log P(x) - S(x) < \frac{1}{2} \sum_{p \leqslant x} \frac{1}{p(p-1)} < \frac{1}{2} \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = \frac{1}{2},$$

так что

$$S(x) > \log P(x) - \frac{1}{2} > \log\log x - \frac{1}{2}.$$

Следовательно, ряд $\sum 1/p$ расходится, и теорема 1 полностью доказана.

Функции ϑ и ψ. Функции Чебышева ϑ и ψ определяются следующим образом:

$$\vartheta(x) = \sum_{p \leqslant x} \log p, \quad x > 0, \quad p \text{ — простое число}, \tag{1}$$

и

$$\psi(x) = \sum_{p^m \leqslant x} \log p, \quad x > 0. \tag{2}$$

Сумма (2) распространяется на все пары p, m, где p — простое, а m — положительные целые числа, такие, что $p^m \leqslant x$. Это означает, что если p^m — наибольшая степень p, не превосходящая x, то $\log p$ в сумме (2) засчитывается точно m раз. Например,

$$\psi(10) = 3\log 2 + 2\log 3 + \log 5 + \log 7.$$

В § 5 гл. VI мы ввели функцию Мангольдта

$$\Lambda(n) = \begin{cases} \log p, & \text{если } n = p^m, \text{ где } m\text{—положительное целое число,} \\ 0, & \text{если } n \neq p^m. \end{cases}$$

Из определения ψ непосредственно следует, что

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

Далее, из (1) и (2) вытекает, что $e^{\vartheta(x)}$ равно произведению всех простых $p \leqslant x$ и при $x \geqslant 1$ $e^{\psi(x)}$ есть наименьшее общее кратное всех положительных целых чисел $\leqslant x$. Если $p^m \leqslant x$, то $p \leqslant x^{1/m}$, и обратно. Тогда из (2) следует, что

$$\psi(x) = \vartheta(x) + \vartheta(x^{1/2}) + \vartheta(x^{1/3}) + \ldots, \tag{4}$$

причем этот ряд конечен, так как $\vartheta(x) = 0$ для $x < 2$. Если $p^m \leqslant x < p^{m+1}$, $x \geqslant 1$, то $\log p$ в формуле (3) для $\psi(x)$ встречается точно m раз и $m = [\log x/\log p]$. Следователь-

но, мы получаем четвертое выражение для $\psi(x)$, именно

$$\psi(x)=\sum_{p\leqslant x}\left[\frac{\log x}{\log p}\right]\cdot\log p. \tag{5}$$

Установим теперь связь между функциями

$$\frac{\pi(x)}{x/\log x},\quad \frac{\vartheta(x)}{x},\quad \frac{\psi(x)}{x}.$$

Теорема 2. *Пусть*

$$l_1=\varliminf_{x\to\infty}\frac{\pi(x)}{x/\log x},\qquad L_1=\varlimsup_{x\to\infty}\frac{\pi(x)}{x/\log x},$$

$$l_2=\varliminf_{x\to\infty}\frac{\vartheta(x)}{x},\qquad L_2=\varlimsup_{x\to\infty}\frac{\vartheta(x)}{x},$$

$$l_3=\varliminf_{x\to\infty}\frac{\psi(x)}{x}.\qquad L_3=\varlimsup_{x\to\infty}\frac{\psi(x)}{x}.$$

Тогда $l_1=l_2=l_3$ *и* $L_1=L_2=L_3$.

Доказательство. Из (4) следует, что $\vartheta(x)\leqslant\psi(x)$. Далее, из (5) вытекает, что

$$\psi(x)\leqslant\sum_{p\leqslant x}\frac{\log x}{\log p}\cdot\log p=\log x\sum_{p\leqslant x}1,$$

так что

$$\psi(x)\leqslant\pi(x)\log x.$$

Следовательно,

$$\vartheta(x)\leqslant\psi(x)\leqslant\pi(x)\log x.$$

Если теперь мы разделим эти неравенства на x и устремим x к бесконечности, то получим

$$L_2\leqslant L_3\leqslant L_1. \tag{6}$$

Выберем действительное число α, $0<\alpha<1$, и пусть $x>1$. Тогда

$$\vartheta(x)\geqslant\sum_{x^\alpha<p\leqslant x}\log p,$$

и так как $\log p > \log x^{\alpha}$, то

$$\vartheta(x) \geqslant \alpha \log x \sum_{x^{\alpha} < p \leqslant x} 1.$$

Таким образом,

$$\vartheta(x) \geqslant \alpha \log x \,(\pi(x) - \pi(x^{\alpha})).$$

Но, очевидно, $\pi(x^{\alpha}) < x^{\alpha}$, так что

$$\vartheta(x) > \alpha \pi(x) \log x - \alpha x^{\alpha} \log x,$$

или

$$\frac{\vartheta(x)}{x} > \alpha \pi(x) \frac{\log x}{x} - \alpha \frac{\log x}{x^{1-\alpha}}.$$

Далее, $0 < \alpha < 1$, откуда $(\log x / x^{1-\alpha}) \to 0$ при $x \to \infty$. Следовательно,

$$L_2 \geqslant \alpha L_1$$

для любого действительного α, $0 < \alpha < 1$. Поэтому $L_2 \geqslant L_1$, и, сравнивая это неравенство с (6), мы получаем

$$L_1 = L_2 = L_3.$$

Доказательство того, что $l_1 = l_2 = l_3$, приводится таким же образом. Из теоремы 2 следует, что если одна из трех функций

$$\frac{\pi(x)}{x/\log x}, \qquad \frac{\vartheta(x)}{x}, \qquad \frac{\psi(x)}{x}$$

имеет предел при $x \to \infty$, то другие две функции также имеют пределы при $x \to \infty$ и все эти три предела совпадают. Таким образом, для того чтобы доказать асимптотический закон распределения простых чисел, достаточно доказать, что $\lim\limits_{x \to \infty} \psi(x)/x = 1$.

§ 2. Теорема Чебышева. Мы используем теорему 2 для доказательства следующей теоремы:

Теорема 3 (Чебышев). *Существуют постоянные a и A, $0 < a < A$, такие, что для всех достаточно больших x*

$$a\frac{x}{\log x} < \pi(x) < A\frac{x}{\log x}.$$

Доказательство. Пусть

$$l = \varliminf_{x\to\infty} \frac{\pi(x)}{x/\log x}, \quad L = \varlimsup_{x\to\infty} \frac{\pi(x)}{x/\log x}.$$

Если мы покажем, что $L \leqslant 4\log 2$ и $l \geqslant \log 2$, то теорема будет доказана. По теореме 2 оба эти неравенства эквивалентны следующим неравенствам:

$$L = \varlimsup_{x\to\infty} \frac{\vartheta(x)}{x} \leqslant 4\log 2, \tag{7}$$

$$l = \varliminf_{x\to\infty} \frac{\psi(x)}{x} \geqslant \log 2. \tag{8}$$

Доказательство неравенства (7). Биномиальный коэффициент

$$N = \binom{2n}{n} = \frac{(n+1)(n+2)\ldots(2n)}{1\cdot 2\cdot 3\ldots n}$$

обладает следующими свойствами: (i) N есть целое число, которое является наибольшим членом в биномиальном разложении выражения $(1+1)^{2n}$, содержащем $(2n+1)$ членов, так что

$$N < 2^{2n}, \quad 2^{2n} < (2n+1)N; \tag{9}$$

(ii) N делится на произведение всех таких простых p, что $n < p \leqslant 2n$, так как эти простые входят в числитель N и не входят в знаменатель.

Поэтому, согласно свойству (ii), мы имеем $N \geqslant \prod\limits_{n<p\leqslant 2n} p$ и, следовательно,

$$\log N \geqslant \sum_{n<p\leqslant 2n} \log p = \vartheta(2n) - \vartheta(n).$$

Но из (9) мы получаем, что $\log N < 2n\log 2$. Значит,

$$\vartheta(2n) - \vartheta(n) < 2n\log 2. \tag{10}$$

Если мы положим в неравенстве (10) $n = 1, 2, 2^2, \ldots, 2^{m-1}$ и сложим полученные неравенства, то получим

$$\vartheta(2^m) - \vartheta(1) < \log 2 \sum_{r=1}^{m} 2^r < 2^{m+1} \log 2,$$

или, поскольку $\vartheta(1) = 0$,

$$\vartheta(2^m) < 2^{m+1} \log 2. \tag{11}$$

Пусть теперь $x > 1$ и m — положительное целое, такое, что $2^{m-1} \leqslant x < 2^m$. Так как функция $\vartheta(x)$ неубывающая, из (11) следует, что

$$\vartheta(x) \leqslant \vartheta(2^m) < 2^{m+1} \log 2 \leqslant 4x \log 2.$$

Следовательно, $\vartheta(x)/x < 4 \log 2$, откуда вытекает, что

$$L = \overline{\lim_{x \to \infty}} \frac{\vartheta(x)}{x} \leqslant 4 \log 2.$$

Тем самым неравенство (7) доказано.

Доказательство неравенства (8). Доказательство второй части теоремы Чебышева проводится другим способом. Оно основано на важной формуле для показателя, с которым простое число p входит в каноническое разложение m.

Мы говорим, что простое число p входит в каноническое разложение целого n с показателем k, если $p^k \mid n$ и $p^{k+1} \nmid n$[1]).

Лемма. *Показатель, с которым простое число p входит в $m!$, равен*

$$\left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \left[\frac{m}{p^3}\right] + \ldots,$$

причем последний ряд конечен, так как $[x] = 0$ для $0 < x < 1$.

Среди чисел 1, 2,..., m имеется точно $[m/p]$ кратных p, а именно

[1]) Мы будем говорить также, что простое p входит в n с показателем k. — *Прим. перев.*

$$p, 2p, \ldots, \left[\frac{m}{p}\right] p, \tag{12}$$

точно $[m/p^2]$ кратных p^2, а именно

$$p^2, 2p^2, \ldots, \left[\frac{m}{p^2}\right] p^2, \tag{13}$$

и т. д. Число целых чисел между 1 и m, которые делятся на p^r, но не делятся на p^{r+1}, в точности равно $[m/p^r] - [m/p^{r+1}]$. Следовательно, простое число p входит в $m!$ с показателем

$$\sum_{r\geqslant 1} r\left(\left[\frac{m}{p^r}\right] - \left[\frac{m}{p^{r+1}}\right]\right) = \sum_{r\geqslant 1}\left[\frac{m}{p^r}\right]; \tag{14}$$

лемма доказана.

Для того чтобы доказать неравенство (8), рассмотрим целое число

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

Пусть p — простое число, $p \leqslant 2n$. Тогда p входит в числитель N с показателем

$$\left[\frac{2n}{p}\right] + \left[\frac{2n}{p^2}\right] + \ldots,$$

а в знаменатель — с показателем

$$2\left(\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots\right).$$

Таким образом, p входит в N с показателем

$$\nu_p = \sum_{r\geqslant 1}\left(\left[\frac{2n}{p^r}\right] - 2\left[\frac{n}{p^r}\right]\right)$$

и, следовательно,

$$N = \prod_{p<2n} p^{\nu_p}.$$

Поскольку $\left[\frac{2n}{p^r}\right] = \left[\frac{n}{p^r}\right] = 0$ при $p^r > 2n$, или, что то же самое, при

$$r > \left[\frac{\log 2n}{\log p}\right],$$

мы имеем

$$\nu_p = \sum_{r=1}^{M_p}\left(\left[\frac{2n}{p^r}\right] - 2\left[\frac{n}{p^r}\right]\right), \quad M_p = \left[\frac{\log 2n}{\log p}\right]. \tag{15}$$

Кроме того, для любого действительного числа y

$$[y] \leqslant y < [y]+1, \quad \text{или} \quad 2[y] \leqslant 2y < 2[y]+2$$

и

$$[2y] \leqslant 2y < [2y]+1.$$

Отсюда следует, что $-1 < [2y] - 2[y] < 2$, откуда

$$[2y] - 2[y] = 0, \quad \text{или} \quad [2y] - 2[y] = 1. \tag{16}$$

Следовательно, используя соотношение (15), мы получаем, что $\nu_p \leqslant M_p$ и тогда

$$N = \prod_{p \leqslant 2n} p^{\nu_p} \leqslant \prod_{p \leqslant 2n} p^{M_p}. \tag{17}$$

С другой стороны, из (5) и (15) мы имеем

$$\psi(2n) = \sum_{p \leqslant 2n}\left[\frac{\log 2n}{\log p}\right]\log p = \sum_{p \leqslant 2n} M_p \log p,$$

так что

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

откуда в силу (17)

$$\log N \leqslant \psi(2n).$$

Далее, из (9) следует, что

$$\log N > 2n \log 2 - \log(2n+1).$$

Следовательно, для любого положительного целого числа n мы имеем

$$\psi(2n) > 2n \log 2 - \log(2n+1). \tag{18}$$

Пусть теперь $x > 2$ — действительное число, и пусть

$n=[x/2]\geqslant 1$. Тогда $n>(x/2)-1$, $2n\leqslant x$, и из (18) мы получаем

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

или

$$\frac{\psi(x)}{x}>\frac{x-2}{x}\log 2-\frac{\log(x+1)}{x}.$$

Следовательно,

$$l=\varliminf_{x\to\infty}\frac{\psi(x)}{x}\geqslant\log 2,$$

и теорема 3 доказана.

Из теоремы 3 сразу же следует, что простых чисел бесконечно много и что ряд $\sum 1/p$, распространенный на все простые числа, расходится.

Действительно, пусть p_n означает n-е простое число. Тогда $\pi(p_n)=n$, и так как

$$\pi(x)>a\cdot\frac{x}{\log x},\quad a>0,$$

для достаточно больших x, то

$$n=\pi(p_n)>a\cdot\frac{p_n}{\log p_n}>\sqrt{p_n}$$

для достаточно больших значений n. Следовательно, $\log p_n<2\log n$, так что

$$ap_n<n\log p_n<2n\log n$$

для достаточно больших n. Сравнивая ряд $\sum_{n=1}^{\infty}1/p_n$ с расходящимся рядом $\sum_{n=2}^{\infty}1/n\log n$, мы видим, что ряд $\sum_{n=1}^{\infty}1/p_n$ также расходится.

§ 3. Постулат Бертрана. Следующая теорема была сформулирована Бертраном и впервые доказана Чебышевым.

Теорема 4 (постулат Бертрана). *Если n — положительное целое, то существует простое число p, такое, что $n<p\leqslant 2n$.*

Доказательство Чебышева этой теоремы основано на соображениях, подобных тем, которые были использованы при доказательстве теоремы 3. Этот результат сначала был доказан для больших значений n, а для малых значений n проверялся с помощью таблицы простых чисел.

Мы приводим здесь доказательство, предложенное С. С. Пиллаи, которое довольно просто, поскольку не использует формулу Стирлинга для $\Gamma(n)$ и сводит число проверок к минимуму.

При доказательстве теоремы Чебышева мы использовали для биномиального коэффициента $N=\binom{2n}{n}$ неравенство (9), а именно

$$\frac{2^{2n}}{2n+1}<N<2^{2n},$$

и вывели из него неравенство (11), а именно

$$\vartheta(2^m)<2^{m+1}\log 2. \tag{11}$$

Для доказательства того, что неравенство (11) выполняется не только для степеней числа 2, но также для всех положительных целых чисел n, т. е.

$$\vartheta(n)<2n\log 2, \quad n\geqslant 1, \tag{19}$$

нам потребуется более точная оценка

$$\frac{2^{2n}}{2\sqrt{n}}<N<\frac{2^{2n}}{\sqrt{2n}}, \quad n\geqslant 2. \tag{20}$$

Доказательство оценки (20). Положим

$$P=\frac{1\cdot 3\cdot 5\ldots(2n-1)}{2\cdot 4\cdot 6\ldots(2n)}.$$

Поскольку

$$P=\frac{1\cdot 3\cdot 5\ldots(2n-1)}{2\cdot 4\cdot 6\ldots(2n)}\cdot\frac{2\cdot 4\cdot 6\ldots(2n)}{2\cdot 4\cdot 6\ldots(2n)}=\frac{(2n)!}{2^{2n}(n!)^2},$$

мы имеем $2^{2n}P=N$. Очевидно, что справедливо неравенство

$$1>\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{4^2}\right)\left(1-\frac{1}{6^2}\right)\dots\left(1-\frac{1}{(2n)^2}\right),$$

которое может быть переписано в виде

$$1>\left(\frac{1\cdot3}{2^2}\right)\left(\frac{3\cdot5}{4^2}\right)\left(\frac{5\cdot7}{6^2}\right)\dots\left(\frac{(2n-1)(2n+1)}{(2n)^2}\right)$$

или в виде

$$1>(2n+1)P^2>2nP^2=\frac{2n}{2^{4n}}N^2.$$

Отсюда следует второе неравенство в оценке (20).

Подобным же образом мы имеем неравенство

$$1>\left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{5^2}\right)\left(1-\frac{1}{7^2}\right)\dots\left(1-\frac{1}{(2n-1)^2}\right),$$

которое может быть записано в виде

$$1>\left(\frac{2\cdot4}{3^2}\right)\left(\frac{4\cdot6}{5^2}\right)\left(\frac{6\cdot8}{7^2}\right)\dots\left(\frac{(2n-2)\,2n}{(2n-1)^2}\right)$$

или в виде

$$1>\frac{1}{4nP^2}=\frac{2^{4n}}{4nN^2}.$$

Отсюда следует первое неравенство в оценке (20). Таким образом, оценка (20) доказана.

Доказательство неравенства (19). Неравенство очевидно для $n=1$ и $n=2$. Предполагая неравенство справедливым для некоторого $n\geqslant2$, мы выведем отсюда, что $\vartheta(2n-1)<2(2n-1)\log 2$, откуда будет следовать соотношение

$$\vartheta(2n)=\vartheta(2n-1)<4n\log 2.$$

Рассмотрим целое число

$$\frac{N}{2}=\frac{1}{2}\binom{2n}{n}=\frac{(2n)!}{(n!)^2}\cdot\frac{n}{2n}=\frac{(2n-1)!}{n!(n-1)!}=\binom{2n-1}{n-1}.$$

Оно делится на все простые p, такие, что $n<p\leqslant2n-1$, а следовательно, и на их произведение. Значит,

$$\frac{N}{2}\geqslant\prod_{n<p\leqslant2n-1}p$$

или, после логарифмирования,

$$\log \frac{N}{2} \geqslant \vartheta(2n-1) - \vartheta(n).$$

Но из (20) мы имеем

$$\log N < 2n \log 2 - \frac{1}{2} \log 2n.$$

Объединяя оба эти неравенства, получаем

$$\vartheta(2n-1) - \vartheta(n) < (2n-1) \log 2 - \frac{1}{2} \log 2n.$$

Но по предположению $\vartheta(n) < 2n \log 2$. Следовательно,

$$\vartheta(2n-1) < 2n \log 2 + (2n-1) \log 2 - \frac{1}{2} \log 2n,$$

откуда следует, поскольку $n \geqslant 2$, что

$$\vartheta(2n-1) < 2(2n-1) \log 2,$$

т. е. мы пришли к искомому неравенству. Таким образом, если (19) доказано для некоторого положительного целого числа $n \geqslant 2$, то оно будет выполняться также и для $2n-1$, а следовательно, и для $2n$. Другими словами, если $\vartheta(n) < 2n \log 2$ для *каждого* целого числа из интервала вида

$$2^{r-1} < n \leqslant 2^r, \quad r \geqslant 1,$$

то это неравенство справедливо также для всех целых n из интервала

$$2^r < n \leqslant 2^{r+1}.$$

Отсюда по индукции следует, что неравенство (19) справедливо для всех $n \geqslant 1$.

Неравенства (19) и (20) потребуются нам при доказательстве теоремы 4.

Доказательство теоремы 4 (С. С. Пиллаи). Для того чтобы доказать теорему 4, мы докажем неравенство $\vartheta(2n) - \vartheta(n) > 0$ для всех $n \geqslant 2^6$ и проверим это неравенство для $1 \leqslant n < 2^6$.

Рассмотрим снова биномиальный коэффициент (см. (17))

$$N = \binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \prod_{p \leqslant 2n} p^{\nu_p},$$

где

$$\nu_p = \sum_{r \geqslant 1} \left(\left[\frac{2n}{p^r} \right] - 2 \left[\frac{n}{p^r} \right] \right).$$

Тогда

$$\log N = \sum_{p \leqslant 2n} \nu_p \log p. \tag{21}$$

В последней сумме интервал суммирования по p мы разобьем на четыре интервала:

(i) $n < p \leqslant 2n$; (ii) $\sqrt{2n} < p \leqslant \frac{2n}{3}$, $n \geqslant 5$;

(ii) $\frac{2n}{3} < p \leqslant n$; (iv) $p \leqslant \sqrt{2n}$.

В соответствии с этим указанная сумма разобьется на четыре суммы $\sum_1$, $\sum_2$, $\sum_3$, $\sum_4$.

В $\sum_1$ мы имеем $n/p < 1$ и $1 \leqslant 2n/p < 2$, так что $[n/p] = 0$, $[2n/p] = 1$ и $[2n/p^2] = 0$. Следовательно, $\nu_p = 1$, и мы получаем

$$\sum_1 = \sum_{n < p \leqslant 2n} \nu_p \log p = \sum_{n < p \leqslant 2n} \log p = \vartheta(2n) - \vartheta(n). \tag{22}$$

В $\sum_2$ мы имеем $1 \leqslant n/p < 3/2$, так что $[n/p] = 1$ и $[2n/p] = 2$. Кроме того, $[2n/p^2] = 0$ при $n \geqslant 3$ и, следовательно,

$$\sum_2 = 0, \quad n \geqslant 3. \tag{23}$$

В $\sum_3$ мы имеем $n \geqslant 5$ и $n/p^2 < 2n/p^2 < 1$, так что $\nu_p = [2n/p] - 2[n/p] = 0$ или 1 (см. (16)). Следовательно,

$$\sum_3 \leqslant \sum_{\sqrt{2n} < p \leqslant 2n/3} \log p = \vartheta\left(\frac{2n}{3}\right) - \vartheta\left(\sqrt{2n}\right).$$

Но

$$\vartheta\left(\sqrt{2n}\right) \equiv \sum_{p \leqslant \sqrt{2n}} \log p \geqslant \log 2 \sum_{p \leqslant \sqrt{2n}} 1 = \pi\left(\sqrt{2n}\right) \log 2,$$

и поэтому

$$\sum\nolimits_3 \leqslant \vartheta\left(\frac{2n}{3}\right) - \pi\left(\sqrt{2n}\right)\log 2. \tag{24}$$

В $\sum_4$ мы используем неравенство Чебышева (см. (17))

$$\nu_p \leqslant M_p = \left[\frac{\log 2n}{\log p}\right]$$

и получаем

$$\sum\nolimits_4 \leqslant \sum_{p \leqslant \sqrt{2n}} M_p \log p \leqslant \sum_{p \leqslant \sqrt{2n}} \frac{\log 2n}{\log p}\log p = \log 2n \sum_{p \leqslant \sqrt{2n}} 1.$$

Таким образом,

$$\sum\nolimits_4 \leqslant \pi\left(\sqrt{2n}\right)\log 2n. \tag{25}$$

Объединяя соотношения (21)—(25), мы приходим при $n \geqslant 5$ к неравенству

$$\log N \leqslant \vartheta(2n) - \vartheta(n) + \vartheta\left(\frac{2n}{3}\right) - \pi\left(\sqrt{2n}\right)(\log 2 - \log 2n),$$

которое можно переписать в виде

$$\vartheta(2n) - \vartheta(n) \geqslant \log N - \vartheta\left(\frac{2n}{3}\right) - \pi\left(\sqrt{2n}\right)\log n. \tag{26}$$

Покажем теперь, что $\vartheta(2n) - \vartheta(n) > 0$ для всех достаточно больших n. Для этого нам потребуются три неравенства:

(a) $\vartheta\left(\frac{2n}{3}\right) = \vartheta\left(\left[\frac{2n}{3}\right]\right) < 2\left[\frac{2n}{3}\right]\log 2,\ n \geqslant 2;$

(b) $\log N > 2n\log 2 - \log\left(2\sqrt{n}\right);$

(c) $\pi(n) \leqslant \frac{n}{2}$, если $n \geqslant 8.$

Неравенства (a) и (b) являются следствиями неравенств (19) и (20) соответственно, а неравенство (c) следует из того, что каждое четное число, большее 2, является составным.

Из (a), (b), (c) и (26) мы получаем при $n \geqslant 32$

$$\vartheta(2n) - \vartheta(n) > 2n \log 2 - \log(2\sqrt{n}) - \\ - \frac{4n}{3} \log 2 - \frac{\sqrt{2n}}{2} \log n,$$

или, что то же самое,

$$\vartheta(2n) - \vartheta(n) > \left(\frac{2n}{3} - 1\right) \log 2 - \frac{\sqrt{2n}+1}{2} \log n. \qquad (27)$$

Остается показать, что

$$\left(\frac{2n}{3} - 1\right) \log 2 - \frac{\sqrt{2n}+1}{2} \log n > 0 \qquad (28)$$

для всех достаточно больших n. Легко видеть, что неравенство (28) выполняется при $n=2^6$. Докажем справедливость этого неравенства для $n>2^6$. Для этого перепишем (28) в виде

$$\sqrt{2n} - \frac{3}{2} \cdot \frac{\log n}{\log 2} - \frac{3\sqrt{2}}{\log 2} \cdot \frac{\log \sqrt{4n}}{\sqrt{4n}} > 0 \qquad (29)$$

и заметим, что при $x \geqslant 2^6$ (мы заменили n действительным переменным x) функции

$$\sqrt{2x} - \frac{3}{2} \cdot \frac{\log x}{\log 2} \quad \text{и} \quad - \frac{3\sqrt{2}}{\log 2} \cdot \frac{\log \sqrt{4x}}{\sqrt{4x}}$$

имеют положительные производные. Значит, в указанной области эти функции возрастают, и так как их сумма положительна при $x=2^6$, то она будет оставаться положительной и при $x>2^6$. Следовательно,

$$\vartheta(2n) - \vartheta(n) > 0, \quad n \geqslant 2^6, \qquad (30)$$

т. е. постулат Бертрана справедлив при $n \geqslant 2^6 = 64$. Далее, в последовательности

$$2, 3, 5, 7, 13, 23, 43, 67 \qquad (31)$$

каждое простое число, за исключением первого, будет меньше удвоенного предыдущего. Следовательно, каждому положительному целому числу $n \leqslant 66$ соответствует по меньшей мере одно простое число p, такое, что

$n<p\leqslant 2n$. Таким образом, теорема 4 полностью доказана.

§ 4. Тождество Эйлера. Тождество

$$\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_p(1-p^{-s})^{-1}, \tag{32}$$

где $s>1$ — *действительное* число и p пробегает все простые числа, является частным случаем следующего результата:

Теорема 5. *Пусть f — мультипликативная арифметическая функция и ряд $\sum\limits_{n=1}^{\infty}f(n)$ абсолютно сходится. Тогда имеет место тождество*

$$\sum_{n=1}^{\infty}f(n)=\prod_p(1+f(p)+f(p^2)+\ldots), \tag{33}$$

причем произведение в правой части также сходится абсолютно.

Далее, если f вполне мультипликативна, т. е. $f(mn)=f(m)f(n)$ для всех положительных целых чисел m, n, то

$$\sum_{n=1}^{\infty}f(n)=\prod_p(1-f(p))^{-1}. \tag{34}$$

Доказательство. Из мультипликативности функции f мы имеем $f(1)=1$. Положим

$$P(x)=\prod_{p\leqslant x}(1+f(p)+f(p^2)+\ldots).$$

Так как $P(x)$ является произведением конечного числа абсолютно сходящихся рядов, то, перемножив эти ряды, мы получим

$$P(x)=\sum f(n'),$$

где n' пробегает все положительные целые числа, которые не имеют простых делителей, больших x. Положим

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

Тогда

$$P(x) - S = -\sum f(n''),$$

где n'' пробегает все положительные целые числа, имеющие по меньшей мере один простой делитель, больший x. Очевидно, $n'' > x$, так что

$$|P(x) - S| \leqslant \sum |f(n'')| \leqslant \sum_{n>x} |f(n)|.$$

Далее, $\sum\limits_{n>x} |f(n)| \to 0$ при $x \to \infty$, так как по предположению ряд $\sum\limits_{n=1}^{\infty} |f(n)|$ сходится. Следовательно, $\lim\limits_{x\to\infty} P(x) = S$ и тем самым тождество (33) доказано.

Произведение в правой части равенства (33) сходится абсолютно, поскольку

$$\sum_{p\leqslant x} |f(p) + f(p^2) + \ldots| \leqslant \sum_{p\leqslant x} (|f(p)| + |f(p^2)| + \ldots) \leqslant$$

$$\leqslant \sum_{n=2}^{\infty} |f(n)| < \infty. \qquad (35)$$

Рассмотрим теперь случай, когда f *вполне* мультипликативна. Из (35) мы видим, что ряд

$$\sum_{p} (|f(p)| + |f(p^2)| + \ldots),$$

где суммирование ведется по всем простым p, сходится. Но тогда $f(p^n) = (f(p))^n$ и, следовательно, ряд

$$\sum_{p} (|f(p)| + |f(p)|^2 + \ldots)$$

тоже сходится. Члены последнего ряда образуют геометрическую прогрессию, откуда $|f(p)| < 1$. Значит,

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} (1 + f(p) + f(p^2) + \ldots) =$$

$$= \prod_{p} (1 + f(p) + (f(p))^2 + \ldots) = \prod_{p} (1 - f(p))^{-1},$$

и теорема 5 доказана.

Тождество Эйлера следует теперь из (34), если мы положим $f(n)=n^{-s}$, $s>1$. Пусть

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

где $s>1$ действительное. Тогда

$$\log\zeta(s)=-\sum_p\log(1-p^{-s})=\sum_{m,p}\frac{1}{mp^{ms}},$$

где p пробегает все простые числа, а m пробегает все положительные целые числа. Почленное дифференцирование даст нам

$$-\frac{\zeta'(s)}{\zeta(s)}=\sum_p\frac{p^{-s}\log p}{1-p^{-s}}=\sum_{m,p}\frac{\log p}{mp^{ms}}.$$

Следовательно, при действительном $s>1$

$$-\frac{\zeta'(s)}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s},\tag{36}$$

где $\Lambda(n)$ — функция Мангольдта, определенная в § 5 гл. VI. Заметим, что почленное дифференцирование допустимо, поскольку оба ряда $\sum_p\log(1-p^{-s})$ и $\sum_p\frac{p^{-s}\log p}{1-p^{-s}}$ равномерно сходятся при $s\geqslant 1+\delta>1$.

Правая часть равенства (36) представляет собой *ряд Дирихле* вида $\sum_{n=1}^{\infty}a_nn^{-s}$, *коэффициенты* a_n которого являются значениями функции Мангольдта $\Lambda(n)$. Используя равенство (36), мы покажем, что если какая-либо из функций

$$\frac{\pi(x)}{x/\log x},\quad\frac{\vartheta(x)}{x},\quad\frac{\psi(x)}{x}$$

имеет предел при $x\to\infty$, то этот предел должен быть равен 1. Из теоремы 2 мы уже знаем, что если какая-либо

из этих трех функций имеет предел при $x\to\infty$, то две другие функции также будут иметь пределы и все эти три предела равны между собой.

Рассмотрим функцию $\psi(x)/x$ и воспользуемся соотношением

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

В дальнейшем нам потребуется тождество

$$-\frac{\zeta'(s)}{\zeta(s)}=s\int_1^\infty\frac{\psi(x)}{x^{s+1}}\,dx \quad (s \text{ действительное}, s>1),$$

которое можно получить из формулы суммирования Абеля.

Теорема 6 (Абель). *Пусть* $0\leqslant\lambda_1\leqslant\lambda_2\leqslant\ldots$ — *последовательность действительных чисел, такая, что* $\lambda_n\to\infty$ *при* $n\to\infty$, *и пусть* (a_n), $n=1, 2, \ldots$, — *последовательность комплексных чисел. Пусть, далее,* $A(x)=\sum\limits_{\lambda_n\leqslant x}a_n$ *и* $\varphi(x)$ — *комплекснозначная функция, определенная при* $x\geqslant 0$. *Тогда*

$$\sum_{n=1}^{k}a_n\varphi(\lambda_n)=A(\lambda_k)\varphi(\lambda_k)-\sum_{n=1}^{k}A(\lambda_n)\bigl(\varphi(\lambda_{n+1})-\varphi(\lambda_n)\bigr). \quad (37)$$

Если φ *имеет непрерывную производную на интервале* $(0, \infty)$ *и* $x\geqslant\lambda_1$, *то* (37) *может быть записано в виде*

$$\sum_{\lambda_n\leqslant x}a_n\varphi(\lambda_n)=A(x)\varphi(x)-\int_{\lambda_1}^{x}A(t)\varphi'(t)\,dt. \quad (38)$$

Если, кроме того, $A(x)\varphi(x)\to 0$ *при* $x\to\infty$, *то*

$$\sum_{n=1}^{\infty}a_n\varphi(\lambda_n)=-\int_{\lambda_1}^{\infty}A(t)\varphi'(t)\,dt \quad (39)$$

при условии, что ряд в левой части и интеграл в правой части сходятся.

Доказательство. Положим $A(\lambda_0)=0$. Тогда мы имеем

$$\sum_{n=1}^{k} a_n \varphi(\lambda_n) = \sum_{n=1}^{k} \big(A(\lambda_n) - A(\lambda_{n-1})\big)\varphi(\lambda_n) =$$

$$= A(\lambda_k)\varphi(\lambda_k) - \sum_{n=1}^{k-1} A(\lambda_n)\big(\varphi(\lambda_{n+1}) - \varphi(\lambda_n)\big);$$

тем самым равенство (37) доказано. Пусть k — наибольшее целое число, такое, что $\lambda_k \leqslant x$. Так как φ имеет непрерывную производную φ', то сумма в правой части (37) равна

$$\sum_{n=1}^{k-1} A(\lambda_n) \int_{\lambda_n}^{\lambda_{n+1}} \varphi'(t)\,dt,$$

а так как $A(t)$ — ступенчатая функция, постоянная в интервале $\lambda_k \leqslant t < \lambda_{k+1}$, то первый член в правой части (37) равен

$$A(\lambda_k)\varphi(\lambda_k) = A(x)\varphi(x) - \int_{\lambda_k}^{x} A(t)\varphi'(t)\,dt.$$

Таким образом,

$$\sum_{\lambda_n \leqslant x} a_n \varphi(\lambda_n) = A(x)\varphi(x) - \int_{\lambda_1}^{x} A(t)\varphi'(t)\,dt$$

и равенство (38) также доказано. Наконец, мы получим равенство (39), если в (38) устремим x к бесконечности. Теорема 6 тем самым доказана.

Положим $\lambda_n = n$, $a_n = \Lambda(n)$ и $\varphi(x) = x^{-s}$ (s действительное, $s>1$). Тогда $A(x)=\psi(x)$ и $A(x)\varphi(x) \to 0$ при $x \to \infty$, поскольку $\psi(x) \leqslant \pi(x)\log x < x\log x$ (см. доказательство теоремы 2), так что $A(x)\varphi(x) = O(x^{1-s}\log x) = o(1)$. Следовательно, мы получаем из (36) и (39) при действительном $s>1$

$$-\frac{\zeta'(s)}{\zeta(s)} = s\int_1^{\infty} \frac{\psi(x)}{x^{s+1}}\,dx. \tag{40}$$

Теперь мы можем доказать следующую теорему:

Теорема 7.

$$\underline{\lim_{x\to\infty}}\,\frac{\pi(x)}{x/\log x}\leqslant 1\leqslant \overline{\lim_{x\to\infty}}\,\frac{\pi(x)}{x/\log x}.$$

Доказательство. Покажем, что

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

и затем воспользуемся теоремой 2.

Пусть $f(s)=-\dfrac{\zeta'(s)}{\zeta(s)}$ для действительного $s>1$, и пусть

$$l=\underline{\lim_{x\to\infty}}\frac{\psi(x)}{x},\qquad L=\overline{\lim_{x\to\infty}}\,\frac{\psi(x)}{x},$$

$$l'=\underline{\lim_{s\to 1+0}}\,(s-1)f(s),\qquad L'=\overline{\lim_{s\to 1+0}}\,(s-1)f(s).$$

Очевидно, $l\leqslant L$ и $l'\leqslant L'$. Докажем сначала, что $l\leqslant l'\leqslant L'\leqslant L$, а затем, что $l'=L'=1$. Вместе эти неравенства дадут утверждение теоремы 7.

Пусть $B>L$. Тогда $\psi(x)/x<B$ для всех $x\geqslant x_0=x_0(B)$, и мы можем предположить, что $x_0>1$. Из формулы (40) мы имеем при $s>1$

$$f(s)=s\int_1^\infty\frac{\psi(x)}{x^{s+1}}\,dx<s\int_1^{x_0}\frac{\psi(x)}{x^{s+1}}\,dx+s\int_{x_0}^\infty\frac{B}{x^s}\,dx,$$

так что

$$f(s)<s\int_1^{x_0}\frac{\psi(x)}{x^{s+1}}\,dx+s\int_{x_0}^\infty\frac{B}{x^s}\,dx<s\int_1^{x_0}\frac{\psi(x)}{x^2}\,dx+\frac{sB}{s-1}.$$

Последнее неравенство можно переписать в виде

$$(s-1)f(s)<s(s-1)K+sB,$$

где

$$\int_1^{x_0}\frac{\psi(x)}{x^2}\,dx=K=K(x_0)=K(x_0,B).$$

Пусть $s \to 1+0$. Тогда мы получаем, что $L' \leqslant B$, и так как это неравенство выполняется для любого $B > L$, то $L' \leqslant L$. Аналогично можно доказать, что $l \leqslant l'$ и потому $l \leqslant l' \leqslant L' \leqslant L$.

Покажем теперь, что

$$\lim_{s \to 1+0} (-(s-1)^2 \zeta'(s)) = 1$$

и

$$\lim_{s \to 1+0} (s-1)\zeta(s) = 1.$$

Отсюда будет следовать, что $(s-1)f(s) \to 1$ при $s \to 1+0$, а значит, и равенство $l' = L' = 1$.

Функция x^{-s} при $s > 1$ является убывающей функцией переменного x, так что

$$\int_1^\infty \frac{dx}{x^s} < \sum_{n=1}^\infty \frac{1}{n^s} < 1 + \int_1^\infty \frac{dx}{x^s}.$$

Таким образом,

$$\frac{1}{s-1} < \zeta(s) < \frac{s}{s-1},$$

откуда следует, что $(s-1)\zeta(s) \to 1$ при $s \to 1+0$.

С другой стороны, при $s > 1$ и $x \geqslant e$ функция $x^{-s}\log x$ также является убывающей по x, так что

$$-\zeta'(s) = \sum_{n=1}^\infty \frac{\log n}{n^s} = \int_1^\infty \frac{\log x}{x^s}\,dx + O(1),$$

откуда после подстановки $x^{s-1} = e^y$ мы получаем

$$-\zeta'(s) = \frac{1}{(s-1)^2} \int_0^\infty y e^{-y}\,dy + O(1) = \frac{1}{(s-1)^2} + O(1).$$

Таким образом,

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

при $s \to 1+0$. Следовательно, $l' = L' = 1$, откуда $l \leqslant 1 \leqslant L$.

Объединив этот результат с теоремой 2, мы получаем утверждение теоремы 7.

Из теоремы 7 вытекает, что если предел функции $\frac{\pi(x)}{x/\log x}$ при $x\to\infty$ существует, то этот предел должен быть равен 1.

§ 5. Некоторые формулы Мертенса.

Теорема 8. *При $x\to\infty$ мы имеем*

$$\sum_{n\leqslant x}\frac{\Lambda(n)}{n}=\log x+O(1),\quad \sum_{p\leqslant x}\frac{\log p}{p}=\log x+O(1), \tag{41}$$

$$\int_1^x\frac{\psi(t)}{t^2}\,dt=\log x+O(1), \tag{42}$$

$$\sum_{p\leqslant x}\frac{1}{p}=\log\log x+C+O\left(\frac{1}{\log x}\right), \tag{43}$$

где C — некоторая константа.

Доказательство. Мы используем слабую форму формулы Стирлинга, а именно

$$\log(m!)=m\log m+O(m) \tag{44}$$

при $m\to\infty$. Из теорем 2 и 3 мы знаем, что при $m\to\infty$

$$\psi(m)=O(m). \tag{45}$$

Далее, по лемме, полученной в ходе доказательства теоремы 3, мы имеем

$$m!=\prod_{p\leqslant m}p^{\left[\frac{m}{p}\right]+\left[\frac{m}{p^2}\right]+\cdots}.$$

или

$$\log(m!)=\sum_{p^r\leqslant m}\left[\frac{m}{p^r}\right]\log p=\sum_{n\leqslant m}\left[\frac{m}{n}\right]\Lambda(n), \tag{46}$$

где $\Lambda(n)$ — функция Мангольдта [см. (3)],

Чтобы доказать (41), положим в формуле (46)

$$\frac{m}{n} = \left[\frac{m}{n}\right] + \varepsilon_n,$$

где $0 \leqslant \varepsilon_n < 1$. Тогда, используя (45), мы имеем

$$\log(m!) = \sum_{n \leqslant m} \frac{m}{n} \Lambda(n) + O(m)$$

и, применяя (44),

$$\sum_{n \leqslant m} \frac{\Lambda(n)}{n} = \log m + O(1).$$

Заменяя теперь целое число m действительным переменным x, мы получаем первую из формул (41). Вторая формула следует из неравенства

$$\left| \sum_{n \leqslant x} \frac{\Lambda(n)}{n} - \sum_{p \leqslant x} \frac{\log p}{p} \right| \leqslant \sum_{p \leqslant x} \left(\frac{1}{p^2} + \frac{1}{p^3} + \cdots \right) \log p <$$

$$< \sum_{p} \frac{\log p}{p(p-1)} < \infty.$$

Используя (45), мы можем вывести из (41) формулу (42). Действительно, $\psi(t) = \sum_{n < t} \Lambda(n)$, и тогда при $x \geqslant 1$

$$\int_1^x \frac{\psi(t)}{t^2}\, dt = \int_1^x \sum_{n \leqslant t} \Lambda(n) \frac{dt}{t^2} = \sum_{n \leqslant x} \Lambda(n) \int_n^x \frac{dt}{t^2} =$$

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

Наконец, формула (43) может быть выведена из (41), если использовать формулу суммирования Абеля. Пусть (p_n) — последовательность простых чисел, занумерованных в порядке их возрастания, и пусть

$$A(x) = \sum_{p_n \leqslant x} a_n, \quad \text{где} \quad a_n = \frac{\log p_n}{p_n},$$

и

$$B(x)=\sum_{p_n\leqslant x} b_n, \quad \text{где} \quad b_n=\frac{1}{p_n}.$$

Тогда по теореме 6 мы имеем при $x\geqslant 2$

$$B(x)=\sum_{p_n\leqslant x}\frac{a_n}{\log p_n}=\frac{A(x)}{\log x}+\int_2^x\frac{A(u)\,du}{u(\log u)^2}.$$

Далее, в силу второй из формул (41) мы имеем $A(x)=\log x+E(x)$, где $|E(x)|<K$ для всех $x\geqslant 2$ при некоторой постоянной K. Следовательно,

$$(x)=1+\frac{E(x)}{\log x}+\int_2^x\frac{du}{u\log u}+\int_2^x\frac{E(u)}{u(\log u)^2}\,du=$$

$$=1+\frac{E(x)}{\log x}+(\log\log x-\log\log 2)+\int_2^x\frac{E(u)}{u(\log u)^2}\,du.$$

Так как $|E(x)|<K$, то интеграл $\int_2^\infty\frac{E(u)}{u(\log u)^2}\,du$ сходится, и тогда

$$B(x)=\log\log x+\left(1-\log\log 2+\int_2^\infty\frac{E(u)}{u(\log u)^2}\,du\right)+E^*(x),$$

где

$$E^*(x)=\frac{E(x)}{\log x}-\int_x^\infty\frac{E(u)}{u(\log u)^2}\,du,$$

так что при $x\geqslant 2$

$$|E^*(x)|<\frac{2K}{\log x}.$$

Таким образом, формула (43) доказана.

ТЕОРЕМЫ ВЕЙЛЯ О РАВНОМЕРНОМ РАСПРЕДЕЛЕНИИ И ТЕОРЕМА КРОНЕКЕРА

§ 1. Введение. Мы видели в гл. III, что для любого заданного иррационального числа ξ найдется бесконечно много рациональных чисел p/q, таких, что $|\xi - p/q| < 1/q^2$. Из этого результата следует теорема Дирихле о том, что каждому иррациональному числу ξ отвечает бесконечно много пар целых чисел p и q, таких, что $q\xi$ отличается от p на сколь угодно малую величину. Действительно, для данного ε, $0<\varepsilon<1$, рассмотрим целое число $1+[1/\varepsilon]$. Поскольку существует бесконечно много рациональных чисел p/q, таких, что $|q\xi - p| < 1/q$, то существует бесконечно много дробей p/q со знаменателями $q \geqslant 1+[1/\varepsilon]$, для которых $|q\xi - p| < 1/q < \varepsilon$.

Теорему Дирихле можно обобщить следующим образом. Если заданы иррациональное число θ, произвольное действительное число α и положительные действительные числа N и ε, то существуют *целые числа* n и p, такие, что

$$n > N \quad \text{и} \quad |n\theta - p - \alpha| < \varepsilon.$$

Если $\alpha=0$, то этот результат сводится к упомянутой выше теореме Дирихле. Если $0<\alpha<1$ и ε — сколь угодно малое положительное число, то последнее неравенство означает, что *дробная часть* $n\theta$, а именно $\{n\theta\} = n\theta - [n\theta]$, сколь угодно близка к α. Другими словами, числа $(\{n\theta\})$, $n=1, 2, 3, \ldots$, всюду плотны в интервале $[0, 1]$.

Это обобщение теоремы Дирихле является частным случаем глубокого результата Г. Вейля *о равномерном распределении*, который будет доказан в этой главе.

Для рассмотрения вопросов, связанных с дробными частями действительных чисел, введем новые понятия. Два действительных числа x_1 и x_2 называются *сравнимыми по модулю* 1, если их разность является целым числом. Отношение сравнимости по модулю 1 будет, очевидно, отношением эквивалентности, которое разбивает все действительные числа на классы эквивалентности,

состоящие из действительных чисел с одной и той же дробной частью. Отображение $x \to e^{2\pi i x}$ индуцирует взаимно однозначное соответствие между этими классами эквивалентности и точками единичной окружности.

§ 2. Равномерное распределение в единичном интервале. Пусть S — *конечное* множество действительных чисел $\alpha_1, \alpha_2, \ldots, \alpha_Q$, содержащихся в интервале $[0, 1)$, т. е.

$$0 \leqslant \alpha_j < 1, \quad 1 \leqslant j \leqslant Q.$$

Для любых действительных чисел a и b, таких, что $0 \leqslant a < b \leqslant 1$, через $\varphi(a, b)$ обозначим количество чисел α, содержащихся в интервале $[a, b)$, т. е. количество чисел α_j, для которых

$$a \leqslant \alpha_j < b, \quad 1 \leqslant j \leqslant Q.$$

Величина

$$D = \sup_{[a,b)} \left| \frac{\varphi(a, b)}{Q} - (b - a) \right| \tag{1}$$

называется *отклонением* множества S. Ясно, что $0 < D \leqslant 1$. Если мы обозначим интервал $[a, b)$ через I, его длину через $|I|$ и $\varphi(a, b)$ обозначим через $\varphi(I)$, то (1) запишется в виде

$$D = \sup_{I \subset [0,1)} \left| \frac{\varphi(I)}{Q} - |I| \right|. \tag{1'}$$

Для *бесконечной последовательности* действительных чисел $\alpha_1, \alpha_2, \ldots$ из интервала $[0, 1)$ через D_n обозначим отклонение первых n членов этой последовательности. Мы назовем последовательность (α_j) *равномерно распределенной*, если $D_n \to 0$ при $n \to \infty$.

Пусть $\varphi_n(a, b) = \varphi_n(I)$ — число тех α_j, для которых $a \leqslant \alpha_j < b$ при $1 \leqslant j \leqslant n$. Из определения следует, что если последовательность (α_j) равномерно распределена в интервале $[0, 1)$, то

$$\frac{\varphi_n(a, b)}{n} \to (b - a) \tag{2}$$

при $n \to \infty$ для *каждой* пары действительных чисел a и b, таких, что $0 \leqslant a < b \leqslant 1$. Справедливо и обратное утверж-

дение: если (2) выполняется для каждого такого интервала $[a, b)$, то последовательность (α_j) равномерно распределена.

Действительно, разобьем интервал $[0, 1)$ на конечное число подинтервалов (I_k), каждый из которых имеет длину δ, $0<\delta<1$. Для любого данного интервала $[c, d)$, где $0\leqslant c<d\leqslant 1$, обозначим через r число интервалов I_k длины δ, лежащих внутри $[c, d)$. Их общая длина равна $r\delta$, и мы имеем $r\delta>(d-c)-2\delta$. Далее, если через r' мы обозначим число интервалов I_k, пересекающихся с $[c, d)$, то $r'\delta<(d-c)+2\delta$.

Поскольку (2) выполняется для каждого интервала $[a, b)$, то оно должно выполняться, в частности, для интервала I_k длины δ. Таким образом, для заданного $\varepsilon>0$ существует число $N(\varepsilon)$, такое, что

$$\delta-\varepsilon\leqslant\frac{\varphi_n(I_k)}{n}\leqslant\delta+\varepsilon$$

для всех $n>N(\varepsilon)$ и всех k. Выберем $\varepsilon=\delta^2$. Тогда мы получим

$$(1-\delta)\,\delta\leqslant\frac{\varphi_n(I_k)}{n}\leqslant(1+\delta)\,\delta$$

для всех $n>N'(\delta)$. Следовательно,

$$r\delta(1-\delta)\leqslant\frac{1}{n}\sum_{I_k\subset[c,d)}\varphi_n(I_k)\leqslant\frac{\varphi_n(c,d)}{n}\leqslant$$

$$\leqslant\frac{1}{n}\sum_{I_k\subset[c,d)\neq\varnothing}\varphi_n(I_k)\leqslant r'\,\delta(1+\delta)$$

для всех $n>N'(\delta)$, **откуда**

$$((d-c)-2\delta)(1-\delta)\leqslant\frac{\varphi_n(c,d)}{n}\leqslant((d-c)+2\delta)(1+\delta).$$

Так как $d-c\leqslant 1$, то для *любого* интервала $[c, d)\subset[0,1)$

$$\left|\frac{\varphi_n(c,d)}{n}-(d-c)\right|\leqslant 3\delta+2\delta^2,$$

при $n>N'(\delta)$ и при δ, не зависящем от этого интервала. Таким образом, $D_n\to 0$ при $n\to\infty$. Итак, доказана

Теорема 1. *Бесконечная последовательность действительных чисел* (α_i), $i=1, 2, \ldots$, *таких, что* $0\leqslant\alpha_i<1$, *равномерно распределена тогда и только тогда, когда*

$$\frac{\varphi_n(a, b)}{n}\to(b-a)$$

при $n\to\infty$ *для каждой пары действительных чисел* a *и* b, *где* $0\leqslant a<b\leqslant 1$. *Здесь* $\varphi_n(a, b)$ *есть число тех* α_j, *которые удовлетворяют неравенству* $a\leqslant\alpha_j<b$ *при* $1\leqslant j\leqslant n$.

Заметим, что равномерно распределенная последовательность (α_i) всюду плотна в единичном интервале $[0, 1)$.

§ 3. Равномерное распределение по модулю 1. Бесконечная последовательность действительных чисел (α_i), не обязательно содержащаяся в единичном интервале, называется *равномерно распределенной по модулю* 1, если соответствующая последовательность дробных частей $(\{\alpha_i\})$ равномерно распределена в том смысле, как это было определено в § 2. Таким образом, если D_n есть отклонение, как и в § 2, первых n членов последовательности $(\{\alpha_i\})$, то $D_n\to 0$ при $n\to\infty$. Мы покажем, что это условие имеет другую эквивалентную формулировку в терминах нового понятия — *отклонения по модулю* 1.

Пусть дано множество S действительных чисел $\alpha_1, \alpha_2, \ldots, \alpha_Q$, и пусть T — это множество действительных чисел (α_k+t), где $1\leqslant k\leqslant Q$, а t пробегает все целые числа. Для любой пары действительных чисел a и b, таких, что $b\geqslant a$, обозначим через $\varphi^*(a, b)$ число элементов множества T, содержащихся в интервале $[a, b)$. Тогда

$$\varphi^*(a+t, b+t)=\varphi^*(a, b) \tag{3}$$

для любого целого числа t. Далее,

$$\varphi^*(a, b)=\varphi(a, b), \text{ если } 0\leqslant a<b\leqslant 1, \tag{4}$$

где $\varphi(a, b)$ определена для $(\{\alpha_k\})$, $1\leqslant k\leqslant Q$, так же, как в § 2.

Отклонением по модулю 1 множества S мы назовем величину

$$D^* = \sup_{0 \leqslant b-a \leqslant 1} \left| \frac{\varphi^*(a,b)}{Q} - (b-a) \right|. \tag{5}$$

В последнем выражении a пробегает *все* действительные числа, но в силу (3) мы можем предполагать, что $0 \leqslant a < 1$.

Если D — отклонение дробных частей чисел множества S, то из (1), (4) и (5) очевидным образом следует, что $D \leqslant D^*$. С другой стороны, мы имеем $D^* \leqslant 2D$. Действительно, так как любой интервал $[a, b)$, где $0 \leqslant a < 1$ и $b-a \leqslant 1$, может быть представлен в виде объединения не более двух непересекающихся интервалов, каждый из которых имеет вид $[a', b')$, где или $0 \leqslant a' < b' \leqslant 1$, или $1 \leqslant a' < b' \leqslant 2$, то

$$\varphi^*(a, b) = \sum \varphi^*(a', b'), \quad b - a = \sum (b'-a'),$$

где каждая из сумм состоит не более чем из двух членов, и тогда, согласно (1), (3) и (4),

$$\left| \frac{\varphi^*(a,b)}{Q} - (b-a) \right| \leqslant \sum \left| \frac{\varphi^*(a', b')}{Q} - (b'-a') \right| \leqslant 2D.$$

Следовательно, $D^* \leqslant 2D$.

Таким образом, для данного множества S действительных чисел (α_j), $1 \leqslant j \leqslant Q$, мы определили, во-первых, отклонение D множества их дробных частей $(\{\alpha_j\})$ и, во-вторых, отклонение D^* множества S по модулю 1 и показали, что

$$D \leqslant D^* \leqslant 2D. \tag{6}$$

Пусть (α_i) — бесконечная последовательность действительных чисел, не обязательно содержащаяся в единичном интервале. Обозначим через D_n отклонение первых n членов соответствующей последовательности дробных частей $(\{\alpha_i\})$, а через D_n^* — отклонение по модулю 1 первых n членов этой последовательности. Из (6) следует, что если $D_n \to 0$ при $n \to \infty$, то и $D_n^* \to 0$ при $n \to \infty$, и обратно. Таким образом, нами доказана

Теорема 2. *Бесконечная последовательность действительных чисел* (α_i) *равномерно распределена по модулю* 1 *тогда и только тогда, когда* $D_n^* \to 0$ *при* $n \to \infty$, *где* D_n^* — *отклонение по модулю* 1 *первых* n *членов этой последовательности.*

§ 4. Теоремы Вейля.

Теорема 3. *Пусть* (α_j) — *бесконечная последовательность действительных чисел, такая, что* $0 \leqslant \alpha_j < 1$ *при* $j = 1, 2, \ldots$. *Для того чтобы последовательность* (α_j) *была равномерно распределена, необходимо и достаточно, чтобы выполнялось соотношение*

$$\lim_{n\to\infty} \frac{1}{n} \sum_{h=1}^{n} f(\alpha_h) = \int_0^1 f(x)\,dx \tag{7}$$

для любой интегрируемой по Риману на отрезке $0 \leqslant x \leqslant 1$ *функции* f.

Доказательство. Мы можем считать функцию f действительнозначной — в противном случае можно отдельно рассмотреть ее действительную и мнимую части.

Достаточность условия (7) доказать нетрудно. Для любого данного интервала $[a, b)$, где $0 \leqslant a < b \leqslant 1$, возьмем в качестве f характеристическую функцию $[a, b)$: $f(x) = 1$ при $a \leqslant x < b$ и $f(x) = 0$ в противном случае. Тогда

$$\frac{1}{n} \sum_{h=1}^{n} f(\alpha_h) = \frac{\varphi_n(a, b)}{n} \tag{8}$$

и $\int_0^1 f(x)\,dx = b - a$. Тогда из (7) следует, что

$$\lim_{n\to\infty} \frac{\varphi_n(a, b)}{n} = b - a, \tag{9}$$

и, значит, по теореме 1 последовательность (α_j) является равномерно распределенной.

Обратно, если (α_j) равномерно распределена, то имеет место соотношение (9), и тогда (7) выполняется для

характеристической функции f любого интервала $[a, b)$, содержащегося в интервале $[0, 1]$, а в силу линейности (7) выполняется для любой ступенчатой функции на $[0, 1]$. Если функция f интегрируема по Риману на отрезке $[0, 1]$, то для данного $\varepsilon > 0$ можно найти две такие ступенчатые функции f_1 и f_2, что $f_1 \leqslant f \leqslant f_2$ и $\int_0^1 (f_2(x) - f_1(x))\,dx < \varepsilon$. Так как соотношение (7) выполняется для f_1, то мы имеем

$$\lim_{n\to\infty} \frac{1}{n} \sum_{h=1}^{n} f_1(\alpha_h) = \int_0^1 f_1(x)\,dx \geqslant \int_0^1 f(x)\,dx - \varepsilon,$$

так что при достаточно большом n

$$\frac{1}{n} \sum_{h=1}^{n} f_1(\alpha_h) > \int_0^1 f(x)\,dx - 2\varepsilon.$$

Далее из неравенства $f \geqslant f_1$ для достаточно большого n следует, что

$$\frac{1}{n} \sum_{h=1}^{n} f(\alpha_h) > \int_0^1 f(x)\,dx - 2\varepsilon.$$

Аналогично, для достаточно большого n

$$\frac{1}{n} \sum_{h=1}^{n} f(\alpha_h) < \int_0^1 f(x)\,dx + 2\varepsilon.$$

Таким образом, для достаточно больших значений n мы имеем

$$\left| \frac{1}{n} \sum_{h=1}^{n} f(\alpha_h) - \int_0^1 f(x)\,dx \right| < 2\varepsilon,$$

и этим соотношение (7) доказано для каждой интегрируемой по Риману на отрезке $[0, 1]$ функции.

Теорема 4. *Пусть* (β_j) — *бесконечная последовательность действительных чисел, не обязательно содержа-*

щаяся в единичном интервале. Для того чтобы последовательность (β_j) *была равномерно распределена по модулю* 1, *необходимо и достаточно, чтобы выполнялось соотношение*

$$\lim_{n\to\infty}\frac{1}{n}\sum_{h=1}^{n}e^{2\pi i m\beta_h}=0 \tag{10}$$

для каждого целого $m\neq 0$, *где* $i^2=-1$.

Доказательство. Пусть (β_j) равномерно распределена по модулю 1, и пусть α_j обозначает дробную часть β_j. Тогда последовательность (α_j) равномерно распределена в единичном интервале. Если мы возьмем $f(x)=e^{2\pi i m x}$, где m целое и $m\neq 0$, то из теоремы 3 вытекает соотношение

$$\lim_{n\to\infty}\frac{1}{n}\sum_{h=1}^{n}e^{2\pi i m\alpha_h}=\int_0^1 e^{2\pi i m x}\,dx=0,$$

а так как α_h отличается от β_h на целое число, это означает, что справедливо соотношение (10).

Обратно, если (10) выполняется для каждого целого $m\neq 0$, то

$$\lim_{n\to\infty}\frac{1}{n}\sum_{h=1}^{n}e^{2\pi i m\alpha_h}=0.$$

Покажем, что в этом случае условие (7) будет выполняться для каждой интегрируемой по Риману на отрезке $[0, 1]$ функции. Очевидно, (7) имеет место для $f(x)=1$ и по нашему предположению для $f(x)=e^{2\pi i m x}$, где m — целое число, отличное от нуля. Тогда оно будет выполняться также для любого тригонометрического полинома вида

$$a_0+(a_1\cos 2\pi x+b_1\sin 2\pi x)+\ldots+(a_m\cos 2\pi m x+b_m\sin 2\pi m x),$$

где a_i и b_i — константы. Далее, любая непрерывная периодическая функция f с периодом 1 может быть аппроксимирована тригонометрическим полиномом такого

рода. Это означает, что для данного $\varepsilon>0$ существует тригонометрический полином f_ε, такой, что

$$|f-f_\varepsilon| < \varepsilon.$$

Пусть $f_1=f_\varepsilon-\varepsilon$ и $f_2=f_\varepsilon+\varepsilon$, так что $f_1\leqslant f\leqslant f_2$ и $\int_0^1 (f_2(x)-f_1(x))\,dx=2\varepsilon$. Так же, как при доказательстве теоремы 3, мы получаем отсюда, что условие (7) выполняется для любой непрерывной периодической функции с периодом 1. Ограничимся теперь основным интервалом [0, 1]. Для любой ступенчатой функции f на отрезке [0, 1] можно найти две непрерывные периодические функции f_1 и f_2, такие, что

$$f_1\leqslant f\leqslant f_2 \quad \text{и} \quad \int_0^1 (f_2(x)-f_1(x))\,dx<\varepsilon.$$

Следовательно, (7) выполняется для любой ступенчатой функции f, определенной на отрезке [0, 1], а тогда, как было показано выше, оно будет выполняться для любой интегрируемой по Риману на отрезке [0, 1] функции. Теорема 4 доказана.

В качестве приложения теоремы 4 докажем следующий результат:

Теорема 5. *Если* ξ *— любое иррациональное число, то бесконечная последовательность* $(n\xi)$, $n=1, 2, \ldots$, *равномерно распределена по модулю* 1.

Доказательство. Пусть m — целое число, отличное от нуля, и пусть $m\xi=\eta$. Покажем, что

$$\lim_{n\to\infty} \frac{1}{n} \sum_{h=1}^{n} e^{2\pi i h\eta} = 0.$$

Число η действительное и, поскольку ξ иррационально, не целое. Тогда мы имеем

$$\left| \sum_{h=1}^{n} e^{2\pi i h\eta} \right| = \left| \frac{e^{2\pi i(n+1)\eta} - e^{2\pi i\eta}}{e^{2\pi i\eta}-1} \right| \leqslant \frac{2}{|e^{2\pi i\eta}-1|} = \frac{1}{|\sin \pi\eta|},$$

так что

$$\lim_{n\to\infty}\frac{1}{n}\sum_{h=1}^{n}e^{2\pi i h\eta}=0,$$

и из теоремы 4 теперь следует, что последовательность $(n\xi)$, $n=1, 2, \ldots$, равномерно распределена по модулю 1.

Следствие. *Если ξ — иррациональное число, то последовательность дробных частей $(\{n\xi\})$, $n=1, 2, \ldots$, всюду плотна в единичном интервале.*

Понятие равномерного распределения можно распространить на пространства высших размерностей. Пусть $(P^{(j)})$ — бесконечная последовательность точек p-мерного евклидова пространства, где $p\geqslant 1$, и пусть $(x_{j1}, x_{j2}, \ldots, x_{jp})$ — координаты точки $P^{(j)}$. Пусть α_{jr} обозначает дробную часть x_{jr}, а именно $\{x_{jr}\}$, так что $0\leqslant\alpha_{jr}<1$ для $1\leqslant r\leqslant p$. Если через $\{P^{(j)}\}$ мы обозначим вектор дробных частей $(\{x_{j1}\}, \{x_{j2}\}, \ldots, \{x_{jp}\})$, то точка $\{P^{(j)}\}$ будет лежать в единичном кубе $0\leqslant x_j<1$, $1\leqslant j\leqslant p$. Обозначим, наконец, через V *прямоугольник,* лежащий в единичном кубе и являющийся декартовым произведением p интервалов, а через $|V|$ — его меру (Лебега), равную произведению длин соответствующих интервалов. Мы говорим, что бесконечная последовательность $(P^{(j)})$ *равномерно распределена по модулю* 1 тогда и только тогда, когда соответствующая последовательность $(\{P^{(j)}\})$ *равномерно распределена* в единичном кубе, т. е. тогда и только тогда, когда

$$\lim_{n\to\infty}\frac{\varphi_n(V)}{n}=|V|$$

для каждого прямоугольника V, содержащегося в единичном кубе, где $\varphi_n(V)$ означает число точек среди первых n членов последовательности $(\{P^{(j)}\})$, содержащихся в V. В одномерном случае это эквивалентно утверждению, что

$$\sup_{V}\left|\frac{\varphi_n(V)}{n}-|V|\right|\to 0$$

при $n\to\infty$.

Теорема 5′. *Последовательность* $\{P^{(j)}\}$ *равномерно распределена в единичном кубе тогда и только тогда, когда*

$$\lim_{n\to\infty}\frac{1}{n}\sum_{h=1}^{n}e^{2\pi i[m_1\alpha_{h1}+m_2\alpha_{h2}+\ldots+m_p\alpha_{hp}]}=0$$

для каждого набора целых чисел $(m_1, m_2, \ldots, m_p)\neq$ $\neq(0, 0, \ldots, 0)$.

Доказательство этой теоремы аналогично доказательству в случае одной переменной. Отметим только, что «ступенчатая функция» может быть аппроксимирована, например, дважды непрерывно дифференцируемыми функциями, которые имеют равномерно сходящиеся ряды Фурье.

В качестве следствия мы получаем отсюда обобщение теоремы 5:

Теорема 6. *Пусть* $\xi_1, \xi_2, \ldots, \xi_p$ — *действительные числа, такие, что* $\xi_1, \xi_2, \ldots, \xi_p, 1$ *линейно независимы над кольцом целых чисел (т. е. не существует линейного соотношения вида* $\sum_{j=1}^{p} l_j\xi_j=l$, *где* l *и* l_j — *целые числа и* $(l_1, l_2, \ldots, l_p, l)\neq(0, 0, \ldots, 0, 0)$. *Тогда последовательность* $n\xi=(n\xi_1, n\xi_2, \ldots, n\xi_p)$, $n=1, 2, \ldots$, *равномерно распределена по модулю* 1.

§ 5. Теорема Кронекера. Из теоремы 6 следует, что последовательность $(\{n\xi\})$, где $\{n\xi\}=(\{n\xi_1\}, \{n\xi_2\}, \ldots, \{n\xi_p\})$, всюду плотна в единичном кубе. Этот результат, представляющий собой содержание теоремы Кронекера, является обобщением на пространства высших размерностей теоремы, упомянутой в § 1, и может быть сформулирован следующим образом:

Теорема 7. *Пусть* $\theta_1, \theta_2, \ldots, \theta_k, 1$ — *действительные числа, линейно независимые над кольцом целых чисел,* $\alpha_1, \alpha_2, \ldots, \alpha_k$ — *произвольные действительные числа и* N, ε — *положительные действительные числа. Тогда суще-*

ствуют целые числа n *и* $p_1, p_2, \ldots, p_k$, *такие, что*

$$n>N \quad и \quad |n\theta_m - p_m - \alpha_m| < \varepsilon$$

для всех $m=1, 2, \ldots, k$.

Приведем теперь другой вариант этой теоремы:

Теорема 8. *Пусть* $\theta_1, \theta_2, \ldots, \theta_k$ — *действительные числа, линейно независимые над кольцом целых чисел,* $\alpha_1, \alpha_2, \ldots, \alpha_k$ — *произвольные действительные числа и* T, ε — *положительные действительные числа. Тогда существуют действительное число* t *и целые числа* $p_1, p_2, \ldots, p_k$, *такие, что*

$$t>T \quad и \quad |t\theta_m - p_m - \alpha_m| < \varepsilon$$

для всех $m=1, 2, \ldots, k$.

Покажем, что теорема 7 эквивалентна теореме 8. Предположим, сначала, что справедлива теорема 8, и выведем из нее теорему 7.

Чтобы доказать теорему 7 в приведенной выше формулировке, достаточно доказать ее для $0<\theta_m\leqslant 1$, где $1\leqslant m\leqslant k$. Действительно, если $1, \theta_1, \ldots, \theta_k$ линейно независимы над кольцом целых чисел, то числа $1, \theta_1', \ldots, \theta_k'$, где $\theta_j' = \theta_j - q_j$ и (q_j) — подходящие целые числа, также будут линейно независимы. Кроме того, из неравенства $|n\theta_m' - p_m' - \alpha_m| < \varepsilon$ при целом p_m' следует неравенство $|n\theta_m - p_m - \alpha_m| < \varepsilon$, где $p_m = p_m' + nq_m$. Предположим поэтому, что $0<\theta_m\leqslant 1$ при $1\leqslant m\leqslant k$, $0<\varepsilon<1$ и что $\theta_1, \theta_2, \ldots, \theta_k, 1$ линейно независимы над кольцом целых чисел. Тогда по теореме 8 с $k+1$ вместо k, $N+1$ вместо T и $\varepsilon/2$ вместо ε, примененной к наборам

$$\theta_1, \theta_2, \ldots, \theta_k, \ 1 \quad и \quad \alpha_1, \alpha_2, \ldots, \alpha_k, \ 0,$$

существуют такие целые числа $p_1, p_2, \ldots, p_{k+1}$ и действительное число t, $t>N+1$, которые удовлетворяют неравенствам

$$|t\theta_m - p_m - \alpha_m| < \varepsilon/2, \quad m=1, 2, \ldots, k,$$

и

$$|t - p_{k+1}| < \varepsilon/2.$$

Так как $t>N+1$ и $\varepsilon<1$, из последнего неравенства следует, что $p_{k+1}>t-\varepsilon/2>N$, а так как $0<\theta_m\leqslant 1$, то

$$|p_{k+1}\theta_m-p_m-\alpha_m|\leqslant|t\theta_m-p_m-\alpha_m|+|(p_{k+1}-t)\theta_m|\leqslant$$
$$\leqslant|t\theta_m-p_m-\alpha_m|+|p_{k+1}-t|<\varepsilon$$

при всех $m=1, 2, \ldots, k$. Отсюда следует справедливость теоремы 7, если положить $n=p_{k+1}$.

Обратно, будем считать справедливой теорему 7 и докажем теорему 8. Если $k=1$, то теорема 8 очевидна. Предположим, что $k>1$. Далее, достаточно доказать теорему для $\theta_m>0$, $m=1, 2, \ldots, k$. Пусть $\theta_1, \theta_2, \ldots, \theta_k$ линейно независимы над кольцом целых чисел. Тогда числа

$$\frac{\theta_1}{\theta_k}, \frac{\theta_2}{\theta_k}, \ldots, \frac{\theta_{k-1}}{\theta_k}, 1$$

будут также линейно независимы. Из теоремы 7 с $N=T\theta_k$, примененной к наборам чисел

$$\frac{\theta_1}{\theta_k}, \frac{\theta_2}{\theta_k}, \ldots, \frac{\theta_{k-1}}{\theta_k} \quad \text{и} \quad \alpha_1, \alpha_2, \ldots, \alpha_{k-1},$$

следует существование целых чисел $p_1, p_2, \ldots, p_{k-1}$ и n, $n>N$, таких, что

$$\left|n\frac{\theta_m}{\theta_k}-p_m-\alpha_m\right|<\varepsilon, \quad m=1, 2, \ldots, k-1.$$

Положим теперь $t=n/\theta_k$. Тогда $t>T$ и

$$|t\theta_m-p_m-\alpha_m|<\varepsilon, \quad m=1, 2, \ldots, k-1.$$

Кроме того, очевидно, что

$$|t\theta_k-n|<\varepsilon,$$

и мы получаем утверждение теоремы 8 для наборов чисел

$$\theta_1, \theta_2, \ldots, \theta_k \quad \text{и} \quad \alpha_1, \alpha_2, \ldots, \alpha_{k-1}, 0.$$

Аналогичным способом мы можем доказать теорему 8 для наборов

$$\theta_1, \theta_2, \ldots, \theta_k \quad \text{и} \quad 0, 0, \ldots, 0, \alpha_k.$$

Отсюда мы можем заключить, что теорема 8 справедлива для наборов чисел $\theta_1, \theta_2, \ldots, \theta_k$ и $\alpha_1, \alpha_2, \ldots, \alpha_k$.

Действительно, если разность между $t\theta_m$ и α_m сколь угодно мало отличается от некоторого целого числа, а разность между $t'\theta_m$ и β_m также сколь угодно мало отличается от целого числа, то разность между $(t+t')\theta_m$ и $\alpha_m+\beta_m$ обладает тем же свойством. Таким образом, эквивалентность теорем 7 и 8 доказана.

Дадим теперь доказательство теоремы 8, предложенное Бором.

Доказательство теоремы 8. Если c — действительное число, $T>0$ и $i^2=-1$, то

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T e^{cit}\,dt=\begin{cases}0, & \text{если } c\neq 0,\\ 1, & \text{если } c=0.\end{cases}$$

Таким образом, если c_ν — действительные числа и

$$\chi(t)=\sum_{\nu=1}^{r} b_\nu e^{c_\nu it}, \quad c_m\neq c_n \text{ при } m\neq n, \tag{11}$$

то

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T \chi(t)e^{-c_\nu it}dt=b_\nu. \tag{12}$$

Пусть

$$F(t)=1+\sum_{m=1}^{k} e^{2\pi i(t\theta_m-\alpha_m)}, \tag{13}$$

где t — действительное переменное и

$$\varphi(t)=|F(t)|.$$

Очевидно,

$$0\leqslant\varphi(t)\leqslant k+1.$$

Если теорема 8 справедлива, то для некоторого достаточно большого t каждое число $t\theta_m-\alpha_m$ сколь угодно мало будет отличаться от некоторого целого и тогда $\varphi(t)$ сколь угодно мало будет отличаться от $k+1$. Действительно, если $x_m=t\theta_m-\alpha_m$, то для данного $\varepsilon>0$ найдется $\delta>0$,

такое, что если $|x_m - p_m| < \delta$ для некоторого целого числа p_m, то $|e^{2\pi i x_m} - 1| < \varepsilon$.

Обратно, если $\varphi(t)$ сколь угодно мало отличается от $k+1$ для некоторого достаточно большого t, то каждый член в сумме (13) должен как угодно мало отличаться от 1, поскольку ни один из этих членов по абсолютной величине не превосходит 1, и тогда теорема 8 должна быть справедливой. Мы можем доказать это следующим образом. Если существует такое η, $0 < \eta < 1$, что $\varphi(t) \geqslant k+1-\eta$, и если $z = e^{2\pi i x_m} = x + iy$, то $|y| \leqslant 2\eta^{1/2}$. В самом деле,

$$k + 1 - \eta \leqslant \varphi(t) \leqslant (k-1) + |1 + e^{2\pi i x_m}|$$

или

$$2 \geqslant |1 + e^{2\pi i x_m}| \geqslant 2 - \eta \quad \text{при} \quad m = 1, 2, \ldots, k.$$

Отсюда мы получаем, что

$$|1+z|^2 = (1+x)^2 + y^2 = (1+x)^2 + (1-x^2) = 2 + 2x \geqslant$$
$$\geqslant (2-\eta)^2 > 4 - 4\eta,$$

так что $1 \geqslant x \geqslant 1 - 2\eta$. Далее,

$$y^2 = 1 - x^2 = (1-x)(1+x) \leqslant 4\eta.$$

Значит, $|y| \leqslant 2\eta^{1/2}$, и потому $|z-1| < 4\eta^{1/2}$.

Следовательно, теорема 8 будет доказана, если мы покажем что

$$\overline{\lim_{t \to \infty}} \varphi(t) \geqslant k + 1. \tag{14}$$

Пусть

$$\psi = \psi(x_1, x_2, \ldots, x_k) = 1 + x_1 + x_2 + \ldots + x_k$$

и p — положительное целое число. Тогда

$$\psi^p = \sum_{\substack{n_1 + \ldots + n_k \leqslant p \\ n_j \geqslant 0, \quad j = 1, \ldots, k}} a_{n_1, \ldots, n_k} x_1^{n_1} x_2^{n_2} \ldots x_k^{n_k}, \tag{15}$$

где коэффициенты $a_{n_1, \ldots, n_k}$ обладают следующими свойствами: (i) $a_{n_1, \ldots, n_k}$ положительны; (ii) $\sum a_{n_1, \ldots, n_k} = \psi^p(1, 1, \ldots, 1) = (k+1)^p$; (iii) их количество не превосходит $(p+1)^k$.

Рассмотрим теперь

$$F^p(t) = \left(1 + \sum_{m=1}^{k} e^{2\pi i(t\theta_m - \alpha_m)}\right)^p.$$

Если в разложении (15) мы возьмем $e^{2\pi i(t\theta_j - \alpha_j)}$ вместо x_j, то $F^p(t)$ будет суммой вида (11), где роль c_ν играют числа $2\pi(n_1\theta_1 + \ldots + n_k\theta_k)$. Так как θ_j линейно независимы, то числа c_ν различны. Роль b_ν в (11) будут играть числа $a_{n_1,\ldots,n_k}$, умноженные на $e^{-2\pi i(n_1\alpha_1 + \ldots + n_k\alpha_k)}$. Следовательно,

$$\sum |b_\nu| = \sum a_{n_1,\ldots,n_k} = (k+1)^p. \tag{16}$$

Поскольку $\varphi(t) \leqslant k+1$, для доказательства неравенства (14) достаточно будет показать, что неравенство

$$\overline{\lim_{t\to\infty}}\, \varphi(t) < k+1 \tag{17}$$

не может иметь места. Неравенство (17) означает, что

$$|F(t)| = \varphi(t) \leqslant \lambda < k+1$$

для всех достаточно больших t и, следовательно, что

$$\overline{\lim_{T\to\infty}} \frac{1}{T} \int_0^T |F(t)|^p\, dt \leqslant \lim_{T\to\infty} \frac{1}{T} \int_0^T \lambda^p\, dt = \lambda^p.$$

Однако

$$b_\nu = \overline{\lim_{T\to\infty}} \frac{1}{T} \int_0^T F^p(t)\, e^{-c_\nu i t}\, dt,$$

откуда

$$|b_\nu| \leqslant \overline{\lim_{T\to\infty}} \frac{1}{T} \int_0^T |F(t)|^p\, dt \leqslant \lambda^p,$$

так что каждый коэффициент в разложении (15) будет удовлетворять неравенству

$$a_{n_1,\ldots,n_k} \leqslant \lambda^p.$$

Поскольку имеется самое большее $(p+1)^k$ таких коэффициентов, мы имеем

$$(k+1)^p = \sum a_{n_1,\ldots,n_k} \leqslant (p+1)^k \lambda^p.$$

Но так как $\mu = \lambda/(k+1) < 1$ и $\mu^p (p+1)^k \to 0$ при $p \to \infty$, то отсюда следует, что неравенство (17) не может иметь места. В таком случае справедливо неравенство (14), а тем самым и теорема 8.

ТЕОРЕМА МИНКОВСКОГО О ЦЕЛЫХ ТОЧКАХ В ВЫПУКЛЫХ МНОЖЕСТВАХ

§ 1. Выпуклые множества. В гл. VI мы столкнулись с задачами о числе целых точек в некоторых областях *на плоскости*. Пусть R^n, $n \geqslant 1$, есть n-мерное евклидово пространство. Точку пространства мы назовем *целой*, если все ее координаты — целые числа. В этой главе мы докажем теорему Минковского о том, что каждое выпуклое симметричное относительно начала координат множество в пространстве R^n, объем которого больше 2^n, содержит по крайней мере одну целую точку, отличную от начала координат.

Определения. Пусть S — множество точек пространства R^n. Для действительного числа λ через λS мы обозначим множество, получающееся из S растяжением в λ раз, т. е.

$$\lambda S = [\lambda x \mid x \in S].$$

Мы говорим, что множество S *выпукло*, если из условия $x \in S$, $y \in S$ следует, что $\lambda x + \mu y \in S$ для всех действительных λ и μ, таких, что $\lambda \geqslant 0$, $\mu \geqslant 0$, $\lambda + \mu = 1$. Если множество S выпукло, то λS также выпукло.

Мы говорим, что множество S *симметрично относительно начала координат,* или просто *симметрично,* если из условия $x \in S$ следует, что $-x \in S$. Если S симметрично, то множество λS также симметрично.

Пусть g — целая точка пространства R^n. Тогда множество S_g, состоящее из точек $x \in R^n$, таких, что $x - g \in S$, мы назовем *трансляцией* множества S на вектор g.

Если множество S измеримо по Лебегу и $V(S)$ — его мера, то $V(S) = V(S_g)$ для любой целой точки g.

Выпуклые симметричные множества. (а) Пусть множество S выпукло и симметрично, и пусть $x \in S$. Тогда $\lambda x \in S$ для каждого действительного числа λ, такого, что $|\lambda| \leqslant 1$.

Действительно, если $x \in S$, то из симметричности мно-

жества S следует, что $-x\in S$, а тогда при $|\lambda|\leqslant 1$ из условия выпуклости S мы имеем

$$\left(\frac{1}{2}+\frac{\lambda}{2}\right)x+\left(\frac{1}{2}-\frac{\lambda}{2}\right)(-x)=\lambda x\in S.$$

(b) Пусть множество S выпукло и симметрично, и пусть $x\in S$, $y\in S$. Тогда $\lambda x+\mu y\in S$ для всех действительных λ и μ, таких, что $|\lambda|+|\mu|\leqslant 1$.

Если $\lambda=0$ или $\mu=0$, то свойство (b) сводится к свойству (a). Предположим поэтому, что $\lambda\neq 0$ и $\mu\neq 0$, и положим $\varepsilon_1=\operatorname{sgn}\lambda$, $\varepsilon_2=\operatorname{sgn}\mu$. Тогда из свойства (a) и условия $|\lambda|+|\mu|\leqslant 1$ мы имеем $x'=\varepsilon'(|\lambda|+|\mu|)x\in S$, $y'=\varepsilon_2(|\lambda|+|\mu|)y\in S$.

Положим

$$\rho=\frac{|\lambda|}{|\lambda|+|\mu|},\quad \sigma=\frac{|\mu|}{|\lambda|+|\mu|}.$$

Тогда $\rho>0$, $\sigma>0$ и $\rho+\sigma=1$, а так как S выпукло, то $\rho x'+\sigma y'\in S$. Но $\rho x'+\sigma y'=\lambda x+\mu y$, и тем самым мы получаем свойство (b).

§ 2. Теорема Минковского.

Теорема 1 (Минковский). *Пусть S — ограниченное измеримое выпуклое симметричное множество точек пространства R^n, и пусть его мера V удовлетворяет неравенству $V>2^n$. Тогда S содержит по крайней мере одну целую точку, отличную от начала координат.*

Мы дадим доказательство этой теоремы, предложенное К. Л. Зигелем и основанное на формуле для меры ограниченного измеримого выпуклого симметричного множества, не содержащего целых точек, отличных от начала координат. Предположение об ограниченности множества S в теореме 1 не является необходимым (см. теорему 3 и примечания к гл. IX).

Доказательство теоремы 1 (Зигель). Пусть S — ограниченное измеримое выпуклое симметричное множество в R^n и V — его мера. Обозначим через $L_2(S)$ множество функций, интегрируемых с квадратом на S. Пусть $\varphi\in L_2(S)$, и пусть $\varphi(x)=0$ при $x\notin S$.

Мы будем употреблять, как обычно, запись $k=(k_1, k_2, ..., k_n)$, $x=(x_1, x_2, ..., x_n)$, $k\cdot x=k_1x_1+k_2x_2+...$ $...+k_nx_n$ и $dx=dx_1dx_2...dx_n$.

Рассмотрим функцию

$$f(x)=\sum_k \varphi(2x-2k), \tag{1}$$

где k пробегает множество всех целых точек пространства R^n. Для любого данного x эта сумма конечна, так как φ равна нулю вне S и S ограничено. Поскольку k пробегает *все* целые точки, эта сумма остается неизменной при подстановке $k_\nu \to k_\nu+1$. Следовательно, $f(x)$ является периодической функцией по каждому переменному $x_1, x_2, ..., x_n$ с периодом 1.

Формула Парсеваля для ряда Фурье функции f дает

$$\int_E |f|^2 dx=\sum_l |a_l|^2, \tag{2}$$

где E есть n-мерный куб со стороной 1, l — целые точки в R^n и a_l — коэффициенты Фурье функции f:

$$a_l=\int_E f(x)e^{-2\pi ilx}dx. \tag{3}$$

Из (1) мы имеем

$$a_l=\int_E \sum_k \varphi(2x-2k)e^{-2\pi ilx}dx=\sum_k \int_E \varphi(2x-2k)e^{-2\pi ilx}dx,$$

где k пробегает все целые точки пространства R^n. Положим $x-k=t$. Если x пробегает точки единичного куба E, а k пробегает все целые точки, то t пробегает все точки пространства R^n. Следовательно,

$$a_l=\int_{R^n} \varphi(2t)e^{-2\pi il(k+t)}dt=\int_{R^n} \varphi(2t)e^{-2\pi ilt}dt.$$

Если мы положим $2t=x$, то, поскольку функция φ равна нулю вне множества S, получим

$$a_l=2^{-n}\int_S \varphi(x)e^{-\pi ilx}dx. \tag{4}$$

С другой стороны, из (1) мы получаем

$$\int_E |f|^2\,dx = \int_E \sum_{k'}\Big(\sum_k \varphi(2x-2k)\,\overline{\varphi(2x-2k')}\Big)\,dx =$$

$$= \int_{R^n} \sum_k \varphi(2x-2k)\,\overline{\varphi(2x)}\,dx = 2^{-n}\int_{R^n}\sum_k \varphi(x-2k)\,\overline{\varphi(x)}\,dx =$$

$$= 2^{-n}\sum_k \int_S \varphi(x-2k)\,\overline{\varphi(x)}\,dx. \quad (5)$$

Тогда, применяя (2), (4) и (5), имеем

$$\sum_k \int_S \varphi(x-2k)\,\overline{\varphi(x)}\,dx = 2^{-n}\sum_l \Big|\int_S \varphi(x)\,e^{-\pi i l x}\,dx\Big|^2. \quad (6)$$

Далее, если $\varphi(x-2k)\,\overline{\varphi(x)} \neq 0$, то $x \in S$ и $x-2k \in S$. Поскольку S симметрично и выпукло, $\frac{1}{2}x + \frac{1}{2}(2k-x) = k \in S$. Следовательно, если S не содержит целых точек, отличных от начала координат, то мы должны иметь $\varphi(x-2k)\,\overline{\varphi(x)} = 0$ при $k \neq 0$, и тогда (6) сводится к соотношению

$$\int_S |\varphi(x)|^2\,dx = 2^{-n}\sum_l \Big|\int_S \varphi(x)e^{-\pi i l x}\,dx\Big|^2. \quad (7)$$

Возьмем теперь $\varphi(x)=1$ при $x \in S$. Тогда $\int_S |\varphi(x)|^2\,dx = V$ и равенство (7) дает

$$V = 2^{-n}\sum_l \Big|\int_S e^{-\pi i l x}\,dx\Big|^2 = 2^{-n}\Big(V^2 + \sum_{l\neq 0}\Big|\int_S e^{-\pi i l x}\,dx\Big|^2\Big).$$

Так как $-l$ пробегает те же самые точки, что и l, мы можем переписать последнее равенство в виде

$$2^n = V + \frac{1}{V}\sum_{l\neq 0}\Big|\int_S e^{\pi i l x}\,dx\Big|^2, \quad (8)$$

что даст нам *формулу Зигеля* для меры V ограниченного измеримого выпуклого симметричного множества S пространства R^n, *не* содержащего целой точки, отличной от начала координат. Из этой формулы следует, что $V \leqslant 2^n$,

откуда непосредственно вытекает утверждение теоремы.

Если мы хотим доказать только теорему 1, а не формулу (8), можно использовать вместо равенства Парсеваля неравенство Шварца

$$\int_E |f|^2\,dx \geqslant |a_0|^2.$$

По формуле (4) имеем

$$a_0 = 2^{-n}\int_S \varphi(x)\,dx = 2^{-n}V,$$

и если S не содержит целых точек, отличных от начала координат, то, согласно (5),

$$\int_E |f|^2\,dx = 2^{-n}V.$$

Следовательно, $V \leqslant 2^n$.

Теорема 1 неверна для ограниченных измеримых выпуклых симметричных множеств меры $V=2^n$. Действительно, рассмотрим множество $|x_i|<1$, $1 \leqslant i \leqslant n$. Оно ограничено, измеримо, выпукло, симметрично и имеет меру $V=2^n$, но не содержит ни одной целой точки, отличной от начала координат.

Однако если S замкнуто, то справедлива

Теорема 2. *Замкнутое ограниченное выпуклое симметричное множество S пространства R^n, имеющее меру $V(S) \geqslant 2^n$, содержит по меньшей мере одну целую точку, отличную от начала координат.*

Доказательство. Для данного ε, $0<\varepsilon<1$, рассмотрим множество $S'=(1+\varepsilon)S$. Так как S измеримо, то S' также измеримо, и если через $V(S)$ и $V(S')$ обозначены соответствующие меры, то

$$V(S') = (1+\varepsilon)^n V(S) \geqslant 2^n(1+\varepsilon)^n > 2^n.$$

Следовательно, по теореме 1 множество S' содержит целую точку l_ε, отличную от начала координат. Множество S ограничено, и таким же будет множество S', а тогда для l_ε имеется только конечное число возможностей. Поэтому существует целая точка l_0, отличная от начала

координат, такая, что $l_0 \in (1+\varepsilon)S$ для каждого ε, $0<\varepsilon<1$, т. е. $l_0/(1+\varepsilon) \in S$. Если $\varepsilon \to 0$, то $l_0 \in S$, поскольку S замкнуто. Этим теорема 2 доказана.

Из теоремы 2 следует

Теорема 2′. *Если S — ограниченное выпуклое симметричное множество, имеющее меру $V(S) \geqslant 2^n$, то его замыкание содержит по меньшей мере одну целую точку, отличную от начала координат.*

Доказательство. Для данного ограниченного выпуклого симметричного множества S рассмотрим его замыкание $\overline{S}$. Множество $\overline{S}$ так же, как и множество S, ограничено выпукло и симметрично, а также замкнуто, и его мера $V(\overline{S}) \geqslant V(S) \geqslant 2^n$. Значит, $\overline{S}$ удовлетворяет условиям теоремы 2 и, следовательно, содержит по меньшей мере одну целую точку, отличную от начала координат.

Чтобы дать другое доказательство теоремы Минковского, мы докажем сначала следующую лемму:

Лемма (Г. Д. Биркгоф). *Если S — измеримое множество пространства R^n, имеющее меру $V(S)>1$, то существуют две различные точки $x \in S$ и $y \in S$, такие, что $x-y$ есть целая точка.*

Доказательство. Пусть $g=(g_1, g_2, \ldots, g_n)$ — какая-либо целая точка. Рассмотрим куб $[x_i | g_i \leqslant x_i < g_i+1]$, $i=1, 2, \ldots, n$, и обозначим через S^g пересечение множества S с этим кубом:

$$S^g \equiv S \cap [(x_1, \ldots, x_n) \in R^n,\ g_i \leqslant x_i < g_i+1,\ 1 \leqslant i \leqslant n].$$

Пусть S^g_{-g} — трансляция множества S^g на вектор $-g$ (см. § 1). Тогда S^g_{-g} содержится в единичном кубе $0 \leqslant x_i < 1$, $1 \leqslant i \leqslant n$. Если V_g есть мера множества S^g_{-g}, то V_g будет также мерой множества S^g и $\sum\limits_g V_g = V > 1$.

Отсюда, так как единичный куб имеет меру 1, следует существование по крайней мере двух множеств S^g_{-g} и $S^{g'}_{-g'}$, где g и g' — различные целые точки, имеющие не-

пустое пересечение. Другими словами, существуют две точки $x \in S^g$ и $y \in S^{g'}$, такие, что $x-g=y-g'$. Следовательно, мы нашли две такие точки $x \in S$ и $y \in S$, что $x-y=g-g'$ есть целая точка. (Она не обязана, конечно, принадлежать множеству S.) Лемма тем самым доказана.

С помощью этой леммы мы докажем следующее утверждение:

Теорема 3 (Минковский). *Если измеримое выпуклое симметричное множество S имеет меру $V>2^n$ (возможно, $V=\infty$), то оно содержит по крайней мере одну целую точку, отличную от начала координат.*

Доказательство. Рассмотрим множество $\frac{1}{2}S$, мера которого есть $\left(\frac{1}{2}\right)^n V>1$. По доказанной выше лемме существуют две *различные* точки $x \in \frac{1}{2}S$ и $y \in \frac{1}{2}S$, такие, что их разность $x-y=g$ будет целой точкой. Так же как и S, множество $\frac{1}{2}S$ является выпуклым и симметричным. Поэтому из свойства (b), сформулированного в § 1, следует, что $\frac{1}{2}x-\frac{1}{2}y=\frac{1}{2}g \in \frac{1}{2}S$, а тогда $g \in S$ и g отлична от начала координат, поскольку x и y различны. Теорема доказана.

Последняя теорема может быть использована для изучения однородных линейных форм. Пусть

$$\xi_i=a_{i1}x_1+a_{i2}x_2+\ldots+a_{in}x_n, \quad i=1, 2, \ldots, n, \tag{9}$$

суть n однородных линейных форм от n неизвестных $x_1, \ldots, x_n$ с действительными коэффициентами a_{ij}, и пусть Δ — определитель матрицы (a_{ij}). Предположим сначала, что $\Delta \neq 0$.

Эти формы определяют линейное преобразование x-пространства в ξ-пространство, и если множество S выпукло и симметрично в x-пространстве, то его образ T в ξ-пространстве также будет выпуклым и симметричным, поскольку выпуклость и симметричность инвариант-

ны относительно линейных преобразований. Но мера меняется при линейных преобразованиях, а именно если $\Delta \neq 0$, то

$$\int_T d\xi_1 d\xi_2 \ldots d\xi_n = |\Delta| \int_S dx_1 dx_2 \ldots dx_n, \tag{10}$$

так что мера множества T получается из меры множества S умножением на множитель $|\Delta|$.

Рассмотрим линейное преобразование L пространства R^n в себя: $(x_1, x_2, \ldots, x_n) \to (\xi_1, \xi_2, \ldots, \xi_n)$. Образ целых точек при этом преобразовании называется *решеткой* Λ пространства R^n, связанной с L. Определитель преобразования L называется *определителем решетки* Λ.

Применение теоремы 3 к ξ-пространству дает следующий результат:

Теорема 4. *Пусть Λ — решетка пространства R^n с определителем $\Delta \neq 0$ и P — измеримое выпуклое симметричное множество, мера которого $V > 2^n|\Delta|$ (возможно, $V = \infty$). Тогда P содержит по крайней мере одну точку решетки Λ, отличную от начала координат.*

Далее из теоремы 2 следует

Теорема 4′. *Пусть Λ — решетка пространства R^n с определителем $\Delta \neq 0$ и P — замкнутое ограниченное выпуклое симметричное множество, имеющее меру $V \geqslant 2^n|\Delta|$. Тогда P содержит по крайней мере одну точку решетки Λ, отличную от начала координат.*

§ 3. Приложения. (А) Рассмотрим в x-пространстве замкнутое множество S, определенное неравенствами

$$|\xi_i| \leqslant c_i, \quad i = 1, 2, \ldots, n. \tag{11}$$

Очевидно, что множество S симметрично. Оно будет также выпуклым. Действительно, если $x \in S$, $y \in S$ и $z = \lambda x + \mu y$, где $\lambda \geqslant 0$, $\mu \geqslant 0$, $\lambda + \mu = 1$, то

$$|a_{i1}z_1 + a_{i2}z_2 + \ldots + a_{in}z_n| \leqslant$$
$$\leqslant \lambda |a_{i1}x_1 + \ldots + a_{in}x_n| + \mu |a_{i1}y_1 + \ldots + a_{in}y_n| \leqslant$$
$$\leqslant \max(|a_{i1}x_1 + \ldots + a_{in}x_n|, \ |a_{i1}y_1 + \ldots + a_{in}y_n|).$$

Кроме того, S ограничено. Действительно, если (α_{ij}) — матрица, обратная к матрице (a_{ij}), то из равенств $\xi_i = \sum_{j=1}^{n} a_{ij}x_j$ следует, что $x_i = \sum_{j=1}^{n} \alpha_{ij}\xi_j$ и тогда $|x_i| \leqslant \leqslant \sum |\alpha_{ij}| c_j$. По формуле (10) мера множества S равна $2^n |\Delta|^{-1} c_1 c_2 \ldots c_n$. Соответствующее множество в ξ-пространстве является параллелепипедом и имеет меру $2^n c_1 c_2 \ldots c_n$.

Применяя теорему 4′, получаем такой результат:

Теорема 5. *Пусть* $\xi_1, \xi_2, \ldots, \xi_n$ — *однородные линейные формы от* n *переменных* $x_1, x_2, \ldots, x_n$ *с действительными коэффициентами и определителем* $\Delta \neq 0$. *Если* $c_1, c_2, \ldots, c_n$ — *положительные действительные числа, такие, что* $c_1 c_2 \ldots c_n \geqslant |\Delta|$, *то существуют целые числа* $x_1, x_2, \ldots, x_n$, *не равные одновременно нулю, для которых* $|\xi_1| \leqslant c_1$, $|\xi_2| \leqslant \leqslant c_2, \ldots, |\xi_n| \leqslant c_n$.

Мы можем, в частности, взять $c_i = |\Delta|^{1/n}$, $i = 1, 2, \ldots, n$, и получить одни и те же оценки для всех n неравенств (11).

Мы предполагали до сих пор, что $\Delta \neq 0$. Если $\Delta = 0$, то легко видеть, что множество S в x-пространстве, определяемое неравенствами (11), имеет бесконечный объем, если $c_i > 0$ для каждого i, и заключение теоремы 5 остается справедливым.

Рассмотрим теперь вместо (11) систему, в которой число неравенств меньше числа неизвестных, а именно:

$$|\xi_i| = |a_{i1}x_1 + \ldots + a_{in}x_n| \leqslant c_i, \quad i = 1, 2, \ldots, m, \quad m < n. \tag{12}$$

Тогда множество, определяемое данной системой в x-пространстве, не будет ограниченным, но в силу теоремы 3 заключение теоремы 5 остается в силе, т. е. существуют целые числа $x_1, x_2, \ldots, x_n$, не равные одновременно нулю, которые удовлетворяют m неравенствам (12).

Заметим, что случай $m < n$ сводится к предшествующему случаю $m = n$, $\Delta = 0$. Для этого достаточно, например, записать неравенство (12) при $i = m$ точно $n - m + 1$ раз.

(B) В качестве второго приложения рассмотрим множество T в ξ-пространстве, определенное неравенством

$$|\xi_1| + |\xi_2| + \ldots + |\xi_n| \leqslant c.$$

Оно, очевидно, симметрично. Множество T будет также выпуклым. Действительно, если $\xi=(\xi_1,\ldots,\xi_n)\in T$, $\xi'=(\xi_1',\ldots,\xi_n')\in T$ и $\lambda\geqslant 0$, $\mu\geqslant 0$, $\lambda+\mu=1$, то

$$\sum_{k=1}^{n}|\lambda\xi_k+\mu\xi_k'|\leqslant\lambda\sum_{k=1}^{n}|\xi_k|+\mu\sum_{k=1}^{n}|\xi_k'|\leqslant$$

$$\leqslant\max\Big(\sum_{k=1}^{n}|\xi_k|,\ \sum_{k=1}^{n}|\xi_k'|\Big).$$

Заметим, что при $n=2$ множество T является квадратом, а при $n=3$ множество T является октаэдром. Объем T может быть вычислен следующим образом. Множество T состоит из 2^n конгруэнтных частей, по одной из каждого октанта, и та часть, которая лежит в октанте $\xi_1>0$, $\xi_2>0,\ldots,\ \xi_n>0$, имеет объем

$$c^n\int_0^1 d\xi_1\int_0^{1-\xi_1} d\xi_2\ldots\int_0^{1-\xi_1-\ldots-\xi_{n-1}} d\xi_n=\frac{c^n}{n!}.$$

Следовательно, T имеет объем $V=(2c)^n/n!$.

Если $c^n\geqslant n!\,|\Delta|$, то из теоремы 4′ вытекает

Теорема 6. *Существуют целые числа x_1, x_2, ..., x_n, не равные одновременно нулю, такие, что*

$$|\xi_1|+|\xi_2|+\ldots+|\xi_n|\leqslant(n!\,|\Delta|)^{1/n}.$$

Так как $|\xi_1\xi_2\ldots\xi_n|^{1/n}\leqslant\frac{1}{n}(|\xi_1|+\ldots+|\xi_n|)$, то отсюда следует

Теорема 6′. *Существуют целые числа x_1, $x_2,\ldots,x_n$, не равные одновременно нулю, такие, что*

$$|\xi_1\xi_2\ldots\xi_n|\leqslant\frac{n!\,|\Delta|}{n^n}.$$

(C) В качестве третьего приложения рассмотрим в ξ-пространстве множество P, определенное неравенством

$$\xi_1^2+\xi_2^2+\cdots+\xi_n^2\leqslant c^2.$$

Это множество симметрично и выпукло. Симметричность множества P очевидна, а выпуклость следует из неравенства

$$\sum_{k=1}^{n}(\lambda\xi_k+\mu\xi_k')^2=\lambda^2\sum_{k=1}^{n}\xi_k^2+2\lambda\mu\sum_{k=1}^{n}\xi_k\xi_k'+\mu^2\sum_{k=1}^{n}\xi_k'^2\leqslant$$

$$\leqslant\left(\lambda\sqrt{\sum_{k=1}^{n}\xi_k^2}+\mu\sqrt{\sum_{k=1}^{n}\xi_k'^2}\right)^2.$$

Далее, объем множества P равен

$$c^n\int\limits_{\sum\xi_k^2\leqslant 1}\cdots\int d\xi_1\ldots d\xi_n=\frac{c^n\pi^{n/2}}{\Gamma(n/2+1)}=c^n s_n.$$

Следовательно, если $c\geqslant 2(|\Delta|/s_n)^{1/n}$, мы можем применить теорему 4′ и получить следующий результат:

Теорема 7. *Существуют целые числа $x_1, x_2,\ldots, x_n$, не равные одновременно нулю, такие, что*

$$\xi_1^2+\xi_2^2+\cdots+\xi_n^2\leqslant 4\left(\frac{|\Delta|}{s_n}\right)^{2/n}.$$

Эта теорема может быть распространена на общие *положительно определенные квадратичные формы*

$$Q(x_1,\ldots,x_n)=\sum_{r,s=1}^{n}a_{rs}x_r x_s$$

с действительными коэффициентами $a_{rs}=a_{sr}$. Мы говорим, что форма Q является *положительно определенной,* если $Q(x_1,\ldots,x_n)>0$ для всех $x_1, x_2,\ldots, x_n$, отличных от $0, 0,\ldots, 0$. Определитель D матрицы (a_{rs}) называется *определителем* формы Q, причем $D>0$, если Q положительно определена. Любая положительно определенная форма Q может быть приведена к виду

$$Q=\xi_1^2+\xi_2^2+\ldots+\xi_n^2,$$

где ξ_k — линейные формы от $x_1, x_2, \ldots, x_n$ с действительными коэффициентами и определителем $\sqrt{D}$.

Теорема 7 может быть, следовательно, сформулирована таким образом:

Теорема 8. *Пусть Q — положительно определенная квадратичная форма от n переменных с определителем D. Тогда существуют целые числа $x_1, x_2, \ldots, x_n$, не все равные нулю, такие, что*

$$Q(x_1, \ldots, x_n) \leqslant 4\left(\frac{D}{s_n^2}\right)^{1/n},$$

где $s_n = \pi^{n/2}/\Gamma(n/2+1)$.

ГЛАВА X

ТЕОРЕМА ДИРИХЛЕ О ПРОСТЫХ ЧИСЛАХ В АРИФМЕТИЧЕСКОЙ ПРОГРЕССИИ

§ 1. Введение. С помощью элементарных рассуждений мы показали, что простых чисел бесконечно много и что каждая арифметическая прогрессия вида $4k+1$ и $4k+3$, $k=1, 2, 3,...$, содержит бесконечно много простых чисел (гл. III, § 3). Мы докажем теперь теорему Дирихле о том, что существует бесконечно много простых чисел в любой арифметической прогрессии $a+mk$, где a и m — целые числа, $m>0$, $(a, m)=1$ и k пробегает все положительные целые числа.

Мы доказали в гл. VII, что ряд $\sum 1/p$, где p пробегает все простые числа, расходится. Можно изменить предложенное там доказательство и получить этот результат следующим образом. Для действительного $s>1$ справедливо тождество Эйлера

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

и для $0<x<1$ мы имеем

$$\log\left(\frac{1}{1-x}\right)=\sum_{n=1}^{\infty}\frac{x^n}{n}<\sum_{n=1}^{\infty}x^n=\frac{x}{1-x},$$

так что при $0<x\leqslant 1/2$

$$\log\left(\frac{1}{1-x}\right)<2x.$$

Тогда для любого простого p и действительного $s>1$ мы получаем неравенство

$$\log\left(1-\frac{1}{p^s}\right)^{-1}<\frac{2}{p^s}.$$

Следовательно, при $s>1$

$$\log \zeta(s)=\sum_p \log\left(1-\frac{1}{p^s}\right)^{-1}<2\sum_p \frac{1}{p^s}.$$

Если мы предположим, что ряд $\sum_p \frac{1}{p}$ сходится, то получим $2\sum_p \frac{1}{p^s}<2\sum_p \frac{1}{p}$. Мы знаем, однако, что $\zeta(1+\varepsilon)\to\infty$ при $\varepsilon\to+0$. Следовательно, ряд $\sum_p \frac{1}{p}$ должен расходиться.

В то время как расходимость ряда $\sum_p \frac{1}{p}$ связана с поведением $\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}$ $(s>1)$, расходимость ряда $\sum_{p\equiv a(\mathrm{mod}\ m)}\frac{1}{p}$, где a и m целые, $m>0$, $(a, m)=1$, связана с поведением *ряда Дирихле* вида $\sum_{n=1}^{\infty}\frac{a_n}{n^s}$, где s и *коэффициенты* a_n суть комплексные числа. Чтобы подготовиться к изучению этого вопроса, рассмотрим функцию $\zeta(s)$ комплексного переменного s.

Пусть $s=\sigma+it$, где σ и t — действительные величины и $i^2=-1$. Предположим сначала, что $\sigma>1$. Для действительного положительного x положим $x^s=e^{s\log x}$, где $\log x$ есть вещественный натуральный логарифм. Тогда мы имеем

$$\sum_{n=1}^{\infty}\frac{1}{|n^s|}=\sum_{n=1}^{\infty}\frac{1}{n^\sigma},$$

так что ряд $\sum_{n=1}^{\infty}\frac{1}{n^s}$ абсолютно сходится при $\sigma>1$ и равномерно сходится в любой полуплоскости $\sigma\geqslant 1+\delta>1$, где он определяет регулярную аналитическую функцию.

Из абсолютной сходимости ряда при $\sigma>1$ и из теоремы 5 гл. VII следует, что тождество

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_p\left(1-\frac{1}{p^s}\right)^{-1}$$

остается справедливым для комплексных s с действительной частью $\sigma>1$.

Из абсолютной сходимости ряда $\sum_p 1/p^s$ при $\sigma>1$ следует, что произведение $\prod_p (1-1/p^s)^{-1}$ при $\sigma>1$ также сходится абсолютно. Таким образом, в полуплоскости $\sigma>1$ функция $\zeta(s)$ может быть представлена абсолютно сходящимся произведением, все сомножители которого отличны от нуля. Следовательно, $\zeta(s)\neq 0$ при $\sigma>1$.

Функция $\zeta(s)$, определенная при $\sigma>1$ соотношением

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

является аналитической функцией в полуплоскости $\sigma>0$, за исключением точки $s=1$, где она имеет простой полюс с вычетом 1. Для того чтобы доказать это, воспользуемся формулой суммирования Абеля, доказанной в теореме 6 гл. VII, с $\lambda_n=n$, $\varphi(x)=x^{-s}$ и $a_n=1$. Тогда $A(x)=[x]$, целой части x, и

$$\sum_{n\leqslant x}\frac{1}{n^s}=\frac{[x]}{x^s}+s\int_1^x\frac{[u]}{u^{s+1}}\,du.$$

Мы имеем при $\sigma>1$, что $[x]/x^s\to 0$, когда $x\to\infty$, и что ряд $\sum_{n=1}^{\infty} 1/n^s$ сходится. Положим теперь $[u]=u-\{u\}$. Тогда мы получим представление

$$\sum_{n=1}^{\infty}\frac{1}{n^s}=s\int_1^{\infty}\frac{du}{u^s}-s\int_1^{\infty}\frac{\{u\}}{u^{s+1}}\,du=\frac{s}{s-1}-s\int_1^{\infty}\frac{\{u\}}{u^{s+1}}\,du,$$

или

$$\sum_{n=1}^{\infty}\frac{1}{n^s}=1+\frac{1}{s-1}-s\int_1^{\infty}\frac{\{u\}}{u^{s+1}}\,du\qquad(\sigma>1).\tag{1}$$

Очевидно, $0\leqslant\{u\}<1$ и, следовательно, интеграл в (1) сходится равномерно в каждой полуплоскости $\sigma\geqslant\delta>0$ и представляет собой регулярную функцию от s для $\sigma>0$. Следовательно, $\zeta(s)$ является мероморфной функ-

цией при $\sigma>0$ и имеет простой полюс в точке $s=1$ с вычетом 1. Функция $\zeta(s)$ называется *дзета-функцией Римана.*

§ 2. Характеры. *Характером* χ конечной абелевой группы G называется не равная тождественно нулю комплекснозначная функция, определенная на этой группе и обладающая тем свойством, что если $A\in G$ и $B\in G$, то

$$\chi(AB)=\chi(A)\chi(B).$$

Обозначим через E единичный элемент в группе G и через A^{-1} обратный элемент для $A\in G$. Характеры группы G обладают следующими свойствами:

(i) $\chi(A)\neq 0$ для каждого $A\in G$. Действительно, если бы $\chi(A)=0$ для некоторого $A\in G$, то $\chi(A)\chi(A^{-1})=\chi(AA^{-1})=\chi(E)=0$, а тогда $\chi(C)=\chi(E)\chi(C)=0$ для каждого $C\in G$, что противоречит определению характера χ. Заметим, кроме того, что $\chi(E)=1$.

(ii) Если G имеет порядок h, то $A^h=E$ для каждого $A\in G$. Следовательно, $\chi(A)^h=\chi(A^h)=\chi(E)=1$, т. е. $\chi(A)$ есть корень степени h из единицы. Характер χ_1, обладающий свойством $\chi_1(A)=1$ для *каждого* $A\in G$, называется *главным характером* группы G.

(iii) Абелева группа порядка h имеет точно h характеров.

Докажем сначала это свойство для *циклических групп.* Группа G называется циклической, если она состоит из степеней A, A^2,..., $A^r=E$ одного элемента A, который называется *образующим элементом* группы G. *Порядок* r группы G есть наименьшее положительное целое число r, такое, что $A^r=E$.

Пусть χ — характер циклической группы G. Тогда (a) χ полностью определяется величиной $\chi(A)$, так как $\chi(A^n)=(\chi(A))^n$, (b) из равенства $A^r=E$ следует, что $(\chi(A))^r=1$, т. е. $\chi(A)$ является корнем степени r из единицы; (c) если ρ — корень степени r из единицы, то мы можем определить характер χ соотношением $\chi(A)=\rho$ (т. е. $\chi(A^n)=\rho^n$), поскольку если $A^{a_1}\cdot A^{a_2}=A^{a_3}$, то $a_1+a_2\equiv a_3 \pmod r$, откуда $\rho^{a_1}\rho^{a_2}=\rho^{a_3}$. Так как существует

только r различных корней степени r из единицы, из условий (a) и (b) следует, что имеется *самое большее* r различных характеров группы G. С другой стороны, из (c) следует, что имеется по меньшей мере r таких характеров. Следовательно, циклическая группа порядка r имеет точно r характеров.

Для того чтобы доказать свойство (iii) для произвольной абелевой группы G, мы используем следующий результат: каждая конечная (мультипликативная) абелева группа G является прямым произведением циклических групп. Предположим, что $G=G_1\times\ldots\times G_k$, где G_j, $1\leqslant j\leqslant k$, — циклические группы. Обозначим через r_j порядок группы G_j и через A_j ее образующий элемент. Тогда для порядка h группы G имеет место равенство $h=r_1r_2\ldots r_k$ и каждый элемент $A\in G$ может быть единственным образом представлен в виде $A=A_1^{t_1}A_2^{t_2}\ldots A_k^{t_k}$, $0\leqslant t_j\leqslant r_j-1$, $j=1, 2,\ldots, k$. Если χ — характер группы G, то

$$\chi(A)=\chi(A_1)^{t_1}\chi(A_2)^{t_2}\ldots\chi(A_k)^{t_k}.$$

Пусть ρ_j — корень степени r_j из единицы. Тогда имеется один и только один характер χ группы G, такой, что $\chi(A_j)=\rho_j$, $j=1, 2,\ldots, k$, а так как ρ_j принимает в точности r_j различных значений, то G имеет точно h различных характеров, где $h=r_1r_2\ldots r_k$.

(iv) Пусть G — конечная мультипликативная абелева группа порядка h. Из свойства (i) следует, что $\chi(E)=1$ для каждого характера χ группы G. Покажем теперь, что для любого заданного $A\in G$, $A\neq E$, существует характер χ, такой, что $\chi(A)\neq 1$.

Мы снова воспользуемся представлением G в виде прямого произведения циклических групп. Как и в (iii), пусть $A=A_1^{t_1}A_2^{t_2}\ldots A_k^{t_k}$. Ввиду того что $A\neq E$, не все t_i равны нулю. Пусть, например, $t_1\neq 0$. Возьмем $\chi(A_2)=\chi(A_3)=\ldots=\chi(A_k)=1$ и $\chi(A_1)=\rho$, где $\rho=e^{(2\pi i)/r_1}$, $i^2=-1$. Тогда $\chi(A)=\rho^{t_1}\neq 1$ при $0<t_1<r_1$.

(v) Характеры конечной мультипликативной абелевой группы G образуют конечную мультипликативную

абелеву группу $\hat{G}$. Под «произведением» двух характеров χ' и χ'' группы G мы будем понимать характер χ, определяемый следующим свойством: $\chi(A)=\chi'(A)\chi''(A)$ для каждого элемента $A\in G$. Мы имеем

$$\chi(AB)=\chi'(AB)\chi''(AB)=\chi'(A)\chi'(B)\chi''(A)\chi''(B)=$$
$$=\chi(A)\chi(B),$$

так что $\chi'\chi''$ действительно является характером.

Главный характер χ_1 группы G является единичным элементом $\hat{G}$. Характер χ^{-1}, обратный к характеру χ, определяется соотношением $\chi^{-1}(A)=\chi(A^{-1})$, так что $\chi^{-1}(A)=(\chi(A))^{-1}$. Так как $\chi^{-1}(AB)=\chi((AB)^{-1})=$ $=\chi(A^{-1})\chi(B^{-1})=\chi^{-1}(A)\chi^{-1}(B)$, то χ^{-1} действительно будет характером.

Характер χ, рассмотренный в (iv), порождает циклическую подгруппу группы $\hat{G}$ порядка r_1. Аналогичным образом можно доказать существование в группе $\hat{G}$ подгрупп порядков $r_2,\ldots, r_k$. Рассуждения, подобные тем, которые были использованы при доказательстве существования точно h различных характеров группы G, где h — ее порядок, показывают, что $\hat{G}$ является прямым произведением этих циклических подгрупп порядков $r_1, r_2,\ldots, r_k$. Следовательно, группы G и $\hat{G}$ изоморфны. Этот изоморфизм зависит от разложения G в произведение циклических сомножителей (вообще говоря, это разложение не единственно) и от выбора образующих элементов этих сомножителей.

§ 3. Суммы характеров. Соотношения ортогональности. Пусть G — конечная мультипликативная абелева группа порядка h. Рассмотрим сумму

$$S=\sum_A \chi(A),$$

где A пробегает все элементы G, и сумму

$$T=\sum_\chi \chi(A),$$

где χ пробегает все элементы группы характеров $\hat{G}$.

Если B — фиксированный элемент группы G и A пробегает все элементы G, то AB также пробегает все элементы группы G. Следовательно,

$$S\cdot\chi(B)=\sum_A\chi(AB)=\sum_A\chi(A)=S,$$

откуда следует, что $(\chi(B)-1)S=0$. Следовательно, или $S=0$, или $S\neq 0$ и $\chi(B)=1$ для каждого элемента $B\in G$. Во втором случае $\chi=\chi_1$ есть главный характер и сумма S равна порядку h группы G. Таким образом,

$$S=\sum_A\chi(A)=\begin{cases}h, & \text{если } \chi=\chi_1,\\ 0, & \text{если } \chi\neq\chi_1.\end{cases}\tag{2}$$

Если мы умножим сумму T на некоторый характер χ' группы G, то аналогичным образом получим

$$\chi'(A)\cdot T=\sum_\chi\chi(A)\chi'(A)=\sum_\chi\chi(A)=T.$$

Следовательно, или $T=0$, или $\chi'(A)=1$ для каждого характера $\chi'\in\hat{G}$. Во втором случае, согласно свойству (iv) из § 2, мы имеем $A=E$, и тогда $T=h$. Таким образом,

$$T=\sum_\chi\chi(A)=\begin{cases}h, & \text{если } A=E,\\ 0, & \text{если } A\neq E.\end{cases}\tag{3}$$

Пусть m — положительное целое число. Мы знаем, что $\varphi(m)$ приведенных классов вычетов по модулю m образуют мультипликативную абелеву группу порядка $h=\varphi(m)$ (гл. II, § 1). Мы можем, следовательно, рассмотреть характеры этой группы. Но определение характера для приведенных классов вычетов по модулю m можно перенести на множество целых чисел следующим образом. Положим

$$\chi(a)=\chi(A),\quad \text{если}\quad a\in A,$$

где A — приведенный класс вычетов по модулю m. Тогда, очевидно, $\chi(a)=\chi(b)$, если $a\equiv b\pmod m$, и $\chi(ab)=\chi(a)\chi(b)$, если $(a, m)=(b, m)=1$. Поскольку $\chi(A)\neq 0$ для каждого приведенного класса вычетов A, то $\chi(a)\neq 0$, если $(a, m)=1$.

Это определение применимо только к целым числам a, которые взаимно просты с m. Мы можем распространить его на *все* целые числа, положив

$$\chi(a)=0, \quad \text{если} \quad (a, m)>1.$$

Следовательно, *характер по модулю* m есть арифметическая функция χ, обладающая следующими свойствами:

$$\chi(a)=\chi(b), \text{ если } a\equiv b \pmod m,$$
$$\chi(ab)=\chi(a)\chi(b) \text{ для всех целых } a \text{ и } b,$$
$$\chi(a) = 0, \text{ если } (a, m) > 1,$$
$$\chi(a)\neq 0, \text{ если } (a, m)=1.$$

Имеется точно $\varphi(m)$ характеров по модулю m, где $\varphi(m)$ — количество положительных целых чисел, не превосходящих m и взаимно простых с m. Они образуют (мультипликативную) абелеву группу, изоморфную группе приведенных классов вычетов по mod m. Единичным элементом этой группы будет *главный характер* χ_1, т. е. такой характер, что $\chi_1(a)=1$, если $(a, m)=1$. Далее, мы имеем следующие *соотношения ортогональности:*

$$\sum_{n \pmod m} \chi(n) = \begin{cases} \varphi(m), & \text{если } \chi=\chi_1, \\ 0, & \text{если } \chi\neq\chi_1, \end{cases} \tag{4}$$

$$\sum_{\chi} \chi(n) = \begin{cases} \varphi(m), & \text{если } n\equiv 1 \pmod m, \\ 0, & \text{если } n\not\equiv 1 \pmod m. \end{cases} \tag{5}$$

Примеры. (1) Пусть $m=4$. Тогда имеются два приведенных класса вычетов, а именно класс E, состоящий из целых чисел, сравнимых с $1 \pmod 4$, и класс A, состоящий из целых чисел, сравнимых с $3 \pmod 4$. Классы A и E образуют циклическую группу порядка 2. Существуют два характера χ_1 и χ_2, где

$$\chi_1(E)=\chi_1(A)=1, \quad \text{главный характер},$$
$$\chi_2(E)=1, \quad \chi_2(A)=-1.$$

По определению характера, перенесенному на все целые числа, мы имеем

$$\chi_1(n)=\begin{cases}0, & \text{если } n \text{ четное},\\ 1, & \text{если } n \text{ нечетное},\end{cases}$$

и

$$\chi_2(n)=\begin{cases}0, & \text{если } n \text{ четное},\\ 1, & \text{если } n\equiv 1 \pmod 4,\\ -1, & \text{если } n\equiv 3 \pmod 4).\end{cases}$$

Далее,

$$\chi_1(1)+\chi_1(3)=2, \qquad \chi_2(1)+\chi_2(3)=0,$$
$$\chi_1(1)+\chi_2(1)=2, \qquad \chi_1(3)+\chi_2(3)=0.$$

(II) Пусть $m=5$. Тогда приведенные классы вычетов суть E, A, A^2, A^3, где A — класс всех целых чисел, сравнимых с $2 \pmod 5$. Класс A^2 представляет собой класс целых чисел, сравнимых с $4 \pmod 5$, и A^3 — класс целых чисел, сравнимых с $3 \pmod 5$. Класс E состоит из целых чисел, сравнимых с $1 \pmod 5$. Четыре характера определяются теперь следующим образом:

$$\chi_1(E)=\chi_1(A)=\chi_1(A^2)=\chi_1(A^3)=1,$$
$$\chi_2(E)=1, \quad \chi_2(A)=i, \quad \chi_2(A^2)=-1, \quad \chi_2(A^3)=-i,$$
$$\chi_3(E)=1, \quad \chi_3(A)=-1, \quad \chi_3(A^2)=1, \quad \chi_3(A^3)=-1,$$
$$\chi_4(E)=1, \quad \chi_4(A)=-i, \quad \chi_4(A^2)=-1, \quad \chi_4(A^3)=i.$$

§ 4. Ряды Дирихле. Теорема Ландау. Рядом Дирихле называется ряд вида $\sum\limits_{n=1}^{\infty} a_n n^{-s}$, где s — комплексное число и *коэффициенты* a_n — также комплексные числа. Рядом Дирихле называется также ряд более общего вида

$$\sum_{n=1}^{\infty}\frac{a_n}{\lambda_n^s}, \quad \text{или} \quad \sum_{n=1}^{\infty} a_n e^{-s\lambda_n},$$

где $0<\lambda_1<\lambda_2<\ldots$ и $\lambda_n\to\infty$ при $n\to\infty$.

Многие ряды Дирихле, встречающиеся в теории чисел, имеют вид $\sum a_n n^{-s}$, и мы рассмотрим некоторые элементарные свойства таких рядов.

Обычно мы будем писать $s=\sigma+it$, где σ и t действительны и $i^2=-1$.

Теорема 1. *Если ряд* $\sum\limits_{n=1}^{\infty} a_n/n^s$ *сходится при* $s=s_0$, *то он равномерно сходится в области* $|\arg(s-s_0)|\leqslant \leqslant \pi/2-\theta<\pi/2$.

Доказательство. Ввиду того что

$$\sum_{n=1}^{\infty}\frac{a_n}{n^s}=\sum_{n=1}^{\infty}\frac{a_n}{n^{s_0}}\cdot\frac{1}{n^{s-s_0}}=\sum_{n=1}^{\infty}\frac{b_n}{n^{s-s_0}}$$

и сходимость ряда $\sum\limits_{n=1}^{\infty} a_n n^{-s}$ при $s=s_0$ эквивалентна сходимости ряда $\sum\limits_{n=1}^{\infty} b_n$, где $b_n=a_n n^{-s_0}$, мы можем предположить, не уменьшая общности, что $s_0=0$.

Пусть ряд $\sum\limits_{n=1}^{\infty} a_n$ сходится. Тогда $\lim\limits_{n\to\infty} r_n=0$, где $r_n=$ $=\sum\limits_{\nu=n+1}^{\infty} a_\nu$. Пусть, далее, M и N — положительные целые числа и $M<N$. Тогда

$$\sum_{n=M}^{N}\frac{a_n}{n^s}=\sum_{n=M}^{N}\frac{r_{n-1}-r_n}{n^s}=\sum_{n=M}^{N}\left(\frac{r_n}{(n+1)^s}-\frac{r_n}{n^s}\right)+$$

$$+\frac{r_{M-1}}{M^s}-\frac{r_N}{(N+1)^s}.$$

При $\sigma>0$ мы имеем

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

$$=\frac{|s|}{\sigma}\left(\frac{1}{n^\sigma}-\frac{1}{(n+1)^\sigma}\right)$$

Для заданного $\varepsilon>0$ мы имеем $|r_n|<\varepsilon$ при $n\geqslant n_0(\varepsilon)$, где n_0 не зависит от s. Следовательно, при $M>n_0$

$$\left|\sum_{n=M}^{N}\frac{a_n}{n^s}\right|\leqslant\frac{\varepsilon|s|}{\sigma}\left(\frac{1}{M^\sigma}-\frac{1}{(N+1)^\sigma}\right)+\frac{\varepsilon}{M^\sigma}+\frac{\varepsilon}{(N+1)^\sigma}.$$

Если $\sigma>0$ и $M>n_0(\varepsilon)$, мы получаем оценку

$$\left|\sum_{n=M}^{N}\frac{a_n}{n^s}\right|\leqslant\frac{\varepsilon|s|}{\sigma}\cdot\frac{1}{M^\sigma}+\frac{\varepsilon}{M^\sigma}\leqslant\frac{2\varepsilon|s|}{\sigma}.$$

Чтобы доказать равномерную сходимость, заметим, что

$$\frac{|s|}{\sigma}=\frac{1}{\cos|\arg s|}\leqslant\frac{1}{\cos(\pi/2-\theta)}=\frac{1}{\sin\theta},$$

т. е. для каждого s, удовлетворяющего условию $|\arg s|\leqslant\leqslant\pi/2-\theta<\pi/2$, мы имеем

$$\left|\sum_{n=M}^{N}\frac{a_n}{n^s}\right|<2\varepsilon\,(\operatorname{cosec}\theta),\quad N>M>n_0(\varepsilon);$$

теорема 1 доказана.

Отсюда следует, что если ряд $\sum\limits_{n=1}^{\infty}\frac{a_n}{n^s}$ сходится при $s_0=\sigma_0+it_0$, то он будет сходиться при всех $s=\sigma+it$ с $\sigma>\sigma_0$.

Таким образом, справедлива

Теорема 2. *Если ряд* $\sum\limits_{n=1}^{\infty}\frac{a_n}{n^s}$ *сходится при* $s=s_0$, *то он сходится в полуплоскости* $\sigma>\sigma_0$ *и равномерно сходится в каждом компактном множестве, содержащемся в этой полуплоскости.*

Из равномерной сходимости следует также

Теорема 3. *Пусть ряд* $\sum\limits_{n=1}^{\infty}\frac{a_n}{n^s}$ *сходится при* $s=s_0$ *и* $\sum\limits_{n=1}^{\infty}\frac{a_n}{n^{s_0}}=f(s_0)$. *Пусть, далее,* $f(s)=\sum\limits_{n=1}^{\infty}\frac{a_n}{n^s}$ *в полуплоскос-*

ти $\sigma > \sigma_0$. *Тогда* $f(s) \to f(s_0)$ *при* $s \to s_0$ *вдоль любого пути, лежащего в области* $|\arg(s-s_0)| \leqslant \pi/2 - \theta < \pi/2$.

Теорема 2 показывает, что область сходимости ряда Дирихле представляет собой полуплоскость. Действительно, если точки действительной оси разделить на два класса U и L, такие, что

$$U = \left\{\sigma \sum_{n=1}^{\infty} \frac{a_n}{n^s} \text{ сходится}\right\},$$

$$L = \left\{\sigma \sum_{n=1}^{\infty} \frac{a_n}{n^s} \text{ расходится}\right\},$$

то каждое число класса U будет больше любого числа класса L и такое разбиение на классы определяет действительное число σ_0, такое, что ряд сходится при $\sigma > \sigma_0$ и расходится при $\sigma < \sigma_0$. В случае $\sigma = \sigma_0$ вопрос о сходимости остается открытым. Если класс U пуст, то положим $\sigma_0 = +\infty$, если же L пуст, то положим $\sigma_0 = -\infty$.

Число σ_0 называется *абсциссой сходимости*, прямая $\sigma = \sigma_0$ — *прямой сходимости*, а полуплоскость $\sigma > \sigma_0$ — *полуплоскостью сходимости* ряда Дирихле $\sum_{n=1}^{\infty} a_n/n^s$.

Ряд $\sum_{n=1}^{\infty} n!/n^s$ всюду расходится ($\sigma_0 = +\infty$), в то время как ряд $\sum_{n=1}^{\infty} 1/(n!n^s)$ всюду сходится ($\sigma_0 = -\infty$).

Теорема 1 вместе с теоремой Вейерштрасса о равномерно сходящихся последовательностях аналитических функций дает нам следующий результат:

Теорема 4. *Ряд Дирихле* $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *в полуплоскости его сходимости представляет собой регулярную аналитическую функцию от* s, *последовательные производные которой получаются почленным дифференцированием этого ряда.*

В этих теоремах ничего не говорится о сходимости или регулярности суммы ряда *на* прямой сходимости.

В отличие от степенных рядов, которые всегда имеют на границе круга сходимости особенность, ряды Дирихле не обязательно имеют особенность на прямой сходимости. Точно так же из сходимости или расходимости ряда Дирихле в фиксированной точке на прямой сходимости мы не можем делать выводы о регулярности или нерегулярности суммы этого ряда в указанной точке. Мы вернемся к этому вопросу несколько позже.

Абсолютная сходимость. Ряд $\sum_{n=1}^{\infty} a_n/n^s$ сходится абсолютно, если сходится ряд $\sum_{n=1}^{\infty} |a_n|/n^\sigma$. *Абсциссой абсолютной сходимости* $\bar{\sigma}$ ряда $\sum_{n=1}^{\infty} a_n/n^s$ называется абсцисса сходимости ряда $\sum_{n=1}^{\infty} |a_n|/n^s$.

Очевидно, $\bar{\sigma} \geqslant \sigma_0$, так как абсолютная сходимость влечет за собой сходимость ряда. Если $\bar{\sigma} > \sigma_0$, то существует полоса в комплексной s-плоскости, в которой ряд сходится, но не абсолютно. Эта полоса $\sigma_0 < \sigma < \bar{\sigma}$ называется *полосой условной сходимости.*

Рассмотрим для примера ряд

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

сходящийся при действительных $s > 0$, поскольку это знакопеременный ряд с убывающими членами. Он, очевидно, расходится при действительных $s < 0$ и, следовательно, $\sigma_0 = 0$. Далее, этот ряд абсолютно сходится при $\sigma > 1$ и абсолютно расходится при $\sigma < 1$. Следовательно, $\bar{\sigma} = 1$, и полоса условной сходимости имеет ширину 1.

Интересно отметить, что при $\sigma > 0$ имеет место равенство

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s} = \left(1 - 2^{1-s}\right) \zeta(s), \tag{6}$$

где $\zeta(s)$ есть дзета-функция Римана. В самом деле, ряд в левой части (6) абсолютно сходится при $\sigma>1$, и после соответствующей перестановки его членов мы получаем при $\sigma>1$

$$\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n^s}=\left(\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\cdots\right)-$$

$$-2\left(\frac{1}{2^s}+\frac{1}{4^s}+\frac{1}{6^s}+\cdots\right)=\left(1-2^{1-s}\right)\zeta(s).$$

Но ряд $\sum(-1)^{n-1}/n^s$ сходится при $\sigma>0$ и функция $\zeta(s)\,(1-2^{1-s})$ регулярна при $\sigma>0$, так как простой полюс $\zeta(s)$ при $s=1$ уничтожится нулем функции $1-2^{1-s}$. Следовательно, по аналитическому продолжению мы получаем, что равенство (6) остается справедливым при $\sigma>0$.

Мы показали, что полоса условной сходимости ряда (6) имеет ширину 1. Можно доказать, что ширина полосы условной сходимости любого ряда Дирихле $\sum a_n/n^s$ не может быть больше 1, так что если ряд Дирихле сходится для данного s_0, то он будет абсолютно сходиться при всех s, у которых действительная часть будет больше действительной части s_0 на величину $1+\varepsilon$ при любом $\varepsilon>0$.

Теорема 5. *Для любого ряда Дирихле* $\sum_{n=1}^{\infty}a_n/n^s$ *мы имеем* $\bar{\sigma}-\sigma_0\leqslant 1$.

Доказательство. Если ряд $\sum_{n=1}^{\infty}a_n/n^s$ сходится, то $\lim_{n\to\infty}|a_n|/n^{\sigma}=0$ и, следовательно, ряд $\sum_{n=1}^{\infty}|a_n|/n^{1+\sigma+\varepsilon}$ сходится для любого $\varepsilon>0$.

Как показывают следующие примеры, эта теорема не выполняется для рядов Дирихле более общего вида $\sum a_n\lambda_n^{-s}$, где (λ_n) не является множеством положитель-

ных целых чисел. В самом деле, ряд

$$\sum_{n=2}^{\infty} \frac{(-1)^n}{(\log n)^s}$$

сходится при $\sigma>0$, но нигде не сходится абсолютно; ряд

$$\sum_{n=2}^{\infty} \frac{(-1)^n}{\sqrt{n}\,(\log n)^s}$$

сходится при всех s, но нигде не сходится абсолютно.

Вернемся теперь к вопросу о регулярности суммы ряда Дирихле $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ на прямой сходимости. В случае когда коэффициенты (a_n) неотрицательны, имеет место

Теорема 6 (Ландау). *Если $a_n \geqslant 0$ для всех $n \geqslant 1$ и σ_0 конечно, то точка пересечения действительной оси с прямой сходимости является особой точкой суммы $f(s)$ ряда Дирихле $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$.*

Доказательство. Так как $a_n \geqslant 0$, то $\bar{\sigma}=\sigma_0$. Без ограничения общности мы можем считать, что $\sigma_0=0$. Нам нужно показать, что точка $s=0$ является особой точкой функции f. Если бы f была регулярна при $s=0$, то ряд Тейлора функции f в точке $s=1$ имел бы радиус сходимости $\rho>1$. Следовательно, должно существовать действительное $s<0$, для которого ряд

$$\sum_{\nu=0}^{\infty} \frac{(s-1)^\nu}{\nu!} f^{(\nu)}(1)$$

сходится. Но при $\sigma>0$

$$f(s) = \sum_{n=1}^{\infty} a_n e^{-s \log n}$$

и по теореме 4

$$f^{(\nu)}(s) = \sum_{n=1}^{\infty} a_n \frac{(-\log n)^\nu}{n^s},$$

так что

$$f^{(\nu)}(1) = \sum_{n=1}^{\infty} a_n \frac{(-\log n)^\nu}{n}.$$

Ряд Тейлора функции f в точке $s=1$ имеет поэтому вид

$$\sum_{\nu=0}^{\infty} \frac{(s-1)^\nu}{\nu!} \sum_{n=1}^{\infty} \frac{a_n(-\log n)^\nu}{n} = \sum_{\nu=0}^{\infty} \frac{(1-s)^\nu}{\nu!} \sum_{n=1}^{\infty} \frac{a_n(\log n)^\nu}{n}.$$

Поскольку все члены этого двойного ряда неотрицательны при $s<0$, можно изменить порядок суммирования. Тогда мы получим, что ряд

$$\sum_{n=1}^{\infty} \frac{a_n}{n} \sum_{\nu=0}^{\infty} \frac{(1-s)^\nu (\log n)^\nu}{\nu!}$$

сходится для некоторого $s<0$. Однако

$$\sum_{\nu=0}^{\infty} \frac{(1-s)^\nu (\log n)^\nu}{\nu!} = e^{(1-s)\log n}.$$

Следовательно, ряд $\sum_{n=1}^{\infty} a_n n^{-s}$ сходится для некоторого $s<0$, что невозможно, так как $\sigma_0=0$. Таким образом, точка $s=0$ должна быть особой точкой функции $f(s)$.

Умножение рядов Дирихле. *Формальным произведением* двух рядов Дирихле $\sum_{k=1}^{\infty} a_k/k^s$ и $\sum_{m=1}^{\infty} b_m/m^s$ называется ряд $\sum_{n=1}^{\infty} c_n/n^s$, где $c_n = \sum_{km=n} a_k b_m$. Если оба эти ряда сходятся абсолютно для некоторого данного s, то ряд $\sum_{n=1}^{\infty} c_n/n^s$ также абсолютно сходится и называется в этом случае *произведением* данных рядов.

Пусть $\sigma > \sigma_0$ и

$$f(s) = \sum_{k=1}^{\infty} \frac{a_k}{k^s}, \quad g(s) = \sum_{m=1}^{\infty} \frac{b_m}{m^s}.$$

Тогда по теореме 5 функция $h(s)$, где $h(s)=f(s)\cdot g(s)$, представляется в полуплоскости $\sigma>\sigma_0+1$ произведением рядов Дирихле функций $f(s)$ и $g(s)$.

Представление функции рядом Дирихле единственно, как показывает следующая

Теорема 7. *Если ряды* $\sum\limits_{n=1}^{\infty}\frac{a_n}{n^s}$ *и* $\sum\limits_{n=1}^{\infty}\frac{b_n}{n^s}$ *сходятся в общей полуплоскости и их суммы совпадают в непустом открытом множестве, содержащемся в этой полуплоскости, то* $a_n=b_n$ *при всех* $n\geqslant 1$.

Доказательство. Рассмотрим ряд Дирихле

$$\sum_{n=1}^{\infty}\frac{a_n-b_n}{n^s}.$$

Он сходится в некоторой полуплоскости $\sigma>\sigma_0$, где определяет регулярную аналитическую функцию. Эта функция тождественно равна нулю в некотором непустом открытом множестве, содержащемся в этой полуплоскости, и, следовательно, тождественно равна нулю во всей этой полуплоскости $\sigma>\sigma_0$.

Пусть M будет первым значением индекса n, при котором $a_n\neq b_n$, и пусть $c_n=a_n-b_n$. Тогда при $\sigma>\sigma_0$ мы имеем

$$\sum_{n=1}^{\infty}\frac{c_n}{n^\sigma}=\sum_{n=M}^{\infty}\frac{c_n}{n^\sigma}=0,$$

или

$$\frac{c_M}{M^\sigma}=-\sum_{n=M+1}^{\infty}\frac{c_n}{n^\sigma}.$$

Следовательно, при $\sigma>\sigma_0+1$

$$|c_M|\leqslant\sum_{n=M+1}^{\infty}|c_n|\cdot\left(\frac{M}{n}\right)^\sigma.$$

Пусть теперь $\sigma\to\infty$. Тогда из равномерной сходимости последнего ряда при $\sigma>\sigma_0+2$ следует, что $c_M=0$. Но это

противоречит определению M. Следовательно, $c_n=0$ для всех $n\geqslant 1$.

§ 5. Теорема Дирихле. Применим теперь результаты, полученные нами в § 3 о характерах и в § 4 о рядах Дирихле, к рядам вида

$$\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s},\quad s=\sigma+it, \tag{7}$$

где χ — характер по модулю m.

Имеется $\varphi(m)$ таких рядов, где φ — функция Эйлера. Так как $|\chi(n)|\leqslant 1$, ряд (7) сходится при $\sigma>1$, что видно из сравнения этого ряда с рядом $\sum 1/n^s$. Обозначим его сумму через $L(s,\chi)$. Для различных характеров χ мы получаем разные функции $L(s,\chi)$. Они называются *L-функциями Дирихле*. При изучении свойств этих функций удобно различать случаи, когда χ — главный характер χ_1 и когда $\chi\neq\chi_1$.

(i) Если $\chi\neq\chi_1$, то ряд (7) сходится в полуплоскости $\sigma>0$. Покажем сначала, что частичные суммы $\sum\limits_{n\leqslant x}\chi(n)$ ограничены.

Разобьем целые числа от 1 до $[x]$ на классы вычетов по $\bmod m$ и запишем $[x]=mq+r$, $0\leqslant r\leqslant m-1$. Тогда

$$\sum_{n\leqslant x}\chi(n)=\sum_{n=1}^{[x]}\chi(n)=\Big(\sum_{1}^{m}+\sum_{m+1}^{2m}+\ldots+\sum_{m(q-1)+1}^{mq}\Big)\chi(n)+\sum_{mq+1}^{mq+r}\chi(n).$$

В силу соотношения ортогональности (4) мы имеем

$$\sum_{n\leqslant x}\chi(n)=\sum_{mq+1}^{mq+r}\chi(n),$$

откуда

$$\Big|\sum_{n\leqslant x}\chi(n)\Big|\leqslant\sum_{mq+1}^{mq+r}|\chi(n)|\leqslant r<m.$$

Так как $n^{-\sigma}$ при $\sigma>0$ монотонно убывает и стремится к нулю при $n\to\infty$, то ряд $\sum\chi(n)/n^s$ сходится для дейст-

вительных $s=\sigma>0$, а следовательно, и для всех s в полуплоскости $\sigma>0$, если $\chi\neq\chi_1$. Если же $\sigma<0$, то этот ряд, очевидно, расходится. Его абсцисса сходимости $\sigma_0=0$, а абсцисса абсолютной сходимости $\overline{\sigma}=1$. По теореме 4 функция $L(s, \chi)$, $\chi\neq\chi_1$, является регулярной аналитической функцией от s при $\sigma>0$.

(ii) Если $\chi=\chi_1$, мы воспользуемся снова тождеством Эйлера

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

где p пробегает все простые числа. Поскольку каждый характер χ является вполне мультипликативной арифметической функцией, то по теореме 5 гл. VII мы имеем для всех χ тождество

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}=\prod_p\left(1-\frac{\chi(p)}{p^s}\right)^{-1},\quad \sigma>1. \tag{8}$$

Отсюда следует, что $L(s,\chi)\neq 0$ при $\sigma>1$.

Если χ_1 — главный характер по $\bmod m$, то

$$\chi_1(a)=\begin{cases}1, & \text{если } (a,m)=1,\\ 0, & \text{если } (a,m)>1.\end{cases}$$

Используя (8), получаем

$$L(s,\chi_1)=\prod_{p\nmid m}(1-p^{-s})^{-1}=\prod_p(1-p^{-s})^{-1}\prod_{p\mid m}(1-p^{-s}),$$

или

$$L(s,\chi_1)=\zeta(s)\prod_{p\mid m}(1-p^{-s})\quad(\sigma>1). \tag{9}$$

Мы видели, что $\zeta(s)$ — мероморфная функция в полуплоскости $\sigma>0$, имеющая в качестве единственной особенности простой полюс при $s=1$ с вычетом 1. Следовательно, $L(s,\chi_1)$ является регулярной функцией при $\sigma>0$, за исключением точки $s=1$, где она имеет простой полюс с вычетом $\prod_{p\mid m}(1-p^{-1})=\frac{\varphi(m)}{m}$ [см. гл. II, (1)].

Для доказательства теоремы Дирихле нам потребуется

Лемма. *Если* $\chi \neq \chi_1$, *то* $L(1, \chi) \neq 0$.

Доказательство. Достаточно показать, что произведение

$$P(s) = \prod_{\chi} L(s, \chi),$$

где χ пробегает все характеры по $\bmod p$, *не* является регулярной функцией при $\sigma > 0$. Действительно, если $L(1, \chi) = 0$ по меньшей мере для одного характера $\chi \neq \chi_1$, то простой полюс функции $L(s, \chi_1)$ при $s = 1$ в произведении $P(s)$ уничтожится нулем функции $L(s, \chi)$ при $s = 1$ и $P(s)$ в таком случае будет регулярной функцией при $\sigma > 0$.

Для $\sigma > 1$ мы имеем $|\chi(p) p^{-s}| \leqslant p^{-\sigma} < 1$ и можем *определить*

$$\log\left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \sum_k \frac{\chi(p^k)}{k p^{ks}}.$$

Тогда функция $\log L(s, \chi)$ однозначно определяется в полуплоскости $\sigma > 1$ равенством

$$\log L(s, \chi) = \sum_{p,k} \frac{\chi(p^k)}{k p^{ks}}, \tag{10}$$

где p пробегает все простые числа, а k — все положительные целые числа. Этот двойной ряд абсолютно сходится при $\sigma > 1$. Далее, мы имеем

$$e^{\log L(s,\chi)} = L(s, \chi).$$

Просуммируем теперь $\log L(s, \chi)$ по всем характерам $\chi(\bmod m)$. Тогда мы получим

$$Q(s) = \log P(s) = \sum_{\chi} \log L(s, \chi) = \sum_{\chi} \sum_{p,k} \frac{\chi(p^k)}{k p^{ks}}.$$

Так как имеется только конечное число характеров χ, мы можем изменить порядок суммирования и получить

$$Q(s) = \sum_{p,k} \frac{1}{k p^{ks}} \sum_{\chi} \chi(p^k).$$

Поскольку

$$\sum_{\chi} \chi(a) = \begin{cases} \varphi(m), & \text{если } a \equiv 1 \pmod m, \\ 0, & \text{если } a \not\equiv 1 \pmod m, \end{cases}$$

мы имеем

$$Q(s) = \varphi(m) \sum_{p^k \equiv 1 \pmod m} \frac{1}{kp^{ks}}. \tag{11}$$

Если мы положим

$$a_n = \begin{cases} \dfrac{\varphi(m)}{k}, & \text{если } n = p^k \equiv 1 \pmod m, \\ 0 & \text{в противном случае,} \end{cases}$$

то

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

где коэффициенты (a_n) неотрицательны. Мы знаем, что этот ряд сходится при $\sigma > 1$. Для того чтобы найти его абсциссу сходимости, рассмотрим простые p, такие, что $p \nmid m$. По теореме Эйлера (теорема 2 гл. II) мы имеем $p^h \equiv 1 \pmod m$, где $h = \varphi(m)$. Если мы рассмотрим ряд (11) для действительных s и возьмем только члены с $k = h$, то получим

$$Q(s) > \sum_{p \nmid m} \frac{1}{p^{hs}} = \sum_{p|m} \frac{1}{p^{hs}} - \sum_{p|m} \frac{1}{p^{hs}}.$$

Поскольку ряд $\sum \frac{1}{p}$ расходится и сумма $\sum_{p|m} \frac{1}{p}$ конечна, отсюда следует, что ряд (11) расходится при $s = 1/h$. Следовательно, если α — абсцисса сходимости ряда Дирихле $Q(s)$, то $\alpha \geqslant 1/h$. Далее, мы имеем

$$P(s) = e^{Q(s)} = 1 + Q(s) + \frac{Q^2(s)}{2!} + \ldots. \tag{12}$$

Произведение двух сходящихся рядов Дирихле с неотрицательными коэффициентами будет снова рядом Дирихле с неотрицательными коэффициентами, который сходится в пересечении двух полуплоскостей сходимости исходных рядов. Следовательно, одновременно с $Q(s)$ все

степени $Q^n(s)$ сходятся абсолютно, так что ряд (12) для $P(s)$ может быть записан в виде ряда Дирихле с неотрицательными коэффициентами.

Таким образом, если ряд Дирихле функции $Q(s)$ сходится, то ряд Дирихле функции $P(s)$ также сходится. Обратно, поскольку эти ряды имеют неотрицательные коэффициенты, из сходимости ряда Дирихле функции $P(s)$ для некоторого действительного s следует сходимость ряда Дирихле функции $Q(s)$ для того же s.

Следовательно, ряд Дирихле функции $P(s)$ однозначно определен и имеет ту же самую абсциссу сходимости $\sigma_0=\alpha$, что и ряд Дирихле функции $Q(s)$. По теореме 6 точка $s=\alpha$ является особой точкой для $P(s)$, и мы знаем, что $\alpha\geqslant 1/h>0$. Значит, функция $P(s)$ *не* будет регулярной во всей полуплоскости $\sigma>0$. Лемма доказана.

Теперь мы можем доказать основную теорему этой главы:

Теорема 8 (Дирихле). *Если m — положительное целое число и $(a, m)=1$, то существует бесконечно много простых $p\equiv a \pmod m$.*

Доказательство. Достаточно доказать, что ряд $\sum 1/p$, где p пробегает все простые числа, сравнимые с $a \pmod m$, расходится. Для доказательства этого утверждения мы воспользуемся функцией $L(s, \chi)$.

При $\sigma>1$ мы имеем, согласно (10),

$$\log L(s, \chi)=\sum_p \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}}.$$

Выделим члены с $k=1$. Тогда мы получим

$$\log L(s, \chi)=\sum_p \chi(p)\, p^{-s}+R(s, \chi), \tag{13}$$

где ряд

$$R(s, \chi)=\sum_p \sum_{k=2}^{\infty} \frac{\chi(p^k)}{kp^{ks}}$$

сходится при $\sigma>1/2$.

Поскольку $(a, m)=1$, найдется целое число b, такое, что $ab\equiv 1 \pmod m$. Умножим обе части равенства (13) на $\chi(b)$ и просуммируем его по всем характерам $\chi \pmod m$. Тогда мы получим при $\sigma>1$

$$\sum_\chi \chi(b) \log L(s, \chi) = \sum_p \sum_\chi \chi(bp)\, p^{-s} + \sum_\chi \chi(b)\, R(s, \chi).$$

Так как функция $R(s,\chi)$ регулярна при $\sigma>1/2$, функция $R^*(s)=\sum\limits_\chi \chi(b) R(s,\chi)$ также будет регулярна при $\sigma>1/2$. Далее,

$$\sum_\chi \chi(bp) = \begin{cases} h, & \text{если } bp\equiv 1 \pmod m, \\ 0, & \text{если } bp \not\equiv 1 \pmod m. \end{cases}$$

Если $ab\equiv 1 \pmod m$, то сравнение $bp\equiv 1 \pmod m$ эквивалентно сравнению $p\equiv a \pmod m$. Поэтому

$$\sum_\chi \chi(b) \log L(s, \chi) = h \sum_{p\equiv a \pmod m} p^{-s} + R^*(s). \tag{14}$$

Пусть теперь $s\to 1+0$ вдоль действительной оси. Тогда левая часть (14) стремится к бесконечности. Действительно, $L(s, \chi_1)\to\infty$ при $s\to 1+0$; функция $L(s, \chi)$, $\chi\neq\chi_1$, регулярна при $\sigma>0$; $L(1, \chi)\neq 0$ при $\chi\neq\chi_1$ по доказанной выше лемме и $\log L(s, \chi)$, $\chi\neq\chi_1$, определенный по формуле (10), имеет конечный предел при $s\to 1+0$, поскольку

$$\log L(s,\chi) = -\int_s^c \frac{L'(u,\chi)}{L(u,\chi)}\, du + \log L(c,\chi) \quad \text{при } s=\sigma>1,\ c>\sigma,$$

если мы заметим, что $L(u, \chi)\neq 0$ при $u\geqslant 1$, $\chi\neq\chi_1$, а $L'(s, \chi)$ регулярна при $\sigma>0$, $\chi\neq\chi_1$. Далее, функция $R^*(s)$ регулярна при $\sigma>1/2$. Следовательно,

$$\sum_{p\equiv a \pmod m} p^{-s}\to\infty \quad \text{при } s\to 1+0.$$

Значит, ряд $\sum\limits_{p\equiv a \pmod m} 1/p$ расходится.

АСИМПТОТИЧЕСКИЙ ЗАКОН РАСПРЕДЕЛЕНИЯ ПРОСТЫХ ЧИСЕЛ

§ 1. Необращение в нуль функции $\zeta(1+it)$. Мы показали в предыдущей главе, что L-функции Дирихле обладают тем свойством, что $L(1, \chi) \neq 0$ при $\chi \neq \chi_1$, и использовали это для доказательства бесконечности множества простых в каждой арифметической прогрессии вида $a+mk$, где $m>0$, $(a, m)=1$ и $k=1, 2, \ldots$.

Покажем теперь, что дзета-функция Римана обладает тем свойством, что $\zeta(1+it) \neq 0$ при $t \neq 0$, и используем это свойство для доказательства асимптотического закона распределения простых чисел.

Асимптотический закон распределения простых чисел обычно записывается в виде

$$\pi(x) \sim \frac{x}{\log x}, \tag{1}$$

где $\pi(x)$ обозначает количество простых чисел, не превосходящих x, а символ $\sim$ означает, что $\pi(x)/(x/\log x) \to 1$ при $x \to \infty$.

В гл. VII мы показали, что сотношение (1) эквивалентно соотношению

$$\lim_{x \to \infty} \frac{\psi(x)}{x} = 1, \tag{2}$$

где ψ — функция Чебышева. Мы будем доказывать асимптотический закон распределения простых чисел именно в этой форме.

Нам потребуется соотношение

$$-\frac{\zeta'(s)}{\zeta(s)} = s \int_1^\infty \frac{\psi(u)\, du}{u^{s+1}}, \tag{3}$$

которое мы вывели в § 4 гл. VII для действительных $s>1$ в качестве следствия из формулы суммирования Абеля. В силу аналитического продолжения формула (3) будет справедлива для всех комплексных s с дейст-

вительной частью $\sigma>1$. (Мы пишем, как обычно, $s=\sigma+it$, где σ, t действительные и $i^2=-1$.)

Положим в равенстве (3) $u=e^x$. Тогда мы получим

$$-\frac{\zeta'(s)}{s\zeta(s)}=\int_0^\infty \psi(e^x)e^{-xs}\,dx, \qquad \sigma>1, \tag{4}$$

откуда мы выведем в дальнейшем, что $\psi(e^x)\sim e^x$, или $\psi(x)\sim x$ при $x\to\infty$.

Мы уже видели, что $\zeta(s)$ является аналитической функцией в полуплоскости $\sigma>0$, за исключением точки $s=1$, где она имеет простой полюс с вычетом 1, и что $\zeta(s)\neq 0$ при $\sigma>1$. Докажем теперь, что $\zeta(s)\neq 0$ на прямой $\sigma=1$.

Теорема (Адамар, Валле-Пуссен). *Если* $t\neq 0$, *то* $\zeta(1+it)\neq 0$.

Доказательство. При $\sigma>1$

$$\zeta(s)=\prod_p (1-p^{-s})^{-1},$$

и, логарифмируя это равенство, мы получаем, как и в гл. X,

$$\log\zeta(s)=\sum_{m,p}\frac{1}{mp^{ms}}, \qquad \sigma>1, \tag{5}$$

где m пробегает все положительные целые числа, а p — все простые числа. Следовательно,

$$\log|\zeta(s)|=\operatorname{Re}(\log\zeta(s))=\operatorname{Re}\left(\sum_{m,p}\frac{1}{mp^{ms}}\right).$$

Далее, ряд $\sum_{m,p}\frac{1}{mp^{ms}}=\sum_{n=2}^{\infty}\frac{c_n}{n^s}$ является рядом Дирихле с коэффициентами

$$c_n=\begin{cases}\dfrac{1}{m}, & \text{если } n=p^m,\\ 0, & \text{если } n\neq p^m.\end{cases}$$

Поэтому

$$\log|\zeta(s)|=\operatorname{Re}\left(\sum\frac{c_n}{n^s}\right),$$

где $c_n \geqslant 0$, и так как

$$\frac{c_n}{n^s} = \frac{c_n}{n^\sigma} \cdot n^{-it} = \frac{c_n}{n^\sigma}(\cos(t \log n) - i \sin(t \log n)),$$

то

$$\log|\zeta(s)| = \sum_{n=2}^{\infty} \frac{c_n}{n^\sigma} \cos(t \log n).$$

Поскольку

$$c_n \geqslant 0 \text{ и } 3 + 4\cos\theta + \cos 2\theta = 2(1 + \cos\theta)^2 \geqslant 0 \quad (6)$$

для всех действительных θ, то

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

$$= \sum_{n=2}^{\infty} \frac{c_n}{n^\sigma}(3 + 4\cos(t \log n) + \cos(2t \log n)) \geqslant 0.$$

Значит,

$$|\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)| \geqslant 1, \quad \sigma > 1,$$

так что

$$|(\sigma-1)\zeta(\sigma)|^3 \cdot \left|\frac{\zeta(\sigma+it)}{\sigma-1}\right|^4 \cdot |\zeta(\sigma+2it)| \geqslant \frac{1}{\sigma-1}. \quad (7)$$

Покажем теперь, что предположение $\zeta(1+it) = 0$ при $t = t_0 \neq 0$ приводит к противоречию. Действительно, если мы в (7) положим $t = t_0$, то при $\sigma \to 1+0$ правая часть будет стремиться к бесконечности, а левая часть будет стремиться к пределу $|\zeta'(1+it_0)|^4 |\zeta(1+2it_0)|$. Но этот предел конечен, поскольку $\zeta(s)$ — аналитическая функция при $\sigma > 0$, $s \neq 1$. Следовательно, $\zeta(1+it_0) \neq 0$ и теорема доказана.

§ 2. Теорема Винера — Икеары. Мы выведем асимптотический закон распределения простых чисел из следующей теоремы:

Теорема 2 (Винер — Икеара). *Пусть $A(x)$ — неотрицательная неубывающая функция от x, определенная*

при $0 \leqslant x < \infty$, *и пусть интеграл*

$$\int_0^\infty A(x)\, e^{-xs}\, dx, \quad s = \sigma + it,$$

сходится при $\sigma > 1$ *к функции* $f(s)$. *Пусть, далее,* $f(s)$ *является аналитической функцией при* $\sigma \geqslant 1$, *за исключением точки* $s = 1$, *где она имеет простой полюс с вычетом* 1. *Тогда*

$$\lim_{x \to \infty} e^{-x} A(x) = 1.$$

Доказательство. Разобьем доказательство теоремы на две части. Положив

$$B(x) = e^{-x} A(x), \tag{8}$$

мы докажем сначала, что для любого $\lambda > 0$

$$\lim_{y \to \infty} \int_{-\infty}^{\lambda y} B\left(y - \frac{v}{\lambda}\right) \frac{\sin^2 v}{v^2}\, dv = \pi. \tag{9}$$

Затем мы выведем из (9), что

$$\lim_{x \to \infty} B(x) = 1. \tag{10}$$

Первая часть. Так как при $\sigma > 1$

$$f(s) = \int_0^\infty A(x)\, e^{-xs}\, dx, \quad \frac{1}{s-1} = \int_0^\infty e^{-(s-1)x}\, dx,$$

то

$$f(s) - \frac{1}{s-1} = \int_0^\infty (B(x) - 1) e^{-(s-1)x}\, dx \ (\sigma > 1).$$

Положим

$$g(s) = f(s) - \frac{1}{s-1}, \quad g_\varepsilon(t) = g(1 + \varepsilon + it), \ \varepsilon > 0.$$

Тогда, в силу предположений о функции $f(s)$, $g(s)$ будет аналитической при $\sigma \geqslant 1$.

Для $\lambda>0$ мы имеем

$$\frac{1}{2}\int_{-2\lambda}^{2\lambda} g_\varepsilon(t)\left(1-\frac{|t|}{2\lambda}\right)e^{iyt}\,dt =$$

$$=\frac{1}{2}\int_{-2\lambda}^{2\lambda}\left(1-\frac{|t|}{2\lambda}\right)e^{iyt}\left(\int_0^\infty (B(x)-1)e^{-(\varepsilon+it)x}dx\right)dt. \quad (11)$$

Покажем, что в (11) можно изменить порядок интегрирования. Так как $A(x)$ является неубывающей и неотрицательной функцией, то при действительных s и $x>0$

$$f(s)=\int_0^\infty A(u)\,e^{-us}\,du \geqslant A(x)\int_x^\infty e^{-us}\,du=\frac{A(x)e^{-xs}}{s},$$

т. е. $A(x)\leqslant sf(s)\,e^{xs}$. Далее, поскольку $f(s)$ — аналитическая функция при $\sigma>1$, то $A(x)=O(e^{xs})$ для каждого $s>1$, а тогда $A(x)=o(e^{xs})$ для каждого $s>1$. Следовательно, $B(x)\,e^{-\delta x}=A(x)\,e^{-(1+\delta)x}=o(1)$ для каждого $\delta>0$, откуда следует, что интеграл

$$\int_0^\infty (B(x)-1)\,e^{-(\varepsilon+it)x}\,dx$$

сходится равномерно в интервале $-2\lambda\leqslant t\leqslant 2\lambda$. Значит, в (11) можно поменять порядок интегрирования, и мы получим

$$\frac{1}{2}\int_{-2\lambda}^{2\lambda} g_\varepsilon(t)\left(1-\frac{|t|}{2\lambda}\right)e^{iyt}\,dt =$$

$$=\int_0^\infty (B(x)-1)\,e^{-\varepsilon x}\left(\int_{-2\lambda}^{2\lambda}\frac{1}{2}e^{i(y-x)t}\left(1-\frac{|t|}{2\lambda}\right)dt\right)dx =$$

$$=\int_0^\infty (B(x)-1)\,e^{-\varepsilon x}\,\frac{\sin^2\lambda(y-x)}{\lambda(y-x)^2}\,dx. \quad (12)$$

Функция $g(s)$ является аналитической при $\sigma\geqslant 1$, и поэтому $g_\varepsilon(t)\to g(1+it)$ равномерно в интервале

$-2\lambda \leqslant t \leqslant 2\lambda$ при $\varepsilon \to 0$. Далее,

$$\lim_{\varepsilon \to 0} \int_0^\infty e^{-\varepsilon x} \frac{\sin^2 \lambda(y-x)}{\lambda(y-x)^2}\, dx = \int_0^\infty \frac{\sin^2 \lambda(y-x)}{\lambda(y-x)^2}\, dx$$

и, следовательно, предел

$$\lim_{\varepsilon \to 0} \int_0^\infty B(x)\, e^{-\varepsilon x} \frac{\sin^2 \lambda(y-x)}{\lambda(y-x)^2}\, dx$$

существует. Кроме того, поскольку подинтегральная функция неотрицательна и монотонно возрастает при $\varepsilon \to 0$, мы имеем

$$\lim_{\varepsilon \to 0} \int_0^\infty B(x)\, e^{-\varepsilon x} \frac{\sin^2 \lambda(y-x)}{\lambda(y-x)^2}\, dx = \int_0^\infty B(x) \frac{\sin^2 \lambda(y-x)}{\lambda(y-x)^2}\, dx.$$

Таким образом, мы получаем из (12)

$$\frac{1}{2} \int_{-2\lambda}^{2\lambda} g(1+it)\left(1 - \frac{|t|}{2\lambda}\right) e^{iyt}\, dt = \int_0^\infty B(x) \frac{\sin^2 \lambda(y-x)}{\lambda(y-x)^2}\, dx - \int_0^\infty \frac{\sin^2 \lambda(y-x)}{\lambda(y-x)^2}\, dx.$$

Пусть теперь $y \to \infty$. Тогда по лемме Римана—Лебега [1] левая часть стремится к нулю, в то время как второй член правой части дает

$$\lim_{y \to \infty} \int_0^\infty \frac{\sin^2 \lambda(y-x)}{\lambda(y-x)^2}\, dx = \lim_{y \to \infty} \int_{-\infty}^{\lambda y} \frac{\sin^2 v}{v^2}\, dv = \pi.$$

Следовательно,

$$\lim_{y \to \infty} \int_{-\infty}^{\lambda y} B\left(y - \frac{v}{\lambda}\right) \frac{\sin^2 v}{v^2}\, dv = \pi;$$

тем самым соотношение (9) доказано.

[1] См. Ахиезер Н. И., Лекции по теории аппроксимации, «Наука», М., 1965, п. 60. — *Прим. перев.*

Вторая часть. Докажем равенство (10) в два этапа, а именно

$$\overline{\lim_{x\to\infty}} B(x)\leqslant 1 \tag{13}$$

и

$$\underline{\lim_{x\to\infty}} B(x)\geqslant 1. \tag{14}$$

Для данных положительных чисел a и λ пусть $y>a/\lambda$. Тогда, согласно (9), мы имеем

$$\overline{\lim_{y\to\infty}} \int_{-a}^{a} B\left(y-\frac{v}{\lambda}\right)\frac{\sin^2 v}{v^2}\,dv\leqslant\pi,$$

так как подинтегральная функция неотрицательна. Далее, функция $A(u)=B(u)e^u$ является неубывающей. Значит, при $-a\leqslant v\leqslant a$

$$e^{y-\frac{a}{\lambda}}B\left(y-\frac{a}{\lambda}\right)\leqslant e^{y-\frac{v}{\lambda}}B\left(y-\frac{v}{\lambda}\right),$$

откуда следует, что

$$B\left(y-\frac{v}{\lambda}\right)\geqslant B\left(y-\frac{a}{\lambda}\right)e^{\frac{v-a}{\lambda}}\geqslant B\left(y-\frac{a}{\lambda}\right)e^{-\frac{2a}{\lambda}}.$$

Следовательно,

$$\overline{\lim_{y\to\infty}} \int_{-a}^{a} B\left(y-\frac{a}{\lambda}\right)e^{-\frac{2a}{\lambda}}\frac{\sin^2 v}{v^2}\,dv\leqslant\pi,$$

или

$$\overline{\lim_{y\to\infty}} B\left(y-\frac{a}{\lambda}\right)e^{-\frac{2a}{\lambda}}\int_{-a}^{a}\frac{\sin^2 v}{v^2}\,dv\leqslant\pi.$$

Далее, для фиксированных a и λ мы имеем

$$\overline{\lim_{y\to\infty}} B\left(y-\frac{a}{\lambda}\right)=\overline{\lim_{y\to\infty}} B(y).$$

Поэтому

$$e^{-\frac{2a}{\lambda}} \overline{\lim_{y\to\infty}} B(y) \int_{-a}^{a} \frac{\sin^2 v}{v^2} dv \leqslant \pi$$

для всех $a>0$, $\lambda>0$. Пусть теперь $a\to\infty$ и $\lambda\to\infty$ таким образом, что $a/\lambda\to 0$. Тогда

$$\overline{\lim_{y\to\infty}} B(y) \int_{-\infty}^{\infty} \frac{\sin^2 v}{v^2} dv \leqslant \pi,$$

или

$$\pi \overline{\lim_{y\to\infty}} B(y) \leqslant \pi.$$

Итак, неравенство (13) доказано.

Используем теперь неравенство (13) для того, чтобы доказать (14). Из (13) следует, что $|B(x)|\leqslant c$ при подходящей константе c, так что для фиксированных положительных a и λ и для достаточно больших y мы имеем

$$\int_{-\infty}^{\lambda y} B\left(y-\frac{v}{\lambda}\right)\frac{\sin^2 v}{v^2} dv \leqslant$$

$$\leqslant c\left[\int_{-\infty}^{-a} + \int_{a}^{\infty}\right]\frac{\sin^2 v}{v^2} dv + \int_{-a}^{a} B\left(y-\frac{v}{\lambda}\right)\frac{\sin^2 v}{v^2} dv. \qquad (15)$$

Как и раньше, при $-a\leqslant v\leqslant a$ мы имеем

$$B\left(y-\frac{v}{\lambda}\right) \leqslant B\left(y+\frac{a}{\lambda}\right) e^{\frac{2a}{\lambda}},$$

так что

$$\int_{-a}^{a} B\left(y-\frac{v}{\lambda}\right)\frac{\sin^2 v}{v^2} dv \leqslant B\left(y+\frac{a}{\lambda}\right) e^{\frac{2a}{\lambda}} \int_{-a}^{a} \frac{\sin^2 v}{v^2} dv. \qquad (16)$$

Из (9), (15) и (16) мы получаем

$$\pi \leqslant c\left[\int_{-\infty}^{-a} + \int_{a}^{\infty}\right]\frac{\sin^2 v}{v^2}dv + \lim_{y\to\infty} B\left(y+\frac{a}{\lambda}\right)e^{\frac{2a}{\lambda}}\int_{-a}^{a}\frac{\sin^2 v}{v^2}dv,$$

т. е.

$$\pi \leqslant c\left[\int_{-\infty}^{-a} + \int_{a}^{\infty}\right]\frac{\sin^2 v}{v^2}dv + \lim_{y\to\infty} B(y)\,e^{\frac{2a}{\lambda}}\int_{-a}^{a}\frac{\sin^2 v}{v^2}dv.$$

Пусть теперь $a\to\infty$ и $\lambda\to\infty$ таким образом, что $a/\lambda\to 0$. Тогда

$$\pi \leqslant \pi \lim_{y\to\infty} B(y),$$

и тем самым (14), а следовательно, и теорема 2 доказаны.

§ 3. Асимптотический закон распределения простых чисел. Если ψ — функция Чебышева (см. гл. VII), положим $A(x)=\psi(e^x)$ и заметим, что функция ψ неубывающая и $\psi(e^x)\geqslant 0$. Соотношение (4) позволяет проверить другие предположения теоремы 2, ибо функция $\zeta(s)$ является аналитической при $\sigma>0$, за исключением точки $s=1$, где она имеет простой полюс, и, согласно теореме 1, $\zeta(s)$ не обращается в нуль в полуплоскости $\sigma\geqslant 1$. Следовательно, по теореме 2 $\psi(e^x)\sim e^x$, или $\psi(x)\sim x$ при $x\to\infty$, и тем самым асимптотический закон распределения простых чисел доказан.

Таким образом, асимптотический закон распределения простых чисел следует из теоремы Винера — Икеары, если мы предположим, что $\zeta(1+it)\neq 0$ для $t\neq 0$. Обратно, если мы предположим, что справедлив асимптотический закон распределения простых чисел, то легко вывести, что $\zeta(1+it)\neq 0$ при $t\neq 0$. Действительно, пусть

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

Тогда $\Phi(s)$ регулярна при $\sigma>0$, за исключением простых полюсов, которые она имеет в точках, являющих-

ся нулями $\zeta(s)$. Асимптотический закон распределения простых чисел означает, что $\psi(x)=x+o(x)$ при $x\to\infty$. Следовательно, для любого данного $\varepsilon>0$ существует число $x_0(\varepsilon)$, такое, что при $x\geqslant x_0(\varepsilon)>1$

$$|\psi(x)-x|<\varepsilon x.$$

Тогда при $\sigma>1$ мы имеем

$$|\Phi(s)|<\int_1^{x_0}\frac{|\psi(x)-x|}{x^2}\,dx+\int_{x_0}^{\infty}\frac{\varepsilon}{x^\sigma}\,dx,$$

и так как

$$\int_{x_0}^{\infty}\frac{\varepsilon}{x^\sigma}\,dx<\int_1^{\infty}\frac{\varepsilon}{x^\sigma}\,dx=\frac{\varepsilon}{\sigma-1},$$

то

$$|\Phi(s)|<K+\frac{\varepsilon}{\sigma-1},\quad \sigma>1,$$

где $K=K(x_0)=K(\varepsilon)$. Таким образом,

$$(\sigma-1)\,|\Phi(s)|<K(\sigma-1)+\varepsilon,\quad \sigma>1.$$

Пусть теперь $\sigma\to1+0$. Тогда для любого фиксированного t

$$\lim_{\sigma\to1+0}(\sigma-1)\,\Phi(\sigma+it)=0. \tag{17}$$

Если $1+it$ при $t\neq0$ будет нулем функции $\zeta(s)$, то предел выражения $(\sigma-1)\,\Phi(\sigma+it)$ при $\sigma\to1+0$ будет равен вычету функции $\Phi(s)$ в простом полюсе $s=1+it$ и, следовательно, будет отличен от нуля. Но это противоречит (17) и, следовательно, $\zeta(1+it)\neq0$ при $t\neq0$.

Таким образом, утверждение, что $\zeta(1+it)\neq0$ при $t\neq0$, «эквивалентно» асимптотическому закону распределения простых чисел. Другим эквивалентным утверждением является утверждение, что $p_n\sim n\log n$, где p_n означает n-е простое число, если простые числа расположены в естественном порядке.

Действительно, если $\frac{\pi(x)\log x}{x}\to 1$ при $x\to\infty$, то

$$\log\pi(x)+\log\log x-\log x\to 0$$

и, следовательно,

$$\frac{\log\pi(x)}{\log x}\to 1.$$

Тогда

$$\frac{\pi(x)\log\pi(x)}{x}\to 1,$$

откуда следует, что $p_n\sim n\log n$, если взять $x=p_n$.

Обратно, если x определить неравенствами $p_n\leqslant x<p_{n+1}$ и если $p_n\sim n\log n$, то $p_{n+1}\sim(n+1)\log(n+1)\sim n\log n$, так что $x\sim n\log n$, или $x\sim y\log y$, где $y=\pi(x)=n$, т. е. $\log x\sim\log y$ и, следовательно,

$$y\sim\frac{x}{\log x}.$$

СПИСОК ЛИТЕРАТУРЫ

1. Dickson L. E., History of the theory of numbers, Carnegie Institution, Washington, I (1919), II (1920), III (1923), reprinted Chelsea, New York, 1952.
2. Hardy G. H. and Wright E. M., An introduction to the theory of numbers, Oxford University Press, 1938, 2nd edition, 1945.
3. Ingham A. E., The distribution of prime numbers, Cambridge University Press, 1932, reprinted Stechert-Hafner, New York, 1964. (Русский перевод: Ингам А. Е., Распределение простых чисел, ОНТИ, 1936.)
4. Landau E., Handbuch der Lehre von der Verteilung der Primzahlen, 2 volumes, Teubner, Leipzig, 1909, reprinted Chelsea, New York, 1953.
5. Uspensky J. V. and Heaslet M. A., Elementary number theory, McGraw-Hill, New York, 1939.
6. Виноградов И. М., Основы теории чисел, «Наука», М., 1965.

ПРИМЕЧАНИЯ

Примечания к главе I

В качестве основных источников см. [2], гл. 1 — 3 и [5], гл. 1—6.

§ 2. Теорема 2 была установлена Гауссом (Gauss C. F., Disquisitiones Arithmeticae, 1801, § 16; см. также Gauss C. F., Werke, I, 1863, S. 15).

Относительно первого доказательства теоремы 2 можно сослаться на работу Цермело (Zermelo E., *Göttinger Nachrichten* (new series), **1** (1934), 43—44). Согласно Цермело, его доказательство датируется 1912 г. См. также Hasse H., *J. für Math.*, **159** (1928), 3—6, и Lindemann F. A., *Quarterly J. Math.* (Oxford), **4** (1933), 319—320.

§ 3. Относительно второго доказательства теоремы 2 см. Hecke E., Vorlesungen über die Theorie der algebraischen Zahlen, 1923, ch. 1. То, что мы называем модулем в множестве целых чисел, есть просто подгруппа аддитивной группы целых чисел.

Относительно теоремы 6 см. Евклид, Начала, ГИТТЛ, М.—Л., 1948—1950, книга 7, предл. 30.

§ 5. Имя Фарея связано с последовательностями Фарея благодаря Коши, который обратил внимание на предложенную в 1816 г. Фареем (без доказательства) теорему 7 и опубликовал свое доказательство. См. Cauchy A., Oeuvres, 2^e série, Paris, t. 6, p. 146. Теоремы 7 и 9, по-видимому, впервые установил и доказал в 1802 г. Харош (Haros C.); см. [1], I, стр. 156. Представляет интерес следующее замечание К. Л. Зигеля к доказательству теоремы 7: «Пусть $kl-hm=1$, $k>0$, $m>0$. Однородная линейная подстановка $\lambda=ka-hb$, $\mu=-ma+lb$ целых переменных a и b имеет обратную $a=\lambda l+h\mu$, $b=m\lambda+k\mu$. Следовательно, условия $h/k\leqslant a/b\leqslant l/m$, $b>0$, $(a, b)=1$, удовлетворяются тогда и только тогда, когда $\lambda\geqslant 0$, $\mu\geqslant 0$, $\lambda+\mu>0$, $(\lambda, \mu)=1$, и тогда $b\leqslant m+k$ точно в трех случаях $\lambda, \mu=0,1$; 1,1; 1,0. В этом рассуждении не используется понятие последовательности Фарея F_n».

§ 6. Относительно теоремы 12 см. Евклид, Начала, ГИТТЛ, 1948—1950, книга 9, предл. 20. Доказательство Пойа теоремы 13 см. в книге Полиа Г. и Сеге Г., Задачи и теоремы из анализа, ГИТТЛ, М., 1956, II, стр. 149, 366. Замечание о том, чтобы положить $f_0=3$, принадлежит К. Л. Зигелю. Доказательство, предложенное Беннетом, результата Эйлера о том, что f_5 делится на 641, дано в книге [2], стр. 15. Другое доказательство дано Крайчиком (Kraitchik, Théorie des nombres, Paris, 1926, II, p. 221).

Примечания к главе II

В качестве основных источников см. [2], гл. 5, [5], гл. 6, 7 и [6], гл. 1, 2.

§ 1. Теория сравнений была развита Гауссом в его Disquisitiones Arithmeticae, loc. cit., хотя Ферма и Эйлеру, возможно, были известны некоторые основные результаты.

§ 2. Относительно формулировки теоремы 3, данной Ферма в 1640 г., см. Fermat P., Oeuvres, Paris, II, 209. Эйлер доказал теорему 2 в 1760 г.; см. Euler L., Opera Omnia, Leipzig-Berlin-Zürich (1), II, 531. См. также книгу Диксона [1], I, гл. 3.

§ 3. Относительно теоремы 7 см. Lagrange J. L., Oeuvres, Paris, 1868, II, p. 667—669.

Примечания к главе III

§ 2. Относительно доказательств теорем 5 и 7 см., например, Rademacher H., Lectures on elementary number theory, Blaisdell, New York, 1964, p. 33—35.

§ 3. Относительно теоремы 6 см. Lucas, Theorie des nombres, 1891, I, p. 353—354.

§ 4. Теорема 9 принадлежит Гурвицу (Hurwitz A., *Math. Annalen*, **39** (1891), 279—284). Приведенное здесь доказательство дано А. Хинчиным (*Math. Annalen*, **111** (1935), 631—637). На это доказательство внимание автора обратил Рагхаван Нарасимхан. В книге автора Einführung in die Analytische Zahlentheorie, Springer Lecture Notes, **29** (1966), ch. 3, был дан набросок другого доказательства, которое восходит к Форду (Ford L. R., *American Math. Monthly*, **45** (1938), 586—601).

Примечания к главе IV

В качестве основных источников см. [2], [5] и [6].

§ 1. Относительно символа Лежандра см. Legendre A. M., Essai sur la théorie des nombres, 1798, 2^{nd} edition, 1808, § 135.

Мы не рассматривали случай $p=2$, поскольку все целые числа являются квадратичными вычетами по модулю 2.

§ 2. Первое опубликованное доказательство (1773 г.) теоремы Вильсона было дано Лагранжем (Lagrange J. L., Oeuvres, Paris, III, 425). Эта теорема впервые была установлена Варингом (Waring E., Meditationes algebraicae, 1770, p. 218) и была приписана Вильсону. Харди и Райт говорят, что «есть основания считать, что она была известна задолго до Лейбница».

§ 3. Теоремы 5, 6, 7 можно найти в книге Харди и Райта [2], стр. 70, 297. Предложенное здесь доказательство теоремы 7 дано Эрмитом (Hermite C., *Journal de Math.* (1), **13** (1848), 15; Oeuvres, Paris, I, 264).

§ 4. Варинг установил без доказательства, что каждое положительное целое число можно представить в виде суммы четырех квадратов (Waring E., Meditationes algebraicae, 1770, p. 204—205); Лагранж доказал это утверждение в том же году; см. его Oeuvres, III, p. 189. См. также [1], II, гл. 8.

Примечания к главе V

§ 1. Теорема 1 была установлена Эйлером и частично доказана Лежандром. Полное доказательство было дано Гауссом в 1795 г. См. Bachmann P., Niedere Zahlentheorie, 1902, I, ch. 6, где приведено несколько доказательств.

§ 2—3. Идея доказательства теоремы 1 с помощью формулы взаимности для сумм Гаусса восходит к Кронекеру (Kronecker L., *Monatsber. Kgl. Preuss. Akad. Wiss. Berlin* (1880), 686—698; 854—860; *J. für die reine und angewandte Math.*, **105** (1889), 267—268; Werke (1929), IV, 278—300). Однако, как указал К. Л. Зигель, в книге Линделёфа (Lindelöf E., Calcul des Résidus, p. 68) имеется ссылка на работу Шаара (Schaar) 1848 г. о формуле взаимности для сумм Гаусса. Эта идея была распространена на числовые алгебраические поля Гекке (Hecke E., *Göttinger Nachrichten* (1919), 265—278; Werke, 235—248) и Зигелем (Siegel C. L., *Göttinger Nachrichten* (1960), 1—16; Ges. Abhandlungen, 1966, III, 334—349). Приведенное здесь доказательство по существу принадлежит Зигелю. Интеграл, использованный в доказательстве теоремы 2, играет важную роль в теории дзета-функции Римана. См. Siegel K. L., *Quellen und Studien zur Geschihte der Math.*, **2** (1932), 45—80; Gesammelte Abhandlungen (1966), I, 275.

Относительно оценок обычных сумм Гаусса с помощью контурного интегрирования см. также Mordell L. J., *Messenger of Math.*, **48** (1919), 54—56.

Благодаря замечаниям Зигеля вывод (14) из (12) здесь несколько короче, чем в книге автора Einführung in die analytische Zahlentheorie (loc. cit., ch. 3).

Так как $g(-m, -n) = g(m, n)$, случай $m<0$, $n>0$ может быть сведен к случаю $m>0$, $n<0$.

Соотношение (21) показывает, что -1 является квадратичным вычетом для простых чисел, сравнимых с $1 \pmod 4$, и квадратичным невычетом для простых чисел, сравнимых с $3 \pmod 4$.

§ 4. Теорема 3 принадлежит Эйлеру (Euler L., Opera Omnia, Leipzig-Berlin-Zürich (1), III, 240).

Примеры и замечания см. в книге Радемахера (Rademacher H., Lectures on elementary number theory, New York, 1964, p. 74, 82.)

Примечания к главе VI

В качестве основных источников см. [2], гл. 16—18 и [6].

§ 2. Утверждение о том, что $r(n)=O(n^{\varepsilon})$ для каждого $\varepsilon>0$, эквивалентно утверждению, что $r(n)=o(n^{\varepsilon})$ для каждого $\varepsilon>0$.
Относительно теоремы 1 см. Gauss C. F., Werke, II, S. 272—275.

§ 3. Относительно теоремы 6 см. Полиа Г. и Сеге Г., Задачи и теоремы из анализа, ГИТТЛ, М., 1956, II, стр. 177, 413.
Относительно теорем 5 и 6 см. Харди и Райт [2], стр. 259.
Теорема 9 была доказана Дирихле в 1849 г. (см. Dirichlet P. G. L., Werke, II, 49—66).
Улучшение Г. Ф. Вороным остаточного члена приведено в *Ann. Sci. Ecole Norm. Sup.* (3), **21** (1904), 207—267; 459—533.
Утверждение о том, что остаточный член не может быть $O(N^{1/4})$, было доказано Харди (Hardy G. H., *Proc. London Math. Soc.* (2), **15** (1916), 192—213).

§ 4. Относительно истории чисел Мерсенна и совершенных чисел см. Диксон [1], I, гл. 1—2.

§ 5. Относительно теорем 15 и 19 см. Möbius A. F., *J. für die reine und angewandte Math.*, **9** (1832), 105—123; *Werke* (1887), IV, 589—612. См. также Ландау [4], § 150—152. Теоремы 16 и 17 были доказаны одновременно Дедекиндом (Dedekind R., *J. für die reine und angewandte Math.*, **54** (1857), 21) и Лиувиллем (Liouville J., *J. de Math. pures et appliquées* (2), **2** (1857), 111).

§ 6. Относительно теоремы 20 см. Ландау [4], § 59. Теорема 22 принадлежит Мертенсу (Mertens F., *J. für die reine und angewandte Math.*, **77** (1874), 290—291). См. также Ландау [4], § 152.
Оценка $\sum_{n=1}^{\infty}\mu(n)n^{-2}$ без использования тождества Эйлера (доказанного позже в гл. VII, § 4) есть результат замечания Рагхавана Нарасимхана. Относительно доказательства формулы $\sum_{n=1}^{\infty}n^{-2}=\pi^2/6$ см., например, Кпорр K., Theory and application of infinite series, 1951, p. 237, 323, 376.

Примечания к главе VII

В качестве основных источников см. [3], гл. 1 и [4], § 12—28.

§ 1. Относительно теоремы 1 см. Euler L., Opera Omnia, Leipzig-Berlin-Zürich (1), 8, § 279; (1), 14, 216—244.

§ 2. Теорема 3 принадлежит Чебышеву; см. Чебышев П. Л., Собрание сочинений, т. I, Изд-во АН СССР, М.—Л., 1944, стр. 191—207.

§ 3. Относительно доказательства Пиллаи теоремы 4 см. Pillai S. S., *Bull. Calcutta Math. Soc.*, **36** (1944), 97—99; **37** (1944), 27. См. также Ландау [4], § 22.

§ 4. Теорема 7 доказана Чебышевым; см. Чебышев П. Л., Собрание сочинений, т. I, Изд-во АН СССР, М.—Л., стр. 173—190. См. также книгу Ингама [3], стр. 16—21. Эйлер использовал *формальное* тождество.

§ 5. Теорема 8 принадлежит Мертенсу (Mertens F., *J. für die reine und angewandte Math.*, **78** (1874), 46—62). См. также книгу Ингама [3], стр. 22.

Формула Стирлинга дана, например, в книге Титчмарша (Titchmarsh E. C., The theory of functions, Oxford, 1932, 2nd edition, 1939, § 187).

Примечания к главе VIII

§ 1—4. Теорема Вейля была доказана им в *Math. Annalen*, **77** (1916), 313—352. Разъяснение понятия «отклонения» дано Дж. В. С. Касселсом (Gassels J. W., An introduction to Diophantine approximation, Cambridge, 1957, ch. 4; русский перевод: Касселс Дж. В. С., Введение в теорию диофантовых приближений, ИЛ, М., 1961.)

§ 5. Кронекер доказал свою теорему в *Berliner Sitzungsberichte* (1884); см. также Kronecker L., Werke, Leipzig, Teubner, III (I), 47—110. Относительно дальнейших достижений см. Koksma J. F., Diophantische Approximationen, *Ergebnisse der Math.*, Bd. IV, Heft 4 (1937).

Доказательство Бора (Bohr H.) теоремы 8 дано в *J. London Math. Soc.*, **9** (1934), 5—6. См. также Харди и Райт [2], гл. 23.

Примечания к главе IX

В качестве основных источников см. Minkowski H., Geometrie der Zahlen, 1st edition, 1896, и Diophantische Approximationen, 1927. См. также Siegel C. L., Geometry of numbers, New York University, 1945.

§ 2. Теорема 1 справедлива без предположения об ограниченности множества S. Действительно, если оно не ограничено и имеет меру $V(S) > 2^n$, то можно взять пересечение множества S с кубом K_M: $|x_k| < M$, $1 \leqslant k \leqslant n$, и если M достаточно велико, то $S_M = S \bigcap K_M$ будет ограниченным множеством, удовлетворяющим требуемым условиям в силу счетной аддитивности меры Лебега.

Мы не стремились к рассмотрению оптимальных предположений, поскольку не желали углубляться в вопросы измеримости. Формулировка и доказательство теоремы 3 продиктованы этими соображениями.

Минковский доказал теорему 3 в 1891 г.; см. его Gesammelte Abhandlungen, I, S. 264.

Доказательство формулы Зигеля (8) дано им в *Acta Math.*, **65** (1935), 307—323.

Лемма, которая расположена между теоремами 2 и 3, принадлежит Г. Д. Биркгофу, как это установил Бликфельдт (Blichfeldt, *Trans. Amer. Math. Soc.*, **15** (1914)). См. также приложение в книге Касселса (loc. cit., примечания к гл. VIII).

В теореме 2 мы использовали тот факт, что замкнутое множество в R_n измеримо по Лебегу.

Минковский (loc. cit.) показал, что ограниченное выпуклое множество в R^n имеет объем в смысле Жордана. См. Minkowski H., Geometrie der Zahlen, Leipzig, Teubner, 1896, 50—60, а также его Theorie der konvexen Körper, Ges. Abh., 2, 142—143, и книгу Бляшке (Blaschke W., Kreis und Kugel, Leipzig, 1916, 57; русский перевод: Бляшке В., Круг и шар, «Наука», М., 1967)

Если выпуклое множество S имеет меру Лебега $V(S), 0<V(S)<\infty$, то оно ограничено. См. Cassels J. W. S., An introduction to the geometry of numbers, Springer, 1959, p. 109; русский перевод: Касселс Дж. В. С., Введение в геометрию чисел, ИЛ, М., 1965.

Примечания к главе X

В качестве основных источников см. Ландау [4], § 95—103. См. также Siegel K. L., Lectures on analytic number theory, New York University, 1945.

§ 5. Основная теорема этой главы, а именно теорема 8, была впервые доказана Дирихле в 1837 г., см. его Werke, I, 307—342. Элементарное доказательство было дано Мертенсом (Mertens F., *Wiener Sitzungsberichte*, **106** (1897), 254—286). Новое элементарное доказательство было предложено Сельбергом (Selberg A., *Annals of Math.* (2), **50** (1949), 297—304; *Canadian J. of Math.*, **2** (1950), 66—78). Другое элементарное доказательство дал Цассенхаус (Zassenhaus H., *Comm. Math. Helvetici*, **22** (1949), 232—259).

Примечания к главе XI

В качестве основных источников см. Ландау [4], включая приложение П. Т. Бейтмана, стр. 929—931, где дана история доказательства асимптотического закона распределения простых чисел. Идея о связи поведения $\pi(x)$ со свойствами функции $\zeta(s)$, где s — компнулей $\zeta(s)$ восходит к Риману (Riemann B., Über die Anzahl der Primzahlen unter einer gegebenen Größe, *Monatsberichte der Preuss. Akad. der Wissenschaften*, Berlin (1859—1860), 671—680; *Werke*, 1st edition, 1876, S. 136—144; 2nd edition, 1892, S. 145—155).

§ 1. Первое доказательство асимптотического закона распределения простых чисел было дано Адамаром (Hadamard J., *Bull. de la Soc. Math. de France*, **24** (1896), 199—220) и Валле-Пуссеном (de la Vallée Poussin C.-J., *Annales de la Soc. sci. de Bruxelles*, $\mathbf{20_2}$ (1896),

183—256). Полное изложение классического доказательства см. в книге Ингама [3], гл. 2.

§ 2. Относительно теоремы Винера — Икеары см. Ikehara S., *J. Math. Phys. Mass. Inst. Tech.*, **10** (1931), 1—12; Wiener N., *Annals of Math.*, 33 (1932), 1—100; 787; и Wiener N., The Fourier integral, Cambridge, 1933, § 19 (русский перевод: Н. Винер, Интеграл Фурье и его приложения, «Наука», 1963, § 19). Теорема справедлива при более слабых предположениях, но для вывода асимптотического закона распределения простых чисел достаточно той формулировки теоремы, которую мы рассмотрели.

Данное здесь доказательство теоремы Винера — Икеары не использует общей тауберовой теоремы Винера и по существу является доказательством Бохнера (Bochner S., *Math. Zeit.*, **37** (1933), 1—9), упрощенным Ландау (Landau E., *Berliner Sitzungsberichte* (1932), 514—521) и Бохнером в его Lectures on Fourier Analysis, Princeton University, 1936. Оно дается в том же самом виде, как и в лекциях автора: Lectures on the Riemann zeta-function, Tata Institute of Fundamental Research, Bombay, 1953. Элементарное доказательство асимптотического закона распределения простых чисел было дано Сельбергом (Selberg A., *Annals of Math.* (2), **50** (1949), 305—313).

УКАЗАТЕЛЬ

ОГЛАВЛЕНИЕ

УВАЖАЕМЫЙ ЧИТАТЕЛЬ!

Ваши замечания о содержании книги, ее оформлении, качестве перевода и другие просим присылать по адресу: 129820, Москва И-110, ГСП, 1-й Рижский пер., 2, изд-во «Мир»

К. Чандрасекхаран
ВВЕДЕНИЕ
В АНАЛИТИЧЕСКУЮ ТЕОРИЮ ЧИСЕЛ

Редактор Д. Ф. Борисова
Художник К. И. Милаев
Художественный редактор В. И. Шаповалов
Технический редактор Е. Н. Лебедева
Корректор С. М. Лебедева

Сдано в набор 16/VII—1973 г. Подписано к печати 17/IV—1974 г. Бумага тип. № 1. $84\times108^{1}/_{32}=2{,}94$ бум. л. 9,87 усл. печ. л. Уч.-изд л. 7,78. Изд. № 1/7266. Цена 62 коп. Зак. 870

Издательство «Мир», Москва, 1-й Рижский пер., 2

Владимирская типография Союзполиграфпрома при Государственном комитете Совета Министров СССР по делам издательств, полиграфии и книжной торговли Гор. Владимир, ул. Победы, д. 18-б.