ПРОСТЫЕ ЧИСЛА

Э. ТРОСТ

ELEMENTE DER MATHEMATIK
VOM HÖHEREN STANDPUNKT AUS

PRIMZAHLEN

von

DR. ERNST TROST

VERLAG BIRKHAUSER · BASEL—STUTTGART

ЭРНСТ ТРОСТ

ПРОСТЫЕ ЧИСЛА

Перевод с немецкого Н. И. ФЕЛЬДМАНА
под редакцией А. О. ГЕЛЬФОНДА

ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1959

АННОТАЦИЯ

Книга посвящена одной из областей арифметики — теории простых чисел. Автор поставил себе целью изложить некоторые теоремы «элементарной» теории простых чисел и сообщить наряду с этим о различных интересных результатах в этой области. Для чтения книги достаточно знания школьной алгебры и простейших фактов дифференциального и интегрального исчисления. В книге изложены элементарные доказательства асимптотического закона распределения простых чисел, найденное Сельбергом и Эрдошем в 1948 г., и теоремы Дирихле о простых числах в арифметической прогрессии. Специальная глава содержит основы метода решета Бруна.

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Простые числа, как основные составные элементы натуральных чисел, более или менее подробно изучаются в каждом учебнике теории чисел, однако при этом обходятся сравнительно немногими теоремами. Самостоятельная теория простых чисел является менее известной специальной областью арифметики. Она отличается просто формулируемыми постановками задач и в то же время сложными, часто аналитическими, доказательствами. Многие проблемы ожидают здесь еще своего решения.

Мы поставили перед собой задачу доказать некоторые теоремы «элементарной» теории простых чисел и наряду с этим сообщить о различных интересных результатах, чтобы помочь ознакомлению читателя с этой богатой замечательными методами областью. Принимая во внимание ограниченный объем книги, многое приходится, конечно, пропустить, в особенности мы экономили в литературном указателе. В работах Ландау [12], Ингама [9] и Диксона [5] читатель найдет в изобилии дальнейшую информацию (см. список литературы на страницах 132—134).

Кроме некоторых простейших фактов из дифференциального и интегрального исчисления и школьной алгебры, никакие предварительные знания у читателя не предполагаются. Необходимые сведения из теории чисел излагаются в двух первых главах.

Сенсацией первого ранга явилось открытие П. Эрдёшем и А. Сельбергом в 1948 году элементарного, т. е. не зависящего от средств теории функций, доказательства асимптотического закона распределения простых чисел. Общее, косвенное доказательство этих авторов (см. Эрдёш [6]) сделано общедоступным ван дер Корпутом и Нагеллем [17]. Мы приводим здесь слегка измененное конструктивное доказательство Сельберга (Сельберг [22]).

Развитая в 1920 году Вигго Бруном в высшей степени оригинальная идея использования эратосфенова решета привела к созданию одного из сильнейших методов теории простых чисел, не лишившегося своей продуктивности и сегодня. Изложенный нами метод Бруна в равной мере пригоден для вывода оценок сверху и снизу, тогда как новый метод решета Сельберга, на который ввиду недостатка места мы можем лишь сослаться, пригоден только при оценках сверху, но зато привел здесь к наилучшим возможным результатам.

Различные господа поддержали меня сообщениями и присылкой работ. Моя благодарность в первую очередь относится к Н. Г. В. Х. Бигеру (Амстердам), В. Бруну (Осло), П. Эрдёшу (Лос-Анжелос), Х. Мейеру (Цюрих), Б. ван дер Полю (Гент), А. Реньи (Будапешт), Д. Риччи (Милан), Х. Е. Рихерту (Геттинген), А. Сельбергу (Принстон), В. Серпинскому (Варшава). За побуждение к составлению этой книги и многочисленные ценные дискуссии сердечно благодарю издателя этой книги, моего коллегу Л. Лохер-Эрнста.

Цюрих, апрель 1953 г.

Эрнст Трост

I. ОСНОВНЫЕ ПОЛОЖЕНИЯ И ПРЕДВАРИТЕЛЬНЫЙ ОБЗОР

1. Делимость. Элементарная теория чисел занимается в первую очередь натуральными числами 1, 2, 3,... Присоединив нуль и целые отрицательные числа, получим область всех целых чисел, в которой неограниченно выполнимы операции сложения, вычитания и умножения. Для деления это не так, поэтому понятие делимости играет важную роль. Если натуральное число a представимо в виде произведения $a=dd'$, где d и d' — натуральные числа, то d называется делителем a. В таких случаях употребляют обозначение $d\,|\,a$. d' называется дополнительным к d делителем a. Каждое a имеет тривиальные делители $1, a$.

Чтобы проверить, имеет ли место $d\,|\,a$, проведем деление $a:d$ и получим представление $a=qd+r$, где $q\geqslant 0$ — частное и $0\leqslant r\leqslant d-1$ — остаток. Случай $r=0$ характерен для $d\,|\,a$. Частное может быть также записано в форме $q=[a/d]$, причем $[\alpha]$ для положительного вещественного α обозначает наибольшее целое число $\leqslant\alpha$ [1]).

2. Простые числа. Натуральное число $p\neq 1$ называется простым [2]), если оно не имеет никаких нетривиальных делителей. Число 1 целесообразно не считать простым, так как каждое целое число делится на 1 в сколь угодно большой степени. Таким образом, последовательность простых чисел начинается числами 2, 3, 5, 7, 11, 13, 17, 19, 23, 29,...; 2 — единственное четное простое.

Легко видеть, что каждое $a>1$ имеет по крайней мере один простой делитель $p\,|\,a$. Действительно, наименьший де-

---

[1]) $[6,78]=6$, $[5]=5$, $[0{,}33]=0$. Легко убедиться в справедливости правил $[[m]:n]=[m:n]$, $[[m:n]:s]=[m:ns]$, $[(m_1+m_2):n]=[m_1:n]+[m_2:n]+0$ или 1.

[2]) p, p_i, p' и т. д. всегда в дальнейшем будут обозначать простые числа, а маленькие латинские буквы всегда будут обозначать целые числа.

литель $p \neq 1$ числа a обязательно должен быть простым, так как в противном случае он сам имел бы нетривиальный делитель, меньший чем p, что противоречит минимальности p.

Докажем теперь фундаментальную теорему элементарной теории чисел, которая показывает, что простые числа являются элементами для мультипликативного построения натуральных чисел.

Теорема 1. *Каждое натуральное число n однозначно, если не учитывать порядок множителей, представимо в виде произведения простых чисел $n = p_1 p_2 \ldots p_r$ $(r \geqslant 1)$.*

Доказательство. Легко доказать существование такого разложения. Отделим в первую очередь наименьший делитель $p_1 \neq 1$, который по предыдущему замечанию является простым числом. В дополнительном делителе снова отделим простое число $p_2 \geqslant p_1$ и т. д.; так как дополнительные делители при этом все время убывают, то эта операция оборвется на простом числе p_r. Таким образом получаем так называемое каноническое разложение $n > 1$:

$$n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k} \quad (p_1 < p_2 < \ldots < p_k),\ e_i \geqslant 1. \qquad (1)$$

Однозначность разложения (1) получим следующим образом: или любое n разлагается однозначно, или существует наименьшее число m с двумя различными разложениями $m = p_1, p_2 \ldots \ldots p_s = q_1 q_2 \ldots q_t$ (q_i — простые числа). Каждое p_i отлично от всех q_k, так как если, например, $p_1 = q_1$, то $m \mid p_1$ имело бы два различных разложения, хотя число $m \mid p_1$ меньше, чем m.

Предположим, что q_1 — наименьшее простое, встречающееся в обоих разложениях m. Делением получим:

$$p_1 = q_1 Q_1 + r_1, \quad p_2 = q_1 Q_2 + r_2, \ldots, \quad p_s = q_1 Q_s + r_s$$

и отсюда перемножением

$$m = p_1 p_2 \ldots p_s = r_1 r_2 \ldots r_s + q_1 Q = q_1 q_2 \ldots q_t.$$

$R = r_1 r_2 \ldots r_s$ также делится на q_1. Так как $q_1 < p_i$, то $0 < R < m$, следовательно, R, как и все r_i, однозначно разложимо в соответствии с предположением. Так как $r_i < q_1$, то простой множитель q_1 не может входить в его разложение и R не делится на q_1. Итак, предположение о существовании числа m с двумя различными разложениями привело к противоречию, что и доказывает однозначность разложения.

Если n составлено из малых простых множителей, то его каноническое разложение легко найти. Нужно лишь перепробовать простые $p \leqslant \sqrt{n}$, так как каждое составное n содержит простой множитель $\leqslant \sqrt{n}$. При этом полезны таблицы множителей, такие, как таблицы Лемера [1]), в которых для любого $n < 10\,017\,000$, не делящегося на 2, 3, 5, 7, указан наименьший делитель.

В дальнейшем нам понадобится каноническое разложение числа $n!$ Очевидно, в $n!$ входят все $p \leqslant n$, так что нужно определить лишь соответствующие показатели e_p. Среди чисел 1, 2, 3, ..., n имеется $[n/p]$ кратных p, $[n/p^2]$ кратных p^2 и т. д. Точно $[n/p^r] - [n/p^{r+1}]$ чисел делятся на p^r, но не делятся на p^{r+1}. Таким образом,

$$\left.\begin{aligned} e_p = \sum r \left\{ \left[\frac{n}{p^r}\right] - \left[\frac{n}{p^{r+1}}\right] \right\} = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots; \\ n! = \prod_{p \leqslant n} p^{e_p}. \end{aligned}\right\} \qquad (2)$$

Ряд для e_p оборвется, как только будет $p^r > n$.

Разложение (1) дает полное представление о делителях n, число которых равно, очевидно, $(e_1 + 1)(e_2 + 1)\ldots(e_k + 1)$. Если в (1) все $e_i = 1$, то среди делителей n нет полных квадратов и n называется свободным от квадратов.

3. Количество простых чисел. Разложение (1) ничего не говорит о количестве различных p. Можно было бы подумать, что все n составлены из конечного числа p. То, что это не так, заметил уже Эвклид [2]), который показал, что для каждого простого числа есть бо́льшее.

Теорема 2. *Число простых чисел бесконечно.*

Доказательство. Допустим, что существует *наибольшее* простое число p и $P = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot p$ — произведение *всех* простых чисел. Число $P + 1$ не делится ни на одно из этих простых чисел, так как в остатке каждый раз получится 1. Поэтому $P+1$ или само является простым числом $> p$ или произведением простых чисел $> p$. Мы пришли к противоречию. Примеры: $2 \cdot 3 + 1 = 7$; $2 \cdot 3\ 5 + 1 = 31$; $2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30\,031 = 59 \cdot 509$.

---

[1]) D. H. Lehmer, Carnegie Inst. Publ. 105 (Вашингтон, 1909). История таблиц множителей очень интересна. См. D. H. Lehmer [13].

[2]) «Начала», книга IX, предл. 20.

Из доказательства Эвклида можно получить грубую оценку сверху для величины n-го простого числа p_n ($p_1 = 2$, $p_2 = 3, \ldots$). Выведем эту оценку по индукции. Предположим, что

$$p_1 \leqslant 2, \quad p_2 \leqslant 2^2, \quad p_3 \leqslant 2^{2^2}, \quad p_4 \leqslant 2^{2^3}, \ldots, \quad p_n \leqslant 2^{2^{n-1}}.$$

Так как p_{n+1} не больше наименьшего простого делителя числа $p_1 p_2 \ldots p_n + 1$, то

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

4. Решето Эратосфена является очень старым и простым методом для составления таблицы простых чисел, не превосходящих числа N. Пишут подряд числа от 2 до N. Число 2, как простое, оставляется, а все остальные четные числа вычеркиваются. Первое незачеркнутое число — это простое число 3. Далее, зачеркиваются все числа, кратные 3. Если таким методом найдены все $p \leqslant p_t$ и зачеркнуты все числа, кратные p_t, то первое следующее за p_t незачеркнутое число — это простое число p_{t+1}, так как оно не делится ни на одно $p \leqslant p_t$. Если найдено $p_t > \sqrt{N}$, то все еще незачеркнутые числа будут простыми, так как кратные $kp_t \leqslant N$ вследствие неравенства $k < \sqrt{N}$ уже вычеркнуты раньше, как кратные простым числам $< p_t$.

Пример. $N = 50$

	2	3	$\overline{4}$	5	$\overline{6}$	7	$\overline{8}$	$\overline{9}$	$\overline{10}$
11	$\overline{12}$	13	$\overline{14}$	$\overline{15}$	$\overline{16}$	17	$\overline{18}$	19	$\overline{20}$
$\overline{21}$	$\overline{22}$	23	$\overline{24}$	$\overline{25}$	$\overline{26}$	$\overline{27}$	$\overline{28}$	29	$\overline{30}$
31	$\overline{32}$	$\overline{33}$	$\overline{34}$	$\overline{35}$	$\overline{36}$	37	$\overline{38}$	$\overline{39}$	$\overline{40}$
41	$\overline{42}$	43	$\overline{44}$	$\overline{45}$	$\overline{46}$	47	$\overline{48}$	$\overline{49}$	$\overline{50}$

В качестве простых чисел < 50 получаем: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

5. Нерегулярности в распределении простых чисел. Просеивание позволяет предположить, что простые числа встречаются все реже по мере продвижения в ряду чисел. Во всяком случае видна большая нерегулярность, которая выглядит противоречащей всякой закономерности. Можно сразу увидеть, что в последовательности простых чисел встречаются

сколь угодно большие пропуски. Среди m последовательных чисел $(m+1)!+2$, $(m+1)!+3, \ldots, (m+1)!+m+1$ простых чисел нет, так как первое делится на 2, второе на 3, последнее на $m+1$. Позднее мы увидим (теорема 40), что имеются сколь угодно длинные цепи сколь угодно больших пропусков. Пропуск длиной 34 лежит между 1327 и 1361, а также между 8467 и 8501. Между 370 261 и 370 373 лежит пропуск длины 112.

С другой стороны, существуют простые числа p, $p+2$ с минимальным расстоянием 2. Примерами таких простых чисел-близнецов являются 41, 43; 2309, 2311; 10 016 957, 10 016 959. До сих пор неизвестно, является ли число таких пар простых близнецов конечным или бесконечным. Однако можно показать, что отношение числа близнецов $\leqslant N$ к числу всех $p \leqslant N$ стремится к нулю с ростом N (ср. § 68). Имеется 1224 пары близнецов до числа 100 000 и 8164 пары до 1 000 000. Для количества простых чисел соответственно имеем 9592 и 78 498. Существуют также тройки p, $p+2$, $p+6$ [1]) и четверки p, $p+2$, $p+6$, $p+8$. Примеры: 5, 7, 11; 10 014 491, 10 014 493, 10 014 497; 294 311, 294 313, 294 317, 294 319, 299 471, 299 473, 299 477, 299 479.

6. Функция распределения простых чисел. Изучение распределения простых чисел концентрируется в первую очередь на поисках функции $\pi(x)$, дающей количество простых чисел $\leqslant x$. Примеры: $\pi(1)=0$, $\pi(2)=1$, $\pi(20)=8$, $\pi(10^7)=664\,579$, $\pi(10^9)=50\,847\,478$, $\pi(p_n)=n$, если p_n — n-е простое число.

Хотя для функции $\pi(x)$ неизвестна никакая простая формула, можно, однако, сформулировать далеко идущие утверждения о ее порядке. Наиболее выразительным является закон распределения простых чисел, предсказанный еще Гауссом и впервые доказанный Адамаром и де ла Валле-Пуссеном, который гласит, что отношение $\pi(x)$ и функции $f(x)=x/\log x$ [2]) стремится к 1 с ростом x. Относительная ошибка $[\pi(x)-f(x)]/\pi(x)$, возникающая при замене $\pi(x)$ на $f(x)$, становится таким образом с ростом x сколь угодно малой. Этот центральный результат мы пока отметим как

---

[1]) Все три числа p, $p+2$, $p+4$ не могут быть простыми, так как одно из них делится на 3.

[2]) $\log x$ означает здесь, как и всегда в дальнейшем, натуральный логарифм.

Теорему 3. $\lim_{x\to\infty}\frac{\pi(x)\log x}{x}=1$ *или* $\pi(x)\sim\frac{x}{\log x}$ [1]).

Элементарное доказательство этой теоремы будет дано в главе VIII. Возможность доказательства этой теоремы без применения методов теории функций долгое время вызывала сомнения, поэтому открытие такого доказательства в 1948 г. Сельбергом и Эрдёшем явилось большой сенсацией.

7. Простые числа в арифметических прогрессиях. Нечетные p имеют вид $4n+1$ или $4n+3$. Методом Эвклида легко показать, что существует бесконечно много простых чисел обоих видов. Покажем это для вида $4n+3$. Положим $P=2^2\cdot 3\cdot 5\cdot\ldots\cdot p-1$, где в первый член входят в качестве множителей все простые числа $\leqslant p$, так что P будет вида $4n+3$. P не может состоять из простых множителей только вида $4n+1$, так как произведение в этом случае также имело бы вид $4n+1$. Таким образом, P делится на простое число вида $4n+3$, которое $>p$.

Аналогично получается, что существует бесконечно много простых чисел вида $6n+5$. За исключением 2 и 3, все простые числа имеют вид $6n+1$ или $6n+5$. $P=2\cdot 3\cdot\ldots\cdot p-1$ имеет вид $6n+5$ и не может состоять только из множителей вида $6n+1$, так как тогда и произведение имело бы такой вид. Таким образом, существует простое число вида $6n+5$, которое $>p$.

Эти факты являются частными случаями следующей знаменитой теоремы Дирихле (теорема об арифметической прогрессии):

Теорема 4. *Каждая арифметическая последовательность* $a+kd$ $(k=0, 1, 2, \ldots)$, *где* k *и* a *не имеют общих делителей, содержит бесконечно много простых чисел.*

Элементарное доказательство этой теоремы будет дано в главе VIII.

8. Общий наибольший делитель. Можно записать (1) также в форме бесконечного произведения, распространенного на все простые числа p_i $(i=1, 2, 3, \ldots)$. При этом показатель α_i простого числа p_i, не входящего в a, равен нулю.

---

[1]) Утверждение $f(x)\sim g(x)$ равносильно утверждению $\lim_{x\to 1} f(x)\,g(x)=1$. В таком случае говорят об асимптотическом равенстве.

$a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$, $\alpha_i \geqslant 0$ для $i \geqslant 1$, $\alpha_i > 0$ лишь для конечного числа i.

Очевидно, утверждение $d \mid a$ равнозначно неравенству $\delta_i \leqslant \alpha_i$ для всех i, если δ_i играет для d ту же роль, что α_i для a. Если a и b представлены в такой форме, а $\tau_i = \min(\alpha_i, \beta_i)$ обозначает наименьшее из чисел α_i и β_i для $\alpha_i \neq \beta_i$ и $\tau_i = \alpha_i$ для $\alpha_i = \beta_i$, то число $t = \prod_{i=1}^{\infty} p_i^{\tau_i}$ является делителем как для a, так и для b, т. е. общим делителем a и b. Так как τ_i для общего делителя увеличить нельзя, то t — общий наибольший делитель (о. н. д.) чисел a и b. Пишут $t = (a, b)$. Каждый другой общий делитель a и b является делителем t. Если $(a, b) = 1$, то a и b называются взаимно простыми. Если под $\mu_i = \operatorname{Max}(\alpha_i, \beta_i)$ понимать наибольшее из чисел α_i и β_i, то число $m = \prod_{i=1}^{\infty} p_i^{\mu_i}$ будет кратным как числу a, так и b. Так как μ_i для общего кратного уменьшить нельзя, то m — общее наименьшее кратное (о. н. к.) чисел a и b. Пишут $m = \{a, b\}$. Из равенства $ab = \prod p_i^{\alpha_i + \beta_i}$ следует полезная формула $\{a, b\} = ab/(a, b)$. О. н. д. (а заодно и о. н. к.) может быть найден без использования разложения на простые множители с помощью алгоритма Эвклида (последовательное деление).

9. Сравнения. Делением на $m > 0$ можно все $n > 0$ разбить на m классов, поместив в один класс все числа, имеющие один и тот же остаток. Каждый класс характеризуется одним из остатков 0, 1, 2, ..., $m - 1$. Два числа a и b одного и того же класса называются сравнимыми по модулю m. Пишут $a \equiv b \pmod m$. Такое сравнение равносильно утверждению: $a - b$ делится на m. В частности, равнозначны утверждения $m \mid a$ и $a \equiv 0 \pmod m$. Различают полную систему вычетов по $\bmod m$ и приведенную систему вычетов по $\bmod m$ в зависимости от того, рассматриваются ли все вычеты 0, 1, 2, ..., $m - 1$ или те из них, которые взаимно просты с модулем.

Как и в случае равенства, из сравнений $a \equiv a_1 \pmod m$, $b \equiv b_1 \pmod m$ следует, что $a \pm b \equiv a_1 \pm b_1 \pmod m$ и $ab \equiv a_1 b_1 \pmod m$. Если $f(x)$ многочлен от x с целыми коэффициентами, то из условия $a \equiv b \pmod m$ следует, что $f(a) \equiv f(b) \pmod m$.

В то время как сравнение можно умножать на любое целое число, делить можно лишь на числа, взаимно простые с модулем, как видно из примера: $5 \cdot 9 \equiv 5 \cdot 3 \pmod{10}$, $9 \not\equiv 3 \pmod{10}$. Из $na \equiv nb \pmod{m}$ следует лишь, что $a \equiv b \left[\mathrm{mod}\, m/(m, n)\right]$, так как в равенстве $a - b = km/n$ правая часть — целое число, кратное $m/(m, n)$.

В качестве приложения докажем важное сравнение, найденное в частном случае $m = p$ Ферма, а в общем случае Эйлером. $\varphi(m)$ обозначает количество чисел $< m$ и взаимно простых с m, в частности $\varphi(p) = p - 1$.

Теорема 5. *Если* $(a, m) = 1$, *то* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Доказательство. Если $a_1, a_2, \ldots, a_{\varphi(m)}$ — вычеты, взаимно простые с m, то также и числа $aa_1, aa_2, \ldots, aa_{\varphi(m)}$ взаимно просты с m и различны по $\mathrm{mod}\, m$, так как из $aa_i \equiv aa_k \pmod{m}$ следует $a_i \equiv a_k \pmod{m}$. Произведение чисел a_i сравнимо по $\mathrm{mod}\, m$ с произведением чисел aa_i и после деления обеих частей этого сравнения на $a_1 a_2 \ldots a_{\varphi(m)}$ получим доказываемое.

Если $f(x)$ — многочлен и существует такое x_0, что $f(x_0) \equiv 0 \pmod{m}$, то x_0 — решение сравнения $f(x) \equiv 0 \pmod{m}$. Вместе с x_0 решениями сравнения будут, естественно, и числа $x_0 + km$, принадлежащие тому же классу вычетов. Из теоремы 5 вытекает, что сравнение $ax \equiv b \pmod{m}$ при $(a, m) = 1$ имеет решение $x_0 = a^{\varphi(m)-1} b$.

Пример. $a = 3$, $m = 5$, $b = 2$, $\varphi(m) = 4$, $3^2 \equiv 4$, $3^3 \equiv 2$, $3^4 \equiv 1$, $x_0 = 2 \cdot 3^3 \equiv 4 \pmod{5}$, $3x \equiv 2 \pmod{5}$ имеет решение $x \equiv 4 \pmod{5}$.

Если многочлен $f(x) = a_0 x^n + \ldots + a_n$ имеет степень n и модулем является простое число p, то сравнение $f(x) \equiv 0 \pmod{p}$ имеет не более n несравнимых корней. Это максимальное число достигается по теореме 5 для сравнения $x^{p-1} \equiv 1 \pmod{p}$, для которого числа $x \equiv 1, 2, \ldots, p - 1$ являются несравнимыми решениями. В общем случае рассуждаем следующим образом: если сравнение $f(x) \equiv 0 \pmod{p}$ имеет решение x_1, то делением получим $f(x) = (x - x_1) f_1(x) + r_1$, где $r_1 \equiv 0 \pmod{p}$. Если $x_2 \not\equiv x_1$ еще одно решение, то должно быть $f_1(x_2) \equiv 0$, так что $f_1(x) = (x - x_2) f_2(x) + r_2$, где $r_2 \equiv 0$. Если имеется точно n несравнимых решений, то получаем тождество

$$f(x) = a_0 (x - x_1) \ldots (x - x_n) + pF(x). \qquad (3)$$

Так как $a_0 \not\equiv 0$, то из $f(x_0) \equiv 0$ следует (ввиду простоты модуля), что для некоторого $i \leqslant n$ $x_0 - x_i \equiv 0$, т. е. $x_0 \equiv x_i$, следовательно, новых решений больше нет.

10. Первообразные корни. Как показывает пример $2^3 \equiv 1 \pmod 7$, сравнение теоремы 7 может выполняться и для показателей $< \varphi(m)$. Если d — наименьший целый положительный показатель, для которого $a^d \equiv 1 \pmod m$, то говорят, что a по $\bmod m$ принадлежит показателю d. Так, 2 по $\bmod 7$ принадлежит показателю 3. Очевидно, для $(a, m) = 1$ $a^n \equiv 1 \pmod m$ тогда и только тогда, когда $d \mid n$; в частности, d является делителем $\varphi(m)$.

d степеней a, a^2, ..., a^d различны по $\bmod m$, так как из $a^r \equiv a^s$ и $d \geqslant r > s$ следует $a^{r-s} \equiv 1$ при $r - s < d$, что противоречит выбору d. Если a принадлежит по $\bmod m$ показателю $\varphi(m)$, то a называется первообразным корнем по $\bmod m$. Тогда $\varphi(m)$ степеней a, a^2, ..., $a^{\varphi(m)}$ представляют собой в точности $\varphi(m)$ вычетов, взаимно простых с m. Не для всякого модуля существуют первообразные корни, а лишь для $m = 2$, 4, p^e, $2p^e$ (p — нечетное простое число).

Для наших дальнейших целей будет достаточно установить существование первообразных корней для $m = p^e$.

Пусть сперва $m = p$, а $\psi(d)$ — количество вычетов, принадлежащих показателю d, делителю $p - 1$.

Если $\psi(d) > 0$ и f один из таких $\psi(d)$ вычетов, то $f, f^2, \ldots, f^d$ — несравнимые решения сравнения $x^d \equiv 1 \pmod p$ и по (3) других решений нет. Следовательно, все вычеты, принадлежащие показателю d, должны находиться среди степеней f^h ($h = 1, 2, \ldots, d$). Но f^h может принадлежать показателю d лишь тогда, когда $(d, h) = 1$. Действительно, если $(d, h) = t > 1$, $d = d_1 t$, $h = h_1 t$, то $(f^h)^{d_1} = (f^{h_1})^d \equiv 1 \pmod p$ и f^h принадлежит показателю $\leqslant d_1 < d$. Отсюда следует, что $\psi(d) \leqslant \varphi(d)$. Так как каждый вычет принадлежит некоторому определенному показателю d, то $p - 1 = \sum \psi(d) \leqslant \sum \varphi(d)$, где сумма распространена на все $d \mid p - 1$. Как мы увидим позднее в § 14 (17), $\sum \varphi(d) = p - 1$, откуда $\psi(d) = \varphi(d)$ для всех d. В частности, $\psi(p - 1) = \varphi(p - 1) > 1$, что и доказывает существование первообразных корней по $\bmod p$.

Пусть ρ — первообразный корень по $\bmod p$. По теореме 5 имеем $\rho^p - \rho = vp$. Покажем теперь, что $r = \rho + p(v - 1)$ является первообразным корнем по $\bmod p^e$ для любого $e \geqslant 1$.

Из $r^p \equiv \rho^p \pmod{p^2}$ следует, что

$$r(r^{p-1}-1) = r^p - r \equiv \rho^p - \rho - p(v-1) = p \pmod{p^2},$$

так что $r^{p-1} - 1 \not\equiv 0 \pmod{p^2}$ и по теореме 5 имеем представление

$$r^{p-1} = 1 + bp, \text{ где } b \not\equiv 0 \pmod{p}.$$

Так как

$$(1+bp^j)^p \equiv 1 + bp^{j+1} \pmod{p^{j+2}}, \quad j \geqslant 1,$$

то по индукции из частного случая $s = 0$ получим:

$$(r^{p-1})^{p^s} \equiv 1 + bp^{s+1} \pmod{p^{s+2}}, \quad s \geqslant 1. \tag{4}$$

Показатель d, которому принадлежит r по $\bmod p^e$, является делителем числа

$$\varphi(p^e) = p^{e-1}(p-1);$$

с другой стороны, d должно быть кратным $p-1$, так как r также является первообразным корнем по $\bmod p$. Таким образом, d имеет вид $(p-1)p^s$. Сравнение (4) показывает, что $s = e-1$ — наименьшее значение, для которого правая часть $\equiv 1 \pmod{p^e}$. Отсюда следует, что $d = \varphi(p^e)$ и r — первообразный корень по $\bmod p^e$.

Пример. 2 — первообразный корень по $\bmod 3$, $r = 2 + 3 \cdot 1 = 5$ — первообразный корень по $\bmod 3^e$. 5, $5^2 \equiv 7$, $5^3 \equiv 8$, $5^4 \equiv 4$, $5^5 \equiv 2$, $5^6 \equiv 1 \pmod 9$ — вычеты по $\bmod 9$.

3 — первообразный корень по $\bmod 4$, но для $m = 2^e$ $(e > 2)$ не существует первообразных корней. Зато для каждого нечетного $a > 0$ имеет место следующее представление с однозначно определяемым c

$$a \equiv (-1)^{\frac{a-1}{2}} 5^c \pmod{2^e}, \quad 0 \leqslant c < 2^{e-2}. \tag{5}$$

Для доказательства используем соотношение, справедливое для $m \geqslant 3$,

$$5^{2^{m-3}} = 1 + u \cdot 2^{m-1} \qquad (u \text{ — нечетное}),$$

которое легко доказывается с помощью индукции.

Так как показатель d, которому принадлежит 5 по $\bmod 2^e$, должен быть делителем числа $\varphi(2^e) = 2^{e-1}$, то $m = e+1$ и $d = 2^{e-2}$. Все 2^{e-2} значений 5^c в (5) таким образом несравнимы по $\bmod 2^e$. Все они, кроме того, $\equiv 1 \pmod 4$. В полной системе вычетов по $\bmod 2^e$ имеется 2^{e-2} вычетов $a \equiv 1 \pmod 4$ и

столько же вычетов $\equiv -1 \pmod 4$; остальные вычеты или $\equiv 0$, или $\equiv 2$, т. е. четные. Числа (5) поэтому совпадают с нечетными вычетами по $\bmod 2^e$.

Пример. $e=4$, $5^0 \equiv 1$, $5^1 \equiv 5$, $5^2 \equiv 9$, $5^3 \equiv 13 \pmod{16}$. Нечетные вычеты $1, 3 \equiv -13, 5, 7 \equiv -9, 9, 11 \equiv -5, 13, 15 \equiv -1$.

11. Квадратичные вычеты. Числа a, взаимно простые с $p>2$, распадаются на два класса, в зависимости от того, разрешимо или нет сравнение $x^2 \equiv a \pmod p$. Числа первого класса называются квадратичными вычетами по $\bmod p$, второго класса — квадратичными невычетами по $\bmod p$. Это свойство выражается символом Лежандра:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a \text{ — квадратичный вычет по } \bmod p, \\ -1, & \text{если } a \text{ — квадратичный невычет по } \bmod p. \end{cases}$$

Если ρ — первообразный корень по $\bmod p$, то, очевидно, каждое ρ^{2k} — квадратичный вычет, а каждое ρ^{2k+1} — квадратичный невычет. Действительно, сравнение $(\rho^t)^2 \equiv \rho^{2k+1}$ невозможно, так как отсюда вытекало бы сравнение $\rho^s \equiv 1$ с нечетным s, тогда как s должно быть кратно четному числу $p-1$. Таким образом, существует $(p-1)/2$ квадратичных вычетов и столько же невычетов по $\bmod p$. Легко устанавливается справедливость важной формулы

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right), \quad (a,\ p)=(b,\ p)=1. \tag{6}$$

Пример. Квадратичные вычеты по $\bmod 7$ — это 1, $2^2=4$, $3^2 \equiv 2$; невычеты — это 3, 5, 6.

По теореме 5 для $(a,\ p)=1$

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

Так как $-1 \not\equiv +1 \pmod p$, то для любого a или только первый, или только второй множитель делится на p. Для $a=\rho^{2k}$ это будет первый, а для $a=\rho^{2k+1}$ — второй множитель. Отсюда вытекает критерий Эйлера

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p. \tag{7}$$

Следствие:

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & \text{для } p \equiv 1 \pmod 4, \\ -1 & \text{для } p \equiv 3 \pmod 4. \end{cases} \tag{8}$$

Гаусс указал простую лемму, служащую для определения квадратичного характера числа a. Положим $p=2k+1$. p чисел $-k, -(k-1), \ldots, -1, 0, 1, 2, \ldots, k$ — это наименьшие по абсолютной величине вычеты по $\bmod p$. Каждому n соответствует один такой минимальный вычет по $\bmod p$. Он будет отрицательным, если наименьший неотрицательный вычет больше чем $\frac{p}{2}$. Пусть $r_1, r_2, \ldots, r_\mu, -r'_1, -r'_2, \ldots, -r'_\lambda$ — минимальные вычеты k чисел νa ($\nu=1, 2, \ldots, k$), причем $\mu+\lambda=k$, $0<r_i<\frac{p}{2}$, $0<r'_j<\frac{p}{2}$. Из $r_i=r'_j$ вытекает $a\nu_1 \equiv -a\nu_2$ или $\nu_1+\nu_2 \equiv 0 \pmod p$, что невозможно, так так $\nu_1<\frac{p}{2}$, $\nu_2<\frac{p}{2}$. Таким образом, все k чисел $r_i+r'_j$ различны и их совокупность — это числа $1, 2, \ldots, k$. Перемножением получим: $a^k k! \equiv (-1)^\lambda k! \pmod p$, так что вследствие (7)

$$\left(\frac{a}{p}\right)=(-1)^\lambda. \tag{9}$$

Пример. $p=19$, $a=5$, $k=9$. Минимальные по абсолютной величине вычеты для чисел $5, 10, 15, \ldots, 45$ — это $5, -9, -4, 1, 6, -8, -3, 2, 7$, так что $\lambda=4$, $\left(\frac{5}{19}\right)=(-1)^4=1$, $10^2 \equiv 5 \pmod{19}$.

Лемма Гаусса дает возможность определить квадратичный характер для $a=2$. В этом случае μ — число положительных четных чисел $<p/2$, т. е. $\mu=[p/4]$. Для λ получаются следующие выражения: если $p \equiv 1 \pmod 4$, то

$$\lambda=\frac{p-1}{2}-\frac{p-1}{4}=\frac{p-1}{4}=\left[\frac{p+1}{4}\right],$$

а если $p \equiv 3 \pmod 4$, то

$$\lambda=\frac{p-1}{2}-\frac{p-3}{4}=\frac{p+1}{4}=\left[\frac{p+1}{4}\right].$$

Отсюда вытекает:

$$\left(\frac{2}{p}\right)=\begin{cases}+1, & \text{если } p \equiv \pm 1 \pmod 8,\\ -1, & \text{если } p \equiv \pm 3 \pmod 8.\end{cases} \tag{10}$$

Из (6) и (8) получается далее

$$\left(\frac{-2}{p}\right)=\begin{cases}+1, & \text{если } p \equiv 1 \text{ или } 3 \pmod 8,\\ -1, & \text{если } p \equiv 1 \text{ или } -3 \pmod 8.\end{cases} \tag{11}$$

Важнейшее утверждение о квадратичных вычетах носит название закона взаимности. Этот закон дает

Теорема 6.

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \quad (p,\ q\text{ — нечетные простые числа}).$$

Доказательство. Пусть снова $p=2k+1$, $q=2l+1$. Для вычисления $\left(\frac{q}{p}\right)$ используем лемму Гаусса и положим

$$q\nu=\left[\frac{q\nu}{p}\right]p+\rho_\nu \quad (\nu=1, 2, \ldots, k). \tag{12}$$

Обозначим через $r_1, r_2, \ldots, r_\mu$ те вычеты ρ_ν, которые $<p/2$, а через $p-r'_1, p-r'_2, \ldots, p-r'_\lambda$ — те, которые $>p/2$. Просуммировав все равенства (12), получаем:

$$\frac{p^2-1}{8}q=\sum_{\nu=1}^{k}\left[\frac{q\nu}{p}\right]p+\sum r_i+\lambda p-\sum r'_j.$$

Так как требуется лишь выяснить четность или нечетность λ, то рассмотрим это равенство по mod 2. При выводе леммы Гаусса было установлено, что

$$\sum r_i+\sum r'_j=\sum_{\nu=1}^{k}\nu=\frac{p^2-1}{8},$$

так что вследствие $p\equiv q\equiv 1 \pmod 2$ получаем:

$$\lambda\equiv\bar{\lambda}=\sum_{\nu=1}^{k}\left[\frac{q\nu}{p}\right] \pmod 2.$$

Таким же образом получаем для показателя степени, соответствующего в формуле (9) символу $\left(\frac{p}{q}\right)$,

$$\lambda_1\equiv\bar{\lambda}_1=\sum_{\tau=1}^{l}\left[\frac{p\tau}{q}\right] \pmod 2.$$

Осталось показать еще, что $\bar{\lambda}+\bar{\lambda}_1\equiv kl \pmod 2$. Здесь имеет место даже равенство. Построим kl величин $q\nu-p\tau$, ни одна из которых не равна нулю. Среди них будет ровно

$\overline{\lambda}$ положительных. Действительно, при фиксированном ν ($\nu = 1, 2, \ldots, k$) будет $q\nu - p\tau > 0$ для $\tau = 1, 2, \ldots, \left[\frac{q\nu}{p}\right]$, т. е. для $\left[\frac{q\nu}{p}\right]$ значений τ, так что после суммирования по ν получим точно $\overline{\lambda}$ положительных значений. Так же при фиксированном τ будет $q\nu - p\tau < 0$ для $\nu = 1, 2, \ldots, \left[\frac{p\tau}{q}\right]$, так что имеется $\overline{\lambda}_1$ отрицательных величин. Теорема 6 доказана.

Закон взаимности показывает, что квадратичный характер p по mod q совпадает с квадратичным характером q по mod p, кроме случая, когда оба числа — и p и q — имеют вид $4n+3$. В этом случае характеры противоположны.

С помощью теоремы 6 символ Лежандра легко вычисляется.

Пример. $\left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) = -\left(\frac{13}{5}\right) = -\left(\frac{3}{5}\right) = -\left(\frac{5}{3}\right) = -\left(\frac{2}{3}\right) = +1$. Проба: $6^2 \equiv 10 \pmod{13}$.

Имея в виду использование этого в дальнейшем, выясним для каких простых модулей p числа ± 3 являются квадратичным вычетом или невычетом.

По теореме 6 и (7) имеем:

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} p \pmod 3.$$

Для выполнения равенства $\left(\frac{3}{p}\right) = 1$ нужно или чтобы $(p-1)/2$ было четным и $p \equiv 1 \pmod 3$, или чтобы $(p-1)/2$ было нечетным и $p \equiv -1 \pmod 3$. В первом случае $p = 12k+1$, а во втором $p = 12k-1$. Равенство $\left(\frac{3}{p}\right) = -1$ получается или при нечетном $(p-1)/2$ и $p \equiv 1 \pmod 3$, или при четном $(p-1)/2$ и $p \equiv -1 \pmod 3$. В первом случае $p = 12k-5$, а во втором $p = 12k+5$. Резюмируя, имеем:

$$\left(\frac{3}{p}\right) = \begin{cases} +1, & \text{если } p \equiv \pm 1 \pmod{12}, \\ -1, & \text{если } p \equiv \pm 5 \pmod{12}. \end{cases} \tag{13}$$

Из (7), (8) и теоремы 6 получаем далее

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right)$$

и отсюда

$$\left(\frac{-3}{p}\right)=\begin{cases}+1, & \text{если } p\equiv 1 \pmod 6,\\ -1, & \text{если } p\equiv -1 \pmod 6\ ^{1}).\end{cases} \tag{14}$$

Аналогично

$$\left(\frac{-7}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{7}{p}\right)=(-1)^{\frac{4(p-1)}{2}}\left(\frac{p}{7}\right)=\left(\frac{p}{7}\right),$$

так что

$$\left(\frac{-7}{p}\right)=\begin{cases}-1, & \text{если } p\equiv 3,\ \equiv 5,\ \equiv 6 \pmod 7,\\ +1, & \text{если } p\equiv 1,\ \equiv 2,\ \equiv 4 \pmod 7.\end{cases} \tag{15}$$

12. Теорема Акселя Туэ. В § 21 мы будем пользоваться следующей леммой Туэ. Пусть $n>1$ и e — наименьшее целое число $>\sqrt{n}$, тогда для каждого натурального числа a, взаимно простого с n, существуют два таких натуральных числа $x\leqslant e-1$, $y\leqslant e-1$, что $ay\equiv\pm x \pmod n$. Для доказательства используется принцип Дирихле, который утверждает, что при распределении N объектов между $N-1$ ящиками хотя бы в одном ящике должно находиться 2 объекта. Рассмотрим все e^2 чисел вида $ay+x$, где $x, y=0, 1, 2, \ldots, e-1$. Так как $e^2>n$, то хотя бы два таких числа должны иметь равные вычеты по mod n, так что существует сравнение $ay_1+x_1\equiv ay_2+x_2 \pmod n$. Отсюда следует, что $a(y_1-y_2)\equiv x_2-x_1 \pmod n$. Вследствие неравенств $|y_1-y_2|\leqslant e-1$, $|x_2-x_1|\leqslant e-1$ из равенства $x_1=x_2$ вытекает, что и $y_1=y_2$ и наоборот, так как в противном случае разность не будет делиться на n. Таким образом, $x_1\neq x_2$, $y_1\neq y_2$, а $y=y_1-y_2$ и $\pm x=x_1-x_2$ при подходящем выборе знака окажутся требуемыми числами.

Пример. $n=23$, $e=5$, $a=9$, $3a\equiv 4 \pmod{23}$ или $a_1=10$, $2a_1\equiv -3 \pmod{23}$.

II. ТЕОРЕТИКОЧИСЛОВЫЕ ФУНКЦИИ

13. Определение. Под теоретикочисловой функцией мы понимаем функцию, определенную для любого натурального числа n. Значения функции могут быть вещественными или комплексными. $f(n)$ называется мультипликативной, если из

[1]) Для нечетного p из сравнения $p\equiv\pm 1 \pmod 3$ следует $p\equiv\pm 1 \pmod 6$.

$(m, n)=1$ следует, что $f(mn)=f(m)\cdot f(n)$. Если это свойство справедливо для всех m, n, то функция называется вполне мультипликативной.

Сумма $\sum_{d|n} f(d)=F(n)$, распространенная по всем делителям d числа n (включая 1 и n), называется сумматорной функцией для $f(n)$. Если $f(n)$ мультипликативна, то мультипликативной будет и $F(n)$.

Для $(m, n)=1$ и $d \mid mn$ имеет место представление $d=d_1d_2$, где $d_1 \mid m$ и $d_2 \mid n$, $(d_1, d_2)=1$. Отсюда

$$F(mn)=\sum_{d|mn} f(d)=\sum_{\substack{d_1|m\\ d_2|n}} f(d_1d_2)=$$
$$=\sum_{d_1|m} f(d_1)\sum_{d_2|n} f(d_2)=F(m)F(n).$$

14. φ-функция Эйлера. Символом $\varphi(n)$ для $n\geqslant 1$ обозначают количество чисел $\leqslant n$, взаимно простых с n.

Пример. $\varphi(1)=1$, $\varphi(7)=6$, $\varphi(10)=4$.

Покажем в первую очередь, что $\varphi(n)$ мультипликативна. Пусть $(m, n)=1$. Если в выражении $mq+r$ r пробегает числа 0, 1, 2, ..., $m-1$, а q — числа 0, 1, 2, ..., $n-1$, то мы получим все неотрицательные целые числа $<mn$ без повторений. Число $mq+r$ взаимно просто с m тогда и только тогда, когда $(r, m)=1$. Существует $\varphi(m)$ таких r. Если r_1 одно из них, то различные по mod n числа r_1, $m+r_1$, $2m+r_1$, ..., $(n-1)m+r_1$ образуют полную систему вычетов по mod n. Среди этих чисел точно $\varphi(n)$ взаимно простых с n, т. е. взаимно простых с mn. Всего получаем $\varphi(m)\varphi(n)$ чисел, взаимно простых с mn.

Для вычисления $\varphi(n)$ теперь достаточно уметь вычислять эту функцию для степени простого числа p^e. Так как только числа kp $(1\leqslant k\leqslant p^{e-1})$ не взаимно просты с p^e, то $\varphi(p^e)=p^e-p^{e-1}$. Отсюда

$$\varphi(n)=\prod_i \varphi(p_i^{e_i})=n\prod_{p|n}\left(1-\frac{1}{p}\right),\quad n=\prod_i p_i^{e_i}. \qquad (16)$$

Для сумматорной функции имеем:

$$\sum_{d|n}\varphi(d)=\prod_i\{1+\varphi(p_i)+\varphi(p_i^2)+\ldots+\varphi(p_i^{e_i})\}=$$
$$=\prod_i p_i^{e_i}=n, \qquad (17)$$

Так как при перемножении скобок получим точно все значения $\varphi(d)$.

15. Функция Мебиуса $\mu(n)$, которая в дальнейшем окажется особенно важной, определена следующими равенствами:

$$\mu(1)=1,\quad \mu(n)=\begin{cases} 0 \text{ для } n, \text{ делящихся на квадрат,} \\ (-1)^k \text{ для } n=p_1 p_2 \dots p_k \ (p_i\neq p_j). \end{cases}$$

Примеры. $\mu(12)=0$, $\mu(15)=1$, $\mu(30)=-1$, $\mu(n)$, очевидно, мультипликативна. Для сумматорной функции имеем:

$$\sum_{d|n}\mu(d)=\begin{cases} 1 \text{ для } n=1, \\ 0 \text{ для } n>1. \end{cases} \tag{18}$$

Доказательство. Для $n=p_1^{e_1} p_2^{e_2}\dots p_k^{e_k}$ $(k\geqslant 1)$

$$\sum_{d|n}\mu(d)=1+\sum_i \mu(p_i)+\sum_{i,j}\mu(p_i p_j)+\dots=$$
$$=1-k+\binom{k}{2}-\binom{k}{3}+\dots=(1-1)^k=0.$$

Важнейшим применением функции $\mu(n)$ является формула обращения Мебиуса, с помощью которой $f(n)$ следующим образом выражается через сумматорную функцию:

$$f(n)=\sum_{d|n}\mu(d)\,F\left(\frac{n}{d}\right),\qquad F(n)=\sum_{d|n}f(d). \tag{19}$$

Доказательство. Изменением порядка суммирования в двойной сумме получим:

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

Вследствие (18) внутренняя сумма последнего выражения не равна нулю лишь для $c=n$ (в этом случае она равна 1), так что двойная сумма сводится к члену $f(n)$, что и требовалось доказать.

В качестве примера можно снова получить (16) из (17) и (19)

$$\varphi(n)=n\sum_{d|n}\frac{\mu(d)}{d}=n\prod_{p|n}\left(1-\frac{1}{p}\right).$$

Для доказательства теоремы 4 мы используем в § 55 более общую формулу обращения[1]). Пусть $P(n)$ — вполне мультипликативная теоретикочисловая функция, для которой $P(1)=1$, а $f(x)$ — функция, определенная для всех вещественных $x>0$, принимающая вещественные или комплексные значения. Тогда

$$\text{из } g(x)=\sum_{n\leqslant x} P(n) f\left(\frac{x}{n}\right) \text{ следует } f(x)=$$

$$=\sum_{n\leqslant x} \mu(n) P(n)\ g\left(\frac{x}{n}\right). \tag{20}$$

Доказательство. Из уравнения, определяющего $g(x)$, следует

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

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

Положим $c=mn$, тогда из (18)

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

16. Функция Мангольдта обозначается символом $\Lambda(n)$. Она имеет значение $\log p$, если n — простое число p или степень простого числа p, а в остальных случаях ее значение — нуль:

$$\Lambda(n)=\log p, \text{ если } n=p^m;\ \Lambda(n)=0, \text{ если } n\neq p^m.$$

Нам будут нужны следующие свойства $\Lambda(n)$:

$$\sum_{d\mid n} \Lambda(d)=\log n, \tag{21}$$

$$\Lambda(n)=\sum_{d\mid n} \mu(d) \log\frac{n}{d}. \tag{22}$$

Очевидно, имеем:

$$\sum_{d\mid n} \Lambda(d)=\sum_{p^\alpha\mid n} \log p=\sum e_p \log p=\log n,$$

[1]) См. Shapiro [25], S. 232.

где p^α пробегает все степени простых, входящие в n, а p входит в n с показателем e_p. (22) следует из (21) с помощью формулы обращения Мебиуса (19).

17. Характеры. Пусть k — натуральное число. Теоретико-числовая функция $\chi(a)$ называется *характером* по mod k, если она обладает следующими четырьмя свойствами:

A. $\chi(a)=0$, если $(a, k)\neq 1$; B. $\chi(1)\neq 0$;

C. $\chi(ab)=\chi(a)\chi(b)$; D. $\chi(a)=\chi(b)$, если $a\equiv b \pmod k$.

Характер, определенный равенством $\chi_1(a)=1$ для всех a, взаимно простых с k, называется *главным характером* по mod k. Очевидно, что при любых возможных определениях $\chi(a)$ всегда $\chi(1)=1$, так как по свойству C $\chi(1)\chi(1)=\chi(1)$, а по свойству B обе части можно разделить на $\chi(1)$. Из свойств C и D и теоремы 5 для $(a, k)=1$ получаем $\{\chi(a)\}^{\varphi(k)}=\chi(a^{\varphi(k)})=1$, следовательно, $\chi(a)$ является корнем из 1 степени $\varphi(k)$ и может принимать таким образом комплексные значения.

Примеры характеров ($i=\sqrt{-1}$):

$k=3$: $\chi(0)=0$, $\chi(1)=1$, $\chi(2)=-1$;

$k=4$: $\chi(0)=0$, $\chi(1)=1$, $\chi(2)=0$, $\chi(3)=-1$;

$k=5$: $\chi(0)=0$, $\chi(1)=1$, $\chi(2)=i$, $\chi(3)=-i$, $\chi(4)=-1$.

Покажем теперь, что для любого $d>0$, $(d, k)=1$ и $d\not\equiv 1 \pmod k$ существует такой характер χ по mod k, для которого $\chi(d)\neq 1$.

Пусть каноническое разложение k имеет вид $k=\prod p^e$ $p>2$. По § 10 существует первообразный корень r по mod p^e, так что при $(a, k)=1$ будет $a\equiv r^t \pmod{p^e}$, $0\leqslant t<\varphi(p^e)=s$, где t однозначно определяется числом a. Теперь характер $\chi(a)$ можно определить с помощью первообразного[1]) корня степени s из единицы

$$\rho=e^{\frac{2\pi i}{s}}=\cos\frac{2\pi}{s}+i\sin\frac{2\pi}{s},$$

если положить $\chi(a)=\rho^t$, для $(a, k)=1$ и $\chi(a)=0$ в противном случае. Условия B, C, D теперь выполняются:

[1]) $\rho^s=1$, но $\rho^n\neq 1$ для $0<n<s$.

B: $\chi(1)=\rho^0=1$; C: если $(a', k)=1$, $a'\equiv r^t \pmod{p^e}$, то $aa'\equiv r^{t+t'} \pmod{p^e}$ и $\chi(a)\chi(a')=\rho^{t+t'}=\chi(aa')$; D: из $a\equiv a' \pmod{k}$ следует $a\equiv a' \pmod{p^e}$, так что $t=t'$ и $\chi(a)=\chi(a')$.

Если $d\not\equiv 1 \pmod{k}$, то для характера, определенного таким образом, очевидно, будет $\chi(d)\neq 1$, так как ρ — первообразный корень из единицы.

Теперь осталось установить существование таких характеров для $k=2^e$, где $e>2$, так как для 2 и 4 первообразные корни существуют. Каждому $a=2n+1$ вследствие (5) соответствует некоторое c и характер в этом случае мы можем определить равенствами $\chi(2n)=0$, $\chi(2n+1)=\rho^c$, где $\rho=e^{2\pi i/s}$, $s=2^{e-2}$. A, B и D выполняются тривиальным образом.

Для доказательства C заметим, что из $(a-1)(a'-1)\equiv 0 \pmod 4$ для нечетных a, a', следует

$$\frac{a-1}{2}+\frac{a'-1}{2}\equiv\frac{aa'-1}{2} \pmod 2 \tag{23}$$

и отсюда

$$aa'\equiv(-1)^{\frac{aa'-1}{2}}5^{c+c'} \pmod{2^e} \quad \text{или} \quad \chi(a)\chi(a')=\chi(aa').$$

Для определенного таким образом характера $\chi(a)=1$ лишь для $c=0$, а в этом случае $a\equiv(-1)^{\frac{a-1}{2}} \pmod{2^e}$. Итак, если $d\equiv 1 \pmod 4$ и $\not\equiv 1 \pmod{2^e}$, то наверняка $\chi(d)\neq 1$. Для $d\equiv -1 \pmod 4$ определяем характер равенствами $\chi_0(2n+1)=(-1)^n$, $\chi_0(2n)=0$, так что $\chi_0(d)=0$. То, что $\chi_0(d)$ является характером, непосредственно следует из (23).

Таким образом, для любого числа $d\not\equiv 1 \pmod k$ можно выбрать такой характер (определенный для всех n), чтобы было $\chi(d)\neq 1$.

Так как характер χ по mod k полностью определяется $\varphi(k)$ значениями $\chi(n)$ $[1\leqslant n\leqslant k,\ (n, k)=1]$, каждое из которых является одним из $\varphi(k)$ корней степени $\varphi(k)$ из единицы, то различных характеров по mod k не более чем $\varphi(k)^{\varphi(k)}$. [Число распределений $\varphi(k)$ элементов по $\varphi(k)$ классам.] Таким образом, количество Z характеров по mod k конечно.

Теперь мы в состоянии установить для характеров некоторые важные соотношения, которые будут использованы позднее при доказательстве теоремы 4:

1. Пусть a пробегает полную систему вычетов по mod k, тогда

$$\sum_a \chi(a) = \begin{cases} \varphi(k) & \text{для } \chi = \chi_1, \\ 0 & \text{для } \chi \neq \chi_1. \end{cases} \tag{24}$$

Доказательство. Достаточно доказать вторую часть. Для $\chi \neq \chi_1$ существует такое натуральное взаимно простое с k число b, для которого $\chi(b) \neq 1$. Вместе с a полную систему вычетов по mod k пробегает и ab, так что $\sum \chi(a) = \sum \chi(ab) = \chi(b) \sum \chi(a)$. Так как $\chi(b) \neq 1$, то $\sum \chi(a)$ должна обращаться в нуль.

2. Пусть a — фиксированное натуральное число, а χ_j пробегает все Z характеров по mod k, тогда

$$\sum_j \chi_j(a) = \begin{cases} Z, & \text{если } a \equiv 1 \pmod{k}, \\ 0, & \text{если } a \not\equiv 1 \pmod{k}. \end{cases} \tag{25}$$

Доказательство. В первом случае $\chi_j(a) = 1$ для всех j. Для $(a, k) \neq 1$ вторая часть (25) справедлива, так как в этом случае $\chi_j(a) = 0$. Таким образом, осталось теперь предположить $(a, k) = 1$, $a \not\equiv 1 \pmod{k}$. В этом случае, как показано выше, существует характер χ_s, для которого $\chi_s(a) \neq 1$. Произведение $\chi_s(a)\chi_j(a)$ вместе с $\chi_j(a)$ пробегает все Z характеров, так как из равенства $\chi_s(a)\chi_i(a) = \chi_s(a)\chi_j(a)$ следует $\chi_j(a) = \chi_i(a)$, поскольку $\chi_s(a) \neq 0$. Отсюда вытекает равенство $\sum_j \chi_j(a) = \sum_j \chi_j(a)\chi_s(a) = \chi_s(a) \sum_j \chi_j(a)$ и так как $\chi_s(a) \neq 1$, то сумма $\sum_j \chi_j(a)$ должна обращаться в нуль. Просуммировав по всем a и χ и изменив порядок суммирования, получаем:

$$Z = \sum_a \sum_\chi \chi(a) = \sum_\chi \sum_a \chi(a) = \varphi(k). \tag{26}$$

3. Пусть $(t, k) = 1$ и $\overline{\chi}(t) = 1/\chi(t)$ — число, комплексно сопряженное с $\chi(t)$, которое, очевидно, также является характером. Тогда

$$\sum_j \chi_j(a)\overline{\chi}_j(t) = \begin{cases} \varphi(k), & \text{если } a \equiv t \pmod{k}, \\ 0, & \text{если } a \not\equiv t \pmod{k}. \end{cases} \tag{27}$$

Доказательство. В соответствии с § 9 мы можем выбрать такое натуральное s, чтобы было $st \equiv 1 \pmod{k}$. Тогда

$$\chi(s)\chi(t) = \chi(st) = 1, \quad \text{или} \quad \chi(s) = \overline{\chi}(t).$$

Теперь

$$\sum_j \chi_j(a)\,\overline{\chi}_j(t) = \sum_j \chi_j(a)\,\chi_j(s) = \sum_j \chi_j(as),$$

где последняя сумма вследствие (25) и (26) для $as \equiv 1 \pmod k$ принимает значение $\varphi(k)$, а в противном случае обращается в нуль. Доказательство завершается умножением сравнения $as \equiv 1 \pmod k$ на t.

III. ОБЩИЕ КРИТЕРИИ ПРОСТЫХ ЧИСЕЛ

18. Постановка задачи. Под критерием простых чисел понимаем теоретикочисловое свойство, которое присуще лишь простым числам и наличие которого может быть установлено независимо от предварительной проверки простоты числа. Простым примером является соотношение

$$\sum_{m \geqslant 1} \left\{ \left[\frac{n}{m}\right] - \left[\frac{n-1}{m}\right] \right\} = 2, \tag{28}$$

которое справедливо тогда и только тогда, когда n является простым числом. Так как слагаемые равны 1, если m делитель n, и равны нулю, если это не так, то сумма (конечная) представляет собой число $d(n)$ делителей n, а равенство $d(n) = 2$ характеризует простые числа. Естественно, (28), как и многие другие критерии, не пригодно для практических целей.

19. Теорема Вильсона. Следующая теорема, впервые доказанная в 1770 г. Варингом и приписанная им Д. Вильсону (1741—1793), представляют собой, пожалуй, наиболее известный критерий простоты числа.

Теорема 7. *Натуральное чцело $n > 1$ тогда и только тогда является простым, когда* $(n-1)! + 1 \equiv 0 \pmod n$.

Доказательство. По теореме 5 $x^{p-1} - 1 \equiv 0 \pmod p$ имеет $p-1$ решений $1, \ldots, p-1$, так что вследствие (3)

$$x^{p-1} = (x-1)(x-2)\ldots(x-p+1) + pF(x).$$

Положим $x = 0$, тогда $(p-1)! \equiv -1 \pmod p$. Если же n составное, то оно содержит простой множитель $q < n$. q является делителем $(n-1)!$, так что $(n-1)! + 1$ не делится на q, а значит, и на n.

В качестве следствия Клементом [4] доказана красивая

Теорема 8. *Числа n и $n+2$ тогда и только тогда являются простыми близнецами, когда* $4[(n-1)! + 1] + n \equiv 0 \pmod{n(n+2)}$, $n > 1$.

Доказательство. Если это условие выполнено, то так как $n \neq 2$ или 4, должно быть $(n-1)! + 1 \equiv 0 \pmod{n}$, следовательно по теореме 7 n — нечетное простое число. Так как $n \equiv -2 \pmod{n+2}$, то $(n+1)! \equiv 2(n-1)! \pmod{n+2}$. Отсюда следует

$$0 \equiv 4[(n-1)! + 1] + n \equiv 2(n+1)! + 2 = 2[(n+1)! + 1] \pmod{n+2}, \quad (29)$$

так что по теореме 7 простым числом является и $n+2$. Предположим, наоборот, что n и $n+2$ — простые числа, тогда $4[(n-1)! + 1] + n$ делится по теореме 7 на n, а вследствие (29) на $n+2$, так что делится и на $n(n+2)$.

20. Обращение теоремы Ферма. Непосредственное обращение теоремы 5 ошибочно, так как сравнение $a^{n-1} \equiv 1 \pmod{n}$ может иметь место и для составных n.

Пример. $341 = 11 \cdot 31$, $2^{10} = 1024 \equiv 1 \pmod{341}$, $(2^{10})^{34} = 2^{340} \equiv 1 \pmod{341}$. Лемер и Поулет составили таблицы, содержащие все составные $n_0 \leqslant 10^8$, для которых $2^{n_0-1} \equiv 1 \pmod{n_0}$. Существует бесчисленное множество таких показателей n_0, так как для $n_1 = 2^{n_0} - 1$, вследствие

$$n_1 - 1 = 2(2^{n_0-1} - 1) = 2qn_0,$$

имеем:

$$2^{n_1-1} - 1 = 2^{2qn_0} - 1 = (2^{n_0} - 1)(2^{(2q-1)n_0} + \ldots + 1) \equiv 0 \pmod{n_1}.$$

Если $n_0 = uv$ — составное, то

$$n_1 = 2^{uv} - 1 = (2^u - 1)(2^{(v-1)u} + \ldots + 1)$$

также составное. В качестве следующего составного решения сравнения $2^{n-1} \equiv 1 \pmod{n}$ можно взять $n = 2^{n_1} - 1$ и т. д. (Steuerwald [28]).

Существуют даже составные числа m (числа Кармайкла), для которых $a^{m-1} \equiv 1 \pmod{m}$ для каждого a, взаимно простого с m. Необходимым и достаточным для этого является выполнение условия $m - 1 \equiv 0 \pmod{p_i - 1}$ для всех $p_i \mid m$ [1]).

Пример. $m = 561 = 3 \cdot 11 \cdot 17$.

---

[1]) Ср. Ore [18], S. 331.

Один из критериев простого числа дает

Теорема 9. *Если существует такое число a, взаимно простое с n, что $a^{n-1} \equiv 1 \pmod n$, но $a^{\frac{n-1}{p}} \not\equiv 1 \pmod n$ для любого простого делителя p числа $n-1$, то n — простое число.*

Доказательство. Так как каждый нетривиальный делитель t числа $n-1$ входит в один из «наибольших» делителей $(n-1)/p$, то из предположения теоремы следует, что также $a^t \not\equiv 1 \pmod n$, так как в противном случае существовало бы p, для которого было бы $a^{\frac{n-1}{p}} \equiv 1 \pmod n$. Если a принадлежит показателю d (§ 10), то $a^d \equiv 1 \pmod n$ и d должно быть делителем $n-1$, что возможно лишь для $d = n-1$. Таким образом, $n-1$ является делителем $\varphi(n)$. Вследствие (16) для составных n всегда $\varphi(n) < n-1$, так что n должно быть простым числом. Если, наоборот, $n = p$, то первообразный корень по mod p осуществляет условия теоремы 9.

Такая проверка простоты числа осуществима, если известны различные простые множители числа $n-1$ и если их не очень много. В качестве основания выберем небольшое число, например 2 или 3, а степени a^x заменим их вычетами по mod n.

Пример. $n = 101$, $n-1 = 100 = 2^2 \cdot 5^2$. Для mod 101 имеем $2^3 \equiv 8, 2^6 \equiv 64, 2^{12} \equiv 56, 2^{25} = 2 \cdot 2^{24} \equiv 2 \cdot 5 = 10, 2^{50} \equiv -1$, $2^{100} \equiv 1$. Так как $2^{50} \not\equiv 1$ и $2^{20} = (2^{10})^2 \equiv 14^2 \equiv 95 \not\equiv 1$, то 101 — простое число. Само собой разумеется, что n не простое число, если $a^{n-1} \not\equiv 1 \pmod n$.

Для практического исследования большого числа n, не имеющего специального вида, полезна следующая теорема Д. Х. Лемера[1]).

Теорема 10. *Если $a^{n-1} \equiv 1 \pmod n$, $a^{\frac{n-1}{p}} \equiv r \not\equiv 1 \pmod n$, где p — простой делитель $n-1$, и $(r-1, n) = \delta$, то все делители n, взаимно простые с δ, имеют вид $p^\alpha x + 1$, где $n-1$ делится точно на p^α $(\alpha \geqslant 1)$.*

Доказательство. Положим $n-1 = qp^\alpha = mp$. Если t — простой делитель n, не входящий в δ, и a по mod t принадлежит показателю τ, то из $a^{n-1} \equiv 1 \pmod t$ следует, что $n-1 \equiv 0 \pmod \tau$. Но τ не может делить m, так как в противном случае было бы $a^m \equiv r \equiv 1 \pmod t$ и, следовательно, t было бы делителем $r-1$ и n, т. е. вопреки предположению

[1]) См. указатель литературы в статье D. H. Lehmer'a [14].

t должно было бы входить в δ. Положим $\tau = n_1 p^\beta$, $(n_1, p) = 1$, $\beta \geqslant 0$. Так как $(n-1)/\tau = (qp^\gamma)/(n_1 p^\beta)$ — целое число и $(p, q) = 1$, то $\alpha \geqslant \beta$ и q/n_1 целое. С другой стороны, $m/\tau = (qp^{\alpha-1})/(n_1 p^\beta)$ — не целое, так что $\beta > \alpha - 1$. Отсюда $\alpha = \beta$, так что $\tau = n_1 p^\alpha$. Так как по теореме 5 $a^{t-1} \equiv 1 \pmod t$, то $t - 1$ делится на τ, и t имеет вид $xp^\alpha + 1$. Так как произведение множителей такого вида имеет такую же форму, то теорема доказана.

Пример. $n = 341$, $n - 1 = 340 = 2^2 \cdot 5 \cdot 17$, $p = 5$, $(n-1)/p = 68$. Из сравнения $2^{10} = 1024 \equiv 1 \pmod{341}$ следует $2^{340} = (2^{10})^{34} \equiv 1 \pmod{341}$, $2^{68} \equiv 2^8 = 256 \pmod{341}$. Так как $(255, 341) = 1$, то $\delta = 1$ и все делители 341 имеют вид $5x + 1$. Действительно, $341 = 11 \cdot 31 = (5 \cdot 2 + 1)(5 \cdot 6 + 1)$.

Вычеты степени a^z по mod n для больших z можно сравнительно просто вычислить с помощью вычислительной машины.

Если предположения теоремы 10 выполнены и $\delta = 1$, а N составное, то оно должно иметь простой делитель $xp^\alpha + 1$ с $x < N^{1/2} p^{-\alpha}$. Если $p^\alpha > N^{1/2}$, то $x = 0$ и N — простое. Если p^α не намного меньше $N^{1/2}$, то нужно будет испытать лишь немногие значения x, число которых можно еще больше ограничить, исходя из специфических свойств N. Так, для нечетных p можно рассматривать лишь четные x и вообще пропускать $xp^\gamma + 1$, кратные небольшим простым числам, не входящим в N. Если, кроме p, известен еще один простой делитель q числа $N - 1$, для которого выполнены условия теоремы 10 при $\delta = 1$, то делители N имеют также вид $yq^\beta + 1$, где теперь должно быть $y = zp^\gamma$. Если $p^\gamma q^\beta > N^{1/2}$, то N — простое. Эту операцию можно продолжать.

Лемер приводит наряду с другими следующий пример:

$$N = \frac{10^{24}+1}{10^8+1} = 10^{16} - 10^8 + 1 = 9\,999\,999\,900\,000\,001,$$

$$N - 1 = 10^8 \frac{10^{16}-1}{10^8+1} = 2^8 \cdot 5^8 \cdot 3^2 \cdot 11 \cdot 73 \cdot 101 \cdot 137.$$

Имеем:

$$7^{\frac{N-1}{10}} \equiv 7\,128\,121\,476\,353\,673 = r \pmod N,$$

$$r^2 \equiv 7^{\frac{N-1}{5}} \equiv 428\,233\,546\,143\,224 \pmod N,$$

$$r^5 \equiv -1 \pmod N, \quad r^{10} \equiv 1 \pmod N.$$

Так как $(r^2 - 1, N) = 1$, что можно установить последовательным делением, то каждый делитель N имеет вид $x \cdot 5^8 + 1$.

Так как $(r^5 - 1, N) = 1$, то каждый делитель N имеет также вид $y \cdot 2^8 + 1$, следовательно, и вид $z \cdot 10^8 + 1$. Так как $10^8 > N^{1/2}$, то N — простое число.

Интересное применение теорема 10 нашла в 1951 году. Если p — простое число > 2 и $k < p/2$ — натуральное число, то $N = 2kp + 1$ будет простым числом, если $a^{2kp} \equiv 1 \pmod N$ и $a^{2k} \not\equiv 1_{2k} \pmod N$. Если $\delta = (r - 1, N)$, где $a^{2k} \equiv r \pmod N$, то все делители N, взаимно простые с δ, имеют вид $xp + 1$, так как $N - 1$ не делится на p^2. Так как $(xp + 1)(yp + 1) = (xyp + x + y)p + 1$, то произведение двух отличных от 1 множителей такого вида уже больше N.

Таким образом, существует разложение $N = 2kp + 1 = (xp + 1)d$, где d во всяком случае множитель, не взаимно простой с δ. Отсюда, однако, следует, что $d \equiv 1 \pmod p$, т. е. d имеет форму $yp + 1$. Таким образом, $d = 1$ и N является простым числом. По теореме 4 таких простых N существует бесконечно много.

Если взять в качестве p наибольшее известное простое число, которым в начале 1951 года еще было $2^{127} - 1$, то можно таким способом открыть новые, еще бóльшие простые числа. С помощью электронных вычислительных машин SEAC (Вашингтон) и EDSAC (Кембридж, Англия) Д. К. П. Миллер и Д. Д. Уилер нашли, что $2k(2^{127} - 1) + 1$ — простое число для $2k = 114$, 124, 388, 408, 498, 696, 738, 774, 780, 934, 978. Аналогичным образом они нашли наибольшее простое число 1951 года, число $180(2^{127} - 1)^2 + 1$, состоящее из 79 цифр.

21. Представление простых чисел квадратичными формами (Numeri idonei). Вследствие тождества $2n + 1 = (n + 1)^2 - n^2$ каждое нечетное число представимо в виде разности двух квадратов. Для любого нечетного простого числа такое представление, очевидно, однозначно, так как из

$$p = 2n + 1 = x^2 - y^2 = (x - y)(x + y)$$

следует

$$x - y = 1, \quad x + y = 2n + 1,$$

т. е.

$$x = n + 1, \quad y = n.$$

Покажем теперь, что и общая форма $ax^2 + by^2$, где a, b — натуральные числа, представляет простое число самое большее *одним* способом.

Из $p = ax^2 + by^2 = au^2 + bv^2$, где x, y, u, v — натуральные числа, $(x, y) = (u, v) = 1$, следует после исключения в

$$p(v^2 - y^2) = a(x^2v^2 - y^2u^2)$$

и так как $a < p$, то

$$yu \equiv \pm xv \pmod{p}. \tag{30}$$

Перемножив оба представления, получим:

$$p^2 = (axu \pm byv)^2 + ab(uy \mp vx)^2, \tag{31}$$

где можно взять или верхние, или нижние знаки. Если $uy = vx$, то вследствие $(u, v) = (x, y) = 1$ будет $u \mid x$ и $x \mid u$, т. е. $u = x$ и $v = y$. Если $uy \neq vx$, то из (30) и (31)

$$|uy \mp vx| = p, \quad a = b = 1, \quad axu \pm byv = 0,$$

так как иначе (31) не выполняется. Таким образом, $xu = \pm yv$ и $x = \pm v$, $y = \pm u$ и представление $p = x^2 + y^2$ $(a = b = 1)$ однозначно.

Если бы мы показали, что составные числа, имеющие *собственное* (т. е. с взаимно простыми x и y) представление $ax^2 + by^2$, допускают более одного представления, то мы получили бы критерий простых чисел, так как в этом случае простые числа характеризовались бы однозначным представлением. Представление $2x^2 + 3y^2 = 14$, имеющее единственное решение $x = 1$, $y = 2$, показывает, что это не выполняется для всех a, b.

Эйлер заметил, что $x^2 + dy^2$ $(d \geqslant 1)$ для специальных значений d однозначно и собственным образом представляет лишь простые числа. Коэффициенты d он назвал «подходящими» числами (Numeri idonei) и указал следующие 65 их значений: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848. Вывод критерия, с помощью которого Эйлер получил Numeri idonei, не является вполне обоснованным, однако Гаусс с помощью своей более тонкой теории квадратичных форм нашел эти же самые 65 чисел, тем самым их существование обосновано.

Хотя Эйлер продолжал свои вычисления за пределы 10 000, он не нашел больше Numeri idonei, что показалось ему пара-

доксальным. Только из новых глубоко лежащих результатов следует конечность количества подходящих чисел, однако не известно, является ли 1848 наибольшим из них.

Докажем, что $d=1, 2, 3, 7$ — «подходящие» числа. Необходимым условием для представимости p в форме x^2+dy^2, $(d, p)=1$ является разрешимость сравнения $x^2+dy^2\equiv 0 \pmod p$, $(x, y)=1$, которое можно также записать в форме

$$z^2\equiv (xy^{-1})^2\equiv -d \pmod p, \tag{32}$$

так как сравнение $yz\equiv x \pmod p$ вследствие $(y, p)=1$ имеет единственное решение z. Таким образом,— d должно быть квадратичным вычетом по $\mathrm{mod}\, p$.

Пусть это условие выполнено, тогда (32) разрешимо с z, взаимно простым с p. Пусть также $x_1<\sqrt{p}$, $y_1<\sqrt{p}$ удовлетворяют сравнению $zy_1\equiv\pm x_1 \pmod p$ (такие числа существуют по теореме Туэ, § 12). Тогда

$$y_1^2(z^2+d)\equiv x_1^2+dy_1^2=mp, \tag{33}$$

где $m\leqslant d$, так как $x_1^2<p$, $y_1^2<p$. Покажем, что для $d=1, 2, 3, 7$ следует положить $m=1$. Тогда для этих d все простые делители числа N, имеющего собственные представления в форме x^2+dy^2, сами будут представимы в такой форме [1]). Из тождества

$$(x_1^2+dy_1^2)(x_2^2+dy_2^2)=(x_1x_2\mp dy_1y_2)^2+d(x_1y_2\pm y_1x_2)^2 \tag{34}$$

вытекает, что вообще все делители N будут представимы в такой форме. Далее, из (34) вытекает, что произведение двух простых чисел, взаимно простых с d, представимо по крайней мере двумя различными способами. Эти два представления осуществляются вследствие $x_1y_1x_2y_2\neq 0$ выбором знаков [2]). Повторное применение (34) показывает, что любое составное N представимо более чем одним способом, так что простые числа характеризуются однозначным собственным представлением.

$d=1$. Сравнение (32) разрешимо лишь для $\left(\frac{-1}{p}\right)=1$, так что вследствие (8) должно быть $p\equiv 1 \pmod 4$. Из (33) немедленно следует, что $m=1$, чем и доказано существование представления. Таким образом, справедлива

---

[1]) Действительно, если разрешимо сравнение $x^2+dy^2\equiv 0 \pmod N$, то это сравнение разрешимо и по $\mathrm{mod}\, p$, где $p \mid N$. (*Прим. перев.*)

[2]) В случае $d=1$ можно предположить, что $x_1>y_1>0$, $x_2>y^2>0$, так что $(x_1x_2+y_1y_2)^2$ больше остальных трех квадратов.

Теорема 11. *Нечетное число вида* $4m+1$ *тогда и только тогда является простым, когда оно лишь единственным образом представимо в виде суммы двух взаимно простых квадратов.*

$d=2$. Из (32) следует $\left(\frac{-2}{p}\right)=1$, так что вследствие (11) $p\equiv 1$ или $3 \pmod 8$. В (33) теперь $m=1$ или 2, так что или $x^2+2y^2=p$, или $x^2+2y^2=2p$. Положим во втором случае $x=2x_1$, тогда $2x_1^2+y^2=p$, т. е. снова имеем представление требуемого вида. Этим доказана

Теорема 12. *Нечетное число вида* $8m+1$ или $8m+3$ *тогда и только тогда является простым, когда оно лишь единственным образом (собственно) представимо в виде* x^2+2y^2.

$d=3$. Из (32) следует $\left(\frac{-3}{p}\right)=1$, так что вследствие (14) $p\equiv 1 \pmod 6$. Теперь следует рассмотреть в (33) случаи $m=1, 2, 3$. Равенство $x^2+3y^2=2p$ невозможно, так как x и y должны быть нечетными, поскольку $p\neq 2$, а тогда $x^2+3y^2\equiv 0 \pmod 4$, что невозможно.

Если $3p=x^2+3y^2$, то, снова положив $x=3x_1$, получим: $p=3x_1^2+y^2$. Отсюда следует

Теорема 13. *Нечетное число вида* $6m+1$ *тогда и только тогда является простым, когда оно имеет лишь единственное собственное представление в виде* x^2+3y^2.

$d=7$. Здесь должно быть $\left(\frac{-7}{p}\right)=1$. По (15) $p\equiv 1$ или 9, или 11 (mod 14). В равенстве (33) следует исследовать случаи $m=1, 2, 3, 4, 5, 6, 7$.

Если $m=2$ или 6, то x и y оба должны быть нечетными, так что $x^2+7y^2\equiv 0 \pmod 8$, что невозможно. Для $m=4$ имеем или $x=2x_1$, $y=2y_1$, откуда получаем $x_1^2+7y_1^2=p$, или x и y оба нечетные, что приводит к тому же противоречию, что и выше. В случае $x^2+7y^2=3p$ будет $(y, 3)=1$, так как $p\neq 3$. Отсюда $-7\equiv (xy^{-1})^2 \pmod 3$, тогда как по (8) должно быть $\left(\frac{-7}{3}\right)=\left(\frac{-1}{3}\right)=-1$. Итак, случай $m=3$ невозможен и также отпадает случай $m=5$, так как вследствие (11) $\left(\frac{-7}{5}\right)=\left(\frac{-2}{5}\right)=-1$. В случае $x^2+7y^2=7p$ положим снова $x=7x_1$ и получим $y^2+7x_1^2=p$, чем и доказано существование представления. Таким образом, получается

Теорема 14. *Нечетное число вида* $14m+1, 14m+9$ *или* $14m+11$ *тогда и только тогда является простым, когда оно лишь единственным образом собственно представимо в виде* x^2+7y^2.

Естественно возникает вопрос, как установить единственность разложения для большого числа. Во всяком случае нужно будет использовать как можно большее подходящее число d. Принцип исследования иллюстрируется следующим примером.

$$N = 18\,518\,809 = 197^2 + 1848 \cdot 100^2 = x^2 + 1848\,y^2.$$

Имеем $y \leqslant (18\,518\,808/1848)^{1/2} \leqslant 100$. Рассмотрим прежде всего представление по mod 5. Сравнение $N \equiv x^2 + 3y^2 \equiv (\mathrm{mod}\ 5)$ допускает решение при квадратичных вычетах $x^2 \equiv 1, 4, 0$ по mod 5 лишь при $y \equiv 0$ или $y \equiv \pm 1$. Таким образом, числа $y = 5k \pm 2$ отпадают, но остается еще 60 возможных значений для y. По mod 13 имеем $N \equiv x^2 + 2y^2 \equiv 10$. Квадратичными вычетами являются числа 1, 4, 9, 3, 12, 10, 0. Отсюда $y^2 \not\equiv 1, 4, 9$, так что можно зачеркнуть числа $13k \pm 1$, $13k \pm 2$, $13k \pm 3$. Остается еще 24 числа. По mod 17 мы имеем квадратичные вычеты 1, 4, 9, 16, 8, 2, 15, 13, 0.

Сравнение $N \equiv x^2 - 5y^2 \equiv 12$ не разрешимо при $y^2 \equiv 9, 16, 2, 0$, так что отпадают числа $17k \pm i$ $(i = 3, 4, 6, 0)$, и остается испытать 19 значений y. Это количество можно свести к 12, если рассмотреть представление еще по mod 19. Теперь можно быстро убедиться в том, что $N - 1848\,y^2$ является квадратом лишь для $y = 100$, следовательно N — простое число.

22. Разложение на множители. В то время как небольшие составные числа можно раскладывать на множители с помощью таблиц простых чисел или таблиц множителей, разложение на множители больших чисел, выходящих за пределы таблиц, является проблемой, для решения которой не известно общего метода. Так, например, из критериев простоты числа известно, что $2^{128}+1$, $2^{256}+1$, $2^{257}-1$ — составные числа, но ни один из их делителей не известен. Наиболее эффективным является и сейчас метод представления N квадратичной формой, употреблявшийся еще Ферма и Эйлером. Встречающиеся при этом вычисления можно значительно сократить искусным использованием особенностей числа N [1]).

---

[1]) Подробное изложение можно найти у Менхена [16]. Ср. также Л. Эйлер, Opera omnia I_3 и I_4.

Метод Ферма относится к представлению N в виде разности двух квадратов. Пусть $N=ab$, $a\geqslant b$ — нечетное составное число, тогда имеем целочисленное представление $N=x^2-y^2$, $x=(a+b)/2$, $y=(a-b)/2$. В равенстве $x^2=N+y^2$ будет $x^2\geqslant N$, так что $x\geqslant\sqrt{N}$. Если z — наименьшее целое число $\geqslant\sqrt{N}$, то мы должны в последовательности чисел z^2-N, $(z+1)^2-N$, $(z+2)^2-N$, ..., $(z+k)^2-N$ отыскать квадрат. Это произойдет не позднее, чем при $z+k=(N+1)/2$. Последнее, однако, приводит к тривиальному разложению $N\cdot 1$.

Для составного $N=ab$ квадрат встретится раньше, так как $(a+b)/2<(N+1)/2$ для $b>1$. В качестве побочного результата получаем следующий старый [1]) критерий простого числа: N тогда и только тогда простое число, когда $N+k^2$ не является квадратом для $k=1, 2, \ldots, (N-3)/2$.

Практическое вычисление $(z+k)^2-N$ производится последовательным добавлением разностей $2z+1, 2z+3, 2z+5, \ldots$

Пример (Ферма). $N=2\,027\,651\,281$, $z=45030$.

$z^2-N=$ 49619	$(z+5)^2-N=$ 499 944	$(z+10)^2-N=$ 950 319
$2z+1=$ 90061	$2z+11=$ 90 071	$2z+21=$ 90 081
$(z+1)^2-N=$ 139 680	$(z+6)^2-N=$ 590 015	$(z+11)^2-N=$ 1 040 400 $=$
$2z+3=$ 90 063	$2z+13=$ 90 073	$=$ 1020^2
$(z+2)^2-N=$ 229 743	$(z+7)^2-N=$ 680 088	
$2z+5=$ 90 065	$2z+15=$ 90 075	
$(z+3)^2-N=$ 319 808	$(z+8)^2-N=$ 770 163	$x=45\,041$
$2z+7=$ 90 067	$2z+17=$ 90 077	$y=1020$
$(z+4)^2-N=$ 409 875	$(z+9)^2-N=$ 860 240	$a=x+y=46\,061$
$2z+9=$ 90 069	$2z+19=$ 90 079	$b=x-y=44\,021$

В этом случае к цели приходят сравнительно быстро, так как a и b мало отличаются друг от друга. Вследствие этого часто подходящее кратное числа N разлагается легче, чем само N. Установить, что число является квадратом будет легче, если иметь в виду, что квадраты могут последней парой знаков иметь лишь 00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96. Таким образом, в нашем примере следует испытывать лишь 499 944 и 1 040 400.

Рассмотренное в § 21 представление формой x^2+dy^2 ($d>0$) использовалось Эйлером для разложения на множители. Если для N существуют два различных представления, то N можно

[1]) А. С. де Монтферре, Corresp. math. phys. 5, 94—96 (1829). Жигмонди показал (Mh. Math. Phys. **5**, 123 (1894)), что $(N-3)/2$ можно заменить на $(N-9)/6$.

разложить на два множителя. Из $N=x_1^2+dy_1^2=x_2^2+dy_2^2$ следует именно

$$x_1^2-x_2^2=d(y_2^2-y_1^2) \text{ или } \frac{x_1-x_2}{y_2-y_1}=d\,\frac{y_2+y_1}{x_1+x_2}.$$

Сократив дроби, получим целые, отличные от нуля, числа u, v, s, t, $(u, v)=1$, такие, что

$$\left.\begin{array}{ll} a)\ x_1-x_2=dut, & b)\ y_2-y_1=vt, \\ c)\ y_2+y_1=us, & d)\ x_1+x_2=vs. \end{array}\right\} \tag{35}$$

Отсюда получаем $x_1=(dut+vs)/2$, $y_1=(us-vt)/2$ и

$$N=x_1^2+dy_1^2=\frac{1}{4}(v^2+du^2)(s^2+dt^2). \tag{36}$$

Если d четное, то вследствие предположения о нечетности N, числа x_1 и x_2 должны быть нечетными, так что по (35, d) хотя бы одно из чисел v, s четное. Если s (соответственно v) нечетное, то по (35, b, c) u (соответственно t) четное, так как y_1+y_2 и y_2-y_1 имеют одинаковую четность. В каждом случае, таким образом, одна из скобок в (36) делится на 4. Для нечетного dx_i и y_i $(i=1,2)$ имеют различную четность, так что $x_1\pm x_2$ и $y_1\pm y_2$ одновременно нечетные или четные. В первом случае u, v, s, t — нечетные и каждая из скобок в (36) — четная. Во втором случае из (35) вследствие $(u, v)=1$ следует, что s и t — четные, так что вторая скобка в (36) делится на 4. Таким образом, во всех случаях (36) дает нетривиальное разложение N.

Разыскивая представления N, снова можно использовать упрощения, упомянутые в методе Ферма, и часто количество случаев, подлежащих испытанию, допускает значительное сокращение.

Пример 1.

$$N=1\,000\,009=1000^2+3^2=972^2+235^2,$$
$$d=1,\ u=7,\ v=58,\ t=4,\ s=34,$$
$$N=(7^2+58^2)(2^2+17^2)=3413\cdot 293.$$

Пример 2.

$$N=13\,717\,421=761^2+7\cdot 1370^2=439^2+7\cdot 1390^2,$$
$$d=7,\ u=23,\ v=10,\ t=2,\ s=120,$$
$$N=(10^2+7\cdot 23^2)(60^2+7\cdot 1^2)=3803\cdot 3607.$$

IV. СПЕЦИАЛЬНЫЕ ПРОСТЫЕ ЧИСЛА

23. Постановка задачи. Были предприняты многочисленные попытки построить числовую функцию, принимающую во всех целых точках (или по крайней мере в бесконечной последовательности целых точек) значения, дающие бесконечную последовательность различных простых чисел. С помощью такой функции $P(n)$ можно было бы действительно вычислить, если и не все, то все же сколь угодно много простых чисел, если можно вычислить $P(n)$ для каждого n [1]).

Легко можно показать, что никакой многочлен, отличный от постоянной, с целыми коэффициентами не может для всех n, или для всех достаточно больших n, представлять простые числа. Для доказательства рассмотрим $y=f(x)=a_0x^k+a_1x^{k-1}+\ldots+a_k$, $a_0>0$. Для достаточно больших x_0 будет $y_0=f(x_0)>1$. Натуральные числа $f(ry_0+x_0)$, $r=0, 1, 2, \ldots$ все делятся на y_0, что видно из разложения членов $a_\nu(ry_0+x_0)^{k-\nu}$ по биному. Таким образом, существуют сколь угодно большие составные значения $f(n)$. Как мы увидим в § 26, даже для квадратичной функции существуют сравнительно длинные последовательности простых значений.

Естественно рассмотреть показательные функции типа $f(n)=a^n\pm b^n$, где a, b — целые. Здесь следует принять во внимание разложения

$$a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\ldots+ab^{n-2}+b^{n-1}), \quad (37)$$

$$a^{2n+1}+b^{2n+1}=(a+b)(a^{2n}-a^{2n-1}b+\ldots-ab^{2n-1}+b^{2n}). \quad (38)$$

Заменив в (37) a и b соответственно на a^m и b^m, увидим, что, кроме тривиальных исключений, число $a^{mn}-b^{mn}$ является составным. Простые числа могут появиться лишь при $a-b=1$ и простом показателе степени. Простейший случай $a=2$, $b=1$ приводит к простым числам вида $M_p=2^p-1$ (простые числа Мерсенна), которые мы рассмотрим в § 24. Из (38) следует, что a^m+b^m может быть простым числом лишь тогда, когда m не имеет нечетных простых делителей, т. е. является степенью числа 2. Для $a=2$, $b=1$ получаем простые числа

---

[1]) Функцию $f(n)=[n\sqrt{2}]$ можно, например, использовать лишь до тех пор, пока известно десятичное разложение для $\sqrt{2}$. Число $[1{,}414\ldots\cdot n]$ для $n>1000$ уже не определено, (так как $\sqrt{2}$ задан здесь только с тремя знаками после запятой).

вида $F_n = 2^{2^n} + 1$ (простые числа Ферма). Ферма полагал, что F_n является простым числом для всех n, однако Эйлер показал, что уже F_5 является составным (см. § 25).

Новые большие простые числа часто также находят вычеркиванием получаемых из (37) или (38) делителей составного $a^m \pm b^m$. Так, А. Ферье в 1951 г. нашел 44-значное число $(2^{148}+1)/17$. Далее, простым является число, состоящее из 23 единиц $(10^{23}-1)/9$.

24. Простые числа Мерсенна $M_p = 2^p - 1$ имеют особое значение вследствие их связи со знаменитой проблемой совершенных чисел. Число N называется совершенным, если оно равно сумме своих собственных делителей, т. е. если для суммы $\sigma(N)$ всех делителей будет $\sigma(N) = 2N$.

Пример. $6 = 1+2+3$. Эвклид доказал, что если $N = 2^t(2^{t+1}-1) = 2^t p$, где p — простое число, то N — совершенное число. Действительно,

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

Так как M_2, M_3, M_5, M_7 — простые числа, то получаем четные совершенные числа 6, 28, 496, 8128.

Эйлер заметил, что и, наоборот, каждое четное совершенное число N имеет форму, указанную Эвклидом. Для доказательства предположим, что $N = 2^t u$, где u — нечетное, является совершенным числом. Каждый делитель N имеет вид $2^\alpha \delta$, где $\delta \mid u$ и $0 \leqslant \alpha \leqslant t$. Отсюда упорядочиванием по степеням 2^α получается:

$$\sigma(N) = \sigma(u)(1+2+\ldots+2^t) = \sigma(u)(2^{t+1}-1) = 2N = 2^{t+1}u,$$

откуда, вследствие нечетности u, $\sigma(u)$ должно иметь вид: $d \cdot 2^{t+1}$, а $u = d(2^{t+1}-1)$. Если бы было $d \neq 1$, то имели бы

$$\sigma(u) > d + (2^{t+1}-1)d = d \cdot 2^{t+1},$$

так что $d = 1$ и u имеет делителями лишь 1 и $2^{t+1}-1$, т. е. является простым числом. До сих пор не известно, существуют ли нечетные совершенные числа.

Число M_p не для всех p является простым, как видно из примера $M_{11} = 2047 = 23 \cdot 89$. Мерсенн в 1664 г. для $p \leqslant 257$ указал все M_p, которые он считал простыми числами. Исследования в этой области, законченные лишь в последнее время, показали, что в пяти случаях Мерсенн ошибся. Сегодня из-

вестно, что M_p является простым числом для $p=2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$ и составным для всех остальных $p \leqslant 257$. С помощью электронной счетной машины SWAC (Калифорния) летом 1952 г. найдены новые простые числа Мерсенна M_{521} и M_{607}. Между M_{127} и M_{521} лежат 66 составных M_p.

Наконец, SWAC установила еще, что M_{1279} является простым числом. Это число имеет 386 знаков, тогда как открытое Лукасом в 1876 г. число M_{127}, которое в течение 75 лет было наибольшим известным простым числом, имеет лишь 39 знаков [1]).

Основой всех этих результатов является критерий для M_p, идущий в основном от Лукаса и весьма изящно доказанный Д. Х. Лемером [15] в следующей форме.

Теорема 15. *Число $M_p=2^p-1$, где p — нечетное простое, тогда и только тогда простое, когда M_p делит $(p-1)$-й член рекуррентной последовательности $s_1=4$, $s_2=14, \ldots, s_k=s_{k-1}^2-2$.*

Пример. $p=7$, $M_p=127$, $s_3 \equiv 67 \pmod{127}$, $s_4 \equiv 67^2-2 \equiv 42 \pmod{127}$, $s_5 \equiv 42^2-2 \equiv -16 \pmod{127}$, $s_6 \equiv 16^2-2=254 \equiv 0 \pmod{127}$. Условие теоремы 15 можно несколько ослабить. Для того чтобы M_p было простым числом, достаточно, очевидно, чтобы $s_{p-2} \equiv \pm 2^{\frac{p+1}{2}} \pmod{M_p}$, так как отсюда следует $s_{p-1} \equiv 2^{p+1}-2 = 2(2^p-1) \equiv 0 \pmod{M_p}$.

Подготавливая доказательство теоремы 15, положим $a=1+\sqrt{3}$, $b=1-\sqrt{3}$, так что $a+b=2$, $ab=-2$, $a-b=2\sqrt{3}$. Определим две последовательности целых чисел u_r и v_r равенствами $u_r=(a^r-b^r)/(a-b)$, $v_r=a^r+b^r$, так что $u_1=1$, $u_2=2$, $u_3=6$, $u_4=16, \ldots$, $v_1=2$, $v_2=8$, $v_3=20, \ldots$ Легко проверяются соотношения

$$2u_{r+s}=u_r v_s+v_r u_s, \tag{39}$$

$$(-2)^{s+1} u_{r-s}=u_s v_r-u_r v_s, \tag{40}$$

$$2v_{r+s}=v_r v_s+12u_r u_s, \tag{41}$$

$$u_{2r}=u_r v_r, \tag{42}$$

$$v_{2r}=v_r^2+(-2)^{r+1}, \tag{43}$$

$$v_r^2-12u_r^2=(-2)^{r+2}. \tag{44}$$

[1]) 386 знаков M_{1279}, так же как 770 знаков соответствующего совершенного числа, см. у Улера (Uhler) [30].

Пусть $p>3$ и $(u_\omega, p)=p$, но $(u_r, p)=1$ для $r<\omega$, т. е. w — наименьший индекс, для которого u_ω делится на p. Таким образом, простому числу p соответствует «ранг» ω; например, 11 имеет ранг 5. Мы увидим, что для каждого $p>3$ существует конечное ω.

Лемма 1. *Если ω — ранг числа p, то p входит в u_r тогда и только тогда, когда r кратно ω.*

Доказательство. Пусть $\mathfrak{M}$ — множество всех индексов r, для которых $u_r \equiv 0 \pmod p$. По (39) и (40) вместе с r и s в состав $\mathfrak{M}$ входят и $r \pm s$. Если ω наименьшее положительное число в $\mathfrak{M}$, то последовательным вычитанием ω получим $r - k\omega = 0$, так как для любого целого k число $r - k\omega$ входит в $\mathfrak{M}$ и не может находиться между 0 и ω. Таким образом, $r = k\omega$.

Лемма 2. $u_p \equiv \left(\frac{3}{p}\right) \pmod p$, $v_p \equiv 2 \pmod p$.

Доказательство. На основании (7) и того факта, что за исключением первого и последнего биномиальные коэффициенты p-й степени делятся на p, получаем:

$$u_p = \frac{1}{2\sqrt{3}}\{(1+\sqrt{3})^p - (1-\sqrt{3})^p\} = \sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k+1} 3^k \equiv$$

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

Так же получаем:

$$v_p = (1+\sqrt{3})^p + (1-\sqrt{3})^p = 2\sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k} 3^k \equiv 2 \pmod p.$$

Лемма 3. *Если ω — ранг p, то $\omega \leqslant p+1$.*

Доказательство. Достаточно показать, что $u_{p+1}u_{p-1}$ делится на p, так как тогда p будет входить в u_{p+1} или u_{p-1}.

Положим в (39) и (40) $r=p$ и $s=1$, тогда вследствие того, что $u_1=1$ и $v_1=2$,

$$2u_{p+1} = 2u_p + v_p,\ 4u_{p-1} = v_p - 2u_p)$$

---

[1]) В оригинале $2u_p - v_p$. В дальнейшем подобные исправления неточностей в формулировках и выкладках автора особо не отмечены.

и по лемме 2

$$8u_{p+1}u_{p-1} = 4u_p^2 - v_p^2 \equiv 4\cdot(+1)^2 - 4 \equiv 0 \pmod{p}.$$

Доказательство теоремы 15. а) Условие необходимо. Пусть M_p — простое число. Мы должны показать, что $S_{p-1} \equiv 0 \pmod{M_p}$; вместо S_k мы можем рассмотреть также $\sigma_k = 2^{2^k} S_k : \sigma_1 = 8$, $\sigma_2 = 56$, $\sigma_3 = 3104$. Именно, так как M_p нечетное, то из $\sigma_{p-1} \equiv 0 \pmod{M_p}$ следует тотчас $S_{p-1} \equiv 0 \pmod{M_p}$. Так как $S_{k+1} = S_k^2 - 2$; то $\sigma_{k+1} = \sigma_k^2 - 2^{2k+1}$. Положим в (43) $r = 2^k$, тогда $v_{2k+1} = v_{2k}^2 - 2^{2k+1}$.

Из обоих последних равенств вследствие $v_2 = 8 = \sigma_1$ следует, что $\sigma_k = v_{2k}$. Теперь нужно показать, что $v_{2^{p-1}} = v_{(M_p+1)/2}$ делится на M_p. Положим в (43) $r = (M_p + 1)/2$, тогда получим:

$$v_{M_p+1} = v_{\frac{M_p+1}{2}}^2 - 4\cdot 2^{\frac{M_p-1}{2}}. \tag{45}$$

Так как M_p имеет форму $8x - 1$, то вследствие (10) $\left(\frac{2}{M_p}\right) = 1$ и по (7)

$$2^{\frac{M_p-1}{2}} \equiv 1 \pmod{M_p}.$$

Подставим это в (45), тогда останется показать, что

$$v_{M_p+1} \equiv -4 \pmod{M_p},$$

так как тогда

$$v_{\frac{M_p+1}{2}} \equiv 0 \pmod{M_p}.$$

По (41) имеем:

$$2v_{M_p+1} = v_{M_p}v_1 + 12u_{M_p}u_1 = 2v_{M_p} + 12u_{M_p}. \tag{46}$$

Вследствие (38) $M_p = (2^p + 1) - 2 \equiv 1 \pmod 3$ и по теореме 6 далее получаем:

$$\left(\frac{3}{M_p}\right) = -\left(\frac{M_p}{3}\right) = -\left(\frac{1}{3}\right) = -1,$$

так что из леммы 2 и (46) следует

$$v_{M_p+1} = v_{M_p} + 6u_{M_p} \equiv 2 - 6 \equiv -4 \pmod{M_p},$$

что и оставалось доказать.

б) Условие достаточно. Пусть S_{n-1} делится на $N=2^n-1$. Тогда N делит также $\sigma_{n-1}=v_{2^{n-1}}$. Пусть p — простой делитель N и ω — его ранг. Так как по (42) N делит $u_{2^n}=u_{2^{n-1}}v_{2^{n-1}}$, то $u_{2^n}\equiv 0 \pmod p$, так что по лемме 1 число ω делит 2^n. С другой стороны, ω не должно входить в 2^{n-1}, так как иначе по лемме 1 наряду с $v_{2^{n-1}}$ на p делилось бы и $u_{2^{n-1}}$, а это противоречило бы равенству (44), правая часть которого $\not\equiv 0 \pmod p$. Отсюда следует, что $\omega=2^n$. По лемме 3 имеем, однако, $p\geqslant\omega-1=2^n-1=N$, так что $p=N$ и N — простое число.

Эйлер заметил, что определенные M_p всегда являются составными. Это следует из

Теоремы 16. *Если числа* $p=4n+3$ *и* $q=2p+1=8n+7$ — *оба простые, то* $M_p\equiv 0 \pmod q$.

Доказательство. Если q — простое число, то вследствие $(10)\left(\frac{2}{q}\right)=1$, так что по (7) $2^{(q-1)/2}=2^p\equiv 1 \pmod q$ и $M_p\equiv 0 \pmod q$. Так как для $p>3$ всегда $2^p-1>2p+1$, то в этом случае $M_p>q$, т. е. составное. Примеры: $23|M_{11}$, $47|M_{23}$, $503|M_{251}$.

Вообще говоря, разложение на множители M_p, о которых известно, что они составные, не найдено. Другой нерешенной проблемой является вопрос о существовании бесчисленного множества простых чисел Мерсенна.

25. Простые числа Ферма $F_n=2^{2^n}+1$ имеют значение для задачи деления круга. Гаусс доказал, что правильный m-угольник тогда и только тогда можно построить с помощью циркуля и линейки, когда в каноническом разложении (1) числа m каждое $p>2$ имеет показатель $e_p=1$ и является простым числом Ферма. В то время как показателям $n=0$, 1, 2, 3, 4 соответствуют простые числа, $F_5=2^{32}+1$, как заметил Эйлер, уже составное. Именно, F_5 делится на 641, как видно из следующих сравнений по mod 641: из равенства $641=5\cdot 2^7+1$ следует $5\cdot 2^7\equiv -1$, так что $5^4\cdot 2^{28}\equiv 1$. Так как $641=5^4+2^4$, то $5^4\equiv -2^4$, откуда $5^4\cdot 2^{28}\equiv -2^{32}\equiv 1$, или $2^{32}+1\equiv 0$. В настоящее время известно, что F_n для $n=5$, 6, 7, 8, 9, 11, 12, 15, 18, 23, 36, 38, 73 является составным. Для каждого из этих F_n, кроме $n=7$ и 8, известен один делитель. Так, F_{73} делится на простое число $5\cdot 2^{75}+1$. Для $n>4$ не известны простые числа F_n, так что количество простых чисел Ферма, вероятно, конечно.

Критерием для простоты чисел F_n служит

Теорема 17. *Число* $F_n = 2^{2^n} + 1$ *тогда и только тогда простое, когда*

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}. \tag{47}$$

Пример. $F_2 = 17$, $3^8 = 81^2 \equiv (-4)^2 \equiv -1 \pmod{17}$.

Доказательство. Так как $4^m \equiv 4 \pmod{12}$ для всех $m > 0$, то F_n для $n \geqslant 1$ имеет вид $12k+5$. Если F_n — простое число, то вследствие (13) имеем $\left(\frac{3}{F_n}\right) = -1$ и (47) тотчас вытекает из (7). Наоборот, из (47) следует, что $3^{F_n-1} \equiv 1 \pmod{F_n}$. Если p простой делитель F_n и по mod p число 3 принадлежит показателю a, то $F_n - 1 = 2^{2^n}$ делится на a, т. е. a является степенью числа 2. Возможно лишь $a = 2^{2^n}$, так как при меньшем a было бы $3^{(F_n-1)/2} \equiv +1 \pmod{p}$, а это для $p > 2$ противоречит сравнению (47). Так как $p - 1 \equiv 0 \pmod{a}$, то $p = k \cdot 2^n + 1$, но тогда $k = 1$ и $p = F_n$.

Мы можем легко указать форму делителей составного F_n с помощью

Теоремы 18. *Для* $n > 1$ *каждый простой делитель числа* $F_n = 2^{2^n} + 1$ *имеет вид* $p = k \cdot 2^{n+2} + 1$.

Доказательство. Так как $2^{2^n} \equiv -1 \pmod{p}$ и $2^{2^{n+1}} \equiv 1 \pmod{p}$, то по mod p число 2 принадлежит показателю 2^{n+1}, так что $p \equiv 1 \pmod{2^{n+1}}$. Для $n > 1$, таким образом, $p \equiv 1 \pmod 8$, так что по (10) и (7) $2^{(p-1)/2} \equiv \left(\frac{2}{p}\right) = 1 \pmod{p}$. Отсюда $(p-1)/2$ делится на 2^{n+1}, т. е. $p = k \cdot 2^{n+2} + 1$.

Возможные простые делители числа F_5 имеют вид $128k+1$, и теперь легко найти делитель $641 = 5 \cdot 128 + 1$. Делители F_{73} имеют вид $N_k = k \cdot 2^{75} + 1$. Для $k = 1, 2, 3, 4$ число N_k делится соответственно на 3, 17, 5, 3. Легко видеть, что F_{73} не делится на эти числа, так что первым делителем F_{73} может быть лишь N_5. Морхед показал, что это действительно так. Так как N_5 наименьший делитель числа F_{73}, то N_5 простое число. Таким способом можно открывать новые большие простые числа.

Последовательность чисел F_n всегда дает новые простые делители, так как F_n взаимно просто со всеми предшествующими $F_s (s < n)$. Это тотчас следует из соотношения $F_0 F_1 F_2 \ldots F_{n-1} = 2^{2^n} - 1 = F_n - 2$, которое выводится пере-

множением n тождеств $(2^{2^r}-1)(2^{2^r}+1)=2^{2^{r+1}}-1$ $(r=0, 1, 2, \ldots, n-1)$. Это дает еще одно доказательство теоремы 2.

Так как $4^m \equiv 4 \pmod{12}$, то $F_n \equiv 5 \pmod{12}$, так что по (13) для $F_n = p$ будет $3^{(p-1)/2} \equiv \left(\frac{3}{p}\right) = -1 \pmod{p}$. Это означает, что число 3 — первообразный корень для любого простого числа Ферма; каждый собственный делитель числа $p-1$ является одновременно делителем $(p-1)/2 = 2^{2^n-1}$, так что $3^{(p-1)/2} \equiv +1$, если 3 не принадлежит по mod p показателю $p-1$. Если бы целое число g могло быть первообразным корнем лишь для конечного числа p, то было бы лишь конечное число простых чисел Ферма. Однако еще не доказанное предположение Артина гласит, что любое $g \neq \pm 1$, не являющееся квадратом [1]), — первообразный корень для бесконечного множества p.

26. Простые числа как значения квадратичной функции. В то время как значения функции $ax+b$ для $(a, b)=1$ по теореме 4 бесконечно много раз бывают простыми числами, соответствующая теорема для $f(x)=ax^2+bx+c$ не известна даже для простейшего частного случая x^2+1. Разумеется, дискриминант $\Delta = b^2-4ac$ не должен быть квадратом и числа c и $a+b$ не могут быть одновременно четными. Так как $4a(ax^2+bx+c)=(2ax+b)^2-\Delta$, то $\left(\frac{\Delta}{p}\right)=1$ для всех простых делителей $f(x)$, где p называется простым делителем $f(x)$, если существует такое x_0, что $f(x_0) \equiv 0 \pmod{p}$.

В 1772 году Эйлер открыл, что $f_1(x)=x^2+x+41$ для $x=0, 1, 2, \ldots, 39$ является простым числом. Все значения этой функции — нечетные и для всех нечетных $p \leqslant \sqrt{f_1(39)} = \sqrt{1601} < 41$ число $\Delta = -163$ является квадратичным невычетом, так что ни одно из 40 чисел $f_1(0), f_1(1), \ldots, f_1(39)$ не может быть составным. Еще более длинные интервалы простых значений имеют функции $f_2(x)=x^2-x+41$ и

$$f_3(x)=x^2-79x+1601=(x-40)^2+(x-40)+41,$$

для которых также $\Delta = -163$. Функция $f_2(x)$ для $0 \leqslant x \leqslant 40$ дает простые числа, так как $f_2(40)=1601$. Функция $f_3(x)$

---

[1]) Для $g=g_0^2$ имеем $g^{\frac{p-1}{2}} = g_0^{p-1} \equiv 1 \pmod{p}$.

для $0 \leqslant x \leqslant 79$ дает простые числа, так как $f_3(79) = f_3(0) = 1601$.

Если поставить вопрос, для каких простых чисел A функция $f_4(x) = x^2 + x + A$ принимает подряд простые значения для $0 \leqslant x \leqslant A - 2$, то легко отыскиваются малые значения $A = 3, 5, 11, 17$. Несмотря на далеко идущие вычисления, не найдено никаких $A > 41$.

Значения функции $f_1(x)$ для $x > 40$ не делятся на $p \leqslant 37$ и следует полагать, что $f_1(x)$ вообще представляет много простых чисел. Действительно, для $x \leqslant 11\,000$ функция $f_1(x)$ дает 4506 простых чисел. Еще больше простых чисел, именно 4923 для $x \leqslant 11\,000$, дает функция $x^2 + x + 72\,491$, дискриминант которой, равный 289 963, является квадратичным невычетом для $2 < p \leqslant 43$, так что ее значения взаимно просты с $p \leqslant 43$ [1]).

Л. Полетти вычислил простые значения между 10^7 и $5 \cdot 10^8$ для некоторых квадратичных функций и нашел 17 200 простых чисел.

Для примитивных квадратичных форм имеет место найденный Дирихле аналог теоремы 4:

Форма $ax^2 + bxy + cy^2$ представляет бесконечно много простых чисел, если a, b, c взаимно просты. Частный случай формы, разлагающейся на множители

$$(\alpha x + \beta y)(\gamma x + \delta y) = \alpha\gamma x^2 + (\alpha\delta + \beta\gamma) xy + \beta\delta y^2, \qquad (48)$$

где $(\alpha, \beta) = (\gamma, \delta) = 1$ легко сводится к теореме 4. Очевидно, должно иметь место уравнение $\alpha x + \beta y = 1$, которое разрешимо, так как $(\alpha, \beta) = 1$. Из решения x_0, y_0 получается бесконечно много решений $x_0 + n\beta$, $y_0 - n\alpha$. Второй множитель в (48) приобретает теперь вид $\gamma x_0 + \delta y_0 + (\gamma\beta - \delta\alpha) n = A + Bn$. Так как $\alpha A + y_0 B = \gamma$, то общий делитель A и B должен входить в γ, следовательно, из-за $(\alpha, y_0) = 1$ также и в δ. Из условия $(\gamma, \delta) = 1$ следует теперь $(A, B) = 1$, так что можно воспользоваться теоремой 4.

27. Один процесс, дающий простые числа. Миллсу удалось построить теоретикочисловую функцию, значениями которой являются лишь простые числа. Он доказал существование иррационального числа A, обладающего тем свойством,

---

[1]) См. N. G. W. H. Beeger, Nieuw Archief voor Wiskunde [2], 20, 48—50 (1939).

что $[A^{3^x}]$ для $x=1, 2, 3 \ldots$, всегда будет простым числом. Этот результат имеет лишь теоретическое значение. Так как известны лишь немногие знаки A, то действительно вычислить можно лишь немногие простые числа. То же возражение вызывает доказанная Е. М. Райтом [31]

Теорема 19. *Существует вещественное число* $\alpha=\alpha_0$, *обладающее тем свойством, что числа* $[2^{\alpha_0}]$, $[2^{\alpha_1}]$, ..., *определенные рекуррентной формулой* $\alpha_{n+1}=2^{\alpha_n}$, *все являются простыми.*

Доказательство. По теореме 31, § 39, между N и $2N$ для $N>1$ всегда лежат простые числа. Таким образом, мы можем построить такую последовательность простых чисел $P_1, P_2, \ldots$, что

$$2^{P_n}<P_{n+1}<P_{n+1}+1<2^{P_n+1} \quad (n=1, 2, \ldots). \qquad (49)$$

Пример. $P_1=3$, $P_2=13$, $P_3=16381, \ldots$ Под $\operatorname{Log} x$ будем понимать логарифм при основании 2, а $\operatorname{Log}^{(n)} x$ обозначает n раз последовательно взятый логарифм $\operatorname{Log}\operatorname{Log}\ldots\operatorname{Log} x$. Из (49) логарифмированием получаем:

$$\operatorname{Log}^{(n)} P_n<\operatorname{Log}^{(n+1)} P_{n+1}<\operatorname{Log}^{(n+1)}(P_{n+1}+1)<$$
$$<\operatorname{Log}^{(n)}(P_n+1).$$

Положим

$$\beta_n=\operatorname{Log}^{(n)} P_n, \quad \gamma_n=\operatorname{Log}^{(n)}(P_n+1),$$

тогда

$$\beta_n<\beta_{n+1}<\gamma_{n+1}<\gamma_n \quad (n=1, 2, 3, \ldots).$$

Вытекающая отсюда цепочка неравенств

$$\beta_1<\beta_2<\beta_3<\ldots<\beta_n<\gamma_n<\gamma_{n-1}<\ldots<\gamma_2<\gamma_1$$

при $n\longrightarrow\infty$ определяет, очевидно, число α как общий предел β_n и γ_n, причем $\beta_n<\alpha<\gamma_n$ для всех n. Возвращаясь от логарифмов к числам, получаем:

$$\operatorname{Log}^{(n-1)} P_n<2^{\alpha}=\alpha_1<\operatorname{Log}^{(n-1)}(P_n+1),$$
$$\operatorname{Log}^{(n-2)} P_n<2^{\alpha_1}=\alpha_2<\operatorname{Log}^{(n-2)}(P_n+1),$$
$$P_n<2^{\alpha_{n-1}}=\alpha_n<P_n+1,$$

или $P_n=[\alpha_n^n]$, ч. т. д.

Для $P_1 = 3$, $P_2 = 13$, $P_3 = 16381$ получаем:

$$\beta_1 = \operatorname{Log} 3 = 1{,}58495, \quad \gamma_1 = \operatorname{Log} 4 = 2{,}00000;$$
$$\beta_2 = \operatorname{Log}^{(2)} 13 = 1{,}88765, \quad \gamma_2 = \operatorname{Log}^{(2)} 14 = 1{,}92877;$$
$$\beta_3 = \operatorname{Log}^{(3)} 16381 = 1{,}92877, \quad \gamma_3 = \operatorname{Log}^{(3)} 16382 = 1{,}92877.$$

Здесь $\alpha = 1{,}92878\ldots$ P_4 имеет уже около 5000 знаков.

28. Простые числа с заданными первыми и последними цифрами. Из критериев делимости следует, что последними цифрами простых чисел могут быть лишь 1, 3, 7 или 9, тогда как первой цифрой может быть каждое из чисел 1, 2, ..., 9, как видно уже на простых числах < 100. Серпинский [27] доказал следующие общие теоремы:

Теорема 20. *Если $c_1, c_2, \ldots, c_m$ — конечное число цифр десятичной системы и $c_1 \neq 0$, то существует сколь угодно много простых чисел, начинающихся последовательностью цифр $c_1, c_2, \ldots, c_m$.*

Доказательство. Пусть a — m-значное число, построенное из $c_1, c_2, \ldots, c_m$, взятых в указанном порядке. Достаточно показать, что

$$\lim_{n \to \infty} \{\pi[(a+1)\,10^n] - \pi(a \cdot 10^n)\} = \infty, \tag{50}$$

так как тогда для заданного a существует бесконечно много таких n, что

$$\pi[(a+1)\cdot 10^n] - \pi(a \cdot 10^n) > 1,$$

а каждое из таких неравенств подтверждает существование простого числа между $a \cdot 10^n$ и $(a+1)\cdot 10^n$, причем все такие числа начинаются теми же цифрами, что и a. Для доказательства (50) воспользуемся теоремой 3. Так как

$$\lim_{n \to \infty} \frac{n \log 10 + \log(a+1)}{n \log 10 + \log a} = 1,$$

то после простых преобразований получаем:

$$\lim_{n \to \infty} \frac{\pi[(a+1)\cdot 10^n]}{\pi(a \cdot 10^n)} = \frac{a+1}{a}, \quad \text{или}$$

$$\lim_{n \to \infty} \frac{\pi[(a+1)\cdot 10^n] - \pi(a \cdot 10^n)}{\pi(a \cdot 10^n)} = \frac{1}{a}.$$

Так как знаменатель стремится к бесконечности, а отношение остается положительным, то и числитель должен стремиться к бесконечности, ч. т. д.

Теорема 21. *Если* $c_1, c_2, \ldots, c_m$ — *конечное число десятичных знаков и* $c_m = 1, 3, 7$ *или* 9, *то существует бесконечно много простых чисел, оканчивающихся последовательностью знаков* $c_1, c_2, \ldots, c_m$.

Доказательство. Число a, построенное из $c_1, c_2, \ldots, c_m$, взятых в такой последовательности, взаимно просто с 10^m. По теореме 4 существует бесконечно много $p = k \cdot 10^m + a$, $k > 0$. Последние m цифр числа p совпадают со знаками a, ч. т. д.

Пример. Существует бесконечно много простых чисел вида 111... или ... 111, где в начале или конце стоит, например, 10^6 единиц.

V. СУММЫ ПО ПРОСТЫМ ЧИСЛАМ

29. Асимптотическое поведение функции. При рассмотрении задач, связанных с распределением простых чисел, приходится по большей части довольствоваться аппроксимативными утверждениями, причем следует уделять особое внимание росту не определенного точно остаточного члена.

Если $f(x)$ и $g(x)$ — две функции неограниченно возрастающей вещественной переменной x, $g(x) > 0$ и существуют два положительных постоянных числа C_1 и C_2 [1]), таких, что $|f(x)| < C_1 g(x)$ для всех $x > C_2$, то пишут $f(x) = O[g(x)]$. Это означает, таким образом, что отношение $|f(x)|/g(x)$ при $x \longrightarrow \infty$ остается конечным. Функция $g(x)$ дает, таким образом, асимптотическое поведение $f(x)$ в указанном выше смысле и, естественно, ни в коем случае не определяется функцией $f(x)$ однозначно. В частности, символом $O(1)$ обозначаем любую функцию, ограниченную для $x > C_2$.

Примеры.

$$2x + \sqrt{x} = O(x), \qquad x + x^{-1} = O(x),$$
$$\sin x = O(1), \quad x(x-3)^{-1} = O(1),$$
$$\log x = O(x), \qquad \log x = O(\sqrt{x}),$$
$$\log\log x = O(\log x), \qquad \operatorname{ch} x = O(e^x),$$
$$3O(x) + 5O(\log x) = O(x).$$

[1]) В дальнейшем будем обозначать символами C_i, где i — любое натуральное число, положительные постоянные.

Если отношение $f(x)/g(x)$ для $x \to \infty$ стремится к нулю, то пишем $f(x) = o[g(x)]$. В частности, $o(1)$ — величина, стремящаяся к нулю. Очевидно, из $f(x) = o[g(x)]$ следует также $f(x) = O[g(x)]$, но не наоборот.

Примеры:

$$x = o(x^2), \quad \sin x = o(\sqrt{x}), \quad \pi(x) = [1 + o(1)]x/\log x.$$

Мы часто пользуемся соотношением

$$\log^\alpha x = o(x^\beta), \quad \alpha \text{ — любое}, \quad \beta > 0. \tag{51}$$

При доказательстве можно предположить, что $\alpha > 0$. Далее, по правилу раскрытия неопределенностей

$$\lim_{x\to\infty} x^{-\beta}\log^\alpha x = (\lim_{x\to\infty} x^{-\frac{\beta}{\alpha}}\log x)^\alpha = (\lim_{x\to\infty} \alpha\beta^{-1}x^{-\frac{\beta}{\alpha}})^\alpha = 0.$$

Таким образом, $\log x$ стремится к бесконечности медленнее, чем любая степень x со сколь угодно малым положительным показателем. $\log\log x$ и $\log\log\log x$ растут еще медленнее; так, $\log\log\log(10^{1000}) = 2{,}04\ldots$

Если отношение $f(x)/g(x)$ стремится к 1 при $x \to \infty$, то пишем $f(x) \sim g(x)$, а функции называем асимптотически равными. В этом случае можно также писать $f(x) = g(x)[1 + o(1)]$.

Примеры. $x + \sin x \sim x$, $\pi(x) \sim x/\log x$. Эти равенства обладают свойствами рефлексивности и транзитивности, так как из $f \sim g$, $g \sim h$ вследствие того, что $(\lim f/g)(\lim g/h) = \lim f/h = 1$, следует, что $f \sim h$.

30. Оценки некоторых сумм. Рассматривая верхнюю и нижнюю интегральные суммы, построенные из прямоугольников единичной ширины, можно получить следующие оценки:

$$\sum_{n\leqslant x}\frac{1}{n} = \int_1^x \frac{du}{u} + C_3 + O\left(\frac{1}{x}\right) = \log x + C_3 + O\left(\frac{1}{x}\right), \tag{52}$$

$$\sum_{n\leqslant x} n^{-1-\rho} = \int_1^x u^{-1-\rho}du + C_4 + O(x^{-1-\rho}) =$$

$$= -\rho^{-1}x^{-\rho} + C_5 + O(x^{-1-\rho}). \tag{53}$$

Для $\rho > 0$ получаем $\sum_{n \leqslant x} n^{-1-\rho} = O(1)$.

$$\sum_{n \leqslant x} \log n = \int_1^x \log u \, du + O(\log x) = \\ = x \log x - x + O(\log x), \tag{54}$$

$$\sum_{n \leqslant x} \frac{\log n}{n} = \int_1^x \frac{\log u}{u} du + C_6 + O\left(\frac{\log x}{x}\right) = \\ = \frac{1}{2} \log^2 x + C_6 + O\left(\frac{\log x}{x}\right), \tag{55}$$

$$\sum_{2 \leqslant n \leqslant x} \frac{1}{n \log n} = \int_2^x \frac{du}{u \log u} + C_7 + O\left(\frac{1}{x \log x}\right) = \\ = \log \log x + C_8 + O\left(\frac{1}{x \log x}\right), \tag{56}$$

$$\sum_{2 \leqslant n \leqslant x} \frac{1}{n \log^2 n} = \int_2^x \frac{du}{u \log^2 u} + C_9 + O\left(\frac{1}{x \log^2 x}\right) = \\ = -\frac{1}{\log x} + C_{10} + O\left(\frac{1}{x \log^2 x}\right). \tag{57}$$

Так как вследствие (51) $\log n < n^{\frac{1}{4}k}$ для постоянных $k > 0$ и $n > n_0$, то для $t \geqslant 1{,}5$ по (53) имеем:

$$\sum_{n \leqslant x} n^{-t} \log^k n < \sum_{n \leqslant x} n^{-t+0{,}25} = O(1). \tag{58}$$

При всех этих оценках следует различать главный член и O-член, или остаточный член. В главный член следует включать лишь такие слагаемые, которые имеют больший порядок, чем остаточный член, и следовательно, не могут быть поглощены им.

31. Следствие из канонического разложения $n!$ [1]. Логарифмированием получаем из (2)

$$\sum_{k=1}^{n} \log k = \sum_{p \leqslant n} \left[\frac{n}{p}\right] \log p + \sum_{p \leqslant n} \left[\frac{n}{p^2}\right] \log p + \dots$$

Для $t \geqslant 2$, $p \geqslant 2$ вследствие $\log p < \sqrt{p}$ и (53) имеем:

$$\sum \left[\frac{n}{p^t}\right] \log p \leqslant n \sum p^{-t} \log p < n \sum p^{-t+0,5} < C_{11} n.$$

Формула (54) приводит теперь к соотношению

$$A(n) = \sum_{p \leqslant n} \left[\frac{n}{p}\right] \log p = n \log n + O(n). \tag{59}$$

Так как $[n/p] = [[n]/p]$, то это имеет место и для нецелых n.

Выясним теперь, что произойдет, если опустить квадратные скобки в (59). Заметив, что неравенство $n/2 < p \leqslant n$ равносильно неравенству $1 \leqslant \frac{n}{p} < 2$, вследствие $[x] - 2[x/2] \geqslant 0$ для $x > 0$, получим:

$$O(n) = A(n) - 2A\left(\frac{n}{2}\right) =$$

$$= \sum_{p \leqslant n} \left\{\left[\frac{n}{p}\right] - 2\left[\frac{n}{2p}\right]\right\} \log p \geqslant \sum_{\frac{n}{2} < p \leqslant n} \left[\frac{n}{p}\right] \log p =$$

$$= \vartheta(n) - \vartheta\left(\frac{n}{2}\right),$$

где для краткости введено обозначение $\vartheta(x) = \sum_{p \leqslant x} \log p$.

Итак, существует такое C_{12}, что

$$\vartheta\left(\frac{n}{2^i}\right) - \vartheta\left(\frac{n}{2^{i+1}}\right) < C_{12} \frac{n}{2^i} \quad \text{для } i = 0, 1, 2, \dots$$

Сложение этих неравенств дает

$$\vartheta(n) < C_{12} n \sum_{i=0}^{\infty} 2^{-i} = 2C_{12} n, \text{ или } \vartheta(n) = O(n). \tag{60}$$

Если теперь опустить в (59) квадратные скобки, то ошибка будет $< \vartheta(n) = O(n)$. Делением на n получается важная

[1] См. Шапиро [26].

Теорема 22.

$$\sum_{p\leqslant x}\frac{\log p}{p}=\log x+O(1).$$

Как следствие, получаем для $\Lambda(n)$ (см. § 16)

$$\sum_{n\leqslant x}\frac{\Lambda(n)}{n}=\log x+O(1), \tag{61}$$

так как вследствие (58) часть суммы, распространенная на $n=p^t\,(t\geqslant 2)$, сходится.

32. Частное суммирование. Абелем было указано следующее очень полезное для оценок формальное преобразование конечной суммы, законность которого легко проверить:

$$\sum_{i=1}^{n}a_ib_i=a_1(b_1-b_2)+(a_1+a_2)(b_2-b_3)+(a_1+a_2+a_3)\times$$
$$\times(b_3-b_4)+\ldots=\sum_{k=1}^{n}\left(\sum_{i=1}^{k}a_i\right)(b_k-b_{k+1})+b_{n+1}\sum_{i=1}^{n}a_i. \tag{62}$$

Положим $a_i=c_i-c_{i-1}$, $c_0=0$, тогда получим формулу, часто оказывающуюся более удобной

$$\sum_{i=1}^{n}(c_i-c_{i-1})\,b_i=\sum_{k=1}^{n}c_k(b_k-b_{k+1})+c_nb_{n+1}. \tag{63}$$

Для приложений используем то, что по формуле Тейлора

$$f(x+1)=f(x)+f'(x)+\frac{f''(x)}{2!}+\frac{f'''(x+\vartheta)}{3!},$$

где $0<\vartheta<1$. Отсюда легко получаются равенства

$$\left.\begin{aligned}\log(k+1)&=\log k+k^{-1}+O(k^{-2}),\\ \frac{1}{\log(k+1)}&=\frac{1}{\log k}-\frac{1}{k\log^2 k}+O\left(\frac{1}{k^2}\right).\end{aligned}\right\} \tag{64}$$

Пример. По определению функции $\vartheta(x)$ в § 31 имеем $\vartheta(n)-\vartheta(n-1)=\log n$ для $n=p$ и нуль в противном случае. По (63) получаем для целых x

$$\sum_{p\leqslant x}\log^2 p=\sum_{i=1}^{x}[\vartheta(i)-\vartheta(i-1)]\log i=$$
$$=\sum_{k=1}^{x}\vartheta(k)\log\frac{k}{k+1}+\vartheta(x)\log(x+1).$$

Вследствие (60), (64), (52)

$$\left|\sum_{k=1}^{x}\vartheta(k)\log\frac{k}{k+1}\right|<2C_{12}x+$$
$$+C_{12}\log x+C_{13}+O\left(\frac{1}{x}\right)=O(x).$$

Так как

$$\vartheta(x)\log(x+1)=\vartheta(x)\log x+C_{14}+O\left(\frac{1}{x}\right),$$

то

$$\sum_{p\leqslant x}\log^2 p=\vartheta(x)\log x+O(x)=O(x\log x).$$

Следующие оценки будем применять в дальнейшем. Из теоремы 22, (60), (63) и (53)

$$\log x+O(1)=\sum_{p\leqslant x}\frac{\log p}{p}=\sum_{n\leqslant x}\frac{\vartheta(n)-\vartheta(n-1)}{n}=$$
$$=\sum_{k\leqslant x}\frac{\vartheta(k)}{k(k+1)}+\frac{\vartheta(x)}{x+1}=\sum_{k\leqslant x}\frac{\vartheta(k)}{k^2}\left\{1-\frac{1}{k}+\ldots\right\}+O(1).$$

Таким образом, имеем:

$$\sum_{k\leqslant x}\frac{\vartheta(k)}{k^2}=\log x+O(1). \tag{65}$$

Из (61), (62), (64), (55), (52), (58) следует далее

$$\sum_{n\leqslant x}\frac{\Lambda(n)}{n}\log n=$$
$$=-\sum_{k\leqslant x}\{\log k+O(1)\}\left[\frac{1}{k}+O\left(\frac{1}{k^2}\right)\right]+$$
$$+[\log x+O(1)]\left[\log x+O\left(\frac{1}{x}\right)\right]=$$
$$=-0{,}5\log^2 x+O(\log x)+O(1)+\log^2 x+O(\log x).$$

Таким образом,

$$\sum_{n\leqslant x}\frac{\Lambda(n)}{n}\log n=\frac{1}{2}\log^2 x+O(\log x). \tag{66}$$

Теперь (61) и (66) дают

$$\sum_{nm\leqslant x}\frac{\Lambda(n)\Lambda(m)}{nm}=\sum_{n\leqslant x}\frac{\Lambda(n)}{n}\sum_{m\leqslant\frac{x}{n}}\frac{\Lambda(m)}{m}=\sum_{n\leqslant x}\left\{\log\frac{x}{n}+O(1)\right\}\frac{\Lambda(n)}{n}=$$

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

$$=\log^2 x-\sum_{n\leqslant x}\frac{\Lambda(n)}{n}\log n+O(\log x)=$$

$$=\frac{1}{2}\log^2 x+O(\log x). \tag{67}$$

Из (67), (62), (64) следует

$$\sum_{mn\leqslant x}\frac{\Lambda(m)\Lambda(n)}{mn\log mn}=\sum_{k\leqslant x}\left\{\frac{1}{2}\log^2 k+O(\log k)\right\}\times$$

$$\times\left\{\frac{1}{\log k}-\frac{1}{\log(k+1)}\right\}+\frac{0{,}5\log^2 x+O(\log x)}{\log(x+1)}=$$

$$=\frac{1}{2}\sum_{k\leqslant x}\frac{1}{k}+O\left(\sum_{k\leqslant x}\frac{1}{k\log k}\right)+\frac{1}{2}\log x+O(1).$$

Таким образом, вследствие (52) и (56)

$$\sum_{mn\leqslant x}\frac{\Lambda(m)\Lambda(n)}{mn\log mn}=\log x+O(\log\log x). \tag{68}$$

33. Сумма величин, обратных простым числам. Хотя гармонический ряд расходится вследствие (52), ряд $\sum\frac{1}{p}$ может сходиться. Это означало бы, что p по сравнению со всеми натуральными n встречаются очень редко. Однако еще Эйлер доказал, что $\sum\frac{1}{p}$ также расходится. Таким образом, простые числа встречаются чаще, чем квадраты, для которых ряд обратных величин сходится по (53). Напротив, в § 68 мы увидим, что ряд из величин, обратных простым близнецам, сходится к конечной сумме.

Из теоремы 1 и (52) следует для достаточно больших x

$$P_x = \prod_{p \leqslant x} (1 - p^{-1})^{-1} = \prod_{p \leqslant x} (1 + p^{-1} + p^{-2} + \ldots) >$$

$$> \sum_{n=1}^{x} \frac{1}{n} > \log x, \qquad (69)$$

поскольку каждое слагаемое правой части встречается в разложении произведения, потому что в разложение n входят лишь $p \leqslant x$. Теперь

$$\log P_x = -\sum_{p \leqslant x} \log\left(1 - \frac{1}{p}\right) = \sum_{p \leqslant x} \frac{1}{p} + \vartheta \sum_{p \leqslant x} \frac{1}{2p(p-1)} =$$

$$= \sum_{p \leqslant x} \frac{1}{p} + O(1), \quad 0 < \vartheta < 1. \qquad (70)$$

Из (69) теперь следует неравенство $\sum \frac{1}{p} \geqslant \log\log x - O(1)$, что и доказывает расходимость ряда.

Для того чтобы точнее определить порядок роста суммы $\sum \frac{1}{p}$, применим частное суммирование в форме (62). С помощью теоремы 22, (64), (56), (57) легко получается:

$$\sum_{p \leqslant x} \frac{1}{p} = \sum_{p \leqslant x} \frac{\log p}{p} \frac{1}{\log p} = \sum_{n=2}^{x} \frac{\vartheta(n) - \vartheta(n-1)}{n} \frac{1}{\log n} =$$

$$= \sum_{k=2}^{x} \{\log k + O(1)\} \left\{\frac{1}{\log k} - \frac{1}{\log(k+1)}\right\} + \frac{\log x + O(1)}{\log(x+1)} =$$

$$= \sum_{k=2}^{x} \frac{1}{k \log k} + O\left(\sum_{k=2}^{x} \frac{1}{k \log^2 k}\right) + 1 + o(1) =$$

$$= \log\log x + C_{15} + o(1).$$

Таким образом, получается

Теорема 23.

$$\sum_{p \leqslant x} \frac{1}{p} = \log\log x + C_{15} + o(1).$$

По Россеру [21] $C_{15} = 0{,}261497\ldots$

Рассмотрим расходящееся к нулю произведение P_x^{-1}. Из (69) следует, что

$$\prod_{p\leqslant x}(1-p^{-1})<\frac{1}{\log x}.$$

С помощью теоремы 23 получается теперь из (70)

Теорема 24.

$$\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)=\frac{e^{-C_{16}[1+o(1)]}}{\log x}.$$

По Мертенсу $C_{16}=0{,}5772157...$ (постоянная Эйлера) [1]. Заменим в (70) $\frac{1}{p}$ на $\frac{2}{p}$ и исключим $p=2$. Тогда аналогичным образом получается.

Теорема 25.

$$\prod_{2<p\leqslant x}\left(1-\frac{2}{p}\right)=\frac{C_{17}+o(1)}{\log^2 x}.$$

По Россеру [21] $C_{17}=0{,}832429...$

VI. ОБЩИЕ ТЕОРЕМЫ ОТНОСИТЕЛЬНО $\pi(x)$ И p_n [2]

34. Вычисление $\pi(x)$. Для $\pi(x)$ существуют выражения, построенные притом из элементарных функций. Легко убедиться, например, в справедливости соотношения

$$\pi(x)=1+\sum_{n=3}^{x}\left\{1-\lim_{m\to\infty}\left[1-\prod_{k=2}^{n-1}\left(\sin\frac{n\pi}{k}\right)^2\right]^m\right\}$$ [3].

На самом деле такие формулы дают мало сведений о природе функции, определяющей распределение простых чисел.

До некоторой степени практически полезный подход к вычислению $\pi(x)$ дает решето Эратосфена (§ 4). Если вычеркнуть из последовательности натуральных чисел $\leqslant x$ простые числа $p_i\leqslant\sqrt{x}$ вместе с их кратными, то останется $\pi(x)-\pi(\sqrt{x})$ простых чисел $>\sqrt{x}$ и сверх того число 1.

---

[1]) Ср. Hardy и Wright, The Theory of Numbers (Clarendon Press, Oxford, 1945), p. 353.

[2]) p_n в этом разделе всегда обозначает n-е простое число.

[3]) W. Sierpinski, El. Math. 8, 44 (1953), Aufgabe 181.

Этот процесс приводит к соотношению

$$\pi(x)-\pi(\sqrt{x})+1=[x]-\sum_i\left[\frac{x}{p_i}\right]+\sum_{i<j}\left[\frac{x}{p_ip_j}\right]-$$

$$-\sum_{i<j<k}\left[\frac{x}{p_ip_jp_k}\right]+\ldots=\sum_{d\mid p_1p_2\cdots p_\pi(\sqrt{x})}\mu(d)\left[\frac{x}{d}\right]. \qquad 1)$$

Так как при вычеркивании $\left[\frac{x}{p_i}\right]$ чисел, кратных p_i, $\left[\frac{x}{p_ip_j}\right]$ чисел, кратных p_ip_j, вычеркиваются дважды, то нужно поэтому прибавить к числу остающихся простых это количество. При этом $\left[\frac{x}{p_ip_jp_k}\right]$ чисел, кратных $p_ip_jp_k$, будут прибавлены дважды и нужно снова один раз отнять это количество и т. д. После конечного числа шагов ряд обрывается.

Пример. $\pi(30)-\pi(5)+1=30-(15+10+6)+(5+3+2)-1$.

Е. Мейссель доказал в 1870 г. теорему, которая позволяет проводить практическое вычисление $\pi(x)$ далеко за пределами таблиц простых чисел. С помощью этой теоремы было вычислено $\pi(10^9)=50\,847\,478$.

Теорема 26. *Пусть $\varphi(x, r)$ означает количество натуральных чисел $\leqslant x$, не делящихся ни на одно из первых r простых чисел $p_1=2$, $p_2=3, \ldots, p_r$. Если положить $\pi(x^{1/3})=m$, $\pi(x^{1/2})=n$ и $n-m=s$, то*

$$\pi(x)=\varphi(x, m)+m(s+1)+\frac{s(s-1)}{2}-1-\sum_{\tau=1}^{s}\pi\left(\frac{x}{p_{m+\tau}}\right). \qquad (72)$$

Доказательство[1]). Существует $\varphi(x, k-1)$ натуральных чисел $\leqslant x$, взаимно простых с $p_1, p_2, \ldots, p_{k-1}$. Из них ровно $\varphi(xp_k^{-1}, k-1)$ делится на p_k, так как в $\varphi(x, k-1)$ учтены лишь те целые кратные hp_k, $h\leqslant xp_k^{-1}$, для которых $(h, p_1p_2\ldots p_{k-1})=1$. Таким образом,

$$\varphi(x, k)=\varphi(x, k-1)-\varphi(xp_k^{-1}, k-1). \qquad (73)$$

Просуммировав (73) для $k=m+1, m+2, \ldots, n$, получим:

$$\varphi(x, n)=\varphi(x, m)-\sum_{\tau=1}^{s}\varphi(xp_{m+\tau}^{-1}, m+\tau-1). \qquad (74)$$

[1]) См. А. Брауэр [I].

Из определения m, n и s следует

$$x^{\frac{1}{3}} < p_{m+\tau} \leqslant x^{\frac{1}{2}} \leqslant x p_{m+\tau}^{-1} < x^{\frac{2}{3}} \quad (\tau = 1, 2, \ldots, s). \tag{75}$$

Для $0 < a \leqslant b \leqslant a^2$ имеем $\varphi[b, \pi(a)] = 1 + \pi(b) - \pi(a)$, так как числами, учитываемыми символом $\varphi[b, \pi(a)]$, являются 1 и простые p, для которых $a < p \leqslant b$. Для $b = x$ и $a = x^{1/2}$

$$\varphi(x, n) = 1 + \pi(x) - n \quad \text{или} \quad \pi(x) = \varphi(x, n) + n - 1. \tag{76}$$

По (75)

$$p_{m+\tau} \leqslant x p_{m+\tau}^{-1} < p_{m+\tau}^2 \quad \text{или} \quad 1 \leqslant x p_{m+\tau}^{-2} < p_{m+\tau},$$

так что

$$\varphi(x p_{m+\tau}^{-2}, m + \tau - 1) = 1.$$

При $a = p_{m+\tau}$, $b = x p_{m+\tau}^{-1}$

$$\varphi(x p_{m+\tau}^{-1}, m + \tau) = 1 + \pi(x p_{m+\tau}^{-1}) - m - \tau$$

и отсюда вследствие (73)

$$\varphi(x p_{m+\tau}^{-1}, m + \tau - 1) = \varphi(x p_{m+\tau}^{-1}, m + \tau) +$$
$$+ \varphi(x p_{m+\tau}^{-2}, m + \tau - 1) = \pi(x p_{m+\tau}^{-1}) - (m + \tau - 2). \tag{77}$$

Из (76), (74) и (77) получаем окончательно

$$\pi(x) = \varphi(x, m) - \sum_{\tau=1}^{s} \varphi(x p_{m+\tau}^{-1}, m + \tau - 1) + m + s - 1 =$$
$$= \varphi(x, m) - \sum_{\tau=1}^{s} \pi(x p_{m+\tau}^{-1}) + \sum_{\tau=1}^{s} (m + \tau - 2) + m + s - 1 =$$
$$= \varphi(x, m) + m(s + 1) + \frac{s(s-1)}{2} - 1 - \sum_{\tau=1}^{s} \pi(x p_{m+\tau}^{-1}).$$

При применении (72) больше всего труда требует вычисление $\varphi(x, m)$. Если $[x] = g p_1 p_2 \ldots p_k + r$, где g и r — неотрицательные целые числа, то

$$\varphi(x, k) = g\varphi(p_1 p_2 \ldots p_k) + \varphi(r, k). \tag{78}$$

Среди чисел $1, 2, \ldots, (p_1 p_2 \ldots p_k), \ldots, g(p_1 p_2 \ldots p_k)$ имеется точно $g\varphi(p_1 p_2 \ldots p_k)$, взаимно простых с $p_1, p_2, \ldots, p_k$, так как каждая полная система вычетов по mod $p_1 p_2 \ldots p_k$ содержит $\varphi(p_1 p_2 \ldots p_k)$ таких чисел. Для того чтобы

$gp_1p_2\dots p_k+z$ $(z=1, 2, \dots, r)$ было взаимно просто с $p_1p_2\dots p_k+z$, нужно чтобы этим качеством обладало и z, так что таких чисел имеется $\varphi(r, k)$. Полезной является также легко проверяемая формула

$$\varphi(p_2p_3\dots p_k, k)=0{,}5\,\varphi(p_1p_2\dots p_k, k)=0{,}5\,\varphi(p_1p_2\dots p_k). \quad (79)$$

С помощью (73), (78) и (79) можно постепенно вычислить $\varphi(x, m)$.

Пример.

$$x=1000,\ m=\pi(10)=4,\ n=\pi(31{,}6)=11,\ s=7,$$

$$\pi(1000)=\varphi(1000,4)+32+21-1-\sum_{\tau=1}^{7}\pi(1000\,p_{4+\tau}^{-1});$$

$$\pi\left(\frac{1000}{11}\right)=24,$$

$$\pi\left(\frac{1000}{13}\right)=21,\ \pi\left(\frac{1000}{17}\right)=16,\ \pi\left(\frac{1000}{19}\right)=15,\ \pi\left(\frac{1000}{23}\right)=14,$$

$$\pi\left(\frac{1000}{29}\right)=11,\ \pi\left(\frac{1000}{31}\right)=11,\ \text{так что}\ \pi(1000)=$$

$$=\varphi(1000,4)-60,$$

$$\varphi(1000,4)=4\varphi(210)+\varphi(160,4)=192+\varphi(160,4),$$

$$\varphi(160,4)=\varphi(160,3)-\varphi(22,3)=$$

$$=5\varphi(30)+\varphi(10,3)-\varphi(22,3)=42-\varphi(22,3),$$

$$\varphi(22,3)=\varphi(22,2)-\varphi(4,2)=3\varphi(6)=6,$$

$$\varphi(1000,4)=192+42-6=228,\ \pi(1000)=228-60=168.$$

Так как $\pi(x^{1/3})=m$, то $p_{m+1}>x^{1/3}$, так что $xp_{m+1}^{-1}<x^{2/3}$. Для того чтобы с помощью (72) можно было вычислить $\pi(x)$, достаточно, таким образом, знать отдельные простые числа $\leqslant x^{1/2}$ и значения $\pi(y)$ для $y\leqslant x^{2/3}$.

35. Простые оценки для $\pi(x)$. Очевидно, что каждое натуральное число однозначно представляется в виде произведения квадрата и числа, свободного от квадратов. Количество квадратных чисел $\leqslant n$ будет $\leqslant\sqrt{n}$. Все числа, не содержащие квадратов, содержатся среди $2^{\pi(n)}$ делителей произведения $p_1p_2\dots p_{\pi(n)}$. Если перемножить все эти делители и все квадратные числа $\leqslant n$, то мы получим все натуральные

числа $\leqslant n$. Отсюда следует, что $n \leqslant 2^{\pi(n)}\sqrt{n}$ или $\pi(n) \geqslant (2\log 2)^{-1}\log n$ [1]).

Для того чтобы оценить $\pi(x)$ сверху, используем метод решета. Если $\varphi(x, r)$ имеет тот же смысл, что и в теореме 26, то аналогично (71) имеем:

$$\varphi(x, r) = \sum \mu(d)\left[\frac{x}{d}\right],$$

где d пробегает все делители числа $p_1 p_2 \ldots p_r$. Очевидно, $\pi(x) \leqslant \varphi(x, r) + r$. Если опустить квадратные скобки, количество которых составляет 2^r, то ошибка будет не больше 2^r. Отсюда вытекает (см. § 15), вследствие (69) и $p_r > r$,

$$\pi(x) \leqslant x \prod_{p \leqslant p_r}(1 - p^{-1}) + r + 2^r < x \prod_{p \leqslant p_r}(1 - p^{-1}) + 2^{r+1} < \frac{x}{\log r} + 2^{r+1}.$$

Выберем $r = c\log x$, $c < 1/\log 2$, так что $x > 2^r$, тогда вследствие $c\log 2 < 1$

$$\pi(x) < \frac{x}{\log c + \log\log x} + 2x^{c\log 2} = O\left(\frac{x}{\log\log x}\right).$$

Таким образом доказана

Теорема 27. $\pi(x) = o(x)$, *т. е.* «*почти все*» *числа составные.*

36. Истинный порядок роста $\pi(x)$. Мы ищем для $\pi(x)$ как можно лучшую приближающую функцию $f(x)$, такую, чтобы относительная погрешность была как можно меньше. Из требования $\lim\limits_{x\to\infty}[\pi(x) - f(x)]/f(x) = 0$ следует $f(x) \sim \pi(x)$. По теореме 3 функцией, удовлетворяющей этому условию, является $x/\log x$. Эту форму функции $f(x)$ открыл эмпирически еще Гаусс, тогда как Лежандр в 1798 г. предположил, что $f(x) = x/(\log x - 1{,}08366)$. Выбор функции $x/\log x$ можно обосновать следующим образом. Из (63) получаем:

$$\sum_{p_i \leqslant x}\frac{1}{p_i} = \sum_{m=1}^{x}\frac{\pi(m) - \pi(m-1)}{m} = \sum_{k=1}^{x}\frac{\pi(k)}{k(k+1)} + \frac{\pi(x)}{x+1}.$$

[1]) Сообщено П. Эрдёшем.

Эта сумма по теореме 23 расходится, тогда как сумма $\sum 1/k(k+1)$ сходится и $\pi(x)=o(x)$; таким образом, расходимость должны вызывать множители $\pi(k)$.

Если $A(k)$ — положительная, ограниченная функция, $A(k)<C_{20}$, то ряд $\sum k^{1-\varepsilon}A(k)\,k(k+1)<C_{20}\sum k^{-1-\varepsilon}$ и сходится для любого $\varepsilon>0$. Таким образом, для бесконечно многих k должно быть $\pi(k)>k^{1-\varepsilon}A(k)$, следовательно, $\pi(k)$ растет быстрее, чем $k^{1-\varepsilon}$ при любом $\varepsilon>0$, однако медленнее, очевидно, чем k. Простой функцией, обладающей таким свойством, является $k/\log k$, так как $k^{\varepsilon}/\log k=(k/\log k):k^{1-\varepsilon}$ вследствие (51) неограниченно возрастает. Естественно, функция $k/\log\log k$ также удовлетворяет этому требованию. Нужно, таким образом, показать, что $k/\log k$ дает истинный порядок роста.

Для этого используем введенную уже в § 31 функцию $\vartheta(x)=\sum_{p\leqslant x}\log p$. По (60) $\vartheta(x)<\beta x$. Рассмотрим часть этой суммы $\sum'\log p$, распространенную на $\alpha x\leqslant p\leqslant x$, $0<\alpha<1$, тогда из теоремы 22 следует

$$\frac{\vartheta(x)}{\alpha x}\geqslant\frac{1}{\alpha x}\sum'\log p\geqslant\sum'\frac{\log p}{p}=$$
$$=\log x-\log\alpha x-O(1)=\log\frac{1}{\alpha}-O(1).$$

Мы можем α выбрать столь малым, что правая часть окажется >1. Таким образом, имеем:

$$\alpha x<\vartheta(x)<\beta x. \tag{80}$$

Если $\sum''$ обозначает часть суммы для $\vartheta(x)$, распространенную на $\sqrt{x}<p\leqslant x$, члены которой, таким образом, больше, чем $\log\sqrt{x}$, то

$$[\pi(x)-\pi(\sqrt{x})]\log\sqrt{x}\leqslant\sum''\log p\leqslant\vartheta(x)\leqslant\pi(x)\log x.$$

Из (80) вследствие $\pi(\sqrt{x})\leqslant\sqrt{x}=O(x/\log x)$, следует

$$\alpha\frac{x}{\log x}<\pi(x)<\sqrt{x}+2\beta\frac{x}{\log x}<\gamma\frac{x}{\log x}.$$

Таким образом получена

Теорема 28. *Для всех* $x\geqslant 2$ *имеем:*

$$C_{21}\frac{x}{\log x}<\pi(x)<C_{22}\frac{x}{\log x}.$$

Теорема 28 принадлежит Чебышеву и является главным результатом классической теории простых чисел. По теореме 3 $C_{21} \leqslant 1 \leqslant C_{22}$ и для достаточно больших x C_{21} и C_{22} могут быть придвинуты к 1 сколь угодно близко.

По (80) $\vartheta(\beta x/\alpha) > \alpha\beta x/\alpha = \beta x > \vartheta(x)$, следовательно, между x и $\beta x/\alpha$ для любого x лежат простые числа. По сделанному выше замечанию из теоремы 3 следует, что для достаточно больших x и достаточно малых $\varepsilon > 0$ между x и $(1+\varepsilon)x$ лежат простые числа. С помощью глубоко лежащих методов Р. Бройш [2] доказал, что для $x \geqslant 48$ между x и $9x/8$ всегда имеются простые числа. Ингам доказал, что для всех достаточно больших x между x^3 и $(x+1)^3$ лежит простое число. Будет ли это справедливо для x^2 и $(x+1)^2$ — до сих пор не установлено. Дальнейшие утверждения этого типа мы получим в § 39.

37. Функции $\vartheta(x)$ и $\psi(x)$. Вместе с $\pi(x)$ и $\vartheta(x)$ в теории простых чисел играет роль и функция $\psi(x) = \sum_{p^m \leqslant x} \log p = \sum_{n \leqslant x} \Lambda(n)$, где $\Lambda(n)$ — функция, определенная в § 16.

Если p^m — наивысшая степень p, не превосходящая x, то в $\psi(x)$ $\log p$ встречается m раз, так что $\psi(x)$ равна логарифму общего наименьшего кратного чисел от 1 до $[x]$

$$\psi(x) = \log\{1, 2, \ldots, [x]\} = \sum_{p \leqslant x} \left[\frac{\log x}{\log p}\right] \log p. \qquad (81)$$

Пример. $\psi(10) = 3\log 2 + 2\log 3 + \log 5 + \log 7$. Так как неравенство $p^i \leqslant x$ равносильно неравенству $p \leqslant \sqrt[i]{x}$, то имеет место соотношение

$$\psi(x) = \vartheta(x) + \vartheta(x^{\frac{1}{2}}) + \vartheta(x^{\frac{1}{3}}) + \ldots = \sum \vartheta(x^{\frac{1}{r}}). \qquad (82)$$

Ряд оборвется, как только будет $x^{\frac{1}{r}} < 2$, т. е. $r > (\log x)/\log 2$. Несмотря не внешне сложное определение, $\psi(x)$ является одной из простейших функций характеризующей распределение простых чисел.

В (60) мы видели, что $\vartheta(x) = O(x)$. Это имеет место и для $\psi(x)$. Так как (82) содержит $O(\log x)$ членов, а для $x \geqslant 2$ будет $\vartheta(x) < x\log x$, $\vartheta(x^{1/r}) < x^{1/r}\log x \leqslant x^{1/2}\log x$ для $r \geqslant 2$, то имеем:

$$\psi(x) = \vartheta(x) + O(x^{\frac{1}{2}}\log^2 x) = \vartheta(x) + o(x) = O(x). \qquad (83)$$

Отсюда следует, что отношения $\psi(x)/x$ и $\vartheta(x)/x$ для $x \to \infty$ или оба стремятся к общему пределу, или оба не имеют предела. Теорема 3 эквивалентна тому факту, что этот предел существует и равен 1. Именно имеет место

Теорема 29. $\vartheta(x) \sim \pi(x) \log x$.

Доказательство. Имеем:

$$\pi(x) \log x \geqq \vartheta(x) \geqq \sum{}' \log p > (1-\delta) \log x \{\pi(x) - \pi(x^{1-\delta})\},$$

где сумма $\sum'$ распространена по всем p, для которых $x^{1-\delta} < p \leqq x$, $0 < \delta < 1$. Отсюда с помощью теоремы 28 вытекает неравенство

$$1 \geqq \frac{\vartheta(x)}{\pi(x) \log x} \geqq 1 - \delta - (1-\delta) \frac{\pi(x^{1-\delta})}{\pi(x)} \geqq 1 - \delta - \frac{C_{22}}{C_{21}} x^{-\delta}.$$

Положим $\delta = 1/\log\log x$, тогда $x^{\delta} \to \infty$ при $x \to \infty$, что и доказывает теорему 29.

Таким образом, соотношения $\vartheta(x) \sim x$, $\psi(x) \sim x$, $\pi(x) \log x \sim x$ равнозначны. Из определения $\vartheta(x)$ и $\psi(x)$ получаются также следующие другие формулировки теоремы 3:

$$p_1 p_2 \ldots p_{\pi(n)} \sim e^{n+o(n)} \quad \text{или} \quad \lim_{n\to\infty} \sqrt[n]{p_1 p_2 \ldots p_{\pi(n)}} = e,$$

$$\{1, 2, 3, \ldots, n\} \sim e^{n+o(n)} \text{или} \quad \lim_{n\to\infty} \sqrt[n]{\{1, 2, \ldots, n\}} = e.$$

Из теоремы 29 без асимптотического закона распределения простых чисел вытекает, что $(p_1 p_2 \ldots p_{\pi(n)})^{\frac{1}{\pi(n)}} \sim n^{1+o(1)}$ (среднее геометрическое).

38. Биномиальный коэффициент $\binom{2n}{n}$ может дать нам сведения о простых числах в интервале $n < p \leqq 2n$, так как вследствие $2p > 2n$ он содержит каждое из этих простых чисел точно в первой степени. Докажем прежде всего с помощью полной индукции неравенство

$$\frac{(2n)!}{n!\,n!} = \binom{2n}{n} > \frac{4^n}{2\sqrt{n}} \qquad (n > 1). \tag{84}$$

Из предположения о справедливости (84) для всех натуральных чисел $\leqq n$ вследствие $(2n+1)^2 > 4n(n+1)$ получаем:

$$\binom{2(n+1)}{n+1} = 2\,\frac{2n+1}{n+1}\binom{2n}{n} > \frac{2(2n+1)\,4^n}{2\sqrt{n(n+1)}\sqrt{n+1}} > \frac{4^{n+1}}{2\sqrt{n+1}},$$

что и доказывает (84) для всех $n>1$. В дальнейшем нам понадобится и сама по себе интересная

Теорема 30.

$$\prod_{p\leqslant x} p<4^x.$$

Доказательство[1]). Мы можем считать x целым. Для $x=2$ теорема справедлива; предположим, что она верна для всех $x\leqslant n-1$. Если n — четное, то теорема верна для $x=n$, так как n — не простое число. Пусть теперь $n=2k+1$. Все p, для которых $k+2\leqslant p\leqslant 2k+1$, являются делителями $\binom{2k+1}{k}$. Этот биномиальный коэффициент $<4^k$, что видно из неравенства

$$(1+1)^{2k+1}>\binom{2k+1}{k}+\binom{2k+1}{k+1}=2\binom{2k+1}{k}.$$

Отсюда и из предположения индукции

$$\prod_{p\leqslant 2k+1} p\leqslant\binom{2k+1}{k}\prod_{p\leqslant k+1} p<4^k\cdot 4^{k+1}=4^{2k+1},$$

что и доказывает теорему. По Россеру [21] более точно $\prod_{p\leqslant x} p<2{,}83^x$, далее $\prod_{p\leqslant x} p>2^x$ для $x>29$.

Рассмотрим теперь каноническое разложение $(2n)!/n!n!=\prod p^{e_p}$. Так как по (2) p входит в $n!$ с показателем $[n/p]+[n/p^2]+\ldots$, имеем:

$$e_p=\left(\left[\frac{2n}{p}\right]-2\left[\frac{n}{p}\right]\right)+\left(\left[\frac{2n}{p^2}\right]-2\left[\frac{n}{p^2}\right]\right)+\ldots \quad (85)$$

Если $n=qp^i+r$, $0\leqslant r<p^i$, то

$$\left[\frac{2n}{p^i}\right]-2\left[\frac{n}{p^i}\right]=\left[\frac{2r}{p^i}\right]=\begin{cases}0, & \text{если } \left[\frac{2n}{p^i}\right] \text{ четное,}\\ 1, & \text{если } \left[\frac{2n}{p^i}\right] \text{ нечетное.}\end{cases}$$

Таким образом, e_p равно количеству нечетных чисел в обрывающейся последовательности $[2n/p]$, $[2n/p^2]$,... Теперь мы можем сделать следующие утверждения:

---

[1]) Эрдёш — Кальмар.

a) Для $p \geqslant \sqrt{2n}$ будет $e_p \leqslant 1$. Для $p^2 = 2n$, где $p = 2 = n$, это ясно. Для $p^2 > 2n$ в (85) отличаться от нуля может не более чем одна круглая скобка.

b) Для $p^\alpha \leqslant 2n < p^{\alpha+1}$ будет $e_p \leqslant \alpha$, так как в (85) отличны от нуля не более α круглых скобок. Таким образом,

$$p^{e_p} \leqslant 2n \text{ и } \binom{2n}{n} \leqslant (2n)^{\pi(2n)}.$$

c) Для $2n/3 < p \leqslant n$ и $n > 2$ будет $e_p = 0$. Так как $2n/p < 3$, то для нечетного $[2n/p]$ следует рассмотреть лишь случай $1 < 2n/p < 2$, а это означает, что $p > n$. В этом случае p должно быть нечетным, так как из $p = 2$ следовало бы $n < 3$, тогда как по предположению $n > 2$.

d) Для $n < p < 2n$ всегда $e_p = 1$, так как $1 < 2n/p < 2$.

39. Теорема Чебышева. В 1852 г. Чебышев доказал, что для любого $n \geqslant 1$ среди чисел $n+1$, $n+2, \ldots$, $2n$ встречается по крайней мере одно простое число. Таким образом, имеет место

Теорема 31. $\pi(2n) - \pi(n) \geqslant 1$ для $n \geqslant 1$.

Доказательство [1]). Достаточно показать, что произведение P_n всех p из интервала $n < p \leqslant 2n$ не является пустым, т. е. > 1. Положим $\binom{2n}{n} = Q_n P_n$, тогда по § 38 (c) в Q_n не входят простые множители $p > 2n/3$. Произведение всех различных $p | Q_n$ не превосходит, таким образом, произведения всех $p \leqslant 2n/3$, следовательно, по теореме 30 оно $< 4^{2n/3}$. По § 38 (a) неравенство $e_p > 1$ возможно лишь для $p < \sqrt{2n}$, а число таких p будет $\leqslant (\sqrt{2n})/2 = \sqrt{n/2}$. Произведение соответственных степеней p^{e_p} по § 38 (b) будет $\leqslant (2n)^{\sqrt{n/2}}$. Таким образом, $Q_n \leqslant 4^{2n/3} (2n)^{\sqrt{n/2}}$, где p с показателем $e_p > 1$, в правой части учитываются с показателями $e_p + 1$ вместо $e_p - 1$.

Учитывая (84), получаем теперь

$$P_n > \frac{4^n}{2\sqrt{n}} Q_n^{-1} \geqslant \frac{4^{\frac{n}{3}}}{2\sqrt{n}\,(2n)^{\sqrt{n}}} \tag{86}$$

Возведя дробь, стоящую в правой части, в квадрат, увидим, что $P_n > 1$, как только $4^{2n/3} > 2(2n)^{\sqrt{2n}+1}$. Положим

[1]) По Финслеру [8].

$2n = x^2$, тогда должно быть $4^{x^2/3} > 2x^{2(x+1)}$. Это верно для $x = 12$. Легко убедиться в том, что производная логарифма левой части для $x \geqslant 7$ больше производной логарифма правой части, так как для $x \geqslant 7$ будет $0{,}667\, x \log 2 > 1 + x^{-1} + \log x$. Таким образом, $p_n > 1$ для всех $n = 0{,}5x^2 \geqslant 72$. Если p — наибольшее простое число интервала $a < p \leqslant 2a$, то теорема 31 очевидно верна для $a \leqslant n \leqslant p - 1$. Таким образом, достаточно простых чисел 2, 3, 5, 7, 13, 23, 43, 83, чтобы обеспечить справедливость теоремы 31 для $n < 72$.

Финслер получил таким методом значительно лучшую оценку для $\pi(2n) - \pi(n)$. Обозначим дробь, стоящую в правой части (86), через $(2n)^x$, так что $P_n > (2n)^x$, тогда $x < \pi(2n) - \pi(n)$, так как по определению P_n не содержит квадратов. Легко убедиться в том, что для $n \geqslant 2500$

$$x \log 2n = \frac{n}{3}\left(\log 4 - \frac{3 \log 4n}{2n} - \frac{3 \log 2n}{\sqrt{2n}}\right) > \frac{n}{3}.$$

Из таблиц простых чисел видно, что $\pi(2n) - \pi(n) \geqslant 2,\ 3,\ 9,\ 25,\ 50,\ 100$, если $n \geqslant 6,\ 9,\ 36,\ 135,\ 321,\ 720$. Так как $n/3 \log 2n < 1,\ 3,\ 9,\ 25,\ 50,\ 100$ для $n \leqslant 8,\ 39,\ 150,\ 500,\ 1000,\ 2500$, то вообще $\pi(2n) - \pi(n) > x > n/3 \log 2n$.

Для того чтобы получить оценку сверху, используем неравенство $\binom{2n}{n} < 4^n$. Оно вытекает из равенства $(1+1)^{2n} = \sum_{k=0}^{2n} C_{2n}^k$. Отсюда

$$[\pi(2n) - \pi(n)] \log n \leqslant \sum_{n < p \leqslant 2n} \log p =$$

$$= \log P_n \leqslant \log \binom{2n}{n} < n \log 4 < \frac{7n}{5}.$$

Таким образом доказана принадлежащая Финслеру

Теорема 32.

$$\frac{n}{3 \log 2n} < \pi(2n) - \pi(n) < \frac{7n}{5 \log n} \qquad (n > 1).$$

40. Числовые значения для постоянных C_{21} и C_{22} теоремы 28. Из § 38 (b) следует, что если $\log(2n)!$ взять за верхнюю, а $\log n!$ за нижнюю интегральную сумму соответ-

ствующего интеграла, то

$$\pi(2n)\log 2n \geqslant \log(2n)! - 2\log n! =$$

$$= \sum_{k=1}^{2n} \log k - 2\sum_{k=1}^{n} \log k > \int_1^{2n} \log x\,dx - 2\int_2^{n+1} \log x\,dx =$$

$$= 2n\log 2n - 2(n+1)\log(n+1) + 4\log 2 - 1,$$

$$\frac{\pi(2n)\log 2n}{2n} > \log 2 - \frac{\log n}{n} - \left(1+\frac{1}{n}\right)\log\left(1+\frac{1}{n}\right) + \frac{4\log 2+1}{2n}.$$

Для $n \geqslant 200$ правая часть $\geqslant 2/3$. Если в левой части заменить $2n$ на $2n-1$, то неравенство сохранится, так как левая часть увеличится, поскольку $\pi(2n) = \pi(2n-1)$. Как показывает непосредственная проверка для $x = p - 1 < 400$, имеем $C_{21} = 2/3$ для всех $x > 1$.

Следующие вспомогательные вычисления способствуют получению хорошего значения для C_{22}. Если $\alpha > 1{,}4$ — вещественная постоянная и $x \geqslant 2^s$, где

$$s \geqslant \frac{5\alpha+7}{5\alpha-7},$$

то имеем:

$$\left(\alpha - \frac{7}{5}\right)\log x = 2\alpha\log x - \left(\alpha+\frac{7}{5}\right)\log x \geqslant \left(\alpha+\frac{7}{5}\right)\log 2,$$

$$\left(\alpha+\frac{7}{5}\right)\frac{x}{\log x} \leqslant \alpha\frac{2x}{\log 2x}. \tag{87}$$

Предположим теперь, что оценка $\pi(x) < \alpha x/x\log x$ справедлива для $x < 2^{s+1}$, следовательно, в частности, и для интервала $2^s \leqslant x < 2^{s+1}$. Из теоремы 32 и (87) теперь следует

$$\pi(2x) = \pi(2x) - \pi(x) + \pi(x) < \left(\frac{7}{5}+\alpha\right)\frac{x}{\log x} \leqslant \alpha\frac{2x}{\log 2x},$$

т. е. оценка с постоянной α имеет место и для интервала $2^{s+1} \leqslant x < 2^{s+2}$ и, следовательно, вообще верна. Для доказательства неравенства для $x < 2^{s+1}$ заметим, что для $x_1 < x < x_2$ из $\pi(x_2) < \alpha x_1/\log x_1$ следует

$$\pi(x) < \pi(x_2) < \frac{\alpha x_1}{\log x_1} < \frac{\alpha x}{\log x}.$$

Положим теперь $\alpha = 8/5$, так что $s = 15$. Так как $30\,000 < 2^{15} < 2^{16} < 70\,000$, приводимая таблица показывает справедливость оценки для $2^{15} \leqslant x < 2^{16}$. Продолжением таблицы [1]) оценка легко проверяется для всех $x < 2^{16}$, так что для всех $x \geqslant 1$ постоянная $C_{22} = 1{,}6$.

x	$\pi(x)$	$1{,}6\,x/\log x$
70 000	6 935	10 041
50 000	5 133	7 395
40 000	4 203	6 043
30 000	3 245	4 657

Очень хорошую численную оценку несколько другого рода указал Россер [21]. Для $x \geqslant 55$ имеем:

$$\frac{x}{\log x + 2} < \pi(x) < \frac{x}{\log x - 4}.$$

41. Логарифмическое свойство $\pi(x)$. Согласно Ишикава [11] имеет место

Теорема 33. $\pi(xy) > \pi(x) + \pi(y)$ для $y \geqslant 2$, $x \geqslant 6$, $x \geqslant y$.

Доказательство. а) Пусть $2 \leqslant y < 10$, $x \geqslant 57$, так что $\pi(y) \leqslant 4$.

Из теоремы 32 теперь вытекает

$$\pi(xy) \geqslant \pi(2x) = \pi(2x) - \pi(x) + \pi(x) > \pi(x) + \frac{x}{3\log 2x} \geqslant$$
$$\geqslant \pi(x) + 4 \geqslant \pi(x) + \pi(y).$$

б) Для $y \geqslant 10$ воспользуемся теоремой 28 с $C_{21} = 2/3$ и $C_{22} = 8/5$. Получаем:

$$\pi(xy) - \pi(x) > \frac{2xy}{3\log xy} - \frac{8x}{5\log x} \geqslant \frac{20x}{3\log x^2} - \frac{8x}{5\log x} =$$
$$= \frac{26\,x}{15\log x} > \frac{8y}{5\log y} > \pi(y).$$

Для $6 \leqslant x < 57$ теорему 33 можно проверить непосредственно, рассматривая простые значения x и y.

[1]) За 20 следующих шагов доходят до $x < 20$.

42. Утверждения о n-м простом числе p_n. Эквивалентной теореме 3 будет

Теорема 34. $p_n \sim n \log n$.

Доказательство. Положим $y = \pi(x)$, тогда из теоремы 3 при $x \to \infty$ следует $\log y + \log\log x - \log x \to 0$, следовательно, $(\log y)/(\log x) \to 1$ и

$$\frac{y \log y}{x} = \frac{y}{x} \frac{\log x}{\log x} \frac{\log y}{\log x} \to 1.$$

Для $x = p_n$ будет $\pi(p_n) = n$, и мы получаем, что $n \log n \sim p_n$. Вывод теоремы 3 из теоремы 34 мы оставляем читателю. Сверх теоремы 34 известно, что для любого n (Россер [20])

$$n \log n < p_n < n(\log n + [1 + o(1)] \log\log n).$$

Обе следующие теоремы принадлежат Ишикава:

Теорема 35. $p_n + p_{n+1} > p_{n+2}$ *для* $n > 1$.

Доказательство. По теореме 32 для $p_n \geqslant 7$ между p_n и $p_n + p_{n+1} > 2p_n$ лежат по крайней мере два простых числа p_{n+1} и p_{n+2}. Так как $3 + 5 > 7$ и $5 + 7 > 11$, то теорема верна вообще.

Теорема 36. $p_m p_n > p_{m+n}$.

Доказательство. Пусть $m \leqslant n$.

а) $m = 1, 2, 3$; $n \geqslant 2$. Из теоремы 35 следует

$$p_1 p_n = 2p_n > p_{n-1} + p_n > p_{n+1},$$
$$p_2 p_n = 3p_n > p_{n-1} + p_n + p_n \geqslant p_{n+1} + p_n > p_{n+2}.$$

Использовав теорему 31, получаем далее

$$p_3 p_n = 5p_n > p_{n-1} + 4p_n \geqslant p_{n+1} + 3p_n > p_{n+2} + 2p_n > p_{n+2} + p_{n+1} > p_{n+3}.$$

б) $m \geqslant 4$. Теорема 33 приводит к неравенству

$$\pi(p_m p_n) > \pi(p_m) + \pi(p_n) = m + n = \pi(p_{m+n}),$$

следовательно, $p_m p_n > p_{m+n}$, ч. т. д.

Из теоремы 36 получаем неравенство

$$\prod_{k=1}^{n} p_k p_{n+1-k} > p_{n+1}^n,$$

которая приводит к оценке [1])

$$p_{n+1} < \left\{ \prod_{k=1}^{n} p_k \right\}^{\frac{2}{n}}. \tag{88}$$

Формула (88) дает возможность доказать следующее утверждение: если постоянное $r \geqslant 1$ и $n \geqslant p_{2(r+1)}^{r+1}$, то среди $\varphi(n)$ чисел $\leqslant n$ и взаимно простых с n существует по крайней мере одна степень простого p_{n+1}^{r+1}. Если бы n делилось на $p_1, p_2, \ldots, p_{2r+2}$ и уже $p_{2r+3}^{r+1} \geqslant n$, то имели бы — в противоречии с (88) — неравенство $p_1 p_2 \ldots p_{2r+2} \leqslant n \leqslant p_{2r+3}^{r+1}$. Для $r = 1$ должно быть $n \geqslant 49$. Известно, что 30 является последним числом m, которое обладает тем свойством, что все числа, взаимно простые с m и меньшие m, являются простыми.

Если $\pi(x)$ известно для достаточно большого количества чисел $x \geqslant n$, то p_n можно вычислить, пользуясь следующим алгоритмом Бруна. Построим числа

$$n_i = n - \pi(n + n_1 + \ldots + n_{i-1}) \qquad (i = 1, 2, \ldots).$$

Очевидно, $n \geqslant n_1 \geqslant n_2 \geqslant \ldots$ Так как

$$n_i - n_{i+1} = \pi(n + n_1 + \ldots + n_i) - \\ - \pi(n + n_1 + \ldots + n_{i-1}) \leqslant n_i,$$

то все $n_i \geqslant 0$, так что всегда $n \geqslant \pi(n + n_1 + \ldots + n_{i-1})$. Так как правая часть возрастает, то должно встретиться $n_r = 0$, чем процесс и будет прерван. Тогда $p_n = n + n_1 + \ldots + n_{r-1}$.

Пример.

$n = 8$,
$n_1 = 8 - \pi(8) = 4$,
$n_2 = 8 - \pi(12) = 3$,
$n_3 = 8 - \pi(15) = 2$,
$n_4 = 8 - \pi(17) = 1$,
$n_5 = 8 - \pi(18) = 1$,
$n_6 = 8 - \pi(19) = 0$,
$p_8 = 8 + 4 + 3 + 2 + 1 + 1 = 19$.

43. Разность между двумя последовательными простыми числами. Значительная нерегулярность в распределении простых чисел проявляется в поведении разности $d_n = p_{n+1} - p_n$, которая была предметом многочисленных исследований [2]).

---

[1]) Более слабую оценку такого типа с постоянным показателем корня получил Э. Цермело [32].

[2]) Подробное представление об этом дает G. Ricci, La differenza di numeri primi consecutivi, Rendiconti Seminario Mat. Torino 11, 149—200 (1951).

Теорема 40 особенно ясно показывает, что d_n не ограничено. Известно даже, что верхняя грань для $d_n/\log p_n$ бесконечна. С другой стороны, существует предположение, что $d_n = 2$ для бесконечного множества n (существование бесконечного множества пар простых близнецов). Это означало бы, что d_n постоянно колеблется между 2 и сколь угодно большими значениями.

Эрдёш и Туран доказали, что нет такого места, начиная с которого d_n монотонно возрастало бы или убывало.

Для достаточно больших n по Ингаму $d_n < p_n^{5/8}$. Полиньяк высказал предположение, что среди чисел $d_2, d_3, \ldots$ каждое четное число встречается бесконечно часто. Прахару недавно удалось показать с помощью метода решета Бруна, что множество различных d_n по меньшей мере имеет положительную плотность [1]).

44. Дзета-функция Римана $\zeta(s)$ [2]) обоими представлениями

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p} (1 - p^{-s})^{-1}, \quad s = \sigma + i\tau \tag{89}$$

определена как аналитическая, регулярная для $\sigma > 1$. Представление бесконечным произведением в (89) является аналитическим эквивалентом теоремы 1; оно показывает, что $\zeta(s)$ тесно связана с распределением простых чисел. Мы можем легко установить зависимость между $\zeta(s)$ и $\pi(x)$. Для $\sigma > 1$ из (89), (63) и теоремы 27 следует

$$\log \zeta(s) = -\sum_{p} \log(1 - p^{-s}) =$$

$$= -\sum_{n=2}^{\infty} \{\pi(n) - \pi(n-1)\} \log(1 - n^{-s}) =$$

$$= \sum_{n=2}^{\infty} \pi(n) \{\log(1 - n^{-s}) - \log[1 - (n+1)^{-s}]\} =$$

$$= \sum_{n=2}^{\infty} \pi(n) \int_{n}^{n+1} \frac{s\,dx}{x(x^s - 1)} = s \int_{2}^{\infty} \frac{\pi(x)}{x(x^s - 1)}\, dx.$$

---

[1]) О понятии плотности см. § 74.

[2]) Этот параграф дает некоторые сведения об аналитической теории простых чисел.

Дзета-функция, определенная до сих пор лишь в полуплоскости $\sigma > 1$, допускает продолжение на всю комплексную плоскость и оказывается регулярной для всех s, кроме $s = 1$, где она имеет простой полюс с вычетом 1. $\zeta(s)$ удовлетворяет функциональному уравнению

$$\zeta(s) = 2^s \pi^{s-1} \sin\frac{\pi s}{2} \Gamma(1-s)\zeta(1-s)^1). \qquad (90)$$

Особый интерес представляют нули функции $\zeta(s)$. Так как произведение в (89) сходится, то $\zeta(s) \neq 0$ для $\sigma > 1$. Из уравнения (90) следует, что $\zeta(s) \neq 0$ для $\sigma < 1$, за исключением точек $s = -2, -4, -6, \ldots$, где $\sin \pi s/2$ обращается в нуль, а $\Gamma(1-s)$ — нет. Таким образом, все нули $\zeta(s)$, кроме «тривиальных» $-2, -4, \ldots$, лежат в полосе $0 \leqslant \sigma \leqslant 1$. Все нетривиальные нули ρ являются комплексными числами и их бесконечно много. Вследствие (90) вместе с $\rho = \alpha + i\beta$ нулями являются также $1-\rho$ и $1-\bar{\rho} = 1 - -\alpha + i\beta$, так что или все ρ лежат на прямой $\sigma = 1/2$, или расположены парами симметрично относительно этой прямой. Риман предположил, что имеет место лишь первая возможность, т. е. что всегда $\alpha = 1/2$. Эта знаменитая гипотеза до сих пор не доказана и не опровергнута. Все же, непосредственным вычислением можно показать, что все ρ, ординаты которых по модулю $\leqslant 1468$, действительно лежат на $\sigma = 1/2$. Если $N_0(T)$ означает количество $\rho = 1/2 + i\tau$, для которых $0 < \tau \leqslant T$, то $N_0 > C_{30} T \log T$. Этот результат, полученный недавно А. Сельбергом, показывает, что на прямой $\sigma = 1/2$ лежит конечная часть ρ, так как известно, что количество всех ρ, удовлетворяющих условию $0 < \tau \leqslant T$, $0 \leqslant \sigma \leqslant 1$, асимптотически равно $(2\pi)^{-1} T \log T$.

Для теории чисел важно как можно больше расширить область, не содержащую нулей $\zeta(s)$. Адамар и Валле — Пуссен доказали в 1896 г., что $\zeta(s)$ не имеет нулей на прямой $\sigma = 1$, а значит, вследствие (90) и на прямой $\sigma = 0$, и пока-

---

[1]) Гамма-функция $\Gamma(s)$ определяется разложением

$$\frac{1}{\Gamma(s)} = s e^{Cs} \prod_{n=1}^{\infty} \left\{ \left(1 + \frac{s}{n}\right) e^{-\frac{s}{n}} \right\}, \quad C = 0{,}577\ldots$$

Она везде регулярна, кроме точек $s = 0, -1, -2, \ldots$, в которых имеет простые полюсы.

зали, что это утверждение эквивалентно асимптотическому закону распределения простых чисел. Формула

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

справедливая для $\sigma > 1$, верна, таким образом, еще и для $\sigma = 1$, и вытекающее отсюда соотношение $\sum \mu(n)/n = 0$, справедливость которого предположил еще в 1748 г. Эйлер, оказывается равнозначным асимптотическому закону распределения простых чисел.

Риман указал интересную зависимость между $\pi(x)$ и комплексными нулями $\zeta(s)$. Пусть

$$f(x) = \pi(x) + \frac{1}{2}\pi\left(x^{\frac{1}{2}}\right) + \frac{1}{3}\pi\left(x^{\frac{1}{3}}\right) + \ldots = \sum_{n=1}^{\infty} \frac{1}{n}\pi\left(x^{\frac{1}{n}}\right). \quad (91)$$

Пример.

$$f(12) = \pi(12) + \frac{1}{2}\pi\left(\sqrt{12}\right) + \frac{1}{3}\pi\left(\sqrt[3]{12}\right) = 5 + \frac{1}{2}\cdot 2 + \frac{1}{3}\cdot 1 = 6\frac{1}{3}.$$

$f(x)$ получается, если к $\pi(x)$ прибавить половину числа тех p, для которых $p^2 \leqslant x$, одну треть тех p, для которых $p^3 \leqslant x$, и т. д. Если $x^{1/m} \geqslant 2$, $x^{1/(m+1)} < 2$, то (91) содержит m членов, отличных от нуля, так как $m \leqslant (\log x)/(\log 2)$. Каждый член, очевидно, не больше предыдущего и так как $\pi(x) = O(x/\log x)$, то

$$f(x) - \pi(x) = \frac{1}{2}\pi\left(x^{\frac{1}{2}}\right) + O\left[\pi\left(x^{\frac{1}{3}}\right)\log x\right] = O\left(\frac{x^{\frac{1}{2}}}{\log x}\right) + O\left(x^{\frac{1}{3}}\right) = O\left(\frac{x^{\frac{1}{2}}}{\log x}\right).$$

Таким образом, при замене $\pi(x)$ на $f(x)$ допускается относительная ошибка $O\left(1/\sqrt{x}\right) = o(1)$. Впрочем, (91) допускает

обращение. Положив $u=mn$ с помощью (18), получаем:

$$\sum_{m=1}^{\infty}\frac{\mu(m)}{m}f\left(x^{\frac{1}{m}}\right)=\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}\frac{\mu(m)}{mn}\pi\left(x^{\frac{1}{mn}}\right)=$$

$$=\sum_{u=1}^{\infty}\sum_{m\mid u}\frac{\mu(m)}{u}\pi\left(x^{\frac{1}{u}}\right)=\pi(x).$$

Если положить теперь $f_0(x)=f(x)$ для $x\neq p^r\,(r\geqslant 1)$ и $f_0(x)=f(x)-\frac{1}{2}r$ для $x=p^r$ (среднее значение в точках скачкообразного разрыва $f(x)$), то имеет место формула Римана, доказанная в 1895 г. фон Мангольдтом [1]),

$$f_0(x)=\operatorname{li}x-\sum_{\rho}\operatorname{li}x^{\rho}+\int_x^{\infty}\frac{du}{(u^2-1)\,u\log u}-\log 2\quad(x>1).$$

Здесь $\operatorname{li}x$ — интегральный логарифм, определенный для вещественных x равенством

$$\operatorname{li}x=\lim_{\delta\to 0}\left(\int_0^{1-\delta}\frac{dy}{\log y}+\int_{1+\delta}^{x}\frac{dy}{\log y}\right)=1{,}04\ldots+\int_2^x\frac{dy}{\log y}>\frac{x}{\log x}.$$

Сумма, распространенная на комплексные нули, расположена по возрастающим ординатам ρ.

Интегрированием по частям находим:

$$\operatorname{li}x=O(1)+\frac{x}{\log x}+\int_2^{\sqrt{x}}\frac{du}{\log^2 u}+\int_{\sqrt{x}}^{x}\frac{du}{\log^2 u}<$$

$$<O(1)+\frac{x}{\log x}+\frac{\sqrt{x}-2}{\log^2 2}+\frac{x-\sqrt{x}}{\log^2\sqrt{x}}=$$

$$=\frac{x}{\log x}+O(1)+O\left(\sqrt{x}\right)+O\left(\frac{x}{\log^2 x}\right)=$$

$$=\frac{x}{\log x}+O\left(\frac{x}{\log^2 x}\right).\qquad(92)$$

---

[1]) Ср. Ингам [9] (русский перевод, стр. 107), где $\operatorname{li}z$ определен для комплексных z.

Отсюда вытекает, что $\operatorname{li} x \sim x/\log x \sim \pi(x)$. Помещенная ниже таблица показывает, как можно было ожидать вследствие формулы Римана, что $\operatorname{li} x$ дает лучшее приближение к $\pi(x)$, чем $x/\log x$. Порядок роста разности $P(x) = \pi(x) - \operatorname{li} x$ обстоятельно изучался.

Если ϑ является верхним пределом вещественной части ρ, следовательно $0{,}5 \leqslant \vartheta < 1$, то $P(x) = O(x^{\vartheta} \log x)$.

Точность приближения $\pi(x)$ функцией $\operatorname{li} x$, таким образом, существенно зависит от расположения ρ. Из справедливости гипотезы Римана следовало бы, таким образом, $P(x) = O(x^{1/2} \log x)$. Это — очень сильная оценка, так как известно, что равенство $P(x) = O(x^{\alpha})$ для $\alpha < 0{,}5$ не может быть справедливым.

Хотя в пределах таблиц $P(x)$ все время остается отрицательной, знак этой величины должен бесконечно много раз изменяться. Этот факт установлен Литтльвудом независимо от того, справедлива или нет гипотеза Римана. Правда, не известно такое x_0, что $P(x_0) > 0$. Принимая гипотезу Римана, Скевес вывел, что существует x_0, меньшее чем $10^{10^{10^{34}}}$.

x	$\pi(x)$	$\operatorname{li} x$	$\frac{\pi(x)}{\operatorname{li} x}$	$\frac{\pi(x)}{x/\log x}$
1 000	168	178	0,94	1,159
10 000	1 226	1 246	0,98	1,132
50 000	5 133	5 167	0,993	1,111
100 000	9 592	9 630	0,996	1,104
500 000	41 538	41 606	0,9983	1,090
1 000 000	78 498	78 628	0,9983	1,084
2 000 000	148 933	149 055	0,9991	1,080
5 000 000	348 513	348 638	0,9996	1,075
10 000 000	664 579	664 918	0,9994	1,071
20 000 000	1 270 607	1 270 905	0,9997	1,068
90 000 000	5 216 954	5 217 810	0,99983	1,062
100 000 000	5 761 455	5 762 209	0,99986	1,061
1 000 000 000	50 847 478	50 849 235	0,99996	1,053

VII. ЭЛЕМЕНТАРНОЕ ДОКАЗАТЕЛЬСТВО АСИМПТОТИЧЕСКОГО ЗАКОНА РАСПРЕДЕЛЕНИЯ ПРОСТЫХ ЧИСЕЛ

45. Формула Сельберга. Основой всех элементарных доказательств является формула А. Сельберга, которую, следуя Исеки и Татузава [10], мы докажем в следующей форме.

Теорема 37.

$$\psi(x)\log x+\sum_{n\leqslant x}\psi\left(\frac{x}{n}\right)\Lambda(n)=2x\log x+O(x). \quad (93)$$

Доказательство. Прежде всего мы покажем, что если $F(x)$ и $G(x)$ определены для $x\geqslant 1$ и $G(x)=\sum\limits_{m\leqslant x}F(x/m)\log x$, то

$$F(x)\log x+\sum_{n\leqslant x}F\left(\frac{x}{n}\right)\Lambda(n)=\sum_{d\leqslant x}\mu(d)\,G\left(\frac{x}{d}\right). \quad (94)$$

Вследствие (18) и (22) имеем:

$$F(x)\log x+\sum_{n\leqslant x}F\left(\frac{x}{n}\right)\Lambda(n)=$$

$$=\sum_{n\leqslant x}F\left(\frac{x}{n}\right)\log\frac{x}{n}\sum_{a\mid n}\mu(d)+\sum_{n\leqslant x}F\left(\frac{x}{n}\right)\sum_{d\mid n}\mu(d)\log\frac{n}{d}=$$

$$=\sum_{n\leqslant x}F\left(\frac{x}{n}\right)\sum_{a\mid n}\mu(d)\left\{\log\frac{x}{n}+\log\frac{n}{d}\right\}=\sum_{n\leqslant x}F\left(\frac{x}{n}\right)\sum_{d\mid n}\mu(d)\log\frac{x}{d}.$$

Изменив порядок суммирования, получим, что последняя двойная сумма равна

$$\sum_{d\leqslant x}\mu(d)\sum_{m\leqslant\frac{x}{d}}F\left(\frac{x}{md}\right)\log\frac{x}{d}=\sum_{d\leqslant x}\mu(d)\,G\left(\frac{x}{d}\right).$$

Положим в (94), во-первых, $F=F_1(x)=\psi(x)$, тогда из (21) и (54), положив $mn=k$, получим:

$$G_1(x)=\sum_{m\leqslant x}\Psi\left(\frac{x}{m}\right)\log x=\log x\sum_{mn\leqslant x}\Lambda(n)=$$

$$=\log x\sum_{k\leqslant x}\sum_{n\mid k}\Lambda(n)=\log x\sum_{k\leqslant x}\log k=$$

$$=x\log^2 x-x\log x+O(\log^2 x).$$

Теперь положим $F = F_2(x) = x - C_3 - 1$, где C_3 — постоянная формулы (52). Тогда с помощью (52) получаем:

$$G_2(x) = \log x \sum_{m \leqslant x} \left\{ \frac{x}{m} - C_3 - 1 \right\} =$$
$$= x \log^2 x + C_3 x \log x + O(\log x) - (C_3 + 1) x \log x =$$
$$= x \log^2 x - x \log x + O(\log x).$$

Так как $O(\log x) = O(\log^2 x) = O(\sqrt{x})$, то G_1 и G_2 будут равны, если в обоих случаях поставить остаточный член $O(\sqrt{x})$. Теперь

$$\sum_{d \leqslant x} \mu(d)\, O\left(\sqrt{\frac{x}{d}}\right) = O\left(\sum_{d \leqslant x} \sqrt{\frac{x}{d}}\right) = O\left(\sqrt{x} \int_0^x \frac{d\xi}{\sqrt{\xi}}\right) = O(x),$$

так что теперь для F_1 и F_2 правые части в (94) совпадают до величин $O(x)$. Это должно иметь место и для левых частей. Для F_1 левая часть совпадает с левой частью формулы (93). Таким образом, нужно вычислить левую часть (94) для F_2. Из (61) и (83) получаем:

$$(x - C_3 - 1) \log x + \sum_{n \leqslant x} \left\{ \frac{x}{n} - C_3 - 1 \right\} \Lambda(n) =$$
$$= 2x \log x - (C_3 + 1)[\log x + \psi(x)] + O(x) = 2x \log x + O(x).$$

Теорема 37 доказана.

46. Применение формулы Сельберга. Мы будем пользоваться (93) с несколько худшим остаточным членом $O(x \log x)$[1]). Асимптотический закон будем доказывать в форме $\psi(x) \sim x$. Положим $\psi(x) = x + R(x)$, тогда нужно будет показать, что $R(x) = o(x)$. Из (61) и (93) следует

$$R(x) \log x + \sum_{n \leqslant x} R\left(\frac{x}{n}\right) \Lambda(n) = o(x \log x). \qquad (95)$$

Вычтем из обеих частей (95) $\sum R(x/n)\Lambda(n)$ и возьмем затем абсолютные величины, тогда

$$|R(x)| \log x \leqslant \sum_{n \leqslant x} \left| R\left(\frac{x}{n}\right) \right| \Lambda(n) + o(x \log x). \qquad (96)$$

[1]) В доказательстве Сельберга применяется $O(x)$ (см. Сельберг [22]).

В первую очередь мы так преобразуем (96), чтобы исчезли множители $\Lambda(n)$.

Напишем (93) в форме

$$\sum_{mn\leqslant x}\Lambda(m)\Lambda(n)=\sum_{n\leqslant x}\psi\left(\frac{x}{n}\right)\Lambda(n)=$$
$$=2x\log x-\psi(x)\log x+o(x\log x),$$

тогда из (62) с учетом (64), (83), (55) и вытекающего из (92) соотношения

$$\sum_{2\leqslant n\leqslant x}\frac{1}{\log n}=O(\operatorname{li}x)=O\left(\frac{x}{\log x}\right)$$

получаем:

$$\sum_{mn\leqslant x}\frac{\Lambda(n)\Lambda(m)}{\log nm}=\sum_{k=2}^{x}\{2k\log k-\psi(k)\log k+o(k\log k)\}\times$$
$$\times\left\{\frac{1}{\log k}-\frac{1}{\log(k+1)}\right\}+[2x\log x-\psi(x)\log x+o(x\log x)]\times$$
$$\times\frac{1}{\log(x+1)}=2x-\psi(x)+o(x). \quad (97)$$

Использовав получающееся из (97) выражение для $\psi(x)$, получаем далее:

$$\sum_{mn\leqslant x}\Lambda(m)\Lambda(n)=\sum_{n\leqslant x}\Lambda(n)\psi\left(\frac{x}{n}\right)=$$
$$=2x\sum_{n\leqslant x}\frac{\Lambda(n)}{n}-\sum_{n\leqslant x}\Lambda(n)\sum_{mr\leqslant\frac{x}{n}}\frac{\Lambda(m)\Lambda(r)}{\log mr}+o\left(x\sum_{n\leqslant x}\frac{\Lambda(n)}{n}\right).$$

Изменив порядок суммирования в двойной сумме, получим вследствие (61)

$$\sum_{mn\leqslant x}\Lambda(m)\Lambda(n)+\sum_{mr\leqslant x}\frac{\Lambda(m)\Lambda(r)}{\log mr}\psi\left(\frac{x}{mr}\right)=$$
$$=2x\log x+o(x\log x)\ ^{1}).$$

---

[1]) Если $k(x)=O[g(x)]$, то из $f(x)=o[k(x)+g(x)]$ следует, что $f(x)=o[g(x)]$.

Это равенство позволяет записать (93) в виде

$$\psi(x)\log x=\sum_{mr\leqslant x}\frac{\Lambda(m)\Lambda(r)}{\log mr}\psi\left(\frac{x}{mr}\right)+o(x\log x). \qquad (98)$$

Из (68) и (98) получаем:

$$R(x)\log x=\sum_{mr\leqslant x}\frac{\Lambda(m)\Lambda(r)}{\log mr}R\left(\frac{x}{mr}\right)+o(x\log x). \qquad (99)$$

Возьмем в (99) абсолютные величины и сложим с (96), тогда будет

$$2|R(x)|\log x\leqslant\sum_{n\leqslant x}\left|R\left(\frac{x}{n}\right)\right|\Lambda(n)+\sum_{mr\leqslant x}\frac{\Lambda(m)\Lambda(r)}{\log mr}\left|R\left(\frac{x}{mr}\right)\right|+$$
$$+o(x\log x).$$

С помощью частного суммирования, учитывая, что последний член в (62) вследствие (83), (97) и неравенства $R[x/(x+1)]|<1$ входит в остаточный член, получаем:

$$2|R(x)|\log x\leqslant\sum_{k\leqslant x}\left\{\sum_{n\leqslant k}\Lambda(n)+\sum_{mr\leqslant k}\frac{\Lambda(m)\Lambda(r)}{\log mr}\right\}\times$$
$$\times\left\{\left|R\left(\frac{x}{k}\right)\right|-\left|R\left(\frac{x}{k+1}\right)\right|\right\}+o(x\log x)$$

или вследствие (97)

$$2|R(x)|\log x\leqslant 2\sum_{k\leqslant x}k\left\{\left|R\left(\frac{x}{k}\right)\right|-\left|R\left(\frac{x}{k+1}\right)\right|\right\}+$$
$$+o\left(\sum_{k\leqslant x}k\left\{\left|R\left(\frac{x}{k}\right)\right|-\left|R\left(\frac{x}{k+1}\right)\right|\right\}\right)+o(x\log x). \qquad (100)$$

При этом вследствие (63)

$$\sum_{k\leqslant x}k\left\{\left|R\left(\frac{x}{k}\right)\right|-\left|R\left(\frac{x}{k+1}\right)\right|\right\}=$$
$$=\sum_{k\leqslant x}\left|R\left(\frac{x}{k}\right)\right|-[x]\left|R\left(\frac{x}{[x]+1}\right)\right|=$$
$$=\sum_{k\leqslant x}\left|R\left(\frac{x}{k}\right)\right|+o(x\log x). \qquad (101)$$

Вследствие (83) $R(x)=O(x)$, так что из (101) и (52) на основании примечания на стр. 82 следует, что первый o- член

в (100) также имеет порядок $o(x\log x)$. Из (100) и (101) получаем теперь важное неравенство

$$|R(x)|\leqslant\frac{1}{\log x}\sum_{k\leqslant x}\left|R\left(\frac{x}{k}\right)\right|+o(x). \tag{102}$$

С помощью (102) мы докажем, что для каждого (сколь угодно малого) $\varepsilon>0$ существует такое $\eta=\eta(\varepsilon)$, что $|R(x)|<\varepsilon x$ для всех $x>\eta$. Это, очевидно, эквивалентно утверждению $R(x)=o(x)$.

47. Лемма А. *Для $z'>z$ имеем* $|R(z)-R(z')|\leqslant z'-z+o(z')$.

Доказательство. Так как $\psi(z')-\psi(z)=z'-z+R(z')-R(z)\geqslant 0$, то при $R(z')-R(z)<0$ утверждение теоремы очевидно. В противном случае, положив в (97) $x=z'$, $x=z$, после вычитания получим:

$$R(z')-R(z)+\sum_{z<mn\leqslant z'}\frac{\Lambda(n)\Lambda(m)}{\log mn}=z'-z+o(z').$$

Так как сумма неотрицательна, то лемма А верна и в этом случае.

48. Лемма В. *Если $\delta<1$ — произвольное фиксированное положительное число, то существуют такое $\rho(\delta)>1$ и такое $x_0=x_0(\delta)$, что для любого $x>x_0$ в промежутке $(x,\ \rho x)$ найдется такая точка y, для которой $|R(y)|<\delta y$.*

Доказательство. Из (83), (65) и (58) следует

$$\sum_{k\leqslant x}\frac{\psi(k)}{k^2}=\sum_{k\leqslant x}\frac{\vartheta(k)}{k^2}+O\left(\sum_{k\leqslant x}k^{-\frac{3}{2}}\log^2 k\right)=\log x+O(1)$$

или вследствие (52)

$$\sum\frac{R(k)}{k^2}=O(1),$$

где $O(1)$ ограничено для любого конечного x. Отсюда вытекает существование такой абсолютной постоянной $K_1>0$, что для всех $x>4$ и $\rho>1$

$$\left|\sum_{x\leqslant k\leqslant\rho x}\frac{R(k)}{k^2}\right|<K_1.$$

Действительно, если бы такой отрезок ряда мог принимать сколь угодно большие значения, то то же самое (с противо-

положным знаком) имело бы место и для суммы по k от 1 до x, тогда как известно, что эта сумма ограничена.

Если $R(k)$ не изменяет знак между x и ρx, то в интервале $x \leqslant y \leqslant \rho x$ существует такое y, что

$$\left|\frac{R(y)}{y}\right| \sum_{(x,\,\rho x)} \frac{1}{k} < \left| \sum_{(x,\,\rho x)} \frac{R(k)}{k^2} \right| < K_1,$$

так что вследствие (52) при соответствующей постоянной $K_2 \geqslant 1$ будет

$$\left|\frac{R(y)}{y}\right| < \frac{K_2}{\log \rho}.$$

Если же в промежутке $(x,\ \rho x)$ $R(k)$ изменяет знак, то будем различать два случая:

а) $R(y) = \psi(y) - y > 0$, $R(y+1) = \psi(y+1) - (y+1) < 0$. Если $\psi(y) = \psi(y+1)$, то $R(y) < 1$ и $R(y)/y < 1/y$. То же самое имеет место для $\psi(y+1) > \psi(y)$, так как из $\psi(y+1) = \psi(y) + \log p < y+1$ снова следует, что $R(y) < 1$ (и $p = 2$).

б) $R(y) < 0$, $R(y+1) > 0$, так что $y+1 = p^r$. Из того, что $R(y+1) = \psi(y) + r^{-1}\log(y+1) - y - 1 = R(y) + r^{-1}\log(y+1) - 1 > 0$, и из условия $R(y) < 0$ следует неравенство

$$\left|\frac{R(y)}{y}\right| < \frac{\log(y+1)}{ry} - \frac{1}{y} \leqslant \frac{\log(y+1) - 1}{y}.$$

Положим теперь $\rho = \rho(\delta) = e^{\frac{K_2}{\delta}}$ и выберем $x_0 = x_0(\delta) > 8$ столь большим, чтобы было $1 < \log(x_0 + 1) - 1 < \delta x_0$. Таким образом, во всех случаях лемма B доказана.

49. Лемма C. *Если $x \geqslant x_1(\delta) \geqslant x_0(\delta)$, то в интервале $(x,\ \rho x)$ содержится такой частичный интервал $y \leqslant z \leqslant e^{\delta/2} y$, что для любого z из него будет $|R(z)| < 3\delta z$.*

Доказательство. Из оценки леммы A следует

$$|R(z)| = |R(z) - R(y) + R(y)| \leqslant$$
$$\leqslant |R(z) - R(y)| + |R(y)| \leqslant |R(y)| + z - y + o(z).$$

Выберем на основании леммы B такое y, чтобы было $|R(y)| < \delta y$. Пусть теперь $x_1 = x_1(\delta)$ будет столь большим, что, во-первых, $x_1 \geqslant x_0(\delta)$ и, во-вторых, чтобы было

$$o(z) < 0{,}5\delta z \leqslant 0{,}5\delta e^{\frac{\delta}{2}} y.$$

Тогда вследствие неравенства $e^s < 1 + s + s^2(1-s)^{-1}$, $s < 1$ имеем:

$$\left|\frac{R(z)}{z}\right| \leqslant \left|\frac{R(z)}{y}\right| \leqslant \delta + e^{\frac{\delta}{2}} - 1 + 0{,}5\delta e^{\frac{\delta}{2}} < 2\delta + \frac{\delta^2}{2-\delta} < 3\delta$$

ч. т. д.

50. Доказательство асимптотического закона. На основании леммы C мы получаем теперь для постоянного $x_2 \geqslant x_1(\delta)$ последовательность (зависящую от δ) интервалов

$$x_2\rho^{i-1} < y_i \leqslant z \leqslant y_i e^{\frac{\delta}{2}} \leqslant x_2\rho^i \leqslant x, \quad (1 \leqslant i \leqslant t), \quad (103)$$

где

$$t = \left[(\log \rho)^{-1} \log\left(\frac{x}{x_2}\right)\right] = \left[\delta K_2^{-1} \log\left(\frac{x}{x_2}\right)\right].$$

Положим $z = x/n$, где x — постоянное и n — целое, тогда из (103) получаем соответствующую последовательность интервалов для n:

$$1 \leqslant \frac{x}{x_2}\rho^{-i} \leqslant \frac{x}{y_i}e^{-\frac{\delta}{2}} \leqslant n \leqslant \frac{x}{y_i} < \frac{x}{x_2}\rho^{-i+1} \leqslant \frac{x}{x_2}, \quad (104)$$
$$(1 \leqslant i \leqslant t).$$

Формула (103) осуществляет разбиение как на «широкие» интервалы $[x_2\rho^{i-1}, x_2\rho^i]$, так и на «узкие», когда выделяются еще и малые интервалы $(y, ye^{\delta/2})$. Из (82), (81), (80), теоремы 28 и § 40 для $x \geqslant 2$ и $0 < \alpha < 1$ получаем:

$$\alpha x < \vartheta(x) \leqslant \psi(x) \leqslant \pi(x)\log x < 1{,}6x,$$

следовательно, $|R(x)| < x$. Таким образом, для $x \geqslant x_2$ справедлива оценка $|R(x)| < \alpha_1 x$, где $\alpha \leqslant 1$. Положим теперь $\delta = \delta_1 = \alpha_1/6$. Тогда на малых интервалах получаем оценку

$$|R(z)| < \frac{\alpha_1 z}{2},$$

тогда как в общем случае было бы лишь $|R(z)| < \alpha_1 z$. Теперь напишем (102) в форме

$$|R(x)| \leqslant \frac{x}{\log x} \sum_{1 \leqslant \frac{x}{n}} \frac{1}{n} \left|\frac{n}{x} R\left(\frac{x}{n}\right)\right| + o(x). \quad (105)$$

Суммирование здесь производится по n, а x — это число из (103) и (104). Для интервала $1 \leqslant x/n < x_2$, примыкающего слева к последовательности интервалов (103), число n лежит в интервале $x/x_2 < n \leqslant x$, примыкающем к интервалам (104) справа. В этом интервале мы воспользуемся лишь оценкой $|R(z)| < z$.

Для остальных интервалов мы можем использовать оценку $\left|\frac{n}{x} R\left(\frac{n}{x}\right)\right| < \alpha_1$. Теперь из (105) и (52) получаем неравенство

$$|R(x)| < \frac{x}{\log x}\left[\log x_2 + O\left(\frac{x_2}{x}\right)\right] + \frac{\alpha_1 x}{\log x}\left[\log \frac{x}{x_2} + C_3 + O\left(\frac{x_2}{x}\right)\right] + o(x) = \alpha_1 x + o(x). \quad (106)$$

Это неравенство не дает какого-либо выигрыша для оценки $|R(x)|$. Учтем, однако, что для малых интервалов $y_i < z < y_i e^{\delta/2}$ справедлива оценка $|R(z)| < 0{,}5\,\alpha_1 z$, тогда можно будет получить более точную оценку для $|R(x)|$, если из правой части (106) вычесть лишнее. $\sum 1/n$ для i-го малого интервала в (104) имеет величину $\delta_1/2 + O(x_2 \rho^{i/x})$. Поэтому из правой части (106) вычитаем величину

$$\frac{\alpha_1 x}{2 \log x}\left\{t\,\frac{\delta_1}{2} + O\left(\frac{x_2}{x}\sum_{i=1}^{t}\rho^i\right)\right\} = \frac{\alpha_1 x}{2 \log x}\left\{t\,\frac{\delta_1}{2} + O\left[\frac{\rho}{\rho-1}\left(1-\frac{x_2}{x}\right)\right]\right\} = \frac{\alpha_1 \delta_1 x}{4 \log \rho}\left(1 - \frac{\log x_2}{\log x}\right) + o(x) = \frac{\alpha_1^3 x}{144 K_2} + o(x)$$

и получаем неравенство

$$|R(x)| < \alpha_1\left(1 - \frac{\alpha_1^2}{144 K_2}\right) x + o(x).$$

Теперь можно выбрать такое постоянное $K > 144 K_2 > 144$ и такое постоянное $x_3 > x_2 \geqslant x_1(\delta)$, чтобы для всех $x > x_3$ было

$$|R(x)| < \alpha_1\left(1 - \frac{\alpha_1^2}{K}\right) x = \alpha_2 x,$$

причем $\alpha_2 < \alpha_1 \leqslant 1$. Положим теперь $\delta_2 = \alpha_2/6$, тогда существует такое достаточно большое постоянное $x_4 \geqslant x_3$, что для любого $x > x_4$ имеет место разбиение на интервалы (103) и

(104) при $\delta = \delta_2$ и x_4 вместо x_2. Для $x < x_4$ используем оценку $|R(x)| < x$, а для $x \geqslant x_4$ — оценку $|R(x)| < \alpha_2 x$. Как и раньше, теперь можно указать такое $x_5 > x_4$, что для всех $x > x_5$ будет

$$|R(x)| < \alpha_2 \left(1 - \frac{\alpha_2^2}{K}\right) x = \alpha_3 x.$$

Таким образом возможен процесс итерации. Положим

$$\alpha_{n+1} = \alpha_n \left(1 - \frac{\alpha_n^2}{K}\right) < \alpha_n \quad (n = 1, 2, \ldots) \tag{107}$$

и построим для δ_n разбиение на интервалы, тогда получим убывающую последовательность постоянных [1]) чисел $x_{2n+1} > x_{2n}$ таких, что

$$|R(x)| < \alpha_{n+1} x \text{ для } x > x_{2n+1}.$$

Из (107) ясно, что α_n стремится к нулю с ростом n. С помощью полной индукции можно показать, что $\alpha_n < \sqrt{K/2n}$. Подставим это в (107). Учитывая, что кубическая функция от α_n в (107) убывает вместе с α_n, если $\alpha_n < \sqrt{K/3}$, из неравенств $n^{-1/2}(1 - 1/2n) < (n+1)^{-1/2}$ для $n \geqslant 1/3$ и $\alpha_2 < \sqrt{K/4}$ получаем неравенство

$$\alpha_{n+1} < \sqrt{\frac{K}{2(n+1)}}.$$

Теперь можно n выбрать столь большим, что будет $\alpha_n < \varepsilon$. Теперь $\eta = x_{2n-1}$ позволяет получить неравенство, упомянутое в конце § 46, что и доказывает асимптотический закон распределения простых чисел.

VIII. ЭЛЕМЕНТАРНОЕ ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ ОБ АРИФМЕТИЧЕСКОЙ ПРОГРЕССИИ

51. Постановка задачи. Хотя многочисленные частные случаи теоремы 4 могут быть просто доказаны (см. § 7), доказательство в общем случае требует сравнительно больших усилий. Так как метод Эвклида в общем случае не действует, попытаемся найти другое соотношение, из которого можно было бы получить бесконечность простых чисел, для

[1]) x_{2n} должно быть постоянным, для того чтобы в (106) все члены, кроме $\alpha_n x$, поглощались остаточным членом.

которых $p \equiv a \pmod m$. Следуя Х. Н. Шапиро [25], нами будет доказана аналогичная теореме 22

Теорема 38.

$$\sum_{\substack{p \leqslant x \\ p \equiv a \pmod m}} \frac{\log p}{p} = \frac{1}{\varphi(m)} \log x + O(1), \qquad (a,\ m) = 1.$$

Так как правая часть бесконечно возрастает вместе с x, то из теоремы 38 тотчас следует теорема 4.

52. Роль характеров. Главной проблемой при доказательстве теоремы 38 является, очевидно, выделение простых чисел, принадлежащих тому же классу вычетов по mod m, что и a. Если мы хотим, чтобы сумма $\sum f(p)$ была распространена лишь на простые числа p, входящие в этот класс, то нужно все слагаемые $f(p)$ умножить на множитель, который обращается в нуль для $p \not\equiv a \pmod m$, а для $p \equiv a$ имеет значение 1. Этим свойством обладает вследствие (27) сумма характеров

$$\varphi(m)^{-1} \sum_{\chi} \chi(p) \bar{\chi}(a).$$

Тем самым в первую очередь возникает задача оценки суммы вида $\sum_{p \leqslant x} f(p) \chi(p)$. В качестве подготовки к этому рассмотрим сперва соответствующие суммы, распространенные на все $n \leqslant x$.

53. Лемма 1. *Если $f(x)$ для достаточно больших x монотонно стремится к нулю при стремлении x к бесконечности, а χ не является главным характером χ_1 по* mod m, *то*

$$\sum_{n > z} \chi(n) f(n) = O[f(z)].$$

Доказательство. Так как $\chi \neq \chi_1$, то вследствие (24) имеем:

$$|S(x)| = \Big|\sum_{n \leqslant x} \chi(n)\Big| \leqslant O(1). \tag{108}$$

Учитывая (108) и то, что $f(n) \to 0$, получаем из (63)

$$\sum_{n \geqslant z} \chi(n) f(n) = \sum_{n \geqslant z} \{S(n) - S(n-1)\} f(n) =$$

$$= \sum_{k \geqslant z} S(k) \{f(k) - f(k+1)\} - S(z-1) f(z) =$$

$$= O\Big(\sum_{k \geqslant z} \{f(k) - f(k+1)\}\Big) + O[(f(z))] = O[f(z)],$$

ч. т. д. Для $f(x)=1/x$, $f(x)=x^{-1}\log x$, $f(x)=x^{-1/2}$ из леммы 1 следует сходимость рядов

$$L_0(\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n},\quad L_1(\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)\log n}{n},\quad L_2(\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{\sqrt{n}}.$$

Далее, получаем оценки

$$\sum_{n\leqslant x}\frac{\chi(n)}{n}=L_0(\chi)+O\left(\frac{1}{x}\right), \tag{109}$$

$$\sum_{n\leqslant x}\frac{\chi(n)\log n}{n}=L_1(\chi)+O\left(\frac{\log x}{x}\right), \tag{110}$$

$$\sum_{n\leqslant x}\frac{\chi(n)}{\sqrt{n}}=L_2(\chi)+O\left(\frac{1}{\sqrt{x}}\right). \tag{111}$$

54. Лемма 2. *Если* $\chi\neq\chi_1$ — *вещественный характер по* $\bmod m$, *то* $L_0(\chi)\neq 0$.

Доказательство. Сумма $F(n)=\sum\limits_{d|n}\chi(d)$, распространенная на все делители d числа n, как сумматорная функция для $\chi(n)$, является мультипликативной по § 13. Так как $\chi(n)$ вполне мультипликативна, то для $n=\prod p_i^{e_i}$ имеем:

$$F(n)=\prod_i F(p_i^{e_i})=\prod_i\{1+\chi(p_i)+\chi^2(p_i)+\ldots+\chi^{e_i}(p_i)\}.$$

Так как $\chi(p_i)=\pm 1$, то для всех n будет $F(n)\geqslant 0$ и $F(n^2)\geqslant 1$. Отсюда вытекает расходимость ряда $G=\sum F(n)/\sqrt{n}$, так как гармонический ряд является для него минорантой. Покажем теперь, что из равенства $L_0(\chi)=0$ вытекала бы сходимость G.

Положим $n=dd'$ и проведем суммирование по d и d', тогда

$$G(x)=\sum_{n\leqslant x}\frac{F(n)}{\sqrt{n}}=\sum_{n\leqslant x}\frac{1}{\sqrt{n}}\sum_{d\,n}\chi(d)=\sum_{dd'\leqslant x}\frac{\chi(d)}{\sqrt{d}\,\sqrt{d'}}.$$

Двойная сумма распространена на все пары натуральных чисел d, d', для которых $dd'\leqslant x$. Эти пары соответствуют целым точкам, лежащим на гиперболе и под гиперболой $dd'=x$, причем точки, лежащие на оси абсцисс ($d'=0$) и оси ординат ($d=0$), исключаются. Разделим эту область на две части перпендикуляром $d=\sqrt{x}$ и будем суммировать

в левой части вдоль вертикалей, а в правой части — вдоль горизонталей. Это дает следующее разбиение суммы

$$G(x)=\sum_{d\leqslant\sqrt{x}}\frac{\chi(d)}{\sqrt{d}}\sum_{d'\leqslant\frac{x}{d}}\frac{1}{\sqrt{d'}}+\sum_{d'<\sqrt{x}}\frac{1}{\sqrt{d'}}\sum_{\sqrt{x}<d\leqslant\frac{x}{d'}}\frac{\chi(d)}{\sqrt{d}}.$$

Применив (53) для $\rho=-0{,}5$, а также (111), получим;

$$G(x)=\sum_{d\leqslant\sqrt{x}}\frac{\chi(d)}{\sqrt{d}}\left\{2\sqrt{\frac{x}{d}}+C_5+O\left(\sqrt{\frac{d}{x}}\right)\right\}+$$
$$+\sum_{d'<\sqrt{x}}\frac{1}{\sqrt{d'}}\left\{O\left(\sqrt{\frac{d'}{x}}\right)+O\left(\frac{1}{\sqrt[4]{x}}\right)\right\}.$$

Проведение суммирований с учетом (108), (109), (111) и (53) дает

$$G(x)=2x^{\frac{1}{2}}\sum_{d\leqslant\sqrt{x}}\frac{\chi(d)}{d}+O(1)=2x^{\frac{1}{2}}\left\{L_0(\chi)+O(x^{-\frac{1}{2}})\right\}+$$
$$+O(1)=2x^{\frac{1}{2}}L_0(\chi)+O(1).$$

Из равенства $L_0(\chi)=0$ теперь получилось бы $G(x)=O(1)$, что противоречит расходимости G. Лемма 2 доказана.

55. Следующая сумма характеров играет важную роль в нашем доказательстве. Она получится применением (20) к функции

$$g(x)=\sum_{n\leqslant x}\frac{\chi(n)x}{n}=x\sum_{n\leqslant x}\frac{\chi(n)}{n}=xL_0(\chi)+O(1)\quad(\chi\neq\chi_1).$$

При $P(n)=\chi(n)$ и $f(x)=x$ получаем:

$$x=\sum_{n\leqslant x}\mu(n)\chi(n)\left\{\frac{x}{n}L_0(\chi)+O(1)\right\}=$$
$$=xL_0(\chi)\sum_{n\leqslant x}\frac{\mu(n)\chi(n)}{n}+O(x)$$

или после деления на x

$$L_0(\chi)\sum_{n\leqslant x}\frac{\mu(n)\chi(n)}{n}=O(1).\qquad(112)$$

Равенство (112) справедливо для всех характеров $\chi \neq \chi_1$. Для не вещественного χ множитель $L_0(\chi)$ может обращаться в нуль, а тогда (112) ничего не дает. В этом случае еще раз применим (20) при $P(n) = \chi(n)$ и $f(x) = x \log x$ и вследствие (109), (110) и $L_0(\chi) = 0$ получим:

$$\begin{aligned} g(x) &= \sum_{n \leqslant x} \chi(n) \frac{x}{n} \log \frac{x}{n} = x \sum_{n \leqslant x} \frac{\chi(n)}{n} \log \frac{x}{n} = \\ &= x \log x \sum_{n \leqslant x} \frac{\chi(n)}{n} - x \sum_{n \leqslant x} \frac{\chi(n) \log n}{n} = \\ &= L_0(\chi)\, x \log x - x L_1(\chi) + O(\log x) = \\ &= -x L_1(\chi) + O(\log x). \end{aligned}$$

Формула обращения дает теперь

$$\begin{aligned} x \log x &= \sum_{n \leqslant x} \mu(n) \chi(n) \left\{ -L_1(\chi) \frac{x}{n} + O\left(\log \frac{x}{n}\right) \right\} = \\ &= -x L_1(\chi) \sum_{n \leqslant x} \frac{\mu(n) \chi(n)}{n} + O(x), \end{aligned}$$

так как из (54) следует

$$\begin{aligned} \left| \sum_{n \leqslant x} \mu(n) \chi(n)\, O\left(\log \frac{x}{n}\right) \right| &< \\ &< C_{40} \left\{ x \log x - \sum_{n \leqslant x} \log n \right\} = O(x). \end{aligned} \tag{113}$$

Итак, если $L_0(\chi) = 0$, то $L_1(\chi) \neq 0$, так как в противном случае получилась бы невозможная оценка $x \log x = O(x)$. Теперь из равенства (112), учитывая, что $L_0(\chi)$ и $L_1(\chi)$ — конечные числа, для $\chi \neq \chi_1$ имеем:

$$L_1(\chi) \sum_{n \leqslant x} \frac{\mu(n) \chi(n)}{n} = \begin{cases} -\log x + O(1), & \text{если } L_0(\chi) = 0, \\ O(1), & \text{если } L_0(\chi) \neq 0. \end{cases} \tag{114}$$

56. Лемма 3. *Для $\chi \neq \chi_1$ справедливо равенство*

$$\sum_{p \leqslant x} \frac{\chi(p) \log p}{p} = \begin{cases} O(1), & \text{если } L_0(\chi) \neq 0, \\ -\log x + O(1), & \text{если } L_0(\chi) = 0. \end{cases} \tag{115}$$

Доказательство. Из (53) для $s \geqslant 1$ имеем:

$$\sum_{p \leqslant x} \frac{\chi(p) \log p}{p} = \sum_{p^s \leqslant x} \frac{\chi(p^s) \log p}{p^s} - O(1) = \sum_{n \leqslant x} \frac{\chi(n) \Lambda(n)}{n} - O(1).$$

Из (22) теперь следует, если положить $n = dd'$ и использовать (110) и (113),

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

$$= \sum_{dd' \leqslant x} \frac{\chi(dd') \mu(d) \log d'}{dd'} = \sum_{d \leqslant x} \frac{\mu(d) \chi(d)}{d} \sum_{d' \leqslant x/d} \frac{\chi(d') \log d'}{d'} =$$

$$= \sum_{d \leqslant x} \frac{\mu(d) \chi(d)}{d} \left\{ L_1(\chi) + O\left(\frac{\log (x/d)}{x/d} \right) \right\} =$$

$$= L_1(\chi) \sum_{d \leqslant x} \frac{\mu(d) \chi(d)}{d} + O(1).$$

Теперь отсюда и из (114) непосредственно вытекает утверждение леммы.

57. Отличие $L_0(\chi)$ от нуля. Покажем теперь, что $L_0(\chi) \neq 0$ для *любого* характера $\chi = \chi_1$, т. е. не только для вещественных χ. Это центральное место в классическом доказательстве теоремы Дирихле. Если N означает количество $\chi \neq \chi_1$, для которых $L_0(\chi) = 0$, то из (25), (26), теоремы 22 и (115) следует

$$Q(x) = \varphi(m) \sum_{\substack{p \leqslant x \\ p \equiv 1 \pmod m}} \frac{\log p}{p} = \sum_{\gamma} \sum_{p \leqslant x} \frac{\chi(p) \log p}{p} =$$

$$= \sum_{\substack{p \leqslant x \\ (p, m) = 1}} \frac{\log p}{p} + \sum_{\chi \neq \chi_1} \sum_{p \leqslant x} \frac{\chi(p) \log p}{p} = (1 - N) \log x + O(1).$$

Так как $Q(x) \geqslant 0$, то $0 \leqslant N \leqslant 1$. Отсюда следует, что $L_0(\chi) \neq 0$ также и для комплексных χ. Действительно, если бы $L_0(\chi)$ обращалось в нуль для комплексного χ, то это было бы и для комплексно-сопряженного характера $\bar{\chi}$ [1]), а тогда было бы $N \geqslant 2$.

---

[1]) Два комплексно-сопряженных числа $a + bi$ и $a - bi$ или оба нули, или оба отличны от нуля.

58. Окончание доказательства. Для всех $\chi = \chi_1$ имеем теперь по (115) $\sum \chi(p) p^{-1} \log p = O(1)$. Из (27), теоремы 22 и конечности числа характеров следует, таким образом, для $(a, m) = 1$ равенство

$$\varphi(m) \sum_{\substack{p \leqslant x \\ p \equiv a \pmod m}} \frac{\log p}{p} = \sum_{\chi} \overline{\chi}(a) \sum_{p \leqslant x} \frac{\chi(p) \log p}{p} =$$

$$= \sum_{\substack{p \leqslant x \\ (p, m) = 1}} \frac{\log p}{p} + \sum_{\chi \neq \chi_1} \overline{\chi}(a) \sum_{p \leqslant x} \frac{\chi(p) \log p}{p} = \log x + O(1),$$

чем и доказана теорема 38.

59. Дальнейшие результаты. Правая часть оценки в теореме 38 для всех классов вычетов a по mod m, взаимно простых с m, содержит один и тот же главный член, поэтому естественно предположить, что все такие классы вычетов содержат асимптотически равное количество простых чисел. Если $\pi_a(x)$ обозначает количество $p = a + km \leqslant x$, $(a, m) = 1$, то действительно

$$\lim_{x \to \infty} \frac{\pi_a(x)}{\pi(x)} = \frac{1}{\varphi(m)}.$$

Это тотчас следует из «асимптотического закона» для арифметической прогрессии

$$\pi_a(x) \sim x [\varphi(m) \log x]^{-1},$$

который сегодня также может быть доказан «элементарно».

Особенно интересен вопрос о наименьшем простом числе, входящем в класс вычетов, взаимно простой с m. Линник получил в этом направлении следующий важный результат: существует такая абсолютная постоянная C_{50}, что для любого натурального m в каждом классе вычетов по mod m, взаимно простом с m, имеется простое число $p < m^{C_{50}}$.

IX. МЕТОД РЕШЕТА

60. Метод решета Бруна служит для «просеивания» чисел $n \leqslant x$ арифметической прогрессии F с начальным членом $a > 0$ и разностью $d > 0$. «Решето» строится следующим образом: из последовательности простых чисел вычеркиваем конечное число членов, в том числе 2 и простые делители d.

Расположенные в порядке роста оставшиеся простые числа обозначим $q_1, q_2, q_3, \ldots$ Пусть $\pi'(y)$ означает количество чисел $q_i \leqslant y$. Каждому $q_i \leqslant y$ сопоставим две[1]) арифметические прогрессии A_i и B_i с начальными членами a_i и b_i и разностью q^i, где $0 \leqslant a_i \leqslant q_i$, $0 \leqslant b_i \leqslant q_i$, $a_i \neq b_i$. $2\pi'(y)$ последовательностей A_i и B_i используем теперь для просеивания, удалив из F те n, которые лежат в одной из последовательностей A_i или B_i. Оставшиеся $n \leqslant x$ удовлетворяют, таким образом, условиям: $n \equiv a \pmod d$, $n \not\equiv a_i \pmod{q_i}$, $n \not\equiv b_i \pmod{q_i}$, $a_i \not\equiv b_i$. Количество таких n обозначим символом $N(d, x, y)$. Мы будем устанавливать лишь такие свойства $N(d, x, y)$, которые не зависят от выбора чисел a, a_i, b_i, так что эти аргументы не нужно вводить в обозначение функции. Цель метода решета — получить как можно лучшие оценки для $N(d, x, y)$.

Иллюстрацией служит следующий пример: $a = 1$, $d = 2$, $q_1 = 3$, $q_2 = 5$, $q_i = p_{i+1}$; $a_i = 0$ для всех i; $b_i \equiv x \pmod{q_i}$ для $x \not\equiv 0 \pmod{q_i}$, но $b_i \not\equiv x \pmod{q_i}$, если $x \equiv 0 \pmod{q_i}$. Если x — четное и $u \geqslant 2$ — целое, то $N(2, x, x^{1/u})$ — количество нечетных $n \leqslant x$, обладающих тем свойством, что ни n, ни $x - n$ не делятся на простые числа $\leqslant x^{1/u}$.

Действительно, из $x - n \equiv 0 \pmod{q_i}$ вытекает, что $n \equiv b_i \pmod{q_i}$, если $x \not\equiv 0 \pmod{q_i}$, и $n \equiv 0 \pmod{q_i}$, если $x \equiv 0 \pmod{q_i}$.

Таким образом, все простые делители n и $x - n$ будут $> x^{1/u}$, т. е. как n, так и $x - n$ состоят не более чем из $u - 1$ простых множителей. Из неравенства $N(2, x, x^{1/2}) \geqslant 2$ вытекало бы существование представления $x = n + (x - n)$, в котором n и $x - n$ — простые числа, как предположил в 1742 г. Гольдбах (см. гл. X).

61. Алгебраическая рекуррентная формула. Разность $N(d, x, q_{k-1}) - N(d, x, q_k)$ равна, очевидно, количеству тех m, которые удовлетворяют следующим условиям:

$$m \leqslant x,\ m \equiv a \pmod d,\ m \equiv a_k \text{ или } \equiv b_k \pmod{q_k},$$

$$(m - a_i)(m - b_i) \not\equiv 0 \pmod{q_i} \quad (i = 1, 2, \ldots, k - 1). \tag{116}$$

Так как $(d, q_k) = 1$, то существуют целые u, v, для кото-

[1]) При решении некоторых задач достаточно сопоставлять q_i одну последовательность A_i; можно, однако, строить также трехили многократное решето. Здесь рассматривается лишь двойное решето.

рых $ud + vq_k = 1$, а также целые u', v', u'', v'', для которых $a - a_k = u'd + v'q_k$, $a - b_k = u''d + v''q_k$. Положим теперь $a - u'd = a_k + v'q_k = a'$, $a - u''d = b_k + v''q_k = a''$, тогда совокупность m, удовлетворяющих (116), совпадает с совокупностью m, для которых

$$m \leqslant x,\ m \equiv a' \text{ или } \equiv a'' \pmod{dq_k},$$
$$(m - a_i)(m - b_i) \not\equiv 0 \pmod{q_i} \quad (i = 1, 2, \ldots, k-1). \tag{117}$$

Действительно, из сравнения $m \equiv a_k \pmod{q_k}$ следует: $m - a' = m - a + u'd \equiv 0 \pmod{d}$, $m - a' = m - a_k - v'q_k \equiv 0 \pmod{q_k}$, так что $m \equiv a' \pmod{dq_k}$. Обратное утверждение получается так же.

Количество чисел m, удовлетворяющих (117), можно обозначить $2N(dq_k, x, q_{k-1})$. Естественно, что слагаемые, соответствующие a' и a'', не равны точно, однако они будут одинаково оцениваться, так что мы можем символически объединить эти члены. Таким образом, получаем рекуррентную формулу

$$N(d, x, q_k) = N(d, x, q_{k-1}) - 2N(dq_k, x, q_{k-1}). \tag{118}$$

Для $k = 1$ пишем справа $N(d, x) - 2N(dq_k, x)$, где $N(d, x)$ означает количество чисел $n \leqslant x$ любой арифметической прогрессии с разностью d. При любом начальном члене имеем:

$$N(d, x) = \frac{x}{d} + \vartheta, \quad |\vartheta| \leqslant 1. \tag{119}$$

С помощью (118) можно, очевидно, выразить $N(d, x, q_k)$ исключительно через слагаемые вида (119) и получить, таким образом, оценку, справедливую при всех a, a_i, b_i.

В первую очередь из (118) выводим равенство

$$N(d, x, q_k) = N(d, x) - 2\sum_{1 \leqslant r_1 \leqslant k} N(dq_{r_1}, x, q_{r_1-1}). \tag{120}$$

Если каждое слагаемое правой части снова выразить по формуле (120), то получим:

$$N(d, x, q_k) = N(d, x) - 2\sum_{r_1 \leqslant k} N(dq_{r_1}, x) + \\ + 4\sum_{r_1 \leqslant k}\sum_{r_2 < r_1} N(dq_{r_1}q_{r_2}, x, q_{r_2-1}). \tag{121}$$

Вообще для $t \leqslant k$ имеем:

$$N(d, x, q_k) = N(d, x) - 2\sum_{r_1 \leqslant k} N(dq_{r_1}, x) + \\ + 4\sum_{r_1 \leqslant k}\sum_{r_2 \leqslant r_1} N(dq_{r_1}q_{r_2}, x) - 8\sum_{r_1 \leqslant k}\sum_{r_2 < r_1}\sum_{r_3 < r_2} N(dq_{r_1}q_{r_2}q_{r_3}, x) + \dots \\ \dots + (-2)^t \sum_{r_1 \leqslant k} \dots \sum_{r_t < r_{t-1}} N(dq_{r_1} \dots q_{r_t}, x, q_{r_t - 1}). \quad (122)$$

Для $t = k$ с помощью (119) легко получаем из (122)

$$N(d, x, q_k) = \frac{x}{d}\prod_{r=1}^{k}(1 - 2q_r^{-1}) + R. \quad (123)$$

Развернув произведение, получим 3^k членов, каждый из которых вносит в остаточный член R величину, не превосходящую по модулю 1. Таким образом, $|R| \leqslant 3^k$.

Для оценки $N(d, x, x^{1/u})$ равенство (123) не пригодно. Действительно, из теоремы 3 $k = \pi(x^{1/u}) \sim ux^{1/u}/\log x$, а по теореме 25

$$\prod(1 - 2q_r^{-1}) \sim \frac{C_{18}u^2}{\log^2 x},$$

так что R имеет больший порядок роста, чем главный член. Вигго Брун [3] показал, как можно так сократить число членов в (123), чтобы R оказалось меньшего порядка, чем главный член.

62. Введение чисел решета k_j. Теперь должна быть выведена оценка сверху[1]) для $N(d, x, q_k)$. Положим в (122) $t = 3$ и потребуем, чтобы, кроме условия $r_3 < r_2$, выполнялось еще неравенство $r_3 \leqslant k_1$. Если в тройной сумме опустить некоторые члены, то правая часть увеличится. Если в получившемся, таким образом, неравенстве члены тройной суммы выразить с помощью (121), то получится в результате пятикратная сумма, из которой можно снова исключить несколько членов с помощью условия $r_5 \leqslant k_2$. Таким образом, мы получим разложение, аналогичное разложению (122), которое оканчивается отрицательной $(2s+1)$-кратной суммой, где должно быть $2s + 1 < k$. Применим к этой сумме еще раз (118),

[1]) Для вывода оценки снизу требуются лишь незначительные изменения.

тогда в конце правой части неравенства окажется положительная $(2s+2)$-кратная сумма. Ее можно еще увеличить, если символы $N(dq_{r_1}\dots q_{r_{2s+2}}, x, q_{r_{2s+2-1}})$ заменить символами $N(dq_{r_1}\dots q_{r_{s+2}}, x)$. Из (119) теперь получаем:

$$N(d, x, q_k) < \frac{x}{d} E + R,$$

где

$$E = 1 - \sum (2q_{r_1}^{-1}) + \sum\sum (2q_{r_1}^{-1})(2q_{r_2}^{-1}) - \dots$$
$$\dots + (-1)^{2s+2} \sum \dots \sum (2q_{r_1}^{-1}) \dots (2q_{r_{2s+2}}^{-1}). \quad (124)$$

Для индексов суммирования имеем:

$$r_{2j+2} \leqslant k, \quad r_{2j+1} < k_j \quad (j = 0, 1, 2, \dots, s),$$
$$k = k_0 \geqslant k_1 \geqslant \dots \geqslant k_s \geqslant 1; \; 1 < r_{2s+2} < r_{2s+1} < \dots < r_2 < r_1. \quad (125)$$

Все члены содержатся в разложении произведения

$$(1 - 2\sum\nolimits_{q_{r_1}}^{-1}) \dots (1 - 2\sum\nolimits_{q_{r_{2s+2}}}^{-1}).$$

Таким образом, $|R|$ не превосходит числа членов $(q_{r_\alpha} q_{r_\beta} \dots)^{-1}$ этого разложения, следовательно,

$$|R| \leqslant (2k_0 + 1)^2 (2k_1 + 1)^2 \dots (2k_s + 1)^2. \quad (126)$$

63. Структура главного члена E. Положительную i-кратную сумму в (124) обозначим символом $E^{(i)}$ и положим $E^{(0)} = 1$. Далее, пусть E_m обозначает сумму всех таких слагаемых $(2q_{r_1}^{-1}) \dots (2q_{r_\nu}^{-1})$ в (124), у которых все $r_\mu > k_m$. Вследствие (125) это возможно лишь для $\mu \leqslant 2m$, так что в $E^{(i)}$ при $i > 2m$ такие слагаемые не входят. Если $E_m^{(i)}$ представляет собой пересечение E_m и $E^{(i)}$, то $E_m^{(i)} = 0$ для $i > 2m$, так что имеем:

$$E_m = \sum_{i=0}^{2m} (-1)^i E_m^{(i)}, \quad E_m^{(0)} = 1.$$

Положим еще $k_{s+1} = 0$ (на конструкцию E это не окажет влияния), тогда $E = E_{s+1}$.

Простые числа $q_1, q_2, \dots q_{k_m}$ по определению не входят в E_m. При переходе от E_m к E_{m+1} добавляются еще $N = k_m - k_{m+1}$ простых чисел q_z с $k_{m+1} < z \leqslant k_m$. Символом $S_{m+1}^{(\mu)}$ обозначим

μ-ю элементарную симметрическую функцию[1]) N чисел $2q_z^{-1}$, тогда легко получим соотношения

$$E_{m+1}^{(i)} = \sum_{v=0}^{i} S_{m+1}^{(i-v)} E_m^{(v)}; \quad E_{m+1} = \sum_{i=0}^{2m+2} \sum_{v=0}^{i} (-1)^i S_{m+1}^{(i-v)} E_m^{(v)}, \quad (127)$$

где $S_{m+1}^{(\mu)} = 0$ для $\mu > N$. С другой стороны, получаем:

$$E_m \prod_z (1 - 2q_z^{-1}) = \sum_{\alpha=0}^{2m} \sum_{\beta=0}^{N} (-1)^{\alpha+\beta} E_m^{(\alpha)} S_{m+1}^{(\beta)} =$$

$$= \sum_{i=0}^{N+2m} \sum_{v=0}^{i} (-1)^i E_m^{(v)} S_{m+1}^{(i-v)}.$$

Положив $\tau = i - 2m$ и приняв во внимание, что $E_m^{(v)} = 0$ для $v > 2m$, из (127) получим:

$$E_{m+1} = E_m \prod_z (1 - 2q_z^{-1}) - \sum_{\tau=3}^{N} (-1)^\tau \sum_{v=0}^{2m} E_m^{(v)} S_{m+1}^{(2m+\tau-v)}. \quad (128)$$

Двойная сумма впервые встречается при $N \geqslant 3$. Для $N = 1$ или 2

$$E_{m+1} \leqslant E_m \prod_z (1 - 2q_z^{-1}).$$

Числа k_j мы определим так, чтобы за исключением конечного числа исключений было

$$S_{m+1}^{(1)} = \sum 2q_z^{-1} < 1.$$

Из оценки[2])

$$S_{m+1}^{(i)} \leqslant \frac{(S_{m+1}^{(1)})^i}{i!}$$

вытекает, что внутренние суммы в двойной сумме равенства

---

[1]) Элементарные симметрические функции $s_n^{(0)}, s_n^{(1)}, \ldots, s_n^{(n)}$ переменных $x_1, x_2, \ldots, x_n$ определяются разложением $(x - x_1)(x - x_2) \ldots (x - x_n) = s_n^{(0)} x^n - s_n^{(1)} x^{n-1} + \ldots + (-1)^n s_n^{(n)}$.

[2]) Имеем $g S_{m+1}^{(g)} \leqslant S_{m+1}^{(1)} S_{m+1}^{(g-1)}$, так как каждое слагаемое из S_{m+1}^{g} можно g способами записать в виде произведения некоторого слагаемого из $S_{m+1}^{(1)}$ и некоторого слагаемого из $S_{m+1}^{(g-1)}$ и все такие произведения встречаются в правой части. Оценка получается после перемножения таких неравенств для $g = 2, 3, \ldots, i$.

(128) монотонно убывают с ростом τ. Так как эти суммы имеют чередующиеся знаки, то двойная сумма больше, чем первый (отрицательный) член. Таким образом, имеем:

$$E_{m+1} < E_m \prod_z (1 + 2q_z^{-1}) + \sum_{v=0}^{2m} E_m^{(v)} S_{m+1}^{(2m+3-v)}. \quad (129)$$

64. Определение чисел k. Пусть ρ, ρ_0 — постоянные и

$$\rho_0 > \rho > 1, \quad 0 < 2 \log \rho_0 < 1.$$

Положим

$$k_m = \pi' (q_k^{\frac{1}{\rho^m}}).$$

Так как для простых чисел q_j также справедливы (правда, с другими постоянными) теоремы 23 и 25, то для N простых чисел q_z, $k_{m+1} < z \leqslant k_m$

$$q_k^{\frac{1}{\rho^{m+1}}} < q_z \leqslant q_k^{\frac{1}{\rho^m}}, \quad \frac{1}{2} S_{m+1}^{(1)} = \sum_z q_z^{-1} = \log \rho + o(1),$$

$$P_{m+1} = \prod_z (1 - 2q_z^{-1}) = \frac{1 + o(1)}{\rho^2}. \quad (130)$$

Существует такое ω, зависящее лишь от ρ и ρ_0, и такое целое M, что для $q_{k_m} > q_{k_{m+1}} > \omega$ соответственно $m < M$, o-члены в (130) так малы, что

$$S_{m+1}^{(1)} < 2 \log \rho_0 < 1, \quad P_{m+1} > \rho_0^{-2}. \quad (131)$$

Теперь мы должны выбрать интервалы $k_{c+1} < i \leqslant k_c$, где $c > M + 1$ для индексов i конечного числа простых чисел $q_i \leqslant \omega$. Для того чтобы сумму в (129) можно было опустить, достаточно положить $k_c - k_{c+1} = 2$ или 1.

65. Оценка E. Сумма в (129) состоит из различных произведений по $2m + 3$ множителей $2q_\mu^{-1}$, где $\mu > k_{m+1}$, поэтому она меньше, чем $(2m + 3)$-я симметрическая функция $T^{(2m+3)}$ величин $2q_\mu^{-1}$, содержащая все произведения такого рода. Пока выполняется (131), имеем:

$$T^{(1)} = \sum 2q_\mu^{-1} = S_{m+1}^{(1)} + S_m^{(1)} + \ldots + S_1^{(1)} < 2(m+1) \log \rho_0.$$

Из общей оценки [1]) следует при $\tau = e \log \rho_0$

$$T^{(2m+3)} < \left(\frac{eT^{(1)}}{2m+3}\right)^{2m+3} < \tau^{2m+3}.$$

Если в (129) сумма еще имеется, из (131) получаем:

$$E_{m+1} < E_m \prod_z (1 - 2q_z^{-1}) + \tau^{2m+3} < P_{m+1}(E_m + \tau^{2m+3}\rho_0^2)$$

и отсюда путем итерации, учитывая, что $E_0 = 1$,

$$E_{m+1} < P_{m+1} P_m \ldots P_1 \{1 + \tau^3\rho_0^2 + \ldots + \tau^{2m+3}\rho_0^{2m+2}\}. \quad (132)$$

Если $\tau\rho_0 = e\rho_0 \log \rho_0 < 1$, то геометрическую прогрессию в (132) можно заменить бесконечной прогрессией, что сделает скобку не зависящей от m. Принимая во внимание соотношение $E_{c+1} \leqslant E_c P_{c+1}$ для $c \geqslant M+1$, получаем, наконец,

$$E = E_{s+1} < \delta \prod_{\nu=1}^{k} (1 - 2q_\nu^{-1}), \quad \delta = 1 + \frac{\tau^3\rho_0^2}{1 - \tau^2\rho_0^2}, \quad q_1 \geqslant 3. \quad (133)$$

66. Оценка остаточного члена R. Вследствие условия $q_1 \geqslant 3$ всегда выполняется неравенство $2m+1 \leqslant q_m$. Поэтому из (126) следует

$$|R| \leqslant q_{k_0}^2 q_{k_1}^2 \ldots q_{k_M}^2 q_{k_{M+1}}^2 \ldots q_{k_s}^2 \leqslant q_k^Q q_{k_{M+1}}^2 \ldots q_{k_s}^2 = q_k^Q A.$$

По § 64 величина A постоянная, зависящая лишь от ρ и ρ_0, а для Q вследствие $q_{k_m} \leqslant q_k^{1/\rho^m}$ находим:

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

Отсюда получается оценка

$$|R| < A q_k^{\frac{2\rho}{\rho-1}}. \quad (134)$$

67. Результат применения метода решета. Если $k = \pi'(x^{1/u})$, то из (133), (134) и теоремы 25 следует при условии $2\rho/(\rho-1) = fu$

$$N(d, x, x^{\frac{1}{u}}) < C_{58} \frac{\delta u^2}{d} \frac{x}{\log^2 x} + C_{59} x^f =$$

$$= C_{58} \frac{\delta u^2}{d} \frac{x}{\log^2 x} \left\{1 + \frac{C_{59} d}{C_{58} \delta u^2} \frac{\log^2 x}{x^{1-f}}\right\}. \quad (135)$$

[1]) Применяется оценка, которая была доказана в примечании на стр. 99, и получающееся из (54) неравенство $l! > l^l e^{-l}$ $(e = 2{,}718\ldots)$.

Вследствие (51) скобка при $f<1$ имеет порядок $1+o(1)$. Это имеет место при $\rho=5/4$ и $u=11$. Если положить $\rho_0=1{,}2501$, то предположения § 64 и § 65 выполняются, так как $\tau\rho_0=0{,}758$. Для этих чисел $\delta=1{,}82$. Скобка в (135), очевидно, и при $u>11$ асимптотически равна 1. Если, наоборот, u при фиксированном x убывает, то решето может лишь расшириться, так как в нем, возможно, будет участвовать большее число простых чисел q_i. Таким образом, $N(d, x, x^{1/u})$ при уменьшении u во всяком случае не увеличится, так что для $u\geqslant 2$ и $x\geqslant x_0$ имеем:

$$N(d, x, x^{1/u})\leqslant \frac{C_{60}x}{\log^2 x}. \tag{136}$$

C_{60}, естественно, зависит от u. Оценка (136) дает истинный порядок роста величины $N(d, x, x^{1/u})$, так как можно методом Бруна доказать также неравенство

$$N(d, x, x^{1/u})\geqslant C_{61}\,x/\log^2 x, \text{ где } C_{61}>0 \text{ для } u\geqslant 10.$$

До сих пор мы предполагали, что $a_i\not\equiv b_i$ для всех i. Если для некоторых «исключительных простых чисел» q_σ будет $a_\sigma\equiv b_\sigma$, то $N(d, x, x^{1/u})$ увеличится. Для того чтобы обобщить (136) на этот случай, сопоставим каждому q_i число v_i таким образом, чтобы было $v_i=2$, если q_i — нормальное простое число, и $v_i=1$, если q_i — исключительное простое число. В предшествующем выводе мы можем вообще заменить $2q_i^{-1}$ на $v_iq_i^{-1}$. Для произведения в (133) с помощью теоремы 24 получаем:

$$\begin{aligned}\prod(1-v_\nu q_\nu^{-1})&\leqslant\prod(1-q_\nu^{-1})^{v_\nu}=\\&=\prod(1-q_\nu^{-1})^2\prod_\sigma(1-q_\sigma^{-1})^{-1}=\\&=O\{(\log x)^{-2}\prod_\sigma(1+q_\sigma^{-1})(1-q_\sigma^{-2})^{-1}\}=\\&=O\{(\log x)^{-2}\prod_\sigma(1+q_\sigma^{-1}),\end{aligned}$$

потому что $\prod_\sigma(1-q_\sigma^{-2})^{-1}$ сходится, как часть ряда $\sum n^{-2}$. Так как остаточный член не увеличится, то имеем общую оценку

$$N(d, x, x^{\frac{1}{u}})=O\{x(\log x)^{-2}\prod_\sigma(1+q_\sigma^{-1})\}. \tag{137}$$

68. Простые близнецы. Из последовательности нечетных чисел n ($a=1$, $d=2$) требуется выделить простые близнецы. Числа $n-2$ и $n\leqslant x$ оба являются простыми $>\sqrt{x}$, если они не делятся ни на одно $p_i\leqslant\sqrt{x}$, т. е. когда $n\not\equiv 0 \pmod{p_i}$, $n-2\not\equiv 0 \pmod{p_i}$. Если символом $Z(x)$ обозначить количество пар близнецов $\leqslant x$, то для $a_i=0$, $b_i=2$, $q_i=p_{i+1}$, $x>x_0$ получим из (136)

$$Z(x)=N(2, x, x^{1/2})+Z(\sqrt{x}+2)<\frac{C_{70}x}{\log^2 x}+$$

$$+\sqrt{x}+2<\frac{C_{71}x}{\log^2 x}.$$

Если t_m большее простое число из m-й пары близнецов, то получаем таким образом

$$m<\frac{C_{71}t_m}{\log^2 t_m} \text{ или } \frac{1}{t_m}<\frac{C_{71}}{m\log^2 t_m}<\frac{C_{71}}{m\log^2 m}.$$

Так как по (57) ряд $\sum\frac{1}{m\log^2 m}$ сходится, то имеет место доказанная Бруном в 1919 г.

Теорема 39. *Ряд из величин, обратных простым близнецам, обрывается или сходится.*

Аналогичный результат можно получить также и для таких пар последовательных простых чисел, разность которых равна любому фиксированному четному числу.

69. Количество представлений натурального числа в виде суммы или разности простых чисел. Символом $L(x, y)$ при заданном четном y обозначим количество решений уравнения $y=p-p'$ при $p\leqslant x$, $p'\leqslant x$[1]).

Очевидно, $L(x^{1/2}, y)\leqslant\sqrt{x}$, так как для $p\leqslant\sqrt{x}$ существует не более чем $\sqrt{x}$ решений. Если $p>\sqrt{x}$ и $p'>\sqrt{x}$, то первые $\pi(\sqrt{x})$ простых чисел p_i $[i=1, 2, \ldots, \pi(\sqrt{x})]$ отличны от p и p'. Если для некоторого $n\leqslant x$ будет $n\not\equiv 0 \pmod{p_i}$ и $n-y\not\equiv 0 \pmod{p_i}$, то n и $n-y$ — это нечетные простые числа — решения p, p'. Такие n можно найти просеиванием при $a=1$, $d=2$, $a_i=0$, $b_i=y$. Исключительными простыми числами в смысле § 67 являются простые делители y, так как

[1]) Если y нечетное, то должно быть $p'=2$ и $y+2$ — простое число.

для них $a_i = b_i$. Так как $\sqrt{x} = o(x/\log^2 x)$, то из (37) получаем:

$$L(x, y) \leqslant N(2, x, x^{1/2}) + 2\sqrt{x} + \\ + C_{72} x (\log x)^{-2} \prod_{p|y} (1 + p^{-1}). \qquad (138)$$

Рассмотрим теперь число решений $L(x)$ уравнения $x = p + p'$. Можно считать x четным и $\neq 4$, тогда p и p' — нечетные. Теперь $p < x$. Для $p \leqslant \sqrt{x}$ или $p' \leqslant \sqrt{x}$ снова существует не более чем $2\sqrt{x}$ решений. Решения с $p > \sqrt{x}$, $p' > \sqrt{x}$, как и прежде, находим просеиванием при $a = 1$, $d = 2$, $a_i = 0$, $b_i = x$, причем исключительными простыми числами являются простые делители x. Таким образом, имеем:

$$L(x) < C_{73} x (\log x)^{-2} \prod_{p|x} (1 + p^{-1}). \qquad (139)$$

70. Одна теорема Эрдёша особенно ясно подчеркивает упомянутую еще в § 5 нерегулярность в распределении простых чисел. По Эрдёшу [7] существует, например, 10^6 последовательных p, для которых разность между соседними простыми числами $> 10^{12}$. Точнее, справедлива

Теорема 40. *Пусть D — фиксированная постоянная и n сколь угодно большое, тогда существует постоянная c, зависящая лишь от D, и $r = [c \log n]$ последовательных простых чисел*

$$p_{k+1} < p_{k+2} < \ldots < p_{k+r} < n,$$

таких, что

$$p_{k+i} - p_{k+i-1} > D \qquad (i = 1, 2, \ldots, r).$$

Доказательство. Количество $f(n)$ решений неравенств $p_{m+1} - p_m \leqslant D$, $p_{m+1} \leqslant n$ меньше, чем общее число решений D уравнений $p - p' = y$, $p \leqslant n$, $1 \leqslant y \leqslant D$. Вследствие (138) получаем $f(n) < C_{74} n (\log n)^{-2}$, где C_{74} зависит от D. Числа $p_{m+1} \leqslant n$ распределим теперь на два класса, причем p_{m+1} принадлежит к первому классу, если $p_{m+1} - p_m \leqslant D$, и ко второму классу, если $p_{m+1} - p_m > D$ [1]). Каждой последовательности последовательных простых чисел p_{a+1}, p_{a+2}, $\ldots$, p_{a+r} второго класса соответствует простое число p_a

[1]) По § 5 второй класс для достаточно больших n не пустой.

первого класса. Если $r \geqslant 1$ — максимальная длина такой последовательности второго класса, то, очевидно, имеем $\pi(n) < 2rf(n)$. Из вышеупомянутой оценки для $f(n)$ и теоремы 28 следует

$$r > \frac{\pi(n)}{2f(n)} > C_{75} \log n,$$

где $C_{75} = C_{21}/2C_{74}$ зависит от D, что и требовалось доказать.

71. Замечания. В качестве простых чисел решета можно взять также p из некоторого подмножества $\mathfrak{M}'$ множества $\mathfrak{M}$ всех простых чисел, если для $p \leqslant x$ из $\mathfrak{M}'$ имеет место формула

$$\sum{}' p^{-1} \log p = \rho \log x + O(1), \quad 0 < \rho \leqslant 1\ ^{1}),$$

аналогичная теореме 22 (Риччи, Р. Д. Джемс). В этом случае величина $O(x/\log^{2\rho} x)$ дает истинный порядок роста $N(d, x, x^{1/u})$. Бухштаб улучшил постоянные C_{61} и C_{60} (ср. (136)) для малых значений u; в частности, $C_{61} > 0$ для $u \geqslant 5$. Недавно А. Сельберг [23], [24] развил интересный метод решета, который приводит к поразительно хорошим результатам. Мы приведем результат просеивания для простейшего случая. Пусть дана любая последовательность из N натуральных чисел n. Предположим, что количество n, делящихся на постоянное число k, может быть записано в форме $N/f(k) + R_k$, где $f(k)$ — мультипликативная функция, для которой $f(1) = 1$, а для «остаточного члена» имеем $|R_k| \leqslant k/f(k)$. Тогда для количества N_z тех n, которые не делятся ни на какие простые числа $p \leqslant z$, получается оценка (ср. Чулановский [47])

$$N_z \leqslant N \left\{ \sum_{t \leqslant z} \mu^2(t) \prod_{p \mid t} \frac{1}{f(p) - 1} \right\}^{-1} + z^2 \prod_{p \leqslant z} \left(1 - \frac{1}{f(p)}\right)^{-2}.$$

Если $n = P(x)$, $1 \leqslant x \leqslant N$, где $P(x)$ целозначный полином без постоянного простого делителя, а $u(d)$ — количество несравнимых по $\bmod d$ решений сравнения $P(x) \equiv 0 \pmod d$, то существует $Nd^{-1}u(d) + R_d$ делящихся на d чисел n, где $|R_d| \leqslant u(d)$. Таким образом, здесь $f(d) = d/u(d)$. Функция $f(d)$ мультипликативна, так как такой является $u(d)$.

---

[1]) Для p из арифметической прогрессии с разностью m по теореме 33 $\rho = 1/\varphi(m)$.

Для $P(x)=x(2+x)$ и $z=(N+2)^{1/2-\varepsilon}$ снова находим оценку для количества простых близнецов, полученную в § 68. Здесь $C_{71}=10{,}6$, тогда как у Бруна $C_{71}=100$. Правда, использование формулы Сельберга является несколько трудным.

Интересные применения нашло также так называемое «большое решето» русского математика Линника. Простыми числами решета служат y любых простых чисел $p_i<\sqrt{N}$ $(i=1, 2, \ldots, y)$. Каждому p_i сопоставляют $f(p_i)$ определенных классов вычетов по $\bmod p_i$, где $f(p_i)<p_i$, и из ряда первых N натуральных чисел $n\leqslant N$ вычеркивают каждое n, которое хотя бы для одного p_i входит в один из $f(p_i)$ зафиксированных классов вычетов по $\bmod p_i$. Если τ — наименьшее из чисел $f(p_i)/p_i$, то после просеивания останется не более чем $20\pi\tau^{-2}y^{-1}N$. Это утверждение можно высказать также и в следующей эквивалентной форме: если каждому простому числу $p<\sqrt{N}$ сопоставить целое число $f(p)<p$, то z любых натуральных чисел $n_1<n_2<\ldots<n_z\leqslant N$ почти для всех $p<\sqrt{N}$ принадлежат по крайней мере $p-f(p)$ различным классам вычетов по $\bmod p$. Количество исключительных простых чисел, которым соответствует меньшее число классов вычетов, не превышает величины $20\pi\tau^{-2}z^{-1}N$, где τ — наименьшее из чисел $f(p)/p$ для $p\leqslant\sqrt{N}$. Реньи заметил, что это вытекает из одной общей теоремы теории вероятностей, которая позволяет еще точнее описать распределение чисел n по классам вычетов по $\bmod p$. Основываясь на своем обобщении большого решета, Реньи удалось показать, что любое достаточно большое четное число является суммой простого и почти простого ($n=\prod p^{e_p}$ называется почти простым, если $\sum e_p\leqslant K$, где K — абсолютная постоянная). Реньи удалось далее показать, что существует бесконечно много простых p, для которых $p+2$ является почти простым.

X. ГИПОТЕЗА ГОЛЬДБАХА

72. Ранее полученные результаты. В 1742 г. в письме к Эйлеру Гольдбах высказал следующие гипотезы:

А) Каждое четное число >2 представимо в виде суммы двух простых чисел.

B) Каждое целое число >5 представимо в виде суммы трех простых чисел.

Очевидно, гипотезы A и B эквивалентны. Из $2n-2=p_1+p_2$ следует $2n=p_1+p_2+2$ и $2n+1=p_1+p_2+3$. Наоборот, из $2n=p_1+p_2+p_3$ следует, что $p_1=2$ и $2n-2=p_2+p_3$. Утверждения A и B до сих пор полностью не доказаны.

Из обобщенной гипотезы Римана в 1922 г. Харди и Литтльвуд смогли вывести, что каждое достаточно большое нечетное число представимо в виде суммы трех простых чисел. В 1937 г. Виноградову удалось получить этот результат независимо от недоказанной гипотезы [1]). Для количества $A(N)$ представлений нечетного N в виде суммы трех простых чисел имеется выражение

$$A(N)=\frac{N^2}{2\log^3 N}\times$$
$$\times\left\{\prod_p\left(1+\frac{1}{(p-1)^3}\right)\prod_{p\mid N}\left(1-\frac{1}{p^2-3p+3}\right)+O(1)\right\},$$

где первое произведение распространено на все p, а второе лишь на простые делители N.

Пиппинг представил все нечетные N из интервала $9\leqslant N\leqslant 360\,749$ в виде суммы трех нечетных простых чисел, наименьшее из которых равно 3, 5 или 7. Он подтвердил также гипотезу A для всех $N\leqslant 100\,000$.

В направлении гипотезы A также достигнуты интересные результаты. Символом $B(x)$ обозначим количество таких четных $n\leqslant x$, которые нельзя представить в виде суммы двух простых, тогда $\lim\limits_{x\to\infty} B(x)/x=0$, т. е. «почти все» четные числа являются суммами двух простых чисел (Эстерман, ван дер Корпут). Несмотря на это, естественно, все еще возможно бесконечно много исключений.

Упомянутый в § 60 путь к доказательству гипотезы A методом решета не приводит к цели, так как оценки снизу положительным числом для $N(2, x, x^{1.2})$ не получены. Все же методом решета можно показать, что каждое достаточно

---

[1]) Другие доказательства дали Линник и Чудаков. Легко доступное изложение имеется в книге: T. Estermann, Introduction to modern prime number theory (Cambridge Tracts № 41, Cambridge University Press, 1952).

большое четное n допускает представление в форме $n=a^{(r)}+b^{(s)}$, где $a^{(r)}$ составное число, состоящее не более чем из r простых множителей ($a^{(1)}=p$, $a^{(2)}=p^2$ или pp', и т. д.). Примеры: $r=s=9$ (Брун, 1919); $r=s=7$ (Радемахер, 1924); $r=s=6$ (Эстерман, 1932); $r=5$, $s=7$; $r=4$, $s=9$; $r=3$, $s=15$; $r=2$, $s=366$ (Риччи, 1936); $r=s=4$ (Бухштаб, 1940); $r=1$, $s=K$ (абсолютная константа) (Реньи, 1947); $r=2$, $s=3$ (А. Сельберг, 1950).

73. Аддитивные представления натуральных чисел простыми числами. По гипотезе B в представлении

$$n=p+p'+p''+\ldots+p^{(n)}$$

всегда можно обойтись тремя слагаемыми. Без ограничения числа слагаемых легко получается доказанная Рихертом [19]

Теорема 41. *Каждое натуральное число $n>6$ представимо в виде суммы неравных простых чисел.*

Доказательство. Разложения $7=7$, $8=5+3$, $9=7+2$, $10=7+3$, $11=11$, $12=7+5$, $13=11+2$, $14=11+3$, $15=7+5+3$, $16=11+5$, $17=7+5+3+2$, $18=11+7$, $19=11+5+3$ показывают, что серия из $s_0=13\geqslant p_6$ последовательных чисел может быть построена из различных простых $p_1=2$, $p_2=3$, $p_3=5$, $p_4=7$, $p_5=11$. Если к этим s_0 числам прибавить $p_6=13$, то всего получим $s_1=s_0+p_6=26$ чисел $7\leqslant n\leqslant 32$, представленных в требуемой форме. Добавление $p_7=17$ к уже представленным s_1 числам расширит нашу область до $s_2=s_1+p_7=43$ чисел $7\leqslant n\leqslant 49$. Эта операция может быть бесконечно продолжаема, если в $s_{k+1}=s_k+p_{6+k}$ всегда $p_{6+k}\leqslant s_k$. В этом мы можем убедиться с помощью полной индукции. Из $p_{6+k-1}\leqslant s_{k-1}$ и теоремы 31 следует

$$p_{6+k}<2p_{6+k-1}\leqslant s_{k-1}+p_{6+k-1}=s_k,\ \text{ч. т. д.}$$

В 1930 г. русским математиком Шнирельманом элементарным методом доказана существенно приближающаяся к гипотезе B

Теорема 42. *Каждое натуральное $n>1$ представимо в виде суммы не более чем S простых чисел. При этом S — абсолютная постоянная (постоянная Шнирельмана).*

Мы легко проведем доказательство существования S после некоторых приготовлений. Численное значение S последовательно снижалось от 800 000 (Шнирельман) до 67 (Риччи,

1936). В 1951 г. Шапиро и Варга [30] методом решета Сельберга получили неравенство $S \leqslant 20$. Из теоремы Гольдбаха — Виноградова следует, что для достаточно больших n будет $S \leqslant 4$, так как из $2n-1=p_1+p_2+p_3$ тотчас следует $2n+2=3+p_1+p_2+p_3$.

74. Плотность числовой последовательности является основным понятием при аддитивном представлении. Пусть $A=\{a_1=1, a_2, \ldots\}$ подпоследовательность последовательности натуральных чисел, содержащая единицу, а $A(x)$ обозначает количество $a_i \leqslant x$, $a_i \in A$. Под плотностью α последовательности A понимают нижнюю грань отношения $A(x)/x$. Таким образом, $A(x) \geqslant \alpha x$ для всех $x \geqslant 1$ и $0 \leqslant \alpha \leqslant 1$. Например, арифметическая прогрессия с первым членом 1 и разностью d имеет плотность $1/d$. Из $\alpha=1$ следует $A=R$.

Из s последовательностей

$$A_1=\{a_{i_1}\}, \quad A_2=\{a_{i_2}\}, \quad \ldots, \quad A_s=\{a_{i_s}\}$$

с плотностями $\alpha_1, \alpha_2, \ldots, \alpha_s$ построим суммарную последовательность $C=A_1+A_2+\ldots+A_s$, которая содержит все различные положительные числа вида $\varepsilon_1 a_{i_1}+\ldots+\varepsilon_s a_{i_s}$ ($\varepsilon_\nu=0$ или 1), расположенные в порядке возрастания. Если $A_1=A_2=\ldots=A_s=A$ и C содержит все натуральные числа $C=sA=R$, то это означает, что любое n допускает представление в виде суммы не более чем s слагаемых из A. Естественно спросить, как плотность γ последовательности C зависит от плотностей $\alpha_1, \alpha_2, \ldots, \alpha_s$. В 1942 г. Х. Манн доказал давно предполагаемое соотношение

$$\gamma \geqslant \alpha_1+\alpha_2+\ldots+\alpha_s \quad \text{или} \quad \gamma=1$$

в зависимости от того, будет ли $\alpha_1+\alpha_2+\ldots+\alpha_s<1$ или $\geqslant 1$. Таким образом, при $\alpha>0$ последовательность sA имеет плотность 1, если $s\alpha \geqslant 1$, а это означает, что каждое n допускает аддитивное представление с помощью не более чем $[\alpha^{-1}]+1$ элементов из A. Так как мы доказываем лишь существование постоянной Шнирельмана, нам достаточно получить худшую оценку для γ, которая зато проще выводится.

Заметим, во-первых, что из $2\alpha \geqslant 1$ тотчас следует $2A=R$. Действительно, если $x>1$ не входит в A, то $A(x-1)=A(x) \geqslant \alpha x > \alpha(x-1)$. Количество положительных $x-a_s \leqslant x-1$ также равно $A(x-1)$. Если бы все a_s

и $x-a_s$ были различными, то существовало бы больше чем $2\alpha(x-1)$ чисел $\leqslant x-1$, что невозможно, так как $2\alpha \geqslant 1$. Таким образом, хотя бы один раз $x-a_s=a_t$ или $x=a_s+a_t$.

Лемма. *Если последовательность A имеет плотность $\alpha>0$, то плотность sA по меньшей мере равна $1-(1-\alpha)^s$.*

Доказательство. Рассмотрим сперва две последовательности A и B с плотностями α и β. Тогда $C=A+B$ наверняка содержит следующие различные элементы $\leqslant x$:

1. $A(x) \geqslant \alpha x$ чисел из $A: a_1=1, a_2, \ldots, a_{A(x)}$.
2. $B(a_{i+1}-a_i-1) \geqslant \beta(a_{i+1}-a_i-1)$ чисел a_i+b_r между a_i и a_{i+1} $[1 \leqslant i < A(x)]$.
3. $B(x-a_{A(x)}) \geqslant \beta(x-a_{A(x)})$ чисел $a_{A(x)}+b_r \leqslant x$.

Сложением получаем:

$$\begin{aligned} C(x) &\geqslant A(x)+\beta\{a_{A(x)}-a_1-[A(x)-1]+x-a_{A(x)}\}= \\ &= A(x)+\beta[x-A(x)]= \\ &= \beta x+(1-\beta)A(x) \geqslant \beta x+(1-\beta)\alpha x= \\ &= (\alpha+\beta-\alpha\beta)x. \end{aligned}$$

Так как $2\alpha-\alpha^2=1-(1-\alpha)^2$, то лемма для $s=2$ доказана. Для любого s доказательство получается полной индукцией. При $\beta=1-(1-\alpha)^{s-1}$ имеем:

$$C(x) \geqslant \{\alpha+1-(1-\alpha)^{s-1}-\alpha[1-(1-\alpha)^{s-1}]\}x=$$
$$=\{\alpha+(1-\alpha)[1-(1-\alpha)^{s-1}]\}x=\{1-(1-\alpha)^s\}x, \text{ ч. т. д.}$$

Так как мы можем теперь предположить, что $\alpha<1/2$, то существует такое наименьшее m, что $1-(1-\alpha)^m \geqslant 1/2$. Тогда $2(mA)=2mA=R$.

75. Доля метода решета в доказательстве существования s. По теореме 27 последовательность простых чисел имеет плотность нуль, даже если добавить впереди 1. Шнирельманом доказана имеющая интерес сама по себе

Теорема 43. *Последовательность, состоящая из 1 и сумм простых чисел $p+p'$, имеет положительную плотность.*

Доказательство. Пусть $M(x)$ означает количество чисел $4 \leqslant n \leqslant x$, представимых в виде суммы $p+p'$, а $D(n)$—

количество представлений для фиксированного n. Из неравенства Шварца [1]) следует

$$\Big\{\sum_{n=4}^{x} 1\cdot D(n)\Big\}^2 \leqslant M(x)\sum_{n=4}^{x} D^2(n) \text{ или}$$

$$M(x) \geqslant \frac{\Big(\sum\limits_{n=4}^{x} D(n)\Big)^2}{\sum\limits_{n=4}^{x} D^2(n)}. \tag{140}$$

Для того чтобы иметь возможность применить (140), используем оценку снизу для числителя и оценку сверху для знаменателя. Оценку снизу легко получаем из теоремы 28

$$\sum_{n=4}^{x} D(n) \geqslant \pi^2\left(\frac{x}{2}\right) > \frac{C_{80}x^2}{\log^2 x}. \tag{141}$$

Для всех $p \leqslant x/2$, $p' \leqslant x/2$ имеем $p+p' \leqslant x$, т. е. $p+p'$ — представление, учтенное в $\sum D(n)$, причем $p+p'$ и $p'+p$ для $p \neq p'$ рассматриваются как различные.

Оценку сверху для $D(n)$ доставит нам оценка (139), доказанная методом решета. Для того чтобы оценить $\sum D^2(n)$, рассмотрим разложение распространенного на все простые делители n произведения $\prod(1+p^{-1})^2 = \sum a^{-1}\sum b^{-1} = \sum (ab)^{-1}$, где a и b независимо пробегают все делители n, свободные от квадратов. Если просуммировать теперь такие равенства для всех $n \leqslant x$, то произведение ab при $a \leqslant x$, $b \leqslant x$ встретится в правой части лишь тогда, когда общее наименьшее кратное $\{a, b\}$ чисел a и b является делителем одного из n, а это для $n \leqslant x$ будет точно $[x\{a, b\}^{-1}]$ раз. Так как $\{a, b\} \geqslant a$, $\geqslant b$, то $\{a, b\} \geqslant \sqrt{ab}$, так что вследствие (53)

[1]) $(\sum a_n b_n)^2 \leqslant \sum a_n^2 \sum b_n^2$. Доказательство: квадратное уравнение $\sum (a_n x + b_n)^2 = 0$ не может иметь вещественных корней, кроме случая $b_i/a_i = \lambda$, когда $x_1 = x_2 = -\lambda$. Следовательно, для дискриминанта имеем:

$$(\sum a_n b_n)^2 - \sum a_n^2 \sum b_n^2 \leqslant 0.$$

при $\rho = +0{,}5$

$$\sum_{n=1}^{x} \sum_{a|n} a^{-1} \sum_{b|n} b^{-1} = \sum_{a=1}^{x} \sum_{b=1}^{x} (ab)^{-1} \left[\frac{x}{\{a, b\}}\right] \leqslant$$

$$\leqslant \sum_{a=1}^{x} \sum_{b=1}^{x} x (ab)^{-\frac{3}{2}} < x \sum_{a=1}^{\infty} a^{-\frac{3}{2}} \sum_{b=1}^{\infty} b^{-\frac{3}{2}} < C_{81} x.$$

Для $x > n \geqslant 8$ можно в неравенстве для $D(n)$, аналогичном (139), заменить $n(\log n)^{-2}$ большей величиной $x(\log x)^{-2}$. Получим:

$$\sum_{n \leqslant x} D^2(n) < C_{82}^2 x^2 (\log x)^{-4} C_{81} x = C_{83} x^3 (\log x)^{-4}.$$

Отсюда и из (140) и (141) следует

$$M(x) > C_{80}^2 x^4 (\log x)^{-4} C_{83}^{-1} x^{-3} (\log x)^4 = C_{84} x, \text{ ч. т. д.}$$

76. Доказательство теоремы 42. На основании § 74 и теоремы 43 существует такое натуральное число k, что $R = kM$, где M — это последовательность, состоящая из чисел 1 и $p + p'$. Таким образом, для представления любого $n > 1$ достаточно k слагаемых 1 или $p + p'$, т. е. $2k$ слагаемых 1 или p. Если $n > 2$, то из разложения числа $n - 2$ получается представление $n = 2 + \sum 1 + \sum p$. Число $2 + \sum 1$ можно записать или в виде $\sum 2$ или в виде $3 + \sum 2$. Таким образом, $s \leqslant 2k$ и конечность s доказана.

ПРИЛОЖЕНИЕ

АНАЛИТИЧЕСКИЙ МЕТОД ОЦЕНКИ ЧИСЛА ПРОСТЫХ ЧИСЕЛ В НАТУРАЛЬНОМ РЯДЕ И АРИФМЕТИЧЕСКОЙ ПРОГРЕССИИ

А. О. Гельфонд

Элементарный метод А. Сельберга, дающий возможность доказать предельный закон распределения простых чисел, не может служить для сколько-нибудь хорошей оценки остаточного члена в формуле

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

Для величины $R(x)$ можно только получить оценку

$$|R(x)| < \frac{x}{\ln^{1+\alpha} x},$$

где α — некоторая постоянная, $0 < \alpha < 1$. Аналитический же метод Адамара — Валле-Пуссена, опирающийся на аналитические свойства функции Римана

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

позволяет дать существенно более точную оценку для $\pi(x)$, именно получить, что

$$\pi(x) = \int_{2}^{x} \frac{dt}{\ln t} + O\left(xe^{-\alpha \ln^{\gamma} x}\right), \qquad (1)$$

где $\alpha > 0$ — постоянная, а $\gamma = \frac{3}{5}$ [1,2,3,4]. Это значение γ — наилучшее известное в настоящее время, первое же полученное

для γ значение было $\frac{1}{2}$. Остаточный член в формуле (1) растет, например, медленнее, чем $x\ln^{-N}x$ для произвольного сколь угодно большого N.

Мы дадим здесь изложение метода Адамара — Валле-Пуссена в упрощенной форме, без более глубокого изучения свойств $\zeta(s)$ и $L(s, \chi)$

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

где $\chi(n)$ — характер модуля $m > 1$, необходимого для получения оценки (1) при $\gamma = \frac{1}{2}$ или, более общо, оценки

$$\pi(x; l, m) = \sum_{\substack{p \leqslant x \\ p \equiv e \pmod m}} 1 = \frac{1}{\varphi(m)} \int_2^x \frac{dt}{\ln t} + O\left(xe^{-\alpha \ln^{\gamma} x}\right), \qquad (2)$$

$$(l, m) = 1,$$

при $\gamma = \frac{1}{2}$ или больших величинах γ. Вместо уточнения оценки остаточного члена мы зато дадим доказательство оценки (2) для любой прогрессии с разностью m и, в частности, для натурального ряда. Прежде всего установим связь между функцией $\psi(x)$

$$\psi(x) = \sum_{n \leqslant x} \Lambda(n), \quad \Lambda(n) = \begin{cases} \ln p, & n = p^k, \\ 0, & n \neq p^k, \end{cases} \qquad (3)$$

где p — простое число, и функцией Эйлера — Римана $\zeta(s)$. Эта связь в простейшем случае, для $\psi(x)$, имеет вид

$$\psi_1(x) = \int_2^x \psi(t)\, dt = \frac{-1}{2\pi i} \int_{\sigma_0} \frac{\zeta'(s)}{\zeta(s)} \frac{x^{1+s}}{s(s+1)} ds, \qquad (4)$$

где интеграл взят в комплексной плоскости s по прямой $Rs = \sigma$, $\sigma > 1$ в положительном направлении.

Докажем справедливость формулы (4) в более общем случае арифметической прогрессии.

Лемма I. *Если*

$$L(s, \chi) = \sum_{1}^{\infty} \frac{\chi(n)}{n^s}, \qquad (5)$$

где $\chi(n)$ *какой-либо характер модуля* $m \geqslant 1$ (при $m=1$ $L(s, \chi)=\zeta(s)$), *то имеет место представление*

$$\psi_1(x, \chi)=\int_2^x \psi(x, \chi)\, dx=\frac{-1}{2\pi i}\int_\sigma \frac{L'(s, \chi)}{L(s, \chi)}\frac{x^{1+s}}{s(s+1)}\, ds, \qquad (6)$$

где интеграл взят по прямой $Rs=\sigma$ от $-\infty$ до ∞, *а* $\psi(x, \chi)$ *имеет вид*

$$\psi(x, \chi)=\sum_{n \leqslant x}\chi(n)\Lambda(n); \quad \psi_1(x, \chi)=\sum_{n \leqslant x}\chi(n)\Lambda(n)(x-n). \qquad (7)$$

Прежде всего заметим, что

$$L(s, \chi)=\prod_p\left(1-\frac{\chi(p)}{p^s}\right)^{-1}=\sum_1^\infty \frac{\chi(n)}{n^s}, \qquad (8)$$

где произведение взято по всем простым числам в силу мультипликативности $\chi(n)$, $\chi(n)\chi(k)=\chi(nk)$ и того, что все целые числа единственным образом представляются в виде произведения простых.

Логарифмируя и разлагая в ряд каждое слагаемое, мы получаем, что

$$\ln L(s, \chi)=-\sum_p \ln\left(1-\frac{\chi(p)}{p^s}\right)=\sum_p\sum_{k=1}^\infty \frac{\chi(p^k)}{kp^{ks}}.$$

Дифференцируя по s, мы окончательно получаем, что

$$-\frac{L'(s, \chi)}{L(s, \chi)}=\sum_p\sum_{k=1}^\infty \frac{\chi(p^k)\ln p}{p^{ks}}=\sum_1^\infty \frac{\chi(n)\Lambda(n)}{n^s} \qquad (9)$$

по определению функции Мангольта $\Lambda(n)$. Полученный ряд равномерно сходится по s в любой полосе $\sigma_1 \geqslant Rs \geqslant \sigma_0 > 1$. Вычислим теперь один вспомогательный интеграл. Пусть, действительно, $x > 0$. Тогда

$$\frac{1}{2\pi i}\int_{\sigma_0}\frac{x^s}{s(s+1)}\, ds=\begin{cases}1-\dfrac{1}{x}, & x \geqslant 1,\\ 0, & x \leqslant 1,\end{cases} \qquad (10)$$

где интеграл взят по прямой $Rs=\sigma_0>0$ ($s=\sigma+it$, $\sigma=\sigma_0$).

Действительно, если $x \leqslant 1$, то, пользуясь теоремой Коши и замыкая контур интегрирования в правой полуплоскости, мы

получаем, что наш интеграл равен нулю, так как в этой полуплоскости

$$\left|\frac{x^s}{s(s+1)}\right| < \frac{x^{\sigma_0}}{t^2+\sigma_0^2}, \quad s=\sigma+it.$$

Если же $x>1$, то, пользуясь теоремой о вычетах и перенося контур интегрирования на прямую $\sigma_1<-1$, получаем, что

$$\frac{1}{2\pi i}\int\limits_{\sigma_0}\frac{x^s}{s(s+1)}ds = 1 - x^{-1} + \frac{1}{2\pi i}\int\limits_{\sigma_1}\frac{x^s}{s(s+1)}ds = 1-\frac{1}{x},$$

так как интеграл по прямой σ_1 равен нулю по той же причине, что и интеграл по σ_0 в случае $x\leqslant 1$. Его можно замкнуть в левой полуплоскости и воспользоваться теоремой Коши. Пользуясь свойствами интеграла (10), мы можем теперь вычислить интеграл

$$\frac{-1}{2\pi i}\int\limits_{\sigma_0}\frac{L'(s,\chi)}{L(s,\chi)}\frac{x^{s+1}}{s(s+1)}ds = \sum_{n=1}^{\infty}\frac{\chi(n)\Lambda(n)x}{2\pi i}\int\limits_{\sigma_0}\frac{\left(\frac{x}{n}\right)^s}{s(s+1)}ds =$$

$$= \sum_{n\leqslant x}\chi(n)\Lambda(n)(x-n), \quad \sigma_0>1, \qquad (11)$$

так как почленное интегрирование ряда (9) возможно в силу равномерной его сходимости на прямой $Rs=\sigma_0>1$.

Далее, если $\psi(x,\chi)=\sum\limits_{n\leqslant x}\chi(n)\Lambda(n)$, то, меняя порядок интегрирования и суммирования, мы будем иметь, что

$$\int_2^x\psi(x,\chi)\,dx = \int_2^x\sum_{n\leqslant t}\chi(n)\Lambda(n)\,dt =$$

$$= \sum_{n\leqslant x}\chi(n)\Lambda(n)\int_n^x dt = \sum_{n\leqslant x}\chi(n)\Lambda(n)(x-n).$$

Этим лемма I доказана.

Для того чтобы из представления (6) функции $\psi_1(x,\chi)$ получить ее главный член и оценку остаточного члена, надо иметь сведения о поведении $\frac{L'(s,\chi)}{L(s,\chi)}$ хоть в какой-либо области, лежащей левее прямой $Rs=1$, другими словами, при $s=\sigma+it$ левее прямой $\sigma=1$. Прежде всего заметим, что направо от прямой $\sigma=1$ функция $L(s,\chi)$ — аналитическая

функция, не имеющая нулей и особенностей. Это следует из равномерной сходимости бесконечного произведения (8) в области $Rs \geqslant \sigma_0 > 1$, $|s| < r$, при любых σ_0 и r, так как в этой области равномерно сходится ряд $\sum_p \frac{1}{p^s}$, где сумма взята по всем простым. Этот последний факт сходимости ряда $\sum_p \frac{1}{p^s}$ есть прямое следствие тривиального неравенства $p_k > k$, где p_k — k-е простое число, $p_1 = 2$. Для дальнейшего нам достаточно будет рассмотреть поведение $L(s, \chi)$ и, в частности, $\zeta(s)$ только в области, определяемой неравенствами

$$1 - \frac{c}{\ln^{\gamma}(|t|+3)} \leqslant \sigma \leqslant 2, \quad s = \sigma + it, \tag{12}$$

где $\gamma \geqslant 1$ — некоторая фиксированная постоянная, а c, $0 < c \leqslant \frac{1}{4}$ — достаточно малая постоянная. Существенную роль при оценке порядка убывания остаточного члена для $\psi_1(x, \chi)$ играет постоянная γ — она определяет порядок в показателе оценки (2), а c связано только с множителем α в том же показателе.

Лемма II. *Если $\chi(n)$ есть главный характер модуля $m \geqslant 1$, другими словами, $\chi(n) = 1$, $(n, m) = 1$, $\chi(n) = 0$, $(m, n) > 1$, то функция $L(s, \chi)$ имеет полюс первого порядка в области* (12) *при $s = 1$ и в этой области, вне кружка $|s - 1| = \delta$, где $\delta > 0$ — любая постоянная, выполняются неравенства*

$$|L(s, \chi)| < A \ln(|t|+3), \quad |L'(s, \chi)| < A \ln^2(|t|+3), \tag{13}$$

где A — положительная постоянная, зависящая только от δ и $s = \sigma + it$.

Для доказательства этой леммы достаточно получить оценку только для $\zeta(s)$, так как при $m > 1$

$$L(s, \chi) = \prod_{(p, m)=1} (1 - p^{-s})^{-1} = \prod_{p|m} (1 - p^{-s}) \zeta(s), \tag{14}$$

где первый множитель в правой части есть целая функция s и в области (12) ограничен вместе с первой производной. Действительно, в области (12)

$$0 < \prod_{p|m} |1 - p^{-s}| \leqslant \prod_{p|m} (1 + p^{-\sigma}) \leqslant \prod_{p|m} 2$$

и, кроме того,

$$\left|\frac{d}{ds}\prod_{p|m}(1-p^{-s})\right|\leqslant\prod_{p|m}(1+\ln p),$$

так как σ в области (12) не меньше $\frac{3}{4}$.

Пусть сначала $Rs>1$. Положим $N=[t]+1$. Тогда

$$\int_N^\infty\frac{[x]\,dx}{x^{s+1}}=\sum_{n=N}^\infty n\int_n^{n+1}\frac{dx}{x^{s+1}}=\frac{1}{s}\sum_N^\infty\left[\frac{n}{n^s}-\frac{n}{(n+1)^s}\right]=$$

$$=\frac{1}{s}\left[N^{1-s}+\sum_{N+1}^\infty\frac{1}{n^s}\right]=\frac{1}{s}\left[\zeta(s)-\sum_1^N\frac{1}{n^s}+N^{1-s}\right],$$

и, кроме того,

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

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

Воспользовавшись этими двумя соотношениями для определения $\zeta(s)$, мы получаем, что, так как $[x]=x-\{x\}$,

$$\zeta(s)=\sum_1^N\frac{1}{n^s}-N^{1-s}+s\int_N^\infty\frac{[x]\,dx}{x^{s+1}}=$$

$$=\sum_1^N\frac{1}{n^s}+\frac{s}{s-1}-N^{1-s}+\frac{s}{s-1}(N^{1-s}-1)-s\int_N^\infty\frac{\{x\}}{x^{s+1}}dx. \quad (15)$$

Уже из этого соотношения видно, что $\zeta(s)$ регулярна в полуплоскости $Rs>0$, за исключением точки $s=1$, где $\zeta(s)$ имеет полюс первого порядка с вычетом единицы, так как все члены в правой части (15) регулярны в правой полуплоскости, за исключением $\frac{s}{s-1}$.

Оценку $|\zeta(s)|$ будем вести при $|t|\geqslant 1$ и $2\geqslant\sigma\geqslant 1-\frac{c}{\ln(|t|+3)}$, $0<c\leqslant\frac{1}{4}$. Мы будем здесь и в дальнейшем пользоваться оценками (52)—(57) из книги Троста без ссылок.

Прежде всего будем иметь, что при

$$\sigma \geqslant 1 - \frac{c}{\ln(|t|+3)}, \quad |s-1| \geqslant \delta > 0,$$

$$\left|\sum_1^N \frac{1}{n^s}\right| < \sum_1^N n^{-1+\frac{c}{\ln(|t|+3)}} < N^{\frac{c}{\ln(|t|+3)}} \sum_1^N \frac{1}{n} =$$

$$= e^{c\frac{\ln(|t|+1)}{\ln(|t|+3)}} O(\ln N) = O[\ln(|t|+3)]; \qquad (16)$$

$$|N^{1-s}| = e^{c\frac{\ln N}{\ln(|t|+3)}} = O(1), \quad \left|\frac{s}{s-1}\right| = O(1).$$

Далее,

$$\left| s\int_N^\infty \frac{\{x\}dx}{x^{s+1}} \right| < |s| \int_N^\infty \frac{dx}{x^{1+\sigma}} = \frac{|t|+2}{\sigma N} N^{1-\sigma} = O(1). \qquad (16')$$

Применяя эти оценки к (15), получаем, что

$$\left.\begin{aligned} |\zeta(s)| = O[\ln(|t|+3)], \ |s-1| \geqslant \delta > 0, \\ 2 \geqslant \sigma \geqslant 1 - \frac{c}{\ln(|t|+3)}, \end{aligned}\right\} \qquad (17)$$

где $c \leqslant \frac{1}{4}$.

Дифференцируя (15) по s, получаем:

$$\zeta'(s) = -\sum_1^N \frac{\ln n}{n^s} - N^{1-s}\ln N - \frac{N^{1-s}}{(s-1)^2} - \frac{sN^{1-s}}{s-1}\ln N -$$

$$- \int_N^\infty \frac{\{x\}dx}{x^{s+1}} + s\int_N^\infty \frac{\{x\}\ln x}{x^{s+1}}\,dx. \qquad (18)$$

Пользуясь только что полученными оценками и присоединяя к ним оценки

$$\left.\begin{aligned} &\left|\sum_1^N \frac{\ln n}{n^s}\right| < N^{1-\frac{c}{\ln(|t|+3)}} \sum_1^N \frac{\ln n}{n} = O[\ln^2(|t|+3)], \\ &|s|\left|\int_N^\infty \frac{\{x\}\ln x}{x^{s+1}}\,dx\right| < |s| \int_N^\infty \frac{\ln x}{x^{1+\sigma}}dx < \\ &< 2\frac{|t|+3}{\sigma N}\ln N \cdot N^{\frac{c}{\ln(|t|+3)}} = O[\ln(|t|+3)], \end{aligned}\right\} \qquad (19)$$

мы получаем для $|\zeta'(s)|$ оценку

$$\left.\begin{aligned} |\zeta'(s)| &= O[\ln^2(|t|+3)],\ 2 \geqslant \sigma > 1 - \frac{c}{\ln(|t|+3)}, \\ & |s-1| \geqslant \delta > 0. \end{aligned}\right\} \quad (20)$$

Применяя оценки (17) и (20) к соотношению (15), мы сразу получаем, что

$$\left.\begin{aligned} &|L(s,\chi)| = O[\ln(|t|+3)],\ |L'(s,\chi)| = O[\ln^2(|t|+3)], \\ &2 \geqslant \sigma \geqslant 1 - \frac{c}{\ln^{\gamma}(|t|+3)},\ \gamma \geqslant 1,\ c \leqslant \frac{1}{4},\ |s-1| \geqslant \delta. \end{aligned}\right\} \quad (21)$$

Кроме того, мы получаем, что если $\chi(n)$ — главный характер модуля m, то в области (12) $L(s,\chi)$ регулярна всюду, кроме точки $s=1$, где она имеет полюс первого порядка.

Этим лемма II доказана.

Пусть теперь $\chi(n)$ — неглавный характер модуля $m \geqslant 2$. Полагая тогда

$$s_n = \sum_1^n \chi(k), \quad N = [|t|+1],$$

будем иметь, что

$$\left.\begin{aligned} L(s,\chi) &= \sum_1^N \frac{\chi(n)}{n^s} + \sum_{N+1}^{\infty} \frac{s_n - s_{n-1}}{n^s} = \\ &= \sum_1^N \frac{\chi(n)}{n^s} - \frac{s_N}{(N+1)^s} + s\sum_{N+1}^{\infty} s_n \int_n^{n+1} \frac{dx}{x^{s+1}}, \\ L'(s,\chi) &= -\sum_1^N \frac{\chi(n)\ln n}{n^s} + \frac{s_N \ln(N+1)}{(N+1)^s} + \\ &+ \sum_{N+1}^{\infty} s_n \int_n^{n+1} \frac{dx}{x^{s+1}} - s\sum_{N+1}^{\infty} s_n \int_n^{n+1} \frac{\ln x\, dx}{x^{s+1}}. \end{aligned}\right\} \quad (22)$$

Пользуясь соотношениями (24) и (108) книги Троста, прежде всего будем иметь оценку $|s_n|<m$. Отсюда следует, что

$$\left.\begin{aligned} |L(s,\chi)| &< \sum_1^N \frac{1}{n^\sigma} + \frac{m}{(N+1)^\sigma} + m|s|\int_N^\infty \frac{dx}{x^{\sigma+1}}, \\ |L'(s,\chi)| &< \sum_1^N \frac{\ln n}{n^\sigma} + \frac{m\ln(N+1)}{N^\sigma} + \int_N^\infty \frac{dx}{x^{\sigma+1}} + \\ &\quad + (|t|+3)\,m\int_N^\infty \frac{\ln x}{x^{\sigma+1}}\,dx. \end{aligned}\right\} \quad (23)$$

Эти неравенства того же типа, что и для $|\zeta(s)|$ и $|\zeta'(s)|$ и не требуют новых оценок для отдельных членов в правых частях. Поэтому, воспользовавшись неравенствами (16), (16′) и (19), мы, так же как и выше, получаем, что

$$\left.\begin{aligned} &|L(s,\chi)| = O[\ln(|t|+3)],\ |L'(s,\chi)| = O[\ln^2(|t|+3)], \\ &2 \geqslant \sigma \geqslant 1 - \frac{c}{\ln^\gamma(|t|+3)},\ c \leqslant \frac{1}{4},\ \gamma \geqslant 1 \end{aligned}\right\} \quad (24)$$

уже при любом t, так как в правых частях (22) стоят регулярные в полуплоскости $\sigma>0$ функции.

Итак, нами доказана

Лемма III. *$L(s,\chi)$ регулярна в полуплоскости $\sigma>0$, $s=\sigma+it$ при $\chi(n)$ неглавном характере модуля m и в области* (12) *выполняются неравенства* (24).

Теперь нам нужно получить оценки снизу для $|L(s,\chi)|$ в области (12). Заметим прежде всего, что в книге Троста, в пп. 56 и 57 гл. VIII уже доказано необращение в нуль $L(1,\chi)$ при неглавном характере $\chi(n)$ модуля m, другими словами, что

$$L(1,\chi) = \sum_1^\infty \frac{\chi(n)}{n} \neq 0,\ \chi \neq \chi_0. \quad (25)$$

Из этого следует вследствие аналитичности $L(s,\chi)$ при любом χ, что существует малая окрестность точки $s=1$, размеры которой зависят только от m, где $L(s,\chi)\neq 0$, так как при χ главном характере в $s=1$ $L(s,\chi)$ имеет полюс.

Лемма IV. *Если* α, p, t и σ *действительны,* $\alpha \geqslant 0$, $\sigma > 0$, $p > 1$, $|t| > 0$, *то имеет место неравенство Адамара*

$$\left|1-\frac{1}{p^{\sigma}}\right|^{3}\left|1-\frac{e^{i\alpha}}{p^{\sigma+it}}\right|^{4}\left|1-\frac{e^{2i\alpha}}{p^{\sigma+2it}}\right|^{-1} > 1. \qquad (26)$$

Действительно, полагая $e^{i\alpha}p^{-it} = e^{i\beta}$, β — действительное число, логарифмируя левую часть (26) и разлагая каждый логарифм в ряд, будем иметь, что

$$\ln\left[\left|1-\frac{1}{p^{\sigma}}\right|^{3}\left|1-\frac{e^{i\alpha}}{p^{\sigma+it}}\right|^{4}\left|1-\frac{e^{2i\alpha}}{p^{\sigma+2it}}\right|^{-1}\right] =$$

$$= R\left\{\sum_{1}^{\infty}\frac{p^{-n\sigma}}{n}\left(3+4e^{in\beta}+e^{2in\beta}\right)\right\} =$$

$$= \sum_{1}^{\infty}\frac{p^{-n\sigma}}{n}\left(3+4\cos n\beta+\cos 2n\beta\right) =$$

$$= 2\sum_{1}^{\infty}\frac{p^{-n\sigma}}{n}\left(1+\cos n\beta\right)^{2} > 0,$$

так как логарифм модуля числа есть действительная часть его логарифма. Знак R обозначает взятие действительной части числа.

Из неравенства (26) следует

Лемма V. *Если* $t \neq 0$, *то при любом* χ *модуля* $m \geqslant 1$ *и* $\sigma > 1$ *имеет место неравенство*

$$|L(\sigma, \chi_0)|^{3}\,|L(s, \chi)|^{4}\,|L(s_1, \chi^2)| > 1, \qquad (27)$$

где $s = \sigma + it$, $s_1 = \sigma + 2it$ *и* χ_0 *главный характер.* Действительно, полагая в лемме IV $e^{i\alpha} = \chi(p)$ и перемножая левые части для всех простых p, что возможно при $\sigma > 1$, мы получаем неравенство (27) вследствие представления (8). Но в силу (14) и (15) при $\sigma > 1$

$$L(\sigma, \chi_0) = \prod_{p|m}\left(1-\frac{1}{p^{\sigma}}\right)\sum_{1}^{\infty}\frac{1}{n^{\sigma}} < 1+\int_{1}^{\infty}\frac{dx}{x^{\sigma}} = \frac{\sigma}{\sigma-1}$$

и в силу оценки (24)

$$|L(\sigma+2it, \chi^2)| < A_1 \ln(|t|+3), \quad A_1 > 0,$$

где A_1 зависит от δ, при $|\sigma - 1 + 2it| > \delta$.

Пользуясь этими оценками, мы из неравенства (27) получаем неравенство

$$|L(s,\chi)|>\left(\frac{\sigma-1}{\sigma}\right)^{\frac{3}{4}}A_1^{-\frac{1}{4}}\ln^{-\frac{1}{4}}(|t|+3), \qquad (28)$$

верное при $\sigma>1$ и любом t, так как если $\chi=\chi_0$ — главный характер и t близко к нулю, то левая часть сколь угодно велика, а если $\chi\neq\chi_0$, то в окрестности $s=1$, как мы уже видели, $L(s,\chi)$ отлично от нуля.

Лемма VI. Существуют такие постоянные c_0 и A_2, зависящие только от m, что в области (12) при $c=C_0$ и $\gamma=\frac{1}{9}$ функция $L(s,\chi)$ при любом χ модуля $m\geqslant 1$ подчиняется неравенству

$$|L(s,\chi)|>\frac{1}{A_2\ln^7(|t|+3)}. \qquad (29)$$

Пусть $\sigma_0<1$, $\sigma_1=2-\sigma_0$, $\sigma\geqslant\sigma_0$, $2>\sigma_0+\sigma$, $s=\sigma+it$, $s_1=\sigma_1+it$, $t>0$. Тогда

$$\int_s^{s_1}L'(s,\chi)\,ds=L(s_1,\chi)-L(s,\chi).$$

Отсюда в силу неравенств (28) и (21) следует неравенство

$$|L(s,\chi)|>|L(s_1,\chi)|-\left|\int_s^{s_1}L'(s,\chi)\,ds\right|>$$

$$>2^{-\frac{3}{4}}A_1^{-\frac{1}{4}}(\sigma_1-1)^{\frac{3}{4}}\ln^{-\frac{1}{4}}(|t|+3)-(\sigma_1-\sigma_0)A'\ln^2(|t|+3)=$$

$$=2^{-\frac{3}{4}}A_1^{-\frac{1}{4}}(1-\sigma_0)^{\frac{3}{4}}\ln^{-\frac{1}{4}}(|t|+3)\times$$

$$\times\left[1-(1-\sigma_0)^{\frac{1}{4}}A^{\frac{1}{4}}A'2^{\frac{7}{4}}\ln^{\frac{9}{4}}(|t|+3)\right],$$

где A и A' можно считать бо́льшими единицы. Из этого неравенства видно, что если σ_0 удовлетворяет условию

$$(1-\sigma_0)^{\frac{1}{4}}2^{\frac{7}{4}}A^{\frac{1}{4}}A'\ln^{\frac{9}{4}}(|t|+3)\leqslant\frac{1}{2},$$

другими словами, условию

$$1-\sigma_0=c_1\ln^{-9}(|t|+3),\quad c_1\leqslant 2^{-11}A^{-1}(A')^{-4},\qquad (30)$$

где $c_1>0$ постоянная, то

$$|L(s,\chi)|>2^{-\frac{7}{4}}A_1^{-\frac{1}{4}}c_1^{\frac{3}{4}}\ln^{-7}(|t|+3)=$$
$$=\frac{1}{A_2'\ln^7(|t|+3)},\qquad (31)$$

где A_2' — постоянная. Эта постоянная зависит от постоянной A', которая в свою очередь зависит от δ, так как оценка $|L'(s,\chi_0)|$ давалась вне кружка $|s-1|=\delta$. Поэтому оценка (31) может быть верна только вне кружка $|s-1|=\delta$. Но, выбирая δ столь малым, чтобы внутри этого кружка не было нулей $L(s,\chi)$, и заменяя c_1 на $c_0\leqslant c_1$, мы можем обеспечить существование неравенства (31) и вблизи точки $s=1$, другими словами, в области (12) с заменой c_1 на c_0 и γ на $\frac{1}{9}$ с константой A_2 вместо A_2', где A_2, возможно, будет больше A_2'.

Лемма VII. *На кривой*

$$\sigma=1-\frac{c_0}{\ln^9(|t|+3)},\quad 0\leqslant|t|<\infty,\qquad (32)$$

где c_0 определено в лемме VI, *имеет место оценка*

$$\left|\frac{L'(s,\chi)}{L(s,\chi)}\right|<A_3\ln^9(|t|+3),\qquad (33)$$

где A_3 — постоянная.

Эта лемма следует непосредственно из неравенств (29) и (24).

Теперь мы можем уже перейти к исследованию представления (6) для любого $\chi(n)$ модуля $m\geqslant 1$.

В представлении (6) интеграл взят по прямой $\sigma=\sigma_1>1$ в положительном направлении. По теореме Коши этот путь интегрирования можно заменить интегрированием вдоль кривой Γ, даваемой уравнением (32), тоже в положительном направлении, так как в области, ограниченной кривой Γ и прямой $\sigma=\sigma_1>1$, подынтегральная функция удовлетворяет неравенству

$$\left|\frac{L'(s,\chi)}{L(s,\chi)}\frac{x^{s+1}}{s(s+1)}\right|=O\left[\frac{\ln^9(|t|+3)}{(|t|+1)^2}\right],$$

при этом учитывается, что в точке $s=1$ $\frac{L'(s,\chi)}{L(s,\chi)}$ может иметь полюс первого порядка с вычетом -1, если χ есть главный характер. В этом последнем случае $L(s,\chi)$ имеет в точке $s=1$, как мы видели, полюс первого порядка. Таким образом, мы будем иметь соотношение

$$\psi_1(x,\chi)=T+\frac{-1}{2\pi i}\int_\Gamma \frac{L'(s,\chi)}{L(s,\chi)}\frac{x^{1+s}}{s(s+1)}ds, \tag{34}$$

$$T=\begin{cases}\frac{1}{2}x^2, & \chi=\chi_0,\\ 0, & \chi\neq\chi_0,\end{cases}$$

где χ_0 — главный характер модуля m. В частном случае $L(s,\chi)=\zeta(s)$ и $T=\frac{1}{2}x^2$.

Оценим остаточный член на кривой Γ. Прежде всего заметим, что на кривой Γ, при $t\geqslant 0$

$$|ds|=\left|d\left[1-\frac{c_0}{\ln^9(t+3)}+it\right]\right|\leqslant A_4 dt,$$

где A_4 — постоянная.

Далее, пользуясь оценкой (33), получаем:

$$\left|\int_\Gamma \frac{L'(s,\chi)}{L(s,\chi)}\frac{x^{s+1}}{s(s+1)}ds\right|<20A_3A_4\int_0^\infty \frac{x^{2-\frac{c_0}{\ln^9(t+3)}}}{(t+3)^2\ln^{-9}(t+3)}dt<$$

$$<20A_3A_4\int_0^\infty \frac{\ln^9(t+3)}{(t+3)^{\frac{3}{2}}}dt\max_{0\leqslant t<\infty}\left[\frac{x^{2-\frac{c_0}{\ln^9(t+3)}}}{\sqrt{t+3}}\right].$$

Интеграл в правой части — постоянная, а максимум находится из решения простой задачи на минимум функции

$$\frac{1}{2}\ln(t+3)+c_0\frac{\ln x}{\ln^9(t+3)}=\frac{1}{2}\left(z+2c_0\frac{\ln x}{z^9}\right),$$

где z меняется от 1 до ∞. Этот минимум достигается при

$z = (18c_0)^{\frac{1}{10}} \ln^{\frac{1}{10}} x$, и мы получаем неравенство

$$\frac{1}{2}\ln(t+3) + c_0 \frac{\ln x}{\ln^9(t+3)} > \\ > \frac{1}{2}\left[(18c_0)^{\frac{1}{10}} + 2c_0\ (18c_0)^{-\frac{9}{10}}\right] \ln^{\frac{1}{10}} x = \alpha \ln^{\frac{1}{10}} x,\ \alpha > 0.$$

Отсюда уже окончательно следует неравенство

$$\frac{1}{2\pi}\left|\int_\Gamma \frac{L'(s,\chi)}{L(s,\chi)} \frac{x^{s+1}}{s(s+1)}\, ds\right| < A_5 x^2 e^{-\alpha \ln^{\frac{1}{10}} x} \tag{35}$$

где A_5 — постоянная и $\alpha > 0$ — постоянная.

Итак, мы пришли к теореме.

Теорема 1.

$$\left.\begin{aligned} \psi_1(x,\chi) = \int_2^x \psi(t,\chi)\, dt = T + O\left(x^2 e^{-\alpha \ln^{\frac{1}{10}} x}\right), \\ T = \begin{cases} \frac{1}{2}x^2, & \chi = \chi_0, \\ 0, & \chi \neq \chi_0, \end{cases} \end{aligned}\right\} \tag{36}$$

и $\psi(x,\chi) = \sum\limits_{n \leqslant x} \Lambda(n)\chi(n)$, а $\alpha > 0$ — постоянная.

Пусть $l \geqslant 1$ и $m \geqslant 1$ — целые числа, $(l, m) = 1$. Если $m = 1$, то и $l = 1$. Введем в рассмотрение функции

$$\psi(x;\ l, m) = \sum_{\substack{n \equiv l \pmod m \\ n \leqslant x}} \Lambda(n),\ \psi_1(x;\ l, m) = \int_2^x \psi(t;\ l, m)\, dt. \tag{37}$$

Тогда, пользуясь простейшими свойствами характеров, мы будем иметь соотношение

$$\sum_\chi \overline{\chi}(l)\,\psi(x,\chi) = \sum_{n \leqslant x} \Lambda(n) \sum_\chi \chi(n)\,\overline{\chi}(l) = \\ = \varphi(m) \sum_{\substack{n \equiv l \pmod m \\ n \leqslant x}} \Lambda(n) = \varphi(m)\,\psi(x;\ l, m),$$

откуда

$$\left.\begin{aligned}\psi(x;\, l,\, m) &= \frac{1}{\varphi(m)}\sum_{\chi}\overline{\chi}(l)\,\psi(x,\,\chi),\\ \psi_1(x;\, l,\, m) &= \frac{1}{\varphi(m)}\sum_{\chi}\overline{\chi}(l)\,\psi_1(x,\,\chi),\end{aligned}\right\} \tag{38}$$

где $\varphi(m)$ — функция Эйлера, $\overline{\chi}(l)$ — характер комплексно-сопряженный $\chi(l)$ и суммы берутся по всем характерам $\bmod m$. Пользуясь соотношениями (36), сразу получаем, что

$$\psi_1(x;\, l,\, m) = \frac{1}{\varphi(m)}\psi(x,\,\chi_0) + \sum_{\chi \neq \chi_0}\overline{\chi}(l)\,\psi(x,\,\chi) =$$

$$= \frac{x^2}{2\varphi(m)} + O\left(x^2 e^{-\alpha \ln^{\frac{1}{10}} x}\right). \tag{39}$$

Благодаря тому что функция $\psi(x;\, l,\, m)$ — неотрицательная монотонно неубывающая, можно легко перейти от оценки $\psi_1(x;\, l,\, m)$ к оценке $\psi(x;\, l,\, m)$. Для этого может служить общая лемма.

Лемма VIII. *Если $\psi(x)$ — неотрицательная монотонно неубывающая функция и имеет место соотношение*

$$\psi_1(x) = \int_2^x \psi(x)\,dx = ax^2 + O\left(x^2 e^{-\alpha \ln^{\gamma} x}\right), \tag{40}$$

$$a > 0,\ \alpha > 0,\ 1 \geqslant \gamma > 0,$$

то

$$\psi(x) = 2ax + O\left(xe^{-\frac{\alpha}{2}\ln^{\gamma} x}\right). \tag{41}$$

Доказательство. Пусть $1 > \theta \geqslant \frac{1}{2}$. Тогда из условия (40) имеем, что

$$\psi_1(x) - \psi_1(\theta x) = \int_{\theta x}^{x} \psi(t)\,dt = ax^2(1-\theta^2) + O\left(x^2 e^{-\alpha \ln^{\gamma} x}\right), \tag{42}$$

так как

$$\ln^{\gamma}\theta x = [\ln x + \ln\theta]^{\gamma} = \ln^{\gamma} x\left(1 + \frac{\ln\theta}{\ln x}\right)^{\gamma} = \ln^{\gamma} x + O(1).$$

Из этого соотношения следует, в силу положительности и монотонного неубывания $\psi(t)$, что

$$x(1-\theta)\,\psi(x) > ax^2(1-\theta^2) - A_0 x^2 e^{-\alpha \ln^{\gamma} x},$$

или, деля на $x(1-\theta)$, что

$$\psi(x) > 2ax - a(1-\theta)\,x - \frac{A_6}{1-\theta}\,xe^{-\alpha \ln^{\gamma} x}, \qquad (43)$$

где $A_6 > 0$ — постоянная.

Совершенно так же из соотношения (42), если в нем заменить x на $\frac{x}{\theta}$, следует, что

$$\int_{x}^{\frac{x}{\theta}} \psi(t)\,dt = \frac{a}{\theta^2}\,x^2(1-\theta^2) + O(x^2 e^{-\alpha \ln^{\gamma} x}),$$

откуда уже следует неравенство

$$\frac{1-\theta}{\theta}\,x\,\psi(x) < \frac{a}{\theta^2}(1-\theta^2)\,x^2 + O(x^2 e^{-\alpha \ln^{\gamma} x}).$$

Далее, деля на $\frac{1-\theta}{\theta}\,x$, получаем, что

$$\psi(x) < 2ax + a\frac{1-\theta}{\theta}\,x + A_7\frac{\theta x}{1-\theta}\,e^{-\alpha \ln^{\gamma} x}, \qquad (44)$$

где $A_7 > 0$ — постоянная. Из неравенств (43) и (44) уже следует, что

$$|\psi(x) - 2ax| < \frac{2a}{\theta}(1-\theta)\,x + \frac{A_6 + \theta A_7}{1-\theta}\,e^{-\alpha \ln^{\gamma} x}\,x.$$

Полагая теперь

$$\theta = 1 - e^{-\frac{\alpha}{2}\ln^{\gamma} x},$$

мы получаем, что

$$|\psi(x) - 2ax| < \left[\frac{2a}{\theta} + A_6 + \theta A_7\right] xe^{-\frac{\alpha}{2}\ln^{\gamma} x},$$

другими словами, получаем неравенство, эквивалентное соотношению (41). Из соотношения (39) и леммы VII непосредственно следует

Теорема II. *Если l и m — целые положительные числа и $m \geqslant 1$, $(m, l) = 1$, то*

$$\psi(x; l, m) = \sum_{\substack{n \equiv l \pmod m \\ n \leqslant x}} \Lambda(n) = \frac{1}{\varphi(m)}\,x + O(xe^{-\frac{\alpha}{2}\ln^{\frac{1}{10}} x}), \qquad (45)$$

где $\varphi(m)$ функция Эйлера, $\varphi(m)=1$, $m=1$, $\alpha>0$ постоянная.

Воспользовавшись теоремой II, можно получить оценку для числа простых чисел в прогрессии или в натуральном ряде.

Из соотношения

$$\sum_{\substack{2\\ n\equiv l \pmod m}}^{x}\frac{\Lambda(n)}{\ln n}=\sum_{\substack{p\leqslant x\\ p\equiv l \pmod m}}1+\sum_{\substack{p^2\leqslant x\\ p^2\equiv l \pmod m}}1+\ldots$$

$$\ldots+\sum_{\substack{p^{q_0}\leqslant x\\ p^{q_0}\equiv l \pmod m}}1,$$

где $q_0=\left[\frac{\ln x}{\ln 2}\right]$, так как

$$\sum_{q=2}^{q_0}\sum_{\substack{p^q\equiv l \pmod m\\ p^q\leqslant x}}1\leqslant\pi(x^{\frac{1}{2}})+\ldots+\pi(x^{\frac{1}{q_0}})<2x^{\frac{1}{2}}\ln x,$$

где $\pi(x)$ число простых чисел, меньших x, следует, что

$$\pi(x;\,l,\,m)=\sum_{\substack{p\equiv l \pmod m\\ p\leqslant x}}1=\sum_{\substack{2\\ n\equiv l \pmod m}}^{x}\frac{\Lambda(n)}{\ln(n)}+O(x^{\frac{1}{2}}\ln x). \quad (46)$$

Далее, полагая $N=[x]$, будем иметь, что

$$\sum_{\substack{2\leqslant n\leqslant x\\ n\equiv l \pmod m}}\frac{\Lambda(n)}{n}=\sum_{2\leqslant n\leqslant x}\frac{1}{\ln n}[\psi(n;\,l,\,m)-\psi(n-1;\,l,\,m)]=$$

$$=\frac{\psi(N;\,l,\,m)}{\ln N}+\sum_{n=2}^{N-1}\psi(n;\,l,\,m)\left[\frac{1}{\ln n}-\frac{1}{\ln(n+1)}\right]=$$

$$=\frac{1}{\varphi(m)}\left[\frac{N}{\ln N}+\sum_{1}^{N-1}n\left[\frac{1}{\ln n}-\frac{1}{\ln(n+1)}\right]+O(xe^{-\frac{\alpha}{2}\ln^{\frac{1}{10}}x})+\right.$$

$$\left.+O\left\{\sum_{2}^{N}n\left(\frac{1}{\ln n}-\frac{1}{\ln(n+1)}\right)e^{-\frac{\alpha}{2}\ln^{\frac{1}{10}}n}\right\}\right]=$$

$$=\frac{1}{\varphi(m)}\sum_{2}^{N}\frac{1}{\ln n}+O(xe^{-\frac{\alpha}{2}\ln^{\frac{1}{10}}x})+O\left[\sum_{2}^{N}\frac{1}{\ln^2 n}e^{-\frac{\alpha}{2}\ln^{\frac{1}{10}}n}\right].$$

Легко видеть, что имеют место оценки

$$\frac{1}{\ln 2}+\int_2^N \frac{dx}{\ln x} > \sum_2^N \frac{1}{\ln n} > \int_2^{N-1} \frac{dx}{\ln x},$$

откуда

$$\sum_{2 \leqslant n \leqslant x} \frac{1}{\ln n} = \int_2^x \frac{dt}{\ln t} + O(1)$$

и при

$$q = Ne^{-\frac{\alpha}{2} \ln^{\frac{1}{10}} N}, \quad N = [t],$$

$$\sum_2^N \frac{1}{\ln^2 n} e^{-\frac{\alpha}{2} \ln^{\frac{1}{10}} n} = \sum_2^q \frac{1}{\ln^2 n} e^{-\frac{\alpha}{2} \ln^{\frac{1}{10}} n} +$$

$$+ \sum_{q+1}^N \frac{1}{\ln^2 n} e^{-\frac{\alpha}{2} \ln^{\frac{1}{10}} n} < \frac{1}{2} Ne^{-\frac{\alpha}{2} \ln^{\frac{1}{10}} N} +$$

$$+ e^{-\frac{\alpha}{2} \ln^{\frac{1}{10}} q} \frac{N}{\ln^2 q} \leqslant Ne^{-\frac{\alpha}{2} \ln^{\frac{1}{10}} N} < xe^{-\frac{\alpha}{2} \ln^{\frac{1}{10}} x}, \quad x > x_0,$$

так как

$$\ln^{\frac{1}{10}} q = \left[\ln N - \frac{\alpha}{2} \ln^{\frac{1}{10}} N\right]^{\frac{1}{10}} = \ln^{\frac{1}{10}} N \left[1 - \frac{\alpha}{2} \ln^{-\frac{9}{10}} N\right]^{\frac{1}{10}} =$$

$$= \ln^{\frac{1}{10}} N + O(1).$$

Отсюда следует, что

$$\sum_{2 \leqslant n < x} \frac{\Lambda(n)}{\ln n} = \int_2^x \frac{dt}{\ln t} + O\left(xe^{-\frac{\alpha}{2} \ln^{\frac{1}{10}} x}\right). \qquad (47)$$

Теорема III. *Если* $\pi(x;\ l,\ m)$ — *число простых чисел* $p \leqslant x$ *и* $p \equiv l \pmod m$, $(l,\ m) = 1$, $m \geqslant l$, *то*

$$\pi(x;\ l,\ m) = \int_2^x \frac{dt}{\ln t} + O\left(xe^{-\frac{\alpha}{2}\ln^{\frac{1}{10}} x}\right), \tag{48}$$

где α — некоторая постоянная.

Эта теорема непосредственно следует из соотношений (46) и (47).

Мы доказали, таким образом, теорему о числе простых чисел в натуральном ряде и арифметической прогрессии с остаточным членом типа Адамара — Валле-Пуссена, в котором получили аналогичную оценку с заменой γ на $\frac{1}{10}$.

ЛИТЕРАТУРА

1. A. Brauer, On the Exact Number of Primes below a given Limit, Amer. math. Month. **53**, 521—523 (1946).
2. R. Breusch, Zur Verallgemeinerung des Bertrandschen Postulates, das zwischen x und $2x$ stets Primzahlen liegen, Math. Z. **34**, 505—526 (1931).
3. V. Brun, Le crible d'Eratosthène et le théorème de Goldbach, Videnskapselskapets Scrifter 1, Nr. 3 (1920). См. также Untersuchungen über das Siebverfahren des Eratosthenes. Jber. DMV **33**, 81—96 (1924).
4. P. A. Clement, Congruences for Sets of Primes, Amer. math Month. **56**, 23—25 (1949).
5. L. E. Dickson, History of the Theory of Numbers (Carnegie Institution, Washington, 1919).
6. P. Erdös, On a New Method in Elementary Number Theory which leads to an Elementary Proof of the Prime Number Theorem, Proc. nat. Acad. Sci. USA **35**, 374—384 (1949).
7. P. Erdös, Some Applications of Brun's Method, Acta sci. math. Szeged **13**, 57—63 (1949).
8. P. Finsler, Über die Primzahlen zwischen n und $2n$, Speiser-Festschrift (Orell-Füssli, Zürich, 1945).
9. A. E. Ingham, The Distribution of Prime Numbers (Cambridge University Press, London, 1932). (Есть русский перевод: Ингам А. Е., Распределение простых чисел. Перев. с англ. Д. А. Райкова с приложением статьи переводчика «О методе Ландау — Икеара доказательства асимптотического закона распределения простых чисел», 1936, ОНТИ).
10. K. Iseki und T. Tatuzawa, On Selberg's Elementary Proof of the Prime Number Theorem, Proc. Japan. Acad. **27**, 340—342 (1951).
11. H. Ishikawa, Über die Verteilung der Primzahlen, Sci. Rep. Tokyo Bunrika Daigaku [A] **2**, 27—40 (1934).

12. E. Landau, Handbuch der Lehre von der Verteilung der Primzahlen (B. G. Teubner, Leipzig, 1909).
13. D. H. Lehmer, Guide to Tables in the Theory of Numbres (National Research Council. nat. Acad. Sci. Washington, 1941).
14. D. H. Lehmer, A. Factorization Theorem applied to a Test for Primality, Bull. Amer. math. Soc. **45**, 132—137 (1939).
15. D. H. Lehmer, On Lucas's Test for the Primality of Mersenne's Numbers, J. London math. Soc. **10**, 162—165 (1935).
16. P. Maennchen, Zerlegung grosser Zahlen, Unterrichtsbl. Math. Naturwiss. **44**, 84—92, 112—122 (1938).
17. T. Nagell, Introduction to Number Theory (Almquist & Wiksell, Stockholm, 1951).
18. O. Ore, Number Theory and its History (McGraw-Hill, New York, 1948).
19. H. E. Richert, Über Zerfällungen in ungleiche Primzahlen, Math. Z. **52**, 342—343 (1941).
20. B. Rosser, The n-th Prime is greater than $n \log n$, Proc. London. math. Soc. **45**, 21—44 (1938).
21. B. Rosser, Explicit Bounds for some Functions of Prime Numbers, Amer. J. Math. **63**, 211—232 (1941).
22. A. Selberg, An Elementary Proof of the Prime Number Theorem, Ann. Math. **50**, 305—313 (1949).
23. A. Selberg, On an Elementary Method in the Theory of Primes, Norske Videnskab. Selskab. Forh. **19**, Nr 18 (1947).
24. A. Selberg, The general sieve Method and its Place in Prime Number Theory, Proc. int. Congr. Math. Cambridge, Mass. 1, 286—292 (1950).
25. H. N. Shapiro, On Primes in Arithmetic Progressions, II, Ann. Math. **52**, 231—243 (1950).
26. H, N. Shapiro. On the Number of Primes less than or equal x, Proc. Amer. math. Soc. 1, 346—348 (1950).
27. W. Sierpinski, Sur l'existence de nombres premiers avec une suite arbitraire de chiffres initiaux, Le Matematiche (Catania, 1951).
28. R. Steuerwald, Über die Kongruenz $2^{n-1} \equiv 1 \pmod{n}$, Sitz-Ber. math. Naturw. Kl. Bayer. Akad. Wiss., München, 1947, 177.
29. H. S. Uhler, A. Brief History of the Investigations on Mersenne Numbers and the Latest Immense Primes, Scripta math. **18**, 122—131 (1952).
30. J. Warga und H. N. Shapiro, On the Representations of Large Integers as Sums of Primes, Comm. pure appl. Math. **3**, 153—176 (1950).

31. E. M. Wright, A Prime-representig Function, Amer. math. Month. **58**, 616—618 (1951).
32. E. Zermelo, Elementare Betrachtungen zur Theorie der Primzahlen, Nachr. Ges. Wiss. Göttingen [NF] Nachr. Math. **1**, 43—46 (1934).
33. А. А. Бухштаб, Асимптотическая оценка одной общей теоретико-числовой функции, Матем. сб. 2 (44) (1937), 1239—1246.
34. А. А. Бухштаб, Новые улучшения в методе эратосфенова решета, Матем. сб. **4** (46) (1938), 375—387.
35. А. А. Бухштаб, О разложении четных чисел на сумму двух слагаемых с ограниченным числом простых множителей, ДАН **29** (1940), 544—548.
36. А. А. Бухштаб, Об одном аддитивном представлении целых чисел, Матем. сб. **10** (52) (1942), 87—91.
37. А. А. Бухштаб, Об одном соотношении для функции $\pi(x)$, выражающей число простых чисел, не превосходящих x, Матем. сб. **12** (54) (1943), 152—160.
38. А. О. Гельфонд, Об одном элементарном подходе к некоторым задачам из области распределения простых чисел, Вестник МГУ, № 2, 21—26 (1953).
39. А. О. Гельфонд, О разбиении натурального ряда на классы группой линейных подстановок, ИАН, сер. мат., т. 18, 297—306 (1954).
40. А. О. Гельфонд, Об арифметическом эквиваленте аналитичности L-ряда Дирихле на прямой $\mathrm{Re}\, s = 1$, ИАН, сер. мат., № 20, 145—166 (1956).
41. Ю. В. Линник Большое решето, ДАН **30** (1941), 290—292.
42. А. Г. Постников и Н. П. Романов, Упрощение элементарного доказательства А. Сельберга асимптотического закона распределения простых чисел, Успехи матем. наук **X**, 4 (66), 75—87 (1955).
43. Н. П. Романов, О некоторых теоремах аддитивной теории чисел, Успехи матем. наук **7** (1940), 47—56.
44. В. А. Тартаковский, О некоторых суммах типа Viggo Brunn'a, ДАН 23 (1939), 122—126.
45. В. А. Тартаковский, Метод избирательного приближенного решета, ДАН **23** (1939), 127—130.
46. А. Я. Хинчин, О сложении последовательностей натуральных чисел, Матем. сб. **6** (48) (1939), 161—166.
47. И. В. Чулановский, Некоторые оценки, связанные с новым методом Selberg'a в элементарной теории чисел, ДАН 63 (1948), 491—494.

48. Л. Г. Шнирельман, Об аддитивных свойствах чисел, Ростов н/Д, Изв. Донск. политехн. инст. **14** (2—3) (1930), 3—28.
49. Л. Г. Шнирельман, Uber additive Eigenschaften von Zahlen, Math. Ann. **107** (1933), 649—690.
50. Л. Г. Шнирельман, On addition of sequences and sets., Матем. сб. **5** (47) (1939), 211—215.
51. Л. Г. Шнирельман, Простые числа, М.—Л., Гостехиздат, 1940, 1—59.
52. Л. Г. Шнирельман, О сложении последовательностей, Успехи матем. наук **7** (1940), 62—63.

ЛИТЕРАТУРА К ПРИЛОЖЕНИЮ

1. Н. Г. Чудаков, On zeros of Dirichlet's L-functions, Матем. сборн. **1** (43):4 (1936), 591—602;
2. Н. М. Коробов, О нулях функции $\zeta(s)$, ДАН СССР **118**, № 3 (1958), 431—434.
3. И. М. Виноградов, Новая оценка функции $\zeta(1+it)$, Изв, АН СССР, сер. матем., № 2, т. 22 (1958), 161—164;
4. Н. М. Коробов, Оценки тригонометрических сумм и их приложения, Успехи мат. наук **XIII**, вып. 4 (82) (1958).

Трост Эрнст

Простые числа

Редактор *А. А. Конопляникин*

Техн. редактор *В. Н. Крючкова*

Корректор *А. С. Каган*

Сдано в набор 29/X 1958 г. Подписано к печати 31/XII 1958 г. Формат 84×108 $_{32}$. Физ. печ. л. 4,25. Условн. печ. л. 6,97. Уч.-изд. л. 7,10. Тираж 15000 экз. Т11577. Цена 2 р. 15 к. Заказ 2408.

Государственное издательство физико-математической литературы

Москва, В-71, Ленинский проспект, 15.

Первая Образцовая типография имени А. А. Жданова Московского городского Совнархоза.

Москва, Ж-54, Валовая, 28.

Цена 2 р. 15 к.