В. Н. Чубариков

ВВЕДЕНИЕ В ТЕОРИЮ ЧИСЕЛ

Москва
2024

УДК 511

Чубариков В. Н.

Введение в теорию чисел. — М.:ООО "УРСС", 2024. — 270 с.

Книга является элементарным введением в современные проблемы высшей арифметики. Она написана на основе лекций, прочитанных автором школьникам и студентам младших курсов в МГУ им. М. В. Ломоновова и специализированной физико-математической школе-интернате № 18 при МГУ, начиная с 1976 г. Добавлены некоторые неэлементарные понятия и факты, которые могут способствовать более глубокому пониманию рассматриваемых вопросов. Они содержатся во второй части книги, являющейся сборником задач.

Для всех интересующихся математикой, включая математиков-профессионалов, преподавателей и учащихся старших классов.

УДК 511

Предисловие

Настоящая книга посвящена, в основном, *изучению свойств натуральных чисел* $1, 2, 3, \ldots$, что составляет *предмет арифметики.* Свойство делимости одного числа на другое является сердцевиной арифметики. Задачи, связанные с делимостью, выделяют в отдельный предмет — мультипликативную теорию чисел. Первые три главы этой книги посвящены изучению основных свойств простых чисел, которые играют в ней ключевую роль. С понятием делимости тесным образом связана теория сравнений по модулю натурального числа. Этой теории и ее приложению к криптографии посвящена четвертая глава.

Со школьных лет мы привыкли к решению алгебраических уравнений. Теорию сравнений также нельзя осмыслить без изучения многочленов. Поэтому отдельная пятая глава описывает основные свойства многочленов.

Числовой континуум, отождествляемый с числовой прямой, не исчерпывается только корнями многочленов с целыми коэффициентами, поэтому возникает необходимость рассматривать трансцендентные числа. Последняя глава посвящена современной теореме Апери об иррациональности значения дзета-функции Римана в точке 3.

В заключение отметим, что эта книга написана на основе лекций, прочитанных автором школьникам и студентам младших курсов в МГУ им. М. В. Ломоновова и специализированной физико-математической школе-интернате № 18 при МГУ, начиная с 1976 г. Необходимо подчеркнуть, что при написании книги были добавлены некоторые неэлементарные понятия и факты, которые, по нашему мнению, могут способствовать более глубокому пониманию рассматриваемых вопросов. Вторую часть книги составляет сборник задач.

Автор благодарит слушателей специальных курсов и участников специальных семинаров по теории чисел за большую помощь при подготовке этой книги к печати.

26.06.2024 г.

Автор

Глава I

ЭЛЕМЕНТАРНЫЕ СВОЙСТВА ЦЕЛЫХ ЧИСЕЛ

На множестве натуральных чисел $1, 2, 3, \ldots$ задаются известные *арифметические операции*: сложение $\{+\}$, умножение $\{\times\}$, а также вычитание $\{-\}$ и деление $\{:\}$. Последние две операции могут быть выполнены во множестве натуральных чисел, если их результатом являются натуральные числа. Кроме того, любые два числа можно *сравнить между собой по величине*, т. е. установить одно из отношений меньше, равно, больше $\{<,\ =,\ >\}$. Можно расширить совокупность натуральных чисел до множества *целых чисел* $\mathbb{Z}$: добавить 0 и отрицательные целые числа $-1, -2, -3, \ldots$. Тогда множество целых чисел будет *замкнуто* еще и относительно операции вычитания, т. е. для любых чисел a и b, принадлежащих $\mathbb{Z}$, их разность $a - b$ также является целым числом.

§ 1. Метод математической индукции

Дальнейшее построение арифметики основано на следующих двух принципах.

a.

Принцип существования наименьшего элемента. В любом непустом подмножестве множества натуральных чисел существует наименьшее число.

Убедимся в том, что этот принцип действительно имеет место. Для этого возьмем какой-нибудь элемент такого подмножества (это можно сделать, так как оно не пусто). Если окажется, что выбранный элемент минимален, то свойство доказано. В противном случае множество натуральных чисел, меньших данного числа, конечно. Рассматривая их последовательно, мы найдем требуемый минимальный элемент.

Принцип существования наименьшего элемента мы будем использовать для обоснования метода (принципа) полной математической индукции.

b.

Метод математической индукции. Для доказательства лю-

бого утверждения, высказанного для всех натуральных чисел $n \geqslant 1$, достаточно ограничиться проверкой справедливости следующих трех высказываний:

1) доказать это утверждение для $n = 1$ (база индукции);

2) предположить его справедливость при $n = k$ и $k \geqslant 1$ (предположение индукции);

3) доказать, что оно верно при $n = k + 1$ (шаг индукции).

Действительно, отсюда следует, что высказанное утверждение верно для всех натуральных чисел n. Допустим противное. Тогда множество тех n, для которых утверждение неверно, содержит наименьший элемент m. Число $m \neq 1$, поскольку утверждение верно для $n = 1$. Число m не может быть больше 1, так как утверждение в этом случае было бы верно для $m - 1$, и в силу условия 3) оно было бы справедливо и для m, что противоречит выбору числа m.

Замечание. Методом математической индукции можно доказывать утверждения, справедливые и при $n \geqslant k$, где $k \geqslant 1$. В ходе доказательства надо изменить только базу индукции — доказать утверждение при $n = k$, — а все остальное оставить, как прежде, при необходимости пользуясь тем, что $n \geqslant k$.

с. Докажем, например, методом математической индукции формулу бинома Ньютона. Сначала определим величину

$$n! = n(n-1)\dots 2 \cdot 1, \quad 0! = 1$$

($n!$ читается: эн-факториал). В частности, имеем

$$0! = 1, \quad 1! = 1, \quad 2! = 2 \cdot 1 = 2, \quad 3! = 3 \cdot 2 \cdot 1 = 6 \quad \text{и т. д.}$$

Теорема 1. *Имеет место равенство* (*формула бинома Ньютона*)

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \dots + \binom{n}{k}x^k + \dots + \binom{n}{n}x^n.$$

(Коротко эту формулу можно записать так:

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k,$$

где $\binom{n}{k} = C_n^k = \dfrac{n!}{k!(n-k)!}$ *— биномиальный коэффициент.)*

► *1. При $n = 1$ формула верна:* $(1+x)^1 = \binom{1}{0} + \binom{1}{1}x$, *поскольку*

$$\binom{1}{0} = \binom{1}{1} = 1.$$

2. Пусть формула бинома Ньютона справедлива при $n = t$, $t \geqslant 1$.

3. Докажем, что она верна при $n = t+1$. Сначала докажем вспомогательное утверждение о биномиальном коэффициенте: при $0 \leqslant k \leqslant n-1$ имеем

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

Действительно,

$$\frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} =$$

$$= \frac{n!}{k!(n-k-1)!}\left(\frac{1}{n-k} + \frac{1}{k+1}\right) = \binom{n+1}{k+1}.$$

Далее имеем

$$(1+x)^{t+1} = (1+x)^t(1+x) =$$

$$= \binom{t}{0} + \binom{t}{1}x + \ldots + \binom{t}{t}x^t + \binom{t}{0}x + \ldots + \binom{t}{t-1}x^t + \binom{t}{t}x^{t+1} =$$

$$= \binom{t+1}{0} + \binom{t+1}{1}x + \ldots + \binom{t+1}{t}x^t + \binom{t+1}{t+1}x^{t+1}. \blacktriangleleft$$

d.

Замечание. *Подобным образом доказывается и формула для* полинома Ньютона *от s неизвестных вида*

$$(x + y + \ldots + z)^n = \sum_{k_1+\ldots+k_s=n} \frac{n!}{k_1! \ldots k_s!} x^{k_1} y^{k_2} \ldots z^{k_s},$$

где $k_1, \ldots, k_s$ — целые неотрицательные числа.

e. *Докажем теперь* неравенство Бернулли.

Теорема 2. *При $x > -1$, $x \neq 0$ и при целом $n \geqslant 2$ справедливо неравенство*

$$(1+x)^n > 1 + xn.$$

► *Доказательство проведем по индукции. Сначала убедимся, что при* $n = 2$ *неравенство верно. Действительно,*

$$(1 + x)^2 = 1 + 2x + x^2 > 1 + 2x.$$

Предположим, что для номера $n = k \geqslant 2$ *оказалось, что утверждение справедливо:*

$$(1 + x)^k > 1 + kx.$$

Докажем его при $n = k + 1$. *Имеем*

$$(1 + x)^{k+1} = (1 + x)^k(1 + x) > (1 + kx)(1 + x) =$$

$$= 1 + (k + 1)x + kx^2 > 1 + (k + 1)x. \text{ ◄}$$

§ 2. Задачи

1. *Доказать, что*

а) $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$; *б)* $1 + 3 + \ldots + (2n - 1) = n^2$;

в) $1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$; *г)* $1^3 + 2^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$.

2. *Найти сумму*

а) $1^2 + 3^2 + 5^2 + \ldots + (2n - 1)^2$; *б)* $1^3 + 3^3 + 5^3 + \ldots + (2n - 1)^3$.

3. *Найти формулу для* n^2, *если*

$1^2 = 0 + 1$, $2^2 = 1 + 3$, $3^2 = 3 + 6$, $4^2 = 6 + 10$ *и т. д.*

4. *Найти формулу для* n^3, *если*

$1^3 = 1$, $2^3 = 3+5$, $3^3 = 7+9+11$, $4^3 = 13+15+17+19$ *и т. д.*

5. *Доказать, что произведение четырех последовательных целых чисел, увеличенное на единицу, является точным квадратом.*

§ 3. Делимость

Натуральное (целое, отличное от нуля) число b *называется* делителем *натурального (целого) числа* a, *если существует такое натуральное (целое) число* c, *что* $a = bc$. *При этом число* c *называется* частным *от деления числа* a *на число* b. *Обозначение:* $b \mid a$ *(читается:* b *делитель* a*) или* $a \vdots b$ *(читается:* b *делится на* a*).*

Справедливы следующие свойства делителей.

$\mathbf{1}^0$. $\forall a \in \mathbb{N} \quad 1 \mid a,\ a \mid a$;
$\mathbf{2}^0$. $\forall a \in \mathbb{N} \quad a \mid 0$;
$\mathbf{3}^0$. $a \mid b,\ b \mid a \ \to a = b$;
$\mathbf{4}^0$. $a \mid b,\ b \mid c \ \to a \mid c$;
$\mathbf{5}^0$. $a \mid b \ \to \forall c \quad ca \mid cb$;
$\mathbf{6}^0$. $\forall c \neq 0 \quad ca \mid cb \ \to a \mid b$;
$\mathbf{7}^0$. $a_1 \mid b_1,\ a_2 \mid b_2 \ \to a_1 a_2 \mid b_1 b_2$;
$\mathbf{8}^0$. $a \mid b_1,\ a \mid b_2 \ \to a \mid b_1 \pm b_2$.

Число b назовем собственным *делителем числа a, если $b \mid a$ и $1 < |b| < |a|$; числа ± 1 и $\pm a$ называются* тривиальными *делителями числа a.*

§ 4. Задачи

1. *Доказать, что для любого натурального числа n выражения*

$$n(n+1)(2n+1), \quad n^3 - n, \quad n^3 + 17n$$

делятся на 6.

2. *Доказать, что для любого нечетного числа n выражение $n(n^2-1)$ делится на* 24.

3. *Доказать, что для любого натурального n количество всех делителей числа $2^n - 1$ не меньше, чем количество всех делителей числа n.*

4. *Число делителей натурального n нечетно тогда и только тогда, когда n — точный квадрат.*

5. *Доказать, что ни при каком целом n выражение $n^2 + 3n + 5$ не делится на* 121.

6. *Сумма квадратов двух нечетных чисел не может быть равна квадрату целого числа.*

7. *Куб любого целого числа представляется в виде разности квадратов двух целых чисел.*

§ 5. Простые и составные числа

а. *Натуральное число p, большее единицы, называется* простым числом, *если все его делители исчерпываются числами* 1 *и p. Все остальные натуральные числа называются* составными.

Лемма 1. *Каждое натуральное число a, большее единицы, обладает по крайней мере одним простым делителем, в частности, наименьший делитель p, больший* 1, *числа a будет простым числом.*

► *Пусть D — множество делителей числа a, больших 1. Оно не пусто, поскольку $a \in D$. Обозначим через p наименьший элемент множества D (по принципу существования минимального элемента такой элемент имеется). Пусть p — не простое число. Тогда найдется такое число q, что $q \mid p$, $1 < q < p$. Следовательно, по свойству 4^0 из условий $q \mid p$, $p \mid a$ вытекает $q \mid a$. Это противоречит тому, что число p — минимальный делитель числа a. Значит, предположение о том, что p — составное число, неверно.* ◄

b.

Лемма 2. *Наименьший отличный от единицы делитель составного числа a не превосходит $\sqrt{a}$.*

► По лемме **??** наименьший отличный от единицы делитель p числа a будет простым числом. Тогда $a = pb \geqslant p^2$. ◄

c.

Лемма 3. *Существует бесконечно много простых чисел.*

► *Предположим, что множество всех простых чисел исчерпываются числами $p_1, \ldots, p_n$. Число $N = p_1 \ldots p_n + 1$ не содержит среди своих делителей чисел $p_1, \ldots, p_n$. Пусть p — наименьший делитель N, больший единицы. Тогда по лемме **??** получим, что p — простое число, но оно отлично от $p_1, \ldots, p_n$. Это противоречит предположению, что все простые исчерпываются числами $p_1, \ldots, p_n$. Следовательно, оно ложно, и простые числа образуют бесконечное множество.* ◄

Если p^k — наивысшая степень простого числа p, делящая n, то пишут $p^k \parallel n$. Например, $2^3 \parallel 24$.

§ 6. Задачи

Доказать следующие утверждения.

1. *Существует бесконечно много простых чисел вида $4n+3$, $6m+5$ и $2k+3l+5$, где $m, n, k, l \in \mathbb{N}$.*

2. *Пусть p_n — n-тое простое число. Тогда для любого $n \geqslant 1$ справедливо неравенство $p_n \leqslant 2^{2^{n-1}}$.*

3. *Нечетное простое число единственным способом представляется в виде разности квадратов натуральных чисел.*

4. *Числа $2^{4n+2} + 1$, $a^4 + 4$ и $4a^4 + 1$ являются составными.*

5. *Число $2^{2^5} + 1$ делится на $641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$.*

6. *Число* $2^{2^6}+1$ *делится на* 274177.

7. *а)* $2^{994} \parallel 1000!$*; б)* $2^{1893} \parallel 1900!$*; в)* $7^{1665} \parallel 10000!$*; г)* $10^{249} \parallel 1000!$.

8. *Пусть* $f(n)$ *— многочлен с целыми коэффициентами, отличный от константы. Тогда абсолютные величины его значений будут составными для бесконечного множества натуральных значений* n.

Указание. *Пусть натуральное число* a *таково, что* $A = |f(a)| > 1$. *Тогда* $A \mid |f(An+a)|$ *для любого натурального числа* n.

d. *Отметим еще один факт, относящийся к расположению простых чисел в натуральном ряде чисел. Для любого натурального* n *существует промежуток длины* n*, не содержащий простых чисел:* $(n+1)!+2, \ldots, (n+1)!+n+1$.

Заметим, что в зависимости от величины $N=(n+1)!+n+1$ *верхней границы рассматриваемого промежутка, число* n имеет порядок $\frac{\ln N}{\ln\ln N}$, *т. е. отношение* n *к* $\frac{\ln N}{\ln\ln N}$ *ограничено сверху и снизу положительными постоянными при* $n \to \infty$.

Пусть $p_r \leqslant n < p_{r+1}$. *Положим* $P = p_1 \ldots p_r$. *Тогда числа* $P+2, \ldots, P+n$ *будут составными. Положим* $N = P+n$. *Тогда из неравенств П. Л. Чебышёва (см. теорему* **??** *на с.* **??***, а также [?], [?], [?]) для количества простых чисел, не превосходящих любой заданной границы, следует, что величина* n *имеет порядок* $\ln N$.

В 1938 г. Р. А. Ранкиным получена наилучшая на сегодняшний день оценка величины n*:*

$$n \geqslant c \ln N \frac{\ln\ln N}{(\ln\ln\ln N)^2} \ln\ln\ln\ln N,$$

где $c > 0$ *— некоторая постоянная (см. [?], [?], [?]).*

§ 7. Основная теорема арифметики

a.

Теорема 2 (Основная теорема арифметики)**.** *Любое число* a *имеет представление* $a = p_1 \ldots p_n$ *в виде произведения* $n \geqslant 0$ *простых чисел* $p_1 \leqslant \ldots \leqslant p_n$*, причем такое представление единственно.*

► *а).* Существование. *При* $a = 1$ *имеем* $n = 0$ *и утверждение, очевидно, верно (пустое произведение равно 1). Пусть утверждение справедливо при* $a < m$, $m \geqslant 1$. *Докажем его справедливость при* $a = m$. *По лемме* **??** *наименьший делитель* p *числа* m *будет простым и имеет место представление* $m = pb$, $1 \leqslant b < m$. *Так*

как $b < m$, по предположению индукции получим $b = p_1 \dots p_k$, где $p_1 \leqslant \dots \leqslant p_k$ — простые числа. Значит, $m = pp_1 \dots p_k$.

б). Единственность. *Вновь будем использовать метод математической индукции. При $a = 1$ утверждение верно. Предположим, что оно верно при $a < m$. Докажем его справедливость при $a = m$, $m > 1$. По лемме* **??**, *как и в случае а), имеем $m = pb = pp_1 \dots p_k$. Пусть существует другое разложение числа m на простые сомножители: $m = qq_1 \dots q_l$, $q \leqslant q_1 \leqslant \dots q_l$.*

Возможны два случая: 1) $p = q$; 2) $p \neq q$.

Если $p = q$, то $b = p_1 \dots p_k = q_1 \dots q_l$. По предположению индукции разложение на простые сомножители числа $b < m$ единственно, поэтому $k = l$ и $p_1 = q_1, \dots, p_k = q_l$.

Пусть $p \neq q$. Тогда $p < q$, поскольку p — наименьший делитель числа m. Следовательно, $m = qc > pc$, $m = pb > pc$. Рассмотрим число $m_1 = m - pc = (q - p)c = p(b - c)$. Числа m_1 и $c = q_1 \dots q_l$ имеют единственные разложения в произведение простых, причем $p < q \leqslant q_1 \dots \leqslant q_l$, в частности, p не совпадает ни с одним из чисел $q_1, \dots, q_l$. Следовательно, в силу однозначности разложения на простые сомножители числа m_1 получим, что $p \mid q - p$. Далее, поскольку $(q - p) + p = q$, имеем $p \mid q$, следовательно, $p = q$. Противоречие. Случай 2) невозможен. ◀

b. *Объединяя равные простые числа, входящие в разложение натурального числа, в степень, получим следующую переформулировку основной теоремы арифметики.*

Теорема 3. *Любое натуральное число a имеет одно и только одно представление $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ в виде произведения некоторого количества $n \geqslant 0$ различных простых чисел $p_1 < \dots < p_n$ с натуральными показателями $\alpha_1, \dots, \alpha_n$.*

Это представление числа называется каноническим разложением *его на простые множители.*

§ 8. Задачи

Доказать следующие утверждения.

1. *Пусть k — четное число, $k > 0$, каноническое разложение числа a имеет вид $a = p_1 \dots p_k$ и d пробегает делители a с условием $0 < d < \sqrt{a}$. Тогда количество таких чисел d с четным числом простых делителей равно количеству таких чисел d с нечетным числом простых делителей.*

2. *Пусть $k \geqslant 2$ и $k \mid a - 1$, $k \mid b - 1$, $k \mid c - 1$. Тогда $k \mid abc - 1$.*

3. *Пусть a и b — натуральные числа. Тогда число $\frac{(a+b)!}{a!b!}$ также натуральное.*

§ 9. Наибольший общий делитель

a. *Число f, делящее a и b одновременно, называется* общим делителем *этих чисел. Наибольший среди общих делителей называется* наибольшим общим делителем d *чисел a и b. Если $a = p_1^{\alpha_1} \dots p_s^{\alpha_s}$, $b = p_1^{\beta_1} \dots p_s^{\beta_s}$ с неотрицательными $\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_s$, то по основной теореме арифметики $d = p_1^{\gamma_1} \dots p_s^{\gamma_s}$, где $\gamma_r = \min(\alpha_r, \beta_r)$, $r = 1, \dots, s$. Обозначение: $d = (a, b)$. В случае, когда $(a, b) = 1$, говорят, что числа a и b* взаимно просты.

b.

Теорема 4 (критерий наибольшего общего делителя)**.** *Для того чтобы число d было наибольшим общим делителем двух натуральных чисел a и b необходимо и достаточно, чтобы*

а) $d \mid a$, $d \mid b$; б) *если* $f \mid a$, $f \mid b$, *то* $f \mid d$.

► Необходимость. *Очевидно, что наибольший общий делитель двух чисел удовлетворяет условиям а) и б) утверждения критерия.*

Достаточность. *Пусть кроме d условиям а) и б) удовлетворяет число c. Тогда из условия, что d удовлетворяет а) и б) при $f = c$, получим, что $c \mid d$. Аналогично, из условия, что c удовлетворяет а) и б), при $f = d$ получим, что $d \mid c$. Следовательно, $d = c$.* ◄

c. *Отсюда, в частности, имеем, что множество всех общих делителей чисел a и b совпадает с множеством всех делителей $\{f\}$ их наибольшего общего делителя d.*

§ 10. Задачи

1. *Пусть $m \neq 0$, $a^2 + b^2 \neq 0$. Тогда $(ma, mb) = m(a, b)$.*

2. *Пусть $F_n = 2^{2^n} + 1$, $n = 0, 1, 2, \dots$, — числа Ферма. Доказать, что для $k > 0$ имеем $F_n \mid (F_{n+k} - 2)$. Вывести отсюда, что для любых $s \neq t$ имеем $(F_s, F_t) = 1$, а также доказать бесконечность количества простых чисел в натуральном ряду.*

3. *Пусть $\{f_n\}$* — последовательность Фибоначчи, *т. е. $f_1 = 1$, $f_2 = 1, f_3 = 2, f_4 = 3, f_5 = 5, \dots$, где $f_{n+1} = f_n + f_{n-1}$ при $n \geqslant 2$. Доказать, что $(f_n, f_{n+1}) = 1 \ \forall\, n \in \mathbb{N}$.*

4. *Найти все целые n, при которых дробь $\frac{5n+6}{7n+11}$ будет несократима.*

§ 11. Наименьшее общее кратное

a. *Это понятие аналогично понятию наибольшего общего делителя. Число q, делящееся на a и b одновременно, называется* общим кратным *этих чисел. Наименьшее среди общих кратных называется* наименьшим общим кратным l *чисел a и b. Если $a = p_1^{\alpha_1} \dots p_s^{\alpha_s}$, $b = p_1^{\beta_1} \dots p_s^{\beta_s}$ с неотрицательными $\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_s$, то по основной теореме арифметики $l = p_1^{\delta_1} \dots p_s^{\delta_s}$, где $\delta_r = \max(\alpha_r, \beta_r)$, $r = 1, \dots, s$. Обозначение: $l = \{a, b\}$.*

b.

Теорема 5 (критерий наименьшего общего кратного)**.** *Для того чтобы число l было наименьшим общим кратным двух натуральных чисел a и b необходимо и достаточно, чтобы* а) *$a \mid l$, $b \mid l$;* б) *если $a \mid q$, $b \mid q$, то $l \mid q$.*

► Необходимость *очевидна, так как наименьшее общее кратное двух чисел удовлетворяет условиям а) и б) утверждения критерия.*

Достаточность. *Пусть кроме l условиям а) и б) удовлетворяет число m. Тогда из условия, что l удовлетворяет а) и б) при $q = m$ получим, что $l \mid m$. Аналогично из условия, что d удовлетворяет а) и б) при $q = l$ получим, что $m \mid l$. Следовательно, $l = m$.* ◄

c. *Отсюда имеем, что множество всех общих кратных чисел a и b совпадает с множеством всех кратных $\{f\}$ их наименьшего общего кратного l.*

§ 12. Задачи

1. *Доказать, что*

$$\text{а) } [a,b] = \frac{ab}{(a,b)}; \quad \text{б) } [a,b,c] = \frac{abc}{(bc,ca,ab)}; \quad \text{в) } (a,b,c) = \frac{abc}{[bc,ca,ab]};$$

$$\text{г) } [a_1, a_2, \dots, a_{n-1}, a_n] = [[a_1, a_2, \dots, a_{n-1}], a_n].$$

2. *Расширение множества целых чисел $\mathbb{Z}$ до множества $\mathbb{Q}$, замкнутого относительно четырех арифметических операций: сложения, вычитания, умножения и деления на ненулевое число, называется* полем рациональных чисел. *Доказать, что каждое рациональное число $a \neq 0$ представимо в виде дроби*

$$a = \frac{m}{n}$$

с однозначно определенными целыми взаимно простыми числами m, n, *причем* $n \geqslant 1$. *Любое другое представление числа* a *дробью* $a = \frac{M}{N}$, $N \geqslant 1$, *получается из него умножением на* $d = (M, N)$, *т. е.* $M = md$, $N = nd$. *Число* m *называется* числителем, *а число* n — знаменателем *несократимой дроби* $\frac{m}{n} = a$.

3. *Если сумма или разность двух обыкновенных несократимых дробей является целым числом, то знаменатели этих дробей равны.*

4. *Алгебраическая сумма сумма любого конечного числа обыкновенных несократимых дробей, знаменатели которых в совокупности взаимно просты, не может равняться целому числу.*

5. *Выражение* $m^p - n^p$, *где* p — *простое число, либо взаимно просто с* p, *либо делится на* p^2.

§ 13. Взаимная простота чисел. Функция Эйлера

a. *Два целых числа с наибольшим общим делителем, равным единице, называются* взаимно простыми. *Для каждого натурального* n *количество* $\varphi(n)$ *натуральных чисел, взаимно простых с* n *и не превосходящих* n, *задает функцию, которая называется* функцией Эйлера. *Например,* $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$.

b. *Справедливы следующие равенства.*

$\mathbf{1}^0$. $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

► Взаимно простыми с p^α будут все числа, не делящиеся на p. Количество таких чисел, не превосходящих p^α, равно в точности $p^\alpha - p^{\alpha-1} = \varphi(p^\alpha)$. ◄

$\mathbf{2}^0$. $\varphi(n) = n \prod\limits_{p|n} \left(1 - \frac{1}{p}\right)$.

► *Доказательство этого утверждения проведем методом мультипликативной индукции. Для* $n = p$, *где* p — *любое простое число, оно верно, поскольку* $\varphi(p) = p - 1$. *Предположим, что оно верно для* $n = m$. *Докажем справедливость этого утверждения для* $n = mp$, *где* p — *любое простое число.*

Имеется две возможности: а) $(m, p) = p$; *б)* $(m, p) = 1$. *На каждом из* p *промежутков вида* $[rm + 1, (r + 1)m]$, $0 \leqslant r < p$ *располагается одинаковое количество чисел, взаимно простых с*

m, *а именно* — $\varphi(m)$. *В силу предположения индукции*

$$\varphi(m) = m \prod_{q|m} \left(1 - \frac{1}{q}\right).$$

Рассмотрим случай а). Здесь условие $p \mid pm$ *эквивалентно* $p \mid m$. *Таким образом, справедлива цепочка равенств*

$$\varphi(n) = \varphi(mp) = p\varphi(m) = pm \prod_{q|pm} \left(1 - \frac{1}{q}\right) = n \prod_{q|n} \left(1 - \frac{1}{q}\right).$$

Рассмотрим теперь случай б). В силу сказанного выше, количество чисел, взаимно простых с m *и не превосходящих* mp, *равно* $p\varphi(m)$. *Из этого множества надо исключить числа, делящиеся на* p, *т. е. числа вида* rp, $(r, m) = 1,\ 1 \leqslant r \leqslant m$. *Тогда*

$$\varphi(mp) = p\varphi(m) - \varphi(m) = (p-1)\varphi(m) = mp \prod_{q|pm} \left(1 - \frac{1}{q}\right).$$

Утверждение 2^0 *доказано.* ◄

с. *Непосредственным следствием утверждения* 2^0 *является следующий факт.*

$\mathbf{3}^0$. *Если* $(m, n) = 1$, *то* $\varphi(mn) = \varphi(m)\varphi(n)$.

d. *Докажем еще одно важное свойство функции Эйлера.*

$\mathbf{4}^0$. $\sum\limits_{d|n} \varphi(d) = n$.

►

Каждое натуральное число k, *не превосходящее* n *можно единственным образом представить в виде* $k = dm$, *где* $d \mid n$, $(m, n) = 1$, *а значит,* $(m, \frac{n}{d}) = 1$. *Для каждого фиксированного* $d \mid n$ *количество таких чисел будет равно* $\varphi\left(\frac{n}{d}\right)$. *Поэтому*

$$n = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d).$$

Утверждение 4^0 *доказано.*◄

§ 14. Задачи

Доказать следующие утверждения.

1. *При $n > 1$ число $\varphi(n)$ является четным.*

2. $\varphi(5186) = \varphi(5187) = \varphi(5188) = 2592$.

3. $\varphi(n) \mid n$ *тогда и только тогда, когда* $n = 1, 2^a, 2^a 3^b$, *где* $a, b \in \mathbb{N}$.

4. *Справедливы следующие неравенства*

$$\varphi(n)\tau(n) \geqslant n, \quad \frac{6}{\pi^2} \leqslant \frac{\varphi(n)\sigma(n)}{n^2} \leqslant 1,$$

где $\tau(n)$ и $\sigma(n)$ обозначают соответственно количество и сумму делителей числа n.

e.Ряд Фарея F_N *порядка N — это расположение в возрастающем порядке правильных дробей, со знаменателями, не превосходящими N. Например,* $F_5 = \{\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}\}$.

5. *Никакие две соседние дроби ряда Фарея F_N при $N \geqslant 2$ не могут иметь одинаковых знаменателей.*

6. *Пусть $\frac{a}{b}$ и $\frac{c}{d}$ — две соседние дроби ряда Фарея. Тогда дроби $\frac{a+c}{b+d}$ и $\frac{a+b}{c+d}$ являются несократимыми.*

7. *Доказать, что медианта $\frac{a+c}{b+d}$ двух соседних дробей $\frac{a}{b}$ и $\frac{c}{d}$ ряда Фарея расположена между ними.*

8. *Пусть $\frac{a}{b} < \frac{c}{d}$ — две соседние дроби ряда Фарея. Тогда $ad - bc = -1$.*

9. *Средняя из трех последовательных дробей ряда Фарея является медиантой оставшихся двух дробей.*

10. *Сумма знаменателей двух соседних дробей ряда F_N превосходит N.*

11. *Количество дробей ряда F_N равно* $1 + \sum\limits_{n=1}^{N} \varphi(n)$.

12. *Для любого вещественного α и натурального N найдется рациональная дробь $\frac{p}{q}$ с условием $q \leqslant N$ и* $\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{q(N+1)}$.

13. *Среди первых N натуральных чисел произвольным образом выбрано более $\frac{N+1}{2}$ различных чисел. Тогда среди выбранных чисел найдутся два таких, что одно из них является делителем другого.*

14. *На любом полуинтервале длины $1/N$ найдется не более $\frac{N+1}{2}$ дробей ряда Фарея F_N.*

15. *Будем говорить, что соседние медианты дробей ряда Фарея F_N при $N \geqslant 2$ образуют* дуги Фарея. *Тогда если дуга Фарея содер-*

жит дробь $\frac{h}{k} \in F_N$, *то длина этой дуги заключена между* $\frac{1}{k(2N-1)}$ *и* $\frac{1}{k(N+1)}$.

§ 15. Метод мультипликативной индукции

a. *Дадим приложение доказанной выше основной теоремы арифметики. Оно показывает, что метод математической индукции допускает многочисленные, иногда неожиданные, модификации. Это приложение взято из книги известного норвежского математика Т. Нагелля «Введение в теорию чисел»* [**?**].

Под методом мультипликативной индукции *мы будем понимать доказательство, которое проводится по следующей схеме.*

1. Опытным или каким-либо другим путем выдвигается гипотеза о том, что для каждого номера $n > 1$ *выполнено свойство* E.

2. Проверяется, что свойством E *обладают все простые числа* p.

3. Предполагается, что некоторое натуральное число m *обладает свойством* E.

4. Исходя из предположения индукции доказывается, что для любого простого числа p *этим свойством обладают все числа вида* mp.

5. Отсюда по теореме об однозначности разложения на простые сомножители натуральных чисел, бóльших единицы, вытекает, что свойством E *обладают все натуральные числа, бóльшие единицы, и тем самым установлена справедливость гипотезы из пункта 1.*

Будем говорить, что функция $f(n)$ *натурального аргумента является* мультипликативной, *если для любых взаимно простых чисел* m *и* n *справедливо равенство* $f(mn) = f(m)f(n)$.

b.

$\mathbf{1}^0$. *Докажем сначала указанным методом мультипликативной индукции свойство мультипликативности* функции Мёбиуса, *определяемой на множестве натуральных чисел следующим образом:*

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1; \\ 0, & \text{если } p^2 \text{ делит } n; \\ (-1)^r, & \text{если } n = p_1 \dots p_r,\ p_k \neq p_l,\ k \neq l,\ 1 \leqslant k, l \leqslant r. \end{cases}$$

▶ *Заметим, что достаточно доказать утверждение о мультипликативности функции Мёбиуса только для чисел m и n, не делящихся на квадрат простого числа, т. е.* бесквадратных *чисел. Зафиксируем произвольное число m. Покажем, что утверждение имеет место для $n = p$, где p — произвольное простое число. Действительно, поскольку $(m, n) = 1$, если $m = p_1 \dots p_r$, где $p_1, \dots, p_r$ — различные простые числа, справедливо равенство $\mu(mp) = (-1)^{r+1}$. Следовательно,*

$$\mu(mp) = \mu(m)\mu(p).$$

Пусть утверждение верно для $n = k$. Докажем его для $n = kp$, где p — произвольное простое число. Так как n — бесквадратное число, имеем $(k, p) = 1$. По условию $(m, n) = 1$, поэтому $(mk, p) = 1$. Тогда по доказанному утверждению для простых чисел и по предположению индукции справедлива цепочка равенств

$$\mu(mn) = \mu(mkp) = \mu(mk)\mu(p) =$$

$$= \mu(m)\mu(k)\mu(p) = \mu(m)\mu(kp) = \mu(m)\mu(n).$$

Тем самым мультипликативность функции Мёбиуса доказана. ◀

с.

2^0. *Докажем теперь тем же методом основное свойство функции Мёбиуса. При любом натуральном a справедливо соотношение*

$$S_a = \sum_{d|a} \mu(d) = \begin{cases} 1, & \text{если } a = 1; \\ 0, & \text{если } a > 1. \end{cases}$$

▶ *Утверждение достаточно доказать для бесквадратных чисел a, поскольку функция Мёбиуса будет отлична от нуля только для его бесквадратных делителей. При $a = 1$ оно верно. Докажем утверждение методом мультипликативной индукции по величине $a > 1$. Пусть $a = p$. Тогда $S_p = \mu(1) + \mu(p) = 0$ Предположим, что оно справедливо при $a = m$. Докажем его при $a = mp$, где p — любое простое число с условием $(m, p) = 1$. Мы можем ограничиться только такими p, так как при $p \mid m$ бесквадратная часть числа mp совпадает с бесквадратной частью числа m. Имеем*

$$S_{mp} = \sum_{d|m} \left(\mu(d) + \mu(dp)\right).$$

Поскольку $\mu(pd) = -\mu(d)$, *сумма* $S_{mp} = 0$. ◀

Заметим, кстати, что функция Мёбиуса возникает во многих областях математики, играя важную роль при изучении ее дискретных объектов.

§ 16. Задачи

Доказать следующие утверждения.

1. *Функции* $\tau(n)$ *(количество делителей числа* n*) и* $\sigma(n)$ *(сумма всех делителей числа* n*) являются мультипликативными.*

2. *Пусть* $\theta(n)$ *— мультипликативная функция. Тогда функция* $\theta_1(n) = \sum_{d|n} \theta(d)$ *также является мультипликативной.*

3. *Справедливы равенства:*

а) $n^{\tau(n)} = \left(\prod\limits_{d|n} d\right)^2$; *б)* $n = \sum\limits_{d|n} d \left(\sum\limits_{k|n} \frac{1}{k}\right)^{-1}$.

4. *При* $(a, m) = 1$ *и любом целом* b *справедливы равенства:*

$$а) \sum_{x=0}^{m-1} \left\{\frac{ax+b}{m}\right\} = \frac{1}{2}(m-1); \quad б) \sum_{\xi} \left\{\frac{a\xi}{m}\right\} = \frac{1}{2}\varphi(m),$$

где ξ *пробегает взаимно простые с* m *числа, которые не превосходят* m.

5. *Справедливо равенство* $\varphi(n) = n \sum\limits_{d|n} \frac{\mu(d)}{d}$.

6. *Мультипликативная функция* $f(n)$ *является функцией Эйлера тогда и только тогда, когда* $\sum\limits_{d|n} f(d) = n$.

7. $G(a) = \sum\limits_{d|a} F(d)$ *тогда и только тогда, когда* $F(a) = \sum\limits_{d|a} \mu(d) G\left(\frac{a}{d}\right)$.

8. $G(a) = \prod\limits_{d|a} F(d)$ *тогда и только тогда, когда* $F(a) = \prod\limits_{d|a} \left(G\left(\frac{a}{d}\right)\right)^{\mu(d)}$.

9. *Функция* $f(n)$ *называется* аддитивной, *если для любых двух взаимно простых чисел* m *и* n *она удовлетворяет соотношению* $f(mn) = f(m) + f(n)$. *Функции* $\ln n$, $\omega(n)$ *— число различных простых делителей* n, $\Omega(n)$ *— число всех простых делителей* n, *являются аддитивными.*

10. *Пусть $f(n)$ — аддитивная функция. Тогда $f(1)=0$.*

11. *Пусть $f(1)=0$ и при $x\to\infty$ имеем $\sum_{n\leqslant x}|f(n+1)-f(n)|=o(x)$. Тогда $f(n)=o(n)$ при $n\to\infty$.*

12. *Пусть $q\geqslant 2$ — натуральное число. Тогда для любых вычетов r и s по модулю q имеем*

$$\left|\sum_{\substack{n\leqslant x\\ n\equiv r\ (\mathrm{mod}\ q)}} f(n)-\sum_{\substack{n\leqslant x\\ n\equiv s\ (\mathrm{mod}\ q)}} f(n)\right|\leqslant\sum_{n\leqslant x}|f(n+1)-f(n)|.$$

13. *Пусть при $x\to\infty$ имеем $\sum_{n\leqslant x}|f(n+1)-f(n)|=o(x)$. Тогда*

$$\sum_{n\leqslant x} f(n)=q\sum_{n\leqslant x/q} f(n)+xf(q)+o(x).$$

14. *Пусть $f(n)$ — аддитивная функция и при $x\to\infty$ имеем $\sum_{n\leqslant x}|f(n+1)-f(n)|=o(x)$. Тогда существует такая постоянная c, что $f(n)=c\ln n$.*

§ 17. Целая и дробная части числа. Деление с остатком

а. *Рассмотрим действительное число α. Множество всех действительных чисел будем обозначать через* $\mathbb{R}$. Целой частью *числа α назовем наибольшее целое число, не превосходящее α. Обозначим ее через $[\alpha]$. Разность $\alpha-[\alpha]=\{\alpha\}$ назовем* дробной частью *числа α. Например,*

$$[2]=2,\quad [\sqrt{3}]=1,\quad [\pi]=3,\quad [-3]=-3,\quad [-\sqrt{2}]=-2,\quad [-\pi]=-4,$$

$$\{2\}=0,\quad \{\sqrt{3}\}=\sqrt{3}-1=0,73\ldots,\quad \{\pi\}=0,14\ldots,$$

$$\{-\sqrt{2}\}=-\sqrt{2}+2=0,58\ldots.$$

Для любого действительного числа α справедливо двойное неравенство

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

В частности, для любого рационального числа $\alpha = a/b$, $(a, b) = 1$, $b \geqslant 1$, *имеем*

$$0 \leqslant \frac{a}{b} - \left[\frac{a}{b}\right] < 1 \quad \textit{или} \quad 0 \leqslant a - b\left[\frac{a}{b}\right] < b,$$

т. е.

$$a = b\left[\frac{a}{b}\right] + r, \quad 0 \leqslant r < b.$$

Тем самым, нашлась такая пара целых чисел q *и* r, *что*

$$a = bq + r, \quad 0 \leqslant r < b. \tag{1.1}$$

b. *Покажем единственность указанной пары* q *и* r. *Предположим, что существует другая пара целых чисел* q_1 *и* r_1, *такая, что*

$$a = bq_1 + r_1, \quad 0 \leqslant r_1 < b. \tag{1.2}$$

Поскольку числа r *и* r_1 *расположены на промежутке* $[0,\ b)$, *справедливо двойное неравенство*

$$0 \leqslant |r - r_1| < b.$$

Вычитая из равенства (**??**) *равенство* (**??**) *и переходя к модулям, при* $q \neq q_1$ *получим противоречивое соотношение*

$$b \leqslant b|q - q_1| = |r - r_1| < b.$$

Следовательно, $q = q_1$, *а значит,* $r = r_1$.

Таким образом, мы доказали следующее утверждение.

Теорема 6. *Для любого целого числа* a *и натурального* b *существует единственная пара целых чисел* q *и* r, *удовлетворяющая соотношениям*

$$a = bq + r, \quad 0 \leqslant r < b.$$

§ 18. Задачи

Доказать следующие утверждения.

1. *Справедливы неравенства*

$$[\alpha + \beta] \geqslant [\alpha] + [\beta], \quad [2\alpha] + [2\beta] \geqslant [\alpha] + [\alpha + \beta] + [\beta].$$

2. *Количество натуральных чисел, кратных натуральному* k *и не превосходящих* $x > 0$, *равно* $[x/k]$.

3. *При любых $\alpha \in \mathbb{R}$ и $n \in \mathbb{N}$ имеет место равенство*

$$[\alpha] + \left[\alpha + \frac{1}{n}\right] + \left[\alpha + \frac{2}{n}\right] + \ldots + \left[\alpha + \frac{n-1}{n}\right] = [n\alpha]$$

4. *Справедливы равенства* $\left[\sqrt{[x]}\right] = [\sqrt{x}]$; $[\log_2 [x]] = [\log_2 x]$.

5. *При любых $\alpha \in \mathbb{R}$ и $n \in \mathbb{N}$ имеет место равенство*

$$\left[\frac{[n\alpha]}{n}\right] = [\alpha].$$

6. *При любом натуральном n выполняются равенства*

$$\left[\sqrt{n} + \sqrt{n+1}\right] = \left[\sqrt{4n+2}\right];$$

$$\left[\sqrt{1}\right] + \left[\sqrt{2}\right] + \ldots + \left[\sqrt{n^2-1}\right] = n(n-1)(4n+1)/6.$$

7. *Пусть p — простое число. Тогда показатель степени p в каноническом разложении $n!$ равен*

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

Указание. *Количество чисел, не превосходящих n и кратных p, равно $\left[\frac{n}{p}\right]$, кратных p^2 равно $\left[\frac{n}{p^2}\right]$ и т. д.*

8. *Пусть $p^{\nu_p(n!)} \parallel n!$, $n = \sum_{0 \leqslant \varepsilon_k \leqslant p-1} \varepsilon_k p^k$, $S_n = \sum \varepsilon_k$. Тогда*

$$\nu_p(n!) = \frac{n - S_n}{p-1}.$$

9. *(*А. Н. Колмогоров*)* Положительным вещественным числом *называется однозначная функция*

$$m = \varphi(n),$$

определенная для всех натуральных чисел n, принимающая целые значения m и обладающая следующими свойствами:

1) для всех натуральных чисел k справедливо равенство

$$\varphi(n) = \left[\frac{\varphi(kn)}{k}\right];$$

2) для любого натурального числа n существует такое натуральное число k, что

$$\varphi(kn) > k\varphi(n).$$

Положительные вещественные числа будем обозначать малыми греческими буквами, а множество всех положительных вещественных чисел — буквой Φ. *Отношение порядка и операции сложения и умножения вводятся в множестве* Φ *следующим образом.*

Неравенство $\varphi < \psi$ между вещественными числами φ, ψ обозначает, что существует такое натуральное число n, для которого имеют место соотношения

$$\varphi(n) < \psi(n), \quad \varphi(1) = \psi(1), \quad \ldots, \quad \varphi(n-1) = \psi(n-1).$$

Сумма $\chi = \varphi + \psi$ обозначает, что для всех натуральных чисел n

$$\chi(n) = \max_k \left[\frac{\varphi(kn) + \psi(kn)}{k} \right],$$

где максимум берется по всем натуральным k.

Произведение $\chi = \varphi \cdot \psi$ обозначает, что для всех натуральных n

$$\chi(n) = \max_{k,k'} \left[\frac{\varphi(kn)\psi(k'n)}{kk'n} \right],$$

где максимум берется по всем парам натуральных чисел k, k'.

Докажите, что множество Φ *с определенными выше отношением порядка и операциями сложения и умножения обладает всеми свойствами обычных положительных вещественных чисел, т. е. изоморфно системе положительных вещественных чисел, построенных любым другим общепринятым способом.*

Указание. *Покажите, что для любого натурального числа r функция $\varphi(n) = \varphi_r(n) = nr - 1$ удовлетворяет условиям 1) и 2), т. е. является положительным вещественным числом. Это «число» φ_r естественно идентифицировать с натуральным числом r.*

Присоединив к множеству Φ *функцию $\varphi \equiv 0$, т. е. число* нуль, *условившись, что*

$$0 + 0 = 0, \quad 0 \cdot 0 = 0,$$

и для всех φ из Φ

$$0 < \varphi, \quad \varphi + 0 = 0 + \varphi = \varphi, \quad \varphi \cdot 0 = 0 \cdot \varphi = 0,$$

получим систему неотрицательных целых чисел.

Для любого φ *из* Φ *положим* $[\varphi] = m$ *— наибольшему целому числу, не превосходящему* φ*, т. е.*

$$m \leqslant \varphi < m + 1$$

(целая часть числа φ*).*

Затем для любого неотрицательного целого числа m *и натурального числа* n *определим операцию деления в* Φ *как действие, обратное умножению, и целое число* $[m/n]$*, которое совпадает с неполным частным этих чисел, определенным непосредственно.*

Наконец, можно доказать, что для любого φ *из* Φ

$$\varphi(n) = \begin{cases} \varphi n - 1, & \text{если } \varphi \text{ — целое число;} \\ [\varphi n] - 1, & \text{если } \varphi \text{ — нецелое число.} \end{cases}$$

Таким образом $\varphi(n)$ *— наибольшее целое число* m*, для которого*

$$\frac{m}{n} < \varphi.$$

§ 19. Целый модуль

Непустое подмножество M *целых чисел, замкнутое относительно операций сложения и вычитания, называется* целым модулем *или просто* модулем*. Это означает, что вместе с любыми* m, n *из* M *числа* $m \pm n$ *также принадлежат модулю* M*. В частности, модулю принадлежит число* 0*, поскольку* $0 = m - m$*, где* m *из* M*. Само число* 0 *образует* нулевой модуль*. Кроме того, вместе с каждым своим элементом* m *модуль содержит все числа, кратные* m*.*

Более того, справедливо обратное утверждение: любой ненулевой модуль есть множество целых чисел, являющихся кратными некоторого натурального числа*.*

► Пусть m — наименьшее натуральное число, принадлежащее модулю M. Возьмем любое число $a \in M$. Разделим его с остатком на m. Получим

$$a = mq + r, \quad 0 \leqslant r < m.$$

Покажем, что $r = 0$. По определению модуля $r = a - mq \in M$. Если $r \neq 0$, то в силу того, что $r \in M$, $0 < r < m$, это противоречит минимальности $m \in M$. Следовательно, $r = 0$. ◄

§ 20. Алгоритм Евклида

a. *Алгоритм Евклида при помощи последовательности делений с остатком позволяет находить наибольший общий делитель* $d = (a, b)$ *двух натуральных чисел* a *и* b. *Имеем*

$$\begin{array}{ll} a = bq_1 + r_1, & 0 < r_1 < b; \\ b = r_1q_2 + r_2, & 0 < r_2 < r_1; \\ \dots & \dots \\ r_{n-2} = r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1}; \\ r_{n-1} = r_nq_{n+1}. & \end{array}$$

Описанную последовательность делений выполняем до тех пор, пока не получится остаток, равный 0. *Это произойдет, поскольку остатки образуют монотонно убывающую последовательность неотрицательных целых чисел.*

b. *Докажем, что* $r_n = (a, b)$. *Если пройти эти равенства снизу вверх, то можно заметить, что*

$$r_n \mid r_{n-1}, \quad r_n \mid r_{n-2}, \quad \dots, \quad r_n \mid r_1, \quad r_n \mid b, \quad r_n \mid a.$$

С другой стороны, пусть f *— общий делитель чисел* a *и* b. *Тогда если пройти эти равенства сверху вниз, то получается цепочка соотношений*

$$f \mid a, \quad f \mid b, \quad f \mid r_1, \quad f \mid r_2, \quad \dots, \quad f \mid r_n.$$

Следовательно, согласно критерию наибольшего общего делителя, $r_n = (a, b)$.

Добавим к этому, что если пройти эти равенства сверху вниз, выражая r_1 *через* a *и* b, *затем* $r_2, \dots, r_n$ *— также через* a *и* b, *то получим, что найдутся такие целые числа* x *и* y, *что*

$$r_n = ax + by.$$

§ 21. Задачи

Доказать следующие утверждения.

1. *Если* p *— простое число, то из* $p \mid ab$ *следует, что* $p \mid a$ *или* $p \mid b$. *Вывести отсюда основную теорему арифметики.*

2. $(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1,\ m, n \in \mathbb{N}$.

3. *Если* $ad - bc = 1$, *то* $(a + b, c + d) = 1$.

4. *Если $ad + bc$ делится на $a + c$, то $ab + cd$ также делится на $a + c$.*

5. *Пусть $d = (a, b)$. Тогда справедливы следующие утверждения:*

а) для любых целых чисел x и y выражение $ax + by$ делится на d;

б) если $r \mid a$ и $r \mid b$, то $r \mid d$;

в) для любого натурального c имеем $(ac, bc) = dc$;

г) уравнение $ax + by = n$ разрешимо в целых числах x, y тогда и только тогда, когда $d \mid n$.

§ 22. Непрерывная дробь числа

а. *При помощи алгоритма Евклида для двух натуральных чисел a и b можно построить* алгоритм разложения в непрерывную дробь *рационального числа $\alpha = a/b > 0$, $(a, b) = 1$:*

$$\begin{aligned}
&\frac{a}{b} = q_1 + \frac{r_1}{b}, && 0 < \frac{r_1}{b} < 1;\\
&\frac{b}{r_1} = q_2 + \frac{r_2}{r_1}, && 0 < \frac{r_2}{r_1} < 1;\\
&\dots && \dots\\
&\frac{r_{n-2}}{r_{n-1}} = q_n + \frac{r_n}{r_{n-1}}, && 0 < \frac{r_n}{r_{n-1}} < 1;\\
&\frac{r_{n-1}}{r_n} = q_{n+1}.
\end{aligned}$$

По-другому это можно записать так:

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots + \cfrac{1}{q_n + \cfrac{1}{q_{n+1}}}}}.$$

Полученная запись называется непрерывной *или* цепной дробью. *Она получается выделением целой части числа α, т. е. представлением его в виде*

$$\alpha = [\alpha] + \frac{1}{\beta}, \quad \beta = \frac{1}{\{\alpha\}},$$

и дальнейшим применением к β той же самой процедуры.

b. *Таким образом, рациональное число представимо в виде конечной цепной дроби. С другой стороны, процесс разложения в цепную дробь иррационального числа не может остановиться на конечном шаге, поскольку конечная цепная дробь равна рациональному числу.*

Тем самым, мы показали, что разложение в непрерывную дробь положительного действительного числа обрывается на конечном шаге тогда и только тогда, когда оно является рациональным числом.

c. *Докажем еще несколько свойств наибольшего общего делителя двух чисел.*

Теорема 7. *Пусть a и b — натуральные числа и d — наименьшее натуральное число, представимое в виде $ax + by$, где x и y — целые числа. Тогда $d = (a, b)$. Более того, все натуральные числа, представимые в этом виде, равны qd, где $q \in \mathbb{N}$.*

► *Обозначим через M множество всех натуральных чисел u, представимых в виде $u = ax + by$, $x, y \in \mathbb{Z}$. Докажем, что любое число u из M делится на d. Разделим u на d с остатком: $u = qd + r$, $0 \leqslant r < d$. Отсюда и из представимости u и d в виде $ax + by$ имеем, что r также представимо в таком виде, а это возможно только при $r = 0$, поскольку $r < d$, а d — минимальное натуральное число, представимое в этом виде. Следовательно,*

$$d \mid a = a \cdot 1 + b \cdot 0,\ d \mid b = a \cdot 0 + b \cdot 1,$$

т. е. d является общим делителем чисел a и b.

Пусть $c \mid a$, $c \mid b$, т. е. $a = ca_0$, $b = cb_0$, и $d = ax_0 + by_0$. Тогда $d = c(a_0x_0 + b_0y_0)$. Следовательно, $c \mid d$. Тем самым, согласно критерию наибольшего общего делителя, $d = (a, b)$. ◄

Теорема 8. *Пусть a и b — взаимно простые целые числа и $n = ax_0 + by_0$, $x_0, y_0 \in \mathbb{Z}$. Тогда любое целочисленное решение x, y уравнения $ax + by = n$ можно представить в виде $x = x_0 + bt$, $y = y_0 - at$, $t \in \mathbb{Z}$.*

► *Имеем $a(x - x_0) + b(y - y_0) = 0$. В силу взаимной простоты чисел a и b получаем $a \mid y - y_0$, т. е. $y = y_0 - at$, $t \in \mathbb{Z}$. Подставляя значение y в предыдущее равенство, получим $x = x_0 + bt$.* ◄

Теорема 9. *Пусть a и b — взаимно простые натуральные числа. Тогда любое целое $n > ab - a - b$ представимо в виде $ax + by = n$, $x, y \geqslant 0$, $x, y \in \mathbb{Z}$. Число $ab - a - b$ в таком виде не представимо.*

► *Пусть* x_0, y_0 — *некоторое решение уравнения* $ax + by = n$. *В силу теоремы* **??** *существует параметризация всех решений:* $x = x_0 + bt$, $y = y_0 - at$, $t \in \mathbb{Z}$. *Возьмем такое число* t, *что* $0 \leqslant y_0 - at \leqslant a - 1$. *Тогда получим*

$$(x_0 + bt)a = n - (y_0 - at)b > ab - a - b - (a-1)b = -a,$$

т. е. $x_0 + bt > -1$, *или* $x = x_0 + bt \geqslant 0$.

Предположим, что имеется представление числа $ab - a - b$ *в виде* $ax + by, x, y \geqslant 0$, $x, y \in \mathbb{Z}$. *Тогда* $ab = a(x+1) + b(y+1)$. *Так как* $(a, b) = 1$, *то* $a \mid y + 1$, $b \mid x + 1$. *Следовательно,* $y + 1 \geqslant a$, $x + 1 \geqslant b$ *и* $ab = a(x + 1) + b(y + 1) \geqslant 2ab$. *Противоречие.* ◄

§ 23. Задачи

1. *Пусть* $a_1, \ldots, a_n$ — *целые числа и* d — *наименьшее натуральное число, представимое в виде* $a_1x_1 + \ldots + a_nx_n$, *где* $x_1, \ldots, x_n$ — *целые числа. Тогда* $d = (a_1, \ldots, a_n)$.

2. *Доказать, что число решений уравнения* $x + 2y + 3z = n$ *в неотрицательных целых числах* x, y, z *равно*

$$\frac{(n+3)^2}{12} - \frac{7}{72} + \frac{(-1)^n}{8} + \frac{2}{9}\cos\frac{2\pi n}{3}.$$

Указание. *Рассмотреть производящую функцию*

$$f(z) = \frac{1}{(1-z)(1-z^2)(1-z^3)} = c_0 + c_1z + c_2z^2 + \ldots,$$

где c_n — *искомое число решений. Затем разложить* $f(z)$ *на простейшие дроби.*

3. *Пусть* a, b, c — *натуральные попарно взаимно простые числа, т. е.* $(b, c) = (c, a) = (a, b) = 1$. *Тогда наибольшее целое, не представимое в виде* $bcx + cay + abz$, *где* x, y, z — *неотрицательные целые числа, равно* $2abc - ab - bc - ca$.

4. *(Нерешенная задача). Найти наибольшее целое число, не представимое в виде* $ax + by + cz$, *где* x, y, z — *неотрицательные целые числа,* $a > 0, b > 0, c > 0$ *и* $(a, b, c) = 1$.

§ 24. Позиционные системы счисления

а. *Рассмотрим натуральное число* $g > 1$.

Теорема 10. *Любое натуральное число* a *представляется единственным способом в виде*

$$\begin{gathered} a = c_0 + c_1 g + \ldots + c_n g^n, \\ n \geqslant 0, \quad c_n > 0, \quad 0 \leqslant c_m < g \quad \text{при} \quad 0 \leqslant m \leqslant n. \end{gathered} \tag{1.3}$$

▶ Существование представления. *При* $a = 1$ *утверждение верно, поскольку* $n = 0$, $c_0 = 1$. *Предположим, что оно верно при* $a < m$. *Докажем его справедливость при* $a = m$. *При некотором* $n \geqslant 0$ *выполняются неравенства* $g^n \leqslant m < g^{n+1}$. *По теореме* **??** *имеем*

$$m = c_n g^n + r, \quad 0 \leqslant r < g^n, \quad 0 < c_n < g.$$

Если $r = 0$, *то искомое представление имеет вид*

$$a = c_n g^n = 0 + 0 \cdot g + \ldots + 0 \cdot g^{n-1} + c_n g^n, \quad 0 < c_n < g.$$

Пусть $r \geqslant 1$. *Тогда* $r < g^n \leqslant a$, *поэтому существует такое число* $s \geqslant 0$, *что* $g^s \leqslant r < g^{s+1} \leqslant g^n$. *По предположению индукции имеем* $0 \leqslant c_t < g$ *при* $0 \leqslant t \leqslant s-1$, $0 < c_s < g$,

$$r = c_0 + c_1 g + \ldots + c_s g^s \leqslant$$

$$\leqslant (g-1) + (g-1)g + \ldots (g-1)g^s = g^{s+1} - 1 < g^{s+1}.$$

Таким образом, мы получили искомое представление числа a *в виде* $a = c_0 + c_1 g + \ldots + c_s g^s + 0 \cdot g^{s+1} + \ldots + 0 \cdot g^{n-1} + c_n g^n$.

Единственность представления. *Предположим, что имеется еще одно представление*

$$\begin{gathered} m = d_0 + d_1 g + \ldots + d_k g^k, \\ 0 < d_k < g, \quad 0 \leqslant d_l < g \quad \text{при} \quad 0 \leqslant l \leqslant k-1. \end{gathered} \tag{1.4}$$

Вычитая из (**??**) *представление числа* a *в виде* (**??**) *(при одинаковых степенях* g^u *производим вычитание соответствующих коэффициентов), получим*

$$0 = e_0 + e_1 g + \ldots + e_q g^q, \quad e_q \neq 0, \quad |e_t| \leqslant g-1 \quad \textit{при} \quad 0 \leqslant t \leqslant q.$$

Следовательно,

$$g^q \leqslant |e_q g^q| = |e_0 + e_1 g + \ldots + e_{q-1} g^{q-1}| \leqslant$$

$$\leqslant (g-1)+(g-1)g+\ldots(g-1)g^{q-1}=g^q-1<g^q,$$

что невозможно. Таким образом, $e_0=e_1=\cdots=e_s=0$, *т. е.* $n=k$ *и* $c_0=d_0,\ c_1=d_1,\ \ldots,c_n=d_n$. ◀

Представление числа в виде (**??**) *называется* представлением его в g-ой системе счисления, *а число* g *называется* основанием позиционной системы счисления. *Например, если* $g=2$, *то такая система счисления называется* двоичной, *а при* $g=10$ *мы имеем дело с* десятиричной *или* десятичной *системой счисления.*

§ 25. Задачи

1. *Доказать, что при* $g\in\mathbb{N},\ g\neq 3$, *число* $g^4+g^3+g^2+g+1$ *не равно квадрату целого числа.*

2. *Доказать, что при* $g\in\mathbb{N},\ g\neq 2$, *число* $g^4+2g^3+2g^2+2g+5$ *не равно квадрату целого числа.*

3. *Пусть* m *и* n *— два натуральных числа, из которых* n *— наименьшее и* $2^k\leqslant n<2^{k+1}$. *Посредством представления* m *и* n *в двоичной системе счисления доказать, что число делений для нахождения наибольшего общего делителя по алгоритму Евклида, не превосходит* $2k$.

4. *Пусть* $\frac{1}{p}=\sum\varepsilon_k 10^{-k}$, $0\leqslant\varepsilon_k\leqslant 9$, p *— простое. Тогда количество цифр в периоде десятичной дроби является делителем числа* $p-1$.

5. *Пусть* $\{f_n\}$ *— последовательность Фибоначчи:* $f_0=1,\ f_1=1$ *и* $f_{n+1}=f_n+f_{n-1}$ *при* $n\in\mathbb{N}$. *Тогда любое натуральное число* N *можно единственным образом представить в виде*

$$N=\sum_{k=0}^{\infty}\alpha_k f_k,$$

где $\alpha_k\alpha_{k+1}=0$ *для любого* $k\geqslant 0$.

Глава II
ПРОСТЫЕ ЧИСЛА. ТЕОРЕМА П. Л. ЧЕБЫШЕВА

§ 1. Совершенные числа. Числа Мерсенна и Ферма

a. *Пусть $\sigma(n)$ обозначает сумму всех делителей натурального числа n, т. е.*

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

Пусть, далее, $n = p_1^{a_1} \dots p_k^{a_k}$ — каноническое разложение числа n на простые множители. Тогда любой его делитель можно представить в виде $d = p_1^{b_1} \dots p_k^{b_k}$, где $0 \leqslant b_1 \leqslant a_1, \ \dots, \ 0 \leqslant b_k \leqslant a_k$. Поэтому для $\sigma(n)$ справедлива формула

$$\sigma(n) = \sum_{b_1=0}^{a_k} \cdots \sum_{b_k=0}^{a_k} p_1^{b_1} \dots p_k^{b_k} =$$

$$= \left(\sum_{b_1=0}^{a_k} p_1^{b_1} \right) \dots \left(\sum_{b_k=0}^{a_k} p_k^{b_k} \right) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \dots \frac{p_k^{a_k+1} - 1}{p_k - 1}.$$

b. *Функция $\sigma(n)$ является мультипликативной, т. е. для любых взаимно простых чисел m и n имеет место равенство $\sigma(mn) = \sigma(m)\sigma(n)$. Доказательство этого утверждения следует из предыдущей формулы для $\sigma(n)$, но его можно провести также методом мультипликативной индукции аналогично тому, как это сделано для функции Мёбиуса*

c. *Натуральное число n называется* совершенным, *если выполняется равенство $\sigma(n) = 2n$. Например, совершенными являются числа $6 = 1 + 2 + 3$ и $28 = 1 + 2 + 4 + 7 + 14$. С другой стороны, натуральные числа n вида $n = p^\nu, \nu \geqslant 1$, где p — простое число, не являются совершенными. Действительно, в этом случае*

$$\sigma(n) = 1 + p + \ldots + p^\nu = \frac{p^\nu - 1}{p - 1} + p^\nu < 2p^\nu.$$

Для четных чисел справедлив следующий критерий совершенности.

Теорема 11. *Четное число является совершенным тогда и только тогда, когда оно имеет вид*

$$2^{n-1}(2^n-1)=\frac{1}{2}p(p+1),$$

где $p=2^n-1$ *— простое число.*

► Необходимость. *В силу мультипликативности функции* $\sigma(n)$ *получим*

$$\sigma\left(p\frac{p+1}{2}\right)=(p+1)(1+2+\ldots+2^{n-1})=(p+1)(2^n-1)=p(p+1).$$

Достаточность. *Пусть* a *— четное совершенное число. Положим* $a=2^{n-1}u$, $n>1$, $u>1$, $(2,u)=1$. *Тогда снова в силу мультипликативности функции* $\sigma(n)$ *получим*

$$2^nu=2a=\sigma(a)=(2^n-1)\sigma(u),$$

поэтому

$$\sigma(u)=\frac{2^nu}{2^n-1}=u+\frac{u}{2^n-1}.$$

Оба числа u *и* $\frac{u}{2^n-1}$ *являются делителями* u. *Поскольку* $\sigma(u)$ *— сумма всех делителей числа* u, *то мы доказали, что* u *имеет ровно два делителя. Следовательно,* u *— простое число и* $\frac{u}{2^n-1}=1$. ◄

Необходимость этого утверждения содержится в «Началах» Евклида, а достаточность доказана Л. Эйлером.

Простые числа p *вида* 2^n-1 *называются* простыми числами Мерсенна. *Их запись в двоичной системе счисления содержит только единицы.*

Если число n *— составное, то* $n=ab$, $1<a,b<n$, *и*

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

так что в этом случае число 2^n-1 *не может быть простым.*

Таким образом, если 2^n-1 *— простое, то* $n=p$ *— простое число. Простые числа Мерсенна обычно обозначают через* $M_p=2^p-1$. *Показано, что* M_p *— простое число при*

$$p=2,3,5,7,13,19,31,61,89,107,127,521,607,1279,2203,$$

$$2281,3217,4253,4423,9689,9941,11213,19937,21701,23209,44497.$$

$$1257787, 1398269, 3021377, 6972593, \ldots$$

(мы привели первые 30 значений p).

44-е простое число Мерсенна найдено в сентябре 2006 г. участниками проекта Great Internet Mersenne Prime Search[1] *К. Купером и С. Буном (они распознали простоту и предыдущего, 43-го, простого числа Мерсенна). Это число, равное*

$$2^{32\,582\,657} - 1 = 124575026015369455 40...11752880154053967871$$

и состоящее из 9 808 358 цифр, является самым большим из известных простых чисел на момент выхода книги в свет.

d. *Имеется предположение, что простых чисел Мерсенна бесконечно много. Таким образом, если обозначить через $\pi_M(x)$ количество простых чисел Мерсенна M_p при $p \leqslant x$, то предположительно*

$$\pi_M(x) \to \infty \quad \textit{при} \quad x \to \infty.$$

Но с другой стороны, существует гипотеза, что

$$\frac{\pi_M(x)}{\pi(x)} \to 0 \quad \textit{при} \quad x \to \infty,$$

где $\pi(x)$ — количество всех простых чисел, не превосходящих x.

В направлении второго предположения в подобной задаче о количестве $\pi_K(x)$ простых чисел Каллена $n2^n + 1$, $n \leqslant x$, К. Хооли доказал, что

$$\frac{\pi_K(x)}{x} \to 0 \quad \textit{при} \quad x \to \infty.$$

Эти исследования Хооли продолжила А. Мильуоло, которая доказала, что

$$\frac{\pi_C(x)}{\pi(x)} \to 0 \quad \textit{при} \quad x \to \infty,$$

где $\pi_C(x)$ — количество простых чисел вида $2^p - p$ (или $2^p + p$), при условии, что p не превосходит x.

Известно, что любое нечетное совершенное число должно

1) превосходить 10^{50} (см. [?]);

2) иметь более 100 110 простых делителей (см. [?]).

На настоящий момент не найдено ни одного нечетного совершенного числа.

[1] Великий интернет-поиск простых чисел Мерсенна (*англ.*).

Определим простые числа Ферма, *имеющие вид* $2^n + 1$.

е. *Если число* n *— составное, то пусть* $n = ab$, *где* a *— нечетный простой делитель, и*

$$2^n + 1 = \left(2^b\right)^a + 1 = (2^b + 1)(2^{b(a-1)} - 2^{b(a-2)} + \ldots + 1).$$

Следовательно, в этом случае число $2^n + 1$ *не может быть простым, если существует нечетный простой делитель, больший единицы.*

Таким образом, если $2^n + 1$ *— простое число, то* $n = 2^m$, $m > 0$. *Число* $F_m = 2^{2^m} + 1$ *при* $m \geqslant 0$ *называется* числом Ферма. *Первые пять чисел Ферма*

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

являются простыми.

е. *В 1732 г. Л. Эйлер показал, что*

$$F_5 = 2^{2^5} + 1 = 641 \times 6700417.$$

Действительно, $2^4 + 5^4 = 1 + 5 \cdot 2^7 = 641$,

$$F_5 = (2^4 + 5^4)2^{28} + 1 - (5 \cdot 2^7)^4 =$$

$$= (1 + 5 \cdot 2^7)2^{28} + (1 + 5 \cdot 2^7)(1 - 5 \cdot 2^7)(1 + 5^2 \cdot 2^{14}) =$$

$$= (1 + 5 \cdot 2^7)\left(2^{28} + (1 - 5 \cdot 2^7)(1 + 5^2 \cdot 2^{14})\right) = 641 \cdot 6700417.$$

На сегодняшний день найдено много составных чисел Ферма, но кроме F_0, F_1, F_2, F_3, F_4 *простых чисел Ферма отыскать не удалось. Поэтому в противоположность гипотезе Ферма утверждается, что простых чисел Ферма конечное число. Было бы интересно доказать, что*

$$\frac{\pi_F(x)}{x} \to 0 \quad \textit{при} \quad x \to \infty,$$

где $\pi_F(x)$ *— количество простых чисел Ферма* F_n *при* $n \leqslant x$.

Как показал Гаусс [?] простые числа Ферма F_n *тесным образом связаны с построением циркулем и линейкой правильных многоугольников. Он перечислил все такие* n*-угольники, где* $n < 300$ *(простыми делителями числá* n *могут быть лишь* $2, 3, 5, 17$*):*

$$n = 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68,$$

$$80, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272.$$

Еще более сложной задачей является описание всех простых чисел p, имеющих в своей записи в двоичной системе счисления ровно 3 единицы, т. е. $p = 2^n + 2^m + 1$.

В 1968 г. А. О. Гельфонд [?] доказал, что в арифметической прогрессии находится асимптотически поровну чисел с четным и нечетным количеством единиц в записи в двоичной системе счисления. Аналогичный вопрос о простых числах с четным и нечетным количеством единиц в натуральном ряде чисел еще ждет своего решения.

Н. П. Романов доказал следующую изящную теорему (см. [?]).

Теорема. *Пусть $g \geqslant 2$. Тогда числа n вида $p + g^m$, где p пробегает все простые числа, m — все натуральные, имеют положительную плотность, т. е. количество таких чисел $n \leqslant x$ будет превосходить cx, где $c > 0$ — некоторая постоянная.*

С другой стороны, ван дер Корпут [?] и Эрдёш [?] доказали, что существует прогрессия, состоящая из нечетных чисел, которая не содержит ни одного числа вида $p + 2^m$.

В 1937 г. И. М. Виноградов вывел асимптотическое выражение для числа представлений нечетного $N > 0$ в форме

$$N = p_1 + p_2 + p_3.$$

Отсюда непосредственно следует, что всякое достаточно большое нечетное число можно представить в виде суммы трех простых чисел. Это есть полное решение проблемы Гольдбаха для нечетных чисел (см. [?]).

Бинарная проблема Эйлера—Гольдбаха о представимости четного числа в виде суммы двух простых чисел еще не решена. Прекрасный результат в направлении этой проблемы получил Чен Джун-ран [?]: каждое достаточно большое четное число представимо в виде суммы простого и числа, равного произведению не более двух простых чисел.

§ 2. Задачи

1. *Доказать, что нечетное число a, имеющее не более двух простых делителей, не является совершенным. Более того, $\sigma(a) < 2a$.*

2. *Доказать, что отношение $\frac{\sigma(n)}{n}$ может принимать сколь угодно большие значения. (*Указание. *Число $n = m!$ имеет делители*

2, $\ldots, m$. *Тогда* $\frac{\sigma(n)}{n} \geqslant 1 + \frac{1}{2} + \ldots + \frac{1}{m} \to \infty$ *при* $m \to \infty$.*)*

3. *Доказать, что простое число* M_{44497} *имеет* 13395 *цифр в десятичной записи (см. [?]).*

4. *Число делений для нахождения наибольшего общего делителя двух натуральных чисел по алгоритму Евклида не превосходит пятикратного числа цифр меньшего числа, записанного в обычной десятичной системе счисления.*

§ 3. Теорема П. Л. Чебышёва (постулат Бертрана)

a. *Тот факт, что в натуральном ряду простых чисел бесконечно много, был доказан еще Евклидом. Однако вопрос о том, содержит ли данная числовая последовательность бесконечно много простых чисел или нет, зачастую оказывается нетривиальным. Выше мы касались этого вопроса в связи с числами Мерсенна* $M_p = 2^p - 1$ *и Ферма* $F_n = 2^{2^n} + 1$. *Приведем еще несколько открытых проблем в данной области.*

$\mathbf{1}^0$. *Бесконечно ли множество пар простых чисел вида* (p, q), *где* $q = p + 2$ *(проблема простых близнецов)?*

$\mathbf{2}^0$. *Каждое ли четное число является разностью между двумя простыми числами?*

$\mathbf{3}^0$. *Каждое ли четное число (начиная с 4) представимо в виде суммы двух простых чисел (проблема Эйлера—Гольдбаха)?*

b. *К подобного рода утверждениям относится и теорема П. Л. Чебышёва о том, что на любом промежутке* $[x; 2x)$, $x > 1$, *лежит хотя бы одно простое число. Это утверждение потребовалось Бертрану в теории групп, и поскольку сам Бертран доказать его не смог, он назвал это утверждение постулатом.*

c. *Прежде чем доказывать постулат Бертрана (теорему Чебышёва), рассмотрим несколько лемм.*

Лемма 1. *При* $x \geqslant 1$ *справедливы равенства*

$$T(x) = \sum_{n \leqslant x} \ln n = \sum_{m \leqslant x} \psi\left(\frac{x}{m}\right),$$

$$T(x) - 2T\left(\frac{x}{2}\right) = \sum_{n \leqslant x} (-1)^{n-1} \psi\left(\frac{x}{n}\right).$$

► *Поскольку*

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

имеем

$$T(x) = \sum_{n\leqslant x} \sum_{d|n} \Lambda(d) = \sum_{d\leqslant x} \Lambda(d) \sum_{\substack{n\leqslant x \\ n=md}} 1 =$$

$$= \sum_{d\leqslant x} \Lambda(d) \sum_{m\leqslant x/d} 1 = \sum_{m\leqslant x} \sum_{d\leqslant x/m} \Lambda(d) = \sum_{m\leqslant x} \psi\left(\frac{x}{m}\right).$$

Второе равенство из утверждения леммы является непосредственным следствием доказанного. ◄

Отметим следующее свойство ряда, замеченное Лейбницем: если последовательность неотрицательных чисел $\{a_n\}$, $n = 1, 2, \ldots$, *не возрастает и стремится к нулю при* $n \to \infty$, *то*

$$a_1 - a_2 \leqslant \sum_{n=1}^{\infty} (-1)^{n-1} a_n \leqslant a_1 - a_2 + a_3.$$

Лемма 2. *При* $x \geqslant 1$ *справедливы неравенства*

$$\psi(x) - \psi(x/2) \leqslant T(x) - 2T(x/2) \leqslant \psi(x) - \psi(x/2) + \psi(x/3).$$

► *Поскольку функция* $\psi(x)$ *не убывает, утверждение леммы следует из отмеченного выше свойства знакочередующегося ряда и леммы* **??**. ◄

Лемма 3. *Для любого натурального числа* m *имеем*

$$\frac{1}{2\sqrt{m}} \leqslant 2^{-2m} \binom{2m}{m} < \frac{1}{\sqrt{2m+1}}.$$

► *Проведем индукцию по* m. *При* $m = 1$ *утверждение леммы справедливо, поскольку*

$$\frac{1}{2} = 2^{-2} \binom{2}{1} < \frac{1}{\sqrt{3}}.$$

Предположим его справедливость при $m = k$. *Докажем, что оно верно при* $m = k + 1$. *По предположению индукции имеем цепочку неравенств*

$$\frac{1}{2\sqrt{m}} 2^{-2} \frac{(2m+1)(2m+2)}{(m+1)^2} \leqslant 2^{-2m-2} \binom{2m+2}{m} <$$

$$< \frac{1}{\sqrt{2m+1}} 2^{-2} \frac{(2m+1)(2m+2)}{(m+1)^2}.$$

Достаточно доказать, что выполняются неравенства

$$\frac{1}{2\sqrt{m+1}} \leqslant \frac{1}{2\sqrt{m}} 2^{-2} \frac{(2m+1)(2m+2)}{(m+1)^2},$$

$$\frac{1}{\sqrt{2m+1}} 2^{-2} \frac{(2m+1)(2m+2)}{(m+1)^2} < \frac{1}{\sqrt{2m+3}}.$$

Первое из них является следствием того, что

$$2m+1 \geqslant 2\sqrt{m(m+1)}, \quad \text{т. е.} \quad 4m^2+4m+1 \geqslant 4m^2+4m,$$

а второе следует из того, что

$$2m+2 \geqslant \sqrt{(2m+1)(2m+3)} \quad \text{т. е.} \quad 4m^2+8m+4 \geqslant 4m^2+8m+3.$$

◀

Лемма 4. *При $x \geqslant 1$ справедливо неравенство*

$$\psi(x) < x \ln 4.$$

▶ *Проверим утверждение леммы при $x \leqslant 16$ непосредственно. При $1 \leqslant x < 2$ оно очевидно, так как на этом промежутке нет простых чисел. При $2 \leqslant x < 4$ имеем*

$$\psi(x) \leqslant \ln 2 + \ln 3 < \frac{3}{2} \ln 4 < x \ln 4.$$

Если $4 \leqslant x < 7$, то

$$\psi(x) \leqslant 2\ln 2 + \ln 3 + \ln 5 = \ln 60 < 3 \ln 4 < x \ln 4.$$

Пусть теперь $7 \leqslant x < 11$. Тогда

$$\psi(x) \leqslant 3\ln 2 + 2\ln 3 + \ln 5 + \ln 7 = \ln 2520 < 6 \ln 4 < x \ln 4.$$

Пусть, наконец, $11 \leqslant x \leqslant 16$, тогда

$$\psi(x) \leqslant 4\ln 2 + 2\ln 3 + \ln 5 + \ln 7 + \ln 11 + \ln 13 =$$

$$= \ln 720720 < 10 \ln 4 < x \ln 4.$$

Проведем доказательство леммы индукцией по параметру x. При $x \leqslant 16$ ее утверждение справедливо. Предположим, что оно имеет место при $2 \leqslant x \leqslant y-2$. Докажем, что утверждение леммы справедливо при $x \leqslant y$.

Возьмем ближайшее к y четное число $2m$. Если $y = 2r+1$, то положим $2m = 2r+2$. Следовательно, $2m-1 \leqslant y < 2m+1$. Взяв в лемме **??** *величину $x = 2m$, получим*

$$\psi(2m) \leqslant A + \psi(m), \quad A = \ln \binom{2m}{m}.$$

Поскольку $m \leqslant y-2$, $y > 16$, воспользуемся предположением индукции. Находим

$$\psi(2m) < 2m \ln 2 - \ln \sqrt{2m+1} + 2m \ln 2 = 2m \ln 4 - \ln \sqrt{2m+1}.$$

Далее, если $2m < y$, то в силу выбора параметра m имеем $y < 2m+1$ и

$$\psi(y) = \psi(2m) < 2m \ln 4 < y \ln 4.$$

Если же $2m \geqslant y$, то согласно выбору m справедливы неравенства $y \geqslant 2m-1$ и

$$\psi(y) \leqslant \psi(2m) \leqslant 2m \ln 4 - \ln \sqrt{2m+1} \leqslant y \ln 4 + \ln 4 - \ln (y+1).$$

Так как $y > 16$, то $\ln 4 \leqslant \ln \sqrt{y+1}$. Таким образом, лемма полностью доказана. ◀

Лемма 5. *При $m \geqslant 1$ справедливо неравенство*

$$\theta(2m) - \theta(m) \geqslant \frac{m}{3} \ln 4 - \ln \sqrt{4n} - \sqrt{2m} \ln 4.$$

► *Пусть, как и раньше, $A = \ln \binom{2m}{m}$. Тогда, пользуясь оценками леммы* **??** *и* **??**, *получим*

$$\psi(2m) - \psi(m) > A - \psi\left(\frac{2m}{3}\right) \geqslant$$

$$\geqslant m \ln 4 - \ln \sqrt{4m} - \frac{2m}{3} \ln 4 = \frac{m}{3} \ln 4 - \ln 4.$$

Далее, имеем

$$\psi(2m) - \psi(m) = \theta(2m) - \theta(m) + r_m,$$

где

$$r_m = \sum_{\substack{m<p^\alpha\leqslant 2m\\ \alpha\geqslant 2}} \ln p.$$

Поскольку $\alpha \geqslant 2$, *в сумму* r_m *входят простые числа* p *с условием* $p \leqslant \sqrt{2m}$, *причем если* $m < p^\alpha \leqslant 2m$, *то другие степени этого простого числа* p *в промежуток* $(m, 2m]$ *не попадают. В силу этого*

$$r_m \leqslant \theta(\sqrt{2m}) \leqslant \psi(\sqrt{2m}) \leqslant \sqrt{2m}\ln 4.$$

Следовательно,

$$\theta(2m) - \theta(m) \geqslant \frac{m}{3}\ln 4 - \ln\sqrt{4m} - \sqrt{2m}\ln 4.$$

◀

Лемма 6. *При* $m \geqslant 2^8$ *справедливо неравенство*

$$\pi(2m) - \pi(m) \geqslant \sqrt{m/2}.$$

▶ *Поскольку при* $m < p \leqslant 2m$ *выполняется неравенство*

$$\ln p \leqslant \ln 2m,$$

в силу леммы **??** *получим цепочку неравенств, последнее из которых справедливо при* $m \geqslant 2^8$*:*

$$\pi(2m) - \pi(m) = \sum_{m<p\leqslant 2m} 1 \geqslant \frac{\theta(2m) - \theta(m)}{\ln 2m} \geqslant$$

$$\geqslant \frac{m\ln 4}{3\ln 2m} - \frac{\ln\sqrt{4m}}{\ln 2m} - \frac{\sqrt{2m}\ln 4}{\ln 2m} \geqslant \frac{m\ln 4}{3\ln 2m} - 1 - \frac{\sqrt{2m}}{2} = g(m).$$

Покажем, что $f(m) = g(m) - \sqrt{m/2} \geqslant 0$. *Сначала заметим, что*

$$f(2^8) = \frac{2^8\ln 4}{3\ln 2^9} - 1 - \sqrt{2^9} > 2^{11} - 1 - 24 > 0.$$

При $m \geqslant 2^8$ *оценим снизу производную:*

$$f'(m) \geqslant \frac{\ln 4}{3\ln 2m}\left(1 - \frac{\ln 4}{\ln 2m}\right) - \frac{1}{\sqrt{2m}} \geqslant \frac{\ln 4}{4\ln 2m} - \frac{1}{\sqrt{2m}} \geqslant 0.$$

Последнее неравенство эквивалентно следующему:

$$\frac{\sqrt{2m}}{\ln 2m} \geqslant \frac{4}{\ln 4},$$

которое справедливо при $m \geqslant 2^8$ *в силу возрастания функции* $\frac{x}{\ln x}$ *на множестве* $x \geqslant 2$. ◀

Теорема 12 (Теорема П. Л. Чебышева — постулат Бертрана)**.** *При* $x \geqslant 2n^2$ *на отрезке* $[x, 2x]$ *лежит по крайней мере* n *различных простых чисел.*

▶ *Положим* $m = [x] \geqslant 2^8$. *Тогда справедливо следующее теоретико-множественное включение*

$$[m+1, 2m] \subset [x, 2x].$$

Следовательно, все простые числа, лежащие на отрезке $[m+1, 2m]$ *будут принадлежать и отрезку* $[x, 2x]$. *В силу леммы* **??**, *если на отрезке* $[x, 2x]$ *лежат по крайней мере* n *различных простых, то* $\sqrt{x/2} \geqslant \sqrt{m/2} \geqslant n$, *т. е.* $x \geqslant 2n^2$.

Осталось доказать утверждение леммы при $2 \leqslant x < 2^8$. *Разобьем этот промежуток на промежутки вида* $I_n = [2n^2, 2(n+1)^2)$, *где* $1 \leqslant n \leqslant 11$. *С помощью таблиц простых чисел нетрудно проверить, что если* $x \in I_n$, *то на отрезке* $[x, 2x]$ *лежит не менее* n *различных простых чисел.* ◀

§ 4. Задачи

Доказать следующие утверждения.

1. *Для любого натурального* $n > 1$ *сумма*

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$$

не является целым числом.

Указание. *Пусть наивысшая степень 2, не превосходящая* n, *равна* 2^l. *Тогда не существует других чисел от 1 до* n, *которые делятся на* 2^l.

2. *Существует такое вещественное число* $\alpha > 1$, *что если* $\alpha = \alpha_0$, $2\alpha_0 = \alpha_1$, $\ldots$, $2\alpha_n = \alpha_{n+1}$, $\ldots$, *то при всех* $n \in \mathbb{N}$ *числа* $[\alpha_n]$ *будут простыми. Другими словами, найдется такое число* $\alpha > 1$, *что при всех* $n \in \mathbb{N}$ *натуральные числа*

$$p_n = \left[2^{2^{\cdot^{\cdot^{\cdot^{2^{\alpha}}}}}} \right]$$

будут простыми.

3. *Ряд*

$$\sum_p \frac{1}{p(\ln\ln p)^\alpha}$$

сходится тогда и только тогда, когда $\alpha > 1$.

§ 5. Оценка количества простых чисел, не превосходящих любой наперед заданной границы

d. *Здесь мы докажем классическую оценку П. Л. Чебышёва об оценке функции* $\pi(x)$. *Сначала сформулируем и докажем несколько вспомогательных утверждений.*

Лемма 7. *Пусть* $n \geqslant 1$ *и* $\theta(n) = \sum_{p\leqslant n} \ln p$, *где суммирование ведется по простым числам. Тогда справедливо неравенство*

$$\theta(n) \leqslant 4n \ln 2.$$

► *Из разложения бинома* $(1+1)^n$ *получим неравенство*

$$\binom{2n}{n} \leqslant 2^{2n}.$$

Поскольку каждое простое число между n *и* $2n$ *делит биномиальный коэффициент* $\binom{2n}{n}$, *имеем*

$$\theta(2n) - \theta(n) \leqslant 2n \ln 2.$$

В частности, при $n = 2^r$ *справедливо неравенство*

$$\theta(2^{r+1}) - \theta(2^r) \leqslant 2^{r+1} \ln 2.$$

Складывая эти неравенства при $r = 0, 1, 2, \ldots, m$, *находим*

$$\theta(2^{m+1}) \leqslant (2^{m+1} + 2^m + \cdots + 2 + 1) \ln 2 \leqslant 2^{m+2} \ln 2.$$

Далее, для любого натурального n *найдется такое число* m, *что* $2^m \leqslant n < 2^{m+1}$. *Следовательно,*

$$\theta(n) = \theta(2^m) + (\theta(n) - \theta(2^m)) \leqslant 2^{m+1} \ln 2 + (\theta(2^{m+1}) - \theta(2^m)) \leqslant$$

$$\leqslant 2^{m+1} \ln 2 + 2^{m+1} \ln 2 \leqslant 4n \ln 2. \blacktriangleright$$

Лемма 8. *При $n \geqslant 1$ справедливо неравенство $\theta(n) \leqslant 2n \ln 2$.*

► *Проведем индукцию по числу n. Если n не простое число, то по предположению индукции имеем*

$$\theta(n) = \theta(n-1) \leqslant 2(n-1)\ln 2.$$

Если же n нечетное число, то запишем его в виде $n = 2m+1$. Каждое простое число между $m+1$ и $2m+1$ делит биномиальный коэффициент $\binom{2m+1}{m}$. Из формулы бинома вытекает неравенство

$$\binom{2m+1}{m} + \binom{2m+1}{m+1} \leqslant 2^{2m+1}, \quad \text{т. е.} \quad 2\binom{2m+1}{m} \leqslant 2^{2m+1}.$$

Следовательно,

$$\theta(2m+1) - \theta(m) \leqslant 2m \ln 2.$$

Далее, пользуясь предположением индукции $\theta(m) \leqslant 2m \ln 2$, получим

$$\theta(2m+1) \leqslant 4m \ln 2 \leqslant 2(2m+1)\ln 2,$$

что и требовалось доказать. ◄

Лемма 9. *Пусть $x \geqslant 1$, p — простое число и*

$$\psi(x) = \sum_{p^\alpha \leqslant x} \ln p = \sum_{n \leqslant x} \Lambda(n),$$

где $\psi(x)$ — функция Чебышёва и $\Lambda(n)$ — функция Мангольдта,

$$\Lambda(n) = \begin{cases} \ln p, & \text{если} \quad n = p^\alpha, \\ 0, & \text{в противном случае.} \end{cases}$$

Тогда

$$\mathrm{НОК}\,[2, 3, \ldots, n] = e^{\psi(n)}.$$

► *Имеем $НОК\,[2, 3, \ldots, n] = \prod\limits_{p \leqslant n} p^{e_p}$, где показатели e_p определяются из неравенств $p^{e_p} \leqslant n < p^{e_p+1}$. Следовательно,*

$$e_p = \left[\frac{\ln n}{\ln p}\right] = \sum_{\substack{\alpha \\ p^\alpha \leqslant n}} 1,$$

откуда вытекает требуемый результат. ◄

Лемма 10. *При $n \geqslant 1$ имеем $\psi(2n+1) \geqslant 2n \ln 2$.*

► *В силу равенств*

$$I = \int\limits_0^1 x^n (1-x)^n \, dx = \sum_{k=0}^{n} \binom{n}{k} (-1)^k \int\limits_0^1 x^{n+k} \, dx = \sum_{k=0}^{n} \binom{n}{k} \frac{(-1)^k}{n+k+1}$$

произведение $НОК[2, 3, \ldots, 2n+1]\, I$ есть натуральное число, а следовательно, $НОК[2, 3, \ldots, 2n+1]\, I \geqslant 1$. Используя лемму **??**, *получаем $e^{\psi(2n+1)} I \geqslant 1$.*

Далее, для любого x с условием $0 \leqslant x \leqslant 1$ имеем $x(1-x) \leqslant 1/4$, поэтому $I \leqslant 2^{-2n}$. Подставляя эту оценку в предыдущее неравенство, получим $e^{\psi(2n+1)} \geqslant 2^{2n}$, что и требовалось доказать. ◄

Теорема 13. *Существуют такие постоянные $0 < A \leqslant 1 \leqslant B$, что для любого $x \geqslant 2$ справедливы неравенства*

$$\frac{Ax}{\ln x} \leqslant \pi(x) \leqslant \frac{Bx}{\ln x}.$$

► *В силу леммы* **??** *имеем*

$$\frac{1}{2} \ln n (\pi(n) - \pi(\sqrt{n})) \leqslant \theta(n) \leqslant 2n \ln 2.$$

Следовательно,

$$\pi(n) \leqslant 4 \ln 2 \frac{n}{\ln n} + \pi(\sqrt{n}) \leqslant 4 \ln 2 \frac{n}{\ln n} + \sqrt{n} \leqslant \frac{Bn}{\ln n},$$

где $B \leqslant 4 \ln 2 + 2$. Пользуясь леммой **??**, *найдем*

$$\psi(x) \geqslant cx, \quad c > 0.$$

Далее, поскольку $\psi(x) = \theta(x) + O(\sqrt{x} \ln^2 x)$, получим

$$\pi(x) \geqslant \frac{Ax}{\ln x},$$

где $A \geqslant 0{,}6$. ◄

§ 6. Замечание о возможностях метода П. Л. Чебышёва

В этом параграфе мы дадим трактовку рассмотренного ранее метода П. Л. Чебышёва на языке теории рядов Дирихле.

1. *При $b > 0$ справедливо равенство*

$$\frac{1}{2\pi i}\int\limits_{b-i\infty}^{b+i\infty}\frac{a^s}{s}\,ds=\begin{cases}1, & \text{если}\quad a>1,\\ 0, & \text{если}\quad 0<a<1.\end{cases}$$

2. *При $b > 1$ имеем*

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

3. *При $b > 1$, $x \geqslant 1$ имеем*

$$T(x)=\sum_{m\leqslant x}\psi\left(\frac{x}{m}\right)=\frac{1}{2\pi i}\int\limits_{b-i\infty}^{b+i\infty}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\left(\sum_{m\leqslant x}\left(\frac{x}{m}\right)^s\right)\frac{ds}{s}=$$

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

4. *Пусть $f(x) = T(x) - 2T(x/2)$ и $F(s) = -\zeta'(s)g(s)$, где $g(s) = 1 - \frac{2}{2^s}$. Тогда*

$$f(x)=\frac{1}{2\pi i}\int\limits_{b-i\infty}^{b+i\infty}F(s)\frac{x^s}{s}\,ds.$$

5. *Имеет место разложение*

$$g(s)=g(1)+g'(1)(s-1)+\frac{1}{2}g''(1)(s-1)^2+\ldots,$$

где $g(1) = 0$, $g'(1) = \ln 2 = 0,693147\ldots$.

6. *Пользуясь формулой контурного интегрирования, получим*

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

7. *Пусть теперь $f_1(x) = T(x)+T(x/30)-T(x/2)-T(x/3)-T(x/5)$,*

$$F_1(s)=(-\zeta'(s))\left(1-\frac{1}{2^s}-\frac{1}{3^s}-\frac{1}{5^s}+\frac{1}{30^s}\right)=-\zeta'(s)g_1(s).$$

Тогда

$$f_1(x) = \frac{1}{2\pi i} \int\limits_{b-i\infty}^{b+i\infty} F_1(s) \frac{x^s}{s}\, ds.$$

8. *Справедливо разложение*

$$g_1(s) = g_1(1) + g_1'(1)(s-1) + \frac{1}{2} g_1''(1)(s-1)^2 + \dots,$$

где $g_1(1) = 0$, $g_1'(1) = \frac{\ln 2}{2} + \frac{\ln 3}{3} + \frac{\ln 5}{5} - \frac{\ln 30}{30} = \ln \frac{2^{1/2} 3^{1/3} 5^{1/5}}{30^{1/30}} = 0,92129202\dots$.

9. *Справедливо разложение*

$$f_1(x) = \sum_{k=1}^{\infty} A_k \psi\left(\frac{x}{k}\right) = \psi(x) - \psi\left(\frac{x}{6}\right) + \psi\left(\frac{x}{7}\right) - \psi\left(\frac{x}{10}\right) +$$
$$+ \psi\left(\frac{x}{11}\right) - \psi\left(\frac{x}{12}\right) + \psi\left(\frac{x}{13}\right) - \psi\left(\frac{x}{15}\right) + \psi\left(\frac{x}{17}\right) - \psi\left(\frac{x}{18}\right) +$$
$$+ \psi\left(\frac{x}{19}\right) - \psi\left(\frac{x}{20}\right) + \psi\left(\frac{x}{23}\right) - \psi\left(\frac{x}{24}\right) + \psi\left(\frac{x}{29}\right) - \psi\left(\frac{x}{30}\right),$$

где

$$A_k = \begin{cases} 1, & \text{если } k \equiv 1, 7, 11, 13, 17, 19, 23, 29 \pmod{30}, \\ 0, & \text{если } k \equiv 2, 3, 4, 5, 8, 9, 14, 16, 21, 22, 25, 26, 27, 28 \pmod{30}, \\ -1, & \text{если } k \equiv 6, 10, 12, 15, 18, 20, 24, 30 \pmod{30}. \end{cases}$$

10. *Пользуясь формулой контурного интегрирования, получим*

$$f_1(x) = \sum_{1 \leqslant n \leqslant x} A_n \psi\left(\frac{x}{n}\right) = x \ln \frac{2^{1/2} 3^{1/3} 5^{1/5}}{30^{1/30}} + o(x).$$

11. *С другой стороны, при* $x \geqslant 2$ *получим*

$$\psi(x) - \psi(x/6) \leqslant f_1(x) \leqslant \psi(x) - \psi(x/6) + \psi(x/7).$$

Отсюда следует, что

$$0{,}92 \frac{x}{\ln x} \leqslant \pi(x) \leqslant 1{,}05 \frac{x}{\ln x}.$$

12. *Таким образом, задача состоит в том, чтобы составить такую линейную комбинацию* $T(x/n)$, *чтобы получился знакочередующийся ряд* $\sum\limits_{k \geqslant 1} B_k \psi(x/k)$ *с условием* $B_k = 0$ *при* $2 \leqslant k \leqslant k_0$. *Ясно, что* $k_0 \ll \ln x$, *но чем ближе к этой границе удастся подойти, тем точнее будут получаться оценки.*

§ 7. Теорема П. Л. Чебышёва о наилучшем приближении функции $\pi(x)$

а. *В настоящем параграфе в предположении существовании асимптотики функции* $\pi(x)$ *при* $x \to \infty$ *показано, что она имеет вид* $\pi(x) \sim \frac{x}{\ln x}$.

Лемма 11. *При* $x \to \infty$ *имеем*

$$T(x) = \sum_{n \leqslant x} \ln n = x \ln x - x + \rho(x) \ln x + c + O(1/x),$$

где $\rho(x) = 1/2 - \{x\}$ *и* c *— некоторая постоянная.*

► *Воспользуемся формулой суммирования Эйлера (см. [?]). Имеем*

$$\sum_{1/2 < n \leqslant x} \ln n = \int\limits_{1/2}^{x} \ln t \; dt + \rho(x) \ln x - \rho(1/2) \ln 1/2 - \int\limits_{1/2}^{x} \frac{\rho(t)dt}{t}.$$

Далее находим

$$\int\limits_{1/2}^{x} \ln t \; dt = x \ln x - x - 1/2 \ln (1/2) + 1/2.$$

Разбивая промежуток интегрирования $[x, \infty)$ *на промежутки длины* $1/2$, *получим знакочередующийся ряд с общим членом, стремящимся к нулю, последовательность модулей членов которого убывает, поэтому*

$$\int\limits_{1/2}^{x} \frac{\rho(t)dt}{t} = \int\limits_{1/2}^{\infty} \frac{\rho(t)dt}{t} + R,$$

где $R = \int\limits_{x_1}^{x_2} \frac{\rho(t)dt}{t} \ll \frac{1}{x}$ *при некоторых числах* x_1, x_2, *удовлетворяющих условиям* $x_1 \geqslant x, x_2 \geqslant x$ *и* $|x_1 - x_2| \leqslant 1/2$, *что и завершает доказательство.* ◄

Лемма 12. *При* $x \to \infty$ *справедливы следующие асимптотические формулы:*
1) $\sum\limits_{n \leqslant x} \frac{\Lambda(n)}{n} = \ln x + O(1)$, *где* $\Lambda(n)$ *— функция Мангольдта;*

2) $\sum\limits_{p\leqslant x}\frac{\ln p}{p}=\ln x+O(1)$, *где* p *пробегает последовательные простые числа.*

► *1) Имеем*

$$T(x)=\sum_{d\leqslant x}\Lambda(d)\left[\frac{x}{d}\right]=x\sum_{d\leqslant x}\frac{\Lambda(d)}{d}+O(\psi(x)).$$

Используя асимптотику леммы **??** *и оценку* $\psi(x)\ll x$, *получим требуемую формулу.*

2) Поскольку

$$\sum_{p\leqslant x}\frac{\ln p}{p}=\sum_{n\leqslant x}\frac{\Lambda(n)}{n}-\sum_{\substack{p^r\leqslant x\\ r\geqslant 2}}\frac{\ln p}{p^r}=S_1-S_2.$$

В силу 1) имеем $S_1=\ln x+O(1)$, *а для величины* S_2 *имеем оценку сверху*

$$S_2\ll\sum_{d=1}^{\infty}\frac{\ln d}{d^2}\ll 1,$$

что и доказывает справедливость формулы 2).◄

Лемма 13. *При* $x\to\infty$ *имеем*

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

► *Используя асимптотику*

$$S_0(x)=\sum_{p\leqslant x}\frac{\ln p}{p}=\ln x+O(1),$$

полученную в предыдущей лемме, с помощью преобразования Абеля (см. **[?]***) найдем*

$$S=\sum_{p\leqslant x}\frac{\ln p}{p}\cdot\frac{1}{\ln p}=\frac{S_0(x)}{\ln x}+\int\limits_1^x\frac{S_0(t)}{t\ln^2 t}\,dt=$$

$$=\int\limits_1^x\frac{\ln t+O(1)}{t\ln^2 t}\,dt+O(1)=\ln\ln x+O(1).\ \blacktriangleleft$$

Теорема 14. *Пусть при* $x \to \infty$

$$\pi(x) \sim \alpha \frac{x}{\ln x}.$$

Тогда при $x \to \infty$

$$S(x) = \sum_{p \leqslant x} \frac{1}{p} \sim \alpha \ln \ln x.$$

Более того, $\alpha = 1$.

►

► Положим $y = \ln \ln x$. Представим $S(x) = S(y) + S_1(x, y)$. Тогда

$$S(y) \ll \frac{y}{\ln y} = o(\ln \ln x).$$

К сумме $S_1(x, y)$ применим преобразование Абеля в интегральной форме (см. [**?**]). Получим

$$S_1(x, y) = \sum_{y < p \leqslant x} \frac{1}{p} = \frac{\pi(x) - \pi(y)}{x} + \int_y^x \frac{\pi(t) - \pi(y)}{t^2}\, dt =$$

$$= \alpha \ln \ln x + o(\ln \ln x).$$

Согласно лемме **??**,

$$S(x) = \sum_{p \leqslant x} \frac{1}{p} \sim \ln \ln x.$$

Следовательно, если асимптотика для функции $\pi(x)$ в условии теоремы имеет место, то $\alpha = 1$. ◄

Глава III

КЛАССЫ ВЫЧЕТОВ И СРАВНЕНИЯ ПО МОДУЛЮ НАТУРАЛЬНОГО ЧИСЛА

К. Ф. Гаусс в «Арифметических исследованиях» ввел понятие сравнимости для целых чисел, имеющих одинаковые остатки при делении на натуральное число m.

Целые числа a и b называются *сравнимыми по модулю* m, если разность $a-b$ делится на m. Натуральное число m называется *модулем сравнения.* Этот факт записывается следующим образом:

$$a \equiv b \pmod{m}.$$

Символ $\equiv$ читается так: *сравнимо с.* Само соотношение между числами a и b называется *сравнением по модулю* m. В случае, если разность $a-b$ не делится на m, то a и b называются *несравнимыми по модулю* m, что записывается так:

$$a \not\equiv b \pmod{m}.$$

§ 1. Основные свойства сравнений

Из определения легко вывести следующие основные свойства сравнений.

$\mathbf{1}^0$. Целые числа a и b сравнимы по модулю m тогда и только тогда, когда они имеют равные остатки при делении на m.

► *Необходимость.* Разделим числа a и b на m с остатком. Тогда найдутся единственные пары целых чисел q_1, r_1 и q_2, r_2 с условиями

$$a = mq_1 + r_1, \quad 0 \leqslant r_1 < m; \quad b = mq_2 + r_2, \quad 0 \leqslant r_2 < m.$$

Без ограничения общности можно считать, что $r_1 \geqslant r_2$. Из предыдущих равенств имеем

$$a - b = m(q_1 - q_2) + (r_1 - r_2) = mq + r, \quad 0 \leqslant r < m.$$

Это означает, что $r = r_1 - r_2$ будет остатком от деления $a-b$ на m. По условию $a-b$ делится на m. Следовательно, $r = 0$ и $r_1 = r_2$. Необходимость доказана.

Достаточность. Если остатки r_1 и r_2 при делении a и b на m равны между собой, т. е. $r_1 = r_2$, то разность $a - b$ делится на m. ◀

Числа, сравнимые по заданному модулю, называются также *равноостаточными* по этому модулю.

2^0. Сравнимость по любому заданному модулю является отношением эквивалентности. Это означает, что выполняются следующие свойства.

а) $a \equiv a \pmod m$ (*рефлексивность*), так как $a - a = 0$ делится на m.

б) Если $a \equiv b \pmod m$, то $b \equiv a \pmod m$ (*симметричность*). В самом деле, по определению имеем $a - b = mq$. Следовательно, $b - a = m(-q)$, т. е. $b \equiv a \pmod m$.

в) Если $a \equiv b \pmod m$, $b \equiv c \pmod m$, то $a \equiv c \pmod m$ (*транзитивность*). Действительно, по условию $a - b = mq_1$, $b - c = mq_2$. Отсюда имеем $a - c = m(q_1 + q_2)$, т. е. $a \equiv c \pmod m$.

Указанное отношение эквивалентности позволяет разбить все целые числа на классы чисел, сравнимых между собой по заданному модулю. Полученные классы эквивалентности по отношению сравнимости называются *классами вычетов по заданному модулю* m. По свойству 1^0 каждый класс вычетов будет состоять только из равноостаточных чисел. Следовательно, с возможными m разными остатками при делении чисел на m связываются m классов вычетов. Система целых чисел, состоящая из m представителей различных классов вычетов называется *полной системой вычетов по модулю* m. При этом $0,\ 1, \ldots, m-1$ — полная система вычетов по модулю m, называемая *наименьшей системой вычетов по модулю* m.

Перейдем к свойствам сравнений, связанными с арифметическими операциями.

3^0. Если $a \equiv b \pmod m$, $c \equiv d \pmod m$, то $a \pm c \equiv b \pm d \pmod m$.

▶ По условию справедливы равенства $a - b = mq_1$, $c - d = mq_2$. Следовательно, $(a \pm c) - (b \pm d) = m(q_1 + q_2)$. ◀

4^0. Если $a \equiv b \pmod m$, $c \equiv d \pmod m$, то $ac \equiv bd \pmod m$.

▶ По условию имеем $a - b = mq_1$, $c - d = mq_2$. Следовательно, $ac - bd = m(dq_1 + bq_2 + q_1q_2m)$. ◀

В частности, если $a \equiv b \pmod m$, то $ac \equiv bc \pmod m$ и $a^n \equiv b^n \pmod m$ для любого натурального числа n. Отсюда следует, что для любого многочлена $P(x)$ с целыми коэффициентами при $a \equiv b \pmod m$ справедливо сравнение $P(a) \equiv P(b) \pmod m$.

Заметим, что множество классов вычетов по заданному модулю в силу свойств 3^0 и 4^0 является замкнутым относительно операций сложения, вычитания и умножения. Следовательно, оно образует кольцо $\mathbb{Z}_m$, которое называется *кольцом классов вычетов по заданному модулю.*

Деление в кольце классов вычетов по модулю m не всегда возможно. Тем не менее, имеет место следующее свойство.

5^0. Если $ac \equiv bc \pmod m$ и $(c, m) = 1$, то $a \equiv b \pmod m$.

► По условию имеем $c(a-b) = mq,\ (c, m) = 1$. Отсюда вытекает равенство $a - b = mq_1$, где $q_1 = q/c$. ◄

Более того, справедливо и такое утверждение.

6^0. Если $ac \equiv bc \pmod m$ и $(c, m) = d$, то $a \equiv b \pmod{\frac{m}{d}}$.

► По условию $c(a-b) = mq,\ c = c_1 d,\ m = m_1 d$. Отсюда получим равенство $a - b = m_1 q_1$, где $q_1 = q/c_1$, т. е. $a \equiv b \pmod{m_1}$. ◄

Часто полезно следующее утверждение.

7^0. Пусть числа m и n взаимно просты, x пробегает полную систему вычетов по модулю n и y пробегает полную систему вычетов по модулю m. Тогда mn чисел

$$mx + ny$$

образуют полную систему вычетов по модулю mn.

► Достаточно доказать, что числа $mx+ny$ несравнимы по модулю mn при различных наборах x, y из указанных систем сравнений по модулям n и m соответственно. Пусть

$$mx + ny \equiv mx' + ny' \pmod{mn}.$$

Отсюда имеем сравнения $mx \equiv mx' \pmod n$ и $ny \equiv ny' \pmod m$. Далее, в силу условия $(m, n) = 1$ получим $x \equiv x' \pmod n,\ y \equiv y' \pmod m$. ►

Докажем еще одно полезное свойство сравнений.

8^0. Пусть целые числа a и b принадлежат одному и тому же классу вычетов по модулю m. Тогда $(a, m) = (b, m)$. Другими словами, для чисел a и b из одного класса вычетов по модулю m их наибольший общий делитель с модулем m будет один и тот же.

► Пусть $d_1 = (a, m),\ d_2 = (b, m)$. Тогда из условий $a - b = mq$ и $d_1 \mid a,\ d_1 \mid m$ имеем, что $d_1 \mid b$. Следовательно, $d_1 \mid d_2 = (b, m)$. Если поменяем местами d_1 на d_2 и a на b, то получим $d_2 \mid d_1$. Значит, $d_1 = d_2$. ◄

Если $(a, m) = 1$, то класс вычетов по модулю m, содержащий число a, называется *классом вычетов, взаимно простых с модулем* m. Совокупность всех классов вычетов, взаимно простых с модулем m, называется *приведенной системой вычетов по модулю* m. Она состоит из $\varphi(m)$ классов вычетов по модулю m и обозначается через $\mathbb{Z}_m^*$.

9^0. Пусть числа m и n взаимно просты, ξ пробегает приведенную систему вычетов по модулю n и η пробегает приведенную систему вычетов по модулю m. Тогда $\varphi(mn)$ чисел

$$m\xi + n\eta$$

образуют приведенную систему вычетов по модулю mn.

► Исходя из свойства 7^0, достаточно доказать, что $(m\xi + n\eta, mn) = 1$. Действительно, поскольку $(m, n) = (\xi, n) = (\eta, m) = 1$, получим

$$(m\xi + n\eta, m) = (n\eta, m) = 1, \quad (m\xi + n\eta, n) = (m\xi, n) = 1.$$

Следовательно, $(m\xi + n\eta, mn) = 1$.

◄

§ 2. Задачи

1. Пусть x пробегает полную систему вычетов по модулю m и $(a, m) = 1$. Тогда для любого целого b числа $ax + b$ пробегают полную систему вычетов по модулю m.

2. Пусть ξ пробегает приведенную систему вычетов по модулю m и $(a, m) = 1$. Тогда числа $a\xi$ пробегают приведенную систему вычетов по модулю m.

3. Пусть $m^a \equiv 1 \pmod{k}$, $m^b \equiv 1 \pmod{k}$. Тогда $m^{(a,b)} \equiv 1 \pmod{k}$.

4. Пусть n — натуральное и p — простое число. Тогда справедливы сравнения $C_{p-1}^n \equiv (-1)^n \pmod{p}$ и $C_{p-2}^n \equiv (-1)^n(n+1) \pmod{p}$.

5. Пусть m — натуральное и p — простое число. Тогда

$$\sum_{x=1}^{p-1} x^m \equiv \begin{cases} -1 \pmod{p}, & \text{если } (p-1) \mid m; \\ 0 \pmod{p}, & \text{если } (p-1) \nmid m. \end{cases}$$

6. Пусть p — простое число. Тогда

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv \begin{cases} 1 \pmod p, & \text{если } p \equiv 3 \pmod 4; \\ -1 \pmod p, & \text{если } p \equiv 1 \pmod 4. \end{cases}$$

§ 3. Сравнения первой степени

Перейдем к задаче о разрешимости сравнений первой степени по модулю m. Класс вычетов x_0 по модулю m называется *решением сравнения* $ax \equiv b \pmod m$, если выполняется сравнение $ax_0 \equiv b \pmod m$.

Если x пробегает полную систему вычетов по модулю m, то при $(a, m) = 1$ числа $ax - b$ пробегают полную систему вычетов по модулю m. Следовательно, существует единственное решение x_0 сравнения $ax_0 - b \equiv 0 \pmod m$. Это и доказывает следующее утверждение.

1^0. Пусть $(a, m) = 1$. Тогда сравнение

$$ax \equiv b \pmod m$$

имеет единственное решение.

Дадим другое доказательство этого свойства.

► Сначала установим существование решения сравнения. Поскольку $(a, m) = 1$, найдутся такие целые числа x, y, что $ax + my = 1$. Следовательно, $au + mv = b$, $u = bx$, $v = by$. Это означает, что для любого b существует решение сравнения $au \equiv b \pmod m$.

Докажем теперь единственность такого решения. Предположим, что существует еще одно решение $au' \equiv b \pmod m$. Тогда имеет место сравнение $a(u - u') \equiv 0 \pmod m$. Так как $(a, m) = 1$, в силу свойства 5^0 из § 1 получим $u \equiv u' \pmod m$. Значит, данное сравнение имеет единственное решение. ◄

Докажем теперь более общее утверждение.

2^0. Пусть $(a, m) = d$. Для того, чтобы сравнение

$$ax \equiv b \pmod m$$

было разрешимо, необходимо и достаточно, чтобы выполнялось условие

$$b \equiv 0 \pmod d.$$

При выполнении последнего условия сравнение $ax \equiv b \pmod m$ имеет в точности d решений, которые входят в один класс по модулю $\frac{m}{d}$.

► В силу свойства 8^0 из § 1 для разрешимости рассматриваемого сравнения необходимо и достаточно, чтобы $d \mid b$. Далее, пусть $b \equiv 0 \pmod{d}$. Представим числа a, b, m в виде $a = a_0 d,\ b = b_0 d,\ m = m_0 d$. Тогда сравнение $ax \equiv b \pmod{m}$ эквивалентно сравнению $a_0 x \equiv b_0 \pmod{m_0}$ с условием $(a_0, m_0) = 1$. Последнее сравнение согласно свойству 1^0 имеет по модулю m_0 единственное решение x_0. Следовательно, данному сравнению удовлетворяют все целые числа вида $x_0 + y m_0$, где y — любое целое число, и только они. Эти числа образуют по модулю m в точности d классов вычетов:

$$x \equiv x_0,\ x_0 + m_0,\ x_0 + 2m_0, \ldots, x_0 + (d-1)m_0.$$

Они и дают все решения сравнения $ax \equiv b \pmod{m}$. ►

Пример 1. Линейное сравнение

$$12x \equiv 3 \pmod{21}$$

имеет $(3, 21) = 3$ решения (в силу 2^0). Сравнение $4x \equiv 1 \pmod{7}$ имеет решение $x_0 \equiv 2 \pmod{7}$. Используя свойство 2^0, получим, что

$$x \equiv 2, 9, 16$$

являются решениями первоначального сравнения.

3^0. Пусть $(a, m) = (b, m) = 1$. Тогда сравнение

$$ax \equiv b \pmod{m}$$

имеет единственное решение в приведенной системе вычетов по модулю m.

► По свойству 1^0 имеется единственное решение рассматриваемого сравнения в полной системе вычетов по модулю m, а по свойству 8^0 из § 1 справедливы равенства $(ax, m) = (b, m) = 1$. Следовательно, $(x, m) = 1$. ◄

§ 4. Теорема Эйлера

В предыдущем параграфе установлено, что приведенная система вычетов $\mathbb{Z}_m^*$ по модулю m относительно операции умножения является конечной группой порядка $\varphi(m)$. Из теоремы П. Лагранжа о том, что порядок подгруппы делит порядок конечной группы следует, что порядок подгруппы степеней числа a, взаимно простого с

модулем m, делит порядок группы $\varphi(m)$. Тем самым установлено следующее утверждение, называемое *теоремой Л. Эйлера.*

1^0. Пусть $a, m > 1$ — натуральные числа и $(a, m) = 1$. Тогда выполняется сравнение

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

Дадим другое доказательство этой теоремы.

► Положим $n = \varphi(m)$. Пусть $a_1, \ldots, a_n$ — приведенная система вычетов по модулю m. Тогда в силу условия $(a, m) = 1$ числа $aa_1, \ldots, aa_n$ также пробегают приведенную систему вычетов. Следовательно,

$$aa_1 \cdot aa_2 \ldots aa_n \equiv a_1 \cdot a_2 \ldots a_n \pmod{m}.$$

Поскольку $(a_1 a_2 \ldots a_n, m) = 1$, используя свойство 5^0 из § 1, разделив это сравнение на $a_1 a_2 \ldots a_n$, получим

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

Утверждение доказано. ◄

Теорема Эйлера обобщает следующую *малую теорему П. Ферма.*

2^0. Пусть p — простое число и a — целое число, не делящееся на p. Тогда справедливо сравнение

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

Приведем другое доказательство этой теоремы.

► Достаточно доказать, что при $a = 0,\ 1,\ 2, \ldots, p-1$ имеет место сравнение

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

Докажем его методом математической индукции. При $a = 1$ сравнение очевидно. Предположим, что оно выполняется при $a = b$, т. е. $b^p \equiv b \pmod{p}$. Докажем его справедливость при $a = b + 1$. Имеем цепочку сравнений

$$(b+1)^p = b^p + 1 + \sum_{n=1}^{p-1} \binom{p}{n} b^n \equiv b^p + 1 \equiv b + 1 \pmod{p},$$

поскольку для любого n, $1 \leqslant n < p$, биномиальный коэффициент

$$\binom{p}{n} = \frac{p(p-1)\dots(p-n+1)}{n!}$$

делится на p.

◀

Примеры. 1. Пусть $m = 8$. Тогда $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$. Следовательно, для любого нечетного числа a справедливо сравнение $a^2 \equiv 1 \pmod 8$. Таким образом, все числа, взаимно простые с 8, имеют порядок 2, что меньше $4 = \varphi(8)$ из теоремы Эйлера.

2. Пусть p — простое число. Тогда если $a^{p-1} \equiv 1 \pmod{p^2}$, то a называется *решением Ферма* для p. Известно, что если для нечетного простого числа p существуют такие целые числа x, y, z, что $x^p + y^p + z^p = 0$, $(xyz, p) = 1$, то $2^{p-1} \equiv 1 \pmod{p^2}$. Число 3 — решение Ферма для 11. Действительно, имеем

$$3^5 = 243 \equiv 1 \pmod{11^2}, \quad \text{так что} \quad 3^{10} \equiv 1 \pmod{11^2}.$$

Число 2 — решение Ферма для 1093. Положим $p = 1093$. Тогда $p - 1 = 1092 = 2^2 \cdot 3 \cdot 7 \cdot 13$. Имеем $3^7 = 2187 = 2p + 1$, так что

$$3^{14} \equiv 4p + 1 \pmod{p^2}. \tag{3.1}$$

Далее получим $2^{14} = 16384 = 15p - 11$. Следовательно,

$$2^{28} \equiv -330p + 121 \pmod{p^2},$$

$$3^2 \cdot 2^{28} \equiv 310p - 4 \pmod{p^2},$$

$$3^2 \cdot 2^{28} \cdot 7 \equiv -16p - 28 \pmod{p^2}.$$

Таким образом,

$$3^2 \cdot 2^{26} \cdot 7 \equiv -4p - 7 \pmod{p^2}.$$

Согласно формуле бинома Ньютона справедливы сравнения

$$3^{14} \cdot 2^{182} \cdot 7^7 \equiv (-4p - 7)^7 \equiv -7 \cdot 4p \cdot 7^6 - 7^7 \pmod{p^2},$$

так что

$$3^{14} \cdot 2^{182} \equiv -4p - 1 \pmod{p^2}.$$

Учитывая (**??**), получим

$$2^{182} \equiv -1 \pmod{p^2}.$$

Возводя последнее сравнение в шестую степень, имеем искомое сравнение

$$2^{1092} \equiv 1 \pmod{p^2}.$$

Отметим также, что свойство 3^0 из § 2 влечет существование обратного элемента для любого взаимно простого вычета по модулю m. Если мы положим $m = p$, где p — простое число, то всякий вычет из полной системы вычетов, отличный от нулевого, будет взаимно простым по модулю p. Следовательно, ненулевые вычеты по модулю p будут обратимы. Значит, множество $\mathbb{Z}_p$ является *полем.*

§ 5. Задачи

1. Сравнение $f(x) = x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod{p}$, $n < p$, p — простое, имеет n корней тогда и только тогда, когда $f(x) \mid (x^p - x)$ в $\mathbb{Z}[x]$.

2. Пусть $d = \left(\frac{a^n - b^n}{a-b}, a - b\right)$. Тогда $d \mid n$.

§ 6. Китайская теорема об остатках

Следующее утверждение называется *китайской теоремой об остатках.* Она была известна древнекитайскому математику Сун Цзе (около 250 г. до Р. Х.).

1^0. Пусть целые числа $m_1, m_2, \ldots, m_r$ попарно взаимно просты и $M = m_1m_2 \ldots m_r$. Тогда система сравнений

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \ldots, \quad x \equiv a_r \pmod{m_r}$$

имеет единственное решение $a \pmod{M}$, т. е. можно указать в точности один класс вычетов $x \equiv a \pmod{M}$, удовлетворяющий этой системе сравнений.

► Положим $M = m_sM_s$, $s = 1, \ldots, r$. Числа $M_1, \ldots, M_r$ в совокупности взаимно просты. Следовательно, найдутся такие целые числа $N_1, \ldots, N_r$, что

$$N_1M_1 + \ldots + N_rM_r = 1.$$

Отсюда при $s = 1, \ldots, r$ имеем

$$e_s = N_s M_s \equiv \begin{cases} 1 \pmod{m_s}, & \text{если } t = s; \\ 0 \pmod{m_t}, & \text{если } t \neq s. \end{cases}$$

Последние сравнения позволяют записать решение исходной системы сравнений в виде

$$x \equiv a_1 e_1 + a_2 e_2 + \ldots + a_r e_r \pmod{M}.$$

Пусть $y \bmod M$ — любое другое решение системы сравнений. Тогда $x - y$ будет делиться на m_s при всех $s = 1, \ldots, r$. Следовательно, $x \equiv y \pmod{M}$. ◀

Пример. Решить систему сравнений

$$x \equiv 2 \pmod 3, \quad x \equiv 1 \pmod 4, \quad x \equiv 3 \pmod 7.$$

▶ Положим $M = 84 = 3 \cdot 4 \cdot 7$, $M_1 = 28$, $M_2 = 21$, $M_3 = 12$. Уравнение

$$28N_1 + 21N_2 + 12N_3 = 1$$

имеет решение $N_1 = -2$, $N_2 = 1$, $N_3 = 3$. Следовательно,

$$x \equiv 2 \cdot (-2) \cdot 28 + 1 \cdot 1 \cdot 21 + 3 \cdot 3 \cdot 12 \equiv 17 \pmod{84}$$

является решением искомой системы сравнений. ◀

§ 7. Приложение к криптографии

В настоящем приложении мы остановимся только на вопросе передачи информации по общедоступному (открытому) каналу связи в преобразованном некоторым образом виде так, чтобы восстановление сообщения было возможно только тому абоненту, которому оно направлено, т. е. законному пользователю. Процесс такого преобразования, т. е. взаимно-однозначного отображения информации, называется процессом шифрования. Обратный процесс восстановления защищаемой информации по шифрованному сообщению называется процессом дешифрования.

Так, например, в I веке по Р. Х. во время войны с галлами Ю. Цезарь пользовался шифром, определяемым функцией $f = f_k$ типа

$$f : x \to x + k \pmod{n},$$

где k, n — некоторые натуральные числа. Здесь при фиксированном n семейство шифрующих отображений $f = f_k$ задается определенным алгоритмом для всего семейства и множеством значений параметров. Множество значений параметров называется *ключом шифрования.* В данном примере такое множество образуют значения параметра k.

Процесс дешифрования задается обратным отображением

$$g : y \to y - k \pmod{n},$$

где для расшифровки следует положить $y \equiv x + k \pmod{n}$, причем в сравнениях по модулю n рассматриваются представители полной системы вычетов: $1, 2, \ldots, n$. Этот процесс так же, как и шифрование, требует наличия некоторого общего алгоритма и ключа дешифрования. В рассматриваемом примере алгоритм дешифрования совпадает с алгоритмом шифрования, а ключ дешифрования задается множеством значений параметра $(-k)$.

Как правило, алгоритмы шифрования и дешифрования, по крайней мере в общем виде, известны, а в тайне держатся только ключи, которые поэтому называются «секретными ключами».

В 1976 г. У. Диффи и М. Хеллман создали новый тип криптосистем с «открытым ключом». Они основаны на следующем принципе: значения шифрующей функции f легко вычисляются, если известны ключи шифрования, в то время, как вычисление значений обратной функции f^{-1}, т. е. дешифрующей функции, является очень сложной задачей. Этот тип криптосистем позволяет очень большому количеству абонентов обмениваться секретной информацией без предварительного согласования и без взаимной проверки, поскольку все необходимые данные для пересылки шифрованной информации находятся в открытом доступе для всех желающих.

В современной теории шифрования обычно имеют дело с большими массивами цифровой информации, записанной в определенной системе счисления, поэтому проблема цифрового шифрования очень актуальна. Сначала остановимся на известных криптосистемах в открытом канале связи (см. [**?**], [**?**], [**?**], [**?**], [**?**], [**?**], [**?**], [**?**], [**?**], [**?**], [**?**]). Здесь возможны три типа задач в соответствии с тем, является ли секретным или открытым абонент и по какому ключу — секретному или открытому — он передает информацию (четвертый тип задач, когда абонент открыт и передача информации идет по открытому ключу обычно исключается из рассмотрения). Для

решения этих задач нам понадобится следующее понятие *односторонней функции.*

Пусть числовая функция $f(x)$ определена на конечном числовом множестве X и для всякого $x \in X$ существует обратная функция $g(y)$, $g(f(x)) \equiv x$, причем вычисление функции $f(x)$ в некотором определенном смысле имеет «малую» сложность, а вычисление функции $g(y)$ имеет в определенном смысле «большую» сложность.

Ниже в качестве односторонней функции рассматривается показательная функция в классах вычетов по простому модулю, а обратной к ней является функция индекса по простому модулю (ей присвоено также и другое название — дискретный логарифм).

1^0. Криптосистема без передачи ключей

А. Шамир первым предложил шифр для обмена секретной информацией по открытому каналу связи без передачи ключей.

Пусть в секретной переписке участвуют абоненты $A, B, C, \ldots$. Для этого они выбирают достаточно большое простое число p, такое, что число $\varphi(p) = p - 1$ имеет удобное для дальнейших действий разложение на простые сомножители. Например, оно является бесквадратным, т. е. не делится ни на какой квадрат натурального числа, больший единицы. Простые числа, обладающие таким свойством, называются *евклидовыми.* Доля евклидовых чисел, не превосходящих x, по отношению к количеству всех простых чисел, не превосходящих x, при $x \to \infty$ асимптотически равна

$$\prod_p \left(1 - \frac{1}{p^2 - p}\right) = 0,39\ldots,$$

где в бесконечном произведении участвуют все простые числа p.

Далее, абоненты $A, B, C, \ldots$ произвольным образом выбирают секретные ключи $a, b, c, \ldots$, соответственно, известные каждому из них в отдельности, удовлетворяющие условиям $1 < a, b, c, \ldots < p-1$, причем каждый ключ взаимно прост с числом $p - 1$. Затем все абоненты находят для себя по второму ключу $\alpha, \beta, \gamma, \ldots$, соответственно, по следующему правилу

$$a\alpha \equiv 1 \pmod{(p-1)},\ b\beta \equiv 1 \pmod{(p-1)},\ c\gamma \equiv 1 \pmod{(p-1)},\ \ldots.$$

Итак, абонент A имеет секретные ключи a, α, абонент B — секретные ключи b, β и т. д.

Пусть, теперь, абонент A посылает сообщение m, $1 \leqslant m \leqslant p-1$, абоненту B. Он зашифровывает его с помощью ключа a следующим

образом

$$m_1 \equiv m^a \pmod{p}, \quad 1 \leqslant m_1 < p,$$

и отправляет абоненту B сообщение m_1. Абонент B зашифровывает это сообщение m_1 с помощью ключа b,

$$m_2 \equiv m_1^b \pmod{p}, \quad 1 \leqslant m_2 < p,$$

и пересылает сообщение m_2 абоненту A. Далее A шифрует сообщение m_2 с помощью ключа α,

$$m_3 \equiv m_2^\alpha \pmod{p}, \quad 1 \leqslant m_3 < p,$$

и пересылает сообщение m_3 абоненту B. Тот шифрует это сообщение с помощью ключа β,

$$m_4 \equiv m_3^\beta \pmod{p}, \quad 1 \leqslant m_4 < p,$$

и получает, что $m_4 \equiv m \pmod{p}$. Действительно,

$$m_4 \equiv m^k \pmod{p},$$

где

$$k \equiv ab\alpha\beta \equiv 1 \pmod{p-1}, \quad p-1 = \varphi(p),$$

т. е. имеем $m_4 \equiv m \pmod{p}$, поэтому в силу условия $1 \leqslant m, m_4 < p$ получаем $m = m_4$.

2^0. Криптосистема Диффи—Хеллмана по простому модулю с открытым ключом

Первую криптосистему с открытым ключом предложили в 1976 г. У. Диффи и М. Хеллман [**?**]. Для защиты информации в системах с большим количеством абонентов она позволила избавиться от трудной задачи обеспечения каждого из них секретными ключами в количестве, сравнимом с количеством абонентов. Опишем криптосистему Диффи—Хеллмана.

Пусть, как и раньше, в секретной переписке участвуют абоненты $A, B, C, \ldots$. Выбираются большое простое число p и первообразный корень g, $1 < g < p-1$, по модулю этого числа. Числа p и g доступны всем желающим.

Затем абоненты $A, B, C, \ldots$ выбирают в качестве секретных ключей большие (в определенном смысле) числа $a, b, c, \ldots$, для

которых $\sqrt{p} < a, b, c, \cdots < p-1$. По секретным ключам каждый абонент строит открытые (доступные всем желающим) ключи $\alpha, \beta, \gamma, \ldots$, соответственно, с условиями $1 < \alpha, \beta, \gamma, \ldots < p-1$, такие, что

$$\alpha \equiv g^a \pmod{p}, \quad \beta \equiv g^b \pmod{p}, \quad \gamma \equiv g^c \pmod{p}, \quad \ldots.$$

Пусть абонент A проводит сеанс связи с абонентом B. По открытому ключу β абонента B и своему секретному ключу a он вычисляет число

$$Z(A,B) \equiv \beta^a \pmod{p}, \quad 1 \leqslant Z(A,B) < p.$$

Аналогично абонент B вычисляет число

$$Z(B,A) \equiv \alpha^b \pmod{p}, \quad 1 \leqslant Z(B,A) < p.$$

При этом справедливо равенство $Z = Z(A,B) = Z(B,A)$. Действительно, имеем

$$Z(A,B) \equiv \beta^a \equiv (g^b)^a \equiv g^{ab} \equiv \alpha^b \equiv Z(B,A) \pmod{p}.$$

Из этих сравнений и условия $1 \leqslant Z(A,B), Z(B,A) < p$ следует искомое равенство $Z(A,B) = Z(B,A)$.

Таким образом абоненты A и B получили одно число Z, которое они могут принять за секретный ключ для дальнейшего шифрования цифровой информации.

3^0. Аналог криптосистемы Диффи—Хеллмана по составному модулю с открытым ключом

З. Шмуели [?], К. С. МакКерли [?] и М. И. Анохин [?] построили криптосистему типа Диффи—Хеллмана по составному модулю n, который является произведением двух различных нечетных простых чисел.

Протокол этой схемы предполагает сначала выработку абонентами A и B общего секретного ключа. Этот предварительный этап состоит из следующих шагов.

Шаг 1. Выбор различных больших простых чисел p и q и вычисление их произведения $n = pq$.

Шаг 2. Выбор вычета g нечетного порядка в приведенной системе вычетов по модулю n. Например, если $p-1 = 2^\alpha p_1, (p_1, 2) = 1$ и $q-1 = 2^\beta q_1, (q_1, 2) = 1$, то, взяв первообразные корни h и l по

модулям p и q соответственно, найдем g по китайской теореме об остатках из системы сравнений

$$\begin{cases} g \equiv h^{2^\alpha} \pmod{p}, \\ g \equiv l^{2^\beta} \pmod{q}. \end{cases}$$

Шаг 3. Числа n и g абоненты A и B представляют в справочник, доступный для всех желающих, при этом сохраняя в секрете числа p и q.

Приведем протокол сеанса связи абонентов A и B.

Шаг 1. Абонент A выбирает секретное сообщение a, причем $1 \leqslant a < \varphi(n)$, $(a, \varphi(n)) = 1$, затем вычисляет $s \equiv g^a \pmod{n}$ и посылает сообщение s абоненту B.

Шаг 2. Абонент B выбирает секретное сообщение b, причем $1 \leqslant b < \varphi(n), (b, \varphi(n)) = 1$, затем вычисляет $t \equiv g^b \pmod{n}$ и посылает сообщение t абоненту A.

Шаг 3. Абонент A вычисляет $Z(A, B) \equiv t^a \pmod{n}$.

Шаг 4. Абонент B вычисляет $Z(B, A) \equiv s^b \pmod{n}$.

Очевидно, справедливо равенство $Z = Z(A, B) = Z(B, A)$.

4^0. Криптосистема Риверса—Шамира—Адлемана с открытым ключом

В некотором смысле система Риверса—Шамира—Адлемана (система RSA, 1978, [**?**]) является обобщением криптосистем Диффи—Хеллмана и Шамира, основанных на существовании первообразного корня по простому модулю и дискретном логарифме, являющемся односторонней функцией, на системы с односторонними степенными функциями по различным составным модулям, требующих для нахождения обратной функции разложения этих модулей на простые множители.

Пусть абонент A пересылает некоторое секретное цифровое сообщение m абоненту B. Для целей этой пересылки абонент B выбирает два больших простых числа q_1 и q_2, вычисляет их произведение $r_B = q_1 q_2$, функцию Эйлера $\varphi(r_B)$ и выбирает достаточно большое натуральное число b с условиями $1 < b < \varphi(r_B), (b, \varphi(r_B)) = 1$. Затем абонент B вычисляет число β следующим образом

$$b\beta \equiv 1 \pmod{\varphi(r_B)}, \quad 1 \leqslant \beta < \varphi(r_B).$$

Наконец, он представляет следующую информацию, доступную для всех желающих:

$$B : r_B, b.$$

Число b называют *открытым ключом,* а число β — *секретным ключом.*

Далее приведем протокол системы RSA. Без ограничения общности будем считать, что $0 < m < r_B$. (В противном случае цифровой текст делят на куски длины r_B до тех пор, пока не получится кусок длины меньшей, чем r_B. Этот кусок текста и берется за сообщение m.)

Шаг 1. Абонент A шифрует сообщение m открытым ключом b, находя число $m_1 \equiv m^b \pmod{r_B}, 0 < m_1 < r_B$, и пересылает число m_1 абоненту B.

Шаг 2. Абонент B расшифровывает сообщение m_1 секретным ключом β, вычисляя $m_2 \equiv m_1^{\beta} \pmod{r_B}, 0 < m_2 < r_B$, и получает $m_2 = m$.

Действительно, имеем

$$m_2 \equiv m_1^{\beta} \equiv \left(m^b\right)^{\beta} \equiv m \pmod{r_B}.$$

Так как $0 < m, m_1, m_2 < r_B$, то $m_2 = m$.

Таким образом, перехват сообщения m абонента A абоненту B по открытому каналу связи может быть осуществлен, если известен секретный ключ β абонента B. Последнее возможно, если известен модуль $\varphi(r_B)$ сравнения $b\beta \equiv 1 \pmod{\varphi(r_B)}$. Поскольку

$$\varphi(r_B) = (q_1 - 1)(q_2 - 1) = r_B - q_1 - q_2 + 1,$$

и q_1, q_2 — достаточно большие простые числа, найти число $\varphi(r_B)$ можно, если известны эти простые числа, т. е. разложение r_B на простые сомножители.

Приведем ряд очевидных способов перехвата сообщения.

1) В случае выбора достаточно близкими простых чисел q_1, q_2. Имеем

$$4r_B = (q_1 - q_2)^2 + (q_1 + q_2)^2.$$

Следовательно, если $s = |q_1 - q_2|$ мало, то перебором различных значений величины s, как только величина $4r_B - s^2$ является точным квадратом, из системы двух уравнений для $q_1 - q_2$ и $q_1 + q_2$ находим простые числа q_1, q_2.

2) В случае, если наибольший общий делитель чисел $q_1 - 1$ и $q_2 - 1$ является достаточно большим числом, то секретный ключ β может быть найден небольшим перебором.

3) По той же причине число $\varphi(r_B)$ не должно разлагаться только на малые простые сомножители. Следует брать простые числа q_1, q_2 вида $2^k p + 1$, где p — простое число и число k мало.
4) В случае, если $m^b \equiv m \pmod{r_B}$, т. е. число m является «неподвижной» точкой отображения $x \to x^b \pmod{r_B}$, то секретное сообщение m возможно восстановить.

5^0. Электронная (цифровая) подпись

Термин «электронная подпись» более известен в России, в то время как в криптографических стандартах других стран употребляется термин «цифровая подпись».

Определим сначала понятие подписи вообще. С этой целью перечислим свойства данного объекта:
1) обладателем данной подписи может быть только ее владелец;
2) владелец подписи не может отказаться от своей подписи;
3) при возникновении сомнений в подлинности подписи возможно участие третьих лиц в разрешении спора;
4) электронная подпись представляет собой набор цифр в некоторой системе счисления.

Рассмотрим криптосистему для электронной подписи, основанную на RSA системе. Последняя система такова, что абонент, получивший сообщение, может и не знать какой из абонентов его отправил. Напротив при электронной подписи участники переписки знают отправителя сообщения.

Предположим, что абонентами открытого канала связи будут банкир B и вкладчики $w_1, w_2, w_3, \ldots$. Пусть вкладчик $w = w_1$ посылает секретное распоряжение банкиру B. Банкир B и вкладчик w независимо друг от друга выбирают по два больших простых числа соответственно P, Q и p, q. Затем банкир вычисляет значения $R = PQ$, $\varphi(R) = (P-1)(Q-1)$ и выбирает произвольное число S с условиями $1 \leqslant S < \varphi(R), (S, \varphi(R)) = 1$. Аналогичным образом поступает и вкладчик w. Он вычисляет $r = pq$, $\varphi(r) = (p-1)(q-1)$ и выбирает произвольное число s с условиями $1 \leqslant s < \varphi(r)$, $(s, \varphi(r)) = 1$. Далее, для всех делается доступной следующая информация:

$$B, R, S; w, r, s.$$

Здесь числа S и s будут открытыми ключами. Для удобства дальнейших действий необходимо выполнение неравенства $1 \leqslant r < R$.

Наконец, банкир B и вкладчик w находят свои секретные ключи

соответственно T и t из соотношений

$$ST \equiv 1 \pmod{\varphi(R)}, \quad 1 \leqslant T < \varphi(R),$$

$$st \equiv 1 \pmod{\varphi(r)}, \quad 1 \leqslant t < \varphi(r).$$

Приведем теперь протокол криптосистемы для электронной подписи. Вкладчик w посылает банкиру B сообщение m. Без ограничения общности будем считать, что $m < r$ и $(m, r) = 1$.

Шаг 1. Вкладчик w шифрует своим секретным ключом t сообщение m. Находит

$$m_1 \equiv m^t \pmod{r}, \quad 1 \leqslant m_1 < r,$$

проверяет, что $(m_1, R) = 1$, а затем вычисляет с помощью открытого ключа S банкира B величину

$$m_2 \equiv m_1^S \pmod{R}, \quad 1 \leqslant m_2 < R,$$

и посылает сообщение m_2 банкиру B.

Шаг 2. Банкир B расшифровывает сообщение m_2 своим секретным ключом T. Получает

$$m_3 \equiv m_2^T \pmod{R}, \quad 1 \leqslant m_3 < R,$$

а затем открытым ключом s вкладчика w вычисляет

$$m_4 \equiv m_3^s \pmod{r}, \quad 1 \leqslant m_4 < r,$$

и имеет, что $m_4 = m$.

Приведем обоснование действий в криптосистеме электронной подписи. Докажем сначала, что $m_3 = m_1$. Имеем

$$m_3 \equiv m_2^T \pmod{R}, \quad m_2 \equiv m_1^S \pmod{R}.$$

Следовательно, используя теорему Эйлера, получим

$$m_3 \equiv m_1^{ST} \equiv m_1 \pmod{\varphi(R)}, \quad \text{т. е.} \quad m_3 \equiv m_1 \pmod{R},$$

поскольку $ST \equiv 1 \pmod{\varphi(R)}$ и $(m_1, R) = 1$. Далее, из неравенств $1 \leqslant m_3 < R$, $1 \leqslant m_1 < r < R$ имеем $m_3 = m_1$.

Докажем теперь, что $m_4 = m$. Действительно, имеем

$$m_4 \equiv m_3^s \equiv m_1^s \equiv m^{st} \equiv m \pmod{r},$$

поскольку $st \equiv 1 \pmod{\varphi(r)}$ и $(m, r) = 1$. Используя неравенства $1 \leqslant m, m_4 < r$, из сравнения $m_4 \equiv m \pmod{r}$ выводим равенство $m_4 = m$.

Отметим, что свойства 1)—3) подписи в данном алгоритме обосновываются тем, для ее расшифровки необходимо знать секретные ключи t и T. Их нахождение требует знания $\varphi(r) = (p-1)(q-1)$ и $\varphi(R) = (P-1)(Q-1)$. Последнее возможно только при разложении на простые множители больших чисел $r = pq$ и $R = PQ$, что представляет весьма трудную задачу даже при возможностях современных компьютеров.

6^0. Схема Эль-Гамаля электронной цифровой подписи

Пусть абонентам A и B известны некоторое большое простое число p, первообразный корень g по простому модулю p и некоторая хэш-функция h (хэш-функция — это легко вычислимое отображение $m \to h(m)$ очень длинного входного сообщения m в достаточно короткое сообщение $h = h(m)$, такое, что вычислительная сложность нахождения двух сообщений m и m' с условием $h(m) = h(m')$ весьма велика).

Подписывающий абонент A выбирает секретный ключ x из промежутка $1 \leqslant x < p-1$, вычисляет открытый ключ $y \equiv g^{-x} \pmod{p}$ и направляет его абоненту B. Затем абонент A выбирает число u, $(u, p-1) = 1$, $1 \leqslant u < p-1$, и составляет для сообщения m искомую подпись в виде пары чисел (r, s), где $r \equiv g^u \pmod{p}$, $s \equiv u^{-1}(h + xr)$ и $h = h(m)$ — хэш-функция для сообщения m.

Абонент B проверяет истинность подписи (r, s) для сообщения m. При выполнении всех следующих условий

$$(r, p) = 1, \quad 1 \leqslant r, \quad s \leqslant p-1, \quad g^h \equiv y^r r^s \pmod{p},$$

подпись принимается, в противном случае подпись отвергается.

Отметим, что криптосистема Эль-Гамаля обладает следующими свойствами:

1) все действия по подготовке и пересылке абонентом A своей подписи (r, s) занимают полиномиальное время по $\ln p$;

2) абонент B за полиномиальное время по $\ln p$ может проверить, что данная подпись действительно принадлежит A;

3) в предположении сложности вычисления индекса (дискретного логарифма) по основанию первообразного корня по простому модулю p она является стойкой для вскрытия ее незаконным пользователем.

Схема криптосистемы Эль-Гамаля была основой для создания схем стандартов цифровой (электронной) подписи (Digital Signature Algorithm) в США (1991) [**?**] и в России (1994) [**?**].

7^0. Схема стандартов электронной цифровой подписи

Опишем схему российского стандарта цифровой подписи и укажем на ее отличия от американской версии ([**?**], [**?**]).

В начале сообщество пользователей выбирает общие несекретные параметры. Выбирают два простых числа: число q длиной 256 бит и число p длиной 1024 бита, связанных между собой соотношением $p = bq + 1$, где b — некоторое натуральное число. Затем выбирают число a, $1 < a \leqslant p - 1$, с условием

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

Таким образом сообщество пользователей выбрало три общих параметра: простые числа p и q и натуральное число a.

Затем каждый из пользователей выбирает свой секретный ключ $x, 1 < x \leqslant q - 1$, и вычисляет открытый ключ

$$y \equiv a^x \pmod{p}.$$

Множество открытых ключей помещается в справочнике, доступном всем, кому необходимо установить истинность подписи.

Пусть пользователь A желает подписать сообщение m. Приведем протокол подписи. Пользователь A выполняет следующие действия.

Шаг 1. Вычисляет хеш-функцию $h = h(m)$ для сообщения m (в российском стандарте хеш-функция определяется ГОСТ Р34.11–94).

Шаг 2. Выбирает некоторое натуральное число $k, 1 \leqslant k < q$.

Шаг 3. Вычисляет число $n \equiv a^k \pmod{p}, 0 \leqslant n \leqslant p - 1$, а затем находит число $r \equiv n \pmod{q}, 0 \leqslant r \leqslant q - 1$. Если $r = 0$, то возвращаемся к шагу 2; в противном случае идем к шагу 4.

Шаг 4. Вычисляет $s \equiv kh + xr \pmod{q}, 0 \leqslant s \leqslant q - 1$. Если $s = 0$, то возвращаемся к шагу 2; в противном случае идем к шагу 5.

Шаг 5. Отправляет подпись $(h; r, s)$ пользователю B.

Пользователь B делает проверку подписи.

Шаг 1. Проверяет выполнение неравенств $0 < r, s \leqslant q - 1$.

Шаг 2. Вычисляет $u_1 \equiv sh^{-1} \pmod{q}, u_2 \equiv -rh^{-1} \pmod{q}$.

Шаг 3. Вычисляет $l \equiv a^{u_1} y^{u_2} \pmod{p}, v \equiv l \pmod{q}, 0 < v < q$.

Шаг 4. Проверяет выполнение равенства $v = r$. Если проверки на шагах 2 и 4 не дают искомого результата, то подпись считается недействительной; в противном случае подпись считается подлинной.

Глава IV

МНОГОЧЛЕНЫ

§ 1. Целозначные многочлены

Многочлен $P(x) \in \mathbb{Q}[x]$ называется *целозначным*, если при целых значениях аргумента x он принимает целые значения.

Так, например, многочлен $P(x) \in \mathbb{Z}[x]$ будет целозначным многочленом. Многочлен

$$\binom{x}{r} = \frac{x(x-1)\dots(x-r+1)}{r!}$$

также будет целозначным.

Положим $\Delta P(x) = P(x+1) - P(x)$.

1^0. Справедливо равенство $\Delta\binom{x}{r} = \binom{x}{r-1}$. Действительно,

$$\Delta\binom{x}{r} = \frac{(x+1)x\dots(x-r+2)}{r!} - \frac{x(x-1)\dots(x-r+1)}{r!} = \binom{x}{r-1}.$$

2^0. Любой целозначный $P(x)$ многочлен степени k может быть записан в виде

$$a_k\binom{x}{k} + a_{k-1}\binom{x}{k-1} + \dots + a_1\binom{x}{1} + a_0, \tag{4.1}$$

где $a_k, \dots a_1, a_0 \in \mathbb{Z}$ и наоборот, любой многочлен указанного вида является целозначным.

► P(x)$\Delta P(x)$, $\Delta^2 P(x) = \Delta(\Delta P(x)), \dots,$ $\Delta^r P(x) = \Delta(\Delta^{r-1}P(x))$.P(x)$\in \mathbb{Q}[x]$ можно представить в виде

$$P(x) = \alpha_k\binom{x}{k} + \alpha_{k-1}\binom{x}{k-1} + \dots + \alpha_1\binom{x}{1} + \alpha_0,$$

где $\alpha_k, \dots, \alpha_1, \alpha_0 \in \mathbb{Q}$. По утверждению 1^0 имеем

$$\Delta P(x) = \alpha_k\binom{x}{k-1} + \alpha_{k-1}\binom{x}{k-2} + \dots + \alpha_1.$$

Следовательно,

$$\alpha_0 = P(0) \in \mathbb{Z}, \quad \alpha_1 = (\Delta P(x))_{x=0} \in \mathbb{Z}, \quad \alpha_k = \left(\Delta^k P(x)\right)_{x=0} \in \mathbb{Z}.$$

Второе утверждение теоремы очевидно. ◄

3^0. Целозначный многочлен $P(x)$ кратен m для любого значения x тогда и только тогда, когда для коэффициентов в выражении (**??**) справедливо соотношение

$$m \mid (a_k, \ldots, a_0)$$

► *Необходимость.* Из определения коэффициентов многочлена в представлении (**??**) имеем

$$m \mid P(0) = a_0 \in \mathbb{Z}, \quad m \mid (\Delta P(x))_{x=0} = a_1 \in \mathbb{Z},$$

$$m \mid \left(\Delta^k P(x)\right)_{x=0} = a_k \in \mathbb{Z},$$

т. е. $m \mid (a_k, \ldots, a_0)$.

Достаточность. Пусть $m \mid (a_k, \ldots, a_0)$. Тогда

$$m \mid a_0 = P(0) \in \mathbb{Z},$$

$$m \mid a_1 = (\Delta P(x))_{x=0} \in \mathbb{Z},$$

$$m \mid a_k = \left(\Delta^k P(x)\right)_{x=0} \in \mathbb{Z},$$

т. е. $a_0 = mb_0, \ldots, a_k = mb_k$, где $b_0, \ldots, b_k \in \mathbb{Z}$.

Следовательно,

$$P(x) = mQ(x),$$

где $Q(x)$ — целозначный многочлен. ◄

4^0. Пусть p — простое число, $P(x)$ — целозначный многочлен, $P(0) = 0$ и a — наивысшая степень числа p, такая, что в представлении (**??**)

$$p^a \mid (a_k, \ldots, a_1).$$

Пусть, кроме того,

$$P'(x) = b_{k-1}\binom{x}{k-1} + \ldots + b_1\binom{x}{1} + b_0, \tag{4.2}$$

где $b_{k-1}, \ldots b_1, b_0 \in \mathbb{Q}$ и p^b делит наименьшее общее кратное знаменателей чисел $b_{k-1}, \ldots, b_0$. Тогда справедливо неравенство

$$b - a \leqslant \left[\frac{k}{p-1}\right] - 1.$$

► Без ограничения общности можно считать, что $a = 0$. Из (**??**) имеем

$$b_{k-1} = \Delta^{k-1}P'(x) = \bigl(\Delta^{k-1}P(x)\bigr)' = a_k,$$

$$b_{k-2} = \bigl(\Delta^{k-2}P'(x)\bigr)_{x=0} = \bigl(\Delta^{k-2}P(x)\bigr)'_{x=0} = -\frac{a_k}{2} + a_{k-1},$$

$$\dots \quad \dots \quad \dots \quad \dots \quad \dots$$

$$b_0 = (\Delta P'(x))'_{x=0} = (-1)^k \left(\frac{a_k}{k} - \frac{a_{k-1}}{k-1} + \frac{a_{k-2}}{k-2} - \dots + (-1)^k a_1\right).$$

Предположим, что $b > \left[\frac{k}{p-1}\right] - 1$. Тогда

$$p^b \mid (a_k, a_{k-1}, \dots, a_{k-p+1}),$$

$$p^{b-1} \mid (a_{k-p}, a_{k-p-1}, \dots, a_{k-2p+2}),$$

$$\dots \quad \dots \quad \dots \quad \dots \quad \dots$$

$$p \mid p^{\left[\frac{k}{p-1}\right]-1} \mid (a_{(\left[\frac{k}{p-1}\right]-1)(p-1)+1}, \dots, a_1).$$

Отсюда заключаем, что $p \mid (a_k, \dots, a_1)$. Это противоречит условию $a = 0$. ◄

§ 2. Задачи

1. Пусть переменные m, n пробегают все натуральные числа. Тогда выражение

$$m + \frac{1}{2}(m+n-1)(m+n-2)$$

принимает все значения из множества $\mathbb{N}$ без повторений.

2. Пусть многочлен $P(x)$ степени k принимает целые значения в $k+1$ последовательных целых числах. Тогда $P(x)$ — целозначный многочлен.

3. Доказать, что для любого целого x значение многочлена $x^p - x$ делится на p.

4. Доказать, что для любого x, взаимно простого с n, значение многочлена $x^{\varphi(n)} - 1$ делится на n.

§ 3. Разложение многочленов на множители

Множество всех многочленов $P(x) = a_0 + a_1x + \ldots + a_nx^n$ от одной переменной x с целыми коэффициентами $a_0, a_1, \ldots, a_n$ обозначим через $\mathbb{Z}[x]$, а с рациональными коэффициентами — через $\mathbb{Q}[x]$. Если $a_n \neq 0$, то $P(x)$ называется *многочленом степени* n. Многочлен, все коэффициенты которого равны 0, называется *нулевым многочленом.* Многочлен называется *примитивным*, если все его коэффициенты взаимно просты.

1^0. Пусть $P(x),\ Q(x) \in \mathbb{Z}[x]$ — ненулевые многочлены с взаимно простыми коэффициентами, $R(x) = P(x)Q(x)$. Тогда коэффициенты многочлена $R(x)$ взаимно просты.

► Коэффициенты многочленов $P(x),\ Q(x)$ таковы, что

$$(a_m, \ldots, a_0) = 1, \quad (b_n, \ldots, b_0) = 1, \quad a_m \neq 0, \quad b_n \neq 0.$$

Предположим, что $p \mid (c_{m+n}, \ldots, c_0)$ и

$$p \mid (a_m, \ldots, a_{k+1}), \quad (a_k, p) = 1; \quad p \mid (b_n, \ldots, b_{l+1}), \quad (b_l, p) = 1.$$

Имеет место равенство

$$c_{k+l} = \sum_{s+t=k+l} a_s b_t.$$

Все слагаемые в этой сумме, кроме a_kb_l, кратны p. Следовательно, $(c_{k+l}, p) = 1$ и $(c_{m+n}, \ldots, c_0, p) = 1$. Противоречие. ◄

Многочлен $P(x) \in \mathbb{Q}[x]$ называется *приводимым*, если существуют такие многочлены $Q(x),\ R(x) \in \mathbb{Q}[x]$, что $P(x) = Q(x)R(x)$. В противном случае $P(x)$ называется *неприводимым многочленом* над $\mathbb{Q}[x]$.

2^0. (*Гаусс*) Пусть многочлен $P(x) \in \mathbb{Z}[x]$, представи́м в виде $P(x) = Q(x)R(x)$, где $Q(x),\ R(x) \in \mathbb{Q}[x]$. Тогда существует такое рациональное число q, что многочлены $qQ(x), q^{-1}R(x)$ имеют целые коэффициенты.

► Без ограничения общности можно предполагать, что коэффициенты многочлена $P(x)$ взаимно просты. Существуют такие целые числа M, N, что

$$MQ(x) = a_mx^m + \ldots + a_0, \quad NR(x) = b_nx^n + \ldots + b_0 \in \mathbb{Z}[x]$$

и $MNP(x) = c_{m+n}x^{m+n} + \ldots + c_0$. Из утверждения 1^0 следует, что

$$MN = (c_{m+n}, \ldots, c_0) = (a_m, \ldots, a_0)(b_n, \ldots, b_0).$$

Тогда можно положить

$$q = \frac{M}{(a_m, \ldots, a_0)} = \frac{(b_n, \ldots, b_0)}{N}.$$

Утверждение 2^0 доказано. ◄

3^0. (*Эйзенштейн*) Пусть $P(x) = a_m x^m + \ldots a_0 \in \mathbb{Z}[x], p$ — простое число, $(a_m, p) = 1,\ p \mid a_k\ (0 \leqslant k < m)$ и a_0 не делится на p^2. Тогда многочлен $P(x)$ неприводим над $\mathbb{Q}[x]$.

► Предположим, что многочлен $P(x)$ приводим. Тогда из утверждения 2^0 имеем

$$P(x) = Q(x)R(x),\ Q(x) = b_n x^n + \ldots + b_0,\ R(x) = c_l x^l + \ldots + c_0 \in \mathbb{Z}[x],$$

где $m = n + l, \quad n > 0,\ l > 0$. Так как $a_0 = b_0 c_0$ и $p \mid a_0$, то $p \mid b_0$ или $p \mid c_0$. Предположим, что $p \mid b_0$. Тогда из того условия, что $a_0 = b_0 c_0$ не делится на p^2, получаем $(c_0, p) = 1$.

Существует такой номер r, что $p \mid (b_0, \ldots, b_{r-1}),\ (b_r, p) = 1$ и $1 \leqslant r \leqslant n$. Поскольку $a_r = b_r c_0 + \ldots + b_0 c_r,\ r \leqslant n < m$, получим $(a_r, p) = 1$, что противоречит условию утверждения. ◄

§ 4. Задачи

Доказать следующие утверждения.

1. Многочлен $x^m - p$, где p — простое число, неприводим над $\mathbb{Q}[x]$, а следовательно, $p^{1/m}$ — иррациональное число.

2. Пусть p — простое число. Тогда многочлен $x^{p-1} + x^{p-2} + \ldots + x + 1$ неприводим над $\mathbb{Q}[x]$.

3. Многочлены $x^2 + 1,\ x^4 + 1,\ x^6 + x^3 + 1$. неприводимы над $\mathbb{Q}[x]$.

4. Многочлен $x^{2n} + x^n + 1$ делится на многочлен $x^2 + x + 1$, если $(n, 3) = 1$.

5. Многочлен $(x + 1)^n - x^n - 1$ делится на многочлен $x^2 + x + 1$, если $n \pm 1$ делится на 6.

6. Многочлен $(x + 1)^n + x^n + 1$ делится на многочлен $x^2 + x + 1$, если $n \pm 2$ делится на 6.

7. Многочлен $x^3 + y^3 + z^3 - 3xyz$ от трех переменных x, y, z делится на многочлен $x + y + z$.

§ 5. Деление в кольце многочленов с остатком

1^0. Пусть $P(x),\ Q(x) \in \mathbb{Z}[x]$ — ненулевые многочлены соответственно степеней m и $n,\ k = \max(m - n + 1, 0),\ a$ — старший ко-

эффициент многочлена $Q(x)$. Тогда существует единственная пара многочленов $q(x)$ и $r(x)$, такая, что

$$a^k P(x) = q(x)Q(x) + r(x),$$

где $r(x)$ либо имеет степень, меньшую чем n, либо является нулевым многочленом.

► *Существование.* Докажем утверждение методом математической индукции по величине m степени многочлена $P(x)$. Пусть $m < n$. Тогда $k = 0$ и можно взять $q(x) = 0$ и $r(x) = P(x)$. Пусть теперь $m \geqslant n$. Тогда $k = m - n + 1$. Предположим, что утверждение верно при $m \leqslant s - 1$. Докажем его при $m = s$. Можно считать, что $s \geqslant n$. Пусть b — старший коэффициент многочлена $P(x)$. Тогда степень многочлена $aP(x) - bx^{s-n}Q(x)$ не превосходит $s - 1$. По предположению индукции найдутся такие многочлены $q_1(x)$ и $r_1(x)$, что

$$a^{(s-1)-n+1}(aP(x) - bx^{s-n}Q(x)) = q_1(x)Q(x) + r_1(x),$$

где степень многочлена $r_1(x)$ меньше n или $r_1(x) = 0$. Положим $q(x) = ba^{s-n}x^{s-n} + q_1(x)$, $r(x) = r_1(x)$.

Единственность. Предположим, что имеется другое представление $a^k P(x) = Q(x)q_0(x) + r_0(x)$, где степень многочлена $r_0(x)$ меньше n или $r_0(x)$ — нулевой многочлен. Тогда

$$(q(x) - q_0(x))Q(x) = r_0(x) - r(x).$$

Если $q(x) - q_0(x) \neq 0$, то левая часть равенства имеет степень, не меньшую чем n, а степень многочлена $r_0(x) - r(x)$ меньше, чем n. Следовательно, $q(x) - q_0(x) = 0, r_0(x) - r(x) = 0$. Утверждение доказано полностью. ◄

Аналогичное утверждение имеет место для $\mathbb{Q}[x]$, $\mathbb{R}[x]$ и $\mathbb{C}[x]$. В дальнейшем любое из этих множеств, включая $\mathbb{Z}[x]$, будем обозначать через $\mathbb{K}[x]$.

2^0. Пусть $P(x) \in \mathbb{K}[x]$ и $a \in \mathbb{K}$. Тогда для того чтобы $P(a) = 0$ необходимо и достаточно, чтобы $x - a$ был делителем $P(x)$ в $\mathbb{K}$.

► Разделим $P(x)$ с остатком на $x - a$. Получим $P(x) = (x - a)q(x) + b$. Следовательно, $P(a) = b$. Это и доказывает утверждение 2^0. ◄

Число $a \in \mathbb{K}$, для которого $P(a) = 0$, называется *корнем* многочлена $P(x)$.

3^0. Пусть $P(x) \in \mathbb{K}[x]$ и $a_1, \ldots, a_m \in \mathbb{K}$ — различные корни многочлена $P(x)$. Тогда $(x-a_1)\ldots(x-a_m)$ является делителем $P(x)$. Если $P(x)$ — ненулевой многочлен, то число корней многочлена $P(x)$ не превосходит степени $P(x)$.

► Утверждение получается индукцией по числу m корней многочлена $P(x)$. Второе утверждение получается из сравнения степеней многочленов $P(x)$ и $(x-a_1)\ldots(x-a_m)$. ◄

§ 6. Теорема о разложении на неприводимые множители

В настоящем параграфе доказывается, что если в кольце $\mathbb{K}$ имеет место однозначность разложения на множители, то это свойство сохраняется и для кольца многочленов над $\mathbb{K}$.

Теорема 15. *Пусть в $\mathbb{K}$ имеет место однозначность разложения на простые сомножители. Тогда в $\mathbb{K}[x]$ каждый многочлен также однозначно разлагается в произведение неприводимых примитивных многочленов.*

► *Существование.* Проведем индукцию по степени n многочлена $P(x)$. При $n = 0$ утверждение верно, так как в $\mathbb{K}$ каждое число однозначно разлагается на простые сомножители. Предположим, что оно верно при $n < m$. Докажем его при $n = m$. Имеем $P(x) = cP_1(x)$, где $c \in \mathbb{K}$ и $P_1(x)$ — примитивный многочлен. Если $P_1(x)$ — неприводимый многочлен, то искомое представление найдено. В противном случае имеем $P_1(x) = Q(x)R(x)$, причем по утверждению 2^0 из § 2 многочлены $Q(x)$ и $R(x)$ будут примитивными и их степени превосходят 1 и меньше n. Согласно предположению индукции они разлагаются в произведение неприводимых многочленов, что и дает искомое представление.

Единственность. Предположим, что вместе с разложением $P(x) = ap_1(x)\ldots p_s(x)$ в произведение неприводимых примитивных многочленов имеется и другое представление в таком виде: $P(x) = bq_1(x)\ldots q_r(x)$. Тогда в силу утверждения 2^0 из § 2 справедливо равенство $a = b$.

Покажем, что если неразложимый примитивный многочлен $p(x)$ делит $q(x)h(x)$, то он делит хотя бы один из сомножителей $q(x), h(x)$. Рассмотрим множество M всех многочленов вида

$$A(x)p(x) + B(x)q(x),$$

где $A(x), B(x) \in \mathbb{K}[x]$. Пусть $m(x)$ — ненулевой многочлен наименьшей степени, принадлежащий M и a — его старший коэффициент.

Согласно утверждению 1^0 из § 3 найдутся неотрицательное целое число k и многочлены $g(x)$ и $r(x)$, такие, что

$$a^k q(x) = m(x)g(x) + r(x),$$

где либо степень $r(x)$ меньше $m(x)$, либо $r(x) = 0$. Поскольку

$$m(x) = A(x)p(x) + B(x)q(x),$$

имеем

$$r(x) = a^k q(x) - m(x)g(x) =$$
$$= (-A(x)g(x))p(x) + (a^k - B(x)g(x))q(x) \in M.$$

Следовательно, $r(x) = 0$, так как многочлен $m(x)$ имеет наименьшую степень среди ненулевых многочленов в M. Отсюда получим $a^k q(x) = m(x)g(x)$. Представим $m(x)$ в виде $m(x) = bm_0(x)$, где $b \in \mathbb{K}$ и $m_0(x)$ — примитивный многочлен. В силу утверждения 2^0 из § 2 имеем, что $m_0(x)$ делит $q(x)$.

Аналогично, деля $p(x)$ на $m(x)$ с остатком и повторяя предыдущие рассуждения, получим, что $m_0(x)$ делит $p(x)$. Но $p(x)$ — неразложимый примитивный многочлен и $p(x)$ не делит $q(x)$. Следовательно, в силу примитивности многочлена $m_0(x)$ имеем, что $m_0(x)$ делит 1, т. е. $m_0(x) \in \mathbb{K}$ и $m = m(x) \in M$, $m \neq 0$. Отсюда получим $m = A(x)p(x) + B(x)q(x)$ и $mh(x) = A(x)p(x)h(x) + B(x)q(x)h(x)$. Поскольку $p(x)$ — неразложимый примитивный многочлен, в силу утверждения 2^0 из § 2 многочлен $p(x)$ делит $h(x)$.

Из доказанного следует, что в вышеприведенных разложениях многочлена $P(x)$ имеют место равенства $s = r$ и неразложимые примитивные многочлены $p_l(x)$ совпадают с соответствующими многочленами $q_j(x)$. ◀

§ 7. Теорема Гильберта о базисе

Рассмотрим подмножество I многочленов $\mathbb{Z}[x]$, удовлетворяющее условиям: 1) для любых $f, g \in I$ имеем $f \pm g \in I$; 2) для любого $f \in I$ и любого $g \in \mathbb{Z}[x]$ имеем, что $fg \in I$. Такое множество I называется *идеалом* кольца многочленов $\mathbb{Z}[x]$.

Теорема 16 (теорема Гильберта о базисе)**.** *Пусть I идеал кольца многочленов $\mathbb{Z}[x]$. Тогда существует конечное число таких многочленов $f_1, \ldots, f_n \in I$, что для любого $f \in I$ при некоторых $g_1, \ldots, g_n \in \mathbb{Z}[x]$ имеет место равенство $f = f_1 g_1 + \ldots + f_n g_n$.*

► Доказательство разбивается на три шага.

1. Пусть A — множество коэффициентов при старших степенях многочленов из I. Докажем, что A — целый модуль (см. § 2 гл. II). Действительно, если

$$a, b \in A, \quad f = ax^n + \ldots \in I, \quad g = bx^m + \ldots \in I,$$

то $fx^m, gx^n \in I$ и $fx^m \pm gx^n = (a \pm b)x^{m+n} + \ldots \in I$. Следовательно, $a \pm b \in A$. По утверждению из § 2 гл. II существует такое число $d_1 \in A$, что все $a \in A$ будут кратны d_1. Возьмем многочлен

$$f_1 = d_1 x^{l_1} + \ldots \in I$$

со старшим коэффициентом d_1 наименьшей степени.

2. Для любого многочлена $f = ax^m + \ldots \in I$ степени m, не меньшей l_1, имеем

$$f - \frac{a}{d_1} x^{m-l_1} f_1 = g \in I, \quad \text{где} \quad \deg g \leqslant m-1 \quad \text{или} \quad g = 0.$$

Если степень многочлена g будет не меньше, чем l_1, то к многочлену g вместо многочлена f можно применить предыдущую процедуру и т. д. до тех пор пока не получим многочлен $h \in I$ степени меньшей, чем l_1.

3. Рассмотрим множество всех таких многочленов $h_1 \in I$, что $\deg h_1 < l_1$. Аналогично п. 1 показывается, что множество коэффициентов при старших степенях $h_1 \in I$ образует модуль, следовательно, они кратны некоторому d_2, причем $d_1 \mid d_2$. Возьмем многочлен

$$f_2 = d_2 x^{l_2} + \ldots \in I, \quad l_2 < l_1.$$

Рассуждая аналогично п. 2, приходим к многочленам $r \in I$ вида $r = h_1 - f_2 q \in I$, где $\deg r < l_2$ или $r = 0$.

Продолжим далее процедуру этого пункта для множества многочленов $h_2 \in I$ и $\deg h_2 < l_2$, $f_3 = d_3 x^{l_3} + \ldots \in I$, где d_3 — наибольший общий делитель коэффициентов при старших степенях многочленов $h_2 \in I$. Тогда получим, что существует конечное число многочленов $f_1, \ldots, f_n$, такое, что любой многочлен $f \in I$ представляется в виде $f = f_1 g_1 + \ldots + f_n g_n$, где $g_1, \ldots g_n \in \mathbb{Z}[x]$. ◄

§ 8. Кольцо многочленов от многих переменных

Одночленом от r переменных назовем выражение

$$a(t_1, \ldots, t_r) x_1^{t_1} \ldots x_r^{t_r},$$

сумму $t_1 + \ldots + t_r$ называют его *степенью. Многочленом* $P = P(x_1, \ldots, x_r)$ называется сумма конечного числа одночленов. Числа $a(t_1, \ldots, t_r) \in \mathbb{K}$ при одночленах, входящих в многочлен P, называются его *коэффициентами. Степенью* $\deg P$ ненулевого многочлена P называется максимум степеней одночленов, входящих в многочлен P с ненулевыми коэффициентами. Множество всех многочленов от r переменных $x_1, \ldots, x_r$ с коэффициентами из $\mathbb{K}$ обозначим через $\mathbb{K}[x_1, \ldots, x_r]$. Справедливо следующее утверждение.

Теорема 17. *Пусть в* $\mathbb{K}$ *имеет место однозначность разложения на простые множители. Тогда в* $\mathbb{K}[x_1, \ldots, x_r]$ *также каждый многочлен однозначно разлагается в произведение неприводимых примитивных многочленов.*

► Доказательство проводится индукцией по двум параметрам: r — числу переменных и n — степени многочлена P. В силу условия утверждение верно при $r = 0$ и любом натуральном n, а также при $n = 1$ и любом r. Предположим, что оно справедливо при $r < s$ и $n \leqslant m$, а также при $r \leqslant s$ и $n < m$. Докажем его при $r = s$ и $n = m$. Запишем многочлен $P(x_1, \ldots, x_s)$ как многочлен от одной переменной x_s с коэффициентами, являющимися многочленами от переменных $x_1, \ldots, x_{s-1}$. Если степень многочлена P по переменной x_s равна нулю, то по предположению индукции утверждение теоремы верно. Поскольку по предположению индукции в кольце $\mathbb{K}_1 = \mathbb{K}[x_1, \ldots, x_{s-1}]$ имеет место однозначность разложения многочлена на простые сомножители, то используя теорему **??**, имеем

$$P(x_1, \ldots, x_s) = g_1(x_s) \ldots g_l(x_s),$$

где коэффициенты многочленов $g_1, \ldots, g_l$ принадлежат $\mathbb{K}_1$. К многочленам $g_1, \ldots, g_l$ применимо предположение индукции. ◄

Теорема 18. *Пусть* I *идеал кольца многочленов* $\mathbb{Z}[x_1, \ldots, x_r]$. *Тогда существует конечное число таких многочленов* $f_1, \ldots, f_n \in I$, *что для любого* $f \in I$ *при некоторых* $g_1, \ldots, g_n \in \mathbb{Z}[x_1, \ldots, x_r]$ *имеет место равенство*

$$f = f_1 g_1 + \ldots + f_n g_n.$$

► Доказательство проводится индукцией по числу переменных r. В качестве базы индукции используется теорема Гильберта о базисе. ◄

§ 9. Кольцо многочленов над конечным полем

Пусть p — фиксированное простое число, $\mathbb{Z}_p$ — поле вычетов по модулю p и $\mathbb{Z}_p[x]$ — кольцо всех многочленов с коэффициентами из поля $\mathbb{Z}_p$. Наивысшая степень d одночлена $a_d x^d$ с ненулевым коэффициентом a_d, входящая в многочлен $f(x) \in \mathbb{Z}_p[x]$, называется *степенью многочлена* $f(x)$. Два многочлена $f(x) \in \mathbb{Z}_p[x]$ и $g(x) \in \mathbb{Z}_p[x]$ называются *равными*, если равны их коэффициенты. *Суммой* (*разностью*) многочленов f и g называется многочлен $f+g$ (соответственно, $f-g$), который получается сложением (вычитанием) коэффициентов при одинаковых степенях f и g. *Произведением* h двух многочленов $f = f(x) = a_m x^m + \ldots + a_0 \in \mathbb{Z}_p[x]$ и $g = g(x) = b_n x^n + \ldots + b_0 \in \mathbb{Z}_p[x]$ называется многочлен $h = h(x) = c_k x^k + \ldots + c_0 \in \mathbb{Z}_p[x]$, где $c_s = \sum_{r=0}^{s} a_r b_{s-r}$. Заметим, что степень многочлена h равна сумме степеней многочленов f и g. В частности, для любого многочлена $f \in \mathbb{Z}_p[x]$ справедливо равенство

$$(f(x))^p = f(x^p).$$

Пусть $f, g \in \mathbb{Z}_p[x]$ и многочлен g отличен от нулевого многочлена в $\mathbb{Z}_p[x]$. Тогда если найдется такой многочлен $q(x) \in \mathbb{Z}_p[x]$, что $f = gq$, то говорят, что f *делится на* g, причем g называется *делителем* f, а многочлен q — *частным* от деления f на g.

Очевидно, что $f \mid f$. Далее, если $f \mid g$ и $g \mid f$ в $\mathbb{Z}_p[x]$, то степени многочленов f и g равны. Тогда в силу делимости f на g имеем, что $f(x) = kg(x)$, $k \in \mathbb{Z}_p$, $k \neq 0$. Многочлены f и g называются *ассоциированными* в кольце $\mathbb{Z}_p[x]$. Многочлен $f \in \mathbb{Z}_p[x]$ называется *нормированным*, если коэффициент при старшей степени его равен 1. Ясно, что количество нормированных многочленов из $\mathbb{Z}_p[x]$ степени n равно p^n.

По аналогии с целочисленными многочленами можно доказать, что в кольце многочленов $\mathbb{Z}_p[x]$ имеет место деление с остатком. Другими словами, для любого $f \in \mathbb{Z}_p[x]$ и ненулевого многочлена $g \in \mathbb{Z}_p[x]$ найдется единственная пара многочленов q, r, такая, что $f = gq + r$, где или степень многочлена r меньше g, или r — нулевой многочлен в $\mathbb{Z}_p[x]$.

Многочлен $f \in \mathbb{Z}_p[x]$ называется *неприводимым*, если он не может быть представлен в виде произведения двух многочленов в $\mathbb{Z}_p[x]$ с меньшими степенями.

Так, например, в кольце $\mathbb{Z}_3[x]$ среди шести нормированных мно-

гочленов второй степени только

$$x^2+1, \quad x^2+x+2, \quad x^2+2x+2$$

являются неприводимыми.

Имеет место основная теорема арифметики в кольце $\mathbb{Z}_p[x]$, доказательство которой в основных чертах подобно доказательству для целочисленных многочленов.

Теорема 19. *Каждый нормированный многочлен единственным образом разлагается в произведение нормированных неприводимых многочленов в* $\mathbb{Z}_p[x]$.

В силу теоремы **??** для любых $f, g \in \mathbb{Z}_p[x]$ определен их *наибольший общий делитель* $d(x) = (f(x), g(x))$. Можно считать, что $d(x)$ — нормированный многочлен. Применяя алгоритм Евклида, можно установить справедливость следующего утверждения.

Теорема 20. *Пусть заданы многочлены* $f, g \in \mathbb{Z}_p[x]$ *и* $d(x)$ *— их наибольший общий делитель. Тогда существуют такие многочлены* $a, b \in \mathbb{Z}_p[x]$, *что* $af + bg = d$.

Пусть $(n) = (n)_p$ обозначает количество нормированных неприводимых многочленов степени n.

Теорема 21. *Справедлива формула*

$$(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}.$$

► Сначала установим, что при $|z| < 1/p$ справедливо тождество

$$\frac{1}{1-pz} = \prod_{m=1}^{\infty} \left(\frac{1}{1-z^m} \right)^{(m)},$$

причем бесконечное произведение в правой части тождества абсолютно сходится при $|z| < 1/p$. Очевидно, что $0 \leqslant (m) \leqslant p^m$. Абсолютная сходимость рассматриваемого бесконечного произведения следует из сходимости ряда

$$\sum_{m=1}^{\infty} a_m, \quad a_m = (m) \left(|z|^m + |z|^{2m} + \ldots \right).$$

Общий член a_m этого ряда при $|z| < 1/p$ мажорируется величиной

$$a_m \leqslant \frac{(p|z|)^m}{1-|z|^m} \leqslant 2(p|z|)^m = b_m.$$

Ряд $\sum b_m$ сходится при $|z| < 1/p$, что и доказывает абсолютную сходимость бесконечного произведения.

Пусть, далее, Q_m пробегает все нормированные неприводимые многочлены, а F_m — все нормированные многочлены степени m. Тогда в силу теоремы **??** имеет место тождество

$$\prod_{m=1}^{\infty}\left(\frac{1}{1-z^m}\right)^{(m)} = \prod_{m=1}^{\infty}\prod_{Q_m}\frac{1}{1-z^m} = 1+\sum_{m=1}^{\infty}\sum_{F_m} z^m =$$

$$= 1+\sum_{m=1}^{\infty} p^m z^m = \frac{1}{1-pz}.$$

Логарифмируя доказанное тождество, при $|z| < 1/p$ получим

$$\ln(1-pz) = \sum_{m=1}^{\infty}(m)\ln(1-z^m) \quad \text{или} \quad \sum_{m=1}^{\infty}(m)\sum_{k=1}^{\infty}\frac{z^{mk}}{k} = \sum_{l=1}^{\infty}\frac{p^l z^l}{l}.$$

Отсюда следует равенство коэффициентов этих степенных рядов:

$$\frac{p^l}{l} = \sum_{mk=l}\frac{(m)}{k} \quad \text{или} \quad p^k = \sum_{d|k}(d)d.$$

Применив к последнему равенству формулу обращения (см. задачи к § 8 гл. I), получим доказываемое равенство. ◀

Теорема 22. *В кольце $\mathbb{Z}_p[x]$ для любой степени $n \geqslant 1$ существуют неприводимые многочлены.*

◀ Пусть $n = q_1^{a_1}\dots q_k^{a_k}$ — каноническое разложение числа n. Тогда по теореме **??** имеем

$$(n)n \equiv (-1)^k p^{n/(q_1\dots q_k)} \pmod{p^{n/(q_1\dots q_k)+1}}.$$

Следовательно, $(n)n > 0$. ◀

Теорема 23. *В кольце $\mathbb{Z}_p[x]$ множество всех классов вычетов по модулю неприводимого многочлена f степени $n \geqslant 1$ образует поле $\mathbb{F}_q$ из $q = p^n$ элементов.*

▶ Для любого многочлена g, принадлежащего ненулевому классу вычетов, имеем $(g, f) = 1$. По теореме **??** существуют такие многочлены a, b, что

$$ag + bf = 1, \quad \text{т. е.} \quad ag \equiv 1 \pmod{f}.$$

Таким образом, многочлен a является обратным к g в рассматриваемом классе вычетов по модулю f. Замкнутость этого множества относительно операций сложения, вычитания и умножения очевидна. Количество элементов в полученном поле равно количеству нормированных многочленов степени n, т. е. равно p^n. ◀

Покажем, что все поля из $q = p^n$ элементов изоморфны. Для этого достаточно доказать следующее утверждение.

Теорема 24. *Мультипликативная группа конечного поля циклична.*

▶ Пусть δ_a — порядок ненулевого элемента a поля, т. е. $a^{\delta_a} = 1$. Обозначим через τ наименьшее общее кратное δ_a по всем $a \neq 0$. Тогда уравнению $x^\tau = 1$ удовлетворяют все $a \neq 0$. Пусть порядок мультипликативной группы поля равен m. Число корней уравнения не превосходит его степени. Следовательно, $\tau \geqslant m$. С другой стороны, по теореме Лагранжа порядок любого элемента делит порядок m группы, т. е. для любого $a \neq 0$ имеем $\delta_a \mid m$. Это означает, что $\tau \mid m$. Поэтому $\tau \leqslant m$. Тем самым доказано, что $\tau = m$. ◀

Таким образом, все поля $\mathbb{F}_{p^n}$ из p^n элементов изоморфны полю корней многочлена

$$x^{p^n} - x = 0.$$

Любая образующая мультипликативной группы поля из p элементов называется *первообразным корнем* по модулю p.

§ 10. Задачи

1. Пусть числа p, q простые, причем для любого q, делящего $p-1$, при условии $(g, p) = 1$ справедливо сравнение $g^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$. Тогда g — первообразный корень по модулю p.

2. Пусть числа p, q простые, причем для любого q, делящего $p-1$, при условии $(g, p) = 1$ справедливо сравнение $x^q \not\equiv g \pmod{p}$. Тогда g — первообразный корень по модулю p.

Глава V

РАЦИОНАЛЬНЫЕ, АЛГЕБРАИЧЕСКИЕ И ТРАНСЦЕНДЕНТНЫЕ ЧИСЛА

Всякое *рациональное число* является решением уравнения первой степени с целыми коэффициентами; в противном случае вещественное число называется *иррациональным.* Древние греки открыли, что *диагональ единичного квадрата не может измеряться рациональным числом*, т. е. $\sqrt{2}$ — число иррациональное.

При рассмотрении в настоящей книге алгоритма Евклида и позиционных систем счисления, по существу, доказаны следующие критерии рациональности чисел.

1^0. Непрерывная дробь вещественного числа обрывается на конечном шаге тогда и только тогда, когда оно является рациональным числом.

2^0. Разложение вещественного числа в бесконечную g-ичную дробь обрывается на конечном шаге или является периодической дробью тогда и только тогда, когда оно является рациональным числом.

Наряду с квадратным корнем из двух аналогичным образом можно построить другие иррациональные числа.

3^0. Пусть многочлен $P(x) = x^n + a_1x^{n-1} + \ldots + a_n$ с целыми коэффициентами имеет корень α. Тогда число α является или целым, или иррациональным.

► Без ограничения общности можно считать, что $a_n \neq 0$. Пусть $\alpha = \frac{a}{b},\ (a, b) = 1,\ b \geqslant 1$. Справедливо равенство

$$a^n + a_1a^{n-1}b + \ldots + a_nb^n = 0.$$

Тогда из делимости b на простое число p следует, что a также делится на p. Это противоречит условию взаимной простоты чисел a и b. Следовательно, $b = 1$. ◄

4^0. Пусть n и a — натуральные числа и число a не является n-той степенью натурального числа. Тогда $\sqrt[n]{a}$ — иррациональное число.

► Число $\sqrt[n]{a}$ является корнем уравнения $x^n - a = 0$. В силу того условия, что a не является n-той степенью натурального числа и

основной теоремы арифметики, этот корень не является натуральным числом. Тогда по 3^0 он является иррациональным числом. ◄

Числа, удовлетворяющие алгебраическому уравнению с рациональными коэффициентами, называются *алгебраическими.* Любое число, которое не является алгебраическим, называется *трансцендентным.*

§ 1. Приближение вещественных чисел рациональными

Сформулируем и докажем *лемму Дирихле.*

Лемма 14 (Дирихле)**.** *Пусть α — вещественное число. Тогда для любого $\tau \geqslant 1$ найдутся такие целые числа $x,\ 1 \leqslant x \leqslant \tau$, и y, что*

$$|\alpha x - y| < \frac{1}{\tau}.$$

► Положим $t = [\tau] + 1$. Разделим промежуток $[0, 1)$ на t равных подпромежутков. Далее полагая $x = 0, 1, \ldots, t$, имеем

$$0 \leqslant \alpha x - [\alpha x] < 1.$$

Поскольку число подпромежутков равно t, существуют натуральное число $b \leqslant t$ и две пары целых чисел x_1, y_1 и x_2, y_2, такие, что

$$\frac{b-1}{t} \leqslant \alpha x_1 - y_1 < \frac{b}{t}, \quad \frac{b-1}{t} \leqslant \alpha x_2 - y_2 < \frac{b}{t}.$$

Следовательно, при $x = x_1 - x_2,\ y = y_1 - y_2$ получим

$$|\alpha x - y| < \frac{1}{t} \leqslant \frac{1}{\tau}.$$

Лемма доказана. ◄

В частности, из леммы Дирихле следует, что для любого вещественного числа α найдется рациональное число $\frac{x}{y}, (x, y) = 1, y \geqslant 1$, с условием

$$\left|\alpha - \frac{y}{x}\right| < \frac{1}{x^2}. \tag{5.1}$$

Докажем следующий критерий иррациональности числа.

Лемма 15. *Неравенство* (**??**) *имеет бесконечно много решений тогда и только тогда, когда число α иррационально.*

▶ *Необходимость.* Предположим, что $\alpha = \frac{a}{b}$ — рациональное число. Возьмем любое рациональное число $\frac{y}{x} \neq \alpha$, $x \geqslant 1$. Получим

$$\frac{1}{x^2} > \left|\alpha - \frac{y}{x}\right| = \left|\frac{a}{b} - \frac{y}{x}\right| = \frac{|ax - by|}{bx} \geqslant \frac{1}{bx}.$$

Следовательно, неравенству (**??**) удовлетворяют только числа x, меньшие b, поэтому указанное неравенство имеет лишь конечное число решений, что противоречит условию утверждения.

Достаточность. Положим $\tau_1 = 1$. Тогда найдутся такие целые числа $x_1 = 1$ и y_1, что

$$\beta_1 = \left|\alpha - \frac{y_1}{x_1}\right| < \frac{1}{x_1\tau_1},$$

причем $\beta_1 \neq 0$, так как α — иррациональное число. Далее, положим $\tau_2 = \frac{1}{\beta_1}$ и по лемме Дирихле найдем такую пару взаимно простых чисел $x_2 \leqslant \tau_2$ и y_2, что

$$\beta_2 = \left|\alpha - \frac{y_2}{x_2}\right| < \frac{1}{x_2\tau_2} \leqslant \beta_1,$$

причем $\beta_2 \neq 0$. Продолжая описанный процесс, получим

$$\beta_k = \left|\alpha - \frac{y_k}{x_k}\right| < \frac{1}{x_k^2}, \quad \beta_1 > \beta_2 > \cdots > \beta_k > \dots .$$

Лемма доказана. ◀

§ 2. Задачи

1. Доказать, что числа e, $\sin 1$, $\cos 1$ являются иррациональными.

Указание. Имеем

$$e = \lim_{n\to\infty} s_n, \quad s_n = 1 + 1 + \frac{1}{2!} + \ldots + \frac{1}{n!}, \quad 0 < r_n = e - s_n \leqslant \frac{1}{n \cdot n!}.$$

Далее предположить рациональность числа e.

2. Доказать, что число e не является квадратичной иррациональностью.

Указание. Предположим, что существуют такие целые числа a, b, c, что $ae^2 + be + c = 0$. Числа a и c не равны нулю, так как e — иррациональное число. Можно считать, что $a > 0$. Имеем

$$e^{-1} = \sum_{k=0}^{n} \frac{(-1)^k}{k!} + \rho_n, \quad \frac{1}{(n+2)n!} < |\rho_n| < \frac{1}{(n+1)!}.$$

Выбирая значение n так, чтобы выполнялись неравенства $c\rho_n > 0$ и $n > a + |c|$, имеем

$$0 = n!(ae + b + ce^{-1}) = n!(as_n + b + ct_n) + R_n, \quad R_n = n!(ar_n + c\rho_n).$$

Отсюда получим противоречие, поскольку $n!(as_n + b + ct_n) \in \mathbb{Z}$ и $0 < R_n \leqslant \frac{a}{n} + \frac{|c|}{n+1} \leqslant \frac{a+|c|}{n} < 1$.

3. Доказать, что число π иррационально.

Указание. Предположим, что $\pi = \frac{a}{b}$, $(a, b) = 1$, $a, b \in \mathbb{N}$. Рассмотрим два многочлена

$$f(x) = \frac{x^n(a - bx)^n}{n!}, \quad F(x) = f(x) - f''(x) + \ldots + (-1)^n f^{(2n)}(x).$$

Получим

$$\frac{d}{dx}(F'(x)\sin x - F(x)\cos x) = f(x)\sin x,$$

причем

$$\int_0^\pi f(x)\sin x dx = F(\pi) + F(0)$$

есть целое число. Но при $0 < x < \pi$ и достаточно большом n имеем

$$0 < f(x)\sin x < \frac{\pi^n a^n}{n!} < \frac{1}{4}.$$

Противоречие.

4. Доказать, что число e трансцендентно.

Указание. Возьмем

$$I(t) = \int_0^t e^{t-x} f(x)\, dx, \quad f(x) = \sum_{s=0}^m b_s x^s.$$

Имеем

$$I(t) = e^t \sum_{k=0}^m f^{(k)}(0) - \sum_{k=0}^m f^{(k)}(t), \quad |I(t)| \leqslant \int_0^t |e^{t-x} f(x)|\, dx \leqslant te^t f_0(t),$$

где $f_0(t) = \sum\limits_{s=0}^m |b_s| x^s$.

Предположим, что e — алгебраическое число. Тогда существуют такие целые числа $a_0, \ldots, a_n$, что $a_n e^n + \ldots + a_1 e + a_0 = 0$, причем $a_0 \neq 0$.

Положим $f(x) = x^{p-1}(x-1)^p \ldots (x-n)^p$, где p — достаточно большое простое число, $m = (n+1)p - 1$. Рассмотрим выражение

$$J = a_0 I(0) + a_1 I(1) + \ldots + a_n I(n).$$

Имеем $f_0(k) \leqslant (2n)^m$, $m \leqslant 2np$. Поэтому

$$|J| \leqslant \sum_{r=0}^{n} |a_r| e^r f_0(r) \leqslant cne^n (2n)^{2np},$$

где $c = \max\{|a_1|, \ldots, |a_n|\}$. При $p \to \infty$ последняя величина растет как a^p при некотором $a > 1$.

Оценим величину J снизу. Для этого сначала покажем, что J — целое число. В самом деле,

$$J = \sum_{r=0}^{n} a_r I(r) = \sum_{r=0}^{n} a_r e^r \sum_{k=0}^{m} f^{(k)}(0) - \sum_{r=0}^{n} a_r \sum_{k=0}^{m} f^{(k)}(r) =$$

$$= -\sum_{k=0}^{m} \sum_{r=0}^{n} a_r f^{(k)}(r).$$

Вычислим $f^{(k)}(r)$. Пусть $1 \leqslant r \leqslant n$. Тогда

$$f^{(k)}(r) = \begin{cases} 0, & \text{если } k < p; \\ \binom{k}{p} p! g^{(k-p)}(r), & \text{если } k \geqslant p, \end{cases}$$

где $g(x) = f(x)/(x-r)^p$. Следовательно, $f^{(k)}(r)$ — целое число, кратное $p!$. Далее, имеем

$$f^{(k)}(0) = \begin{cases} 0, & \text{если } k < p-1; \\ \binom{k}{p-1} (p-1)! h^{(k-p+1)}(0), & \text{если } k \geqslant p-1. \end{cases}$$

где $h(x) = f(x)/x^{p-1}$. Отсюда получим

$$f^{(k)}(0) \quad \text{делится на} \begin{cases} p!, & \text{если } k \neq p-1; \\ (p-1)!, & \text{если } k = p-1 \text{ и } p > n. \end{cases}$$

Поэтому $J \neq 0$ и $(p-1)! \mid J$, откуда следует, что $|J| \geqslant (p-1)!$. При больших p эта оценка снизу для величины $|J|$ противоречит верхней оценке, полученной выше.

§ 3. Теорема Апери об иррациональности значения дзета-функции Римана в точке 3

Функцию

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

применял в своих исследованиях еще Л. Эйлер, но именно Б. Риман в середине XIX в. начал рассматривать ее как функцию комплексной переменной. Здесь мы приводим схему доказательства теоремы Апери об иррациональности значения $\zeta(3)$.

1. Пусть задано вещественное число α и пусть существуют последовательности $P_n \in \mathbb{Z}$ и $Q_n \in \mathbb{N}$ и арифметическая функция $f(n)$, удовлетворяющие условиям:

а) $\left|\alpha - \dfrac{P_n}{Q_n}\right| \leqslant \dfrac{1}{Q_n f(Q_n)}$, $(P_n, Q_n) = 1$;

б) $Q_n \to +\infty$ при $n \to +\infty$;

в) $f(Q_n) \to +\infty$ при $n \to +\infty$.

Тогда последовательность P_n/Q_n называется *последовательностью хороших приближений вещественного числа* α.

Докажите, что если α — рациональное число, то не существует последовательности P_n/Q_n его хороших приближений.

Указание. Предположим противное. Пусть существует последовательность P/Q хороших приближений числа $\alpha = p/q$, $(p, q) = 1$. Очевидно, имеют место неравенства

$$\frac{1}{qQ} \leqslant \left|\frac{p}{q} - \frac{P}{Q}\right| < \frac{1}{Qf(Q)},$$

откуда следует, что $f(Q) < q$. Последнее неравенство противоречит условию неограниченности последовательности $\{f(Q)\}$.

2. Пусть $r, s \in \mathbb{N} \cup \{0\}$, $r > s$. Докажите, что

а) $\displaystyle\int_0^1 \int_0^1 \frac{x^r y^s}{1-xy}\, dxdy = \frac{P}{Q}$, где $(P, Q) = 1$, причем $Q \mid m^2$ и $m = [2, \ldots, r]$;

б) $\displaystyle\int_0^1 \int_0^1 \frac{\ln xy}{1-xy}\, dxdy = \frac{P}{Q}$, где $(P, Q) = 1$, причем $Q \mid m^3$;

в) $\int\limits_0^1\int\limits_0^1 \frac{x^r y^r}{1-xy}\,dxdy = \zeta(2) - 1 - \frac{1}{2^2} - \cdots - \frac{1}{r^2}$;

г) $\int\limits_0^1\int\limits_0^1 \frac{\ln xy}{1-xy} x^r y^r\,dxdy = \zeta(3) - 1 - \frac{1}{2^3} - \cdots - \frac{1}{r^3}$.

Указание. Возьмем любое $\sigma > 0$. Имеем тождество

$$I(\sigma) = \int\limits_0^1\int\limits_0^1 \frac{x^{r+\sigma}y^{s+\sigma}}{1-xy}\,dxdy = \int\limits_0^1\int\limits_0^1 x^{r+\sigma}y^{s+\sigma}\sum_{k=0}^{\infty}(xy)^k\,dxdy =$$

$$= \sum_{k=0}^{\infty}\frac{1}{k+r+\sigma+1}\frac{1}{k+s+\sigma+1} =$$

$$= \frac{1}{r-s}\left(\frac{1}{s+\sigma+1} + \ldots + \frac{1}{r+\sigma}\right) = \frac{P}{Q},$$

причем $(P, Q) = 1$.

а) При $\sigma = 0$ получим

$$\int\limits_0^1\int\limits_0^1 \frac{x^r y^s}{1-xy}\,dxdy = \frac{1}{r-s}\left(\frac{1}{s+1} + \ldots + \frac{1}{r}\right) = \frac{P}{Q}.$$

Отсюда имеем

$$Q \mid [r-s, s+1, s+2, \ldots, r] \mid [2, \ldots, r]^2.$$

б) Справедливо равенство

$$I'(\sigma) = \int\limits_0^1\int\limits_0^1 \frac{\ln xy}{1-xy} x^{r+\sigma}y^{s+\sigma}\,dxdy =$$

$$= \frac{1}{r-s}\left(-\frac{1}{(s+\sigma+1)^2} - \cdots - \frac{1}{(r+\sigma)^2}\right) = \frac{P}{Q}.$$

Кроме того, справедливы соотношения

$$Q \mid [r-s, (s+1)^2, (s+2)^2, \ldots, r^2] \mid [2, \ldots, r]^3.$$

в) При $r = s$ для величины $I(\sigma)$ имеем

$$\int_0^1 \int_0^1 \frac{x^{r+\sigma} y^{r+\sigma}}{1-xy}\, dxdy = \sum_{k=0}^{\infty} \frac{1}{(k+r+\sigma+1)^2}.$$

Отсюда при $\sigma = 0$ получим

$$\int_0^1 \int_0^1 \frac{x^r y^r}{1-xy}\, dxdy = \zeta(2) - 1 - \frac{1}{2^2} - \cdots - \frac{1}{r^2}.$$

г) Дифференцируя по σ выражение п. в), получим

$$-\int_0^1 \int_0^1 \frac{\ln xy}{1-xy} x^{r+\sigma} y^{r+\sigma}\, dxdy = \sum_{k=0}^{\infty} \frac{2}{(k+r+\sigma+1)^3}.$$

Следовательно,

$$-\int_0^1 \int_0^1 \frac{x^r y^r}{1-xy} \ln(xy)\, dxdy = 2\left(\zeta(3) - 1 - \frac{1}{2^3} - \cdots - \frac{1}{r^3}\right).$$

3. Докажите, что при достаточно большом r справедливо неравенство

$$[2, \ldots, r] < 3^r.$$

Указание. Наименьшее общее кратное $L = L(r)$ чисел $2, \ldots, r$ можно представить в виде $\prod_{p \leqslant r} p^{k_p}$, где $k_p = [\ln r / \ln p]$. Следовательно,

$$L = \prod_{p \leqslant r} p^{[\ln r / \ln p]} \leqslant \prod_{p \leqslant r} e^{\ln r} = e^{\pi(r) \ln r},$$

где $\pi(r)$ — количество простых чисел, не превосходящих r. Для величины $\pi(r)$ при $r \to \infty$ известна асимптотика $\pi(r) \sim \frac{r}{\ln r}$[1]. Используя это, получим, что существует r_0 такое, что для всех $r > r_0$ выполняется неравенство $L < 3^r$.

4. Докажите, что

а) (*Эйлер*) число $\zeta(2)$ иррационально;

[1] См., например, [?, с. 362, вопрос 9].

б) (*Апери*) число $\zeta(3)$ иррационально.

Указание. а) Рассмотрим многочлен Лежандра

$$P_n(x) = \frac{1}{n!}\frac{d^n}{dx^n}\left(x^n(1-x)^n\right).$$

Используя результаты пп. а) и в) задачи 6, имеем

$$J_n = \int\limits_0^1\int\limits_0^1 \frac{(1-y)^n P_n(x)}{1-xy}\,dxdy = \frac{A_n + B_n\zeta(2)}{d_n^2}.$$

Оценим сверху $|J_n|$. Интегрируя по частям, получим

$$|J_n| = \left|\int\limits_0^1\int\limits_0^1 \frac{y^n(1-y)^n x^n(1-x)^n}{(1-xy)^{n+1}}\,dxdy\right| \leqslant$$

$$\leqslant \max_{x,y\in[0,1]}\left(\frac{xy(1-x)(1-y)}{1-xy}\right)^n \int\limits_0^1\int\limits_0^1 \frac{dxdy}{1-xy} = \left(\frac{\sqrt{5}-1}{2}\right)^{5n}\frac{\pi^2}{6}.$$

Следовательно,

$$\left|\zeta(2) + \frac{A_n}{B_n}\right| \leqslant \frac{1}{B_n}d_n^2\left(\frac{\sqrt{5}-1}{2}\right)^{5n}\frac{\pi^2}{6} \leqslant$$

$$\leqslant \frac{1}{B_n}\left(3\left(\frac{\sqrt{5}-1}{2}\right)^5\right)^n\frac{\pi^2}{6} < \frac{1}{B_n}\frac{\pi^2}{6}\left(\frac{5}{6}\right)^n.$$

Это означает, что последовательность $\left\{\frac{-A_n}{B_n}\right\}$ является последовательностью хороших приближений числа $\zeta(2)$. Отсюда согласно задаче 1 число $\zeta(2)$ иррационально.

б) Согласно задаче 2 б), г) имеем

$$G_n = -\int\limits_0^1\int\limits_0^1 \frac{\ln xy}{1-xy}P_n(x)P_n(y)dxdy = \frac{A_n + B_n\zeta(3)}{d_n^3}.$$

Воспользуемся тем, что $-\frac{\ln xy}{1-xy} = \int\limits_0^1 \frac{dz}{1-(1-xy)z}$. Получим

$$G_n = \int\limits_0^1 \int\limits_0^1 \int\limits_0^1 \frac{(1-x)^n(1-y)^n(1-z)^n x^n y^n z^n}{(1-(1-xy)z)^{n+1}}\, dxdydz \leqslant (\sqrt{2}-1)^{4n} I,$$

где

$$I = \int\limits_0^1 \int\limits_0^1 \int\limits_0^1 \frac{dxdydz}{1-(1-xy)z}.$$

Отсюда следуют неравенства

$$\left|\zeta(3) + \frac{A_n}{B_n}\right| \leqslant \frac{1}{B_n} d_n^3 (\sqrt{2}-1)^{4n} I < \frac{1}{B_n}\left(\frac{4}{5}\right)^n.$$

Поэтому согласно задаче 1 число $\zeta(3)$ иррационально.

Глава VI
ЗАДАЧИ ПО ТЕОРИИ ЧИСЕЛ И АЛГЕБРЕ

Содержание

§ 1. Квадратичные вычеты и невычеты по простому модулю. Символ Лежандра

1. Пусть a, m — натуральные числа, $(2a, m) = 1$. Тогда сравнение $ax^2 + bx + c \equiv 0 \pmod{m}$ эквивалентно сравнению $z^2 \equiv b^2 - 4ac \pmod{m}$.

► Имеем цепочку равносильных сравнений

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{m}, (2ax + b)^2 \equiv b^2 - 4ac \pmod{m}.$$

Полагая $z = 2ax + b$, получим сравнение $z^2 \equiv b^2 - 4ac \pmod{m}$. ◄

Обозначим буквой p нечетное простое число. Далее при $(a, p) = 1$ рассмотрим следующее сравнение

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

Число a называется квадратичным вычетом по модулю p, если сравнение (1) разрешимо и квадратичным невычетом по модулю p, если оно не имеет решений.

2. Пусть сравнение (1) разрешимо. Тогда оно имеет два решения.

► Пусть $x_0 \pmod{p}$ — решение сравнения (1). Тогда вычет $(-x_0) \pmod{p}$ также является решением (1) и $x_0 \not\equiv -x_0 \pmod{p}$. ◄

3. Приведенная система вычетов по модулю p состоит из $\frac{p-1}{2}$ квадратичных вычетов, сравнимых по модулю p с числами $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$, и $\frac{p-1}{2}$ квадратичных невычетов по модулю p.

► Пусть a — квадратичный вычет по модулю p. Тогда существует вычет x_0 из приведенной системы вычетов такой, что $x_0^2 \equiv a \pmod{p}$. Все вычеты из приведенной системы вычетов исчерпываются следующими:

$$-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2}.$$

Их квадраты $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$, являются несравнимыми по модулю p. Следовательно, они представляют собой все $\frac{p-1}{2}$ квадратичных вычетов по модулю p. Остальные $\frac{p-1}{2}$ вычетов из приведенной системы вычетов являются квадратичными невычетами по модулю p. ◄

4. Пусть все числа $1, 2, \ldots, p-1$ разбиты на две совокупности, причем вторая из них содержит не менее одного числа. Кроме того, имеем:

1) произведение чисел одной совокупности сравнимо по модулю p с числом первой совокупности,

2) произведение двух чисел различных совокупностей сравнимо по модулю p с числом второй совокупности.

Эти условия являются необходимыми и достаточными для того, чтобы первая совокупность состояла из всех квадратичных вычетов по модулю p, а вторая — из всех квадратичных невычетов по модулю p.

► Согласно условию 1) среди чисел первой совокупности окажутся все квадратичные вычеты по модулю p :

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

Поскольку вторая совокупность содержит по крайней мере одно число, это число будет квадратичным невычетом по модулю p. Следовательно, по условию 2) второй совокупности принадлежат все квадратичные невычеты по модулю p. ◄

5. Для любого простого числа p сравнение

$$(x^2 - 2)(x^2 - 3)(x^2 - 6) \equiv 0 \pmod{p}$$

имеет решение.

► Это сравнение имеет решение, поскольку хотя бы одно из чисел $2, 3, 6$ является квадратичным вычетом по модулю p. ◄

6. Пусть $c_1, \ldots, c_m$ — различные корни сравнения

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}, (a_n, p) = 1,$$

где коэффициенты многочлена $f(x)$ — целые числа. Тогда многочлен $f(x)$ можно представить в виде

$$f(x) = (x - c_1) \ldots (x - c_m) g(x) + p h(x),$$

причем степень многочлена $g(x)$ равна $n - m$ и степень многочлена $h(x)$ не превосходит $m - 1$. Кроме того, m — количество корней сравнения $f(x) \equiv 0 \pmod{p}$ не превосходит его степени n.

► Применим метод математической индукции по m. При $m = 1$ запишем многочлен $f(x)$ по формуле Тейлора в точке $x = c_1$. Получим

$$f(x) = a_n (x - c_1)^n + b_{n-1}(x - c_1)^{n-1} + \cdots + b_1 (x - c_1) + b_0,$$

причем коэффициенты $b_{n-1}, \ldots, b_1, b_0$ однозначно определяются по коэффициентам $a_n, a_{n-1}, \ldots, a_1, a_0$. Поскольку $f(c_1) \equiv 0 \pmod{p}$, коэффициент b_0 делится на p, т.е. $b_0 = p b_0'$. Тем самым, многочлен

$f(x)$ представлен в виде $f(x) = (x - c_1)g_1(x) + ph_1(x), h_1(x) = b_0'$. Кроме того, имеем $m = 1 \leqslant n$.

Предположим утверждение верно для $m-1$ корня $c_1, \ldots, c_{m-1}$ сравнения $f(x) \equiv 0 \pmod p$. Тогда многочлен $f(x)$ представляется в виде $f(x) = (x - c_1) \ldots (x - c_{m-1})g_{m-1}(x) + ph_{m-1}(x)$ и $m - 1 \leqslant n$. Подставим $x = c_m$ в многочлен $f(x)$. Получим

$$f(c_m) \equiv (c_m - c_1) \ldots (c_m - c_1)g_{m-1}(c_m) \pmod p.$$

Поскольку корни $c_1, \ldots, c_{m-1}, c_m$ различны по модулю p, то $g_{m-1}(c_m) \equiv 0 \pmod p$. Следовательно, по доказанному при некотором целом числе d_0 имеем $g_{m-1}(x) = (x - c_m)g_m(x) + pd_0$. Подставляя это равенство в выражение для $f(x)$, найдем

$$\begin{aligned} f(x) &= (x - c_1) \ldots (x - c_m)g_m(x) + ph_m(x), h_m(x) = \\ &= (x - c_1) \ldots (x - c_{m-1})d_0 + h_{m-1}(x). \end{aligned}$$

Кроме того, из сравнения степеней имеем $m \leqslant n$. ◀

Символ Лежандра $\left(\frac{a}{p}\right)$ определяется следующим образом. Он равен 1, если сравнение (1) разрешимо и равен -1, если сравнение (1) не имеет решений.

7. (*Критерий Эйлера*). Справедливо сравнение

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

Другими словами, для того чтобы вычет a по модулю p являлся квадратичным вычетом по модулю p, необходимо и достаточно, чтобы выполнялось сравнение

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

▶ По малой теореме Ферма имеем сравнение

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

Оно эквивалентно следующему

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

Оба сомножителя в последнем сравнении не могут одновременно делиться на p, поскольку их разность 2 не делится на p. Сравнению

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

удовлетворяют все $\frac{p-1}{2}$ квадратичных вычетов по модулю p. Так как сравнение не может иметь решений больше его степени, то квадратичными вычетами по модулю исчерпываются все его решения. Следовательно, сравнению

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

удовлетворяют только квадратичные невычеты по модулю p. ◄

8. Имеют место следующие равенства

$$\alpha)\ \left(\frac{1}{p}\right) = 1, \quad \beta)\ \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \gamma)\ \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

$$\delta)\ \left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right) \text{ для } (b,p) = 1.$$

► По критерию Эйлера (задача 6), подставляя значения a, равные $1, -1, ab$, получим утверждения $\alpha), \beta), \gamma)$. Так как для $(b,p) = 1$ имеем $\left(\frac{b^2}{p}\right) = 1$, то из $\gamma)$ следует $\delta)$. ◄

9. Имеем $\sum\limits_{x=1}^{p-1} \left(\frac{x}{p}\right) = 0$. Кроме того, если $(a,p) = 1$ и b — произвольное число, то $\sum\limits_{x=0}^{p-1} \left(\frac{ax+b}{p}\right) = 0$.

► Поскольку количество квадратичных вычетов и невычетов по модулю p одинаково, то сумма $\sum\limits_{x=1}^{p-1} \left(\frac{x}{p}\right)$ равна нулю. При $(a,p) = 1$ и произвольном b, если x пробегает полную систему вычетов по модулю p, то $ax + b$ будет пробегать полную систему вычетов по модулю p. Следовательно,

$$\sum_{x=0}^{p-1} \left(\frac{ax+b}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) = 0. \blacktriangleleft$$

10. Пусть n является квадратичным невычетом по модулю p. Тогда имеем

$$\sum_{d|n} d^{\frac{p-1}{2}} \equiv 0 \pmod{p}.$$

▶ По критерию Эйлера имеем

$$\sum_{d|n} d^{\frac{p-1}{2}} \equiv \sum_{d|n} \left(\frac{d}{p}\right) \pmod{p}.$$

Пусть $n = \prod\limits_{q|n} q^{a_q}$ — каноническое разложение числа n на простые сомножители. Тогда свойству мультипликативности символа Лежандра имеем

$$\sum_{d|n} \left(\frac{d}{p}\right) = \prod_{q|n} \left(1 + \left(\frac{q}{p}\right) + \cdots + \left(\frac{q^{a_q}}{p}\right)\right).$$

Так как $\left(\frac{n}{p}\right) = -1$, то при некотором $q \mid n$ имеем $\left(\frac{q^{a_q}}{p}\right) = -1$. Следовательно, одна из скобок последнего произведения обращается в нуль. ◀

11. Пусть n_p — наименьший положительный квадратичный невычет по модулю p. Тогда имеем

$$n_p < \frac{1}{2} + \sqrt{\frac{1}{4} + p}.$$

▶ Так как n_p — наименьший положительный квадратичный невычет по модулю p, то вычеты $n_p, \ldots, (n_p - 1)n_p$ будут являться квадратичными невычетами по модулю p. Далее имеем $n_p(n_p - 1) < p$. В противном случае нашлось бы число k такое, что $(k-1)n_p < p < kn_p$. Следовательно, вычет kn_p был бы наименьшим положительным квадратичным невычетом по модулю p, что противоречит выбору n_p. Неравенство $n_p^2 - n_p - p < 0$ справедливо при $n_p < \frac{1}{2} + \sqrt{\frac{1}{4} + p}$. ◀

12. Пусть $(a, p) = 1, p_1 = \frac{p-1}{2}$, и имеет место сравнение

$$ax \equiv \varepsilon_x r_x \pmod{p}, 1 \leqslant x, r_x \leqslant p_1, \tag{2}$$

где ε_x равно либо 1, либо -1. Тогда имеем

$$\varepsilon_x = (-1)^{[2ax/p]}.$$

▶ Преобразуем $[2ax/p]$. Имеем

$$\left[\frac{2ax}{p}\right] = \left[2\left[\frac{ax}{p}\right] + 2\left\{\frac{ax}{p}\right\}\right] = 2\left[\frac{ax}{p}\right] + \left[2\left\{\frac{ax}{p}\right\}\right].$$

Таким образом, число $[2ax/p]$ будет четным, если наименьший неотрицательный вычет числа ax по модулю p не превосходит p_1, т.е. $\varepsilon_x = 1$; число $[2ax/p]$ будет нечетным, если наименьший неотрицательный вычет числа ax по модулю p превосходит p_1, т.е. $\varepsilon_x = -1$. Следовательно, $\varepsilon_x = (-1)^{[2ax/p]}$. ◀

13. (*Гаусс*). Пусть $(a, p) = 1, p_1 = \frac{p-1}{2}$. Тогда имеем

$$\left(\frac{a}{p}\right) = (-1)^{\alpha_{a,p}},\ \alpha_{a,p} = \sum_{x=1}^{p_1} \left[\frac{2ax}{p}\right].$$

▶ Перемножая сравнения (2) предыдущей задачи, получим

$$a^{\frac{p-1}{2}} p_1! \equiv \varepsilon_1 \dots \varepsilon_{p_1} r_1 \dots r_{p_1} \pmod{p}.$$

Поскольку $p_1! = r_1 \dots r_{p_1}$, отсюда имеем

$$a^{\frac{p-1}{2}} \equiv \varepsilon_1 \dots \varepsilon_{p_1} \pmod{p}.$$

Далее, используя критерий Эйлера и утверждение предыдущей задачи, найдем

$$\left(\frac{a}{p}\right) = (-1)^{\alpha_{a,p}},\ \alpha_{a,p} = \sum_{x=1}^{p_1} \left[\frac{2ax}{p}\right]. \blacktriangleleft$$

14. Пусть $(a, p) = 1, (a, 2) = 1, p_1 = \frac{p-1}{2}$. Тогда имеем

$$\left(\frac{2a}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\beta_{a,p}},\ \beta_{a,p} = \sum_{x=1}^{p_1} \left[\frac{ax}{p}\right] + \frac{p^2-1}{8}.$$

▶ Поскольку a — нечетное, число $a+p$ будет четным. Используя свойство мультипликативности символа Лежандра и утверждение предыдущей задачи, получим цепочку равенств

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) = (-1)^{\alpha((a+p)/2,p)}.$$

Следовательно,

$$\alpha((a+p)/2, p) = \sum_{x=1}^{p_1} \left[\frac{(a+p)x}{p}\right] = \sum_{x=1}^{p_1} \left[\frac{ax}{p}\right] + \sum_{x=1}^{p_1} x = \beta(a, p). \blacktriangleleft$$

15. (*Второе дополнительное соотношение квадратичного закона взаимности*). Справедливо равенство

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

► В утверждении предыдущей задачи подставим $a = 1$, получим искомую формулу. ◄

16. Пусть $p \equiv 3 \pmod 4$ и $q = 2p + 1$ — простые числа. Тогда число Мерсенна $M_p = 2^p - 1$ является составным и число q будет его делителем.

► По малой теореме Ферма имеем

$$2^{2p} - 1 \equiv 0 \pmod q, \quad (2^p - 1)(2^p + 1) \equiv 0 \pmod q.$$

Поскольку числа $2^p - 1$ и $2^p + 1$ взаимно просты, то число q может делить только одно из них. По утверждению предыдущей задачи число 2 является квадратичным вычетом по модулю q. Действительно,

$$\left(\frac{2}{q}\right) = (-1)^{\frac{1}{8}((2p+1)^2-1)} = (-1)^{\frac{p(p+1)}{2}} = 1.$$

По критерию Эйлера это утверждение эквивалентно тому, что $2^p \equiv 1 \pmod q$. ◄

17. Пусть $(a, p) = 1, (a, 2) = 1, p_1 = \frac{p-1}{2}$. Тогда имеем

$$\left(\frac{a}{p}\right) = (-1)^{\alpha_{a,p}},\ \alpha_{a,p} = \sum_{x=1}^{p_1} \left[\frac{ax}{p}\right].$$

► Утверждение этой задачи следует из утверждений задач 14 и 15. ◄

18. (*Квадратичный закон взаимности*). Пусть p, q — различные нечетные простые числа. Тогда имеем

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

► Из утверждения задачи 15 имеем

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

Величина $\alpha(q,p)+\alpha(p,q)$ равна

$$\sum_{x=1}^{p_1}\left[\frac{qx}{p}\right]+\sum_{y=1}^{q_1}\left[\frac{px}{q}\right].$$

Но последняя сумма равна количеству целых точек внутри прямоугольника со сторонами $0<x<p/2$ и $0<y<q/2$, т.е. равна $\frac{p-1}{2}\frac{q-1}{2}$. Диагональ $y=\frac{qx}{p}$ этого прямоугольника делит его на два треугольника. Количество целых точек треугольника, лежащего под этой диагональю равно $\alpha(q,p)$, а количество целых точек треугольника, лежащего над этой диагональю равно $\alpha(p,q)$. Это и доказывает искомое утверждение. ◄

19. Справедливы соотношения:

$$1)\quad \left(\frac{3}{p}\right)=\begin{cases}1, & \text{если} \quad p\equiv\pm1 \pmod{12}\\ -1, & \text{если} \quad p\equiv\pm5 \pmod{12},\end{cases}$$

$$2)\quad \text{при } p>3 \quad \text{имеем } \left(\frac{-3}{p}\right)=\left(\frac{p}{3}\right).$$

► 1). По квадратичному закону взаимности имеем

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

Далее, по свойству символа Лежандра при $p\geqslant 3$ получим

$$\left(\frac{p}{3}\right)=\begin{cases}\left(\frac{1}{3}\right)=1, & \text{если} \quad p\equiv1 \pmod 3\\ \left(\frac{-1}{3}\right)=-1, & \text{если} \quad p\equiv2 \pmod 3\end{cases}$$

Наконец, имеем

$$(-1)^{\frac{p-1}{2}}=\begin{cases}1, & \text{если}\, p\equiv1 \pmod 4\\ -1, & \text{если}\, p\equiv-1 \pmod 4\end{cases}$$

Отсюда следует искомая формула.

2). Используя предыдущее утверждение, имеем

$$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right). \blacktriangleleft$$

20. а). Сравнение $x^2+1\equiv 0 \pmod p$ разрешимо тогда и только тогда, когда $p\equiv 1 \pmod 4$.

б). Сравнение $x^2+3\equiv 0 \pmod p$ разрешимо тогда и только тогда, когда $p\equiv 1 \pmod 6$.

в). Простых чисел вида $p\equiv 1 \pmod 4$ бесконечно много.

г). Простых чисел вида $p\equiv 1 \pmod 6$ бесконечно много.

д). Сравнение $x^2+2\equiv 0 \pmod p$ разрешимо тогда и только тогда, когда $p\equiv 1 \pmod 8$ или $p\equiv 3 \pmod 8$.

► а). Условие разрешимости сравнения $x^2+1\equiv 0 \pmod p$ эквивалентно тому, что символ Лежандра $\left(\frac{-1}{p}\right)$ равен 1. По первому дополнительному соотношению квадратичного закона взаимности имеем

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1, & \text{если } p\equiv 1 \pmod 4,\\ -1, & \text{если } p\equiv -1 \pmod 4.\end{cases}$$

б). Имеем

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

в). Предположим, что простых чисел вида $p\equiv 1 \pmod 4$ конечное число: $p_1,\dots,p_n$. Число $(2p_1\dots p_n)^2+1$ в качестве своих простых делителей будет иметь только простые числа вида $4k+1$ и они все будут отличны от чисел $p_1,\dots,p_n$. Наименьший, отличный от единицы, среди делителей числа $(2p_1\dots p_n)^2+1$ будет простым. Это противоречит предположению об исчерпании всех простых вида $4k+1$ числами $p_1,\dots,p_n$. Следовательно, простых чисел вида $p\equiv 1 \pmod 4$ бесконечно много.

г). Пусть простые числа вида $6k+1$ исчерпываются числами $p_1,\dots,p_n$. Число $(2p_1\dots p_n)^2+3$ имеет простые делители только вида $6k+1$, наименьший из которых, отличный от единицы, будет простым и отличным от $p_1,\dots,p_n$. Следовательно, предположение о том, что простых чисел вида $6k+1$ конечно, не имеет места.

д). Разрешимость сравнения $x^2+2\equiv 0 \pmod p$ эквивалентна условию $\left(\frac{-2}{p}\right)=1$. По дополнительным соотношениям квадратичного закона взаимности имеем

$$\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{2}+\frac{p^2-1}{8}}=(-1)^{\frac{(p-1)(p+5)}{8}}.$$

Следовательно,

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

21. При нечетном простом числе p число -4 будет биквадратичным вычетом по модулю p тогда и только тогда, когда $p \equiv 1 \pmod 4$.

► Из тождества

$$x^4 + 4 = ((x+1)^2 + 1)((x-1)^2 + 1)$$

следует, что число -4 будет биквадратичным вычетом по модулю p тогда и только тогда, когда число -1 будет квадратичным вычетом по модулю p. По утверждению предыдущей задачи последнее эквивалентно тому, что $p \equiv 1 \pmod 4$. ◄

22. Пусть $p \equiv 5 \pmod 8$. Тогда сравнение $x^4 + 1 \equiv 0 \pmod p$ не имеет решений.

► Предположим противное. Пусть существует решение x_0 сравнения $x_0^4 + 1 \equiv 0 \pmod p$. Справедливо равенство $p - 1 = 4u$, где u — нечетное число. Тогда имеет место следующая противоречивая цепочка сравнений

$$-1 \equiv x_0^4 \pmod p, -1 = (-1)^u \equiv x_0^{4u} \equiv x_0^{p-1} \equiv 1 \pmod p.$$

Следовательно, предположение о разрешимости сравнения $x^4 + 1 \pmod p$ неверно. ◄

23. а). При нечетном простом числе p число -1 будет биквадратичным вычетом по модулю p тогда и только тогда, когда $p \equiv 1 \pmod 8$.

б). Существует бесконечно много простых чисел вида $8k + 1$.

► а). Пусть $p \equiv 1 \pmod 8$. Тогда $(p-1)/2$ квадратичный вычет по модулю p удовлетворяет сравнению $x^{(p-1)/2} \equiv 1 \pmod p$. Предположим, теперь, что сравнение $x^4 \equiv -1 \pmod p$ не имеет решений. Тогда сравнению $x^{(p-1)/4} \equiv 1 \pmod p$ не удовлетворяет ни один квадратичный вычет по модулю p. Поскольку они удовлетворяют либо сравнению $x^{(p-1)/4} \equiv 1 \pmod p$, либо сравнению $x^{(p-1)/4} \equiv -1 \pmod p$, все $(p-1)/2$ квадратичных вычета по модулю p удовлетворяют второму сравнению. Но это невозможно, поскольку количество несравнимых вычетов по модулю p не превосходит степени сравнения $(p-1)/4$. Следовательно, сравнение $x^4 + 1 \equiv 0 \pmod p$ имеет по крайней мере одно решение.

По предыдущей задаче для $p \equiv 5 \pmod 8$ сравнение $x^4 + 1 \equiv 0 \pmod p$ не имеет решений.

Пусть $p \equiv 3$ или $7 \pmod 8$, т.е. $p \equiv 3 \pmod 4$. Но тогда даже сравнение $x^2 + 1 \equiv 0 \pmod p$ не имеет решений.

б). Пусть существует только конечное число простых чисел вида $8k+1$. Буквой P обозначим их произведение. Тогда по утверждению предыдущей задачи число $(2P)^4 + 1$ будет иметь простые делители вида $8k + 1$ и они будут взаимно просты с P. Таким образом, предположение о существовании только конечного числа простых чисел вида $8k + 1$ неверно. ◄

24. Пусть k — натуральное число, p — простое число и $p \equiv 2^k + 1 \pmod{2^{k+1}}$. Тогда сравнение $x^{2^k} + 1 \equiv 0 \pmod p$ не имеет решений.

► Предположим противное. Пусть существует решение x_0 сравнения $x_0^{2^k} + 1 \equiv 0 \pmod p$. Справедливо равенство $p - 1 = 2^k u$, где u — нечетное число. Тогда имеет место следующая противоречивая цепочка сравнений

$$-1 \equiv x_0^{2^k} \pmod p, -1 = (-1)^u \equiv x_0^{2^k u} \equiv x_0^{p-1} \equiv 1 \pmod p.$$

Следовательно, предположение о разрешимости сравнения $x^{2^k} + 1 \pmod p$ неверно. ◄

25. Пусть k — натуральное число и сравнение $x^{2^k} + 1 \equiv 0 \pmod p$ разрешимо. Тогда $p \equiv 1 \pmod{2^{k+1}}$.

► Представим число $p - 1$ в виде $p - 1 = 2^r u$, где u — нечетное число. Предположим, что $r \leqslant k$. По условию задачи существует решение x_0 сравнения $x_0^{2^k} \equiv -1 \pmod p$. Тогда имеет место следующая противоречивая цепочка сравнений

$$-1 = (-1)^u \equiv x_0^{2^k u} \equiv x_0^{2^{k-r} 2^r u} \equiv x_0^{2^{k-r}(p-1)} \equiv 1 \pmod p.$$

Следовательно, предположение, что $r \leqslant k$ неверно, и $p \equiv 1 \pmod{2^{k+1}}$. ◄

26. Пусть a — одно из чисел 2 или 3, число p — нечетное простое, и сравнение $z^2 + a \equiv 0 \pmod p$ разрешимо. Тогда существует единственное представление числа p в виде $p = x^2 + ay^2$, где x, y — натуральные числа, $x \equiv zy \pmod p$.

► Пусть $|z_0| \leqslant \frac{p-1}{2}$ решение сравнения $z_0^2 + a \equiv 0 \pmod p$. Тогда получим $mp = z_0^2 + a$. Оценим величину m. Имеем

$$1 \leqslant m = \frac{1}{p}(z_0^2 + a) \leqslant \frac{1}{p}\left(\frac{(p-1)^2}{4} + a\right) \leqslant \frac{p^2 - 2p + 13}{4p} < p.$$

Пусть m_0 — наименьшее натуральное число в представлении вида $m_0 p = x^2 + ay^2$. Тогда из доказанного выше находим $1 \leqslant m_0 < p$. Предположим, что $m_0 > 1$. Возьмем числа u, v из условий

$$u \equiv x \pmod{m_0}, v \equiv y \pmod{m_0}, 1 \leqslant |u| \leqslant m_0/2, 1 \leqslant |v| \leqslant m_0/2.$$

Тогда получим

$$u^2 + av^2 \equiv x^2 + ay^2 \equiv 0 \pmod{m_0}$$

Следовательно, при некотором r имеем $m_0 r = u^2 + av^2$, где либо $r \leqslant \frac{(1+a)m_0}{4} < m_0$, либо $r = m_0, u = m_0/2, v = m_0/2, a = 3$. Последний случай не возможен, поскольку

$$x = y = m_0/2 = u = v, m_0 p = x^2 + 3y^2 = u^2 + 3v^2 = m_0^2, 1 < m_0 < p.$$

Таким образом

$$\begin{aligned} m_0^2 rp &= (x^2 + ay^2)(u^2 + av^2) = x^2u^2 + a^2y^2v^2 + a(x^2v^2 + y^2u^2) = \\ &= (xu + ayv)^2 + a(xv - yu)^2. \end{aligned}$$

Кроме того, справедливы сравнения

$$xv - yu \equiv xy - yx \equiv 0 \pmod{m_0}, xu + ayv \equiv x^2 + ay^2 \equiv 0 \pmod{m_0}.$$

Из последних соотношений получим

$$rp = X^2 + aY^2, 1 \leqslant r < m_0.$$

Это противоречит тому, что $m_0 > 1$ — минимальное число в указанном представлении. Следовательно, $m_0 = 1$.

Докажем, что представление вида $p = x^2 + ay^2, x \equiv zy \pmod{p}$ — единственно. Пусть $p = x_1^2 + ay_1^2, x_1 \equiv zy_1 \pmod{p}$ — другое представление простого числа p. Тогда

$$p^2 = (x^2 + ay^2)(x_1^2 + ay_1^2) = (xx_1 + ayy_1)^2 + a(xy_1 - yx_1)^2$$

Поскольку $xy_1 - yx_1 \equiv 0 \pmod{p}$, имеем $xy_1 - yx_1 = 0$. Следовательно, $xx_1 + ayy_1 = p$. Отсюда получим

$$xp = x(xx_1 + ayy_1) - ay(xy_1 - yx_1) = x^2x_1 + ay^2x_1 = x_1(x^2 + ay^2) = x_1 p,$$

т.е. $x = x_1, y = y_1$. ◀

27. Пусть $p \equiv 1 \pmod 4, (k,p) = 1$,

$$S(k) = \sum_{x=0}^{p-1} \left(\frac{x(x^2+k)}{p} \right).$$

Тогда 1) $S(k)$ — четное число,
2) $S(kt^2) = \left(\frac{t}{p}\right) S(k)$,
3) при $\left(\frac{r}{p}\right) = 1$ и $\left(\frac{n}{p}\right) = -1$ имеем

$$p = \left(\frac{S(r)}{2} \right)^2 + \left(\frac{S(n)}{2} \right)^2,$$

4) справедливо неравенство $|S(k)| \leqslant 2\sqrt{p}$.

► 1). Поскольку $\left(\frac{-1}{p}\right) = 1$, слагаемые, отвечающие $x = x_1$ и $x = -x_1$, равны между собой, а слагаемое, отвечающее $x = 0$, равно 0. Следовательно, $S(k)$ — четное число.

2). Имеем

$$S(kt^2) = \sum_{x=0}^{p-1} \left(\frac{xt(x^2t^2+kt^2)}{p} \right) = \left(\frac{t}{p} \right) S(k).$$

3). Положим $p_1 = (p-1)/2$. Поскольку для любого числа t от 1 до p_1 справедливы равенства

$$S^2(rt^2) = S^2(r), S^2(nt^2) = S^2(n), S(0) = 0,$$

где r — некоторый квадратичный вычет и n — некоторый квадратичный невычет по модулю p.

Заметим, что, если t пробегает все числа от 1 до p_1, то rt^2 пробегает все квадратичные вычеты, а nt^2 — все квадратичные невычеты по модулю p. Следовательно,

$$p_1(S^2(r) + S^2(n)) = \sum_{t=1}^{p_1} S^2(rt^2) + \sum_{t=1}^{p_1} S^2(nt^2) + S^2(0) =$$

$$= \sum_{k=0}^{p-1} S^2(k) = \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \left(\frac{xy}{p} \right) \sum_{k=0}^{p-1} \left(\frac{(x^2+k)(y^2+k)}{p} \right).$$

Далее имеем

$$T(x,y)=\sum_{k=0}^{p-1}\left(\frac{(x^2+k)(y^2+k)}{p}\right)=\sum_{k=1}^{p-1}\left(\frac{k(y^2-x^2+k)}{p}\right).$$

Следовательно, при $kk_1\equiv 1 \pmod p$ имеем

$$T(x,y)=\sum_{k=1}^{p-1}\left(\frac{kk_1((y^2-x^2)k_1+kk_1)}{p}\right)=\sum_{k=1}^{p-1}\left(\frac{(y^2-x^2)k+1)}{p}\right).$$

Таким образом

$$T(xy)=\begin{cases}p-1, & \text{если} \quad x\equiv\pm y \pmod p,\\ -1, & \text{если} \quad x\not\equiv\pm y \pmod p.\end{cases}$$

Наконец, получаем

$$p_1(S^2(r)+S^2(n))=\sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\left(\frac{xy}{p}\right)T(x,y)=\sum_{x=1}^{p-1}(T(x,x)+T(x,-x))+$$

$$+\sum_{\substack{x=1\\ x\not\equiv\pm y \pmod p}}^{p-1}\sum_{y=1}^{p-1}\left(\frac{xy}{p}\right)T(x,y)=2(p-1)^2-2(p-1)(-1)=2(p-1)p.$$

Отсюда имеем искомую формулу

$$p=\left(\frac{S(r)}{2}\right)^2+\left(\frac{S(n)}{2}\right)^2.$$

4) Из утверждения 3) следует, что $|S(k)|\leqslant 2\sqrt{p}$. ◄

28. Число 2 является квадратичным невычетом по модулю нечетного простого числа p тогда и только тогда, когда имеет вид $4k+3$, где k — любое натуральное число.

► По второму дополнительному соотношению квадратичного закона взаимности имеем

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

Отсюда получаем

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{если} \quad p \equiv 1 \pmod 4, \\ -1, & \text{если} \quad p \equiv 1 \pmod 4. \end{cases}$$

◄

29. Число 3 является наименьшим положительным квадратичным невычетом по модулю нечетного простого числа p тогда и только тогда, когда $p \equiv 5 \pmod{12}$. ► Имеем

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

Следовательно, $p \equiv 1 \pmod 4$, и по квадратичному закону взаимности получаем

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

Отсюда находим, что число p принадлежит прогрессиям $p \equiv 1 \pmod 4$ и $p \equiv 2 \pmod 3$. Из этого однозначно определяется прогрессия с разностью 12 и начальным членом 5 такая, что $p \equiv 5 \pmod{12}$. ◄

30. Пусть q_k — k-е простое число, которое является наименьшим положительным квадратичным невычетом по модулю p. Тогда число p принадлежит одной из $\varphi(4q_2 \dots q_k)/2^k$ с разностью $4q_2 \dots q_k$ и некоторыми начальными членами a, взаимно простыми с $4q_2 \dots q_k$.

► Используя квадратичный закон взаимности, найдем, что число p удовлетворяет условиям

$$p \equiv 1 \pmod 4, p \equiv 1 \pmod 3,$$

$$\left(\frac{p}{q_s}\right) = 1,\ s = 2, \dots, k-1; \left(\frac{p}{q_k}\right) = -1.$$

Отсюда и следует искомое утверждение. ◄

31. Имеем $\sum\limits_{x=1}^{p-2} \left(\frac{x(x+1)}{p}\right) = -1$.

► Определим вычет x_1 по модулю p из сравнения $xx_1 \equiv 1$

(mod p). Далее преобразуем сумму

$$\sum_{x=1}^{p-2}\left(\frac{x(x+1)}{p}\right)=\sum_{x=1}^{p-2}\left(\frac{x_1^2}{p}\right)\left(\frac{x(x+1)}{p}\right)=\sum_{x=1}^{p-2}\left(\frac{xx_1(xx_1+x_1)}{p}\right)=$$
$$=\sum_{x=1}^{p-2}\left(\frac{1+x_1)}{p}\right).$$

Поскольку при $1\leqslant x\leqslant p-2$ последовательность $1+x_1$ пробегает все вычеты приведенной системы вычетов по модулю p, кроме 1, искомая сумма будет равна -1. ◄

32. Пусть $p>2$ — простое число и N — количество натуральных чисел n с условием $1\leqslant n\leqslant p-2$ таких, что n и $n+1$ одновременно являются квадратичными вычетами по модулю p. Тогда имеем $N=\frac{1}{4}\left(p-4-\left(\frac{-1}{p}\right)\right)$.

► Имеем

$$N=\frac{1}{4}\sum_{n=1}^{p-2}\left(1+\left(\frac{n}{p}\right)\right)\left(1+\left(\frac{n+1}{p}\right)\right)=$$

$$=\frac{1}{4}\sum_{n=1}^{p-2}\left(1+\left(\frac{n}{p}\right)\right)\left(1+\left(\frac{n+1}{p}\right)\right)=$$

$$=\frac{1}{4}\sum_{n=1}^{p-2}\left(1+\left(\frac{n}{p}\right)+\left(\frac{n+1}{p}\right)+\left(\frac{n(n+1)}{p}\right)\right).$$

Отсюда следует искомая формула для N. ◄

33. Пусть $p>2$ — простое число и $f(x)=ax^2+bx+c$ — многочлен с целыми коэффициентами, $(a,p)=1$, и $\Delta=b^2-4ac$. Тогда имеем

$$S=\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)=\begin{cases}-\left(\frac{a}{p}\right), & \text{если} \quad p\not|\Delta, \left(\frac{\Delta}{p}\right)=1,\\ \left(\frac{a}{p}\right), & \text{если} \quad p\not|\Delta, \left(\frac{\Delta}{p}\right)=-1,\\ (p-1)\left(\frac{a}{p}\right), & \text{если} \quad p\mid\Delta.\end{cases}$$

► Имеем цепочку равенств

$$S=\sum_{x=0}^{p-1}\left(\frac{4a^2}{p}\right)\left(\frac{ax^2+bx+c}{p}\right)=\left(\frac{a}{p}\right)\sum_{x=0}^{p-1}\left(\frac{4a^2x^2+4abx+4ac}{p}\right)=$$

$$= \left(\frac{a}{p}\right) \sum_{x=0}^{p-1} \left(\frac{(2ax+b)^2 - \Delta}{p}\right) = \left(\frac{a}{p}\right) V,$$

где $V = V(\Delta) = \sum\limits_{x=0}^{p-1} \left(\frac{x^2-\Delta}{p}\right)$.

Рассмотрим случай $\left(\frac{\Delta}{p}\right) = 1$, т.е. при некотором d, взаимно простом с p, имеем $\Delta \equiv d^2 \pmod{p}$. Делая замену переменной x на dx, получим

$$V = \sum_{x=0}^{p-1} \left(\frac{x^2-1}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{x(x+2)}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{1+2x'}{p}\right),$$

где $xx' \equiv 1 \pmod{p}$.

Следовательно,

$$V = \sum_{x=0}^{p-1} \left(\frac{1+2x}{p}\right) - 1 = -1.$$

Пусть, теперь, $\left(\frac{\Delta}{p}\right) = -1$ и число n обозначает наименьший невычет по модулю p. Тогда имеем

$$\sum_{\Delta=1}^{p-1} V(\Delta) = \frac{p-1}{2}(V(1) + V(n)) = 0.$$

Отсюда получаем искомую формулу для суммы S. ◄

34. Пусть $p > 2$ — простое число $(a, p) = 1$ и τ_a — сумма Гаусса вида

$$\tau_a = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e^{2\pi i \frac{ax}{p}}, \tau = \tau_1.$$

Тогда имеем

$$\tau_a = \left(\frac{a}{p}\right) \tau, \quad |\tau| = \sqrt{p}.$$

► Имеем

$$\tau_a = \sum_{x=1}^{p-1} \left(\frac{a^2}{p}\right) \left(\frac{x}{p}\right) e^{2\pi i \frac{ax}{p}} = \left(\frac{a}{p}\right) \sum_{x=1}^{p-1} \left(\frac{ax}{p}\right) e^{2\pi i \frac{ax}{p}} = \left(\frac{a}{p}\right) \tau.$$

Преобразуем квадрат модуля суммы Гаусса, делая замену переменной суммирования $y = tx$. Получим

$$|\tau|^2 = \tau\bar{\tau} = \sum_{x=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{x}{p}}\sum_{y=1}^{p-1}\left(\frac{y}{p}\right)e^{-2\pi i\frac{y}{p}} =$$

$$= \sum_{x=1}^{p-1}\sum_{t=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{x(1-t)}{p}} = \sum_{t=1}^{p-1}\left(\frac{x}{p}\right)\sum_{x=1}^{p-1}e^{2\pi i\frac{x(1-t)}{p}}.$$

При $t = 1$ сумма по x равна $p-1$, а при $t \neq 1$ она равна $-\left(\frac{t}{p}\right)$. Следовательно, имеем

$$|\tau|^2 = p - 1 - \sum_{t=2}^{p-1}\left(\frac{t}{p}\right) = p, |\tau| = \sqrt{p}. \blacktriangleleft$$

35. Пусть $m > 2, (a, m) = 1$,

$$S_{a,m} = \sum_{x=0}^{m-1} e^{2\pi i\frac{ax^2}{m}}.$$

Тогда

a) при любом простом числе p имеем

$$S_{a,p} = \tau_a, |S_{a,p}| = \sqrt{p};$$

b) справедливы следующие соотношения

$$|S_{a,m}| = \begin{cases} \sqrt{m}, & \text{если} \quad m \equiv 1 \pmod 2, \\ 0, & \text{если} \quad m \equiv 2 \pmod 4, \\ \sqrt{2m}, & \text{если} \quad m \equiv 0 \pmod 4, \end{cases}$$

c) имеем равенство

$$S_{1,m} = \frac{1 + i^{-m}}{1 + i^{-1}}\sqrt{m};$$

d) при $m > 1, (2A, m) = 1$ и любом целом числе a имеем

$$\left|\sum_{x=0}^{m-1} e^{2\pi i\frac{Ax^2+ax}{m}}\right| = \sqrt{m}.$$

► a). Имеем

$$S_{a,p} = \sum_{x=0}^{p-1} e^{2\pi i \frac{ax^2}{p}} = 1 + \sum_{y=1}^{p-1} \left(1 + \left(\frac{y}{p}\right)\right) e^{2\pi i \frac{ay}{p}},$$

так как

$$1 + \left(\frac{y}{p}\right) = \begin{cases} 2, & \text{если} \quad y \equiv x^2 \pmod p, \\ 0, & \text{если} \quad y \not\equiv x^2 \pmod p. \end{cases}$$

Таким образом, получим

$$S_{a,p} = 1 + \sum_{x=1}^{p-1} e^{2\pi i \frac{ax}{p}} + \tau_a = \tau_a.$$

Следовательно, по утверждению предыдущей задачи имеем

$$|S_{a,p}| = |\tau_a| = |\tau| = \sqrt{p}.$$

b). Преобразуем модуль суммы $S_{a,m}$, делая замену переменной $y = x + t$. Получим

$$|S_{a,m}|^2 = \sum_{x=0}^{m-1} \sum_{y=0}^{m-1} e^{2\pi i \frac{x^2 - y^2}{m}} = \sum_{t=0}^{m-1} e^{-2\pi i \frac{at^2}{m}} \sum_{x=0}^{m-1} e^{-2\pi i \frac{2atx}{m}}.$$

Далее, имеем

$$\sum_{x=0}^{m-1} e^{-2\pi i \frac{2atx}{m}} = \begin{cases} m, & \text{если} \quad m \mid 2t, \\ 0, & \text{если} \quad m \not| 2t. \end{cases}$$

Следовательно, при $m \equiv 1 \pmod 2$ имеем

$$|S_{a,m}|^2 = m e^{-2\pi i \frac{a \cdot 0^2}{m}} = m, \quad |S_{a,m}| = \sqrt{m}.$$

Пусть, теперь, $m = 2m_1$ — четное число. Тогда имеем

$$|S_{a,m}|^2 = m \left(e^{-2\pi i \frac{a \cdot 0^2}{m}} + e^{-2\pi i \frac{a \cdot m_1^2}{m}} \right) = m \left(1 + e^{-2\pi i \frac{a m_1}{2}}\right).$$

Отсюда получим

$$|S_{a,m}|^2 = \begin{cases} 0, & \text{если} \quad m_1 \equiv 1 \pmod 2, \\ 2m, & \text{если} \quad m_1 \equiv 0 \pmod 2. \end{cases}$$

Последние соотношения влекут искомые равенства.

c). Воспользуемся формулой Пуассона суммирования значений функции в целых точках в следующем виде. Пусть a и b — полуцелые числа, $f(x)$ имеет непрерывную первую производную на отрезке $[a,b]$ и $M = \max\limits_{x\in[a,b]} |f'(x)|$. Тогда при любом $K \geqslant 1$ справедливо соотношение

$$\sum_{a<n\leqslant b} f(n) = \sum_{k=-K}^{K} \int_a^b f(x)e^{2\pi ikx}\,dx + R, \quad |R| \leqslant \frac{8M(b-a)\ln K}{K}.$$

При $K \geqslant 1$ получим

$$S_{1,m} = \sum_{n=1}^{m} e^{2\pi i\frac{n^2}{m}} = \sum_{k=-2K}^{2K} I_k + R,$$

где

$$I_k = \int_{0,5}^{N+0,5} e^{2\pi i\left(\frac{x^2}{m}+kx\right)}, |R| \ll \frac{m\ln K}{K}.$$

Преобразуем интеграл I_k. Имеем

$$I_k = e^{-\frac{\pi i}{2}k^2m} \int_{0,5}^{m+0,5} e^{\frac{2\pi i}{m}(x+0,5km)^2}\,dx = e^{-\frac{\pi i}{2}k^2m} \int_{0,5+0,5km}^{0,5+(1+0,5k)m} e^{\frac{2\pi i}{m}x^2}\,dx$$

Суммируя интегралы I_k отдельно по четным $k = 2l$ и по нечетным $k = 2l-1$, находим

$$S_{1,m} = \sum_{l=-K}^{K} \int_{0,5+lm}^{0,5+(1+l)m} e^{2\pi ix^2/m}\,dx + i^{-m} \int_{0,5+(l-0,5)m}^{0,5+(l+0,5)m} e^{2\pi ix^2/m}\,dx + R =$$

$$\sqrt{m}(1+i^{-m}) \int_{-\infty}^{\infty} e^{2\pi iz^2}\,dz + O(m^{1/4}K^{-1/2}) + R.$$

Переходя к пределу при $K \to \infty$, получим

$$S_{1,m} = \sqrt{m}(1+i^{-m}) \int_{-\infty}^{\infty} e^{2\pi iz^2}\,dz.$$

При $m = 1$ имеем $S_{1,1} = 1$. Следовательно,

$$1 = S_{1,1} = (1 + i^{-1}) \int\limits_{-\infty}^{\infty} e^{2\pi i z^2}\, dz.$$

Таким образом имеем

$$S_{1,m} = \frac{1 + i^{-m}}{1 + i^{-1}} \sqrt{m}.$$

d). Определим число b из сравнения $a \equiv 2Ab \pmod m$. Тогда имеем

$$|T_{A,m}| = \left| \sum_{x=0}^{m-1} e^{2\pi i \frac{A(x+b)^2}{m}} \right|$$

Так как m — нечетное число, то по утверждению предыдущей задачи имеем $|T_{A,m}| = |S_{A,m}| = \sqrt{m}$. ◄

36. Пусть p — нечетное простое число, M, Q — целые числа, $1 \leqslant M < M + Q \leqslant p$. Тогда

а) имеем неравенство

$$\left| \sum_{x=M}^{M+Q-1} \left(\frac{x}{p}\right) \right| \leqslant \sqrt{p} \ln p;$$

b) справедливы соотношения

$$|R - Q/2| < (\sqrt{p} \ln p)/2, \quad |N - Q/2| < (\sqrt{p} \ln p)/2,$$

где R — количество квадратичных вычетов и N — количество квадратичных невычетов по модулю p на отрезке от M до $M + Q - 1$.

► а). Имеем равенство

$$S = \sum_{x=M}^{M+Q-1} \left(\frac{x}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \sum_{y=M}^{M+Q-1} \left(\frac{1}{p} \sum_{a=0}^{p-1} e^{2\pi i \frac{a(x-y)}{p}} \right) =$$

$$= \frac{1}{p} \sum_{a=0}^{p-1} \left(\sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e^{2\pi i \frac{ax}{p}} \right) \left(\sum_{y=M}^{M+Q-1} e^{-2\pi i \frac{ay}{p}} \right) = \frac{1}{p} \sum_{a=1}^{p-1} \tau_a L_{a,p}.$$

Следовательно

$$|S| \leqslant \frac{1}{\sqrt{p}} \sum_{a=1}^{p-1} |L_{a,p}| = \frac{1}{\sqrt{p}} \sum_{a=1}^{p-1} \left| \frac{e^{-2\pi i \frac{aM}{p}} - e^{-2\pi i \frac{a(M+Q)}{p}}}{1 - e^{-2\pi i \frac{a}{p}}} \right| \leqslant$$

$$\leqslant \frac{1}{\sqrt{p}} \sum_{a=1}^{p-1} \frac{1}{|\sin(\frac{\pi a}{p})|} = \frac{2}{\sqrt{p}} \sum_{a=1}^{(p-1)/2} \frac{1}{\sin(\frac{\pi a}{p})}.$$

Поскольку при $0 \leqslant y \leqslant 1/2$ справедливо неравенство $\sin \pi y \geqslant 2y$, имеем оценку

$$|S| \leqslant \frac{1}{\sqrt{p}} \sum_{a=1}^{(p-1)/2} \frac{p}{a} \leqslant \sqrt{p} \left(\int_1^{\frac{p-1}{2}} \frac{dt}{t} + \left(\frac{1}{2} + \int_1^{\infty} \frac{\rho(t)}{t^2}\, dt \right) + \right.$$

$$\left. + \frac{1}{p-1} - \int_{\frac{p-1}{2}}^{\infty} \frac{\rho(t)}{t^2}\, dt \right) <$$

$$< \sqrt{p}(\ln((p-1)/2) + \gamma + \frac{1}{p-1}) < \sqrt{p} \ln p.$$

b). По утверждению предыдущей задачи имеем $|R-N| < \sqrt{p} \ln p$. Кроме того, $R+N=Q$. Отсюда следует искомое утверждение. ◄

37. Пусть p — нечетное простое число, $N \geqslant 1$, и

$$S = \max_N |T(N)|, \quad T(N) = \sum_{n=1}^{N} \left(\frac{n}{p} \right).$$

Тогда при $p \to \infty$ справедливо неравенство $S \leqslant (c+o(1))\sqrt{p} \ln p$, где

$$c = \begin{cases} 1/\pi^2, & \text{если} \quad \left(\frac{-1}{p}\right) = 1, \\ 1/(2\pi), & \text{если} \quad \left(\frac{-1}{p}\right) = -1. \end{cases}$$

► Пользуясь приемом И.М.Виноградова, получим

$$T(N) = \sum_{n=1}^{N} \left(\frac{n}{p} \right) = \sum_{n=1}^{p-1} \left(\frac{n}{p} \right) \sum_{m=1}^{N} \frac{1}{p} \sum_{a=0}^{p-1} e^{2\pi i \frac{a(n-m)}{p}} =$$

$$\frac{1}{p} \sum_{a=1}^{p-1} \left(\sum_{n=1}^{p-1} \left(\frac{n}{p} \right) e^{2\pi i \frac{an}{p}} \right) \left(\sum_{m=1}^{N} e^{-2\pi i \frac{am}{p}} \right).$$

Пользуясь периодичностью с периодом p всех функций в сумме $T(N)$, находим

$$T(N) = \frac{\tau}{p} \sum_{0<|a|\leqslant(p-1)/2} \left(\frac{a}{p} \right) \sum_{m=1}^{N} e^{-2\pi i \frac{am}{p}}.$$

Просуммируем геометрическую прогрессию. Имеем

$$\sum_{m=1}^{N} e^{-2\pi i \frac{am}{p}} = \frac{e^{-2\pi i \frac{a}{p}} - e^{-2\pi i \frac{a(N+1)}{p}}}{1 - e^{-2\pi i \frac{a}{p}}}.$$

Таким образом

$$T(N) = \frac{\tau}{p} \sum_{0<|a|\leqslant(p-1)/2} \left(\frac{a}{p}\right) \frac{e^{2\pi i \frac{aN}{p}} - 1}{1 - e^{2\pi i \frac{a}{p}}}.$$

Воспользуемся при $0 < |a| \leqslant (p-1)/2$ и $p \to \infty$ следующим асимптотическим соотношением

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

Рассмотрим сначала случай $\left(\frac{-1}{p}\right) = 1$. Получим

$$|T(N)| = \frac{\sqrt{p}}{2\pi} \left| \sum_{0<a\leqslant(p-1)/2} \left(\frac{a}{p}\right) \frac{e^{-2\pi i \frac{aN}{p}} - e^{2\pi i \frac{aN}{p}}}{a} \right| + O(\sqrt{p}) =$$

$$= \frac{\sqrt{p}}{\pi} \left| \sum_{0<a\leqslant(p-1)/2} \left(\frac{a}{p}\right) \frac{\sin 2\pi \frac{aN}{p}}{a} \right| + O(\sqrt{p}).$$

Так как для любого вещественного числа α справедливо неравенство

$$\sum_{n\leqslant x} \frac{|\sin(\alpha n)|}{n} \leqslant \frac{2}{\pi} \ln x + O(1), \qquad (*)$$

то имеем

$$|T(N)| \leqslant \frac{\sqrt{p}}{\pi} \sum_{0<a\leqslant(p-1)/2} \frac{\left|\sin 2\pi \frac{aN}{p}\right|}{a} + O(\sqrt{p}) \leqslant$$

$$\leqslant \frac{2\sqrt{p}}{\pi^2} \ln \frac{p-1}{2} (1 + o(1)).$$

Следовательно,

$$S = \max_{N\geqslant 1} |T(N)| \leqslant (\frac{2}{\pi^2} + o(1))\sqrt{p} \ln p.$$

Рассмотрим случай $\left(\frac{-1}{p}\right) = -1$. Объединяя в сумме $T(N)$ слагаемые, отвечающие значениям a и $-a$, получим

$$|T(N)| = \frac{\sqrt{p}}{2\pi}\left|\sum_{0<a\leqslant(p-1)/2}\left(\frac{a}{p}\right)\frac{e^{-2\pi i\frac{aN}{p}}+e^{2\pi i\frac{aN}{p}}-2}{a}\right| + O(\sqrt{p}) =$$

$$= \frac{\sqrt{p}}{\pi}\left|\sum_{0<a\leqslant(p-1)/2}\left(\frac{a}{p}\right)\frac{1-\cos 2\pi\frac{aN}{p}}{a}\right| + O(\sqrt{p}).$$

Далее, так как для любого вещественного α и $x \to \infty$ справедливо неравенство

$$\sum_{n\leqslant x}\frac{1-\cos(\alpha n)}{n} \leqslant \ln x + O(1), \qquad (**)$$

то

$$|T(N)| \leqslant \frac{\sqrt{p}}{\pi}\sum_{0<a\leqslant(p-1)/2}\frac{1-\cos 2\pi\frac{aN}{p}}{a} + O(\sqrt{p}) \leqslant$$

$$\leqslant \frac{\sqrt{p}}{\pi}\ln p(1+o(1)).$$

Таким образом,

$$S = \max_{N\geqslant 1} \leqslant (\frac{1}{\pi}+o(1))\sqrt{p}\ln p.$$

Э.Ландау улучшил эти оценки в два раза. Приведем их вывод. Положим $p_1 = \sqrt{p}\ln p$. Разобьем промежуток суммирования на два: $0 < |a| \leqslant p_1$ и $p_1 < |a| \leqslant (p-1)/2$.

Представим модуль суммы $T(N)$ в следующем виде

$$|T(N)| = \frac{\sqrt{p}}{2\pi}|T_1(N)+T_2(N)| + O(\sqrt{p}),$$

где

$$T_1(N) = \sum_{0<|a|\leqslant p_1}\left(\frac{a}{p}\right)\frac{e^{2\pi i\frac{aN}{p}}-1}{a},$$

$$T_2(N) = \sum_{p_1<|a|\leqslant(p-1)/2}\left(\frac{a}{p}\right)\frac{e^{2\pi i\frac{aN}{p}}-1}{a}.$$

Рассуждения, аналогичные приведенным выше, дают для суммы $T_1(N)$ следующие выражения

$$T_1(N) = 2i \sum_{0<|a|\leqslant p_1} \left(\frac{a}{p}\right) \frac{\sin 2\pi \frac{aN}{p}}{a},$$

если $\left(\frac{-1}{p}\right) = 1$;

$$T_1(N) = -2 \sum_{0<|a|\leqslant p_1} \left(\frac{a}{p}\right) \frac{1-\cos 2\pi \frac{aN}{p}}{a},$$

если $\left(\frac{-1}{p}\right) = -1$.

Пользуясь неравенствами (*),(**), получим

$$|T_1(N)| \leqslant \begin{cases} \frac{4}{\pi}\ln p_1 + O(1) = \frac{2}{\pi}\ln p(1+o(1)), & \text{если} \quad \left(\frac{-1}{p}\right) = 1, \\ 2\ln p_1 + O(1) = \ln p(1+o(1)), & \text{если} \quad \left(\frac{-1}{p}\right) = -1, \end{cases}$$

Теперь оценим модуль суммы $T_2(N)$. Заметим, что при $1 \leqslant x \leqslant p$ и любом целом a неполная сумма Гаусса имеет оценку

$$\left| \sum_{n\leqslant x} \left(\frac{n}{p}\right) e^{2\pi i \frac{an}{p}} \right| \ll \sqrt{p}\ln p.$$

Используя формулу Абеля суммирования по целым числам промежутка, положив $f(x) = 1/x, C(x) = \sum_{n\leqslant x} c_n, c_n = \left(\frac{a}{p}\right)(e^{2\pi i \frac{aN}{p}} - 1)$, преобразуем сумму

$$T_2(N) = \sum_{p_1<|a|\leqslant(p-1)/2} \left(\frac{a}{p}\right) \frac{e^{2\pi i \frac{aN}{p}} - 1}{a} =$$

$$= f(\frac{p-1}{2})C(\frac{p-1}{2}) - \int\limits_{p_1}^{\frac{p-1}{2}} C(x)f'(x)\,dx.$$

Получим $T_2(N) \ll 1$. Таким образом, $|T(N)| \leqslant (c+o(1))\sqrt{p}\ln p$, где

$$c = \begin{cases} 1/\pi^2, & \text{если} \quad \left(\frac{-1}{p}\right) = 1 \\ 1/(2\pi), & \text{если} \quad \left(\frac{-1}{p}\right) = -1. \end{cases}$$

Тем самым, искомое неравенство доказано. ◄

38. Пусть $k \geqslant 1$ — натуральное число, $p_1, \ldots, p_k$ — различные простые числа, $Q = p_1 \ldots p_k, a_1, \ldots, a_k$ — целые числа, $Q \geqslant x \geqslant 1$ — вещественное число и

$$S(x) = \sum_{m \leqslant x} \left(\frac{m + a_1}{p_1}\right) \ldots \left(\frac{m + a_k}{p_k}\right).$$

Тогда при $Q \to \infty$ имеем неравенство

$$|S(x)| \leqslant 2\pi^2 \sqrt{Q} \ln Q(1 + o(1)).$$

► Имеем

$$S(x) = \sum_{m \leqslant Q} \left(\frac{m + a_1}{p_1}\right) \ldots \left(\frac{m + a_k}{p_k}\right) \sum_{n \leqslant x} \frac{1}{Q} \sum_{a=0}^{Q-1} e^{2\pi i a \frac{m-n}{Q}} =$$

$$= \frac{1}{Q} \sum_{a=0}^{Q-1} A(a)B(a),$$

где

$$A(a) = \sum_{m=1}^{Q} \left(\frac{m + a_1}{p_1}\right) \ldots \left(\frac{m + a_k}{p_k}\right) e^{2\pi i a \frac{m}{Q}}, \quad B(a) = \sum_{n \leqslant x} e^{-2\pi i a \frac{n}{Q}}.$$

Преобразуем сумму $A(a)$. Для каждого $s = 1, \ldots, k$, положим $Q = p_s Q_s$. Тогда по китайской теореме об остатках для любого вычета m по модулю Q найдется единственный набор вычетов $(m_1, \ldots, m_k), 0 \leqslant m_1 < p_1, \ldots, 0 \leqslant m_k < p_k$, такой, что

$$m \equiv m_1 Q_1 + \cdots + m_k Q_k \pmod{Q}.$$

Отсюда имеем

$$A(a) = \prod_{s=1}^{k} A_s, \quad A_s = \sum_{m_s=0}^{p_s-1} \left(\frac{m_s Q_s + a_s}{p_s}\right) e^{-2\pi i a \frac{m_s}{p_s}}.$$

Определим Q'_s из сравнения $Q_s Q'_s \equiv 1 \pmod{p_s}$ и обозначим символом $\tau(p)$ сумму Гаусса

$$\tau(p) = \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) e^{2\pi i \frac{m}{p}}.$$

Тогда сумму A_s можно представить в виде

$$A_s = e^{2\pi i a \frac{a_s Q'_s}{p_s}} \left(\frac{-aQ'_s}{p_s}\right) \tau_{p_s}.$$

Следовательно,

$$A(a) = \chi(a)\tau, \chi(a) = \prod_{s=1}^{k} e^{2\pi i a \frac{a_s Q'_s}{p_s}} \left(\frac{-aQ'_s}{p_s}\right), \tau = \prod_{s=1}^{k} \tau_{p_s}, |\tau| = \sqrt{Q}.$$

Таким образом, сумма $S(x)$ примет вид

$$S(x) = \frac{\tau}{Q} \sum_{0<|a|<Q/2} \chi(a)B(a) = \frac{\tau}{Q} \sum_{0<|a|<Q/2} \chi(a) \frac{e^{2\pi i a \frac{x}{Q}} - 1}{1 - e^{2\pi i \frac{a}{Q}}}.$$

Пользуясь асимптотическим разложением при $0 < |a| < Q/2$ и $Q \to \infty$ для дроби вида

$$\frac{1}{1 - e^{2\pi i \frac{a}{Q}}} = -\frac{Q}{2\pi i a} + O(1),$$

получим

$$|S(x)| \leqslant \frac{\sqrt{Q}}{2\pi} \left| \sum_{0<|a|<Q/2} \chi(a) \frac{e^{-2\pi i a \frac{x}{Q}} - 1}{a} \right| + O(\sqrt{Q}).$$

Отсюда имеем

$$|S(x)| \leqslant \frac{\sqrt{Q}}{\pi} \sum_{0<a<Q/2} \frac{|\sin \pi a \frac{x}{Q}|}{a} + O(\sqrt{Q}).$$

Воспользовавшись неравенством (*) из предыдущей задачи, находим

$$|S(x)| \leqslant \frac{2}{\pi^2} \sqrt{Q} \ln Q(1 + o(1)).$$

Таким образом искомая оценка доказана. ◄

§ 2. Извлечение квадратного корня из вычета по простому модулю

1. Пусть $p \equiv 3 \pmod 4$. Тогда все решения сравнения (1) можно представить в виде

$$x \equiv \pm a^{(p+1)/4} \pmod p.$$

► По критерию Эйлера разрешимость сравнения $x^2 \equiv a \pmod p, (a,p) = 1$, эквивалентна выполнению сравнения $a^{(p-1)/2} \equiv 1 \pmod p$. Отсюда получим

$$a^{2(p+1)/4} \equiv a^{(p+1)/2} \equiv a \pmod p.$$

Следовательно, искомое решение сравнения имеет вид $x \equiv \pm a^{(p+1)/4} \pmod p$. ◄

2. Пусть $p \equiv 5 \pmod 8$. Тогда все решения сравнения (1) можно представить в виде

$$x \equiv \pm a^{(p+3)/8} 2^{(p-1)s/4} \pmod p,$$

где

$$s = \begin{cases} 0, & \text{при } a^{(p-1)/4} \equiv 1 \pmod p, \\ 1, & \text{при } a^{(p-1)/4} \equiv -1 \pmod p. \end{cases}$$

► По критерию Эйлера имеем $a^{(p-1)/2} \equiv 1 \pmod p$. Отсюда получим $a^{(p-1)/4} \equiv \pm 1 \pmod p$. Если $a^{(p-1)/4} \equiv 1 \pmod p$, то

$$a^{2(p+3)/8} \equiv a^{(p+3)/4} \equiv a \pmod p.$$

Тогда в этом случае искомое решение имеет вид $x \equiv \pm a^{(p+3)/8} \pmod p$.

Пусть теперь $a^{(p-1)/4} \equiv -1 \pmod p$. Поскольку 2 — квадратичный невычет по модулю p, по критерию Эйлера имеем $2^{(p-1)/2} \equiv -1 \pmod p$. Следовательно,

$$\left(2^{(p-1)/4} a^{(p+3)/8}\right)^2 \equiv 2^{(p-1)/2} a^{(p+3)/4} \equiv a \pmod p.$$

Таким образом, в этом случае искомое решение представляется в виде

$$x \equiv \pm 2^{(p-1)/4} a^{(p+3)/8} \pmod p. \blacktriangleleft$$

3. Пусть $p \equiv 1 \pmod 8$, N — квадратичный невычет по модулю p и $p = 2^k h + 1, k \geqslant 3, (h, 2) = 1$ Тогда все решения сравнения (1) можно представить в виде

$$x \equiv \pm a^{(h+1)/2} N^{(hu_{k-1})/2} \pmod p,$$

где $u_0 = 0; u_r = 2^{k-1} s_r + \frac{u_{r-1}}{2}, 1 \leqslant r \leqslant k-1;$

$$s_r = \begin{cases} 0, & \text{при } a^{2^{k-r-1}h} N^{(hu_{r-1})/2} \equiv 1 \pmod p, \\ 1, & \text{при } a^{2^{k-r-1}h} N^{(hu_{r-1})/2} \equiv -1 \pmod p. \end{cases}$$

► По критерию Эйлера имеем

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

Таким образом $a^{2^{k-1}h} \equiv 1 \pmod p$. Извлекаем из $a^{2^{k-1}h}$ квадратные корни до тех пор, пока не получим сравнение $a^{2^{k_1}h} \equiv -1 \pmod p, 0 \leqslant k_1 < k$ или сравнение $a^h \equiv 1 \pmod p$. В первом случае перейдем к сравнению $N^{2^{k_0}h} a^{2^{k_1}h} \equiv 1 \pmod p, k_0 = k-1$ и повторим процедуру извлечения квадратных корней из выражения $N^{2^{k_0}h} a^{2^{k_1}h}$ до тех пор, пока не приходим либо к сравнению $N^{2^{k_0-k_1+k_2}h} a^{2^{k_2}h} \equiv -1 \pmod p$, либо к сравнению $N^{2^{k_0-k_1}h} a^h \equiv 1 \pmod p$ и т.д. Наконец, при некотором s имеем либо

$$N^{2^{sk_0-k_s}h} a^h \equiv 1 \pmod p,$$

либо

$$N^{2^{(s+1)k_0-k_s}h} a^h \equiv 1 \pmod p,$$

Таким образом, при некотором $m > 0$ получим

$$\left(N^{2^{m-1}h} a^{(h+1)/2}\right)^2 \equiv N^{2^m h} a^{h+1} \equiv a \pmod p.$$

Отсюда находим искомое решение сравнения $x^2 \equiv a \pmod p$. Имеем

$$x \equiv \pm N^{2^{m-1}h} a^{(h+1)/2} \pmod p. \blacktriangleleft$$

§ 3. Символ Якоби

Пусть P — нечетное число, $P > 1$, и $P = p_1 p_2 \dots p_r$ — разложение его на простые сомножители (среди них могут быть и равные). Пусть, далее, $(a, P) = 1$. Тогда *символ Якоби* $\left(\frac{a}{P}\right)$ определяется следующим равенством

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_r}\right).$$

1. Пусть P — нечетное число, $P > 1, (a, P) = 1$, и $a \equiv a_1 \pmod{P}$. Тогда имеем

$$\left(\frac{a}{P}\right) = \left(\frac{a_1}{P}\right).$$

► Поскольку для символа Лежандра для нечетного простого числа p и при $(a, p) = 1, a \equiv a_1 \pmod{p}$ справедливо справедливо равенство

$$\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right),$$

по определению символа Якоби имеет место искомое равенство. ◄

2. Пусть P_1, P_2 — нечетные числа. Тогда имеем

$$P_1 P_2 - 1 \equiv (P_1 - 1) + (P_2 - 1) \pmod{4},$$

$$P_1^2 P_2^2 - 1 \equiv (P_1^2 - 1) + (P_2^2 - 1) \pmod{64}.$$

► Поскольку

$$P_1 P_2 - P_1 - P_2 + 1 \equiv (P_1 - 1)(P_2 - 1) \equiv 0 \pmod{4},$$

$$P_1^2 P_2^2 - P_1^2 - P_2^2 + 1 \equiv (P_1^2 - 1)(P_2^2 - 1) \equiv 0 \pmod{64},$$

искомые сравнения имеют место. ◄

3. При нечетном $P > 1$ справедливы следующие соотношения:
1) $\left(\frac{1}{P}\right) = 1$;
2)при $(a, P) = (b, P) = 1$ имеем $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$,
3) $\left(\frac{ab^2}{P}\right) = \left(\frac{a}{P}\right)$;
4)при $(a, P) = (a, Q) = 1, (P, 2) = (Q, 2) = 1$, имеем $\left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right)\left(\frac{a}{Q}\right)$;
5) $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$;

6) $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$;
7)при $(P,2) = (Q,2) = 1, (P,Q) = 1$, имеем $\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right)$.

► Равенства 1) – 4)прямо следуют из определения символа Якоби.

Равенства 5) и 6) докажем методом математической индукции по параметру P. При $P = 3$ они имеют место. Предположим они справедливы при $P < Q$, где Q — нечетное число. Докажем, что они верны при $P = Q$. Если Q — простое число, то искомые равенства следуют из квадратичного закона взаимности для символа Лежандра. Если же Q — составное число, то его можно представить в виде $Q = Q_1Q_2, 1 < Q_1, Q_2 < Q$. Далее, имеем цепочку равенств

$$\left(\frac{-1}{Q}\right) = \left(\frac{-1}{Q_1}\right)\left(\frac{-1}{Q_2}\right) = (-1)^{\frac{Q_1-1}{2}+\frac{Q_2-1}{2}} = (-1)^{\frac{Q_1Q_2-1}{2}} = (-1)^{\frac{Q-1}{2}}.$$

Утверждение 7) докажем по индукции по двум параметрам P и Q. Оно верно при $P = 3$ и любом нечетном $Q > 3$, а также при $Q = 3$ и любом нечетном $P > 3$. Докажем утверждение при $P = 3$. Если Q — простое число, то оно справедливо по квадратичному закону взаимности для символа Лежандра. Пусть Q — составное число. Тогда его можно представить в виде $Q = Q_1Q_2, 1 < Q_1, Q_2 < Q$. По предположению индукции и утверждениям 2),4) имеем

$$\left(\frac{Q}{3}\right) = \left(\frac{Q_1}{3}\right)\left(\frac{Q_2}{3}\right) = (-1)^{\frac{Q_1-1}{2}}\left(\frac{3}{Q_1}\right)(-1)^{\frac{Q_2-1}{2}}\left(\frac{3}{Q_2}\right) = \\ = (-1)^{\frac{Q-1}{2}}\left(\frac{3}{Q}\right).$$

Предположим, что при всех неравных между собой нечетных P, Q, с условиями либо $P < P_0, Q \leqslant Q_0$, либо $P \leqslant P_0, Q < Q_0$, где P_0, Q_0 — нечетные числа, справедливо равенство

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

Докажем это утверждение при $P = P_0$ и $Q = Q_0$. Если P_0, Q_0 — простые числа, то утверждение следует из квадратичного закона взаимности для символа Лежандра. Пусть, теперь, хотя бы одно из

чисел P_0, Q_0 является составным. Для определенности, пусть P_0 — составное число. Тогда $P_0 = P_1P_2, 1 < P_1, P_2 < P_0$. По свойству 4) мультипликативности символа Якоби и по предположению индукции имеем

$$\left(\frac{Q}{P}\right) = \left(\frac{Q}{P_1}\right)\left(\frac{Q}{P_2}\right) = (-1)^{\frac{P_1-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P_1}{Q}\right)(-1)^{\frac{P_2-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P_2}{Q}\right) =$$
$$= (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right). \blacktriangleleft$$

4. Пусть P и Q — нечетные взаимно простые числа. Тогда имеем

$$\left(\frac{P}{|Q|}\right)\left(\frac{Q}{|P|}\right) = \begin{cases} -(-1)^{\frac{P-1}{2}\frac{Q-1}{2}}, & \text{если } P<0, Q<0; \\ (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}, & \text{в противном случае.} \end{cases}$$

► При $P > 0, Q > 0$ искомая формула получена в предыдущей задаче.

Пусть $P < 0, Q < 0$. Тогда имеем

$$\left(\frac{P}{|Q|}\right)\left(\frac{Q}{|P|}\right) = \left(\frac{-|P|}{|Q|}\right)\left(\frac{-|Q|}{|P|}\right) = \left(\frac{|P|}{|Q|}\right)\left(\frac{|Q|}{|P|}\right)\left(\frac{-1}{|Q|}\right)\left(\frac{-1}{|P|}\right) =$$
$$= (-1)^{\frac{|P|-1}{2}\frac{|Q|-1}{2}+\frac{|P|-1}{2}+\frac{|Q|-1}{2}} = -(-1)^{\left(\frac{|P|-1}{2}+1\right)\left(\frac{|Q|-1}{2}+1\right)} =$$
$$-(-1)^{\frac{|P|+1}{2}\frac{|Q|+1}{2}} = -(-1)^{\frac{-P+1}{2}\frac{-Q+1}{2}} = -(-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.$$

Пусть, теперь, числа P и Q имеют разные знаки. Для определенности положим $P > 0, Q < 0$. Тогда, используя предыдущую задачу, находим

$$\left(\frac{P}{|Q|}\right)\left(\frac{Q}{|P|}\right) = \left(\frac{P}{|Q|}\right)\left(\frac{-|Q|}{P}\right) = \left(\frac{P}{|Q|}\right)\left(\frac{|Q|}{P}\right)\left(\frac{-1}{P}\right) =$$
$$= (-1)^{\frac{P-1}{2}\frac{|Q|-1}{2}+\frac{P-1}{2}} = (-1)^{\frac{P-1}{2}\frac{|Q|+1}{2}} =$$
$$= (-1)^{\frac{P-1}{2}\frac{-Q+1}{2}} = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}. \blacktriangleleft$$

5. При $n > 1$ имеем $\left(\frac{n}{4n-1}\right) = 1, \left(\frac{-n}{4n-1}\right) = -1$.

► Имеем

$$\left(\frac{n}{4n-1}\right) = \left(\frac{4n}{4n-1}\right) = \left(\frac{1}{4n-1}\right) = 1,$$
$$\left(\frac{-n}{4n-1}\right) = \left(\frac{-4n}{4n-1}\right) = \left(\frac{-1}{4n-1}\right)\left(\frac{4n}{4n-1}\right) = -1. \blacktriangleleft$$

§ 4. Извлечение квадратного корня из вычета по составному модулю

1. Пусть $\alpha > 0$ — натуральное число, $(a, p) = 1$. Тогда $T = T(p^\alpha)$ — число решений сравнения

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

равно следующему значению

$$T(2^\alpha) = \begin{cases} 1, & \text{если } \alpha = 1, \\ 0, & \text{если } \alpha = 2, a \equiv 3 \pmod 4, \\ 2, & \text{если } \alpha = 2, a \equiv 1 \pmod 4, \\ 0, & \text{если } \alpha > 2, a \not\equiv 1 \pmod 8, \\ 4, & \text{если } \alpha > 2, a \equiv 1 \pmod 8; \end{cases}$$

$$T(p^\alpha) = 1 + \left(\frac{a}{p}\right), \text{ если } p > 2.$$

▶ Пусть $p = 2$. Тогда при $\alpha = 1$ сравнение (2) принимает вид $x^2 \equiv 1 \pmod 2$ и $T(2) = 1$. Если $\alpha = 2, a \equiv 3 \pmod 4$, то сравнение (2) имеет вид $x^2 \equiv 3 \pmod 4$ и оно не имеет решений. Если же $\alpha = 2, a \equiv 1 \pmod 4$, то (2) имеет 2 решения $x \equiv \pm 1 \pmod 4$. Если нечетное a не сравнимо с единицей по модулю 8, то сравнение (2) по модулю 8 не имеет решений, следовательно и по модулю $2^\alpha, \alpha \geqslant 3$, оно не имеет решений.

Пусть, теперь, $\alpha > 2, a \equiv 1 \pmod 8$. Для каждого нечетного числа $x, 0 < x < 2^\alpha$, найдется число $b, 0 < b < 2^\alpha, b \equiv 1 \pmod 8$, такое, что

$$x^2 \equiv b \pmod{2^\alpha}.$$

Пусть нечетное x_0 решение предыдущего сравнения. Найдем количество всех его решений. Для любого другого решения x имеем

$$x^2 \equiv x_0^2 \pmod 2^\alpha,$$

т.е. $2^\alpha \mid (x - x_0)(x + x_0)$. Отсюда получим

$$2^{\alpha-2} \mid \frac{x - x_0}{2} \cdot \frac{x + x_0}{2},$$

поскольку числа x и x_0 — нечетные. Число не может одновременно делить числа $\frac{x-x_0}{2}$ и $\frac{x+x_0}{2}$. Следовательно, выполняется сравнение

$$x \equiv \pm x_0 \pmod{2^{\alpha-1}}.$$

Среди чисел $0 < x < 2^\alpha$ этому сравнению удовлетворяют точно четыре различных числа, т.е. если $T(b) \neq 0$, то $T(b) = 4$.

Таким образом, имеем

$$\sum_{\substack{b=1 \\ b\equiv 1 \pmod 8}}^{2^\alpha} T(b) = 2^{\alpha-1}.$$

Значит, количество различных чисел b, для которых $T(b) \neq 0$, равно $2^{\alpha-3}$. Это в точности те числа, которые удовлетворяют условиям $b, 0 < b < 2^\alpha, b \equiv 1 \pmod 8$. Последнее и доказывает, что $T(2^\alpha) = 4$ при $\alpha > 2, a \equiv 1 \pmod 8$.

Пусть $p \geqslant 3$. Возможны две ситуации:

$$a) \left(\frac{a}{p}\right) = -1 \text{и} b) \left(\frac{a}{p}\right) = 1.$$

В случае a) сравнение $x^2 \equiv a \pmod p$ не имеет решений. Следовательно

$$T(p^\alpha) = 0 = 1 + \left(\frac{a}{p}\right).$$

Рассмотрим случай b). Сравнение $x^2 \equiv a \pmod p$ имеет два решения $x \equiv \pm x_0 \pmod p$. Предположим, что x_α решение сравнения $x_\alpha^2 \equiv a \pmod{p^\alpha}$. Найдем $x_{\alpha+1} \equiv x_\alpha \pmod{p^\alpha}$ и $x_{\alpha+1}^2 \equiv a \pmod{p^{\alpha+1}}$. Положим $x_{\alpha+1} = x_\alpha + p^\alpha y, 0 \leqslant y < p$. Имеем

$$(x_\alpha + p^\alpha y)^2 \equiv a \pmod{p^{\alpha+1}}.$$

Следовательно, при $\alpha > 0$ получим

$$2x_\alpha y \equiv a_1 \pmod p, a_1 = p^{-\alpha}(a - x_\alpha^2).$$

Поскольку $(2x_\alpha, p) = 1$, последнее сравнение имеет единственное решение.

Таким образом, сравнение $x^2 \equiv a \pmod{p^\alpha}$ имеет два решения, и поэтому всегда справедливо равенство

$$T(p^\alpha) = 1 + \left(\frac{a}{p}\right). \blacktriangleleft$$

2. Пусть a, m — натуральное число, $(a, m) = 1$. Тогда $T = T(m)$ — число решений сравнения

$$x^2 \equiv a \pmod m \tag{3}$$

равно

$$T(m)=\begin{cases}0, & \text{если } 4\|m, a\not\equiv 1 \pmod 4,\\ 0, & \text{если } 8\mid m, a\not\equiv 1 \pmod 8,\\ 0, & \text{если } \exists p\mid m, p>2, \left(\frac{a}{p}\right)=-1.\end{cases}$$

Пусть, далее, каноническое разложение на простые сомножители числа m имеет вид $m=2^{\alpha}p_1^{\alpha_1}\dots p_k^{\alpha_k}, (a,m)=1$ и k обозначает количество нечетных простых делителей числа m. Пусть, наконец, выполнены следующие необходимые условия разрешимости сравнения $x^2\equiv a \pmod m$:

$$a\equiv 1 \pmod 4 \text{при} \alpha=2, a\equiv 1 \pmod 8 \text{при} \alpha\geqslant 3,$$

$$\left(\frac{a}{p_1}\right)=1, \left(\frac{a}{p_2}\right)=1,\dots,\left(\frac{a}{p_k}\right)=1.$$

Тогда количество решений $T(m)$ этого сравнения равно

$$T(m)=\begin{cases}2^k, & \text{если } 4\not| m,\\ 2^{k+1}, & \text{если } 4\|m,\\ 2^{k+2}, & \text{если } 8\mid m.\end{cases}$$

► Функция $T(m)$ — мультипликативная, т.е. $T(m)=T(2^{\alpha})T(p_1^{\alpha_1})\dots T(p_k^{\alpha_k})$. Отсюда, используя утверждение предыдущей задачи, получим искомое утверждение. ◄

3. Пусть $V(n)$ — число решений сравнения $\omega^2\equiv -1 \pmod n$ и каноническое разложение на простые сомножители числа n имеет вид $n==2^{\alpha}p_1^{\alpha_1}\dots p_k^{\alpha_k}$. Тогда $V(n)$ равно

$$V(n)=\begin{cases}0, & \text{если либо} 4\mid n, \text{либо} \exists p\mid n, p\equiv 3 \pmod 4,\\ 2^k, & \text{если} 4\not| n, \forall p\mid n, p\equiv 1 \pmod 4.\end{cases}$$

► Поскольку

$$\left(\frac{-1}{p}\right)=\begin{cases}1, & \text{если} p\equiv 1 \pmod 4,\\ -1, & \text{если} p\equiv -1 \pmod 4,\end{cases}$$

искомое утверждение следует из утверждения предыдущей задачи. ◄

4. Пусть n — натуральное число, $n > 1$, и пусть ω — решение сравнения $\omega^2 \equiv -1 \pmod{n}$. Тогда существует единственное представление числа n в виде $n = x^2 + y^2$, где x, y — взаимно простые числа и $y \equiv \omega x \pmod{n}$.

► Дробь $\frac{\omega}{n}$ — несократимая, так как вычет ω является решением сравнения $\omega^2 \equiv -1 \pmod{n}$. По лемме Дирихле при $\tau = \sqrt{n}$ и $\alpha = \frac{\omega}{n}$ существует несократимая дробь a/b со знаменателем b, не превосходящем $\sqrt{n}$, такая, что

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b\tau}.$$

Положим $\omega b - na = c$. Имеем $\omega b \equiv c \pmod{n}$. Из леммы Дирихле получим $0 < |c| < \sqrt{n}, 0 < b \leqslant \sqrt{n}$. Следовательно,

$$0 < b^2 + c^2 < 2n.$$

Кроме того, справедливы сравнения

$$b^2 + c^2 \equiv b^2 + \omega^2 b^2 \equiv (1 + \omega^2)b^2 \equiv 0 \pmod{n}.$$

Таким образом имеем равенство $b^2 + c^2 = n$.

Докажем, что числа b и c взаимно просты. Имеем цепочку равенств

$$n = b^2 + (\omega b - na)^2 = (1 + \omega^2)b^2 - 2\omega nba + n^2a^2,$$

$$1 = \frac{1 + \omega^2}{n}b^2 - \omega ba - \omega ba + na^2 = db - ac.$$

Равенство $db - ac = 1$ и доказывает, что $(b, c) = 1$. Если $c > 0$, то искомое решение имеет вид $x = b, y = c$. Если же $c < 0$, то следует положить $x = -c, y = b$. Действительно,

$$n = (-c)^2 + b^2, -c > 0, b > 0, (-c, b) = 1,$$

$$b \equiv -\omega^2 b \equiv -\omega c \equiv \omega(-c) \pmod{n}.$$

Докажем единственность решения (x, y). Предположим, что (x_1, y_1) — другое решение, удовлетворяющее условию задачи. Имеем цепочку соотношений

$$n^2 = (x^2 + y^2)(x_1^2 + y_1^2) = (xx_1 + yy_1)^2 + (xy_1 - yx_1)^2,$$

$$xx_1 + yy_1 \equiv xx_1 + \omega x\omega x_1 \equiv (1+\omega^2)xx_1 \equiv 0 \pmod{n},$$

$$xx_1 + yy_1 > 0, xx_1 + yy_1 = n, xy_1 - yx_1 = 0,$$

$$xn = x(xx_1 + yy_1) - y(xy_1 - yx_1) = x_1(x^2 + y^2) = x_1 n.$$

Следовательно, $x = x_1, y = y_1$. ◄

5. Пусть $m > 1$. Тогда число представлений числа m в виде

$$m = x^2 + y^2, (x, y) = 1,$$

где x, y — целые числа, равно учетверенному числу решений сравнения

$$z^2 + 1 \equiv 0 \pmod{m}.$$

► Так как $(x, y) = 1$, то $x \neq 0, y \neq 0, x \neq y$. Далее, вместе с решением (x, y) уравнения $x^2 + y^2 = m$ решениями его являются $\pm x, \pm y$. Следовательно, решению $(x, y), x > 0, y > 0$, отвечают четыре решения.

По предыдущей задаче для каждого ω, удовлетворяющего сравнению $\omega^2 \equiv -1 \pmod{m}$, существует единственное решение уравнения $x^2 + y^2 = m$, для которого $(x, y) = 1, x > 0, y > 0, y \equiv \omega x \pmod{m}$.

Пусть, теперь, (x, y) решение уравнения $x^2 + y^2 = m, (x, y) = 1, x > 0, y > 0$. Тогда имеем $(x, m) = 1$ и существует единственное ω, удовлетворяющее сравнению $y \equiv \omega x \pmod{m}$. Кроме того, имеет место цепочка сравнений

$$0 \equiv m \equiv x^2 + y^2 \equiv x^2 + \omega^2 x^2 \equiv (1+\omega^2)x^2 \pmod{m},$$

$$1 + \omega^2 \equiv 0 \pmod{m}.$$

Таким образом, каждому решению уравнения поставлено во взаимно однозначное соответствие решение сравнения $1 + \omega^2 \equiv 0 \pmod{m}$. ◄

6. Пусть $m \geqslant 1$ и $U(m)$ — число представлений числа m в виде

$$m = x^2 + y^2,$$

где x, y — целые числа. Тогда $U(n)$ равно

$$U(m) = 4 \sum_{d^2 | m} V(m/d^2),$$

где $V(n)$ — число решений сравнения

$$z^2 + 1 \equiv 0 \pmod{n}.$$

► Все решения уравнения $x^2 + y^2 = m$, имеющие d наибольшим общим делителем чисел x и y соберем вместе. Получим

$$m/d^2 = x_1^2 + y_1^2, x_1 = x/d^2, y_1 = y/d^2, (x_1, y_1) = 1.$$

Следовательно, используя утверждение предыдущей задачи, получим искомую формулу. ◄

7. Функции $V(n), U(n)/4, W(n) = \sum\limits_{d|n} \chi_4(d)$, где $\chi_4(m)$ — неглавный характер Дирихле по модулю 4,

$$\chi_4(m) = \begin{cases} 0, & \text{если} m \equiv 0 \pmod 4, \\ 1, & \text{если} m \equiv 1 \pmod 4, \\ -1, & \text{если} m \equiv 3 \pmod 4, \end{cases}$$

являются мультипликативными.

► Мультипликативность функции $V(m)$ следует из китайской теоремы об остатках. Далее, пусть $m = m_1 m_2, (m_1, m_2) = 1$. Тогда

$$U(m_1 m_2)/4 = \sum_{d^2 | m_1 m_2} V(m_1 m_2/d^2) =$$

$$= \sum_{d_1^2 | m_1} V(m_1/d^2) \sum_{d_2^2 | m_2} V(m_2/d^2) = U(m_1)/4 \cdot U(m_2)/4,$$

где $d_1 \mid m_1, d_2 \mid m_2, d = d_1 d_2$. Таким образом, функция $U(m)/4$ является мультипликативной.

Наконец, при $(m_1, m_2) = 1$ имеем

$$W(m_1 m_2) = \sum_{d | m_1 m_2} \chi_4(d) = \sum_{d_1 | m_1} \chi_4(d_1) \sum_{d_2 | m_2} \chi_4(d_2) =$$

$$= W(m_1) W(m_2). \blacktriangleleft$$

8. Справедливо равенство

$$U(m) = 4 \sum_{d | m} \chi_4(d).$$

► В силу мультипликативности функций в правой и левой частях равенств достаточно проверить равенство при $m = p^\alpha$. Имеем

$$W(p^\alpha) = \sum_{0 \leqslant \beta \leqslant \alpha} \chi_4(p^\beta) = \begin{cases} 1, & \text{если} \quad p = 2, \\ \alpha + 1, & \text{если} \quad p \equiv 1 \pmod 4, \\ 1, & \text{если} \quad p \equiv 3 \pmod 4, 2 \mid \alpha, \\ 0, & \text{если} \quad p \equiv 3 \pmod 4, 2 \not| \alpha. \end{cases}$$

Далее, справедливы соотношения

$$V(p^m) = \begin{cases} 1, & \text{если} \quad p = 2, m = 1, \\ 0, & \text{если} \quad p = 2, m > 1, \\ 0, & \text{если} \quad p \equiv 3 \pmod 4, m \geqslant 1, \\ 2, & \text{если} \quad p \equiv 1 \pmod 4, m \geqslant 1. \end{cases}$$

Следовательно, при четном α получим

$$U(p^\alpha)/4 = V(p^\alpha) + V(p^{\alpha-2}) + \cdots + V(p^2) + V(1) =$$

$$= \begin{cases} 1, & \text{если} \quad p = 2, \\ 2 \cdot \alpha/2 + 1 = \alpha + 1, & \text{если} \quad p \equiv 1 \pmod 4, \\ 1, & \text{если} \quad p \equiv 3 \pmod 4, \end{cases}$$

и при нечетном α имеем

$$U(p^\alpha)/4 = V(p^\alpha) + V(p^{\alpha-2}) + \cdots + V(p) =$$

$$= \begin{cases} 1, & \text{если} \quad p = 2, \\ 2 \cdot (\alpha + 1)/2 = \alpha + 1, & \text{если} \quad p \equiv 1 \pmod 4, \\ 0, & \text{если} \quad p \equiv 3 \pmod 4. \end{cases}$$

Отсюда следует искомое равенство. ◄

§ 5. Целая часть квадратного корня из натурального числа

1. Пусть a — фиксированное положительное число, x_1 — любое положительное число и последовательность $\{x_n\}$ при $n \geqslant 1$ задана следующей итерационной формулой Герона

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{a}{x_n}\right).$$

Тогда имеем
1) при $n \geqslant 2$ последовательность x_n ограничена снизу числом $\sqrt{a}$;
2) последовательность x_n — невозрастающая;
3) $\lim\limits_{n\to\infty} x_n = \sqrt{a}$;
4) $\frac{x_{n+1}-\sqrt{a}}{x_{n+1}+\sqrt{a}} = \left(\frac{x_n-\sqrt{a}}{x_n+\sqrt{a}}\right)^2$;
5) $\Delta_n := x_n - \sqrt{a} = \frac{2q^{2^{n-1}}}{1-q^{2^{n-1}}}\sqrt{a} \to 0$ при $n \to \infty$, где $q = \frac{x_1-\sqrt{a}}{x_1+\sqrt{a}}$.

► 1). При $n \geqslant 2$ имеем

$$x_n - \sqrt{a} = \frac{1}{2}\left(x_{n-1} + \frac{a}{x_{n-1}}\right) - \sqrt{a} = \frac{(x_{n-1}-\sqrt{a})^2}{2x_{n-1}} \geqslant 0.$$

2). Используя утверждение 1), при $n \geqslant 1$ находим

$$x_n - x_{n+1} = x_n - \frac{1}{2}\left(x_n + \frac{a}{x_n}\right) = \frac{x_n^2 - a}{2x_n} \geqslant 0.$$

3). Из утверждений 1) и 2) имеем, что последовательность $x_n, n \geqslant 2$, ограничена снизу числом $\sqrt{a}$ и является невозрастающей. По теореме Вейерштраса она имеет предел, равный $x \geqslant \sqrt{a} > 0$. Следовательно, справедливо равенство

$$\lim_{n\to\infty} x_{n+1} = \frac{1}{2}\left(\lim_{n\to\infty} x_n + \frac{a}{\lim\limits_{n\to\infty} x_n}\right),$$

т.е. $x = (x + a/x)/2, x = \sqrt{a}$.

4). Справедливо равенство

$$x_{n+1} \pm \sqrt{a} = \frac{(x_n \pm \sqrt{a})^2}{2x_n}.$$

Следовательно,

$$\frac{x_{n+1}-\sqrt{a}}{x_{n+1}+\sqrt{a}} = \left(\frac{x_n-\sqrt{a}}{x_n+\sqrt{a}}\right)^2.$$

5). Полагая $\frac{x_1-\sqrt{a}}{x_1+\sqrt{a}} = q$, из предыдущего утверждения находим цепочку соотношений

$$\frac{x_n-\sqrt{a}}{x_n+\sqrt{a}} = q^{2^{n-1}}, \quad x_n = \frac{1+q^{2^{n-1}}}{1-q^{2^{n-1}}}.$$

Таким образом, поскольку $|q| < 1$, имеем

$$\Delta_n := x_n - \sqrt{a} = \frac{2q^{2^{n-1}}}{1 - q^{2^{n-1}}}\sqrt{a} \to 0$$

при $n \to \infty$. ◀

2. Пусть n — натуральное число, $s_1 = \left[\frac{n+1}{2}\right]$ и последовательность $\{s_k\}$ при $k \geqslant 1$ задана следующей итерационной формулой

$$s_{k+1} = \left[\frac{1}{2}\left(s_k + \frac{n}{s_k}\right)\right].$$

Тогда имеем:
1) если $y \geqslant x$, то $[y] \geqslant [x]$;
2) $[(n+1)/2] \geqslant [\sqrt{n}]$;
3) при $k \geqslant 2$ справедливо неравенство $s_k \geqslant [\sqrt{n}]$;
4) если справедливо неравенство $s_k > [\sqrt{n}]$, то $s_k > s_{k+1}$;
5) найдется натуральное m такое, что $s_m = [\sqrt{n}]$.

▶ 1). От противного. Предположим, что $[y] < [x]$. Тогда имеем цепочку неравенств

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

Последнее противоречит неравенству $y \geqslant x$, имеющему место по условию.

2). Справедливо неравенство $\frac{n+1}{2} \geqslant \sqrt{n}$. Следовательно, по утверждению 1) имеем $\left[\frac{n+1}{2}\right] \geqslant [\sqrt{n}]$.

3). Имеем неравенство $\frac{1}{2}\left(s_{k-1} + \frac{n}{s_{k-1}}\right) \geqslant \sqrt{n}$. Следовательно, по утверждению 1) находим

$$s_k = \left[\frac{1}{2}\left(s_{k-1} + \frac{n}{s_{k-1}}\right)\right] \geqslant [\sqrt{n}].$$

4). От противного. Предположим, что $s_k \leqslant s_{k+1}$. Тогда имеем цепочку равносильных неравенств

$$\left[\frac{1}{2}\left(s_k + \frac{n}{s_k}\right)\right] \geqslant s_k, \frac{1}{2}\left(s_k + \frac{n}{s_k}\right) - \left\{\frac{1}{2}\left(s_k + \frac{n}{s_k}\right)\right\} \geqslant s_k.$$

Следовательно,

$$\frac{1}{2}\left(\frac{n}{s_{k-1}} - s_k\right) \geqslant \left\{\frac{1}{2}\left(s_k + \frac{n}{s_k}\right)\right\} \geqslant 0.$$

С другой стороны, по условию задачи имеет место следующая цепочка неравенств

$$s_k > [\sqrt{n}], s_k \geqslant [\sqrt{n}] + 1 > \sqrt{n}, s_k > \sqrt{n}, s_k^2 > n, \frac{1}{2}\left(\frac{n}{s_k} - s_k\right) < 0.$$

Последнее неравенство противоречит полученному выше. Следовательно, сделанное выше предположение неверно.

5). По утверждениям 2) и 3) для любого натурального числа k выполняется неравенство $s_k \geqslant \sqrt{n}$. Далее, по утверждению 4), если бы всегда выполнялось строгое неравенство $s_k > \sqrt{n}$, то бесконечная последовательность натуральных чисел $\{s_k\}$ была бы монотонно убывающей. Следовательно, существует натуральное m такое, что $s_m = \sqrt{n}$. ◄

§ 6. Символ Кронекера

Пусть $d \equiv 0$ или $1 \pmod 4$, и пусть d отлично от точного квадрата, т.е. $d = 5, 8, 13, 17, 20, 21, \ldots$ или $-3, -4, -7, -8, \ldots$.

При $p \mid d$ положим $\left(\frac{d}{p}\right) = 0$.

При $p \not| d$ положим

$$\left(\frac{d}{p}\right) = \begin{cases} \left(\frac{2}{|d|}\right) \text{ символ Якоби}, & \text{если} p = 2, \\ \left(\frac{d}{p}\right) \text{ символ Лежандра}, & \text{если} p > 2. \end{cases}$$

Пусть, также, m — натуральное число, $m = p_1 p_2 \ldots p_r$ — его разложение на простые сомножители. Тогда *символ Кронекера* $\left(\frac{d}{m}\right)$ определяется следующим равенством

$$\left(\frac{d}{m}\right) = \left(\frac{d}{p_1}\right)\left(\frac{d}{p_2}\right)\ldots\left(\frac{d}{p_r}\right).$$

Положим, также, $\left(\frac{d}{1}\right) = 1$

1. Пусть $d \equiv 0$ или $1 \pmod 4$, и пусть d отлично от точного квадрата. Пусть, также, m — нечетное положительное число. Тогда значения символов Якоби и Кронекера $\left(\frac{d}{m}\right)$ совпадают.

► Утверждение задачи прямо следует из определений символов Якоби и Кронекера. ◄

2. Пусть $m_1 > 0$ и $m_2 > 0$. Тогда имеем $\left(\frac{d}{m_1 m_2}\right) = \left(\frac{d}{m_1}\right)\left(\frac{d}{m_2}\right)$.

► Утверждение прямое следствие определения символа Кронекера. ◄

3. Пусть m — натуральное число, $(d, m) = 1$. Тогда $R = R(4m)$ — число решений сравнения $x^2 \equiv d \pmod{4m}$ равно

$$R(4m) = 2 \sum_{r|d}{}' \left(\frac{d}{r}\right),$$

где штрих в знаке суммирования означает, что r пробегает бесквадратные значения.

► Рассмотрим сначала случай нечетного числа d, т.е. $d \equiv 1 \pmod 4$. Имеем $(d, 4m) = 1$. Пусть $4m = \prod\limits_{p|4m} p^{l_p}$ — каноническое разложение числа $4m$ на простые сомножители. Тогда число $R(4m)$ решений сравнения $x^2 \equiv d \pmod{4m}$ равно

$$R(4m) = \prod_{p|4m} R(p^{l_p}).$$

По утверждению IV. 1 имеем

$$R(2^l) = \begin{cases} 2, & \text{если} \quad l = 2, \\ 2\left(1 + \left(\frac{d}{2}\right)\right), & \text{если} \quad l \geqslant 3. \end{cases}$$

Кроме того, при $p \geqslant 3$ по тому же утверждению получим $R(p^l) = 1 + \left(\frac{d}{p}\right)$.

Таким образом, находим

$$R(4m) = 2 \prod_{p|m} \left(1 + \left(\frac{d}{p}\right)\right) = 2 \sum_{r|d}{}' \left(\frac{d}{r}\right).$$

Это и есть искомая формула.

Пусть, теперь, d будет четным числом. Тогда $d \equiv 0 \pmod 4$. Поскольку $(d, m) = 1$, число m будет нечетным. Сравнение $x^2 \equiv d \equiv 0 \pmod 4$ имеет два решения.

Далее, находим

$$R(4m) = 2 \prod_{p|m} R(p^{l_p})$$

и по утверждению IV.1 справедливо равенство $R(p^l) = 1 + \left(\frac{d}{p}\right)$. Отсюда следует искомое равенство. ◄

4. Пусть m — натуральное число, $(d,m)=1$. Тогда
1) для нечетного числа d имеем $\left(\frac{d}{m}\right)=\left(\frac{m}{|d|}\right)$ (символ Якоби);
2) для четного числа $d=2^b u, (u,2)=1$, имеем $\left(\frac{d}{m}\right)=\left(\frac{2}{m}\right)^b(-1)^{\frac{u-1}{2}\frac{m-1}{2}}\left(\frac{m}{|u|}\right)$ (оба символа в правой части равенства — символы Якоби).

► 1). Поскольку d — нечетное число, $d\equiv 1 \pmod 4$ и d не является квадратом. Представим число m в виде $m=2^a u$, где u — нечетное число. По утверждению задачи 2 и по определению символа Кронекера имеем

$$\left(\frac{d}{m}\right)=\left(\frac{d}{2^a u}\right)=\left(\frac{d}{2}\right)^a\left(\frac{d}{u}\right)=\left(\frac{2}{|d|}\right)^a\left(\frac{d}{u}\right).$$

Из утверждения III.4 имеем

$$\left(\frac{d}{m}\right)=\left(\frac{2}{|d|}\right)^a\left(\frac{u}{|d|}\right)=\left(\frac{2^a u}{|d|}\right)=\left(\frac{m}{|d|}\right).$$

2). Пусть, теперь, d четное число. Тогда $d=2^b u$, где u — нечетное число. По определению символа Кронекера имеем

$$\left(\frac{d}{m}\right)=\left(\frac{2^b u}{m}\right)=\left(\frac{2}{m}\right)^b\left(\frac{u}{m}\right).$$

Далее, из утверждения III.4 получим

$$\left(\frac{d}{m}\right)=\left(\frac{2}{m}\right)^b(-1)^{(u-1)(m-1)/4}\left(\frac{m}{|u|}\right). \blacktriangleleft$$

Теперь покажем, что символ Кронекера как функция от m при фиксированном d является групповым характером $\chi_d(m)=\left(\frac{d}{m}\right)$.

5. Символ Кронекера $\left(\frac{d}{m}\right)$ как функция от m обладает следующими свойствами:
1) $\left(\frac{d}{m}\right)=0$ при $(d,m)>1$,
2) $\left(\frac{d}{1}\right)=1$,
3) $\left(\frac{d}{m_1 m_2}\right)=\left(\frac{d}{m_1}\right)\left(\frac{d}{m_2}\right)$,
4) $\left(\frac{d}{m}\right)=\left(\frac{d}{m}\right)$ при $m_1\equiv m_2 \pmod{|d|}$,
5) найдется m такое, что $\left(\frac{d}{m}\right)=-1$.

► Утверждения 1) и 2) следуют прямо из определения символа Кронекера. Утверждение 3) совпадает с утверждением задачи 2.

4). Пусть $(|d|, m_1) > 1$. Тогда из условия $m_1 \equiv m_2 \pmod{|d|}$ следует, что $(|d|, m_2) > 1$. Поэтому имеем

$$\left(\frac{d}{m_1}\right) = 0 = \left(\frac{d}{m_2}\right).$$

Пусть $(|d|, m_1) = 1$. Тогда имеем $(|d|, m_2) = 1$. Рассмотрим сначала случай нечетного d. Используя утверждение предыдущей задачи и свойство символа Якоби, получим

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

Пусть, теперь, d — четное число, $d = 2^b u$. Из утверждения предыдущей задачи имеем

$$\left(\frac{d}{m_1}\right) = \left(\frac{2}{m_1}\right)^b (-1)^{(u-1)(m_1-1)/4} \left(\frac{m_1}{|u|}\right),$$

$$\left(\frac{d}{m_2}\right) = \left(\frac{2}{m_2}\right)^b (-1)^{(u-1)(m_2-1)/4} \left(\frac{m_2}{|u|}\right).$$

Поскольку $|u|$ делит $|d|$, имеем $m_1 \equiv m_2 \pmod{|u|}$. Следовательно, по свойству символа Якоби получим

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

Далее, так как 4 делит $|d|$, то $m_1 \equiv m_2 \pmod{4}$. Отсюда имеем

$$(-1)^{(u-1)(m_1-1)/4} = (-1)^{(u-1)(m_2-1)/4}.$$

Наконец, по закону взаимности для символа Якоби получим

$$\left(\frac{2}{m_1}\right) = (-1)^{\frac{m_1^2-1}{8}}, \left(\frac{2}{m_2}\right) = (-1)^{\frac{m_2^2-1}{8}},$$

и при $b > 2$ из условия 8 делит $|d|$ следует, что $m_1 \equiv m_2 \pmod{8}$. Отсюда при $b > 2$ находим

$$\left(\frac{2}{m_1}\right)^b = \left(\frac{2}{m_2}\right)^b.$$

При $b = 2$ это утверждение очевидно.

5). Рассмотрим сначала случай нечетного числа d, взаимно простого с числом m. В этом случае $d \equiv 1 \pmod 4$ и d не является квадратом. При $d < 0$ имеем $|d| \equiv 3 \pmod 4$. Следовательно, найдется простое число p такое, что $|d| = p^l u, (p, u) = 1, u, l$ — нечетные числа. Возьмем число s квадратичным невычетом по модулю p. По китайской теореме об остатках найдется вычет m по модулю $|d|$, удовлетворяющий условиям

$$m \equiv s \pmod p, m \equiv 1 \pmod u.$$

По утверждению предыдущей задачи имеем

$$\left(\frac{d}{m}\right) = \left(\frac{m}{|d|}\right) = \left(\frac{m}{p}\right)^l \left(\frac{m}{u}\right) = \left(\frac{s}{p}\right)^l \left(\frac{1}{u}\right) = (-1)^l = -1.$$

Пусть, теперь, d — четное число. Тогда $d = 2^b u, b \leqslant 2, u$ — нечетное число.

Пусть, сначала, b будет нечетным числом. Тогда выберем число $m > 0$ из условий

$$m \equiv 5 \pmod 8, m \equiv 1 \pmod{|u|},$$

что возможно, поскольку $(8, |u|) = 1$. Далее, имеем $(|d|, m) = 1$ и по утверждению предыдущей задачи получим

$$\left(\frac{d}{m}\right) = \left(\frac{2}{m}\right)^b (-1)^{(u-1)(m-1)/4} \left(\frac{m}{|u|}\right) = \left(\frac{2}{m}\right) \cdot 1 \cdot \left(\frac{1}{|u|}\right) = -1.$$

Рассмотрим оставшийся случай: $d = 2^b u$ и b — четные числа, u — нечетное число и не является точным квадратом. При $m > 0$ и $(|d|, m) = 1$ по утверждению предыдущей задачи получим

$$\left(\frac{d}{m}\right) = (-1)^{(u-1)(m-1)/4} \left(\frac{m}{|d|}\right).$$

Пусть, сначала, будет $u \equiv 3 \pmod 4$. Выберем $m > 0$, удовлетворяющее условиям

$$m \equiv -1 \pmod 4, m \equiv 1 \pmod{|u|}.$$

Тогда числа m и $|d|$ — взаимно просты. Следовательно, имеем

$$\left(\frac{d}{m}\right) = (-1)^{\frac{u-1}{2}} \left(\frac{1}{|d|}\right) = -1.$$

Пусть, теперь, $u \equiv 1 \pmod 4$. Тогда при $m > 0$ и $(|d|, m) = 1$ находим

$$\left(\frac{d}{m}\right) = \left(\frac{m}{|u|}\right).$$

Число $|u|$ не является точным квадратом (при положительном d это очевидно; если же $d < 0$, то $|u| = -u \equiv -1 \pmod 4$). Следовательно, найдется нечетное простое число p такое, что $|u| = p^l v, (p, v) = 1$, и числа v, l — нечетные. Выберем квадратичный невычет s по модулю p. Так как числа $2, p, v$ взаимно просты, то по китайской теореме об остатках существует $m > 0$ такое, что

$$m \equiv s \pmod p, m \equiv 1 \pmod v, m \equiv 1 \pmod 2.$$

Числа m и $|d|$ взаимно просты. Имеем

$$\left(\frac{d}{m}\right) = \left(\frac{d}{p^l v}\right) = \left(\frac{d}{p}\right)^l \left(\frac{m}{v}\right) = \left(\frac{s}{p}\right)\left(\frac{1}{v}\right) = -1. \blacktriangleleft$$

6. $\left(\frac{d}{|d|-1}\right) = \begin{cases} 1, & \text{если } d > 0, \\ -1, & \text{если } d < 0. \end{cases}$

► Пусть d — нечетное число. Тогда по утверждению задачи 4 имеем

$$\left(\frac{d}{|d|-1}\right) = \left(\frac{|d|-1}{|d|}\right) = \left(\frac{-1}{|d|}\right) = (-1)^{\frac{|d|-1}{2}} = \begin{cases} 1, & \text{если } d > 0, \\ -1, & \text{если } d < 0. \end{cases}$$

Пусть, теперь, d будет четным числом. Представим его в виде $d = 2^b u, b \geqslant 2, u$ — нечетное число. По утверждению задачи 4 находим

$$\left(\frac{d}{|d|-1}\right) = \left(\frac{2}{|d|-1}\right)^b (-1)^{\frac{u-1}{2}} \left(\frac{|d|-1}{|u|}\right).$$

При $b = 2$, очевидно, $\left(\frac{2}{|d|-1}\right)^b = 1$. При $b \geqslant 3$ имеем

$$\left(\frac{2}{|d|-1}\right) = (-1)^{\frac{(|d|-1)^2-1}{8}} = 1.$$

Далее, поскольку $|u|$ делит $|d|$, получим

$$(-1)^{\frac{u-1}{2}} \left(\frac{|d|-1}{|u|}\right) = (-1)^{\frac{u-1}{2}} \left(\frac{-1}{|u|}\right) =$$

$$= (-1)^{\frac{u-1}{2}+\frac{|u|-1}{2}} = \begin{cases} 1, & \text{если } d > 0, \\ -1, & \text{если } d < 0. \end{cases}$$

Тем самым, искомая формула доказана. ◄

7. Пусть n, m — натуральные числа, $n \equiv -m \pmod{|d|}$. Тогда имеем

$$\left(\frac{d}{n}\right) = \begin{cases} \left(\frac{d}{m}\right), & \text{если } d > 0, \\ -\left(\frac{d}{m}\right), & \text{если } d < 0. \end{cases}$$

► Имеем

$$\left(\frac{d}{n}\right) = \left(\frac{d}{|d|m - m}\right) = \left(\frac{d}{m(|d| - 1)}\right) = \left(\frac{d}{m}\right)\left(\frac{d}{|d| - 1}\right).$$

Отсюда искомая формула следует из утверждения предыдущей задачи. ◄

8. Пусть $m \geqslant 1$ — нечетное число, $(n, m) = 1$. Тогда символ Якоби $\left(\frac{n}{m}\right)$ можно представить через символ Кронекера следующими способами:

$$\left(\frac{n}{m}\right) = \begin{cases} 1, & \text{если } m = k^2, \\ \left(\frac{m}{n}\right), & \text{если } m \equiv 1 \pmod 4, m \neq k^2, \\ \left(\frac{-m}{n}\right), & \text{если } m \equiv 3 \pmod 4. \end{cases}$$

► Если m — полный квадрат, то определению символа Якоби имеем $\left(\frac{n}{m}\right) = 1$.

Пусть, теперь, $m \equiv 1 \pmod 4, m$ — не квадрат и $n = 2^b u, u$ — нечетное число. Тогда по квадратичному закону взаимности для символа Якоби и по утверждению последней задачи получим

$$\left(\frac{n}{m}\right) = \left(\frac{2^d}{m}\right)\left(\frac{|u|}{m}\right) = \left(\frac{m}{2^d}\right)\left(\frac{m}{|u|}\right) = \left(\frac{m}{2^d|u|}\right) = \left(\frac{m}{|n|}\right) = \left(\frac{m}{n}\right).$$

Пусть, далее, $m \equiv 3 \pmod 4, u > 0$. Используя предыдущие аргументы, найдем

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

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

Пусть, наконец, $m \equiv 3 \pmod 4, u < 0$. Повторяя с очевидными изменениями предыдущие рассуждения, получим

$$\left(\frac{n}{m}\right) = \left(\frac{2^d}{m}\right)\left(\frac{-1}{m}\right)\left(\frac{|u|}{m}\right) = -\left(\frac{m}{2^d}\right)(-1)^{\frac{|u|-1}{2}}\left(\frac{m}{|u|}\right) =$$

$$= -(-1)^{\frac{|u|-1}{2}}\left(\frac{m}{2^d|u|}\right) = -(-1)^{\frac{|u|-1}{2}}\left(\frac{m}{|n|}\right) = \left(\frac{-m}{n}\right). \blacktriangleleft$$

9. Пусть $d \equiv 0$ или $1 \pmod 4$ и не является полным квадратом, m — натуральное число. Тогда символ Кронекера $\left(\frac{d}{m}\right)$ можно представить через символ Якоби следующим способом:

$$\left(\frac{d}{m}\right) = \begin{cases} 1, & \text{если } (m,d) > 1, \\ \left(\frac{m}{|d|}\right), & \text{если } (m,d) = 1, d \equiv 1 \pmod 4, \\ \left(\frac{d/4}{m}\right), & \text{если } (m,d) = 1, d \equiv 0 \pmod 4. \end{cases}$$

► Из определения символа Кронекера следует, что при $(m,d) > 1$ имеем $\left(\frac{d}{m}\right) = 0$. Далее, из утверждения задачи 4 при $(m,d) = 1, d \equiv 1 \pmod 4$, получим $\left(\frac{d}{m}\right) = \left(\frac{m}{|d|}\right)$. Наконец, при $(m,d) = 1, d \equiv 0 \pmod 4, d = 2^b u, (u,2) = 1$, из утверждения задачи 4 находим

$$\left(\frac{d}{m}\right) = \left(\frac{2}{m}\right)^b (-1)^{(u-1)(m-1)/4}\left(\frac{m}{|u|}\right) =$$

$$= \left(\frac{2}{m}\right)^{b-2}(-1)^{(u-1)(m-1)/4}\left(\frac{m}{|u|}\right) = \left(\frac{d/4}{m}\right).$$

Таким образом, искомая формула доказана. ◄

10. 1). Существует нечетное простое число p такое, что символ Кронекера $\left(\frac{d}{p}\right)$ равен -1.

2). Пусть n не является точным квадратом. Тогда существует бесконечно много нечетных простых чисел p таких, что $\left(\frac{n}{p}\right) = -1$.

3). Пусть сравнение $x^2 \equiv n \pmod p$ разрешимо для всех достаточно больших простых чисел p. Тогда n — полный квадрат.

► 1). Из утверждения предыдущей задачи достаточно рассмотреть случай $d \equiv 1 \pmod 4$. Имеем

$$\left(\frac{d}{p}\right) = \left(\frac{p}{|d|}\right).$$

Поскольку $|d|$ не является полным квадратом, в каноническом разложении его степень некоторого простого числа q входит в нечетной степени. Найдем число p из условий

$$\left(\frac{p}{q}\right) = -1, \left(\frac{p}{r}\right) = 1$$

для любого простого делителя $r \neq q$ числа $|d|$. Это число p должно принадлежать некоторой арифметической прогрессии с разностью $|d|$.

2). Так как n не является полным квадратом, то в каноническом разложении n на простые сомножители найдется простое число q, которое входит в это каноническое разложение в нечетной степени. Простые числа p будем искать из следующих условий

$$\left(\frac{q}{p}\right) = -1, \left(\frac{r}{p}\right) = 1$$

для любого простого делителя $r \neq q$ числа n.

3). По условию задачи существует p_0 такое, что для всех $p \geqslant p_0$ разрешимо сравнение $x^2 \equiv n \pmod{p}$, т.е. $\left(\frac{n}{p}\right) = 1$. В силу утверждения 2), если n — не квадрат, то существует бесконечно много простых чисел p, для которых $\left(\frac{n}{p}\right) = -1$. Это противоречит условию, что $\left(\frac{n}{p}\right) = 1$ для всех достаточно больших p. ◄

§ 7. Простейшие теоремы о распределении простых чисел

1. Пусть $n \geqslant 2$ — натуральное число. Тогда справедливо следующее неравенство $\prod\limits_{p \leqslant n} p < 4^n$, где p пробегает все простые числа, не превосходящие n.

► Проведем индукцию по n. При $n = 2$ утверждение задачи верно. Предположим, что утверждение задачи имеет место при $n = m$. Докажем его при $n = m + 1$. Если $m + 1$ — четное число, то

$$\prod_{p \leqslant m+1} p = \prod_{p \leqslant m} p < 4^m < 4^{m+1}.$$

Пусть, теперь, $m + 1 = 2k + 1, k \geqslant 1$. Тогда каждое простое число p из отрезка от $k + 2$ до $2k + 1$ является делителем биномиального

коэффициента $\binom{2k+1}{k}$, т.е.

$$\prod_{k+2\leqslant p\leqslant 2k+1} p \mid \binom{2k+1}{k}.$$

Кроме того, при $k \geqslant 1$ справедливо неравенство

$$\binom{2k+1}{k} < 4^k.$$

Оно также доказывается индукцией по k. При $k = 1$ неравенство верно. Предположим, что оно верно при $k = r$. Докажем его при $k = r + 1$. Имеем

$$\binom{2r+3}{r+1} = \binom{2r+1}{r} \frac{(2r+3)(2r+2)}{(r+2)(r+1)} < 2\frac{2r+3}{r+2} 4^r < 4^{r+1}.$$

Отсюда находим

$$\prod_{p\leqslant 2k+1} p \leqslant \binom{2k+1}{k} \prod_{p\leqslant k+1} p < 4^{2k+1}. \blacktriangleleft$$

Пусть $x > 1$ и p — простое число. Определим функцию Мангольдта $\Lambda(n)$ натурального аргумента n следующим соотношением

$$\Lambda(n) = \begin{cases} \ln p, & \text{если} \quad n = p^\alpha, \\ 0, & \text{в противном случае.} \end{cases}$$

Далее, определим функцию Чебышёва $\psi(x)$ вещественного аргумента x равенством

$$\psi(x) = \sum_{n\leqslant x} \Lambda(n) = \sum_{\substack{p,\alpha \\ p^\alpha \leqslant x}} \ln p.$$

Пусть символ $[a, b, \ldots, c]$ обозначает наименьшее общее кратное чисел $a, b, \ldots, c$.

2. При $n \geqslant 2$ справедливо равенство

$$[2, 3, \ldots, n] = e^{\psi(n)}.$$

► Имеем $[2,3,\dots,n]=\prod\limits_{p\leqslant n}p^{e_p}$, где показатели e_p определяются из неравенств $p^{e_p}\leqslant n\leqslant p^{e_p+1}$. Следовательно,

$$e_p=\left[\frac{\ln n}{\ln p}\right]=\sum_{\substack{\alpha\\ p^\alpha\leqslant n}}1.$$

С другой стороны, находим

$$\psi(n)=\sum_{m\leqslant n}\Lambda(m)=\sum_{p\leqslant n}\ln p\sum_{\substack{\alpha\\ p^\alpha\leqslant n}}1=\sum_{p\leqslant n}e_p\ln p.$$

Отсюда получим

$$e^{\psi(n)}=\prod_{p\leqslant n}p^{e_p}.\ \blacktriangleleft$$

3. При $n\geqslant 1$ имеем неравенство $\psi(2n+1)\geqslant 2n\ln 2$.

► Из цепочки равенств

$$I=\int\limits_0^1 x^n(1-x)^n\,dx=\sum_{k=0}^n\binom{n}{k}(-1)^k\int\limits_0^1 x^{n+k+1}\,dx=$$
$$=\sum_{k=0}^n\binom{n}{k}\frac{(-1)^k}{n+k+1}$$

следует, что $[n+1,n+2,\dots,2n+1]I$ является натуральным числом. Следовательно, $[2,3,\dots,2n+1]I\geqslant 1$. Отсюда, используя утверждение предыдущей задачи, находим $e^{\psi(2n+1)}I\geqslant 1$.

Далее, для любого x из отрезка $[0,1]$ имеем неравенство $x(1-x)\leqslant 1/4$. Стало быть, $I\leqslant 2^{-2n}$. Подставим эту оценку величины I в предыдущее неравенство, получим $e^{\psi(2n+1)}\geqslant 2^{2n}$, т.е. $\psi(2n+1)\geqslant 2n\ln 2$. ◄

Обозначим символом $\pi(x)$ количество всех простых чисел, не превосходящих x. Пусть, далее, $\theta(x)$ обозначает сумму $\theta(x)=\sum\limits_{p\leqslant x}\ln p$. Из утверждения задачи 1 при $n=[x]$ имеем

$$\theta(x)=\theta(n)\leqslant 2n\ln 2\leqslant 2x\ln 2.$$

4. Для любого $x\geqslant 4$ справедливы неравенства

$$\frac{Ax}{\ln x}\leqslant\pi(x)\leqslant\frac{Bx}{\ln x},$$

где A и B — некоторые положительные постоянные, удовлетворяющие условиям $A \leqslant 1 \leqslant B$.

► Имеем

$$\ln \sqrt{x}(\pi(x) - \pi(\sqrt{x})) \leqslant \theta(x) \leqslant 2x \ln 2.$$

Следовательно,

$$\pi(x) \leqslant 2 \ln 2 \frac{x}{\ln \sqrt{x}} + \pi(\sqrt{x}) \leqslant 4 \ln 2 \frac{x}{\ln x}(1 + \frac{1}{4 \ln 2 \sqrt{x} \ln x}) \leqslant$$

$$\leqslant 6 \ln 2 \frac{x}{\ln x}, B = 6 \ln 2.$$

Оценим функцию $\pi(x)$ снизу. Очевидно, имеем $\pi(x) \geqslant \frac{\theta(x)}{\ln x}$. Далее, находим

$$\theta(x) = \psi(x) - \sum_{\substack{p^\alpha \leqslant x \\ \alpha \geqslant 2}} \ln p \geqslant \psi(x) - \sqrt{x} \ln x \log_2 x.$$

Отсюда и из утверждения предыдущей задачи получим

$$\theta(x) \geqslant (x-2) \ln 2 - \sqrt{x} \ln x \log_2 x \geqslant \frac{\ln 2}{3} x.$$

Таким образом, находим $\pi(x) \geqslant \frac{\ln 2}{3} \cdot \frac{x}{\ln x}$. ◄

§ 8. Распознавание простых и составных чисел

1. Для того чтобы натуральное число $n \geqslant 2$ было простым необходимо и достаточно, чтобы выполнялось сравнение

$$(n-1)! \equiv -1 \pmod{n}.$$

► *Необходимость.* Пусть n — простое число. Тогда для любого вычета a по модулю n, отличного от 1 и -1, найдется вычет b по модулю n такой, что $ab \equiv 1 \pmod{n}$ и $a \not\equiv b \pmod{n}$. В произведении $(n-1)!$ сгруппируем попарно такие вычеты a и b. Без пары останутся только 1 и -1. Следовательно, $(n-1)! \equiv -1 \pmod{n}$.

Достаточность. Предположим противное, т.е. n — составное число, $a \mid n, 1 < a < n$. Из условия $n \mid (n-1)! + 1$ следует, что $a \mid (n-1)! + 1$. Отсюда имеем противоречивую цепочку сравнений

$$-1 \equiv (n-1)! \equiv 0 \pmod{a}.$$

Таким образом, предположение о том, что число n — составное является неверным. Следовательно, n — простое число. ◀

2. Пусть a, n — натуральные числа, $(a, n) = 1$ и $a^{n-1} \not\equiv 1 \pmod{n}$. Тогда n — составное число.

▶ Это утверждение есть логическое обращение малой теоремы Ферма: пусть p — простое число, $(a, p) = 1$; тогда $a^{p-1} \equiv 1 \pmod{p}$. ◀

Составное число n, для которого $a^{n-1} \equiv 1 \pmod{n}$, называется псевдопростым числом Ферма (по основанию a). Составное число n, удовлетворяющие для всякого a, взаимно простого с n, условию $a^{n-1} \equiv 1 \pmod{n}$, называется числом Кармайкла. Наименьшим таким числом является $561 = 3 \cdot 11 \cdot 17$.

3. Пусть n — нечетное число, a — натуральное число, $(a, n) = 1$, и

$$a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod{n}.$$

Тогда n — составное число.

▶ Это утверждение есть логическое обращение критерия Эйлера для квадратичного вычета по простому модулю n: пусть n — нечетное простое число, a — натуральное число, $(a, n) = 1$, $\left(\frac{a}{n}\right)$ — символ Якоби. Тогда

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

Нечетное составное число n, для которого при a, взаимно простом с n, выполняется сравнение

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n},$$

называется псевдопростым числом Эйлера (по базе a).

Известно, что число 561 является числом Кармайкла, но по утверждению задачи 1 нельзя установить, что оно составное. Так как $5^{280} \equiv 67 \pmod{561}$, то по утверждению задачи 2 число 561 является составным.

4. Пусть p — простое число, k — натуральное число, $k < p, n = kp^2 + 1$ и

$$2^k \not\equiv 1 \pmod{n}, \quad 2^{n-1} \equiv 1 \pmod{n}.$$

Тогда число n — простое.

▶ Покажем сначала, что $p \mid \varphi(n)$. Пусть $d > 1$ обозначает минимальное натуральное число такое, что $2^d \equiv 1 \pmod{n}$. Разделим

числа $n-1, \varphi(n)$ с остатком на d. Получим

$$n-1 = dq_1 + r_1, \varphi(n) = dq_2 + r_2, 0 \leqslant r_1, r_2 \leqslant d-1.$$

Отсюда имеем

$$2^{r_1} - 1 \equiv 2^{(n-1)-dq_1} - 1 \equiv 0 \pmod{n},$$

$$2^{r_2} - 1 \equiv 2^{\varphi(n)-dq_2} - 1 \equiv 0 \pmod{n}.$$

Следовательно, в силу выбора числа d минимальным с условием $2^d - 1 \equiv 0 \pmod{n}$ имеем, что $r_1 = 0, r_2 = 0$.

Далее, d не делит k, так как $2^k \not\equiv 1 \pmod{n}$.

Таким образом, находим $kp^2 = n - 1 = dm, d \not| k$. Отсюда имеем $p \mid d$. Значит, $p \mid d \mid \varphi(n)$.

Предположим, что n составное число. Тогда покажем, что существует простой делитель q числа n такой, что $q \equiv 1 \pmod{p}$. Число n взаимно просто с p, поскольку $n = kp^2 + 1$. Пусть $n = q_1^{\alpha_1} \dots q_r^{\alpha_r}$. Тогда имеем $\varphi(n) = (q_1^{\alpha_1} - q_1^{\alpha_1 - 1}) \dots (q_1^{\alpha_r} - q_1^{\alpha_r - 1})$. Поскольку $p \mid \varphi(n)$, найдется простой делитель q числа n такой, что $p \mid (q^\alpha - q^{\alpha-1})$. Далее, $(p, q) = 1$, поэтому $p \mid q - 1$.

Положим $q = up + 1$. Имеем $n = kp^2 + 1 = (up + 1)(vp + 1)$. Следовательно, $uvp + u + v = kp$. Отсюда при некотором натуральном s находим, что $u + v = ps$. Далее получим противоречивое неравенство

$$p \leqslant uv < k < p.$$

Таким образом предположение о том, что число n составное неверно. ◀

В 1951 г. Миллер и Вилер [**?**], используя компьютер и утверждение предыдущей задачи, доказали, что $180(2^{127} - 1)^2 + 1$ — простое число.

5. Пусть p — нечетное простое число, k — натуральное число, $k \leqslant 2p + 1, n = 2kp + 1$, и пусть существует натуральное число a такое, что

$$a^{n-1} \equiv 1 \pmod{n}, a^{2k} \not\equiv 1 \pmod{n}.$$

Тогда n — простое число.

▶ Покажем, как и предыдущей задаче, что $p \mid \varphi(n)$. Пусть d обозначает порядок элемента a по модулю n. Тогда, проводя те же рассуждения, что и в предыдущей задаче, находим $d \mid n-1, d \mid \varphi(n)$. Поскольку $a^{2k} \not\equiv 1 \pmod{n}$, число d не является делителем числа

$2k$. Следовательно, из равенства $n-1=2kp=dm$ имеем $p \mid d$. Но $d \mid \varphi(n)$, поэтому $p \mid \varphi(n)$.

Пусть число n — составное и $n=\prod\limits_{q|n} q^{\alpha_q}$ — каноническое разложение его на простые сомножители. Имеем $\varphi(n)=\prod\limits_{q|n}(q^{\alpha_q}-q^{\alpha_q-1})$. Так как $p \mid \varphi(n)$, то найдется $q \mid n$ такое, что $p \mid q^{\alpha_q}-q^{\alpha_q-1}$. Следовательно, $p \mid q-1$, т.е. $q \equiv 1 \pmod p$. Поскольку q нечетное число, имеем $q \equiv 1 \pmod{2p}$, т.е. при некотором натуральном u справедливо равенство $q=1+2pu$. Далее, $n=1+2kp$, поэтому $n=(1+2pu)(1+2pv)$. Отсюда находим $n \geqslant (1+2p)^2$. С другой стороны, $n=1+2kp \leqslant 1+2(2p+1)p<(1+2p)^2$. Последние два неравенства противоречивы. Следовательно, предположение о том, что n составное число неверно. ◀

Наименьшее натуральное число l с условием $a^l \equiv 1 \pmod m, (a,m)=1$, называется порядком натурального числа a по модулю m или число a по модулю m принадлежит показателю l.

Заметим, что для простого числа p и $d \mid p-1$ количество $I=I(d)$ решений сравнения $x^d \equiv 1 \pmod p$ равно d. Действительно, по утверждению задачи I.6 величина $I(d) \leqslant d$. Далее, по малой теореме Ферма сравнение $x^{p-1} \equiv 1 \pmod p$ имеет $p-1$ решений, — все вычеты из приведенной системы вычетов по модулю p. Рассмотрим сравнение

$$\frac{x^{p-1}-1}{x^d-1}=(x^d)^{\frac{p-1}{d}-1}+\cdots+x^d+1 \equiv 0 \pmod p.$$

По теореме I.6 количество его решений $p-1-I(d)$ не превосходит степени многочлена $p-1-d$. Следовательно, $I(d) \geqslant d$. Таким образом, $I(d)=d$.

6. Пусть p — простое число и l делит $p-1$. Тогда количество чисел порядка l из приведенной системы вычетов по модулю p равно $\varphi(l)$.

▶ Обозначим символом $\psi(l)$ количество чисел порядка l из приведенной системы вычетов по модулю p. Сначала докажем, что $\psi(l)$ обладает свойством мультипликативности, т.е. для любых $(l_1,l_2)=1, l_1 \mid p-1, l_2 \mid p-1$ имеем $\psi(l_1l_2)=\psi(l_1)\psi(l_2)$.

Пусть число h_1 имеет порядок l_1, число h_2 — порядок l_2 и число h_1h_2 — порядок l. Докажем, что $l=l_1l_2$. Действительно, находим $(h_1h_2)^{l_1l_2} \equiv 1 \pmod p$, т.е. $l \leqslant l_1l_2$. С другой стороны, имеем $1 \equiv$

$(h_1h_2)^{ll_2} \equiv h_1^{ll_2} \pmod p$. Следовательно, $l_1 \mid ll_2$. Но так как $(l_1, l_2) = 1$, то $l_1 \mid l$. Аналогично доказывается, что $l_2 \mid l$. Отсюда $l_1l_2 \mid l$. Значит, $l_1l_2 \leqslant l$. Таким образом, получаем $l = l_1l_2$.

Итак, установлено соответствие: паре чисел (h_1, h_2) с указанными выше свойствами ставится в соответствие их произведение h_1h_2 по модулю p. Покажем, что оно взаимно-однозначное. Пусть (h_1', h_2') — другая пара с тем же произведением $h_1'h_2' \equiv h_1h_2 \pmod p$. Тогда $h_1'h_1^{-1} \equiv h_2'h_2^{-1} \pmod p$. Таким образом, числа $h_1'h_1^{-1}$ и $h_2'h_2^{-1}$ имеют один и тот же порядок δ, причем $\delta \mid l_1, \delta \mid l_2$. Следовательно, $\delta = 0$ и $h_1'h_1^{-1} \equiv h_2'h_2^{-1} \equiv 1 \pmod p$. Это означает, что пары (h_1, h_2) и (h_1', h_2') по модулю p совпадают.

Заметим, что обратное отображение можно задать так: $h_1 = h^{l_2}, h_2 = h^{l_1}$.

Таким образом установлено, что $\psi(l_1)\psi(l_2) = \psi(l_1l_2)$.

Пусть, далее, $q^t \mid p-1, q$ — простое число. Тогда для того, чтобы число h имело порядок q^t по модулю p, необходимо и достаточно, чтобы выполнялись условия

$$h^{q^t} \equiv 1 \pmod p, h^{q^{t-1}} \not\equiv 1 \pmod p.$$

Поскольку сравнение $x^{q^t} \equiv 1 \pmod p$ имеет q^t не сравнимых по модулю p решений, находим

$$\psi(q^t) = q^t - q^{t-1} = \varphi(q^t).$$

По свойству мультипликативности функций $\psi(l)$ и $\varphi(l)$ отсюда следует, что $\psi(l) = \varphi(l)$. ◀

Число a называется первообразным корнем по модулю m, если порядок его равен $\varphi(m)$. Из утверждения предыдущей задачи следует, что количество первообразных корней по нечетному простому модулю p равно $\varphi(p-1)$. Тем не менее, докажем теорему о существовании первообразного корня по простому модулю, дающую способ построения его.

7. Для нечетного простого числа существует первообразный корень.

► Пусть p и q — простые числа, l — натуральное число и $p \equiv 1 \pmod{q^l}$. Докажем, что найдется число a, принадлежащее показателю q^l по модулю p. Так как по утверждению задачи I.6 количество не сравнимых корней полиномиального сравнения не превосходит его степени, то при $p \geqslant 3$ количество решений сравнения

$x^{(p-1)/q} \equiv 1 \pmod p$ не превосходит $\frac{p-1}{q} \leqslant \frac{p-1}{2} \leqslant p-2$. Следовательно, найдется такой вычет $b, (b,p)=1$, что $b^{(p-1)/q} \not\equiv 1 \pmod p$. Положим $a = b^{(p-1)/q^l}$. Тогда имеем

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

Пусть a принадлежит по модулю p показателю δ. Из предыдущего сравнения имеем, что δ делит q^l. Возможны два случая $\delta = q^l$ и $\delta \mid q^{l-1}$. Рассмотрим второй случай. Из определения порядка по модулю p числа a имеем

$$b^{(p-1)/q} = a^{q^{l-1}} \equiv 1 \pmod p.$$

Это противоречит выбору числа b. Следовательно, число a по модулю p принадлежит показателю q^l.

Докажем теперь, что существует число g, принадлежащее показателю $p-1$ по модулю p, т.е. число g будет первообразным корнем по модулю p.

При $p=2$ число 1 удовлетворяет условию задачи. Пусть p будет нечетным простым числом и каноническое разложение на простые сомножители числа $p-1$ имеет вид $p-1 = \prod\limits_{q|p-1} q^{\alpha_q}$. Ранее доказано, что существует число a_q, принадлежащее показателю q^{α_q} по модулю p. Положим $g = \prod\limits_{q|p-1} a_q$ и буквой Δ обозначим показатель, которому число g принадлежит по модулю p. Из теоремы Эйлера имеем $\Delta \mid p-1$. Возможны два случая: либо $\Delta = p-1$, либо при некотором простом q и натуральном u имеем $p-1 = qu\Delta$.

Рассмотрим второй случай. Имеем

$$1 \equiv g^{\Delta u} \equiv g^{(p-1)/q} \equiv a_q^{(p-1)/q} \prod_{\substack{r|p-1 \\ r \neq q}} a_r^{(p-1)/q} \equiv a_q^{(p-1)/q} \not\equiv 1 \pmod p.$$

Это соотношение противоречиво. Следовательно, второй случай не возможен. Таким образом, $\Delta = p-1$. ◀

Пусть $m > 1$ — натуральное число и пусть существует натуральное число g такое, что числа $g^0, g^1, g^2, \ldots, g^{\varphi(m)-1}$ образуют приведенную систему вычетов по модулю m. Тогда число g называется первообразным корнем по модулю m.

8. Для того чтобы по модулю $m > 1$ существовал первообразный корень необходимо и достаточно, чтобы число m имело вид $2, 4, p^\alpha, 2p^\alpha$, где p — нечетное простое и l — натуральное.

▶ Пусть $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ — каноническое разложение числа m на простые сомножители. По теореме Эйлера для каждого числа a, взаимно простого с p, и любого натурального α, справедливо сравнение $a^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$.

Пусть буква q обозначает наименьшее общее кратное чисел $\varphi(p_1^{\alpha_1}), \dots, \varphi(p_r^{\alpha_r})$. Тогда имеем $a^q \equiv 1 \pmod{m}$. Следовательно, если $q < \varphi(m)$, то первообразных корней по модулю m не существует.

Если p — нечетное простое и α — натуральное число, то $\varphi(p^\alpha)$ — четное число. Отсюда получим, что если по модулю m существует первообразный корень, то m не может иметь двух различных нечетных простых делителей.

Таким образом, первообразный корень может существовать по модулям m вида $2^\alpha, p^\alpha, 2^\beta p^\alpha$. Пусть $\beta \geqslant 2$. Тогда $\varphi(2^\beta) = 2^{\beta-1}$ — четное число и по модулю $m = 2^\beta p^\alpha$ не существует первообразных корней. Следовательно, первообразные корни могут существовать по модулям $2^\alpha, p^\alpha, 2p^\alpha$.

Рассмотрим случай $m = 2^\alpha$. При $\alpha = 1$ число 1 — первообразный корень по модулю 2, при $\alpha = 2$ число 3 — первообразный корень по модулю 4.

Индукцией по α докажем, что при $\alpha \geqslant 3$ по модулю 2^α нет первообразных корней. При $\alpha = 3$ для любого нечетного $a = 2b + 1$ имеем $a^2 = 4b(b + 1) + 1 \equiv 1 \pmod{8}$. Следовательно, по модулю 8 первообразных корней нет.

Предположим, что утверждение справедливо при $\alpha = l$, т.е. для любого нечетного числа порядок его меньше $\varphi(2^l) = 2^{l-1}$. Это означает, что

$$a^{2^{l-2}} \equiv 1 \pmod{2^l} \quad \text{или} \quad a^{2^{l-2}} = 1 + 2^l d$$

при некотором целом числе $d = d(a)$.

Докажем утверждение при $\alpha = l + 1$. Имеем

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

Таким образом, порядок любого нечетного числа по модулю 2^l при $l \geqslant 3$ не превосходит $2^{l-2} = \varphi(2^l)/2$, т.е. по модулю $2^l, l \geqslant 3$ нет первообразных корней.

Рассмотрим теперь случай $m = p^\alpha$, где p — нечетное простое число.

Индукцией по α докажем, что при $\alpha \geqslant 1$ по модулю p^α существует первообразный корень. При $\alpha = 1$ это утверждение совпадает с утверждением предыдущей задачи.

Пусть g — первообразный корень по модулю p. Положим

$$h = \begin{cases} g, & \text{если} \quad g^{p-1} \not\equiv 1 \pmod{p^2}, \\ g+p, & \text{если} \quad g^{p-1} \equiv 1 \pmod{p^2}. \end{cases}$$

Тогда имеем $h^{p-1} \not\equiv 1 \pmod{p^2}$. Достаточно проверить, что в случае $g^{p-1} \equiv 1 \pmod{p^2}$, выполняется следующее соотношение

$$h^{p-1} - 1 \equiv (g+p)^{p-1} - 1 \equiv -pg^{p-2} \not\equiv 0 \pmod{p^2}.$$

Покажем сначала, что h является первообразным корнем по модулю p^2. Пусть h по модулю p^2 принадлежит показателю δ. Тогда имеем $h^\delta \equiv 1 \pmod{p^2}$. Следовательно, $h^\delta \equiv g^\delta \equiv 1 \pmod{p}$. Так как g — первообразный корень по модулю p, то δ кратно $p-1$. С другой стороны, по теореме Эйлера δ делит $\varphi(p^2) = p(p-1)$. Таким образом, показатель δ может быть равен либо $p-1$, либо $p(p-1)$. По выбору числа h имеем

$$h^{p-1} = 1 + kp, \quad k \not\equiv 0 \pmod{p}; h^{p-1} \not\equiv 1 \pmod{p^2}.$$

Это означает , что h не принадлежит по модулю p^2 показателю $p-1$. Остается только возможность $\delta = p(p-1)$, т.е. h является первообразным корнем по модулю p^2.

Предположим, что число h является первообразным корнем по модулю p^l, т.е. h по модулю p^l принадлежит показателю $\varphi(p^l)$.

Докажем, что утверждение верно при $\alpha = l+1$, т.е. h — первообразный корень по модулю p^{l+1}. Пусть h по модулю p^{l+1} принадлежит показателю Δ. Поскольку выполняется сравнение $h^\Delta \equiv 1 \pmod{p^{l+1}}$, получим $h^\Delta \equiv 1 \pmod{p^l}$. Но число h — первообразный корень по модулю p^l. Следовательно, Δ кратно $\varphi(p^l) = p^{l-1}(p-1)$. По теореме Эйлера имеем $h^{p^l(p-1)} \equiv 1 \pmod{p^{l+1}}$. Следовательно, Δ является делителем числа $\varphi(p^{l+1}) = p^l(p-1)$. Отсюда находим, что Δ равно либо $\varphi(p^l) = p^{l-1}(p-1)$, либо $\varphi(p^{l+1})$. Далее, по биному Ньютона имеем

$$h^{p^{l-1}(p-1)} = (1+kp)^{p^{l-1}} \equiv 1 + kp^l \not\equiv 1 \pmod{p^{l+1}},$$

т.е. h по модулю p^{l+1} не принадлежит показателю $\varphi(p^l)$ и $\Delta \neq \varphi(p^l)$. Следовательно, $\Delta = \varphi(p^{l+1})$ и число h — первообразный корень по модулю p^{l+1}.

Рассмотрим случай $m = 2p^\alpha, p$ — нечетное простое число. Пусть g — первообразный корень по модулю p^α. Тогда

$$h = \begin{cases} g, & \text{если} g \equiv 1 \pmod 2, \\ g + p^\alpha, & \text{если} g \equiv 0 \pmod 2 \end{cases}$$

является первообразным корнем по модулю $2p^\alpha$. ◀

Утверждение следующей задачи дает способ разыскания первообразных корней по некоторому модулю m. Из утверждения предыдущей задачи имеем, что m равно одному из значений $2, 4, p^\alpha, 2p^\alpha$, где p — нечетное простое число и α — натуральное число.

9. Для того чтобы число g, взаимно простое с m, было первообразным корнем по модулю m, необходимо и достаточно, чтобы для любого простого делителя q числа $\varphi(m)$ выполнялось условие

$$g^{\varphi(m)/q} \not\equiv 1 \pmod m.$$

▶ *Необходимость.* Поскольку g — первообразный корень по модулю m, число g по модулю m принадлежит показателю $\varphi(m)$ и, следовательно, для любого простого делителя q выполняются условия

$$g^{\varphi(m)/q} \not\equiv 1 \pmod m.$$

Достаточность. Пусть δ — показатель, которому принадлежит g по модулю m. По теореме Эйлера число g является делителем $\varphi(m)$. Предположим, что $\delta < \varphi(m)$. Тогда имеем $\varphi(m) = \delta q u$, где q — некоторое простое число. Следовательно,

$$g^{\varphi(m)/q} = g^{\delta u} \equiv 1 \pmod m,$$

что противоречит условию задачи. ◀

Следующий признак распознавания простоты числа принадлежит Е. Люка и Д.Х.Лемеру [**?**].

10. Пусть $N \geqslant 2$ — натуральное число, $N - 1 = \prod\limits_{q \mid N-1} q^{\alpha_q}$ — каноническое разложение числа $N - 1$ на простые сомножители, и пусть найдется натуральное число a такое, что

$$a^{N-1} \equiv 1 \pmod N,$$

и для любого $q \mid N - 1$ выполняется условие

$$a^{(N-1)/q} \not\equiv 1 \pmod N.$$

Тогда число N является простым.

► Пусть число a по модулю N принадлежит показателю δ. Тогда из условия $a^{N-1} \equiv 1 \pmod N$ следует, что $\delta \mid N-1$. Предположим, что $\delta < N-1$. Тогда найдется простое число q, делящее $N-1$, такое, что $N-1 = qu\delta$. Далее, имеем

$$1 \equiv a^{\delta u} \equiv a^{(N-1)/q} \not\equiv 1 \pmod N.$$

Противоречие. Следовательно, $\delta = N-1$, и число a по модулю N принадлежит показателю $N-1$.

Далее, по теореме Эйлера находим $a^{\varphi(N)} \equiv 1 \pmod N$. Отсюда имеем, что $N-1 \mid \varphi(N)$. Следовательно, $N-1 \leqslant \varphi(N)$.

Пусть N — составное число. Тогда найдется число p такое, что $p \mid N, 1 < p < N$. Стало быть, справедливы неравенства

$$\varphi(N) < N(1-\frac{1}{p}) < N(1-\frac{1}{N}) = N-1.$$

Это противоречит предыдущему неравенству для $N-1$. Таким образом, доказано, что N — простое число. ◄

11. Пусть $N \geqslant 2$ — натуральное число, $N-1 = \prod\limits_{q \mid N-1} q^{\alpha_q}$ — каноническое разложение числа $N-1$ на простые сомножители, и пусть для каждого простого числа $q \mid N-1$ найдется натуральное число a_q такое, что

$$a_q^{N-1} \equiv 1 \pmod N,$$

и для любого $q \mid N-1$ выполняется условие

$$a_q^{(N-1)/q} \not\equiv 1 \pmod N.$$

Тогда число N является простым.

► Пусть q — простое число, являющееся делителем $N-1$ и число a_q по модулю N принадлежит показателю δ_q. Тогда из условия $a_q^{N-1} \equiv 1 \pmod N$ следует, что $\delta_q \mid N-1$, т.е. при некотором натуральном числе u_q имеем $N-1 = \delta_q u_q$.

Докажем, что $(q, u_q) = 1$. Предположим противное, т.е. $q \mid u_q$. Тогда при некотором натуральном v_q получим $N-1 = \delta_q q v_q$. Отсюда, используя условие задачи, получим противоречивое соотношение

$$1 \equiv a_q^{\delta_q v_q} = a_q^{(N-1)/q} \not\equiv 1 \pmod N.$$

Следовательно, $(q, u_q) = 1$. Значит, $\delta_q = q^{\alpha_q} w_q, (q, w_q) = 1$.

Рассмотрим число $b = \prod\limits_{q|N-1} a_q^{w_q}$. Докажем, что число b по модулю N принадлежит показателю $N-1$ и удовлетворяет условию предыдущей задачи.

Для любого простого $q \mid N-1$ число $a_q^{w_q}$ по модулю N принадлежит показателю q^{α_q}. Следовательно, число b по модулю N принадлежит показателю $\prod\limits_{q|N-1} q^{\alpha_q} = N-1$.

Далее, имеем

$$b^{N-1} = \prod_{q|N-1} a_q^{\delta_q w_q \frac{N-1}{\delta_q}} \equiv 1 \pmod{N}.$$

Рассмотрим любой простой делитель r числа $N-1$. Находим

$$b^{\frac{N-1}{r}} = a_r^{\frac{(N-1)w_r}{r}} \prod_{\substack{q|N-1 \\ q \neq r}} a_q^{\frac{(N-1)w_q}{r}} \not\equiv 1 \pmod{N},$$

поскольку при простом $q \mid N-1, q \neq r$, имеем

$$a_q^{\frac{(N-1)w_r}{r}} = a_q^{\delta_q \frac{(N-1)w_q}{r\delta_q}} \equiv 1 \pmod{N},$$

и поскольку показатель $\frac{(N-1)w_r}{r}$ не делится на δ_r, получим

$$a_r^{\frac{(N-1)w_r}{r}} \not\equiv 1 \pmod{N}.$$

Таким образом для числа N выполнены условия предыдущей задачи. Следовательно, N — простое число. ◀

12. Пусть $N \geqslant 2$ — натуральное число, $N-1 = FR, (F, R) = 1, R < F, F = \prod\limits_{q|F} q^{\alpha_q}$ — каноническое разложение числа F на простые сомножители, и пусть найдется натуральное число a такое, что

$$a^{N-1} \equiv 1 \pmod{N},$$

и для любого $q \mid F$ выполняется условие

$$(a^{(N-1)/q} - 1, N) = 1.$$

Тогда число N является простым.

► Предположим, что N — составное число. Пусть $p \geqslant 2$ — наименьший простой делитель числа N. Тогда $p \leqslant \sqrt{N}$. По условию задачи имеем $a^{N-1} \equiv 1 \pmod p$, и для любого простого $q \mid F$ справедливо соотношение $a^{(N-1)/q} \not\equiv 1 \pmod p$. Буквой δ обозначим показатель, которому принадлежит число a по модулю p. Тогда $\delta \mid N-1$ и $N-1 = \delta u$. Возьмем любой простой делитель q числа F. Покажем, что $(q, u) = 1$. Предположим противное, т.е. $q \mid u$. Тогда при некотором натуральном v имеем $N - 1 = \delta q v$. Из определения δ и условия задачи находим противоречивое соотношение

$$1 \equiv a^{\delta v} = a^{(N-1)/q} \not\equiv 1 \pmod p.$$

Следовательно, для любого $q \mid F$ имеем $(q, u) = 1$ и $q^{\alpha_q} \mid \delta$. Отсюда получим, что $F \mid \delta$. Из малой теоремы Ферма находим $\delta \mid p - 1$. Таким образом, $F \mid p - 1$. Стало быть, $p \geqslant F + 1 > \sqrt{N}$. Это противоречит тому, что наименьший простой делитель составного числа N не превосходит $\sqrt{N}$. Значит, число N — простое. ◄

§ 9. Непрерывные (цепные) дроби. Критерий Лежандра для подходящих дробей

Рассмотрим любое вещественное число α. Пусть $a_0 = [\alpha]$ — наибольшее целое число, не превосходящее α, и $\{\alpha\} = \alpha - a_0$ — дробная часть числа α. Положим $\alpha = \alpha_0$

$$\alpha_1 = \begin{cases} 0, & \text{если} \quad \{\alpha\} = 0, \\ 1/\{\alpha\} & \text{в противном случае.} \end{cases}$$

Для нецелого α имеем

$$\alpha = a_0 + \frac{1}{\alpha_1}, \alpha_1 > 1.$$

Подобным образом при $s \geqslant 1$ для нецелого α_s имеем

$$\alpha_s = a_s + \frac{1}{\alpha_{s+1}}, \alpha_{s+1} > 1.$$

Таким образом число α разлагается в следующую простую непрерывную дробь

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_s + \cfrac{1}{\alpha_{s+1}}}}}.$$

Для удобства будем обозначать непрерывную дробь числа α в виде

$$\alpha = [a_0, a_1, a_2, \ldots, a_s, \alpha_{s+1}].$$

1. Для того чтобы вещественное число α разлагалось в конечную непрерывную дробь необходимо и достаточно, чтобы оно было рациональным числом.

▶ *Необходимость.* Процесс разложения числа α оборвется, скажем, на s-м шаге, если α_{s+1} равно целому числу a_{s+1}. Отсюда следует, что α — рациональное число.

Достаточность. Пусть $\alpha = p/q, (p, q) = 1$, — рациональное число. Тогда при нецелом α имеем $a_0 = [p/q]$ и

$$\frac{1}{\alpha_1} = \frac{p}{q} - \left[\frac{p}{q}\right], \alpha_1 > 1, \alpha_1 = [\alpha_1] + \frac{1}{\alpha_2}, a_1 = [\alpha_1],$$

т.е. для целого числа r_1 находим

$$p - q\left[\frac{p}{q}\right] = \frac{q}{\alpha_1} = r_1, 0 < r_1 < q.$$

Подобно этому получим

$$q - r_1\left[\frac{q}{r_1}\right] = \frac{r_1}{\alpha_2} = r_2, 0 < r_2 < r_1, \alpha_2 = [\alpha_2] + \frac{1}{\alpha_3}, a_2 = [\alpha_2].$$

Наконец, имеем

$$r_{s-1} - r_s\left[\frac{r_{s-1}}{r_s}\right] = \frac{r_s}{\alpha_{s+1}} = r_{s+1}, 0 < r_{s+1} < r_s,$$

и отношение r_s/r_{s+1} — натуральное число.

Таким образом, если α — рациональное число, то вычисление непрерывной дроби подобно алгоритму Евклида для нахождения наибольшего общего делителя чисел p и q, причем находим

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_s + \cfrac{1}{a_{s+1}}}}}.$$

Тем самым получено искомое разложение рационального числа α в конечную непрерывную дробь. ◀

Числа $a_0, a_1, a_2, \ldots$ называются неполными частными числа α, а дробь

$$\frac{p_n}{q_n} = [a_0, a_1, a_2, \ldots, a_n]$$

называется n-й подходящей дробью.

2. Подходящие дроби p_n/q_n при $n \geqslant 2$ удовлетворяют следующим соотношениям

$$\begin{cases} p_n = a_n p_{n-1} + p_{n-2}, \\ q_n = a_n q_{n-1} + q_{n-2}, \end{cases}$$

кроме того, имеем

$$p_0 = a_0, q_0 = 1; p_1 = a_0 a_1 + 1, q_1 = a_1.$$

▶ По определению имеем

$$\frac{p_0}{q_0} = [a_0] = \frac{a_0}{1}, \quad \frac{p_1}{q_1} = [a_0, a_1] = \frac{a_0 + \frac{1}{a_1}}{1} = \frac{a_1 a_0 + 1}{a_1}.$$

Проведем индукцию по параметру $n \geqslant 2$. При $n = 2$ находим

$$\frac{p_2}{q_2} = [a_0, a_1, a_2] = \frac{\left(a_1 + \frac{1}{a_2}\right) a_0 + 1}{a_1 + \frac{1}{a_2}} = \frac{a_2 p_1 + p_0}{a_2 q_1 + q_0},$$

т.е. справедливы равенства

$$\begin{cases} p_2 = a_2 p_1 + p_0, \\ q_2 = a_2 q_1 + q_0. \end{cases}$$

Предположим, что утверждение имеет место при $n = m$, т.е.

$$\begin{cases} p_m = a_m p_{m-1} + p_{m-2}, \\ q_m = a_m q_{m-1} + q_{m-2}. \end{cases}$$

Докажем его при $n = m + 1$. Используя замену a_m на $a_m + \frac{1}{a_{m+1}}$ и предположение индукции, находим

$$\frac{p_{m+1}}{q_{m+1}} = \frac{\left(a_m + \frac{1}{a_{m+1}}\right) p_{m-1} + p_{m-2}}{\left(a_m + \frac{1}{a_{m+1}}\right) q_{m-1} + q_{m-2}} =$$

$$= \frac{a_{m+1}(a_m p_{m-1} + p_{m-2}) + p_{m-1}}{a_{m+1}(a_m q_{m-1} + q_{m-2}) + q_{m-1}} = \frac{a_{m+1} p_m + p_{m-1}}{a_{m+1} q_m + q_{m-1}}.$$

Отсюда следуют искомые равенства для числителей и знаменателей подходящих дробей

$$\begin{cases} p_{m+1} = a_{m+1} p_m + p_{m-1}, \\ q_{m+1} = a_{m+1} q_m + q_{m-1}. \end{cases} \quad \blacktriangleleft$$

3. При $n \geqslant 1$ справедливы следующие равенства

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$$

или

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}},$$

а при $n \geqslant 2$ имеем

$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n.$$

При $n \geqslant 0$ подходящие дроби p_n/q_n несократимы.

► Проведем индукцию по параметру n. Базовые утверждения индукции справедливы. Действительно,

$$p_1 q_0 - p_0 q_1 = (a_1 a_0 + 1) \cdot 1 - a_0 \cdot a_1 = 1,$$

$$p_2 q_0 - p_0 q_2 = (a_2 p_1 + p_0) q_0 - p_0 (a_2 q_1 + q_0) = a_2 (p_1 q_0 - p_0 q_1) = a_2.$$

Предположим, что утверждения имеют место при $n = m$, т.е.

$$p_m q_{m-1} - p_{m-1} q_m = (-1)^{m-1}$$

$$p_m q_{m-2} - p_{m-2} q_m = (-1)^m a_m.$$

Докажем его при $n = m+1$. По предположению индукции находим

$$p_{m+1} q_m - p_m q_{m+1} = (a_m p_m + p_{m-1}) q_m - p_m (a_m q_m + q_{m-1}) =$$

$$= p_{m-1} q_m - p_m q_{m-1} = -(-1)^{m-1} = (-1)^m,$$

$$p_{m+1} q_{m-1} - p_{m-1} q_{m+1} = (a_m p_m + p_{m-1}) q_{m-1} - p_{m-1} (a_m q_m + q_{m-1}) =$$

$$= a_m (p_m q_{m-1} - p_{m-1} q_m) = (-1)^{m-1} a_m = (-1)^{m+1} a_m.$$

Искомые равенства доказаны. При $n \geqslant 1$ из равенства $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$ следует, что числа p_n и q_n взаимно просты. ◄

4. 1). Пусть $n \geqslant 2$. Тогда для знаменателей подходящих дробей справедливо неравенство $q_n \geqslant q_{n-1} + 1$, так что $q_n \geqslant n$.

2). При $n \geqslant 1$ имеем

$$\frac{p_{2n+1}}{q_{2n+1}} < \frac{p_{2n-1}}{q_{2n-1}}, \quad \frac{p_{2n}}{q_{2n}} > \frac{p_{2n-2}}{q_{2n-2}}.$$

► 1). По утверждению задачи 2 при $n \geqslant 2$ имеем

$$q_n = a_n q_{n-1} + q_{n-2} \geqslant q_{n-1} + 1.$$

Далее $q_2 = a_2 a_1 + 1 \geqslant 2$. Следовательно, используя предыдущее неравенство, получим

$$q_n \geqslant q_{n-1} + 1 \geqslant q_{n-2} + 2 \geqslant \ldots \geqslant q_2 + n - 2 \geqslant n.$$

2). По утверждению предыдущей задачи при $n \geqslant 2$ имеем

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n a_n}{q_n q_{n-2}}.$$

Отсюда при $n = 2m$ получим

$$\frac{p_{2m}}{q_{2m}} - \frac{p_{2m-2}}{q_{2m-2}} > 0,$$

а при $n = 2m+1$

$$\frac{p_{2m+1}}{q_{2m+1}} - \frac{p_{2m-1}}{q_{2m-1}} < 0. \blacktriangleleft$$

5. Пусть $A_n = [a_0, a_1, a_2, \ldots, a_n]$ является n-й подходящей дробью числа α. Тогда при $n \to \infty$ существует предел последовательности A_n.

► По утверждению 2) предыдущей задачи и первому тождеству задачи 3 имеем $A_1 \geqslant A_{2n+1} \geqslant A_{2n} \geqslant A_2$. Отсюда следует существование пределов при $n \to \infty$ последовательностей $\{A_{2n}\}$ и $\{A_{2n+1}\}$.

Далее по первому тождеству задачи 2 и утверждению 1) задачи 3 получим

$$|A_{2n} - A_{2n-1}| = \frac{1}{q_{2n}q_{2n-1}} \leqslant \frac{1}{2n(2n-1)}.$$

Следовательно, $\lim\limits_{n\to\infty} A_{2n} = \lim\limits_{n\to\infty} A_{2n+1}$, а это означает, что существует предел последовательности $\{A_n\}$. ◄

Число $\alpha_n = [a_n, a_{n+1}, a_{n+2}, \dots]$ называется n-м остатком разложения числа α в непрерывную дробь.

6. Справедливы следующие соотношения

$$\alpha = \alpha_0, \quad \alpha = \frac{\alpha_1 a_0 + 1}{\alpha_1}, \quad \alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}, n \geqslant 2.$$

Для рационального числа $\alpha = [a_0, a_1, \dots, a_N]$ эти равенства справедливы от $n = 0$ до N.

► Проведем индукцию по параметру n. При $n = 1$ по определению имеем

$$\alpha = a_0 + \frac{1}{\alpha_1} = \frac{\alpha_1 a_0 + 1}{\alpha_1}.$$

Пусть утверждение верно при $n = m$, т.е.

$$\alpha = \frac{\alpha_m p_{m-1} + p_{m-2}}{\alpha_m q_{m-1} + q_{m-2}}.$$

Докажем его при $n = m + 1$. Для этого воспользуемся равенством $\alpha_m = a_m + \frac{1}{\alpha_{m+1}}$, предположением индукции и утверждением задачи 2. Получим

$$\alpha = \frac{\left(a_m + \frac{1}{\alpha_{m+1}}\right) p_{m-1} + p_{m-2}}{\left(a_m + \frac{1}{\alpha_{m+1}}\right) q_{m-1} + q_{m-2}} = \frac{\alpha_{m+1}(a_m p_{m-1} + p_{m-2}) + p_{m-1}}{\alpha_{m+1}(a_m q_{m-1} + q_{m-2}) + q_{m-1}} =$$

$$= \frac{\alpha_{m+1} p_m + p_{m-1}}{\alpha_{m+1} q_m + q_{m-1}}. \blacktriangleleft$$

7. Любое иррациональное число однозначным образом разлагается в непрерывную дробь.

► Предположим, что имеется два различных разложения числа α в непрерывную дробь $\alpha = [a_0, a_1, a_2, \dots] = [b_0, b_1, b_2, \dots]$. Очевидно, что $a_0 = [\alpha] = b_0$. Далее, найдется такой номер n, что при $0 \leqslant k < n$ справедливы равенства $a_k = b_k$ и $a_n \neq b_n$. Из разложений $\alpha = [a_0, a_1, \dots, a_{n-1}, \alpha_n] = [a_0, a_1, \dots, a_{n-1}, \beta_n]$ по утверждению предыдущей задачи получим

$$\alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}} = \frac{\beta_n p_{n-1} + p_{n-2}}{\beta_n q_{n-1} + q_{n-2}}.$$

Отсюда следует, что

$$(\alpha_n - \beta_n)(p_{n-1}q_{n-2} - p_{n-2}q_{n-1}) = 0.$$

Из утверждения задачи 3 выводим, что $\alpha_n = \beta_n$. Следовательно, $a_n = [\alpha_n] = [\beta_n] = b_n$, что противоречит сделанному выше предположению. ◄

Заметим, что для рационального числа $\alpha = [a_0, a_1, \dots, a_N]$ при $a_N > 1$ имеется еще одно разложение в непрерывную дробь $\alpha = [a_0, a_1, \dots, a_{N-1}, a_N - 1, 1]$. Если же $a_N = 1$, то $[a_0, \dots, a_{N-1}, a_N] = [a_0, \dots, a_{N-1} + 1]$. Следовательно, для рационального числа существуют два разложения в непрерывную дробь: длина дроби N в одном случае четное число, а в другом — нечетное. В случае же иррационального числа α при любом $n \geqslant 1$ имеем $\alpha_n > 1, a_n = [\alpha_n]$.

8. Для любого иррационального числа α при $n \geqslant 1$ справедливо равенство

$$q_n\alpha - p_n = \frac{(-1)^n \delta_n}{q_{n+1}}, \quad 0 < \delta_n < 1,$$

причем последовательность δ_n/q_{n+1} — убывающая.

Если же α — рациональное число, то при $1 \leqslant n \leqslant N - 2$, где N — длина непрерывной дроби, имеет место то же утверждение, и $\delta_{N-1} = 1$.

► Используя утверждение задачи 6, имеем цепочку равенств

$$\alpha - \frac{p_n}{q_n} = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \\ = -\frac{p_n q_{n-1} - p_{n-1}q_n}{q_n(\alpha_{n+1}q_n + q_{n-1})} = \frac{(-1)^n}{q_n(\alpha_{n+1}q_n + q_{n-1})}.$$

Следовательно,

$$\delta_n = \frac{q_{n+1}}{\alpha_{n+1}q_n + q_{n-1}} = \frac{a_{n+1}q_n + q_{n-1}}{\alpha_{n+1}q_n + q_{n-1}}.$$

Поскольку $a_n < \alpha_n < a_n + 1$ при иррациональном α и при $1 \leqslant n \leqslant N-2$ при рациональном α, получим неравенство $0 < \delta_n < 1$. Далее докажем, что последовательность δ_n/q_{n+1} убывает. Имеем цепочку соотношений

$$\frac{\delta_n}{q_{n+1}} = \frac{1}{\alpha_{n+1}q_n + q_{n-1}} \geqslant \frac{1}{(a_{n+1}+1)q_n + q_{n-1}} =$$

$$= \frac{1}{q_{n+1} + q_n} \geqslant \frac{1}{a_{n+2}q_{n+1} + q_n} = \frac{1}{q_{n+2}} > \frac{\delta_{n+1}}{q_{n+2}}. \blacktriangleleft$$

9. Пусть α — иррациональное число. Тогда предел при $n \to \infty$ подходящих дробей p_n/q_n равен α.

► Настоящее утверждение прямо следует из утверждения предыдущей задачи. ◄

10. Пусть α — вещественное число. Тогда для подходящих дробей p_n/q_n справедливо неравенство

$$\left|\alpha - \frac{p_n}{q_n}\right| \leqslant \frac{1}{q_n q_{n+1}}.$$

Если $\alpha = p_{n+1}/q_{n+1}$, то неравенство обращается в равенство.

► Утверждение непосредственно следует из утверждений задач 9 и 3. ◄

11. Известно следующее разложение числа π в непрерывную дробь

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 21, 31, 14, 2, 1, 2, 2, 2, 2, 84, 2,$$
$$1, 1, 15, 3, 13, 1, 4, 2, 6, 6, 1, \dots].$$

Тогда имеем следующую таблицу

n		0	1	2	3	4	5	6	7
a_n		3	7	15	1	292	1	1	1
p_n	1	3	22	333	355	103993	104348	208341	312689
q_n	0	1	7	106	113	33102	33215	66317	99532

Кроме того, справедливо неравенство

$$\left|\pi - \frac{312689}{99532}\right| < \frac{1}{99532 \cdot 2156489} < \frac{1}{2 \cdot 10^{11}}.$$

► Таблица составлена применением формулы задачи 2. Неравенство следует из утверждения задачи 10. ◄

Рациональное число $a/b, (a,b)=1, b \geqslant 1$ называется наилучшим приближением к числу α, если для любой дроби $c/d, (c,d)=1$ с условиями $\frac{c}{d} \neq \frac{a}{b}, 1 \leqslant d \leqslant b$ выполняется неравенство

$$|d\alpha - c| > |b\alpha - a|.$$

12. Всякое наилучшее рациональное приближение к вещественному числу есть его подходящая дробь.

▶ Пусть дробь a/b — будет наилучшее рациональное приближение к числу $\alpha = [a_0, a_1, a_2, \dots]$, и пусть a/b не совпадает ни с одной подходящей дробью $p_n/q_n, n \geqslant 0$, числа α.

Возможны следующие случаи расположения числа a/b :

$$1)\frac{a}{b} < \frac{p_0}{q_0} = a_0, \quad 2)\frac{p_0}{q_0} \leqslant \frac{a}{b} \leqslant \frac{p_1}{q_1}, \quad 3)\frac{a}{b} > \frac{p_1}{q_1}.$$

В случае 1) имеем $a/b < a_0 = [\alpha] \leqslant \alpha$. Следовательно, поскольку $b \geqslant 1$, справедливы неравенства

$$0 \leqslant \alpha - a_0 < \alpha - \frac{a}{b} \leqslant b\alpha - a.$$

Таким образом число a/b не является наилучшим приближением к числу α, что противоречит предположению и поэтому случай 1) невозможен.

Рассмотрим случай 2). Имеем, что дробь a/b не совпадает ни с одной из подходящих дробей и заключена между подходящими дробями p_{k-1}/q_{k-1} и p_{k+1}/q_{k+1} с номерами одинаковой четности.

При $p_{k-1}/q_{k-1} < p_{k+1}/q_{k+1}$ справедливы неравенства

$$\left|\frac{a}{b} - \frac{p_{k-1}}{q_{k-1}}\right| = \frac{|aq_{k-1} - bp_{k-1}|}{bq_{k-1}} \geqslant \frac{1}{bq_{k-1}},$$

$$\left|\frac{a}{b} - \frac{p_{k-1}}{q_{k-1}}\right| < \left|\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}}\right| = \frac{1}{q_k q_{k-1}}.$$

Отсюда следует, что $b > q_k$.

Далее, имеем

$$\left|\alpha - \frac{a}{b}\right| \geqslant \left|\frac{p_{k+1}}{q_{k+1}} - \frac{a}{b}\right| \geqslant \frac{1}{bq_{k+1}},$$

т.е. $|b\alpha - a| \geqslant 1/q_{k+1}$.

С другой стороны, по утверждению задачи 8 находим $|q_k\alpha - p_k| < 1/q_{k+1}$.

Следовательно, получим $|q_k\alpha - p_k| < |b\alpha - a|$. Это противоречит тому, что дробь a/b является наилучшим приближением числа α.

Если же $p_{k-1}/q_{k-1} > p_{k+1}/q_{k+1}$, то вместо дроби p_{k-1}/q_{k-1} следует взять дробь p_{k+1}/q_{k+1} и провести те же рассуждения. Получим, что $b > q_k$, и рассуждения, подобные предыдущим, приводят к противоречию. Тем самым случай 2) невозможен.

Рассмотрим, теперь, случай 3). Имеем $\frac{a}{b} > \frac{p_1}{q_1} \geqslant \alpha$. Следовательно, получим

$$\left|\alpha - \frac{p_1}{q_1}\right| > \left|\frac{p_1}{q_1} - \frac{a}{b}\right| \geqslant \frac{1}{bq_1},$$

т.е. $|b\alpha - a| > 1/q_1 = 1/a_1$.

Из определения непрерывной дроби находим $|\alpha - a_0| \leqslant 1/a_1$. Следовательно, $|b\alpha - a| > |\alpha - a_0|$. Это вновь противоречит тому, что дробь a/b является наилучшим приближением числа α.

Таким образом, ни один из рассматриваемых случаев невозможен, что и доказывает утверждение задачи. ◀

13. Всякая подходящая дробь с номером $n \geqslant 1$ вещественного числа является его наилучшим приближением, за исключением числа $\alpha = a + \frac{1}{2}$, где a — любое целое число.

► Проведем индукцию по номеру подходящей дроби. При $\alpha = a + \frac{1}{2}$ и целом a имеем $\frac{p_0}{q_0} = a$, $\frac{p_1}{q_1} = a + \frac{1}{2} = \alpha$. Следовательно,

$$\left|\alpha - \frac{p_0}{q_0}\right| = |\alpha - (a+1)|,$$

т.е. число $a + 1$, не являющееся подходящей дробью, будет также наилучшим приближением α. Тем не менее, подходящая дробь $p_1/q_1 = \alpha$ будет наилучшим рациональным приближением числа α при $n = 1$.

При $\alpha < [\alpha] + \frac{1}{2}$ любое целое число, отличное от $p_0/q_0 = [\alpha]$, отстоит от него на расстояние, большее, чем $1/2$, т.е. не будет наилучшим приближением. Следовательно, дробь p_0/q_0 будет наилучшим приближением при $n = 0$.

При $\alpha > [\alpha] + \frac{1}{2}$ имеем $\frac{p_1}{q_1} = [\alpha] + 1, q_1 = 1$, и подходящая дробь с номером $n = 1$ числа α является наилучшим рациональным приближением.

Предположим, что утверждение верно при $n = m - 1$, где $m \geqslant 1$ при $\alpha < [\alpha] + \frac{1}{2}$ и $m \geqslant 2$ при $\alpha \geqslant [\alpha] + \frac{1}{2}$. Докажем утверждение при

$n = m$. Для любого $q \leqslant q_{m-1}$ и любого целого числа pпо предположению индукции имеем $|q_{m-1}\alpha - p_{m-1}| < |q\alpha - p|$. Далее покажем, что $|q_m\alpha - p_m| < |q_{m-1}\alpha - p_{m-1}|$, поэтому достаточно рассмотреть случай, когда $q_{m-1} < q \leqslant q_m$.

Пусть сначала $q = q_m$. Рассмотрим случай $q_{m+1} = 2$. Тогда по утверждению задачи 3 имеем $m = 1$ и $q_2 = a_1a_2 + 1 = 2$. Следовательно, $a_1 = a_2 = 1$, $\frac{p_1}{q_1} = a_0 + 1$, $\frac{p_2}{q_2} = a_0 + \frac{1}{2}$, и для величины α справедливо неравенство $a_0 + \frac{1}{2} < \alpha < a_0 + 1$. Таким образом, при $1 \leqslant q \leqslant q_1 = 1$ получим при любом целом числе z $\left|\alpha - \frac{p_1}{q_1}\right| < \frac{1}{2} < |\alpha - z|$, т.е. подходящая дробь p_1/q_1 является наилучшим приближением к числу α.

Пусть, теперь, $q_{m+1} > 2$. Тогда для любого $p \neq p_m$ и $q = q_m$ имеем неравенство $\left|\frac{p_m}{q_m} - \frac{p}{q}\right| \geqslant \frac{1}{q_m}$. Кроме того, из утверждения задачи 10 получим

$$\left|\alpha - \frac{p_m}{q_m}\right| \leqslant \frac{1}{q_m q_{m+1}} < \frac{1}{2q_m}.$$

Следовательно,

$$\left|\alpha - \frac{p}{q}\right| \geqslant \left|\frac{p}{q} - \frac{p_m}{q_m}\right| - \left|\frac{p_m}{q_m} - \alpha\right| \geqslant \frac{1}{q_m} - \left|\alpha - \frac{p_m}{q_m}\right| > \left|\alpha - \frac{p_m}{q_m}\right|,$$

т.е. дробь p_m/q_m может являться наилучшим приближением числа α.

Рассмотрим оставшийся случай $q_{m-1} < q < q_m$. Представим p и q в виде следующей линейной комбинации векторов (p_{m-1}, q_{m-1}) и (p_m, q_m) с неизвестными коэффициентами u и v. Имеем

$$\begin{cases} up_m + vp_{m-1} = p, \\ uq_m + vq_{m-1} = q. \end{cases}$$

Решая эту систему уравнений и используя утверждение задачи 3, находим $u = (-1)^{m-1}(pq_{m-1} - qp_{m-1}) \neq 0, v = (-1)^{m-1}(pq_m - qp_m) \neq 0$. Поскольку $q_m > q = uq_m + vq_{m-1}$, целые числа u и v имеют противоположные знаки. Далее по утверждению задачи 8 выражения $q_m\alpha - p_m$ и $q_{m-1}\alpha - p_{m-1}$ имеют разные знаки, следовательно, выражения $u(q_m\alpha - p_m)$ и $v(q_{m-1}\alpha - p_{m-1})$ имеют одинаковый знак. Таким образом, находим

$$q\alpha - p = u(q_m\alpha - p_m) + v(q_{m-1}\alpha - p_{m-1}).$$

Отсюда и из утверждения задачи 8 получим

$$|q\alpha - p| > |q_{m-1}\alpha - p_{m-1}| > |q_m\alpha - p_m|. \blacktriangleleft$$

Пусть заданы вещественное число α и рациональное число $p/q, (p,q) = 1, q \geqslant 1$ с условием $0 < \alpha - \frac{p}{q} = \frac{\theta}{q^2}$. Разложим число p/q в непрерывную дробь при $\theta > 0$ с нечетным числом неполных частных и при $\theta < 0$ с четным числом неполных частных. Пусть p'/q' обозначает предпоследнюю подходящую дробь в этой непрерывной дроби.

14.(Лежандр). Для того чтобы число p/q было подходящей дробью числа α, необходимо и достаточно, чтобы выполнялось неравенство $|\theta| \leqslant \frac{q}{q+q'}$.

► *Необходимость.* Пусть $\alpha = [a_0, a_1, a_2, \dots]$ — разложение числа α в непрерывную дробь и $\frac{p}{q} = \frac{p_k}{q_k}$ есть k-я подходящая дробь этого числа. Тогда имеем $\frac{p'}{q'} = \frac{p_{k-1}}{q_{k-1}}$. Следовательно, из утверждения задачи 6 получим

$$\alpha - \frac{p}{q} = \frac{p\alpha_k + p'}{q\alpha_k + q'} - \frac{p}{q} = \frac{p'q - pq'}{q(q\alpha_k + q')} = \frac{(-1)^k}{q(q\alpha_k + q')} = \frac{\theta}{q^2}.$$

Поскольку $\alpha_k \geqslant 1$, отсюда находим неравенство

$$|\theta| = \frac{q}{q\alpha_k + q'} \leqslant \frac{q}{q + q'}.$$

Достаточность. По условию имеем $|\theta| \leqslant qq + q'$. Рассмотрим указанное выше разложение числа $\frac{p}{q} = [a_0, a_1, \dots, a_k]$ в непрерывную дробь, $\frac{p'}{q'} = [a_0, a_1, \dots, a_{k-1}]$ — предпоследняя дробь в этом разложении. Тогда получим $pq' - p'q = (-1)^{k-1}$.

Пусть число α_k определяется из уравнения $\alpha = \frac{p\alpha_k + p'}{q\alpha_k + q'}$. Тогда находим

$$\alpha - \frac{p}{q} = \frac{p\alpha_k + p'}{q\alpha_k + q'} - \frac{p}{q} = \frac{p'q - pq'}{q(q\alpha_k + q')} = \frac{(-1)^k}{q(q\alpha_k + q')} = \frac{\theta}{q^2}.$$

Отсюда и из условия задачи имеем

$$|\theta| = \frac{q}{q\alpha_k + q'} \leqslant \frac{q}{q + q'}.$$

Следовательно, $\alpha_k \geqslant 1$. Поскольку имеем равенство $\alpha = [a_0, a_1, \dots, a_k, \alpha_k]$, где $\alpha_k \geqslant 1$, находим, что α_k — полное частное

числа α, а p/q — подходящая дробь в разложении числа α в непрерывную дробь. ◀

15. Пусть справедливы неравенства $0 < \left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{2q^2}$. Тогда рациональное число p/q является подходящей дробью числа α.

▶ Неравенство $|\theta| \leqslant \frac{q}{q+q'}$ предыдущей задачи будет выполнено, если $|\theta| \leqslant \frac{1}{2}$, поскольку $q' \leqslant q$. Это означает, что выполнено неравенство $\alpha - \frac{p}{q} \leqslant \frac{1}{2q^2}$. Итак, по утверждению предыдущей задачи число p/q будет подходящей дробью числа α. ◀

16. При $k \geqslant 1$ по крайней мере для одной из двух последовательных подходящих дробей $\frac{p}{q} = \frac{p_k}{q_k}$ и $\frac{p_{k+1}}{q_{k+1}}$ числа α выполняется следующее неравенство $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$.

▶ Предположим противное, т.е. выполняются неравенства

$$\left|\alpha - \frac{p_k}{q_k}\right| \geqslant \frac{1}{2q_k^2}, \quad \left|\alpha - \frac{p_{k+1}}{q_{k+1}}\right| \geqslant \frac{1}{2q_{k+1}^2}.$$

Подходящие дроби p_k/q_k и p_{k+1}/q_{k+1} числа α на числовой оси лежат по разные стороны от этого числа α. Имеем цепочку соотношений

$$\frac{1}{q_k q_{k+1}} = \left|\frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k}\right| = \left|\frac{p_{k+1}}{q_{k+1}} - \alpha\right| + \left|\alpha - \frac{p_k}{q_k}\right| \geqslant \frac{1}{2q_k^2} + \frac{1}{2q_{k+1}^2}.$$

Отсюда следует, что $(q_{k+1} - q_k)^2 \leqslant 0$, т.е. $q_{k+1} = q_k$. Это равенство невозможно при $k \geqslant 1$. ◀

17. При $k \geqslant 1$ по крайней мере для одной из трех последовательных подходящих дробей $\frac{p}{q} = \frac{p_k}{q_k}$, $\frac{p_{k+1}}{q_{k+1}}$ и $\frac{p_{k+2}}{q_{k+2}}$ числа α выполняется следующее неравенство $\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}$.

▶ Предположим противное, т.е. при $n = k, k+1, k+2$ выполняются неравенства

$$\left|\alpha - \frac{p_n}{q_n}\right| \geqslant \frac{1}{\sqrt{5}q_n^2}.$$

Используя утверждение задачи 6, при $n = k, k+1, k+2$ имеем цепочку равенств

$$\left|\alpha - \frac{p_n}{q_n}\right| = \left|\frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_n(\alpha_{n+1}q_n + q_{n-1})} =$$

$$= \frac{1}{q_n^2(\alpha_{n+1} + \beta_{n+1})},$$

где $\beta_{n+1} = q_{n-1}/q_n$.

Отсюда при $m = k-1, k, k+1$ находим $\alpha_m + \beta_m \leqslant \sqrt{5}$. Далее воспользуемся равенствами

$$\alpha_m = a_m + \frac{1}{\alpha_{m+1}}, \quad \frac{1}{\beta_m} = \frac{q_{m-1}}{q_{m-2}} =$$

$$= \frac{a_{m-1}q_{m-2} + q_{m-3}}{q_{m-2}} = a_{m-1} + \beta_{m-1}.$$

При $m = k, k+1$ получим

$$\frac{1}{\alpha_m} + \frac{1}{\beta_m} = \alpha_{m-1} + \beta_{m-1} \leqslant \sqrt{5}.$$

Следовательно,

$$1 = \frac{1}{\alpha_m}\alpha_m \leqslant \left(\sqrt{5} - \frac{1}{\beta_m}\right)(\sqrt{5} - \beta_m),$$

т.е. $\beta_m + 1/\beta_m \leqslant \sqrt{5}$. Так как β_m рациональное число, то в предыдущем неравенстве выполняется строгое неравенство. Воспользовавшись также тем, что $\beta_m < 1$, имеем $\beta_m > \frac{1}{2}(\sqrt{5}-1)$.

Далее имеем

$$a_k = \frac{1}{\beta_{k+1}} - \beta_k < \sqrt{5} - \beta_{k+1} - \beta_k < \sqrt{5} - 2\frac{\sqrt{5}-1}{2} = 1.$$

Это противоречит тому, что $a_k \geqslant 1$. ◄

18. Для любого иррационального числа α существует бесконечная последовательность p/q подходящих дробей числа α, удовлетворяющих неравенству

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

► Это утверждение прямое следствие предыдущей задачи. ◄

19. Для числа $\alpha = \frac{\sqrt{5}+1}{2}$ при $A > \sqrt{5}$ неравенство

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Aq^2}$$

имеет только конечное число решений.

Другими словами, константа $A = \sqrt{5}$ в предыдущей задаче является наилучшей возможной.

► Пусть справедливы соотношения

$$\alpha = \frac{p}{q} + \frac{\delta}{q^2}, |\delta| < \frac{1}{A} < \frac{1}{\sqrt{5}}.$$

Тогда имеем

$$\frac{\delta}{q} - \frac{q}{2}\sqrt{5} = \frac{q}{2} - p.$$

Возводим это равенство в квадрат. Находим

$$\frac{\delta^2}{q^2} - \delta\sqrt{5} = \left(\frac{q}{2} - p\right)^2 - \frac{5q^2}{4} = p^2 - pq - q^2.$$

При достаточно большом q получим

$$\left|\frac{\delta^2}{q^2} - \delta\sqrt{5}\right| < 1.$$

Следовательно, $p^2 - pq - q^2 = 0$, т.е. $(2p-q)^2 = 5q^2$, что невозможно. ◄

Имеется гипотеза о том, что для всякого алгебраического числа его неполные частные ограничены. В силу периодичности непрерывной дроби для квадратичной иррациональности эта гипотеза справедлива для таких чисел. С другой стороны, Г.Давенпорт [?] доказал, что для любого сколь угодно большого числа M найдется иррациональное алгебраическое число, отличное от квадратичной иррациональности, такое, что бесконечная последовательность его неполных частных превосходит M. Более точно его результат формулируется следующим образом.

20. Пусть θ — любое иррациональное число, $P > 2$ — любое большое простое число. Тогда, по крайней мере, одно из чисел

$$P^2\theta, \theta, \theta + \frac{1}{P}, \ldots, \theta + \frac{P-1}{P},$$

имеет для бесконечного множества номеров n неполные частные a_n, превосходящие $P - 2$.

► По утверждению задачи 8 для иррационального числа $P\theta$ имеем

$$P\theta - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n((P\theta)_{n+1}q_n + q_{n-1})},$$

где символ $(P\theta)_{n+1}$ обозначает $(n+1)$-й остаток (полное частное) при разложении числа $P\theta$ в непрерывную дробь.

Следовательно,

$$\left| P\theta - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}.$$

Если q_n делится на P для бесконечного множества номеров n, то $q_n = Pq_n^{'}$. Тогда для бесконечного множества рациональных приближений $\frac{p_n}{q_n^{'}}$ к числу $P^2\theta$ справедливо неравенство

$$\left| P^2\theta - \frac{p_n}{q_n^{'}} \right| < \frac{1}{P(q_n^{'})^2}.$$

Поскольку $P > 2$, по утверждению задачи 15 имеем, что $p_n/q_n^{'}$ является подходящей дробью иррационального числа $P^2\theta$. Далее, из утверждения задачи 8 для иррационального числа $P^2\theta$ находим

$$P^2\theta - \frac{p_n}{q_n^{'}} = \frac{(-1)^n}{q_n^{'}(\alpha_{n+1}q_n^{'} + q_{n-1}^{'})},$$

где символ α_{n+1} обозначает остаток (полное частное) при разложении числа $P^2\theta$ в непрерывную дробь, отвечающий подходящей дроби $p_n/q_n^{'}$.

Таким образом получим неравенство

$$\frac{1}{q_n^{'}(\alpha_{n+1}q_n^{'} + q_{n-1}^{'})} < \frac{1}{P(q_n^{'})^2}.$$

Воспользуемся тем, что $1 \leqslant a_{n+1} \leqslant \alpha_{n+1} < a_{n+1} + 1$. Тогда из предыдущего неравенства имеем

$$Pq_n^{'} < \alpha_{n+1}q_n^{'} + q_{n-1}^{'} < (a_{n+1}+2)q_n^{'}.$$

Следовательно, $(n+1)$-е неполное частное a_{n+1} числа $P^2\theta$ превосходит $P-2$.

Пусть, теперь, для всех достаточно больших номеров n знаменатели q_n подходящих дробей p_n/q_n числа $P\theta$ взаимно просты с P. Определим целые числа A_n из сравнения $p_n \equiv A_n q_n \pmod P, 0 \leqslant A_n < P$. По крайней мере одно из чисел $0, 1, \ldots, P-1$ бесконечно часто встречается как A_n. Обозначим это число буквой A. Тогда для указанных номеров n при некотором целом числе r_n имеем $p_n = Aq_n + Pr_n$.

Таким образом получим

$$\left|\theta - \frac{A}{P} - \frac{r_n}{q_n}\right| < \frac{1}{Pq_n^2}.$$

Отсюда имеем, что r_n/q_n является подходящей дробью числа $\theta - \frac{A}{P}$, и бесконечное множество неполных частных этого числа превосходит $P-2$. ◀

§ 10. Арифметика квадратичных полей. Метод Лемера распознавания простых чисел

Целые числа из кольца $\mathbf{Z}$ будем называть целыми рациональными числами. Пусть $\mathbf{Q}$ — поле рациональных чисел. Рассмотрим D — бесквадратное целое рациональное число. Множество всех чисел α вида $\alpha = r + s\sqrt{D}$ с рациональными числами r и s образует поле $\mathbf{Q}(\sqrt{D})$ — квадратичное расширение поля рациональных чисел.

Числа α из $\mathbf{Q}(\sqrt{D})$, удовлетворяющие уравнению

$$z^2 + pz + q = 0$$

с целыми рациональными коэффициентами p и q, называются целыми в поле $\mathbf{Q}(\sqrt{D})$. Положим

$$\rho = \begin{cases} \sqrt{D}, & \text{если} \quad D \equiv 2 \quad \text{или} \equiv 3 \pmod 4, \\ (1+\sqrt{D})/2, & \text{если} \quad D \equiv 1 \pmod 4. \end{cases}$$

1. Любое целое число α из $\mathbf{Q}(\sqrt{D})$ имеет вид $\alpha = r + s\rho$, где r и s — целые рациональные числа.

▶ По теореме Виета число $\alpha = r + s\sqrt{D}$ будет целым числом из $\mathbf{Q}(\sqrt{D})$, тогда и только тогда, когда $\alpha + \bar{\alpha} = 2r = m$ и $\alpha\bar{\alpha} = r^2 - Ds^2$ являются целыми рациональными числами. Поскольку $\frac{m^2}{4} - Ds^2$ — целое рациональное число и число D свободно от квадратов, рациональное число s в представлении в виде несократимой дроби в знаменателе может иметь только 2, т.е. $s = n/2, n \in \mathbf{Z}$ и число $(m^2 - Dn^2)/4$ является целым рациональным.

Так как число D свободно от квадратов, то $D \not\equiv 0 \pmod 4$. Возможны два случая: 1) $D \equiv 1 \pmod 4$ и 2) $D \equiv 2$ или $\equiv 3 \pmod 4$.

Сначала рассмотрим случай 1) $D \equiv 1 \pmod 4$. Имеем $m^2 \equiv n^2 \pmod 4$. Это эквивалентно $m \equiv n \pmod 2$. Следовательно, $m = n + 2k$. Отсюда при целых рациональных k и n получим

$$\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{D} = k + n\frac{1+\sqrt{D}}{2} = k + n\rho.$$

Это означает, что в случае $D \equiv 1 \pmod 4$ в качестве базиса в кольце целых поля $\mathbf{Q}(\sqrt{D})$ можно взять числа 1 и $\rho = \frac{1+\sqrt{D}}{2}$.

Рассмотрим случай 2) $D \equiv 2$ или $\equiv 3 \pmod 4$. Поскольку выполняется сравнение $m^2 - Dn^2 \equiv 0 \pmod 4$, число n не может быть нечетным. Действительно, тогда имели бы $D \equiv m^2 \pmod 4$, т.е. либо $D \equiv 0 \pmod 4$ при четном m, либо $D \equiv 1 \pmod 4$ при нечетном m, что не так. Пусть теперь n — четное число. Тогда $m^2 \equiv 0 \pmod 4$. Следовательно, m — четное число. Таким образом, в случае 2) $D \equiv 2$ или $\equiv 3 \pmod 4$ в качестве базиса кольца целых поля $\mathbf{Q}(\sqrt{D})$ можно взять числа 1 и $\rho = \sqrt{D}$. ◀

Число $\alpha + \bar{\alpha} = \mathrm{Sp}(\alpha)$ называется следом числа α, а число $\alpha\bar{\alpha} = N(\alpha)$ — нормой этого числа.

Пусть $\alpha = r + s\rho \in \mathbf{Q}(\sqrt{D})$. Тогда

$$N(\alpha) = \begin{cases} r^2 - Ds^2, & \text{если} \quad D \equiv 2 \quad \text{или} \quad \equiv 3 \pmod 4, \\ r^2 + rs + \frac{1-D}{4}s^2, & \text{если} \quad D \equiv 1 \pmod 4. \end{cases}$$

Как функция от α след $\mathrm{Sp}(\alpha)$ является линейной функцией, т.е.
1) для любых $\alpha_1, \alpha_2 \in \mathbf{Q}(\sqrt{D})$ имеем $\mathrm{Sp}(\alpha_1 + \alpha_2) = \mathrm{Sp}(\alpha_1) + \mathrm{Sp}(\alpha_2)$,
2) для любого $c \in \mathbf{Q}$ имеем $\mathrm{Sp}(c\alpha) = c\,\mathrm{Sp}(\alpha)$,
а функция норма $N(\alpha)$ числа α является мультипликативной
1) для любых $\alpha_1, \alpha_2 \in \mathbf{Q}(\sqrt{D})$ имеем $N(\alpha_1\alpha_2) = N(\alpha_1)N(\alpha_2)$,
2) $N(\alpha) = 0$ тогда и только тогда, когда $\alpha = 0$.

Целое число ε поля $\mathbf{F} = \mathbf{Q}(\sqrt{D})$ называется единицей, если ε делит число 1.

2. Целое число ε из $\mathbf{F}$ будет единицей тогда и только тогда, когда $N(\varepsilon) = \pm 1$.

▶ *Необходимость.* Пусть $\varepsilon \in \mathbf{F}$ — целое число и $\varepsilon \mid 1$. Тогда найдется целое число η такое, что $\varepsilon\eta = 1$. Следовательно, $N(\varepsilon\eta) = N(\varepsilon)N(\eta) = 1$. Отсюда находим, что $N(\varepsilon) = \pm 1$.

Достаточность. Так как ε — целое число поля $\mathbf{F}$, то число ε удовлетворяет уравнению с целыми рациональными коэффициентами

$$\varepsilon^2 - \mathrm{Sp}(\varepsilon)\varepsilon + N(\varepsilon) = 0.$$

Отсюда имеем, что

$$\bar{\varepsilon} = \frac{N(\varepsilon)}{\varepsilon} = -\varepsilon + \mathrm{Sp}(\varepsilon) \in \mathbf{F}$$

является целым числом в $\mathbf{F}$. Далее, поскольку $N(\varepsilon) = \varepsilon\bar{\varepsilon} = \pm 1$, число ε будет делителем единицы. ◄

3. Пусть $\mathbf{F} = \mathbf{Q}(\sqrt{D})$ — мнимое квадратичное поле ($D < 0$). Тогда множество всех единиц этого поля является конечной циклической группой порядка w, причем

$$w = \begin{cases} 6, & \text{если} \quad D = -3 \\ 4, & \text{если} \quad D = -1, \\ 2 & \text{в остальных случаях.} \end{cases}$$

► По утверждению задачи 3 целое число ε является единицей тогда и только тогда, когда $N(\varepsilon) = \pm 1$. Целое число ε можно представить в виде $\varepsilon = r + s\rho$, где r и s — целые рациональные числа.

Пусть $D \equiv 2$ или $\equiv 3 \pmod 4$. Тогда $\rho = \sqrt{D}$ и

$$0 < N(s + r\rho) = r^2 - Ds^2 = 1.$$

Рассмотрим сначала случай $D = -1$. Уравнение $r^2 + s^2 = 1$ имеет четыре решения $(r, s) = (\pm 1, 0), (0, \pm 1)$, которым отвечают единицы $\pm 1, \pm i$ и число i является образующей группы четвертого порядка.

Пусть $|D| > 1$. Тогда $s = 0$, поскольку в противном случае $1 = r^2 - Ds^2 \geqslant |D| > 1$. Следовательно, в этом случае имеется только две единицы ± 1.

Пусть, теперь, $D \equiv 1 \pmod 4$. Тогда $\rho = \frac{1+\sqrt{D}}{2}$ и $N(r + s\rho) = r^2 + rs + s^2\frac{1-D}{4}$.

Рассмотрим сначала случай $D = -3$. Тогда уравнение $0 < N(r + s\rho) = r^2 + rs + s^2 = 1$ в целых r и s имеет 6 решений $(r, s) = (\pm 1, 0), (0, \pm 1), (\pm 1, \mp 1)$. Этим решениям отвечают единицы

$$\pm 1, \pm i, \omega = \frac{1 - \sqrt{D}}{2}, -\omega.$$

Число $-\omega = \frac{-1+\sqrt{D}}{2}$ является первообразным корнем 6-й степени из единицы и образующей группы единиц.

Пусть $|D| \geqslant 4$. Тогда $s = 0$, поскольку в противном случае при $|D| > 4$ имеем

$$N(r + s\rho) = r^2 + rs + s^2\frac{1 - D}{4} \geqslant \frac{-D}{4} = \frac{|D|}{4} > 1,$$

и при $D = -4$

$$N(r + s\rho) = r^2 + rs + s^2\frac{5}{4} \geqslant \frac{5}{4} > 1.$$

Следовательно, уравнение $N(r + s\rho) = \pm 1$ имеем два решения $(r, s) = (\pm 1, 0)$. Им отвечают единицы ± 1. ◀

4. Пусть $\mathbf{F} = \mathbf{Q}(\sqrt{D})$ — вещественное квадратичное поле ($D > 0$). Тогда существует нетривиальная единица этого поля, отличная от ± 1.

▶ Докажем сначала, что для любого натурального числа m существует ненулевое целое число α из поля $\mathbf{F}$ такое, что

$$|\alpha| < 1/m, |N(\alpha)| < 1 + \sqrt{D}.$$

Любое целое число α можно представить в виде $\alpha = x + y\rho$ с целыми рациональными числами x и y. По лемме Дирихле целое число x и натуральное число y, не превосходящее m, такие, что $|\alpha| = |x + y\rho| < 1/m$. Так как $y \neq 0$, то и $\alpha \neq 0$.

Далее оценим сопряженное число к α. Имеем цепочку соотношений

$$\bar{\alpha} = x + y\bar{\rho} = (x + y\rho) + y(\bar{\rho} - \rho) = \alpha + y\sqrt{D}.$$

Следовательно,

$$|\bar{\alpha}| \leqslant |\alpha| + |y|\sqrt{D} \leqslant \frac{1}{m} + m\sqrt{D}.$$

Таким образом, находим

$$|N(\alpha)| = |\alpha\bar{\alpha}| < \frac{1}{m^2} + \sqrt{D} < 1 + \sqrt{D}.$$

Отсюда получим, что существует бесконечно много целых $\alpha \neq 0$ и таких, что $|N(\alpha)| < 1 + \sqrt{D}$. Поэтому найдется натуральное число $m < 1 + \sqrt{D}$ такое, что для бесконечного множества целых $\alpha \neq 0$ выполняется равенство $|N(\alpha)| = m$.

Далее разобьем все числа $\alpha = x + y\rho$ на классы вычетов по модулю m следующим образом: в один класс попадут все числа α с одинаковыми остатками при делении на m чисел x и чисел y, т.е. для любой пары чисел $(r, s), 0 \leqslant r, s < m$, в один класс попадут числа с условием $x \equiv r \pmod m, y \equiv s \pmod m$. Таких классов будет ровно m^2. Для чисел α, β из одного класса имеем $\alpha \equiv \beta \pmod m$.

Отсюда находим, что найдутся два различных ненулевых целых α, β, удовлетворяющие условиям

$$|N(\alpha)| = |N(\beta)| = m, \alpha \equiv \beta \pmod{m}.$$

Домножив последнее сравнение на $\bar{\beta}$, получим

$$\alpha\bar{\beta} \equiv N(\beta) \equiv 0 \pmod{m},$$

т.е. $\alpha\bar{\beta} = m\varepsilon$ при некотором целом ε из bfF.

Разделим последнее равенство на $N(\beta)$. Имеем $\frac{\alpha}{\beta} = \pm\varepsilon$. Поскольку $|N(\alpha)| = |N(\beta)|$, находим $N(\varepsilon) = \pm 1$. По утверждению задачи 3 целое число ε является единицей кольца целых поля $\mathbf{F}$ тогда и только тогда, когда $N(\varepsilon) = \pm 1$.

Таким образом число ε является единицей, причем нетривиальной, поскольку $\alpha \neq \pm\beta$. ◀

Нетривиальные единицы поля $\mathbf{F}$ можно объединить в группы по четыре: $\varepsilon, \bar{\varepsilon}, -\varepsilon, -\bar{\varepsilon}$. Тогда одна из них будет удовлетворять условию $\varepsilon > 1$. Наименьшую среди нетривиальных единиц ε_1 с условием ε_1 назовем основной единицей поля $\mathbf{F}$.

5. Пусть $\mathbf{F} = \mathbf{Q}(\sqrt{D})$ — вещественное квадратичное поле ($D > 0$). Тогда группа единиц кольца целых этого поля $\mathbf{F}$ есть прямое произведение группы второго порядка, состоящей из единиц ± 1 и бесконечной циклической группы.

Другими словами, существует ε_1 — основная единица поля $\mathbf{F}$ такая, что для любой единицы ε кольца целых поля $\mathbf{F}$ найдутся целые числа $\nu = 0, 1$ и n имеет место представление

$$\varepsilon = (-1)^{\nu}\varepsilon_1^n.$$

► Без ограничения общности можно считать, что $\varepsilon > 1$, поскольку в противном случае ее следует заменить на одну из единиц вида $\pm\varepsilon^{\pm 1}$.

Далее, найдется единственное натуральное число n такое, что

$$\varepsilon_1^n \leqslant \varepsilon < \varepsilon_1^{n+1}.$$

Отсюда имеем

$$1 \leqslant \frac{\varepsilon}{\varepsilon_1^n} < \varepsilon_1,$$

что в силу минимальности $\varepsilon_1 > 1$ возможно только, если $\varepsilon = \varepsilon_1^n$. Таким образом найдено искомое представление $\varepsilon = (-1)^{\nu}\varepsilon_1^n$, где $\nu = 0, 1$ и n — любое целое рациональное число. ◀

Отметим, что при $D = 2$ основная единица поля $\mathbf{Q}(\sqrt{2})$ равна $\varepsilon_1 = 1 + \sqrt{2}$ и ее норма $N(\varepsilon_1) = \varepsilon_1\bar{\varepsilon_1}$ равна $N(\varepsilon_1) = 1^2 - 2 \cdot 1^2 = -1$, при $D = 3$ имеем $\varepsilon_1 = 2 + \sqrt{3}, N(\varepsilon_1) = 1$,
при $D = 5$ имеем $\varepsilon_1 = \frac{1+\sqrt{5}}{2}, N(\varepsilon_1) = -1$.

Перейдем к приложению теории квадратичных полей к распознаванию простоты натуральных чисел.

Пусть многочлен $\lambda^2 - P\lambda + Q$ с целыми коэффициентами P, Q неприводим над полем рациональных чисел $\mathbf{Q}$, и пусть a и $b = \bar{a}$ — корни этого многочлена, при этом число b будет сопряженным числу a. Тогда по теореме Виета имеем $a + b = P, ab = Q$.

При $n \geqslant 0$ определим две последовательности

$$U_n = \frac{a^n - b^n}{a - b}, V_n = a^n + b^n.$$

Очевидно, имеем $U_0 = 0, U_1 = 1, V_0 = 2, V_1 = a + b = P$. Последовательности $\{U_n\}, \{V_n\}, n \geqslant 0$, называются последовательностями Люка.

6. При $m \geqslant n \geqslant 0$ справедливы следующие соотношения

$$U_{m+n} = U_m V_n - Q^n U_{m-n}, V_{m+n} = V_m V_n - Q^n V_{m-n};$$

$$U_{m+1} = PU_m - QU_{m-1}, U_0 = 0, U_1 = 1;$$

$$V_{m+1} = PV_m - QV_{m-1}, V_0 = 2, V_1 = P;$$

$$U_{2n} = U_n V_n, \quad U_{2n+1} = U_{n+1}V_n - Q^n;$$

$$V_{2n} = V_n^2 - 2Q^n, \quad V_{2n+1} = V_{n+1}V_n - PQ^n.$$

Пусть, далее, $n = h2^s, (h, 2) = 1, s \geqslant 0$. Тогда

$$U_n = U_h V_h V_{2h} \dots V_{2^{s-1}h},$$

$$V_n = V_{2^s h} = V_{2^{s-1}h}^2 - 2Q^{2^{s-1}h}, \dots, V_{2h} = V_h^2 - 2Q^h.$$

► Искомые тождества проверяются непосредственными вычислениями

$$U_{m+n} = \frac{a^{m+n} - b^{m+n}}{a - b} = \frac{(a^m - b^m)(a^n + b^n)}{a - b} - \\ - \frac{(ab)^n(a^{m-n} - b^{m-n})}{a - b} = U_m V_n - Q^n U_{m-n},$$

$$V_{m+n} = a^{m+n} + b^{m+n} = (a^m + b^m)(a^n + b^n) - \\ - (ab)^n(a^{m-n} + b^{m-n}) = V_m V_n - Q^n V_{m-n}.$$

Положим в этих равенствах $n = 1$. Получим

$$U_{m+1} = (a+b)U_m - abU_{m-1} = PU_m - QU_{m-1},$$

$$V_{m+1} = (a+b)V_m - abV_{m-1} = PV_m - QV_{m-1}.$$

Следовательно, $\{U_n\}, \{V_m\}$ — рекуррентные последовательности второго порядка. Поскольку первые два члена этих последовательностей целые числа, они будут целочисленными последовательностями.

Положим, теперь, $m = n$. Имеем

$$U_{2n} = U_n V_n, V_{2n} = V_n^2 - 2Q^n.$$

Если положим $m = n + 1$, то получим

$$U_{2n+1} = U_{n+1}V_n - Q^n, V_{2n+1} = V_{n+1}V_n - PQ^n.$$

Наконец, применяя последовательно, найденные выше тождества, имеем

$$U_n = U_{2^s h} = U_{2^{s-1}h}V_{2^{s-1}h} = \cdots = U_h V_h V_{2h} \dots V_{2^{s-1}h},$$

$$V_n = V_{2^s h} = V_{2^{s-1}h}^2 - 2Q^{2^{s-1}h}, \dots, V_{2h} = V_h^2 - 2Q^h. \blacktriangleleft$$

7. Пусть p — нечетное простое число, $N = 2^p - 1$, и пусть задана последовательность $s_1 = 4, s_{k+1} = s_k^2 - 2$ при $k \geqslant 1$. Тогда для простоты числа N необходимо и достаточно, чтобы $s_{p-1} \equiv 0 \pmod N$.

► *Необходимость.* Дано, что $N = 2^p - 1$ — простое число. Покажем, что $s_{p-1} \equiv 0 \pmod N$. Сначала докажем, что многочлен $P(x) = x^2 - 2^{(p+1)/2}x - 1$ является неприводимым над полем $\mathbf{F}_N$. Так как квадратичный многочлен $ax^2 + bx + c$ будет неприводимым над $\mathbf{F}_N$ тогда и только тогда, когда его дискриминант $\Delta = b^2 - 4ac$ не будет квадратичным вычетом по модулю N, то имеем

$$\Delta = (2^{(p+1)/2})^2 - 4(-1) \equiv (2^{p+1} - 2) + 2 + 4 \equiv 6 \pmod N.$$

Следовательно,

$$\left(\frac{\Delta}{N}\right) = \left(\frac{2}{N}\right)\left(\frac{3}{N}\right).$$

Находим

$$\left(\frac{2}{N}\right) = +1,$$

поскольку $(2^{(p+1)/2})^2 \equiv 2 \pmod N$.

Из квадратичного закона взаимности символа Лежандра имеем

$$\left(\frac{3}{N}\right) = (-1)^{(N-1)/2}\left(\frac{N}{3}\right) = -\left(\frac{1}{3}\right) = -1,$$

поскольку $N = 2^p - 1 = (3-1)^p - 1 \equiv 1 \pmod 3$.

Таким образом, $\left(\frac{\Delta}{N}\right) = -1$, и многочлен $P(x)$ неприводим над $\mathbf{F}_N$.

Пусть a и b — корни многочлена $P(x)$. Положим $V(2^k) = a^{2^k} + b^{2^k}$. Имеем, что для любого натурального числа k сумма $V(2^k) \in \mathbf{F}_N$. Докажем индукцией по k, что

$$s_k \equiv V(2^k) \pmod N.$$

При $k = 1$ утверждение справедливо, так как

$$V(2) = a^2 + b^2 = (a+b)^2 - 2ab = (2^{(p+1)/2})^2 - 2(-1) \equiv 4 \pmod N.$$

Предположим утверждение верно при $k = m$, т.е. $s_m \equiv V(2^m) \pmod N$. Докажем справедливость утверждения при $k = m+1$. Имеем

$$s_{m+1} = s_m^2 - 2 \equiv (a^{2^m} + b^{2^m})^2 - 2 =$$

$$= a^{2^{m+1}} + b^{2^{m+1}} + 2a^{2^m}b^{2^m} - 2 \equiv V(2^{m+1}) \pmod N.$$

Следовательно, $s_p \equiv V(2^p) \equiv a^{N+1} + b^{N+1} \equiv -2 \pmod N$, так как $a^{N+1} \equiv b^{N+1} \equiv ab \equiv -1 \pmod N$. Поскольку $s_p = s_{p-1}^2 - 2$, получим $s_{p-1} \equiv 0 \pmod N$.

Достаточность. Предположим противное, т.е. N — составное число и q — наименьший простой делитель N. Тогда $3 \leqslant q \leqslant \sqrt{N}$. Так как $s_{p-1} \equiv 0 \pmod N$, то $s_{p-1} \equiv 0 \pmod q$. Тогда из $s_{p-1} \equiv V(2^{p-1}) \pmod q$ имеем цепочку сравнений

$$a^{2^{p-1}} + b^{2^{p-1}} \equiv 0 \pmod q,$$

$$a^{2^p} + (ab)^{2^{p-1}} \equiv \pmod q,$$

$$a^{2^p} \equiv -1 \pmod q.$$

Число a принадлежит полю $\mathbf{F}_{q^2}$, порядок a равен 2^{p+1} и он делит порядок q^2-1 мультипликативной группы поля $\mathbf{F}_{q^2}$, т.е. $2^{p+1} \mid q^2-1$. Последнее невозможно, поскольку $2^{p+1} > n, q^2 \leqslant n$. Это противоречие доказывает, что N — простое число. ◄

8. Пусть $N \geqslant 2$ — натуральное число, $N+1 = \prod\limits_{q \mid N+1} q^{\alpha_q}$ — каноническое разложение числа $N+1$ на простые сомножители, и пусть найдется последовательность Люка U_n с условием $(2QD, N) = 1$, такая, что

$$U_{N+1} \equiv 0 \pmod{N},$$

и для любого $q \mid N+1$ выполняется условие

$$(U_{(N+1)/q}, N) = 1.$$

Тогда число N является простым.

► Будем рассуждать от противного. Пусть N — составное число и p — наименьший простой делитель числа N. Тогда из условия задачи следует, что $U_{N+1} \equiv 0 \pmod{p}$ и для любого простого $q \mid N$ выполняется соотношение $U_{(N+1)/q} \not\equiv 0 \pmod{p}$. Буквой d обозначим наименьшее натуральное число такое, что $U_d \equiv 0 \pmod{p}$. ◄

§ 11. Разложение вещественных квадратичных иррациональностей в непрерывную дробь. Теорема Эйлера – Лагранжа

Пусть θ — иррациональное число из поля $\mathbf{Q}(\sqrt{D})$. Тогда имеем $\theta = r + s\sqrt{D}, r, s \in \mathbf{Q}, s \neq 0$. Число θ удовлетворяет однозначно определенному квадратному уравнению вида $a\theta^2 - b\theta - c = 0$ с целыми рациональными взаимно простыми коэффициентами a, b, c и $a > 0$. Поскольку $\theta \in \mathbf{Q}(\sqrt{D})$, его дискриминант равен $b^2 + 4ac = m^2 D$ для некоторого натурального числа m. Число θ называется принадлежащим дискриминанту $m^2 D$. Оно имеет вид

$$\theta = \frac{b \pm m\sqrt{D}}{2a} = \frac{2c}{-b \pm m\sqrt{D}}.$$

Назовем иррациональное число θ приведенным, если $\theta > 1$ и для сопряженного числа θ' справедливо неравенство $-\frac{1}{\theta'} > 1$, т.е. имеем $\theta > 1, -1 < \theta' < 0$.

Далее имеем

$$\theta' = \frac{-b \mp m\sqrt{D}}{2a} = \frac{2c}{b \mp m\sqrt{D}}.$$

Следовательно, по теореме Виета получим

$$\frac{b}{a} = \theta + \theta' > 0, b > 0; \frac{c}{a} = \theta\theta' = \frac{b^2 - m^2 D}{4a^2} < 0.$$

Отсюда находим $0 < b < m\sqrt{D}$. Поэтому для приведенного числа θ справедливы соотношения

$$\theta = \frac{b + m\sqrt{D}}{2a} = \frac{2c}{-b + m\sqrt{D}} > 1, -1 < \theta' < 0.$$

Тем самым коэффициенты многочлена удовлетворяют неравенствам

$$0 < b < m\sqrt{D}, \frac{-b + m\sqrt{D}}{2} < a, c < \frac{b + m\sqrt{D}}{2}.$$

Это показывает, что a, b, c — натуральные числа с условием $0 < a, b, c < m\sqrt{D}$, т.е. приведенных чисел данного дискриминанта $m^2 D$ существует конечное число.

1. Пусть иррациональное число θ принадлежит дискриминанту $m^2 D$. Тогда этому дискриминанту принадлежат все остатки θ_n разложения числа θ в непрерывную дробь. Более того, начиная с некоторого номера все остатки θ_n будут приведенными числами.

► Для справедливости первого утверждения достаточно доказать, что вместе с числом θ дискриминанту $m^2 D$ принадлежит и число θ_1, определяемое соотношением $\theta = a_1 + \frac{1}{\theta_1}$. Подставим вместо θ его выражение $a_1 + \frac{1}{\theta_1}$ в квадратное уравнение $a\theta^2 - b\theta - c = 0$. Получим относительно новой переменной θ_1 квадратное уравнение

$$(aa_1^2 - ba_1 - c)\theta_1^2 - (b - 2aa_1)\theta_1 + a = 0.$$

Его коэффициенты будут взаимно простыми числами, а дискриминант этого уравнения равен

$$(b - 2aa_1)^2 - 4a(aa_1^2 - ba_1 - c) = b^2 + 4ac = m^2 D.$$

Первое утверждение доказано. Перейдем к доказательству второго утверждения. По определению непрерывной дроби имеем, что $\theta_{n+1} > 1$. Докажем, что, начиная с некоторого номера n, справедливо неравенство $-1/\theta'_{n+1} > 1$.

При $n > 1$, исходя из равенства

$$\theta = \frac{\theta_{n+1} p_n + p_{n-1}}{\theta_{n+1} q_n + q_{n-1}},$$

получим

$$-\frac{1}{\theta'_{n+1}} = \frac{q_n\theta' - p_n}{q_{n-1}\theta' - p_{n-1}} = \frac{q_n}{q_{n-1}} - \frac{(-1)^n}{q_{n-1}\left(q_{n-1}\theta' - p_{n-1}\right)}.$$

Отсюда при $n > 1$ находим

$$-\frac{1}{\theta'_{n+1}} - 1 = \frac{1}{q_{n-1}}\left((q_n - q_{n-1}) - \frac{(-1)^n}{q_{n-1}\left(\theta' - \frac{p_{n-1}}{q_{n-1}}\right)}\right).$$

Далее, при $n \to \infty$ имеем

$$\frac{(-1)^n}{q_{n-1}\left(\theta' - \frac{p_{n-1}}{q_{n-1}}\right)} \to 0,$$

поскольку

$$\lim_{n\to\infty} A_n == \theta' - \theta \neq 0,$$

где $A_n = \left(\theta' - \frac{p_{n-1}}{q_{n-1}}\right)$.

Следовательно, существует номер n_0 такой, что для всех $n > n_0$ выполняется неравенство $|A_n| \leqslant 1/2$. Поэтому для всех $n > n_0$ имеем

$$-\frac{1}{\theta'_{n+1}} - 1 \geqslant \frac{q_n - q_{n-1} - 0,5}{q_{n-1}} > 0.$$

Тем самым доказано, что, начиная с некоторого номера, все остатки θ_n разложения числа θ в непрерывную дробь являются приведенными числами. ◀

2. (Эйлер – Лагранж). Пусть $\theta > 1$ — вещественная квадратичная иррациональность. Тогда, начиная с некоторого номера, разложение в непрерывную дробь числа θ будет периодичным. Более того, если θ является приведенным числом, то это разложение будет чисто периодическим.

▶ Пусть иррациональное число $\theta > 1$ принадлежит дискриминанту m^2D. Тогда по утверждению предыдущей задачи этому дискриминанту принадлежат все остатки θ_n разложения числа θ в непрерывную дробь, причем, начиная с некоторого номера n_0, все они будут приведенными числами. Количество приведенных чисел, принадлежащих данному дискриминанту, конечно. Поэтому найдутся натуральные числа $k \geqslant 1$ и $l \geqslant n_0$ такие, что $\theta_l = \theta_{l+k}$. Тогда имеем

$$\theta = [a_0, a_1, \ldots, a_{l-1}, \theta_l] = [a_0, a_1, \ldots, a_{l-1}, a_l, \ldots, a_{l+k-1}, \theta_{l+k}].$$

Отсюда следует, что разложение числа θ в непрерывную дробь будет иметь период $k \geqslant 1$ с непериодической начальной частью этого разложения длины l.

Докажем теперь вторую часть утверждения. Пусть l является минимальным номером, при котором $\theta_l = \theta_{l+k}$. Предположим, что $l \geqslant 1$, т.е. разложение числа θ не чисто периодическая непрерывная дробь. Поскольку θ — приведенное иррациональное число, имеем $\theta > 1, -\frac{1}{\theta'} > 1$.

Далее, из определения непрерывной дроби находим

$$\theta_{l-1} = a_{l-1} + \frac{1}{\theta_l}, \quad \theta_{l+k-1} = a_{l+k-1} + \frac{1}{\theta_{l+k}}.$$

Следовательно,

$$-\frac{1}{\theta'_l} = a_{l-1} + (-\theta'_{l-1}), \quad -\frac{1}{\theta'_{l+k}} = a_{l+k-1} + (-\theta'_{l+k-1}).$$

Так как θ — приведенное число, то a_{l-1} и a_{l+k-1} будут целыми частями соответственно чисел $-1/\theta'_l$ и $-1/\theta'_{l+k}$, а $-\theta_{l-1}$ и $-\theta_{l+k-1}$ — остатками этих чисел. Поскольку $\theta'_l = \theta'_{l+k}$, имеем $a_{l-1} = a_{l+k-1}$ и $\theta'_{l-1} = \theta'_{l+k-1}$. Стало быть, $\theta_{l-1} = \theta_{l+k-1}$. Последнее равенство противоречит минимальности выбранного номера l. Таким образом доказано, что $l = 0$ и приведенное иррациональное число θ разлагается в чисто периодическую непрерывную дробь. ◄

3. Пусть вещественное число $\theta > 1$ разлагается в периодическую непрерывную дробь. Тогда θ — квадратичная иррациональность. Кроме того, если непрерывная дробь числа θ — чисто периодическая, то θ — приведенное число. Более того, пусть число θ разлагается в чисто периодическую непрерывную дробь следующего вида

$$\theta = [\overline{a_1, \ldots, a_k}],$$

тогда число $-1/\theta'$ разлагается в чисто периодическую непрерывную дробь вида

$$-\frac{1}{\theta'} = [\overline{a_k, \ldots, a_1}].$$

► Докажем первое утверждение. Пусть k — период непрерывной дроби числа $\theta > 1$. Тогда существует целое число l (длина предпериода) такое, что для всех номеров n с условием $n \geqslant l$ остатки непрерывной дроби удовлетворяют равенствам $\theta_{n+k} = \theta_n$. Пользуясь формулой для выражения числа через остаток непрерывной

дроби, найдем

$$\theta = \frac{\theta_n p_{n-1} + p_{n-2}}{\theta_n q_{n-1} + q_{n-2}} = \frac{\theta_{n+k} p_{n+k-1} + p_{n+k-2}}{\theta_{n+k} q_{n+k-1} + q_{n+k-2}} = \frac{\theta_n p_{n+k-1} + p_{n+k-2}}{\theta_n q_{n+k-1} + q_{n+k-2}}.$$

Следовательно, θ_n удовлетворяет квадратному уравнению

$$\frac{\theta_n p_{n-1} + p_{n-2}}{\theta_n q_{n-1} + q_{n-2}} = \frac{\theta_n p_{n+k-1} + p_{n+k-2}}{\theta_n q_{n+k-1} + q_{n+k-2}}.$$

Таким образом из равенства

$$\theta = \frac{\theta_n p_{n-1} + p_{n-2}}{\theta_n q_{n-1} + q_{n-2}}$$

имеем, что число θ является квадратичной иррациональностью.

Докажем теперь второе утверждение. Поскольку непрерывная дробь для числа θ является чисто периодической с периодом, равным k, имеем

$$\theta = [a_0, a_1, \ldots, a_{k-1}, \theta].$$

Отсюда получим

$$\theta = \frac{\theta p_{k-1} + p_{k-2}}{\theta q_{k-1} + q_{k-2}}, \quad q_{k-1}\theta^2 - (p_{k-1} - q_{k-1})\theta - p_{k-2} = 0.$$

Коэффициенты последнего квадратного уравнения — целые взаимно простые числа. Его дискриминант равен

$$(p_{k-1} - q_{k-1})^2 + 4q_{k-1}p_{k-2} > 0.$$

Следовательно, вещественное число $\theta > 1$ является квадратичной иррациональностью.

Покажем, что θ является приведенным числом. Из равенства

$$-\frac{1}{\theta'_k} = a_{k-1} + (-\theta'_{k-1}),$$

найденного при решении предыдущей задачи, получим

$$-\frac{1}{\theta'_k} = \left[a_{k-1}, \ldots, a_0, -\frac{1}{\theta'}\right].$$

Таким образом из условия $\theta_k = \theta$ следует, что число $-1/\theta'$ удовлетворяет уравнению

$$-\frac{1}{\theta'} = \left[a_{k-1}, \ldots a_0, -\frac{1}{\theta'}\right],$$

тем самым доказано, что θ — приведенное число. ◀

§ 12. Разложение квадратного корня из натурального числа в непрерывную дробь

1. Разложить число $\sqrt{31}$ в непрерывную дробь. Доказать, что

$$\left|\sqrt{31} - \frac{1520}{273}\right| < \frac{1}{273 \cdot 2885} < \frac{1}{7 \cdot 10^5}.$$

► Имеем $5^2 < 31 < 6^2$. Следовательно, $a_0 = 5$. Далее получим

$$\sqrt{31} = 5 + (\sqrt{31} - 5) = 5 + \frac{6}{\sqrt{31} + 5},$$

$$\frac{\sqrt{31} + 5}{6} = 1 + \frac{\sqrt{31} - 1}{6} = 1 + \frac{5}{\sqrt{31} + 1}, a_1 = 1,$$

$$\frac{\sqrt{31} + 1}{5} = 1 + \frac{\sqrt{31} - 4}{5} = 1 + \frac{3}{\sqrt{31} + 4}, a_2 = 1,$$

$$\frac{\sqrt{31} + 4}{3} = 3 + \frac{\sqrt{31} - 5}{3} = 3 + \frac{2}{\sqrt{31} + 5}, a_3 = 3,$$

$$\frac{\sqrt{31} + 5}{2} = 5 + \frac{\sqrt{31} - 5}{2} = 5 + \frac{3}{\sqrt{31} + 5}, a_4 = 5,$$

$$\frac{\sqrt{31} + 5}{3} = 3 + \frac{\sqrt{31} - 4}{3} = 3 + \frac{5}{\sqrt{31} + 4}, a_5 = 3,$$

$$\frac{\sqrt{31} + 4}{5} = 1 + \frac{\sqrt{31} - 1}{5} = 1 + \frac{6}{\sqrt{31} + 1}, a_6 = 1,$$

$$\frac{\sqrt{31} + 1}{6} = 1 + \frac{\sqrt{31} - 5}{6} = 1 + \frac{1}{\sqrt{31} + 5}, a_7 = 1,$$

$$\sqrt{31} + 5 = 10 + (\sqrt{31} - 5) = 10 + \frac{6}{\sqrt{31} + 5}, a_8 = 10.$$

Таким образом приходим для числа $\sqrt{31}$ к периодической непрерывной дроби с периодом, равным 8. В понятных обозначениях имеем

$$\sqrt{31} = [5, \overline{1, 1, 3, 5, 3, 1, 1, 10}].$$

Схематически предыдущие действия можно изобразить в виде следующей таблицы для неполных частных a_n, числителей p_n и знаменателей q_n подходящих дробей числа $\sqrt{31}$.

n		0	1	2	3	4	5	6	7	8
a_n		5	1	1	3	5	3	1	1	10
p_n	1	5	6	11	39	206	657	863	1520	16063
q_n	0	1	1	2	7	37	118	155	273	2885

При $n \geqslant 1$ для вычисления числителей p_n и знаменателей q_n подходящих дробей использована следующая формула задачи 2,IX:

$$p_n = a_n p_{n-1} + p_{n-2}, q_n = a_n q_{n-1} + q_{n-2}, p_{-1} = 1, q_{-1} = 0.$$

Из утверждений задач 2,IX и 10,IX находим

$$\frac{p_7}{q_7} = \frac{1520}{273}, \quad \left|\sqrt{31} - \frac{1520}{273}\right| < \frac{1}{273 \cdot 2885} < \frac{1}{7 \cdot 10^5}. \blacktriangleleft$$

2. Для того чтобы алгебраическое число $\alpha > 1$ имело следующее разложение в непрерывную дробь

$$\alpha = [b, \overline{a_1, \ldots, a_{k-1}, 2b}] = [b, \overline{a_{k-1}, \ldots, a_1, 2b}],$$

где $b, a_1, \ldots, a_{k-1}$ — натуральные числа, необходимо и достаточно, чтобы число α было квадратным корнем из рационального числа, большего 1 и не являющегося точным квадратом.

► *Необходимость.* Пусть α имеет указанное выше разложение в непрерывную дробь. Тогда для остатка находим

$$\frac{1}{\alpha - b} = [\overline{a_1, \ldots, a_{k-1}, 2b}].$$

Отсюда по утверждению задачи 3,XI получим

$$-\alpha' + b = [\overline{2b, a_{k-1}, \ldots, a_1}].$$

Следовательно,

$$-\alpha' = [b, \overline{a_1, \ldots, a_{k-1}, 2b}] = \alpha.$$

Таким образом имеем, что $\alpha'^2 = \alpha^2 = a$ — рациональное число, причем $a > b \geqslant 1$ и a не является квадратом.

Достаточность. Дано, что число $\alpha = \sqrt{a}$, где $a > 1$ — рациональное число и не является точным квадратом. Положим $b = [\sqrt{a}] \geqslant 1$. Для остатка $\theta = \frac{1}{\alpha - b}$ имеем неравенство $\theta > 1$. Покажем, что число θ будет приведенным числом. Это следует из следующей цепочки соотношений

$$\alpha' = -\alpha, \alpha - b = \frac{1}{\theta}, -\frac{1}{\theta'} = -\alpha' + b = \alpha + b > 2b > 1.$$

Тогда по утверждению задачи 3,XI находим

$$\theta = [\overline{a_1, \ldots, a_k}], \quad -\frac{1}{\theta'} = [\overline{a_k, \ldots, a_1}].$$

Далее имеем

$$\left[-\frac{1}{\theta'}\right] = [\alpha + b] = [\alpha] + b = 2b, a_k = 2b.$$

Следовательно,

$$-\frac{1}{\theta'} = [\overline{2b, a_{k-1}, \ldots, a_1}], \theta = [\overline{a_1, \ldots, a_{k-1}, 2b}].$$

Таким образом

$$\alpha = -\frac{1}{\theta'} - b = [b, \overline{a_{k-1}, \ldots, a_1, 2b}], \quad \alpha = b + \theta = [b, \overline{a_1, \ldots, a_{k-1}, 2b}].$$

Эти равенства дают искомые разложения числа α в непрерывную дробь. ◀

§ 13. Вычисление основной единицы вещественного квадратичного поля

1. Пусть θ — приведенное число из $\mathbf{F} = \mathbf{Q}(\sqrt{D})$, т.е. $\theta > 1$ и $-\frac{1}{\theta'} > 1$, принадлежащее определителю m^2D, и пусть $\theta = [\overline{a_0, \ldots, a_{k-1}}]$ — чисто периодическое разложение в непрерывную дробь числа θ, имеющее период $k \geqslant 1$. Пусть, далее, p_{k-2}/q_{k-2} и p_{k-1}/q_{k-1} — последние перед повторением периода подходящие дроби числа θ. Тогда $\varepsilon = q_{k-1}\theta + q_{k-2}$ будет нетривиальной единицей кольца дискриминанта m^2D с условиями $\varepsilon > 1$ и $N(\varepsilon) = (-1)^k$. Кроме того, эту единицу можно представить в виде

$$\varepsilon = \frac{u + vm\sqrt{D}}{2},$$

где целые рациональные числа u и v определяются следующим образом

$$u = p_{k-1} + q_{k-2}, \quad v = (q_{k-1}, p_{k-1} - q_{k-2}, p_{k-2}).$$

► По утверждению задачи 6, IX получим

$$\theta = \frac{p_{k-1}\theta + p_{k-2}}{q_{k-1}\theta + q_{k-2}},$$

поскольку разложение в чисто периодическую дробь числа θ имеет период k и $\theta_k = \theta$. Следовательно, найдется число ε из $\mathbf{F}$ такое, что выполняется пара равенств

$$\varepsilon\theta = p_{k-1}\theta + p_{k-2}, \quad \varepsilon = q_{k-1}\theta + q_{k-2}.$$

Имеем цепочку равенств

$$\theta = \frac{\varepsilon - q_{k-2}}{q_{k-1}}, \quad \varepsilon\frac{\varepsilon - q_{k-2}}{q_{k-1}} = p_{k-1}\frac{\varepsilon - q_{k-2}}{q_{k-1}} + p_{k-2},$$

$$\varepsilon^2 - \varepsilon(p_{k-1} + q_{k-2}) + p_{k-1}q_{k-2} - p_{k-2}q_{k-1} = 0.$$

Поскольку $p_{k-1}q_{k-2} - p_{k-2}q_{k-1} = (-1)^k$, для числа ε находим уравнение

$$\varepsilon^2 - \varepsilon(p_{k-1} + q_{k-2}) + (-1)^k = 0.$$

По утверждению задачи 2,X число ε является единицей поля $\mathbf{F}$ с нормой $N(\varepsilon) = (-1)^k$. Далее имеем явное выражение для $\varepsilon = q_{k-1}\theta + q_{k-2}$. Отсюда следует, что $\varepsilon > 1$.

С другой стороны, число θ удовлетворяет квадратному уравнению

$$\theta(q_{k-1}\theta + q_{k-2}) = p_{k-1}\theta + p_{k-2},$$

т.е. уравнению вида

$$q_{k-1}\theta^2 - (p_{k-1} - q_{k-2})\theta - p_{k-2} = 0.$$

Пусть v — наибольший общий делитель чисел $q_{k-1}, p_{k-1} - q_{k-2}$ и p_{k-2}. Положим

$$q_{k-1} = av, p_{k-1} - q_{k-2} = bv, p_{k-1} = cv, (a, b, c) = 1, p_{k-1} + q_{k-2} = u.$$

Тогда уравнение для числа θ примет вид

$$a\theta^2 - b\theta - c = 0.$$

Как и раньше, для приведенного числа θ находим

$$\theta = \frac{b + m\sqrt{D}}{2a}.$$

Следовательно,

$$\varepsilon = q_{k-1}\theta + q_{k-2} = q_{k-1}\frac{b + m\sqrt{D}}{2a} + q_{k-2} =$$

$$= q_{k-1}\frac{bv + vm\sqrt{D}}{2av} + q_{k-2} = \frac{u + vm\sqrt{D}}{2}. \blacktriangleleft$$

2. Каждая единица $\varepsilon > 1$, принадлежащая дискриминанту m^2D и имеющая форму

$$\varepsilon = \frac{u + v\sqrt{D}}{2}$$

с натуральными числами u и v, представляется в виде

$$\varepsilon = q\theta + q',$$

где q и q' — знаменатели двух соседних подходящих дробей в разложении приведенного числа θ дискриминанта m^2D в непрерывную дробь.

► Возьмем любую единицу $\varepsilon = \frac{u+vm\sqrt{D}}{2} > 1$ с целыми рациональными числами $u \geqslant 1$ и $v \geqslant 1$.

Пусть число θ удовлетворяет уравнению $a\theta^2 - b\theta - c = 0$ с целыми коэффициентами a, b, c и дискриминантом $b^2 + 4ac = m^2D$.

Положим

$$p = \frac{u + bv}{2}, q = av, p' = cv, q' = \frac{u - bv}{2}.$$

Рациональные числа p, q, p', q' будут целыми, поскольку числа ε и $a\theta$ являются целыми в поле $\mathbf{F} = \mathbf{Q}(\sqrt{D})$. Кроме того, имеем

$$pq' - p'q = \frac{u^2 - (b^2 + 4ac)v^2}{4} = \frac{u^2 - v^2m^2D}{4} = N(\varepsilon).$$

Отсюда следует, что дроби p/q и p'/q' будут несократимы.

Так как набор чисел $q, p - q', p'$ пропорционален набору a, b, c, то число θ удовлетворяет уравнению

$$q\theta^2 - (p - q')\theta - p' = 0$$

или

$$\theta = \frac{p\theta + p'}{q\theta + q'}.$$

Как и раньше, из условия, что θ — приведенное число, имеем

$$b < m\sqrt{D}, \quad 2a - b < m\sqrt{D} < 2a + b.$$

Далее, используя условие $\varepsilon > 1$, находим

$$q' = \frac{a - bv}{2} > \frac{a - vm\sqrt{D}}{2} = \varepsilon' = \frac{N(\varepsilon)}{\varepsilon} > \begin{cases} 0, & \text{если} N(\varepsilon) = 1, \\ -1, & \text{если} N(\varepsilon) = -1, \end{cases}$$

$$q - q' = \frac{-u + (2a + b)v}{2} > \frac{-u + vm\sqrt{D}}{2} = -\varepsilon' =$$

$$= -\frac{N(\varepsilon)}{\varepsilon} > \begin{cases} -1, & \text{если} N(\varepsilon) = 1, \\ 0, & \text{если} N(\varepsilon) = -1, \end{cases}$$

$$p - q = \frac{u - (2a - b)v}{2} > \frac{u - vm\sqrt{D}}{2} = \varepsilon' =$$

$$= \frac{N(\varepsilon)}{\varepsilon} > \begin{cases} 0, & \text{если} N(\varepsilon) = 1, \\ -1, & \text{если} N(\varepsilon) = -1. \end{cases}$$

Следовательно,

$$0 < q' \leqslant q, \frac{p}{q} > 1, \text{если} N(\varepsilon) = 1,$$

$$0 \leqslant q' < q, \frac{p}{q} \geqslant 1, \text{если} N(\varepsilon) = -1.$$

Разложим число p/q в непрерывную дробь

$$\frac{p}{q} = [a_0, a_1, \ldots, a_k] = \frac{p_k}{q_k},$$

причем число k будет четным или нечетным в соответствии с равенством $N(\varepsilon) = (-1)^k$.

Покажем, что $\frac{p_{k-1}}{q_{k-1}} = \frac{p'}{q'}$. Имеем соотношения

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^k = N(\varepsilon), 0 \leqslant q_{k-1} \leqslant q_k,$$

причем равенство имеет место в первом неравенстве только при $k = 1$, а во втором, — быть может, только при $k = 2$.

Таким образом,

$$p_k(q_{k-1} - q') - q_k(p_{k-1} - p') = 0,$$

что возможно только при $q_{k-1} = q'$, иначе несократимая дробь p_k/q_k была представлена дробью с меньшим знаменателем $|q_{k-1} - q'|$, а это невозможно. Следовательно, $p_{k-1} = p', q_{k-1} = q'$.

Из равенств

$$\theta = \frac{p\theta + p'}{q\theta + q'} = \frac{p_k\theta + p_{k-1}}{q_k\theta + q_{k-1}}$$

имеем

$$\theta = [a_0, a_1, \ldots, a_k, \theta],$$

а натуральные числа $a_0, \ldots, a_k$ являются неполными частными разложения числа θ в непрерывную дробь, причем они могут представлять собой несколько периодов в этом разложении θ. Следовательно, получим

$$v = (q_k, p_k - q_{k-1}, p_{k-1}), u = p_k + q_{k-1},$$

или $q_k = cv, p_k - q_{k-1} = bv, p_{k-1} = cv$. Эти соотношения по доказательству утверждения предыдущей задачи определяют $\varepsilon = q_k\theta + q_{k-1}$ по разложению числа θ в непрерывную дробь. ◀

Вычислим основную единицу поля $\mathbb{F} = \mathbb{Q}(\sqrt{D})$. Дискриминант этого поля равен d,

$$d = \begin{cases} D, & \text{если} D \equiv 1 \pmod 4, \\ 4D, & \text{если} D \equiv 2, 3 \pmod 4. \end{cases}$$

Базисом кольца целых чисел этого поля являются числа 1 и ρ, где

$$\rho = \begin{cases} \frac{1+\sqrt{D}}{2} = \frac{1+\sqrt{d}}{2}, & \text{если} D \equiv 1 \pmod 4, \\ \sqrt{D} = \frac{0+\sqrt{d}}{2}, & \text{если} D \equiv 2, 3 \pmod 4. \end{cases}$$

Для наименьшего положительного дискриминанта $d = D = 5$ базисное число ρ имеет следующее разложение в чисто периодическую непрерывную дробь

$$\rho = \frac{1 + \sqrt{5}}{2} = [\overline{1}]$$

с периодом 1. Числители p_n и знаменатели q_n подходящих дробей удовлетворяют при $n \geqslant 1$ рекуррентным формулам вида

$$\begin{cases} p_{n+1} = p_n + p_{n-1}, \\ q_{n+1} = q_n + q_{n-1}, \end{cases}$$

причем $p_0 = p_1 = 1, q_0 = 0, q_1 = 1$.

Схематически разложение числа ρ в непрерывную дробь представим в виде следующей таблицы для неполных частных a_n, числителей p_n и знаменателей q_n подходящих дробей этого числа.

n		0	1	2	3	4	5	6	7	8	...
a_n		1	1	1	1	1	1	1	1	1	...
p_n	1	1	2	3	5	8	13	21	34	55	...
q_n	0	1	1	2	3	5	8	13	21	34	...

Заметим, что в данном случае при $n \geqslant 0$ имеем $p_n = q_{n+1}$. Любое решение $u = u_n, v = v_n$ уравнения Пелля $u^2 - 5v^2 = 1$ по утверждению предыдущей задачи представляется в виде

$$\rho^n = \frac{u_n + v_n\sqrt{5}}{2},$$

где $\rho = \frac{1+\sqrt{5}}{2}$ — основная единица поля $\mathbf{Q}\sqrt{5}$ и

$$u_n = p_n + q_{n-1} = q_{n+1} + q_{n-1},$$
$$v_n = (q_n, p_n - q_{n-1}, p_{n-1}) = (q_n, q_n, q_n) = q_n.$$

3. Пусть ρ — базисное число квадратичного поля дискриминанта d, отличного от пяти. Тогда число

$$\rho^* = \frac{1}{\rho - a_0}$$

является приведенным, где $a_0 = [\rho]$.

► Имеем $\rho > 1, \rho^* > 1$. Для величины $-1/\rho^{*'}$ находим

$$-\frac{1}{\rho^{*'}} = a_0 - \rho' =$$

$$= \begin{cases} a_0 - \frac{1-\sqrt{D}}{2} = a_0 + \rho - 1 > 2a_0 - 1 \geqslant 1, & \text{если} D \equiv 1 \pmod 4, \\ a_0 + \sqrt{D} > 2a_0 \geqslant 2, & \text{если} D \equiv 2, 3 \pmod 4, \end{cases}$$

т.е. $-1/\rho^{*'} > 1$.

Таким образом, число ρ^* будет приведенным. ◄

4. Найти основную единицу поля $\mathbf{Q}(\sqrt{31})$.

► В этом случае базисное число $\rho = \sqrt{31}$. Из утверждения задачи 1,XII получим разложение в периодическую непрерывную дробь с периодом 8 следующих чисел

$$\rho = \sqrt{31} = [5, \overline{1, 1, 3, 5, 3, 1, 1, 10}],$$

$$\rho^* = \frac{5+\sqrt{31}}{6} = \overline{[1,1,3,5,3,1,1,10]}.$$

Представим в виде таблицы при $0 \leqslant n \leqslant 7$ значения неполных частных a_n, числители p_n и знаменатели q_n подходящих дробей числа ρ^*. Имеем

n		0	1	2	3	4	5	6	7
a_n		1	1	3	5	3	1	1	10
p_n	1	1	2	7	37	118	155	273	2885
q_n	0	1	1	4	21	67	88	155	1638

Используя утверждения задач 1–3, получим

$$u_1 = 2885 + 155 = 2 \cdot 1520, v_1 = (1638, 2730, 273) = 273.$$

Следовательно, основная единица ε_1 равна

$$\varepsilon_1 = 1520 + 273\sqrt{31}. \blacktriangleleft$$

§ 14. Теорема П. Л. Чебышёва о попадании простых чисел в интервалы (постулат Бертрана)

Далее докажем известную теорему П. Л. Чебышёва о том, что при $x > 1$ на промежутке $[x, 2x)$ лежит хотя бы одно простое число. Пусть, как и раньше в VI, $\psi(x) = \sum\limits_{n \leqslant x} \Lambda(n)$ обозначает функцию Чебышёва, $\theta(x) = \sum\limits_{p \leqslant x} \ln p$,

$$\Lambda(n) = \begin{cases} \ln p, & \text{если} \quad n = p^r, \\ 0, & \text{в противном случае,} \end{cases}$$

где p обозначает простое число, n, r — натуральные числа.

1. При $x \geqslant 1$ справедливы равенства

$$T(x) = \sum_{n \leqslant x} \ln n = \sum_{n \leqslant x} \psi(x/m),$$

$$T(x) - 2T(x/2) = \sum_{n \leqslant x} (-1)^{n-1} \psi(x/n).$$

▶ Поскольку $\ln n = \sum\limits_{d|n} \Lambda(d)$, имеем

$$T(x) = \sum_{n \leqslant x} \sum_{d|n} \Lambda(d) = \sum_{d \leqslant x} \Lambda(d) \sum_{\substack{n \leqslant x \\ n = md}} 1 =$$

$$= \sum_{d \leqslant x} \Lambda(d) \sum_{m \leqslant x/d} 1 = \sum_{m \leqslant x} \sum_{d \leqslant x/m} \Lambda(d) =$$

$$= \sum_{m \leqslant x} \psi(x/m).$$

Отсюда получим

$$T(x) - 2T(x/2) = \sum_{n \leqslant x} \psi(x/n) - 2 \sum_{n \leqslant x/2} \psi(x/(2n)) =$$

$$= \sum_{n \leqslant x} (-1)^{n-1} \psi(x/n). \blacktriangleleft$$

Приведем следующий признак сходимости ряда, принадлежащий Лейбницу. Пусть задана невозрастающая последовательность $\{a_n\}, n \geqslant 1$, неотрицательных чисел, стремящаяся к нулю при $n \to \infty$. Тогда справедливы неравенства

$$a_1 - a_2 \leqslant \sum_{n=1}^{\infty} (-1)^{n-1} a_n \leqslant a_1 - a_2 + a_3.$$

2. При $x \geqslant 1$ имеем

$$\psi(x) - \psi(x/2) \leqslant T(x) - 2T(x/2) \leqslant \psi(x) - \psi(x/2) + \psi(x/3).$$

$\blacktriangleright$ Поскольку функция $\psi(x)$ не отрицательна и не убывает, и $\psi(x) = 0$ при $0 < x < 2$, по признаку Лейбница и по утверждению предыдущей задачи следуют искомые неравенства. $\blacktriangleleft$

3. Для любого натурального числа m справедливы неравенства

$$\frac{1}{2\sqrt{m}} \leqslant 2^{-2m} \binom{2m}{m} < \frac{1}{\sqrt{2m+1}}.$$

$\blacktriangleright$ Проведем индукцию по m. При $m = 1$ утверждение справедливо, поскольку

$$\frac{1}{2} = 2^{-2} \binom{2}{1} < \frac{1}{\sqrt{3}}.$$

Предположим, что оно справедливо при $m = k$. Докажем, что оно верно при $m = k + 1$. По предположению индукции имеем цепочку соотношений

$$\frac{1}{2\sqrt{m}} 2^{-2} \frac{(2m+1)(2m+2)}{(m+1)^2} \leqslant 2^{-2m} \binom{2m}{m} 2^{-2} \frac{(2m+1)(2m+2)}{(m+1)^2} =$$

$$= 2^{-2m-2}\binom{2m+2}{m+1} < \frac{1}{\sqrt{2m+1}}2^{-2}\frac{(2m+1)(2m+2)}{(m+1)^2}.$$

Следовательно, достаточно доказать, что выполняются неравенства

$$\frac{1}{2\sqrt{m+1}} \leqslant \frac{1}{2\sqrt{m}}2^{-2}\frac{(2m+1)(2m+2)}{(m+1)^2},$$

$$\frac{1}{\sqrt{2m+1}}2^{-2}\frac{(2m+1)(2m+2)}{(m+1)^2} < \frac{1}{2m+3}.$$

Первое из них является следствием того, что

$$2m+1 \geqslant 2\sqrt{m(m+1)}, \text{т.е.} \quad 4m^2+4m+1 \geqslant 4m^2+4m,$$

а второе следует из того, что

$$2m+2 > \sqrt{(2m+1)(2m+3)}, \text{т.е.} \quad 4m^2+8m+4 > 4m^2+8m+3. \blacktriangleleft$$

4. При $x \geqslant 1$ имеем неравенство

$$\psi(x) < x\ln 4.$$

► Проведем индукцию по параметру x. Сначала проверим справедливость неравенства при $1 \leqslant x < 17$. При $1 \leqslant x < 2$ оно, очевидно, справедливо. При $2 \leqslant x < 4$ имеем

$$\psi(x) \leqslant \ln 2 + \ln 3 < 2\ln 4 \leqslant x\ln 4.$$

При $4 \leqslant x < 7$ находим

$$\psi(x) \leqslant 2\ln 2 + \ln 3 + \ln 5 = \ln 60 < 3\ln 4 < x\ln 4.$$

Пусть $7 \leqslant x < 11$. Тогда имеем

$$\psi(x) \leqslant 3\ln 2 + 2\ln 3 + \ln 5 + \ln 7 = \ln 2520 < 6\ln 4 < x\ln 4.$$

Пусть, теперь, $11 \leqslant x < 13$. Тогда

$$\psi(x) \leqslant 3\ln 2 + 2\ln 3 + \ln 5 + \ln 7 + \ln 11 = \ln 27720 < 10\ln 4 < x\ln 4.$$

Пусть, наконец, $13 \leqslant x < 17$. Тогда получим

$$\psi(x) \leqslant 4\ln 2 + 2\ln 3 + \ln 5 + \ln 7 + \ln 11 + \ln 13 =$$

$$= \ln 720720 < 12 \ln 4 < x \ln 4.$$

Предположим, что утверждение справедливо при $17 \leqslant x < y$. Докажем, что оно верно при $y \leqslant x < y+2$. Пусть $[y] = n$, т.е. $n \leqslant y < n+1$, где n — целое число. Возможны два случая: 1) $n = 2m$ — четное число и 2) $n = 2m-1$ — нечетное число. Рассмотрим сначала случай 1). Имеем

$$2m \leqslant y < 2m + 1 < 2m + 2 \leqslant y + 2.$$

Пусть $x \in [y, 2m + 1)$. Тогда из утверждения задачи 2 и предположения индукции получим

$$\psi(x) = \psi(2m) < \ln \binom{2m}{m} + \psi(m) < 2m \ln 4 - \ln \sqrt{2m - 1} \leqslant x \ln 4.$$

Пусть, теперь, $x \in [2m + 1, 2m + 2)$. Тогда, вновь используя утверждение задачи 2 и предположение индукции, находим

$$\psi(x) \leqslant \psi(2m+2) < (2m+2) \ln 4 - \ln \sqrt{2m + 1} < (2m+1) \ln 4 \leqslant x \ln 4,$$

поскольку $\ln 4 < \ln \sqrt{17} \leqslant \ln \sqrt{2m + 1}$.

Пусть, наконец, $x \in [2m + 2, y)$. Тогда из тех же соображений, что и раньше, имеем

$$\psi(x) = \psi(2m + 2) < \ln \binom{2m + 2}{m + 1} + \psi(m + 1) <$$

$$< (2m + 2) \ln 4 - \ln \sqrt{2m + 1} \leqslant x \ln 4.$$

Случай 1) полностью рассмотрен.

Рассмотрим, теперь, случай 2). Имеем

$$2m - 1 \leqslant y < 2m < 2m + 1 \leqslant y + 2 < 2m + 2.$$

Пусть $x \in [y, 2m)$. Тогда из утверждения задачи 2 и предположения индукции получим

$$\psi(x) < \psi(2m) < \ln \binom{2m}{m} + \psi(m) < 2m \ln 4 - \ln \sqrt{2m - 1} \leqslant$$

$$\leqslant (2m - 1) \ln 4 \leqslant x \ln 4,$$

поскольку $\ln 4 = \ln \sqrt{16} \leqslant \ln \sqrt{2m - 1}, 16 \leqslant [y] = 2m - 1$.

Пусть, теперь, $x \in [2m, 2m+1)$. Тогда, вновь используя утверждение задачи 2 и предположение индукции, находим

$$\psi(x) \leqslant \psi(2m) < (2m)\ln 4 - \ln\sqrt{2m} \leqslant 2m\ln 4 \leqslant x\ln 4.$$

Пусть, наконец, $x \in [2m+1, y)$. Тогда из тех же соображений, что и раньше, имеем

$$\psi(x) = \psi(2m+2) < \ln\binom{2m+2}{m+1} + \psi(m+1) <$$

$$< (2m+2)\ln 4 - \ln\sqrt{2m+3} \leqslant (2m+1)\ln 4 \leqslant x\ln 4.$$

Этим завершается рассмотрение случая 2). ◄

5. Пусть m — натуральное число. Тогда имеем

$$\theta(2m) - \theta(m) \geqslant \frac{\ln 4}{3}m - \ln\sqrt{4m} - \sqrt{2m}\ln 4.$$

► Используя утверждения задач 2 и 4, находим

$$\psi(2m) - \psi(m) > \ln\binom{2m}{m} - \psi(\frac{2m}{3}) \geqslant$$

$$\geqslant m\ln 4 - \ln\sqrt{4m} - \frac{2m}{3}\ln 4 = \frac{\ln 4}{3}m - \ln\sqrt{4m}.$$

Далее, имеем

$$\psi(2m) - \psi(m) = \theta(2m) - \theta(m) + r_m,$$

где

$$r_m = \sum_{\substack{m < p^\alpha \leqslant 2m \\ \alpha \geqslant 2}} \ln p.$$

Поскольку $\alpha \geqslant 2$, в сумму r_m входят простые числа p с условием $p \leqslant \sqrt{2m}$, причем в силу условия $m < p^\alpha \leqslant 2m$ при каждом фиксированном простом числе p в эту сумму r_m может входить не более одной степени данного числа. Следовательно,

$$r_m \leqslant \theta(\sqrt{2m}) \leqslant \psi(\sqrt{2m}) \leqslant \sqrt{2m}\ln 4.$$

Отсюда следует искомое неравенство. ◄

6. Пусть $m \geqslant 2^8$ — натуральное число. Тогда справедливо неравенство

$$\pi(2m) - \pi(m) \geqslant \sqrt{m/2}.$$

► Из утверждения задачи 5 при любом натуральном числе m имеем неравенство

$$\pi(2m) - \pi(m) = \sum_{m<p\leqslant 2m} 1 \geqslant \frac{\theta(2m) - \theta(m)}{\ln 2m} \geqslant$$

$$\geqslant \frac{m \ln 4}{3 \ln 2m} - \frac{\ln \sqrt{4m}}{\ln 2m} - \frac{\sqrt{2m} \ln 4}{\ln 2m} = f_1(m).$$

Далее, при $m \geqslant 2^8$ оценим $f_1(m)$ снизу. Получим

$$f_1(m) = \frac{m \ln 4}{3 \ln 2m} - \frac{1}{2} - \frac{\ln 2}{2 \ln 2m} - \frac{\sqrt{2m} \ln 4}{\ln 2m} \geqslant$$

$$\geqslant \frac{m \ln 4}{3 \ln 2m} - \frac{5}{9} - \frac{2\sqrt{2m}}{9} = f(m).$$

Покажем, что при $m \geqslant 2^8$ функция $g(m) = f(m) - \sqrt{m/2}$ будет положительной. При $m = 2^8$ имеем

$$g(2^8) = \frac{2^8 \ln 4}{3 \ln 2^9} - \frac{5}{9} - \frac{2\sqrt{2^9}}{9} - \sqrt{2^7} = \frac{2^9 - 15 - 312\sqrt{2}}{27} > \frac{29}{27} > 0.$$

Найдем производную функции $g(x)$. Имеем

$$g'(x) = \frac{\ln 4}{3} \frac{\ln 2x - 1}{(\ln 2x)^2} - \frac{13}{18\sqrt{2x}}.$$

Поскольку при $x \geqslant 2^8$ справедливо неравенство $\ln 2x - 1 \geqslant \frac{7}{9} \ln 2x$, получим

$$g'(x) \geqslant \frac{7 \ln 4}{27 \ln 2x} - \frac{13}{18\sqrt{2x}} = g_1(x).$$

При $x > e^2$ функция $\sqrt{x}/\ln x$ является возрастающей, поэтому при $x \geqslant 2^8$ имеем

$$\sqrt{2x} g_1(x) \geqslant \frac{224\sqrt{2}}{243} - \frac{13}{18} > 0.$$

Следовательно, при $x \geqslant 2^8$ функция $g(x)$ возрастающая и $g(x) > 0$. Это и доказывает искомое неравенство. ◄

7. Пусть n — натуральное число. Тогда при $x \geqslant 2n^2$ на отрезке $[x, 2x]$ лежит по крайней мере n различных простых чисел.

► Положим $m = [x] \geqslant 2^8$. Имеем теоретико-множественное включение $[m+1, 2m] \subset [x, 2x]$. Следовательно, все простые числа, находящиеся на отрезке $[m+1, 2m]$, будут принадлежать и отрезку $[x, 2x]$. В силу утверждения задачи 6 при $m \geqslant 2^8$ на отрезке $[m+1, 2m]$ не менее $\sqrt{m/2}$ различных простых чисел. Поскольку при $x \geqslant 2n^2$ справедливы неравенства $\sqrt{x/2} \geqslant \sqrt{m/2} \geqslant n$, при $x \geqslant \max\{2^8, 2n^2\}$ на отрезке $[x, 2x]$ находится по крайней мере n различных простых чисел.

Осталось доказать утверждение задачи при $2 \leqslant x < 2^8$. Разобьем этот промежуток на промежутки вида $I_n = [2n^2, 2(n+1)^2)$, где $1 \leqslant n \leqslant 11$. Используя таблицы простых чисел, проверяем, что если $x \in I_n$, то на отрезке $[x, 2x]$ находится по крайней мере n различных простых чисел. Например, при $n = 1$ имеем $I_1 = [2, 8)$. Рассматривая x в промежутках $2 \leqslant x < 3, 3 \leqslant x < 5, 5 \leqslant x < 7$ и $7 \leqslant x < 8$, видим, что $3 \in [x, 2x]$ при $x \in [2, 3), 5 \in [x, 2x]$ при $x \in [3, 5), 7 \in [x, 2x]$ при $x \in [5, 7), 11 \in [x, 2x]$ при $x \in [7, 8)$. ◄

§ 15. Алгебраическое приложение. Группы. Коммутативные кольца. Многочлены. Поля. Поля частных. Конечные поля

I. Группы

Пусть K — непустое множество элементов $a, b, c, \ldots$. На множестве K задана бинарная операция $\circ$, если для любой упорядоченной пары (a, b) из декартова квадрата K^2 однозначно определен элемент $c \in K$ такой, что $c := a \circ b$. В этом случае говорят, что множество K замкнуто относительно операции $\circ$.

Группой G называется непустое множество G, замкнутое относительно операции $\circ$ и удовлетворяющее следующим условиям:
1) для любых элементов $a, b, c \in G$ выполняется ассоциативный закон: $(a \circ b) \circ c = a \circ (b \circ c)$;
1) существует (единичный) нейтральный элемент $e \in G$ такой, что для любого элемента $a \in G$ имеем $e \circ a = a = a \circ e$;
2) для любого элемента $a \in G$ найдется обратный элемент $b \in G$ такой, что $b \circ a = e = a \circ b$.

1. Нейтральный элемент e в группе G единствен.

► Пусть e' — другой нейтральный элемент. Тогда имеем $e' = e \circ e' = e'$. ◄

2. Для любого $a \in G$ обратный элемент $b \in G$ определяется однозначно.

► Пусть b' — другой обратный элемент. Тогда $b' = b' \circ e = b' \circ (a \circ b) = (b' \circ a) \circ b = e \circ b = b$. ◄

3. Для любых a, b из группы G уравнения $a \circ x = b$ и $y \circ a = b$ имеют единственные решения $x = a^{-1} \circ b \in G$ и соответственно $y = b \circ a^{-1}$.

► Действительно, пусть x' и y' — другие решения соответственно. Тогда

$$a \circ x = b = a \circ x', \quad y \circ a = b = y' \circ a.$$

Отсюда находим

$$x = a^{-1} \circ a \circ x = a^{-1} \circ a \circ x' = x', \quad y = y \circ a \circ a^{-1} = y' \circ a \circ a^{-1} = y'. \blacktriangleleft$$

Непустое подмножество H группы G, замкнутое относительно операции $\circ$, называется подгруппой.

4. Нейтральные элементы (единицы) группы и любой ее подгруппы совпадают.

► Пусть e_G — единица в группе G и e_H — единица в любой ее подгруппе H. Тогда для любого элемента $h \in H$ имеем $he_H = h = he_G$. Отсюда находим $e_H = h^{-1}he_H = h^{-1}he_G = e_G$. ◄

5. Для того чтобы непустое подмножество H группы G было подгруппой группы G необходимо и достаточно, чтобы для любых двух элементов a и b из H элемент ab^{-1} принадлежал H.

► *Необходимость.* Для любых элементов $a, b \in H$ имеем $b^{-1} \in H$. Следовательно, $ab^{-1} \in H$.

Достаточность. Пусть для любых $a, b \in H$ элемент $ab^{-1} \in H$. Тогда при $a = b$ находим $e = aa^{-1} \in H$. Далее, при $a = e$ для любого $b \in H$ получим $b^{-1} \in H$, т.е. для любого элемента $b \in H$ существует обратный элемент b^{-1}. Ассоциативный закон в H очевидным образом выполняется. ◄

Пусть H — подгруппа группы G и для любого $a \in G$ определим множество aH, состоящее из элементов $ah, h \in H$. Оно называется левым смежным классом по подгруппе H группы G, а множество Ha — правым смежным классом.

6. Два правых (так же, как и левых) смежных класса Ha и Hb, где $f, b \in G$, либо не пересекаются, либо совпадают.

► Пусть $h_1a = h_2b$, где $h_1, h_2 \in H$. Тогда $h_1h_2^{-1} = ba^{-1}$. Следовательно, $ba^{-1} \in H$, и смежные классы Hba^{-1} и H совпадают, т.е.

$Hb = Ha$. В противном случае смежные классы Ha и Hb не пересекаются. Таким образом каждый элемент группы G принадлежит только одному смежному классу по подгруппе H, т.е. смежные классы дают разбиение группы G на классы. ◀

Порядком конечной группы называется число элементов в ней.

7. Пусть G — конечная группа. Тогда для любой ее подгруппы H порядок H делит порядок группы G.

▶ Обозначим символами $|G|$ и $|H|$ порядки групп G и H соответственно. По утверждению 6 все элементы группы G распределятся по правым смежным классам подгруппы H. Каждый класс содержит в точности $|H|$ элементов. Отсюда следует, что $|H| \mid |G|$. ◀

Группа G называется циклической, если найдется элемент a такой, что любой элемент $g \in G$ может быть представлен в виде $g = a^n$, где n — некоторое целое число, причем, если $n > 0$, то $a^n := \underbrace{a \circ \cdots \circ a}_{n}$, при $n < 0$ имеем $a^n = (a^{-1})^{-n}$, и $a^0 = e$. Элемент a называется образующей циклической группы G.

8. Всякая подгруппа циклической группы является циклической.

▶ Пусть a — образующая циклической группы, и пусть натуральное число k является наименьшим показателем степени элемента a таким, что элемент $b = a^k$ принадлежит подгруппе. рассмотрим любой элемент $c = a^m$ из подгруппы. Разделим число m остатком на k. Получим $m = kq + r, 0 \leqslant r < k$. Тогда $a^r = a^{m-kq} = a^m(a^k)^{-q}$ принадлежит подгруппе. Следовательно, $r = 0$. В противном случае показатель k не был бы минимальным. ◀

9. Пусть порядок группы равен простому числу. Тогда эта группа является циклической и любой, отличный от единицы элемент, является ее образующей.

▶ Поскольку порядок любого элемента группы является делителем порядка группы, он либо равен порядку группы (простое число), либо равен 1. В последнем случае этот элемент является единицей. В противном случае он является образующей циклической группы простого порядка. ◀

Взаимно однозначное отображение f группы G на группу G' называется изоморфизмом этих групп, а сами группы называются изоморфными, если для любых элементов a, b из G имеем $f(ab) = f(a)f(b)$. В частности, если G и G' совпадают, то отображение f

называется автоморфизмом группы G. Суперпозиция автоморфизмов как отображений является автоморфизмом.

10. Все автоморфизмы данной группы G образуют группу, называемую *группой автоморфизмов группы G.*

► Тождественное отображение G на себя задает единицу в группе автоморфизмов, а обратное отображение — обратный элемент. ◄

Пусть a — любой фиксированный элемент группы G. Тогда автоморфизм G, задаваемый для любого x из G соотношением $f(x) = axa^{-1}$, называется внутренним автоморфизмом. Все остальные автоморфизмы группы G называются внешними.

11. При внутреннем автоморфизме подгруппа H группы G переходит в подгруппу aHa^{-1}. Последняя подгруппа aHa^{-1} называется *сопряженной подгруппой* с подгруппой H.

► Множество $H' = aHa^{-1}$ "замкнуто" относительно операции умножения в группе H. Для любых $h_1, h_2 \in H$ имеем

$$ah_1a^{-1} \cdot ah_2a^{-1} = a(h_1h_2)a^{-1}.$$

Таким образом H' является группой. ◄

Подгруппа H называется нормальной (или инвариантной, или нормальным делителем) группы G, если для каждого $a \in G$ имеем $aH = Ha$; другими словами, для каждого $a \in G$ и для каждого $h \in H$ элемент $a^{-1}ha$ должен принадлежать H. В частности, любая подгруппа H, инвариантная относительно всех внутренних автоморфизмов является нормальной.

12. Пусть p — наименьшее простое число, делящее порядок n конечной группы G и H — ее подгруппа порядка n/p. Тогда H — нормальная подгруппа группы G.

► Возьмем любой элемент $a \in G$, не принадлежащий H. Тогда порядок элемента a равен p, поскольку элементы смежных классов $H, aH, a^2H, \ldots, a^{p-1}H$ должны исчерпывать всю группу G и число p является минимальным простым делителем порядка n группы G. Далее, пусть при некоторых k, l с условием $0 \leqslant k, l < p$ имеем $a^kH = Ha^l$. Возьмем единичный элемент в H. Получим $a^k = a^lh$, где h — некоторый элемент из H, т.е. $a^{k-l} \in H$ и $k = l$, так как в противном случае смежные классы a^kH и a^lH совпадали. ◄

13. На множестве $j_a = Ha$ правых (левых) смежных классов по нормальной подгруппе H группы G для любых $a, b \in G$ определим операцию $j_a \cdot j_b = j_{a \circ b}$. Относительно этой операции множество правых смежных классов будет группой. Ее называют факторгруппой

G по H и обозначают G/H.

► Элемент j_e будет единицей факторгруппы G/H, а элемент $j_{a^{-1}}$ является обратным к j_a. ◄

Пусть заданы две группы G_1 и G_2. Гомоморфным отображением или гомоморфизмом группы G_1 в группу G_2 называется отображение f, удовлетворяющее следующим условиям: если $a, b \in G_1$, то $f(ab) = f(a)f(b)$.

Прообраз единицы из G_2 называется ядром гомоморфизма.

14. При гомоморфизме группы G_1 на группу G_2 единица группы G_1 переходит в единицу группы G_2, и для любого элемента a группы G_1 его обратный элемент a^{-1} переходит в элемент $f^{-1}(a) \in G_2$.

► Для любого $g \in G$ имеем $f(g) = f(eg) = f(e)f(g)$, причем $g' = f(g)$ пробегает по всем $g' \in G_2$, если g пробегает по всем элементам группы G_1. Следовательно, $e' = f(e)$ — единица группы G_2. Далее имеем $e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1})$, т.е. $f^{-1}(a) = (f(a))^{-1}$. ◄

15. Образ группы G_1 при гомоморфизме группы G_1 в G_2 будет подгруппой группы G_2.

► Поскольку $f(gg') = f(g)f(g')$ для любых g, g' из G_1, все элементы образа $f(G_1)$ относительно операции в группе G_2 образуют "замкнутое" множество, т.е. $f(G_1)$ является группой. ◄

16. Ядро гомоморфизма является нормальной подгруппой группы G_1.

► Пусть $H \subset G_1$ ядро гомоморфизма $f : G_1 \to G_2$. Очевидно, H — подгруппа G_1, причем для любого $h \in H$ имеем $f(h) = e' \in G_2$.

$$a^{-1}Ha \subset H, \text{т.е.} H \subset aHa^{-1}.$$

Следовательно, $aHa^{-1} = H$, и H является нормальной подгруппой группы G_1. ◄

Гомоморфизм группы G_1 на группу G_2, который является взаимно однозначным отображением, будет изоморфизмом групп G_1 и G_2.

17. Для того чтобы гомоморфизм f группы G_1 в группу G_2 являлся изоморфизмом необходимо и достаточно, чтобы ядро гомоморфизма f состояло только из единицы группы G_1.

► Пусть гомоморфизм f является изоморфизмом групп G_1 и G_2. Тогда его ядро, которое является нормальной подгруппой G_1, состоит только из единицы G_1.

Пусть, теперь, ядро гомоморфизма $f : G_1 \to G_2$ состоит только из единицы G_1. Предположим, что существуют такие $g, g' \in G_1$,

для которых $f(g) = f(g')$, т.е. $f(gg'^{-1}) = e' \in G_2$. Так как ядро гомоморфизма состоит только из единицы G_1, то $g = g'$. Значит, отображение f является взаимно однозначным, т.е. гомоморфизм групп является их изоморфизмом. ◄

18. Пусть f является изоморфизмом группы G_1 на группу G_2. Тогда f^{-1} является изоморфизмом группы G_2 на группу G_1.

► Отображение f является взаимно однозначным, поэтому определено f^{-1}, и f^{-1} — гомоморфизм G_2 на G_1. ◄

19. Гомоморфный образ (абелевой) коммутативной группы будет коммутативной группой.

► Имеем $f(g)f(g') = f(gg') = f(g'g) = f(g')f(g)$, где f — гомоморфизм коммутативной группы, а g, g' — любые элементы этой группы. ◄

Гомоморфизм группы G в себя называется эндоморфизмом группы G; изоморфизм группы G на себя называется автоморфизмом группы G.

Группа G называется абелевой, если для любых $a, b \in G$ выполняется коммутативный закон: $a \circ b = b \circ a$.

20. Любая конечная группа порядка, не превосходящего 5, абелева.

► Группы порядков $2, 3, 5$ являются циклическими, а групп порядка 4 ровно две: циклическая и группа с образующими a, b второго порядка: $a^2 = e, b^2 = e, ab = ba$, т.е. во втором случае группа четвертого порядка является прямым произведением циклических групп второго порядка. ◄

Наименьшее число $n \in \mathbf{N}$ называется показателем группы G, если для любого $x \in G$ имеем $x^n = 1$.

21. Пусть G — конечная абелева группа порядка m, имеющая показатель n. Тогда найдется натуральное число k такое, что m делит n^k.

► Индукция по величине порядка m. При $m = 1$ утверждение очевидно верно. Предположим, что утверждение для всех групп порядка, меньшего m. Докажем его для групп порядка m. Возьмем любой элемент $b \in G$, отличный от единицы. Пусть H обозначает циклическую группу, порожденную элементом b, H — подгруппа G и $b^n = e$. Следовательно, $|H|$ делит n. Для факторгруппы G/H число n также является показателем. По предположению индукции найдется число r такое, что порядок группы $|G/H|$ является делителем n^r. Так как $|G| = |G/H| \cdot |H|$, то $|G|$ делит n^{r+1}. ◄

Конечная группа G называется p-группой, если ее порядок равен степени простого числа p.

22. Пусть G — конечная абелева группа порядка m и простое число p делит m. Тогда G содержит подгруппу порядка p.

▶ Так как показатель группы равен n, то найдется элемент $x \in G$ такой, что m делит некоторую степень n. Следовательно, p делитель числа n, т.е. $n = ps$. Отсюда имеем, что циклическая группа с образующей x^s имеет порядок p. ◀

23. Пусть G — конечная группа. Тогда

$$|G| = \sum_{a \in C} (G : G_a),$$

где a пробегает множество C представителей различных классов сопряженных элементов.

▶ Зафиксируем любой элемент a группы G. Рассмотрим множество сопряженных с a элементов gag^{-1}, где $g \in G$. Заметим сразу, что два сопряженных элемента gag^{-1} и hah^{-1} равны между собой тогда и только тогда, когда элемент $g^{-1}h$ перестановочен с a. Действительно, если

$$gag^{-1} = hah^{-1}, \quad \text{то} \quad g^{-1}ha = ag^{-1}h,$$

и наоборот, если $g^{-1}h$ перестановочен с a, т.е. $g^{-1}ha = ag^{-1}h$, то $gag^{-1} = hah^{-1}$. Пусть G_a обозначает множество всех элементов $g \in G$, перестановочных с a. Оно является группой и называется *нормализатором элемента a в G.*

Элемент h лежит в смежном классе gG_a тогда и только тогда, когда $g^{-1}h \in G_a$. Таким образом, для каждого смежного класса gG_a установлено взаимно однозначное соответствие с gag^{-1}, сопряженным с a. Следовательно, число различных сопряженных с a элементов равно числу смежных классов по подгруппе G_a, т.е. равно индексу $(G : G_a)$ группы G_a в группе G. ◀

Центром $Z = Z(G)$ группы G называется множество всех таких элементов $z \in G$, что для любого $g \in G$ имеем $xgx^{-1} = g$. Очевидно, $Z(G)$ является нормальной подгруппой в G.

24. Пусть p — простое число, n — натуральное число и группа G состоит из p^n элементов. Тогда ее центр не может состоять из одного единичного элемента.

▶ Для любой подгруппы G_a по теореме Лагранжа имеем $(G : G_a) = p^t, t \geqslant 0$, причем $t = 0$ только для элементов центра. Следовательно, по предыдущему утверждению $|G| = |Z(G)| + pm$, где

m — некоторое неотрицательное целое число. Отсюда имеем, что число элементов в центре $Z(G)$ делится на p. ◄

Конечная группа, состоящая из p^n элементов, где p — простое и n — натуральное число, называется p-группой.

25. Пусть p — простое число и группа G состоит из p^2 элементов. Тогда G является абелевой группой, задаваемая следующими определяющими соотношениями: либо 1) циклическая, $a^{p^2} = 1$; либо 2) элементарная абелева, $a^p = 1, b^p = 1, ab = ba$.

► Центр $Z(G)$ либо совпадает с G, либо $|Z(G)| = p$ (по предыдущей задаче центр — не тривиален). Если $|Z(G)| = |G|$, то группа G — абелева и если в ней найдется элемент порядка p^2, то она является циклической. В противном случае все элементы, исключая единицу, имеют порядок p. Таким образом, как и в случае $|Z(G)| = p$, найдется нормальная подгруппа H порядка p. Тогда $|G/H| = p$ и группа G/H является циклической, а группа G изоморфна прямому произведению H и G/H. ◄

Пусть p^n — наибольшая степень простого числа p, делящая порядок группы G. Тогда ее подгруппа H порядка p^n называется силовской p-подгруппой.

Утверждения следующих двух задач называются *теоремами Силова.*

26. Пусть G — конечная группа и p — простое число, делящее порядок группы. Тогда в G существует силовская p-подгруппа.

► Пусть $|G| = n = p^k m, (p, m) = 1$. Проведем "двойную" индукцию по величине чисел $m \geqslant 1$ и $k \geqslant 1$. При $m = 1$ утверждение задачи верно для любого натурального числа k. Пусть, теперь, $k = 1$. Тогда $|G| = n = pm, (p, m) = 1$. Проведем индукцию по $m \geqslant 1$. Утверждение верно при $m = 1$. Пусть $m > 1$. Возможны два случая. 1). Порядок центра $|Z(G)|$ делится на p. Так как $Z(G)$ абелева группа, то по утверждению задачи 22 в ней существует циклическая подгруппа H. Она будет силовской p-группой в $Z(G)$ и в G. 2) Порядок центра $|Z(G)|$ взаимно прост с p. Тогда порядок факторгруппы $G/Z(G)$ делится на p. По предположению индукции в $G/Z(G)$ существует силовская p-группа. Она будет силовской p-группой в G. База индукции по параметрам m, k рассмотрена.

Предположим, что утверждение справедливо для любых пар (m, k) таких, что $m < s, k \leqslant t$ и $m \leqslant s, k < t$.

Докажем его при $m = s, k = t$. Имеем две возможности: 1) существует элемент $x \in G, x \notin Z(G)$ такой, что $(G : G_x)$ взаимно прост с p; 2) для любого $x \in G, x \notin Z(G)$ индекс подгруппы G_x делится на

p.

В случае 1) имеем, что $|G| = n = p^k s, |G_x| = p^k r, 1 \leqslant r < s$, и силовская p-подгруппа в G_x является силовской подгруппой в G. К группе G_x применимо предположение индукции. Тем самым в случае 1) имеется для группы G силовская p-группа.

Рассмотрим случай 2). Из утверждения задачи 23 находим, что $|Z(G)|$ делится на p. По утверждению задачи 22 в группе $Z(G)$ существует циклическая подгруппа H порядка p. Поскольку H подгруппа нормальной подгруппы $Z(G)$ в G, подгруппа H является нормальной в G. Следовательно, существует факторгруппа G/H и $|G/H| = p^{k-1}s$. Пусть K' силовская p-группа в G/H, и пусть $K = f^{-1}(K')$, где $f : G \to G/H$ — канонический гомоморфизм. Тогда H — нормальная подгруппа в K и группа K/H изоморфна K'. Следовательно, порядок группы K равен $p^{k-1} \cdot p = p^k$ и она является силовской p-группой в G. ◀

27. Пусть G — конечная и p — простое, делящее порядок группы. Тогда

а) каждая p-подгруппа содержится в некоторой силовской p-группе;

б) все силовские p-подгруппы сопряжены;

в) количество силовских p-подгрупп n_p является делителем порядка группы G и число n_p сравнимо с 1 по модулю p.

▶ а). Пусть $|G| = p^k m, (p, m) = 1, k \geqslant 1$, и пусть H — любая p-подгруппа группы $G, |H| = p^l, l \leqslant k$. Очевидно, утверждение а) верно при $m = 1$. Пусть $m > 1$. По утверждению задачи 26 в G найдется силовская p-подгруппа S порядка p^k. Рассмотрим множество различных левых классов смежности $M = \{xS : x \in G.\}$ Их число равно $|M| = |G|/|H| = m$, и оно взаимно просто с p.

Далее, рассмотрим действие группы H на множестве левых смежных классов M, т.е. умножение любого элемента $h \in H$ на правый смежный класс xS подгруппы S. Эта операция умножения введена корректно, поскольку для совпадающих классов xS и $x'S$ в результате умножения на элемент $h \in H$ получим $hxS = hx'S$. Действительно, из условия $xS = x'S$ имеем $x = x's, hx = hx's$, т.е. $hxS \subset hx'S$, и наоборот, равенство $x' = xs'$ дает, что $hx'S \subset hxS$.

Для каждого элемента $x \in G$ множество HxS состоит из конечного числа непересекающихся классов $h_1xS, \ldots, h_rxS$, которые образуют орбиту точки xS с числом элементов $r = r(x)$. Число r — элементов орбиты, является делителем числа элементов p^l подгруппы H. Таким образом, если $r > 1$, то r делится на p.

Далее, применяя задачу 23 к группе S, находим, что существуют $x \in G$ такие, что орбита точки xS будет одноэлементной, т.е. $HxS = xS$. В самом деле, число элементов в S взаимно просто с p, а в каждой неодноэлементной орбите число элементов делится на p, и число элементов во всех орбитах должно совпадать с числом элементов группы S. Следовательно, $Hx \subset xS$ и $H \subset xSx^{-1}$, т.е. p-подгруппа H содержится в подгруппе, сопряженной с силовской p-подгруппой S. Поскольку $|xSx^{-1}| = |S| = p^k$, подгруппа xSx^{-1} является силовской p-подгруппой.

б). Пусть H в п. а) является силовской p-подгруппой. Тогда по доказанному H является подгруппой некоторой сопряженной силовской p-подгруппы xSx^{-1} с тем же числом элементов p^k, т.е. все силовские p-подгруппы сопряжены.

в). Из утверждения п. б) следует все силовские подгруппы образуют одну из орбит действия с помощью сопряжений в G на одну из силовских p-подгрупп, т.е. орбита будет состоять из n_p элементов. Так как все орбиты не пересекаются и имеют одно и то же число элементов, то число n_p делит число $|G|$.

Далее, пусть $\Sigma = \{S_1, \ldots, S_{n_p}\}$ — множество всех различных силовских p-подгрупп в G, и пусть $S = S_1$. Рассмотрим действие сопряжениями элементов из S на подгруппы из Σ, т.е. рассматриваем aS_ka^{-1} для любого $a \in S$ и для любого $S_k \in \Sigma$.

Подгруппа S будет единственной неподвижной точкой относительно указанного действия сопряжениями, т.е. для любого $a \in S$ имеем $aSa^{-1} = S$. Докажем это утверждение от противного. Пусть существует $S' = S_k, k \neq 1$ такое, что для всех $a \in S$ справедливо соотношение $aS' = S'$. Это означает, что $S'S = SS'$. Следовательно, множество $H = S'S$ является подгруппой в G и $S, S' \trianglelefteq H$ силовские p-подгруппы в H. По утверждению б) находим, что существует $h = ss' \in H, s \in S, s' \in S'$ такой, что $S = hS'h^{-1}$. Следовательно,

$$S = hS'h^{-1} = (ss')S'(ss')^{-1} = s(s'S'(s')^{-1})s^{-1} = sS's^{-1} = S'.$$

Равенство $S = S'$ противоречит тому, что в Σ все подгруппы различны. Таким образом, для любой подгруппы $S' \neq S$ из Σ ее орбита в S является одноэлементной. Число элементов в ней делит порядок p^k группы S. Стало быть, число элементов орбиты делится на p. Тем самым доказано, что $n_p \equiv 1 \pmod{p}$. ◀

28. Пусть p — простое число, n — натуральное число и группа G состоит из p^n элементов. Тогда для любого натурального $l \leqslant n$ найдется подгруппа группы G, состоящая из p^l элементов.

▶ Индукция по n. Утверждение верно при $n = 1$ (задача 22). Пусть оно имеет место для $n < k$. Докажем его для $n = k$. Центр $Z(G)$ группы G является нормальной p-подгруппой группы G и нетривиален, т.е. состоит из $p^r, r \geqslant 1$, элементов. Из утверждения задачи 22 следует, что существует циклическая подгруппа H порядка p группы $Z(G)$, причем H является нормальной подгруппой G. Рассмотрим факторгруппу G/H. Она состоит из p^{k-1} элемента и к этой факторгруппе применимо предположение индукции. Следовательно, в ней существует подгруппа H' из p^{l-1} элемента. Отсюда имеем, что группа $G_0 = H \times H'$ является искомой. ◀

29. Описать все группы шестого порядка.

▶ Имеется две группы шестого порядка: циклическая и неабелева группа с образующими $a^2 = e, b^3 = e$. Она состоит из элементов e, a, b, b^2, ab, ba. ◀

30. Всякая группа порядка 15 — циклическая.

▶ Из утверждения задачи 27 в) имеем, что количества силовских 3- и 5-подгрупп удовлетворяют условиям

$$n_3 \mid 15, n_3 \equiv 1 \pmod 3), n_5 \mid 15, n_5 \equiv 1 \pmod 5).$$

Следовательно, $n_3 = 1, n_5 = 1$. Это означает, что силовские 3- и 5-подгруппы H_3 и H_5 соответственно являются нормальными в группе G из 15 элементов. Отсюда находим, что множество H_3H_5 — подгруппа группы G. Далее, $H_3 \cong \mathbf{Z_3}, H_5 \cong \mathbf{Z_5}$. Тем самым получаем, что $H_3 \cap H_5 = \{e\}$ и $H_3H_5 = H_3 \times H_5$ — прямое произведение групп и оно состоит из 15 элементов. Таким образом имеем

$$G = H_3H_5 = H_3 \times H_5 \cong \mathbf{Z_3} \oplus \mathbf{Z_5} \cong \mathbf{Z_{15}},$$

т.е. группа порядка 15 — единственная и она является циклической. ◀

31. Пусть p, q — различные простые числа, G — конечная группа порядка $n = pq$ и $(n, \varphi(n)) = 1$. Тогда группа G — циклическая.

▶ Из утверждения п. в) задачи 27 следует, что

$$n_p \mid n, n_p \equiv 1 \pmod p), n_q \mid n, n_q \equiv 1 \pmod q).$$

Отсюда имеем $n_p \not| p, n_p \mid q$ и $n_q \not| q, n_q \mid p$. Тем самым $n_p = 1$ или $n_p = q$, а $n_q = 1$ или $n_q = p$.

Далее, из условия $(n, \varphi(n)) = 1$, где $\varphi(n) = (p-1)(q-1)$, находим $q \not\equiv 1 \pmod p)$ и $p \not| 1 \pmod q)$. С другой стороны из утверждения

п. в) задачи 27 при условии $n_p = q$ или $n_q = p$ получаем, что $q \equiv 1 \pmod{p}$ или соответственно $p \equiv 1 \pmod{q}$. Таким образом количество n_p силовских p-подгрупп равно 1 и $n_q = 1$ и они нормальны в G. Эти силовские подгруппы изоморфны $\mathbf{Z}_p$ и $\mathbf{Z}_q$. Следовательно, $G \cong \mathbf{Z}_p \oplus \mathbf{Z}_q \cong \mathbf{Z}_{pq} = \mathbf{Z}_n$. Тем самым единственность группы указанного порядка доказана. ◀

32. Пусть p, q, r — три различных простых числа, G — конечная группа порядка $n = pqr$ и $(n, \varphi(n)) = 1$. Тогда группа G — циклическая.

▶ Из п. в) задачи 27 имеем

$$n_p \mid n, n_p \equiv 1 \pmod{p}, n_q \mid n, n_q \equiv 1 \pmod{q}, n_r \mid n, n_r \equiv 1 \pmod{r}.$$

Следовательно,

$$n_p \mid qr, n_q \mid pr, n_r \mid pq.$$

Отсюда находим, что возможны следующие случаи:

$$n_p = 1, q, r, qr; n_q = 1, p, r, pr; n_r = 1, p, q, pq.$$

Из условия $(n, \varphi(n)) = 1$ получаем $p \not\equiv 1 \pmod{q}, p \not\equiv 1 \pmod{r}$, а также $q \not\equiv 1 \pmod{p}, q \not\equiv 1 \pmod{r}$, и $r \not\equiv 1 \pmod{p}, r \not\equiv 1 \pmod{q}$. Рассмотрим сначала случай силовских p-подгрупп. В силу симметрии остальные случаи рассматриваются аналогично.

1). Пусть n_p равно q или r. Имеем $n_p = q \equiv 1 \pmod{p}$, что противоречит условию $q \not\equiv 1 \pmod{p}$, найденному выше. Следовательно, $n_p \neq q$. По аналогичной причине $n_p \neq r$.

2). Пусть $n_p = qr$. Тогда $qr \equiv 1 \pmod{p}, (q-1)(r-1) \not\equiv 1 \pmod{p}$. Эта система соотношений противоречива. Следовательно, $n_p \neq qr$.

Таким образом доказано, что $n_p = 1, n_q = 1, n_r = 1$. Значит, все силовские p-, q- и r-подгруппы нормальны в G, изоморфны соответственно $S_p \cong \mathbf{Z}_p, S_q \cong \mathbf{Z}_q, S_r \cong \mathbf{Z}_r$.

По доказанному в задаче 32 имеем $G/S_p \cong \mathbf{Z}_q \oplus \mathbf{Z}_r$. Следовательно, $G \cong \mathbf{Z}_p \oplus \mathbf{Z}_q \oplus \mathbf{Z}_r \cong \mathbf{Z}_n$. ◀

33. Для того чтобы существовала единственная конечная группа G порядка n необходимо и достаточно, чтобы $(n, \varphi(n)) = 1$, где $\varphi(\cdot)$ — функция Эйлера.

▶ *Достаточность.* Имеем $(n, \varphi(n)) = 1$. Следовательно, n — бесквадратное число, т.е. $n = p_1 \dots p_s$ — произведение s различных простых чисел. Проведем доказательство методом математической

индукции по параметру s. При $s = 1$ утверждение верно: $G \cong \mathbf{Z}_{p_1}$. Предположим, что оно верно при $s < t$.

Докажем его справедливость при $s = t$. Рассмотрим центр $Z(G)$ группы G. Имеется две возможности: 1) $Z(G)$ — не тривиален, т.е. $Z(G) \neq \{e\}$, 2) $Z(G) = \{e\}$. В случае 1) находим, что $Z(G)$ — нормальная подгруппа, порядок которой делит порядок группы G, равный n, и больше 1. Следовательно, найдется простое число p, являющееся делителем порядка группы $Z(G)$. Из утверждения задачи 22 найдется циклическая подгруппа H порядка, скажем, $p = p_t$ группы $Z(G)$, которая также является нормальным делителем группы G. Следовательно, факторгруппа G/H имеет порядок, являющийся произведением $t-1$ различных простых чисел. К этой факторгруппе применимо предположение индукции, т.е. $G/H \cong \mathbf{Z}_{p_1} \oplus \cdots \oplus \mathbf{Z}_{p_{t-1}}$. Таким образом $G \cong G/H \oplus H \cong \mathbf{Z}_{p_1} \oplus \cdots \oplus \mathbf{Z}_{p_{t-1}} \oplus \mathbf{Z}_{p_t}$, и в случае 1) единственность установлена.

Рассмотрим случай 2): $Z(G) = \{e\}$, т.е. центр $Z(G)$ тривиален. Докажем, что этот случай не реализуется. Воспользуемся утверждением задачи 23 о разбиении группы G на классы сопряженных элементов. Получим

$$n = |G| = |Z(G)| + \sum_{g \in C} (G : G_g) = 1 + \sum_{g \in C} \frac{n}{n_g}.$$

◀

II. Кольца

Множество K называется кольцом, если на нем заданы две бинарные операции: "$+$"(сложение) и "$\times$"(умножение), удовлетворяющие следующим условиям:

1) множество K — абелева группа по сложению;

2) операция умножения ассоциативна, т.е. для любых $a, b, c \in K$ имеем

$$a \times (b \times c) = (a \times b) \times c;$$

3) имеет место дистрибутивный закон, т.е. для любых $a, b, c \in K$ имеем

$$a \times (b + c) = a \times b + a \times c, (a + b) \times c = a \times c + b \times c.$$

В дальнейшем для удобства будем писать ab вместо $a \times b$. Нейтральный элемент абелевой группы по сложению обозначим через

0 и называть нулем, а нейтральный элемент по умножению — через 1 и называть единицей кольца K. Если кольцо состоит не только из 0, то будем предполагать, что $1 \neq 0$.

Элемент $a \in K$ называется левым (правым) делителем 0, если существует элемент $b \in G$, отличный от нуля, и такой, что $ab = 0$ (или $ba = 0$). Делитель нуля $a \in G$ называется также собственным делителем нуля, если $a \neq 0$. Кольцо K, не имеющее собственных делителей, называется кольцом без делителей нуля.

Непустое подмножество R кольца K подкольцом кольца K, если относительно кольцевых операций сложения и умножения кольца K оно является кольцом.

1. Непустое подмножество R кольца K будет подкольцом тогда и только тогда, когда выполняются следующие условия:
а) если $a, b \in R$, то $a - b \in R$;
б) множество R замкнуто относительно операции умножения, т.е. для любых $a, b \in R$ имеем $ab \in R$;

Кольцо K называется коммутативным, если операция умножения в K коммутативна, т.е. для любых $a, b \in G$ имеем $ab = ba$.

Коммутативное кольцо с единицей, не имеющее делителей нуля, называется областью целостности.

Глава VII

Л.ЭЙЛЕР — ОСНОВАТЕЛЬ СОВРЕМЕННОЙ ТЕОРИИ ЧИСЕЛ

Оригинальные проблемы, решенные и поставленные Л. Эйлером, явились основополагающими направлениями развития современной теории чисел. Эту мысль впервые прекрасно выразил П. Л. Чебышёв во введении к своей диссертации "Теория сравнений". Он писал:

"Эйлером положено начало всех изысканий, составляющих общую часть теории чисел. В этих изысканиях Эйлеру предшествовал Фермат; он первый начал заниматься исследованием свойств чисел в отношении их способности удовлетворять неопределенным уравнениям того или другого вида, и результатом его изысканий было открытие многих общих теорем теории чисел. Но изыскания этого геометра не имели непосредственного влияния на развитие науки: его предложения остались без доказательств и без приложений. В этом состоянии открытия Фермата служили только вызовом геометров на изыскания в теории чисел. Но несмотря на весь интерес этих изысканий, до Эйлера на них никто не вызывался. И это понятно: эти изыскания требовали не новых приемов, открытия новых начал, одним словом основания новой науки. Это сделано было Эйлером."

В 1849 г. В. Я. Буняковский и П. Л. Чебышёв подготовили к изданию "Собрание арифметических сочинений" Л. Эйлера [**?**], к которому они составили "Систематический указатель" его работ по теории чисел.

Все эти работы они разбили на 4 раздела. Приведем полностью их классификацию работ.

1. Делимость чисел.

а). Целые числа в связи с их разложением на множители; количество целых чисел, взаимно простых с некоторым целым числом и меньшим, чем оно; сумма делителей чисел; дружественные числа.

б). Делимость различных выражений.

в). Теория вычетов и квадратичные вычеты.

2. Разложение чисел на суммы различных форм.
а). Разложение чисел на квадраты, на треугольные числа и на члены, пропорциональные квадратам.
б). Разбиение чисел.
3. Диофантов анализ.
а). Определение двух или нескольких неизвестных, заданных одним уравнением; невозможные уравнения.
б). Определение нескольких неизвестных, заданных двумя уравнениями.
в). Определение нескольких неизвестных, заданных тремя уравнениями.
г). Определение нескольких неизвестных, заданных четырьмя уравнениями.
д). Определение нескольких неизвестных, заданных более чем четырьмя уравнениями.
е). Неопределенные задачи, которые приводят к числу уравнений, большему чем число неизвестных.
4. Смесь.
Сюда были отнесены другие арифметические работы, не включенные в предыдущие разделы.

Кроме того, Эйлер дал решения ряда задач математического анализа, использующие непрерывные дроби, получил разложение в непрерывную дробь числа $\frac{e-1}{2}$, нашел первое обобщение алгоритма непрерывных дробей. Эйлеру принадлежат первые постановки задач, касающихся трансцендентных чисел.

Эйлер подготовил таблицы натуральных чисел со специальными арифметическими свойствами. В частности, опираясь на собственную модификацию метода решета Эратосфена, он составил таблицы простых чисел.

Далее приведем разделы современной теории чисел, в которых результаты и направления исследований Л. Эйлера получили фундаментальное развитие в новое время.

§ 1. Элементарная теория чисел

В основе этого раздела арифметики лежат вопросы, связанные с делимостью и простотой натуральных чисел. Они постоянно привлекают внимание человечества со времен Пифагора. Среди них — совершенные числа, привлекшие внимание людей в христианскую эру.

1. *Критерий четного совершенного числа.*

Пусть $\sigma(n) = \sum\limits_{d|n}$ обозначает сумму всех делителей натурального числа n. Число n называют совершенным, если $\sigma(n) = 2n$. Например, совершенными числами являются $6 = 1 + 2 + 3$ и $28 = 1 + 2 + 4 + 7 + 14$.

Критерий четного совершенного числа. Пусть $p = 2^n - 1$ — простое число. Тогда

$$\frac{1}{2}p(p+1) = 2^{n-1}(2^n - 1)$$

совершенное число. Более того, каждое четное совершенное число имеет эту форму.

Необходимость (*Евклид*). Имеем

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

Достаточность (*Эйлер*"De numeris amicabilibus", Comm. Arithm., 1849, **2**, 630). Пусть a — любое четное совершенное число. Тогда его можно представить в виде $a = 2^{n-1}b,\ b > 1, 2 \not| b$. Далее имеем

$$2a = 2^n b = \sigma(a) = \sigma(2^{n-1})\sigma(b) = (2^n - 1)\sigma(b).$$

Следовательно

$$\sigma(b) = \frac{2^n b}{2^n - 1} = b + \frac{b}{2^n - 1}.$$

Таким образом b и $b/(2^n - 1)$ делители числа b. Поскольку $\sigma(b)$ сумма всех делителей числа b, делители числа исчерпываются двумя делителями: b — простое число и $b/(2^n - 1) = 1$. Теорема доказана.

Отметим, что еще в 1638 г. Р. Декарт утверждал, что он может доказать приведенный выше критерий совершенного числа, и что каждое нечетное совершенное число имеет вид ps^2, где p — простое число.

Эйлеру принадлежит следующая гипотеза.

Если существуют нечетные совершенные числа, то они имеют вид

$$(4m+1)^{4n+1}x^2,$$

где $4m+1$ *— простое число,* x *— нечетное число и* $4n+1$ *— натуральное число.*

2. *Числа Мерсенна.*

Простые числа M_p вида $2^p - 1$, где p — простые числа, называются простыми числами Мерсенна. Эйлер знал, что M_p простое число при $p = 2, 3, 5, 7, 13, 19, 31$. На август 1999 г. было известно 38 простых чисел Мерсенна при

$$p = 2, 3, 5, 7, 13, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281,$$

$$3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497,$$

$$1257787, 1398269, 3021377, 6972593$$

(последнее 38-е простое число Мерсенна $M_{6972593}$ имеет 2098960 в десятичной записи).

Имеется предположение, что простых чисел Мерсенна бесконечно много. С другой стороны, существует гипотеза, что при $x \to \infty$ справедливо предельное соотношение

$$\frac{\pi_M(x)}{\pi(x)} \to 0,$$

где $\pi(x)$ — количество простых чисел, не превосходящих x и $\pi_M(x)$ — количество простых чисел Мерсенна с индексом, не превосходящим x.

В направлении второй гипотезы в подобной задаче о количестве $\pi_K(x)$ простых чисел Каллена вида $n2^n + 1$, $n \leqslant x$, К. Хооли доказал, что при $x \to \infty$ имеем $\pi_K(x)/x \to 0$. Эти исследования Хооли продолжила выпускница механико-математического факультета МГУ им. М.В.Ломоносова А. Мильуоло, которая доказала, что при $x \to \infty$ справедливо соотношение

$$\frac{\pi_C(x)}{\pi(x)} \to 0,$$

где $\pi_C(x)$ — количество простых чисел вида $2^p - p$ (или $2^p + p$) при условии, что простые числа p не превосходят x.

3. *Числа Ферма*

Числа F_n вида $2^{2^n} + 1$ называются числами Ферма. П. Ферма предполагал, что для любого неотрицательного целого n числа F_n являются простыми. Это в самом деле так при $n = 0, 1, 2, 34$. Первые пять простых чисел Ферма имеют вид

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537.$$

Но Эйлер в своей первой работе по теории чисел"Observationes de theoremate quodam Fermationo, aliisque ad numeros primos spectantibus" (1732, Comm. ar. coll., t.1, p.1) показал, что $2^{2^5}+1$ делится на 641. Действительно, указанная делимость следует из цепочки равенств и сравнений

$$5\cdot 2^7+1=641, \qquad 5\cdot 2^8\equiv -2 \pmod{641},$$

$$5^4\cdot 2^{32}\equiv (-2)^4 \pmod{641}, \qquad 5^4+2^4=641.$$

При этом Эйлер доказал, что форма вида $a^{2^m}+b^{2^m}$ не может иметь других делителей, кроме тех, которые имеют вид $2^{m+1}n+1$. В частности, при $a=2, b=1$ отсюда имеем, что делитель числа $2^{2^m}+1$ может иметь делителями только числа вида $2^{m+1}n+1$.

На сегодняшний день найдено много составных чисел Ферма, но кроме F_0, F_1, F_2, F_3, F_4 простых чисел Ферма отыскать не удалось. Поэтому в противоположность предположению Ферма существует современная гипотеза о том, что простых чисел Ферма конечное число. Эта гипотеза противоречит факту "случайности" в законе распределения простых чисел в последовательности $F_n,\ n\geqslant 0$.

Было бы интересно доказать, что при $x\to\infty$ справедливо соотношение

$$\frac{\pi_F(x)}{x}\to 0,$$

где $\pi_F(x)$ — количество простых чисел Ферма F_n при $x\to\infty$.

Как показал Гаусс простые числа Ферма тесным образом связаны с построением циркулем и линейкой правильных многоугольников. Он перечислил все n-угольники при $n<300$, для которых возможно такое построение.

4. *Числа, представимые в виде суммы квадратов.*

Утверждение о том, что любое простое число вида $4n+1$ имеет давнюю историю, идущую от Диофанта, Баше, Жирара, Ферма. Впервые в 1742 г. Эйлер обсуждает проблемы представимости чисел в виде суммы двух квадратов в письмах к Х. Гольдбаху [**?**, 96, 107-111].

Отправной точкой этих обсуждений явилось утверждение о разложении чисел на простые сомножители.

Пусть число $4n+1$ — составное. Тогда либо оно не является суммой двух квадратов целых чисел, либо оно представляется суммой двух квадратов натуральных чисел более чем одним способом.

В 1751 г. Л. Эйлер [**?**, 35–49, 204] дает следующие утверждения.
1. Пусть число представимо в виде суммы двух квадратов взаимно простых чисел. Тогда его простыми делителями могут быть только числа 2 и простые числа вида $4n+1$.
2. Любое простое число вида $4n+1$ представимо в виде суммы двух квадратов целых чисел и притом одним способом.
3. Сумма двух квадратов взаимно простых чисел не делится на любое простое число вида $4n+1$.
4. Пусть простое число вида $4n+1$ представлено формой $4n+1 = p^2+q^2$, причем известны целые числа f и g такие, что $pg-qf = \pm 1$. Тогда $a \equiv pf+qg \pmod{4n+1}$ является решением сравнения $a^2+1 \pmod{4n+1}$.

В 1730 г. Эйлер в письме к Гольдбаху рассматривает задачу о представлении натурального числа в виде суммы четырех квадратов целых чисел. Первое утверждение, доказанное Эйлером было о том, что каждое рациональное число представляется в виде суммы четырех квадратов рациональных чисел.

Далее он представлял в виде четырех целых квадратов числа вида $(a^2+b^2+c^2+d^2)(p^2+q^2), (a^2+b^2+c^2+d^2)(p^2+q^2+r^2), (a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2)$. Для последнего выражения Эйлер получил тождество, легшее в основу теории кватернионов

$$(a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2) =$$
$$= (ap+bq+cr+ds)^2+(bp-aq+dr+cs)^2+$$
$$+(cp-dq-ar+bs)^2+(dp+cq+br-as)^2.$$

В 1770 г. Ж.Лагранж, продолжая исследования Эйлера, доказал теорему о четырех квадратах целых чисел. В 1773 г. Эйлер упростил доказательство Лагранжа [**?**, 538–548].

5. *Элементарное доказательство последней теоремы Ферма* в случае уравнений $x^3+y^3=z^3$ и $x^4+y^4=z^4$.

§ 2. Теория сравнений по модулю натурального числа

1. *Критерий Эйлера квадратичного вычета и понятие первообразного корня по простому модулю.* “Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia” (1772, Comm. ar. coll., t.1, p.516)

2. *Функция Эйлера* $\varphi(n)$ и сравнение $a^{\varphi(n)} \equiv 1 \pmod{n}$. “Theoremata arithmetica nova methodo demonstrata” (1753, Comm. ar. coll., t.1, p.274, см. также работу LII в т. 2).

3. *О совпадении количества решений квадратного диофантова уравнения от двух переменных и количества решений квадратичного сравнения по некоторому модулю.*

Количество решений уравнения $x^2 + y^2 = n$ и количество решений сравнения $\nu^2 \equiv -1 \pmod{n}$ равны между собой.

4. *Разложение больших чисел на простые сомножители.*

Пусть $N = 4n + 1$. Для того чтобы N было простым числом необходимо и достаточно, чтобы число N единственным образом представлялось в виде суммы квадратов двух натуральных чисел, $N = x^2 + y^2, x < y$ (работы XII, XV, Comm. ar. coll., t.1). В частности, Эйлер показывает, что число

$$1000009 = 3^2 + 1000^2 = 235^2 + 972^2$$

является составным.

Подобные теоремы Эйлер доказывает для чисел, представимых в виде $x^2 + 2y^2$ или $x^2 + 3y^2$ (работы VI, XIII, XXI, LIV, LV, LXVII Comm. ar. coll., t.1, 2).

Числа $k = \alpha\beta$ Эйлер назвал удобными числами, если только простые числа единственным образом представляются в виде $\alpha x^2 + \beta y^2, x < y$.

§ 3. Аддитивная теория чисел

Сюда Эйлер относит следующие проблемы:

1. *Разбиение натуральных чисел на натуральные слагаемые.*

2. *Проблема Варинга.*

3. *Бинарная и тернарная проблемы Гольдбаха — Эйлера.*

В частности, при решении проблемы Варинга Эйлер отмечает интересное свойство, которое в дальнейшем неоднократно использовалось многими авторами.

Пусть $1 < X < u, v < 2X,\ u - v \geqslant 1$. Тогда $u^n - v^n > X^{n-1}$.

§ 4. Мультипликативная теория чисел

1. *Тождество Эйлера в теории простых чисел.*

Эйлер вводит в рассмотрение следующую функцию, с которой связывает бесконечное произведение, получившее название эйле-

ровского произведения:

$$\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_p\left(1-\frac{1}{p^s}\right)^{-1}=\left(\sum_{d=1}^{\infty}\frac{\mu(d)}{d^s}\right)^{-1};\ s=\sigma+it,\ \sigma>1.$$

§ 5. Аналитическая теория чисел

1. *Формула Эйлера для мнимой экспоненты.*

$$e^{i\varphi}=\cos\varphi+i\sin\varphi,\varphi\in R;e^{i\pi}=-1.$$

2. *Формулы Эйлера — Фурье.*

$$\int_0^1 e^{2\pi ixn}\,dx=\begin{cases}1, & \text{если } n=0,\\ 0, & \text{если } n \text{ — целое, } n\neq 0.\end{cases}$$

3. *Значение дзета-функции Эйлера — Римана $\zeta(s)$ в точке $s=2$.*

$$\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}.$$

Тождество следует из соотношения

$$\sin\{\pi x\}=\pi x-\frac{\pi^3x^3}{6}+\cdots=\pi x\prod_{n=1}^{\infty}\left(1-\frac{x^2}{n^2}\right).$$

4. *Формула Эйлера суммирования значений функций в целых точках.*

Пусть $f\in D[a,b]$ (или $f\in V[a,b]$), $\rho(x)=0,5-\{x\}$. Тогда имеем

$$\sum_{a<n\leqslant x}f(n)=\int_a^x f(t)\,dt+\rho(x)f(x)-\rho(a)f(a)-\int_a^x\rho(t)f'(t)\,dt.$$

5. *Постоянная Эйлера* $\gamma=0,577\ldots$, где

$$\gamma=\lim_{n\to\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}-\ln n\right).$$

Список литературы

[1] Euler L. Commentationes Arithmeticae Collectae. V.I-II. — S.-P.: Изд–во АН,1849.
[2] Euler L. Elements d'Algebre. V.I-II. — Paris: Изд–во АН,1807.
[3] Euler L. Introductio in analysis infinitorum. V.I-II. — Lozanne:1748.
[4] Чебышёв П. Л. Избранные труды. — М.: Изд–во АН СССР,1952.
[5] Leonhard Euler und Christian Goldbach. Briefwechsel. 1729–1764. Herausgegeben und eingeleiten von A. P. Juškevič und E. Winter. Berlin. 1965.
[6] Виноградов И. М. Метод тригонометрических сумм в теории чисел. — М.: Наука,1976.
[7] Виноградов И. М. Избранные труды. — М.: Изд–во АН СССР,1952.
[8] Dickson L. E. History of the theory of numbers. Vol. 1. Divisibility and primality. Publ. No. 256. — Washington: The Carnegie Instituion of Washington,1919.
[9] Венков Б. А. О работах Леонарда Эйлера по теории чисел. Леонард Эйлер (1707–1783). Сб. статей и материалов к 150-летию со дня смерти. Тр. ин-та истории науки и техники. Сер. II, вып.1. — М.-Л.: Изд–во АН СССР,1935.

Глава VIII
МЕТОД И.М.ВИНОГРАДОВА И ЕГО РАЗВИТИЕ

П. С. Александров дал яркую картину развития математики. Он писал: “Нет "чистой"и прикладной математики, что, несмотря на внешнюю разобщенность своих частей, математика едина и ее единство основано на самой сущности математики.

Обучение математике нельзя подменять обучением ряду ее приложений и методов, не разъясняя сущности математических понятий и не учитывая внутреннюю логику самой математики. Так подготовленные специалисты могут оказаться беспомощными при изучении новых конкретных явлений, поскольку будут лишены необходимой математической культуры и не приучены к рассмотрению абстрактных математических моделей.”

Мысль о единстве математики продемонстрируем, затрагивая лишь исследования по аналитической теории чисел. Наиболее емко и конкретно об этом сказал И. М. Виноградов [**?**]: "Арифметические задачи наиболее естественно, казалось бы, и решать арифметическими методами, т.е. не вводя в доказательство элементы, посторонние арифметике, и в частности элементы анализа. Однако, история теории чисел дает немало примеров, когда для решения арифметических проблем одних арифметических методов оказывалось недостаточно. Обнаруживалась необходимость вводить в доказательство элементы анализа бесконечно-малых. Из теории чисел выделился ряд крупных проблем, решаемых методами анализа. Отсюда и возникла аналитическая теория чисел...

Анализ дает возможность значительно расширить круг вопросов теории чисел и способствует более быстрому развитию этой науки.

Кроме этого следует отметить и другую полезную сторону аналитического метода в теории чисел. Анализ, получая для разрешения новые трудные задачи, сам растет и совершенствуется. Как пример приведу ряды Дирихле, теорию функции $\zeta(s)$, некоторые свойства Бесселевых функций, ряд замечательных теорем, относящихся к теории функций комплексного переменного (например, теоремы Линделёфа, Фрагмена, Меллина), разрывные суммы и ин-

тегралы и т.д.".

§ 1. Формулы суммирования значений функций

Новое развитие математика получила с появлением формул суммирования значений теоретико-числовых функций [?, ?]. В первую очередь это связано с именем Л. Эйлера.

В качестве приложения формулы Ньютона–Лейбница выведем формулы Эйлера и Абеля для суммирования значений функций по дискретному множеству точек.

Теорема 1.1. *(Формула Эйлера – Маклорена суммирования значений гладкой функции в целых точках). Пусть функция $f(t)$ является непрерывно дифференцируемой на отрезке $[a,b]$ и $\rho(x) = 1/2 - \{x\}$, где символ $\{x\}$ обозначает дробную часть числа x. Тогда для любого $x \in [a,b]$ справедлива формула*

$$\sum_{a<n\leqslant x} f(n) - \rho(x)f(x) = \int\limits_a^b f(t)\,dt - \int\limits_a^b \rho(t)f'(t)\,dt - \rho(a)f(a).$$

▷ *Пусть $G(x)$ обозначает левую часть последнего неравенства. Функция $G(x)$ непрерывна на отрезке $[a,b]$. Разрыв может быть только в целой точке, но "скачок" суммы $\sum\limits_{a<n\leqslant x} f(n)$ гасится "скачком" функции $\rho(x)f(x)$. В нецелых точках функция является дифференцируемой. Далее по теореме Ньютона–Лейбница имеем*

$$G(x) = G(a) + \int\limits_a^x G'(u)\,du = -\rho(a)f(a) + \int\limits_a^x (-\rho(u)f(u))'\,du =$$

$$-\rho(a)f(a) + \int\limits_a^x f(u)\,du - \int\limits_a^x \rho(u)f'(u)\,du.\triangleleft$$

Теорема 1.2. *(Формула Абеля суммирования по частям значений функции в целых точках). Пусть функция $f(t)$ является непрерывно дифференцируемой на отрезке $[a,b]$ и $C(x) = \sum\limits_{a<n\leqslant x} c_n$, где символ $\{c_n\}$ обозначает произвольную последовательность ком-*

плексных чисел. Тогда для любого $x \in [a,b]$ справедлива формула

$$\sum_{a<n\leqslant x} c_n f(n) - C(x)f(x) = -\int_a^b C(t)f'(t)\,dt.$$

Теорема 1.3. *(Формула Пуассона суммирования значений функции в целых точках). Пусть функция $f(t)$ является непрерывно дифференцируемой на отрезке $[a,b]$ и a и b — полуцелые числа. Тогда справедлива формула*

$$\sum_{a<n\leqslant b} f(n) = \lim_{N\to+\infty} \sum_{n=-N}^{n=N} \int_a^b f(t)e^{2\pi int}\,dt.$$

Более точно, имеет место формула

$$\sum_{a<n\leqslant b} f(n) = \sum_{n=-N}^{n=N} \int_a^b f(t)e^{2\pi int}\,dt + R_N,$$

где

$$R_N \leqslant \frac{8M(b-a)\ln N}{N}, \quad M = \max_{x\in[a,b]} |f'(x)|.$$

▷ *По формуле Эйлера суммирования значений функции в целых точках при полуцелых a и b имеем*

$$S = \sum_{a<n\leqslant b} f(n) = \int_a^b f(x)\,dx - \int_a^b \rho(x)f'(x)\,dx.$$

Далее воспользуемся разложением $\rho(x)$ в ряд Фурье. Получим

$$\rho(x) = s_N(x)+\sigma_N(x), s_N(x) = \sum_{k=1}^{N} \frac{\sin 2\pi kx}{\pi k}, |\sigma_N(x)| \leqslant \frac{4}{\sqrt{1+N^2\sin^2\pi x}}.$$

Следовательно,

$$S = \int_a^b f(x)\,dx - \int_a^b s_N(x)f'(x)\,dx + R_N, R_N = -\int_a^b \sigma_N(x)f'(x)\,dx.$$

Учитывая, что $s_N(a) = s_N(b) = 0$, *после интегрирования по частям получим*

$$\int\limits_a^b f(x)\,dx - \int\limits_a^b s_N(x)f'(x)\,dx = \int\limits_a^b f(x)\,dx + \int\limits_a^b s'_N(x)f(x)\,dx =$$

$$= \int\limits_a^b f(x)\,dx + \int\limits_a^b f(x)\left(\sum_{k=-N}^{N}\cos 2\pi kx - 1\right)dx =$$

$$= \sum_{k=-N}^{N}\int\limits_a^b f(x)\cos 2\pi kx\,dx.$$

Осталось оценить остаток R_N. *Поскольку для любого* x *из отрезка* $[a,b]$ *справедливо неравенство* $|f'(x)| \leqslant M$, *находим*

$$|R_N| = \left|\int\limits_a^b \sigma_N(x)f'(x)\,dx\right| \leqslant 4M\int\limits_a^b \frac{dx}{\sqrt{1+N^2\sin^2\pi x}}.$$

В последнем интеграле подынтегральная функция является периодической с периодом 1 и четная, поэтому

$$|R_N| \leqslant 8M(b-a)\int\limits_0^{1/2}\frac{dx}{\sqrt{1+N^2\sin^2\pi x}} \leqslant 8M(b-a)\left(\int\limits_0^{1/N} dx + \int\limits_{1/N}^{1/2}\frac{dx}{2Nx}\right) =$$

$$= 8M(b-a)\left(\frac{1}{N} + \frac{\ln(N/2)}{2N}\right) < \frac{8M(b-a)\ln N}{N}.\triangleleft$$

Изящное приложение формулы Пуассона суммирования по целым точкам дал Дирихле. Он нашел точное значение суммы Гаусса вида

$$\sum_{n=1}^{N}\cos\frac{2\pi n^2}{N}, \quad \sum_{n=1}^{N}\sin\frac{2\pi n^2}{N}.$$

Более точно, при любом натуральном числе N *справедлива формула*

$$\sum_{n=1}^{N} e^{\frac{2\pi i n^2}{N}} = \frac{1+i^{-N}}{1+i^{-1}}\sqrt{N}.$$

§ 2. Метод тригонометрических сумм

Многие задачи теории распределения значений функций вещественной переменной сводятся к изучению тригонометрических сумм вида

$$S_t = \sum_{(x_1,\dots,x_r)\in\Omega} f(x_1,\dots,x_r) = \sum_{(x_1,\dots,x_r)\in\Omega} e^{2\pi i t F(x_1,\dots,x_r)},$$

где наборы $(x_1,\dots,x_r)$ пробегают значения из дискретного множества Ω, t — вещественный параметр и $F(x_1,\dots,x_r)$ — вещественнозначная функция. Постановка задачи распределения значений функций с помощью тригонометрических сумм принадлежит И.М. Виноградову [?]. Он писал: "Из весьма разнообразных более частных видов этой в столь общей формулировке поставленной проблемы (проблемы распределения значений функций), получаемых при тех или иных ограничениях, налагаемых как на функцию $f(x_1,\dots,x_r)$, так и на совокупность Ω, мы выделим три достаточно большие и весьма важные для теории чисел проблемы...

1. Весьма важной является проблема распределения значений показательной функции

$$f(x_1,\dots,x_r) = e^{2\pi i F(x_1,\dots,x_r)},$$

где $F(x_1,\dots,x_r)$ — вещественная функция; наиболее существенным в этой проблеме является установление верхней границы модуля суммы

$$S = \sum_{\Omega} f(x_1,\dots,x_r) = \sum_{\Omega} e^{2\pi i F(x_1,\dots,x_r)}$$

всех значений $f(x_1,\dots,x_r)$ в том случае, когда число T точек совокупности Ω конечно.

2. С рассмотренной проблемой 1 самым тесным образом связана проблема распределения значений дробной части

$$f(x_1,\dots,x_r)=\{2\pi iF(x_1,\dots,x_r)\}$$

вещественной функции $F(x_1,\dots,x_r)$.

3. Особый интерес представляют законы распределения значений функции $f(x_1,\dots,x_r)$, *принимающей для точек* $(x_1,\dots,x_r)$ *совокупности* Ω *целочисленные значения. Здесь в отношении каждого данного целого* N *возникает вопрос: для скольких точек совокупности* Ω *это* N *будет служить значением функции* $f(x_1,\dots,x_r)$; *иными словами: каково будет число* $I(N)$ *решений неопределенного уравнения*

$$f(x_1,\dots,x_r)=N. \qquad (*)$$

В некоторых случаях здесь речь идет только об установлении неравенства $I(N)>0$, *показывающего, что уравнение (*) разрешимо; в других случаях оказывается возможным установить для* $I(N)$ *асимптотическую формулу; наконец иногда вопрос сводится о разыскании точного выражения для* $I(N)$, *и т.д."*

Следует отметить, что вообще говоря, сформулированные И.М. Виноградовым проблемы 1,2,3 представляют интерес в том случае, когда $f(x_1,\dots,x_r)$ *и область* Ω *несут в себе те или иные арифметические свойства. Выбирая соответствующим образом функцию* $f(x_1,\dots,x_r)$ *и область* Ω, *мы приходим к таким классическим задачам, как проблемы Гольдбаха, Варинга, Гольдбаха–Варинга, Гильберта–Камке, оценки сумм Г. Вейля и т.д.*

§ 3. Тригонометрические интегралы

В аддитивных проблемах теории чисел при исследовании тригонометрических сумм возникают задачи изучения поведения тригонометрических интегралов и их средних значений [?]-[?].

Пусть $r,n_1,\dots,n_r$ — *натуральные числа,* $\nu\max(n_1,\dots,n_r)=1$ *и многочлен* $F=F(x_1,\dots,x_r)=F_A(x_1,\dots,x_r)$ *с вещественными коэффициентами* $\alpha(t_1,\dots,t_r)$ *имеет следующий вид*

$$F(x_1,\dots,x_r)=\sum_{t_1=0}^{n_1}\cdots\sum_{t_r=0}^{n_r}\alpha(t_1,\dots,t_r)x_1^{t_1}\dots x_r^{t_r},\quad F(0,\dots,0)=0.$$

Здесь буква A обозначает набор коэффициентов

$$\alpha(t_1,\dots,t_r),0\leqslant t_1\leqslant n_1,\dots,0\leqslant t_r\leqslant n_r,t_1+\dots+t_r\geqslant 1.$$

Пусть, далее, буква α обозначает максимум модулей всех коэффициентов многочлена F. Тогда для тригонометрического интеграла

$$I_r = I_r(A) = \int_0^1 \cdots \int_0^1 \exp 2\pi i F(x_1, \ldots, x_r)\, dx_1 \ldots dx_r$$

справедлива оценка

$$|I_r| \leqslant \min\,(1, 32^r \alpha^{-\nu} (\ln(\alpha + 1) + 2)^{r-1}).$$

Последнее неравенство можно применить к оценке сверху показателя сходимости $k_0 = k_0(r)$ среднего значения $\gamma = \gamma_r(k; n_1, \ldots, n_r)$ тригонометрического интеграла $I_r(A)$, имеющего вид

$$\gamma = \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} |I_r(A)|^{2k}\, dA, \quad dA = \prod_{\substack{t_1=0 \\ t_1+\cdots+t_r \geqslant 1}}^{n_1} \cdots \prod_{t_r=0}^{n_r} d\alpha(t_1, \ldots, t_r).$$

Имеем $2k_0 \leqslant \nu^{-1} m$, $m = (n_1 + 1) \ldots (n_r + 1)$. Точное значение показателя сходимости k_0 при $r \geqslant 2$ неизвестно. Для однократного интеграла $I_1(A)$ справедливо равенство $2k_0 = \frac{n(n+1)}{2} + 1$, где n — степень многочлена F.

С помощью интеграла $I_r(A)$ определяется особый интеграл многомерной аддитивной проблемы об одновременном представлении набора натуральных чисел $N(t_1, \ldots, t_r), 0 \leqslant t_1 \leqslant n_1, \ldots, 0 \leqslant t_r \leqslant n_r, t_1 + \cdots + t_r \geqslant 1$, слагаемыми вида $x_1^{t_1} \ldots x_r^{t_r}$, где $1 \leqslant x_1 \leqslant P_1, \ldots, 1 \leqslant x_r \leqslant P_r$ пробегают множество всех натуральных чисел и $P_1, \ldots, P_r$ — некоторые натуральные числа. Особый интеграл $\theta = \theta_r(k)$ имеет вид

$$\theta = \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} I_r^k(A) e^{-2\pi i B}\, dA,$$

$$B = \sum_{t_1=0}^{n_1} \cdots \sum_{t_r=0}^{n_r} \alpha(t_1, \ldots, t_r) N(t_1, \ldots, t_r) P_1^{-t_1} \ldots P_r^{-t_r}.$$

Мы полагаем $N(t_1,\dots,t_r)P_1^{-t_1}\dots P_r^{-t_r}=\beta(t_1,\dots t_r)+O(P^{-1/2})$, *где* $P=\min(P_1,\dots,P_r)\to\infty,\beta(t_1,\dots,t_r)$ — *положительные постоянные, и поэтому особый интеграл* θ *можно считать не зависящим от параметров* $P_1,\dots,P_r$.

Для нетривиальности асимптотической формулы для количества решений диофантовой системы уравнений многомерной аддитивной проблемы необходимо установить положительность особого интеграла θ. *Рассмотрим область* Ω, *определяемую неравенствами*

$$\left|\sum_{j=1}^{k}x_{1,j}^{t_1}\dots x_{r,j}^{t_r}-\beta(t_1,\dots,t_r)\right|\leqslant h, h\geqslant 0,$$

$$(0\leqslant t_1\leqslant n_1,\dots,0\leqslant t_r\leqslant n_r, t_1+\dots+t_r\geqslant 1)$$

где $x_{s,j}, 1\leqslant s\leqslant r, 1\leqslant j\leqslant k$ — *вещественные числа с условиями* $0\leqslant x_{s,j}\leqslant 1$. *Символом* $\mu(h)$ *обозначим объем области* Ω.

При $k>\nu^{-1}m$ *справедливо равенство* $\theta=\lim\limits_{h\to 0}2^{-m+1}h^{-m+1}\mu(h)$.

Пусть, далее, при $k>m$ *ранг матрицы Якоби, отвечающей системе уравнений*

$$G_{t_1,\dots,t_r}(\bar{x})=\sum_{j=1}^{k}x_{1,j}^{t_1}\dots x_{r,j}^{t_r}=\beta(t_1,\dots,t_r)$$

$$(0\leqslant t_1\leqslant n_1,\dots,0\leqslant t_r\leqslant n_r, t_1+\dots+t_r\geqslant 1)$$

является максимальным, т.е. равен m, *и пусть найдется ее подматрица размера* $(m-1)\times(m-1)$, *определитель которой равен* $\varepsilon>0$. *Тогда*

1) при достаточно малом $h>0$ *для объема* $\mu(h)$ *области* Ω *справедливо неравенство* $\mu(h)\geqslant c(\varepsilon)2^{m-1}h^{m-1}$, *где* $c(\varepsilon)>0$ — *некоторая постоянная;*

2) при $k>\nu^{-1}m$ *для особого интеграла* θ *имеем* $\theta\geqslant c(\varepsilon)>0$.

Более точный результат имеет место при $r=1$. *Рассмотрим систему уравнений*

$$x_1^s+\dots+x_k^s=\beta(s), s=1,\dots,n; k\geqslant n.$$

Пусть $x_1,\dots,x_k$ *будет решением этой системы. Некоторым способом* ψ *выберем из них* n *чисел:* $z_1,\dots,z_n$ *и добавим к ним числа*

$z_0 = 0, z_{n+1} = 1$. *Характеристикой данного решения системы уравнений будем называть величину*

$$\Delta(x_1, \ldots, x_k) = \max_{\psi} \min_{0 \leqslant i < j \leqslant n+1} |z_i - z_j|.$$

Пусть τ *— наибольшее значение характеристики решений* $(x_1, \ldots, x_k)$ *указанной выше системы уравнений. Тогда справедливы неравенства*

$$2^{2n(n-k)} k^{n-k} n^{-k-n} \tau^{n(k-n)} \leqslant \theta \leqslant 2^{2n^2} k^{2n} n^{k-2n} \tau^{k-3n-n^2}.$$

Таким образом условия $\theta > 0$ *и* $\tau > 0$ *эквивалентны между собой.*

§ 4. Применения тригонометрических сумм и интегралов в анализе

Тригонометрические суммы и интегралы нашли широкие применения в теории равномерного распределения, теории дифференциальных уравнений, спектральной теории и аналитической теории чисел. В основе этих применений лежат оценки таких сумм и интегралов.

§ 5. Специальные тригонометрические ряды

Пусть k *— натуральное число. Пусть* E *обозначает единичный* k*-мерный куб, состоящий из векторов* $\alpha = (\alpha_1, \ldots, \alpha_k)$ *с вещественными координатами* $\alpha_s, s = 1, \ldots, k$, *и пусть* $f(x) = f_k(x) = \sum_{s=1}^{k} \alpha_s x^s$ *— многочлен степени* k.

Рассмотрим ряд

$$h(f) = \sum_{n \neq 0} \frac{e^{2\pi i f(n)}}{n},$$

суммирование распространяется по всем целым n, *исключая* $n = 0$, *и его симметричные частичные суммы вида*

$$h_N(f) = \sum_{1 \leqslant |n| \leqslant N} \frac{e^{2\pi i f(n)}}{n}, N \geqslant 1.$$

Используя метод И.М. Виноградова тригонометрических сумм [?], Г.И. Архипов and К.И. Осколков [?] доказали следующее утверждение о равномерной ограниченности симметричных частичных сумм $h_N(f)$.

Теорема 4.1.1. *Пусть $k \geqslant 2$ — фиксированное натуральное число. Тогда для многочлена $f_k \neq 0$ имеем*

$$\sup_{N \geqslant 1} \sup_{f_k} |h_N(f_k)| = g_k < \infty.$$

Более того, для каждого многочлена $f_k \neq 0$, последовательность $\{h_N(f_k)\}$ сходится при $N \to \infty$, и так что сумма ряда $h(f_k)$, рассматриваемая как предел ее симметричных частичных сумм $h_N(f_k)$, определена и ограничена всюду на множестве многочленов степени k.

§ 6. Обобщенное решение уравнения Шрёдингера

В частности, К. И. Осколков [?] нашел, что утверждение теоремы 4.1.1. может быть сформулировано в терминах функциональных свойств обобщенных решений задачи Коши для уравнения Шрёдингера

$$\frac{\partial \Psi}{\partial t} = \frac{1}{2\pi i} \frac{\partial^2 \Psi}{\partial x^2}, \Psi(x,t)|_{t=0} = f(x),$$

с периодическими (период 1) начальными условиями $f(x)$. Он доказал следующее утверждение.

Теорема 4.2.1. *Пусть $f(x)$ — функция ограниченной вариации на периоде. Тогда существует решение уравнения Шрёдингера, ограниченное всюду на плоскости $\{x,t\}$.*

§ 7. Обобщенное решение уравнения Кортевега–де Фриза

Г.И. Архипов нашел следующий интересный результат.

Теорема 4.3.1. *Пусть $u = u(x,t)$ — обобщенное решение задачи Коши уравнения*

$$\frac{\partial u}{\partial t} = \frac{\partial^3 u}{\partial x^3}, \quad u|_{t=0} = \{x\}.$$

Тогда оно существует, ограничено и для всех иррациональных t непрерывно по x. Если $t = a/q$, $(a,q) = 1$, то при некоторых ограничениях на знаменатель q функция $u(a/q, x)$ имеет только разрывы 1-го рода со скачками $b(q)$ в числе q на периоде.

§ 8. Простые числа и дзета-функция Римана

В связи с исследованиями П.Л. Чебышёва следует сказать о новом методе в теории простых чисел, предложенном Б. Риманом в

его известной работе "О числе простых, не превышающих данной величины"(1859).

Дзета-функция Римана представляет собой функцию комплексного переменного s, определенную в полуплоскости $\Re s > 1$ абсолютно сходящимся рядом

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

Б. Риман продолжил $\zeta(s)$ на всю комплексную плоскость $\mathbf{C}$ как мероморфную функцию с простым полюсом в точке $s = 1$ и вычетом в нем, равном 1, т.е. функция $\zeta(s) - \frac{1}{s-1}$ является целой.

При $\Re s > 1$ Б. Риман вывел формулу, подобную формуле Чебышёва

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

а затем, деформируя контур интегрирования в комплексной плоскости, он получил представление, справедливое для любого комплексного числа s.

Отметим, что в неопубликованных заметках Б. Римана, сохранившихся в математической библиотеке Гёттингенского университета, имеется несколько ссылок на мемуары П.Л. Чебышёва, хотя в его единственной опубликованной работе по теории чисел они отсутствуют.

Далее Риман показал, что дзета-функция удовлетворяет функциональному уравнению

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

что позволяет свойства $\zeta(s)$ при $\Re s = \sigma < 0$ выводить из ее свойств при $\sigma > 1$. В частности, из-за полюсов функции $\Gamma(s/2)$ дзета-функция Римана будет иметь нули в точках $s = -2, -4, -6, \ldots$, которые называются тривиальными нулями $\zeta(s)$. Часть комплексной плоскости, отвечающая неравенству $0 \leqslant \sigma \leqslant 1$ называется критической полосой, а прямая $\sigma = 1/2$ — критической прямой.

Используя тождество Эйлера, при $\Re s = \sigma > 1$ Риман вывел

следующее интегральное преобразование

$$\frac{\log\zeta(s)}{s}=\int\limits_1^\infty \Pi(x)x^{-s-1}\,dx,\quad \Pi(x)=\pi(x)+\pi(\sqrt{x})+\pi(\sqrt[3]{x})+\dots,$$

а по формуле обращения Фурье – Меллина, он при $a>1$ нашел

$$\Pi(x)=\frac{1}{2\pi i}\int\limits_{a-i\infty}^{a+i\infty}\log\zeta(s)\frac{x^s}{s}\,ds.$$

Открытие Б. Римана 1859 г., состоящее в том, что комплексные нули дзета-функции определяют закон распределения простых чисел, сделало эпоху в теории простых чисел. Риман нашел явную формулу, связывающую функцию $\pi(x)$ с суммой по нулям дзета-функции. Отметим, что в 1895 г. Мертенс доказал другую явную формулу, связывающую функцию Чебышева $\psi(x)$ и нули $\zeta(s)$, и имеющую более простой вид:

$$\psi(x)=x-\sum_\rho\frac{x^\rho}{\rho}-\frac{\zeta'(0)}{\zeta(0)}-\frac{1}{2}\log(1-x^{-2}),$$

где ρ — нетривиальные нули дзета-функции Римана, лежащие в критической полосе $0<\Re s<1$.

§ 9. Простые числа и тригонометрические суммы

В работе "Об одном преобразовании числовых рядов" (1879) П.Л. Чебышёв нашел, что тождество Эйлера $\zeta(s)=\prod\limits_p(1-p^{-s})^{-1}$ и формула Чебышёва, заменяющая сумму логарифмов натуральных чисел (до известного предела) суммами, относящимися к простым числам:

$$\sum_{n\leqslant x}\log n=\sum_{m\leqslant x}\psi\left(\frac{x}{m}\right),$$

являются следствием одного общего тождества

$$\sum_{n=2}^\infty f(n)\log n=\sum_p F(p)\log p,$$

где

$$F(x)=\sum_{n=1}^\infty\sum_{m=1}^\infty f(nx^m).$$

Из последней формулы тождество Эйлера получается при $f(x) = x^{-s}$, *а тождество Чебышёва при*

$$f(n) = \begin{cases} 1, & \text{если} \quad n \leqslant x; \\ 0, & \text{если} \quad n > x. \end{cases}$$

Подобное тождество лежит в основе метода И. М. Виноградова оценок тригонометрических сумм с простыми числами:

$$\Phi(1) + \sum_{H<y\leqslant N} \Phi(y) = \sum_{dm\leqslant x} \sum \mu(d)\Phi(dm),$$

где H *— любое число с условием* $1 < H \leqslant \sqrt{N}$, y *пробегает числа, не делящиеся на простые числа, не превосходящие* H, d *пробегает произведение простых чисел (включая пустое произведение, равное 1), не превосходящих* H, *наконец,* m *пробегает натуральные числа.*

Тождество Эйлера получается отсюда при $\Phi(m) = m^{-s}$ *путем предельного перехода.*

В 1937 г. И.М. Виноградов нашел нетривиальную оценку для суммы $\sum\limits_{p\leqslant N} e^{2\pi i\alpha p}$, *с помощью которой вывел асимптотическую формулу для числа представлений нечетного числа суммой трех нечетных простых чисел (тернарная проблема Гольдбаха).*

В том же 1937 г. И.М. Виноградов получил нетривиальную оценку для тригонометрической суммы

$$\sum_{p\leqslant N} e^{2\pi i(\alpha_n p^n + \cdots + \alpha_1 p)},$$

где суммирование ведется по простым числам p. *Отметим, что идея И. М. Виноградова оценки сумм с простыми числами состояла в том, что он с помощью указанного выше тождества сводил эти суммы к небольшому количеству двойных сумм специального вида, переменные суммирования в которых были независимы.*

Для двойных же сумм несколько ранее (1934 г.) И. М. Виноградов открыл способ получения их нетривиальных оценок. В частности, это позволило ему получить выдающееся продвижение в проблеме Варинга о представлении натуральных чисел суммами степеней натуральных чисел. И. М. Виноградов сразу оценил широкие перспективы своего метода. С данного момента он стал говорить о создании нового метода тригонометрических сумм в теории чисел, хотя основы метода заложены

им за 20 лет до этого. Новый метод выдвинул ряд новых задач в теории чисел и анализе. Как отмечалось ранее, И. М. Виноградов в его монографии "Метод тригонометрических сумм в теории чисел" (1947 г.) выделил три актуальных направления исследований, связанных с его методом:

оценки кратных тригонометрических сумм с вещественной функцией в экспоненте,

распределение значений арифметических функций от многих переменных и

диофантов анализ для целозначных функций от большого числа переменных, причем переменные могут пробегать различные множества значений, например, множество простых чисел.

Венцом метода И.М. Виноградова в применении к оценкам однократных тригонометрических сумм Г. Вейля было получение оценок тригонометрических сумм по простым числам приблизительно такой же силы, как и для сумм по сплошному промежутку суммирования. Для кратных сумм подобная задача ставилась самим Виноградовым.

В 1984 г. автор решил эту проблему И.М. Виноградова. Он нашел нетривиальную оценку для кратной тригонометрической сумме по простым числам с многочленом общего вида в экспоненте

$$\sum_{p_1 \leqslant N_1} \cdots \sum_{p_r \leqslant N_r} e^{2\pi i F(p_1,\ldots,p_r)},$$

где переменные $p_1, \ldots, p_r$ пробегают все последовательные простые числа и

$$F(x_1, \ldots, x_r) = \sum_{t_1=0}^{n_1} \cdots \sum_{t_r=0}^{n_r} \alpha(t_1, \ldots, t_r) x_1^{t_1} \ldots x_r^{t_r}, \alpha(0, \ldots, 0) = 0.$$

Эта оценка близка к той, которую мы с Г.И.Архиповым получили для кратных тригонометрических сумм Г. Вейля по сплошным промежуткам суммирования.

§ 10. Тригонометрические суммы Г. Вейля

В тот момент сложилась парадоксальная ситуация. Для однократных сумм Г.Вейля И.М. Виноградов разработал теорию, основу которой составила точная оценка моментов этих сумм. Она получила название теоремы И.М. Виноградова о среднем: Пусть

$n \geqslant 2$ — натуральное число, $\alpha_1, \dots, \alpha_n$ — вещественные числа. Тогда для интеграла J вида

$$J = J(P; k, n) = \int_0^1 \cdots \int_0^1 \left| \sum_{x \leqslant P} e^{2\pi i(\alpha x^n + \cdots + \alpha_1 x)} \right|^{2k} d\alpha_n \dots d\alpha_1$$

справедлива оценка

$$J = J(P; k, n) \leqslant D P^{2k - 0.5n(n+1) + \delta(\tau)},$$

$$\delta = 0,5n(n+1)(1 - 1/n)^\tau, \quad D = D(\tau) = (n\tau)^{6n\tau}(2n)^{4n(n+1)\tau}.$$

В то же время для кратных сумм Г. Вейля ничего не было известно, хотя сама задача была поставлена Виноградовым еще в сороковые годы. Первые оценки кратных сумм были получены Г.И. Архиповым в 1971 г. и опубликованы им в 1974 г. В 1975 г. мы с Г.И. Архиповым решили проблему моментов для кратных сумм, на основе которой была построена теория, подобная теории И.М. Виноградова для однократных сумм Г. Вейля.

Другими словами, мы получили правильную оценку сверху по порядку растущих параметров $\bar{P} = (P_1, \dots, P_r)$, $P_1 = \min(P_1, \dots, P_r)$ при $P_1 \to \infty$ следующей величины:

$$J = J(\bar{P}; \bar{n}, k) = \int_\Omega \cdots \int |S(\Omega)|^{2k} \, d\Omega,$$

где $S(\Omega)$ — кратная тригонометрическая сумма Г. Вейля вида

$$S(\Omega) = \sum_{x_1 \leqslant P_1} \cdots \sum_{x_r \leqslant P_r} \exp 2\pi i F(x_1, \dots, x_r),$$

$$F(x_1, \dots, x_r) = \sum_{t_1=0}^{n_1} \cdots \sum_{t_r=0}^{n_r} \alpha(t_1, \dots, t_r) x_1^{t_1} \dots x_r^{t_r}, \alpha(0, \dots, 0) = 0,$$

причем Ω — набор вещественных коэффициентов $\alpha(\bar{t}) = \alpha(t_1, \dots, t_r)$ многочлена $F(x_1, \dots, x_r), n_1, \dots n_r \geqslant 1$, $\bar{t} = (t_1, \dots, t_r)$ и $d\Omega = \prod\limits_{\substack{t_1=0 \\ t_1 + \cdots + t_r \geqslant 1}}^{n_1} \cdots \prod\limits_{t_r=0}^{n_r} d\alpha(t_1, \dots, t_r)$.

§ 11. Показатель сходимости особого интеграла

В рамках теории тригонометрических сумм исследовались тригонометрические интегралы. Приведем последний вариант оценки И.М. Виноградова (1981 г.). Пусть $\alpha = \max(|\alpha_n|, \dots, |\alpha_1|)$. *Тогда имеем*

$$\left| \int_0^1 e^{2\pi i(\alpha_n x^n + \dots + \alpha_1 x)}\, dx \right| \leqslant (1, 32\alpha^{-1/n}).$$

В 1976 г. автор получил следующую оценку кратного тригонометрического интеграла. Пусть $F(x_1, \dots, x_r)$ — *многочлен с вещественными коэффициентами* $\alpha(\bar{t}), n = \max n_1, \dots, n_r$, $\alpha = \max\limits_{\bar{t}} |\alpha(\bar{t})|$. *Тогда*

$$\left| \int_0^1 \dots \int_0^1 e^{2\pi i F(x_1,\dots,x_r)}\, dx_1 \dots dx_r \right| \leqslant \min(1, 32\alpha^{-1/n} \ln^{r-1}(\alpha + 2)).$$

Отдельной проблемой математики является определение показателя сходимости γ *для моментов тригонометрических интегралов, т.е. нахождение такого вещественного числа* γ, *что при* $2k > \gamma$ *сходится интеграл*

$$\theta(k) = \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} \left| \int_0^1 e^{2\pi i(\alpha_n x^n + \dots + \alpha_1 x)}\, dx \right|^{2k} d\alpha_n \dots d\alpha_1,$$

а при $2k \leqslant \gamma$ *он расходится. Эта проблема была сформулирована Хуа Ло-кеном в 1952 г. Он получил первые оценки сверху величины* γ. *В 1978 г. Г.И. Архипов, А.А. Карацуба и автор доклада решили проблему Хуа Ло-кена. Нами было установлено, что интеграл* $\theta(k)$ *сходится при* $2k > 0,5n(n+1)+1$ *и расходится при* $2k \leqslant 0,5n(n+1)+1$.

Для "выщербленного" многочлена

$$f(x) = \alpha_n x^n + \dots + \alpha_m x^m + \alpha_r x^r,$$

где $n > \dots > m > r, n + \dots + m + r < 0,5n(n+1)$, *был обнаружен неожиданный эффект. Показатель сходимости* γ' *интеграла*

$$\theta'(k) = \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} \left| \int_0^1 e^{2\pi i f(x)}\, dx \right|^{2k} d\alpha_n \dots d\alpha_m d\alpha_r$$

равен $\gamma' = n + \cdots + m + r$. *Значения показателя сходимости для кратных тригонометрических интегралов на сегодяшний день не найдены.*

Далее обсудим некоторые арифметические свойства дифференциалов и разностей значений многочленов.

§ 12. Арифметика разностей и производных многочленов

Начнем рассмотрение с примеров, принадлежащих И.М.Виноградову, Хуа Ло-кену и Г.И.Архипову.

Пусть $f(x)$ — *целозначный многочлен степени* n,

$$f(x) = a_n \binom{x}{n} + a_{n-1} \binom{x}{n-1} + \cdots + a_1 \binom{x}{1} + a_0,$$

где при $0 \leqslant k \leqslant n$ *имеем*

$$\binom{x}{k} = \frac{x(x-1)\dots(x-k+1)}{k!}, \binom{x}{0} = 1,$$

и коэффициенты a_k — *целые.*

Рассмотрим специальный многочлен вида

$$H_n(x) = 2^{n-1} \binom{x}{n} - 2^{n-2} \binom{x}{n-1} + \cdots + (-1)^{n-1} \binom{x}{1}.$$

Находим

$$H_{n+1}(x+1) + H_n(x) = 2^n \binom{x}{n} + (-1)^{n+1},$$

$$H_n(x) = 2^{n-1} \binom{x}{n} - H_{n-1}(x), \quad H_n(x+2) - H_n(x) = 2^n \binom{x}{n-1}.$$

Другими словами, получим

$$2H_n(x) \equiv 1 - (-1)^x \pmod{2^{n+1}}.$$

Это означает, что для четных x, *значения многочлена* $H_n(x)$ *сравнимы с нулем по модулю* 2^n *и, для нечетных* x, *сравнимы с единицей по тому же модулю..*

Г.И.Архипов доказал [?] следующее утверждение.

Теорема A. *Предположим, целые числа $a_1, \dots, a_n$ являются коэффициентами многочлена $H_n(x)$. Для того чтобы система сравнений*

$$\sum_{m=1}^{k} x_m^s \equiv N_s \pmod{2^n}, \quad s = 1, \dots, n,$$

имела решение, необходимо, чтобы выполнялось следующее неравенство:

$$k \geqslant b_0,$$

где b_0 — наименьший неотрицательный вычет числа b по модулю 2^n,

$$b = \sum_{s=1}^{n} a_s N_s.$$

Другой пример *дал Хуа Ло-кен (Hua Lo-ken[?]).*

Пусть $Q(x)$ — многочлен с рациональными коэффициенттами и α — наибольшее целое такое,что наименьший общий знаменатель коэффициентов $Q(x)$ делится на p^α. Тогда

$$Q(x) \equiv 0 \pmod{p^\alpha}$$

для любого целого x.

Необходимое и достаточное условие для

$$Q(x) \equiv 0 \pmod{p^\alpha}$$

есть то, что

$$p^\alpha \| (a_1, \dots, a_n),$$

где $Q(x) = a_n \binom{x}{n} + \dots + a_1 \binom{x}{1}$.

Теорема B. *Если a — наибольшее целое такое, что*

$$Q(x) \equiv 0 \pmod{p^a},$$

и если

$$Q'(x) \equiv 0 \pmod{p^b},$$

то

$$b - a \leqslant [n/(p-1)] - 1.$$

Доказательство этой теоремы основано на следующем свойстве s-й разности $Q(x)$. Имеем

$$(\Delta^s Q'(x))_{x=0} = (\Delta^s Q(x))'_{x=0}.$$

Третий пример *принадлежит И.М.Виноградову [?]. Для целого* $n \geqslant 2$ *и для вещественных чисел* $\alpha_n, \dots, \alpha_1$, *положим* $f(x) = \alpha_n x^n + \dots + \alpha_x$. *Пусть* P *обозначает целое большее, чем 1.*

Теорема С. *Каждому целому* y *соответствует точка* $(Y_{n-1}, \dots, Y_1)$ *в* $(n-1)$*-мерном пространстве, определяемая разложением*

$$f(x+y) - f(y) = \alpha_n x_n + Y_{n-1}x^{n-1} + \dots + Y_1 x$$

разности $f(x+y) - f(y)$ *по степеням* x.

Пусть Y *будет положительное целое меньшее, чем* P. *Необходимое условие того, что точка, соответствующая определенному целому числу* y *из последовательности* $0, \dots, Y$, *может быть сделано добавлением членов, не превосходящих численно*

$$L_{n-1} = P^{-n+1}, \dots, L_1 = P^{-1},$$

к ее координатам, сравнимом с точкой, соответствующей некоторому определенному числу y_0 *из той же последовательности, такое, что неравенство*

$$\|n \dots s\alpha_s(y - y_0)\| \leqslant n \dots (s+1)(3n/2)^{n-s} L_{s-1}$$

будет справедливо при $s = n, \dots, 2$, *and* $\|x\| = \min(\{x\}, 1 - \{x\})$.

§ 13. Нули многочленов и его производных

Предположим, что $n \geqslant 2$ *и многочлен* $g(x)$ *задан соотношением*

$$g(x) = a(x - \alpha_1) \dots (x - \alpha_n),$$

где $\alpha_1 < \alpha_2 < \dots < \alpha_n$.

Тогда имеем

$$g'(x) = na(x - \beta_1) \dots (x - \beta_{n-1}).$$

Theorem 1.1. *Пусть* $\delta = \min\limits_{1 \leqslant s \leqslant n-1} (\alpha_{s+1} - \alpha_s)$ *будет минимальное расстояние между нулями многочлена* $g(x)$. *Тогда имеем*

$$\alpha_1 < \beta_1 < \alpha_2 < \beta_2 < \dots < \alpha_{n-1} < \beta_{n-1} < \alpha_n,$$

$$\min_{s,t} |\alpha_s - \beta_t| > \frac{\delta}{2(1 + \ln(2n-3))},$$

$$\left| \int_0^1 e^{2\pi i g(x)}\, dx \right| \ll \alpha^{-1/2}\delta^{1-n/2}.$$

§ 14. Инвариант многочлена

Теорема 2.1. *Предположим, что* $n \geqslant 1$, $\alpha_1, \ldots, \alpha_n$ — *вещественные числа,*

$$f(x) = \alpha_n x^n + \cdots + \alpha_1 x, \beta_r(x) = f^{(r)}(x)/r!, r = 1, \ldots, n,$$

$$H = H(\alpha_n, \ldots, \alpha_1) = \min_{a \leqslant x \leqslant b} \sum_{r=1}^{n} |\beta_r(x)|^{1/r}.$$

Тогда для интеграла

$$J = \int_a^b e^{2\pi i f(x)}\, dx$$

справедлива оценка

$$|J| \leqslant \min\,(b-a, 6en^3H^{-1}).$$

Теорема 2.2. *Пусть* $n \geqslant 1, \alpha_0, \alpha_1, \ldots, \alpha_n$ — *вещественные числа, и пусть*

$$f(x) = \alpha_n x^n + \cdots + \alpha_1 x + \alpha_0, \quad \beta_r(x) = f^{(r)}(x)/r!, \quad r = 1, \ldots, n,$$

$$H = H(\bar{\alpha}) = H(\alpha_n, \ldots, \alpha_1, \alpha_0) = \min_{a \leqslant x \leqslant b} \max_{1 \leqslant r \leqslant n} |\beta_r(x)|^{1/r},$$

$$J = \int_a^b \rho(f(x))\, dx, \rho(x) = 0,5 - \{x\}.$$

Тогда для интеграла J *имеет место оценка*

$$|J| \leqslant \min\left(b-a; 4en^2H^{-1}\right).$$

Теоремы, сформулированные выше, дают правильную (по порядку величины H) оценку интеграла с многочленом $f(x)$ в экспоненте. Более точно, для любого многочлена $f(x)$ на отрезке интегрирования $[a,b]$ существует точка c такая, что тригонометрический интеграл

$$J(c) = \int\limits_a^c e^{2\pi i f(x)}\, dx$$

имеет как верхнюю, так и нижнюю оценку порядка T, где $T = \min\{b-a, H^{-1}\}$ и H те же самые, что и в теореме 2.1.

§ 15. Особый интеграл в проблеме Терри

Показателем сходимости несобственного интеграла

$$\theta = \int\limits_{-\infty}^{+\infty} \cdots \int\limits_{-\infty}^{+\infty} |G(u_1,\dots,u_m)|^{2k}\, du_1 \dots du_m$$

по определению будет число γ такое, что θ сходится при $2k > \gamma+\varepsilon$ и расходится при $2k < \gamma-\varepsilon$, где $\varepsilon > 0$ — произвольно малое число.

Особый интеграл θ_1 в проблеме Терри имеет вид

$$\theta_1 = \int\limits_{-\infty}^{+\infty} \cdots \int\limits_{-\infty}^{+\infty} \left| \int\limits_0^1 e^{2\pi i(\alpha_n x^n + \cdots + \alpha_1 x)}\, dx \right|^{2k} d\alpha_n \dots d\alpha_1.$$

Г.И.Архипов, А.А.Карацуба и В.Н.Чубариков доказали следующие утверждения.

Теорема 3.1. *Интеграл θ_1 сходится при $2k > 0.5(n^2+n)+1$ и расходится при $2k \leqslant 0.5(n^2+n)+1$.*

Теорема 3.2. *Предположим, что натуральные числа $r,\dots,m,n$ удовлетворяют условиям $1 \leqslant r < \cdots < m < n$ and $r+\cdots+m+n < 0.5(n^2+n)$,*

$$\theta_1' = \int\limits_{-\infty}^{+\infty} \cdots \int\limits_{-\infty}^{+\infty} \left| \int\limits_0^1 e^{2\pi i(\alpha_n x^n + \alpha_m x^m + \cdots + \alpha_r x^r)}\, dx \right|^{2k} d\alpha_n d\alpha_m \dots d\alpha_r.$$

Тогда интеграл θ_1' сходится при $2k > n+m+\cdots+r$ и расходится при $2k \leqslant n+m+\cdots+r$.

§ 16. Деревья Хуа Ло-кена

Теорема 4.1. *Предположим, что $g(x)$ — многочлен с целыми коэффициентами и a — корень кратности m многочлена $g(x)$ по модулю p. Предположим также, что u — наивысшая степень p, которая делит все коэффициенты многочлена*

$$h(x) = g(px + a).$$

Тогда число корней многочлена $p^{-u}h(x)$ по модулю p с учетом их кратности, не превосходит m.

§ 17. Особый ряд в проблеме Терри

Пусть $n \geqslant 3$ — натуральное число, $(a_1, q_1) = \cdots = (a_n, q_n) = 1$ и $q = q_1 \dots q_n$,

$$S(q, f(x)) = \sum_{x=1}^{q} e^{2\pi i f(x)}, f(x) = \frac{a_1}{q_1}x + \cdots + \frac{a_n}{q_n}x^n.$$

Особый ряд σ_1, определяемый выражением

$$\sigma_1 = \sum_{q_n=1}^{+\infty} \cdots \sum_{q_1=1}^{+\infty} \sum_{\substack{a_n=0 \\ (a_n,q_n)=1}}^{q_n-1} \cdots \sum_{\substack{a_1=0 \\ (a_1,q_1)=1}}^{q_1-1} \left|q^{-1}S(q, f(x))\right|^{2k},$$

где штрих в знаке суммирования означает,что a_s пробегает приведенную систему вычетов по модулю $q_s (s = n, \dots, 1)$.

Хуа Ло-кен доказал утверждение.

Теорема 5.1. *Особый ряд σ_1 сходится при $2k > 0.5n(n + 1) + 2$ и расходится при $2k \leqslant 0.5n(n + 1) + 2$.*

Автор нашел показатель сходимости для ряда σ_1', отвечающего "выщербленным" многочленам $f(x) = a_m x^m + \cdots + a_n x^n, m < \cdots < n, m + \cdots + n < 0, 5n(n + 1)$. Пусть

$$f(x) = \frac{a_m}{q_m}x^m + \cdots + \frac{a_n}{q_n}x^n, 1 \leqslant m < \cdots < n, m + \cdots + n < 0.5n(n+1),$$

$$\sigma_1' = \sum_{q_n=1}^{+\infty} \cdots \sum_{q_m=1}^{+\infty} \sum_{\substack{a_n=0 \\ (a_n,q_n)=1}}^{q_n-1} \cdots \sum_{\substack{a_m=0 \\ (a_m,q_m)=1}}^{q_m-1} \left|q^{-1}S(q, f(x))\right|^{2k}, q = q_m \dots q_n.$$

Тогда особый ряд σ_1' сходится $2k > m + \cdots + n + 1$ и расходится при $2k \leqslant m + \cdots + n + 1$.

Пусть s — натуральное число, $F(x)$ — 1-периодическая функция, которая для любого натурального числа m и a, взаимно простого с m, для всех вещественных чисел x удовлетворяет следующему функциональному уравнению

$$m^{1-s}F(mx) = F(x) + F\left(x + \frac{a}{m}\right) + \cdots + F\left(x + \frac{a(m-1)}{m}\right). \quad (1)$$

К.Ф.Гаусс нашел подобное уравнение для гамма-функции Эйлера, которое получило название гауссовой теоремы умножения.

При $0 \leqslant x < 1$ соотношение (1) выполняется для многочленов Бернулли $B_s(x)$, которые $s \geqslant 1$ можно определить таким образом:

$$B_0(x) = 1, B_s'(x) = sB_{s-1}(x), \int_0^1 B_s(x)\,dx = 0,$$

более того

$$B_s(x) = -\frac{s!}{(2\pi i)^s} \sum_{|\nu| \geqslant 1} \frac{e^{2\pi i \nu x}}{\nu^s}, B_s(1-x) = (-1)^s B_s(x),$$

где при $s = 1$ сумма ряда рассматривается как главное значение по Коши.

Кроме того, при $s = 1$ функция F вида

$$F(x) = \ln\left(1 - e^{2\pi i x}\right) = \ln|2\sin \pi x| - i\pi\rho(x),$$

удовлетворяет уравнению (1), где $\rho(x) = 0,5 - \{x\}$.

Предположим, что функция $F(x)$ ограничена, т.е. существует $C > 0$ такое, что для всех вещественных чисел x имеем $F(x) \leqslant C$. Пусть $F(x)$ — кусочно-непрерывна и кусочно-монотонна на периоде, т.е. $F(x)$ удовлетворяет условиям теоремы Дирихле о разложении функции в сходящийся ряд Фурье.

Пусть, далее, p — нечетное простое число, l — натуральное число. Назовем полной рациональной арифметической суммой $S(F)$ сумму вида:

$$S(F) = S\left(\frac{f(x)}{p^l}; F\right) = \sum_{x=1}^{p^l} F\left(\frac{f(x)}{p^l}\right), \quad (2)$$

где $f(x) = a_n x^n + \cdots + a_1 x + a_0$ — *многочлен с целыми коэффициентами* $a_n, \ldots, a_1$, *коэффициент* a_0 — *вещественное число и* $(a_n, \ldots, a_1, p) = 1$.

Назовем средним значением $\sigma_p = \sigma_p(2k)$ *полной рациональной арифметической суммы* $S\left(\frac{f(x)}{p^l}; F\right)$ *выражение вида*

$$\sigma_p = 1 + \sum_{l=1}^{+\infty} A(p^l),$$

где

$$A(p^l) = \sum_{\substack{a_n=0 \\ (a_n,\ldots,a_1,p)=1}}^{p^l-1} \cdots \sum_{a_1=0}^{p^l-1} \int_0^1 \left| p^{-l} S\left(\frac{f(x)}{p^l}; F\right)\right|^{2k} d\alpha_0,$$

$$f(x) = a_n x^n + \cdots + a_1 x + \alpha_0.$$

Автор доказал следующую теорему.

Теорема 5.2. *Ряд* $\sigma_p = \sigma_p(2k)$ *сходится при* $2k > 0,5n(n+1)+1$ *и расходится при* $2k \leqslant 0,5n(n+1)+1$.

§ 18. Многочлены от нескольких переменных с вещественными коэффициентами

Пусть $F(x_1, \ldots, x_r)$ — *многочлен с вещественными коэффициентами,*

$$F(x_1, \ldots, x_r) = \sum_{t_1=0}^{n_1} \cdots \sum_{t_r=0}^{n_r} \alpha(t_1, \ldots, t_r) x_1^{t_1} \ldots x_r^{t_r},$$

$$F(x_1+y_1, \ldots, x_r+y_r) - F(x_1+z_1, \ldots, x_r+z_r) = \sum_{t_1=0}^{n_1} \cdots \sum_{t_r=0}^{n_r} B(\bar{t}) x_1^{t_1} \ldots x_r^{t_r},$$

$$B(\bar{u}) = \sum_{s=0}^{n-u} A(\bar{u}; s), n = \sum_{k=1}^{r} n_k, u = \sum_{k=1}^{r} u_k, A(\bar{u}; s) =$$

$$= \sum_{\substack{v_1=u_1 \\ v=s+u}}^{n_1} \cdots \sum_{v_r=u_r}^{n_r} \alpha(\bar{v}) \binom{v_1}{u_1} \ldots \binom{v_r}{u_r} (y_1^{v_1-u_1} \ldots y_r^{v_r-u_r} - z_1^{v_1-u_1} \ldots z_r^{v_r-u_r}),$$

$$A(\bar{u}; 1) = \sum_{j=1}^{r} (u_j + 1) \alpha(u_1, \ldots, u_j + 1, \ldots, u_r)(y_j - z_j).$$

Справедлива следующая теорема.

Теорема 6.1. *Существуют многочлены $H(\bar{u},\bar{v};s)$ с целыми коэффициентами от переменных $\bar{y},\bar{z}$ такие, что*

$$A(\bar{u};s)=\frac{1}{u_1!\dots u_r!s!}\sum_{\substack{v_1=u_1\\ v=s-1+u}}^{n_1}\cdots\sum_{v_1=u_1}^{n_r}v_1!\dots v_r!H(\bar{u},\bar{v};s)A(\bar{v};1);$$

сумма коэффициентов каждого из многочленов $H(\bar{u},\bar{v};s)$ не превосходит sr^{s-1}.

Пусть L_1 — число решений системы неравенств

$$\|B(\bar{u})\|\leqslant P_1^{-u_1}\dots P_r^{-u_r}\quad(0\leqslant u_1\leqslant n_1,\dots,0\leqslant u_r\leqslant n_r,1\leqslant u\leqslant n-1);$$

пусть L_2 — число решений линейной системы с теми же условиями

$$\left\|\frac{n!}{(u+1)!}\cdot\frac{(n+1)!}{(u+2)!}A(\bar{u};1)\right\|\leqslant\frac{n!}{(u+1)!}\cdot\frac{(n+1)!}{(u+2)!}(4rn^2)^{n-u-1}\prod_{s=1}^{r}P_s^{-u_s}.$$

Тогда имеем $L_1\leqslant L_2$.

§ 19. Полные рациональные тригонометрические суммы

Хуа Ло-кен получил точную по порядку роста величины q оценку модуля полной рациональной тригонометрической суммы

$$S=S(q,f)=\sum_{x=1}^{q}e^{2\pi i\frac{f(x)}{q}},\quad|S|\leqslant e^{nA(n)}q^{1-1/n},$$

где последние значения функций $A(n)$ были найдены Чэном Джунраном

$$A(3)=6.1,A(4)=5.5,A(5)=5,A(6)=4.7,A(7)=4.4,$$

$$A(8)=4.2,A(9)=4.05,A(n)=4\quad for\quad n\geqslant 10,$$

и $f(x)=a_nx^n+\dots+a_1x$ — многочлен с целыми коэффициентами, $(a_n,\dots,a_1,q)=1,\ q\geqslant 1,n\geqslant 3$.

Автор получил следующую верхнюю границу для полной рациональной кратной тригонометрической суммы.

Пусть $n\geqslant 2$ — целое число, $n=\max(n_1,\dots,n_r),q$ — натуральное число, и пусть

$$S(q,F)=\sum_{x_1=1}^{q}\cdots\sum_{x_r=1}^{q}e^{2\pi i\frac{F(x_1,\dots,x_r)}{q}},$$

где

$$F(x_1,\dots,x_r)=\sum_{t_1=0}^{n_1}\cdots\sum_{t_r=0}^{n_r}a(t_1,\dots,t_r)x_1^{t_1}\dots x_r^{t_r}$$

многочлен с целыми коэффициентами, в совокупности взаимно простыми с q. Тогда

$$|S(q,F)|\leqslant e^{7nr}3^{r\omega(q)}(\tau(q))^{r-1}q^{r-1/n}.$$

В 1952 г. Хуа Ло-кен решил задачу о показателе сходимости среднего значения полной рациональной тригонометрической суммы.

Пусть $n\geqslant 3,\ f(x)=\frac{a_1}{q_1}x+\dots+\frac{a_n}{q_n}x^n,\ (a_1,q_1)=\dots=(a_n,q_n)=1,$ *и* $q=q_1\dots q_n$. *Среднее значение* σ *полной рациональной тригонометрической суммы*

$$S(q,f)=\sum_{x=1}^{q}e^{2\pi if(x)}$$

(особый ряд в проблеме Терри) определяется выражением

$$\sigma=\sum_{q_n=1}^{+\infty}\cdots\sum_{q_1=1}^{+\infty}\sum_{a_n=0}^{q_n-1}{}'\dots\sum_{a_1=0}^{q_1-1}{}'|q^{-1}S(q,f)|^{2k},$$

где знак штрих в суммировании означает, что a_s *пробегает приведенную систему вычетов по модулю* $q_s,\ s=1,\dots,n$.

Хуа Ло-кен доказал следующее утверждение. Особый ряд σ *сходится при* $2k>0.5n(n+1)+2$ *и расходится при* $2k\leqslant 0.5n(n+1)+2$.

Пусть, далее, $1\leqslant m<r<\dots\leqslant n$ *— натуральные числа, и пусть* $n\geqslant 3,\ f(x)=\frac{a_m}{q_m}x^m+\dots+\frac{a_n}{q_n}x^n,\ (a_m,q_m)=\dots=(a_n,q_n)=1,$ *и* $q=q_m\dots q_n$. *Определим среднее значение полной рациональной тригонометрической суммы с "выщербленным" многочленом в виде*

$$\sigma'=\sum_{q_n=1}^{+\infty}\cdots\sum_{q_m=1}^{+\infty}\sum_{a_n=0}^{q_n-1}{}'\dots\sum_{a_m=0}^{q_m-1}{}'|q^{-1}S(q,f)|^{2k},$$

В 1981 г. автор нашел показатель сходимости особого ряда для "выщербленного" многочлена. Особый ряд σ' *для* $1\leqslant m<r<\dots<n,\ m+r+\dots+n<0.5n(n+1)$ *сходится при* $2k>m+r+\dots+n+1$ *и расходится при* $2k\leqslant m+r+\dots+n+1$.

§ 20. Аддитивные задачи варинговского типа с простыми числами

Исследования по тригонометрическим суммам привели автора к рассмотрению проблемы Гильберта – Камке в простых числах, т.е. к проблеме разрешимости в простых числах $p_1, \dots, p_k$ системы уравнений

$$\begin{cases} p_1 + \dots + p_k = N_1, \\ \dots\dots\dots \\ p_1^n + \dots + p_k^n = N_n, \end{cases}$$

где $(N_1, \dots, N_n)$ — наборы натуральных чисел, удовлетворяющие условиям $N_k = P^k(\gamma_k + o(1)), \gamma_k \neq 0, k = 1, \dots, n$ и P — некоторый вещественный параметр, стремящийся к $+\infty$. Эту проблему условно и независимо друг от друга решили К.К. Марджанишвили и Хуа Ло-кен. Полное ее решение дал автор в 1985 г.

Более того, в 1985 г. автором была решена общая многомерная аддитивная проблема следующего вида

$$p_{11}^{t_1} \dots p_{r1}^{t_r} + \dots + p_{1k}^{t_1} \dots p_{rk}^{t_r} = N(t_1, \dots, t_r),$$

$$0 \leqslant t_1 \leqslant n_1, \dots 0 \leqslant t_r \leqslant n_r, t_1 + \dots + t_r \geqslant 1,$$

причем наборы $N(t_1, \dots, t_r)$ удовлетворяют условиям регулярности $N(t_1, \dots, t_r) = P_1^{t_1} \dots P_r^{t_r}(\gamma(t_1, \dots, t_r) + o(1))$, $\gamma(t_1, \dots, t_r) \neq 0$, и $P_1 = \min\{P_1, \dots, P_r\} \to +\infty$.

Как известно, следствием оценки И.М. Виноградова явилась асимптотическая формула в проблеме Варинга в простых числах. В 2009 г. автор доказал, что последовательность p^n, где p пробегает все простые числа, а n — любое фиксированное натуральное число, является базисом конечного порядка для натурального ряда чисел.

§ 21. Бинарные аддитивные задачи с простыми числами

В конце 30-х годов прошлого столетия после решения И.М. Виноградовым тернарной проблемы Гольдбаха была открыта возможность оценки сверху мощности исключительного множества в бинарной проблеме Гольдбаха – Эйлера, т.е. оценки количества натуральных чисел n, не превосходящих $x \geqslant 6$, и не представимых суммой двух нечетных простых чисел. В 2002 г. Г.И. Архипов и автор доклада оценили сверху $T(x)$ — количество

$n \leqslant x$, не представимых в виде $[\lambda_1 p_1] + [\lambda_2 p_2]$, где p_1, p_2 — простые числа, λ_1, λ_2 — положительные вещественные числа, причем отношение λ_1/λ_2 является иррациональным алгебраическим числом. Имеет место неравенство $T(x) \ll_\varepsilon x^{2/3+\varepsilon}$, где $\varepsilon > 0$ — сколь угодно малое число и постоянная в знаке $\ll_\varepsilon$ — неэффективная. Первые более грубые результаты в этой задаче были получены нами в 1997 г. Заметим, что при $\lambda_1 = \lambda_2 = 1$ удается получить только оценки вида $T(x) \ll x^{1-\delta}$, где $\delta < 1/10$.

§ 22. Абсцисса и экспонента Карлсона в проблеме моментов дзета-функции Римана

Абсциссой Карлсона называют величину $\sigma_k = \sigma(k)$, определяемую соотношениями $\sigma_k = \inf\{M\}$, где M — множество всех вещественных чисел $\sigma < 1$, для которых справедлива оценка

$$I_k = I_k(\sigma, T) = T^{-1} \int\limits_1^T |\zeta(\sigma + it)|^{2k}\, dt \ll_\varepsilon T^\varepsilon,$$

где $k > 0$ и $\varepsilon > 0$ — произвольные вещественные числа. Экспонентой Карлсона называют величину $m(\sigma)$, определяемую равенством $m(\sigma) = 2f(\sigma)$, где $f(\sigma)$ — функция, обратная к $\sigma(k)$. Другими словами, функция $m(\sigma)$ определяется как $\sup\{m\}$, где $m > 0$ таково, что при произвольном $\varepsilon > 0$ выполняется оценка $\int\limits_1^T |\zeta(\sigma + it)|^{2m}\, dt \ll_\varepsilon T^{1+\varepsilon}$.

Если справедлива гипотеза Линделёфа, утверждающая, что при $t \to \infty$ справедлива оценка

$$\zeta(1/2 + it) \ll_\varepsilon |t|^\varepsilon,$$

то при всех $k > 0$ имеем $\sigma_k = 1/2$. Из оценки четвертого момента $\zeta(s)$ следует, что $\sigma_k = 1/2$ при $0 < k \leqslant 2$. При $k > 2$ из стандартных соображений устанавливается, что $\sigma_k < 1 - 1/k$. В 1981 г. Д.Р. Хис-Браун доказал, что $\sigma_8 \leqslant 5/8$, отсюда $m(5/8) \geqslant 8$. Более того, из оценки дзета-функции Римана в окрестности единичной прямой, впервые найденной Х.-Э. Рихертом (1960 г.), при $1/2 < \sigma < 1$ вытекает неравенство

$$m(\sigma) \gg_\varepsilon (1 - \sigma)^{-3/2}.$$

Г.И. Архипов, Е.Е. Баядилов и автор (2003 г.) доказали следующее утверждение. Пусть при некотором $a, 1 \leqslant a < 20$, для всех $t \geqslant 1$ и $1/2 < \sigma < 1$ справедлива оценка $\zeta(\sigma + it) \ll t^{a(1-\sigma)^{3/2}}$, и пусть $k_0 = 44 - [22/a]$. Тогда
а) для функции σ_k при всех $k \geqslant 45$ имеет место оценка

$$\sigma_k \leqslant 1 - \frac{1}{(3a(k-k_0) + (3a(k-k_0))^{1/2})^{2/3}},$$

б) при всех $\sigma \geqslant \sigma_1 = \frac{2701}{2880}$ справедливо неравенство

$$\frac{m(\sigma)}{2} \geqslant k_0 - 1 + \frac{1}{3a(1-\sigma)^{3/2}} - \frac{1}{(3a)^{1/2}(1-\sigma)^{3/4}}.$$

§ 23. Аддитивная проблема Ингама

Пусть $\tau(n)$ обозначает количество делителей натурального числа n, k — натуральное число и $\sigma_{-1}(n) = \sum\limits_{d|n} d^{-1}$. Тогда имеет место асимптотика при $x \to \infty$

$$I(x) = \sum_{n \leqslant x} \tau(n)\tau(n+k) \sim \frac{6}{\pi^2}\sigma_{-1}(k) x \ln^2 x,$$

установленная А.Е. Ингамом в 1927 г. В 1931 г. Т. Эстерман нашел асимптотическую формулу

$$I(x) = x(A_0 \ln^2 x + A_1 \ln x + A_2) + R(x),$$

где $R(x) \ll x^{11/12} \ln^{17/3} x, A_0, A_1, A_2$ — некоторые постоянные. В 1979 г. Д.И.Исмоилов, развивая элементарный метод Эстермана, получил новую оценку $R(x) \ll x^{5/6+\varepsilon}$, где $\varepsilon > 0$ — сколь угодно малая постоянная. В том же году ту же оценку другим методом, но равномерную по $k \leqslant x^{2/3}$ получил Д.Р. Хис-Браун.

В 2006 г. мы с Г.И.Архиповым доказали, что $R(x) \ll x^{3/4} \ln^4 x$.

§ 24. Распределение значений очень коротких тригонометрических сумм

Пусть $f(n)$ — периодическая функция натурального аргумента, имеющая период p. Тогда суммы вида

$$\sum_{n \leqslant h} f(n), \quad \sum_{x < n \leqslant x+h} f(n),$$

называются короткими, если длина интервала суммирования h не превосходит величины p, и эти суммы называются очень короткими, если значение h является функцией от p, удовлетворяющей условиям

$$h \to \infty, \quad \frac{\log h}{\log p} \to 0 \quad \textit{при} \quad p \to \infty.$$

§ 25. Суммы символов Лежандра

Далее, пусть p — простое число и пусть

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \textit{если} \quad a \quad \textit{квадратичный вычет} \pmod p, \\ -1, \textit{если} \quad a \quad \textit{квадратичный невычет} \pmod p, \\ 0, \textit{если} \quad a \equiv 0 \pmod p, \end{cases}$$

символ Лежандра. Положим

$$S_h(x) = \sum_{x<n\leqslant x+h} \left(\frac{n}{p}\right).$$

И. М. Виноградов и Д. Пойа (1918) при $1 \leqslant x < x + h \leqslant p$ доказали следующее неравенство

$$|S_h(x)| < \sqrt{p}\ln p.$$

Д. А. Бёрджесс (1958) получил следующий результат: для произвольной постоянной $\varepsilon > 0$ найдется функция $\delta(\varepsilon) > 0$ такая, что $S_h(x) \ll hp^{-\delta(\varepsilon)}$ as $h > p^{\frac{1}{4}+\varepsilon}$, т.е. количество квадратичных вычетов и невычетов по модулю p в интервалах $[x, x + h]$ при $h > p^{\frac{1}{4}+\varepsilon}$, асимптотически поровну.

Г. Давенпорт и П. Эрдёш (1952) для очень короткой суммы $S_h(x)$ символов Лежандра доказали следующее утверждение. Пусть $M_p(\lambda)$ обозначает количество целых чисел x таких, что $0 \leqslant x < p$ и $S_h(x) \leqslant \lambda h^{1/2}$. Тогда имеем

$$\frac{1}{p}M_p(\lambda) \to \frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{\lambda} e^{-t^2/2}\, dt \quad \textit{при} \quad p \to \infty$$

для любого фиксированного λ.

§ 26. Суммы символов Лежандра по различным модулям

Пусть $p_1, \dots, p_k$ *— различные простые числа,* $Q = p_1 \dots p_k$, $1 \leqslant x < x + h \leqslant Q$, $\varepsilon_s = \pm 1$ *as* $1 \leqslant s \leqslant k$, *и пусть* T *— количество целых чисел* n, *удовлетворяющих соотношениям*

$$\left(\frac{n + a_1}{p_1}\right) = \varepsilon_1, \dots, \left(\frac{n + a_k}{p_k}\right) = \varepsilon_k,$$

для произвольных фиксированных целых чисел $a_1, \dots, a_k$.

Автор и его ученик Э. К. Жимбо (2001) установили следующие результаты. Имеем

$$T = \frac{h}{2^k} + \theta\sqrt{Q}\ln Q$$

где $|\theta| \leqslant 1$ *и* $h > 2^k\sqrt{Q}\ln Q$.

Пусть

$$S_h(x) = S_h(x; p_1, \dots, p_k) = \left(\frac{n + a_1}{p_1}\right) \dots \left(\frac{n + a_k}{p_k}\right)$$

очень короткая сумма произведений символов Лежандра по различным модулям, т.е. $h \to \infty$, $\frac{\log h}{\log Q} \to 0$ *при* $Q \to \infty$. *Пусть* $N_Q\{x : \dots\}$ *обозначает количество целых чисел* x, *удовлетворяющих условиям, поставленным вместо точек.*

Пусть $\xi = \xi(h, Q) = \frac{S_h(x)}{\sqrt{h}}$ *— очень короткая нормированная сумма. Тогда имеем*

$$\frac{1}{Q}N_Q\{x : \xi < y\} \to \frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{y} e^{-y^2/2}\, dy \quad \textit{при} \quad Q \to \infty$$

для любого фиксированного вещественного числа y.

§ 27. Неполные суммы Гаусса

Пусть $\chi(n)$ *— неглавный характер Дирихле по простому модулю* p, $0 \leqslant x < p$, $1 \leqslant h \leqslant p$, *и* $N_p\{x : \dots\}$ *обозначает количество целых чисел* x, *удовлетворяющих условиям, указанным в скобках. Рассмотрим сумму Гаусса* $G_h(x)$ *вида*

$$G_h(x) = \sum_{n=x+1}^{x+h} \chi(x) e^{2\pi i \frac{an}{p}}.$$

Если $h = p$, то имеем полную сумму Гаусса, и $|G_p(x)| = \sqrt{p}$. При $0 < h < p$ справедлива оценка $|G_h(x)| < \sqrt{p}\log p$. Э. К. Жимбо (2001) доказал следующее утверждение. Пусть $\xi = \xi(h,p) = \left|\frac{G_h(x)}{\sqrt{h}}\right|^2$ — очень короткая нормированная сумма Гаусса. Тогда имеем

$$\frac{1}{p}N_p\{x : \xi < y\} \to 1 - e^{-y} \quad \textit{при} \quad p \to \infty$$

для любого фиксированного вещественного числа y.

§ 28. Очень короткая сумма по обратным к простым числам по произвольному простому модулю

Пусть p, q — простые числа. Пусть q^* определяется сравнением $qq^* \equiv 1 \pmod p$, $3 < h < p$, $1 \leqslant x \leqslant p-1$, и

$$K_h(x) = \sum_{q \leqslant h} e^{2\pi i \frac{xq^*}{p}}.$$

Автор и Э. К. Жимбо (2001) установили следующую теорему. Пусть $\xi = \xi(x,h) = \left|\frac{K_h(x)}{\sqrt{h}}\right|^2$ — очень короткая нормированная сумма по обратным к простым по модулю p. Тогда имеем

$$\frac{1}{p}N_p\{x : \xi < y\} \to 1 - e^{-y} \quad \textit{при} \quad p \to \infty$$

для любого фиксированного вещественного числа y.

§ 29. Очень короткие суммы характеров Дирихле по простым числам

Пусть $m > 1, n, h$ — натуральные числа, p — простые числа, и пусть $\chi(n)$ — характер Дирихле по модулю m, $\varphi(m)$ — функция Эйлера. Положим

$$D = \sum_{p \leqslant h} 1, \; S_h(\chi) = \sum_{p \leqslant h} \chi(p), \xi_h(\chi) = \left|\frac{S_h(\chi)}{\sqrt{D}}\right|^2,$$

$$N_m(\lambda) = {}^{\#}\{\chi : \xi_h(\chi) \leqslant \lambda\}.$$

Мой ученик И. С. Нгонго (2002) доказал следующую теорему. Пусть $\xi = \xi_h(\chi) = \left|\frac{S_h(\chi)}{\sqrt{D}}\right|^2$ — очень короткая нормированная сумма

характеров Дирихле по простым числам. Тогда имеем

$$\frac{N_m(\lambda)}{\varphi(m)} \to 1 - e^{-\lambda} \quad \textit{при} \quad m \to \infty$$

для любого фиксированного вещественного числа λ.

§ 30. Рациональные тригонометрические суммы по числам Фибоначчи

Дадим теперь обобщение нескольких результатов А. Г. Постникова (1959) и М. П. Минеева (1959).

Члены последовательности $\{f_n\}$, *где* $f_0 = 1$, $f_1 = 1$ *и* $f_{n+1} = f_n + f_{n-1}$ *при* $n \geqslant 1$, *называются числами Фибоначчи. Пусть* $m > 1$ — *натуральное число,* $\lambda > 0$ — *постоянная, и пусть* $N_m\{n : \dots\}$ *обозначает количество целых чисел* n, *удовлетворяющих условиям, которые указаны в скобках. Пусть, далее,*

$$S_m(h; a) = \sum_{n=0}^{h-1} e^{2\pi i \frac{a f_n}{m}}$$

очень короткая тригонометрическая сумма, и

$$N_m(\lambda) = N_m\{a : 0 \leqslant a \leqslant m-1,\ |S_m(h; a)| < \sqrt{\lambda h}\}.$$

Автор и его ученик Р. Н. Бояринов (2001) получили следующий результат. Пусть $m \to \infty$ *и* h *как функция от* m *удовлетворяет условиям* $h = h(m) \to \infty$ *и* $h \leqslant 0.5 \log_\tau m$, *где* $\tau = \frac{\sqrt{5}+1}{2}$. *Тогда справедливо соотношение*

$$\lim_{m\to\infty} \frac{N_m(\lambda)}{\lambda} = 1 - e^{-\lambda}$$

для любого фиксированного вещественного $\lambda > 0$.

§ 31. L-функции Дирихле по модулю, равному степени простого числа

В 1955 г. А.Г.Постников впервые получил принципиально новую оценку сумм неглавных характеров Дирихле по модулю, равному степени нечетного простого числа, и установил более точные границы нулей соответствующих L-*функций Дирихле, чем имеющиеся границы для произвольного модуля. Эта работа была*

продолжена С.М. Розиным, А.А. Карацубой, Н.Г. Чудаковым, автором и др. В 2000 г. мы с Б.А. Турешбаевым в окрестности единичной прямой доказали следующие оценки. Пусть χ *— примитивный характер по модулю* $D = p^k, p$ *— нечетное простое число,* $1 - 4\gamma < \sigma < 1, b = \frac{2}{3\sqrt{3\gamma}}, A > 0$ *и* $1/1024 > \gamma > 0$ *— некоторые постоянные.*

Тогда (а1) при $p \leqslant e^{Ak^2}, |t| \leqslant 2D$ *имеем*

$$|L(s,\chi)| \ll \frac{D^{b(1-\sigma)^{3/2}} \ln^{2/3} D}{(1-\sigma)^{1/4} \ln^{1/6} D + 1},$$

(а2) при $D \geqslant D_0 = D_0(A)$ *функция* $L(s,\chi)$ *не имеет нулей в области*

$$|t| \leqslant D, \quad \sigma \geqslant 1 - \frac{c}{\ln^{2/3} D (\ln\ln D)^{1/3}}, c = \frac{1}{500 b^{2/3}},$$

(б1) при $p \leqslant e^{A \ln^{2/3} |t|}, |t| \geqslant D$ *имеем*

$$|L(s,\chi)| \ll \frac{|t|^{b(1-\sigma)^{3/2}} \ln^{2/3} |t|}{(1-\sigma)^{1/4} \ln^{1/6} |t| + 1}.$$

(б2) при $D \geqslant D_0 = D_0(A)$ *функция* $L(s,\chi)$ *не имеет нулей в области*

$$|t| \geqslant D, \quad \sigma \geqslant 1 - \frac{c}{\ln^{2/3} |t| (\ln\ln |t|)^{1/3}}.$$

Список литературы

[1] Виноградов И.М. Основы теории чисел. Учеб. для вузов. 9-е изд., испр. — М.: Наука, гл. ред. физ.- мат. лит., 1981, 168 с.

[2] Виноградов И. М. Метод тригонометрических сумм в теории чисел. — М.: Труды МИАН СССР, XXIII, 1947, с.109.

[3] Виноградов,И. М. О проблемах аналитической теории чисел. Труды ноябрьской юбилейной сессии АН СССР. 1933.

[4] Виноградов,И. М. Метод тригонометрических сумм в теории чисел, 2-е изд., Москва, Наука., 1980.

[5] Vinogradov,I. M. A new method of estimation of trigonometrical sums, Math. USSR-Sb. **43***, 1936, No.2, 175–188.*

[6] Hua,L.-K. An improvement of Vinogradov's mean-value theorem and several applications, Quart. J. Math., **20***, 1949, 48–61.*

[7] Архипов,Г. И. Теорема о среднем значении модуля кратной тригонометрической суммы, Матем. заметки **17**, *1975, 84–90.*

[8] Архипов,Г. И., Чубариков,В. Н. Кратные тригонометрические суммы, Изв. АН СССР, Сер. мат. **40**, *No.1, 1976, 209–220.*

[9] Hua,L.-K. On an exponential sums, J. Chinese Math. Soc., **2**, *1940, 301–312.*

[10] Chen,J.-R. On Professor Hua's estimate on exponential sums, Acta Sci. Sinica, **20**, *1977, No.6, 711–719.*

[11] Чубариков,В. Н. О кратных рациональных тригонометрических суммах и кратных интегралах, Матем. заметки, **20**, *1976, 589–593.*

[12] Архипов,Г. И., Карацуба,А. А., Чубариков,В. Н. Тригонометрические интегралы, Изв. АН СССР, Сер. мат. **43**, *No.5, 1979, 971–1003. .*

[13] Titchmarsh,E. C. The Theory of the Riemann Zeta-function, 2nd ed., The Clarendon Press, Oxford University Press, New York, 1986.

[14] Arkhipov,G. I., Chubarikov,V. N., Karatsuba,A. A. Trigonometric Sums in Number Theory and Analysis, De Gruyter expositions in mathematics; 39, Berlin, New York, 2004.

[15] Архипов,Г. И., Осколков,К. И. Специальные тригонометрические ряды и их применения, Мат. Сб. **62**, *1989, No.2, 145–155.*

[16] Oskolkov,K. I. The I.M.Vinogradov series and integrals, and its applications, Proc. Steklov Math. Inst. of Acad. Sciences of USSR. **190**, *1989, 186–221.*

[17] Hua,L.-K. Additive theory of prime numbers. Trudy MIAN SSSR., **22**, *1947, 1–179.*

[18] Тырина,О. В. Новая оценка тригонометрического интеграла И. М. Виноградова, Изв. АН СССР, Сер. мат., **51**, *No.2, 1987, 363–378.*

[19] Hua,L.-K. On the number of solutions of Tarry's problem, Acta Sci. Sinica, **1**, *1953, 1–76.*

[20] Чубариков,В. Н. Об асимптотических формулах для интеграла И. М. Виноградова и его обобщений, Труды МИАН СССР **157**, *1981, 214–232.*

[21] Чубариков,В. Н. Оценки кратных тригонометрических сумм с простыми числами, Изв. АН СССР, Сер. мат., **49**, *No.5, 1985, 1031–1067.*

[22] Архипов Г.И., Садовничий В.А., Чубариков В.Н. Лекции по математическому анализу. Учеб. для вузов. 5-е изд., испр. — М.: Дрофа, 2005, 640 с.

Глава IX
МЕТРИЧЕСКАЯ ТЕОРИЯ ЧИСЕЛ

§ 1. Верхний и нижний пределы арифметической последовательности

Нам будут полезны следующие соотношения:

$$\overline{\lim_{n\to\infty}}\frac{\ln\tau(n)\ln\ln n}{\ln n}=\ln 2,\qquad \overline{\lim_{n\to\infty}}\frac{\omega(n)\ln\ln n}{\ln n}=\ln 2,$$

$$\overline{\lim_{n\to\infty}}\frac{\sigma(n)}{n\ln\ln n}=e^{\gamma},\qquad \underline{\lim_{n\to\infty}}\frac{\varphi(n)\ln\ln n}{n}=e^{-\gamma},$$

где $\tau(n)$ — число делителей числа n, $\omega(n)$ — число различных простых делителей числа n, $\sigma(n)$ — сумма всех делителей числа n и $\varphi(n)$ — функция Эйлера.

В курсе математического анализа доказывается, что верхний предел последовательности равен верхнему предельному числу, а нижний предел — нижнему предельному числу, т.е.

$$\overline{\lim_{n\to\infty}}f(n)=\inf_{n\geqslant 1}\sup_{m\geqslant n}f(m)=L,\qquad \underline{\lim_{n\to\infty}}f(n)=\sup_{n\geqslant 1}\inf_{m\geqslant n}f(m)=l.$$

Таким образом, для того чтобы доказать, что число L является верхним пределом последовательности $f(n)$ достаточно показать, что выполняются следующие два условия:
1) для любого натурального n имеем $\sup\limits_{m\geqslant n}f(m)\geqslant L$, т.е. найдется бесконечная последовательность натуральных чисел $m_k, k\geqslant 1$, такая, что $f(m_k)\geqslant L$,
2) для любого $\varepsilon>0$ найдется номер n_0 такой, что $\sup\limits_{m\geqslant n_0}f(m)<L+\varepsilon$, т.е. для всех номеров m, не меньших n_0, значения функции $f(m)$ меньше $L+\varepsilon$.

Это замечание полезно при доказательстве утверждений о верхних и нижних пределах функций.

§ 2. Лемма Бореля–Кателли

Многие утверждения метрической теории чисел в основе их вывода полагаются на следующую лемму Бореля – Кантелли, от-

носящуюся к событиям, которые случаются "почти наверное".

Лемма 1.2. *Пусть $A_1, A_2, \ldots$ — последовательность событий на вероятностном пространстве $(\Omega, \mathcal{B}, P)$, и пусть*

$$B = \overline{\lim_{n\to\infty}} A_n = \bigcap_{k=1}^{\infty} \bigcup_{n=1}^{\infty} A_n.$$

Тогда, если

1) ряд $\sum\limits_{n=1}^{\infty} P(A_n)$ сходится, то $P(B) = 0$;

2) события A_n независимы и ряд $\sum\limits_{n=1}^{\infty} P(A_n)$ расходится, то $P(B) = 1$.

§ 3. Ариметические следствия

В качестве арифметических следствий отсюда получаются знаменитые теорема Э.Бореля о "нормальных числах" и закон А.Я.Хинчина повторного логарифма.

Пусть x — иррациональное число, $0 < x < 1$. Разложим x в двоичную дробь. Рассмотрим первые n цифр в его разложении. Символом $\mu_n(x)$ обозначим разность между количеством нулей в его записи и числом $n/2$. Э.Борель установил, что для всех иррациональных x, за исключением множества меры нуль, при $n \to \infty$ имеем соотношение

$$\mu_n(x) = o(n).$$

В 1914 г. Ф.Хаусдорф уточнил это предельное соотношение. Он доказал, что при $\alpha > 1/2$

$$\mu_n(x) = o(n^{\alpha}).$$

В том же году Г.Харди и Дж.Литтлвуд получили, что

$$\overline{\lim_{n\to\infty}} \frac{|\mu_n(x)|}{\sqrt{n \ln n}} \leqslant \frac{\sqrt{2}}{2}.$$

С другой стороны, они доказали, что $\mu_n(x) = \Omega(\sqrt{n})$.

Теорема. (А.Я.Хинчин). *Пусть x — иррациональное число, которое представлено в виде двоичной дроби. Пусть в первых n цифрах его двоичного разложения нуль встречается $m(n)$ раз, и пусть $\mu(n) = m(n) - n/2$. Тогда для всех x, за исключением множества*

меры нуль, при $n \to \infty$ *имеем*

$$\overline{\lim_{n\to\infty}} \frac{|\mu_n(x)|}{\sqrt{n \ln\ln n}} = \frac{\sqrt{2}}{2}.$$

§ 4. Метрические теоремы о непрерывных дробях

В 1923 г. А.Я.Хинчин доказал ряд теорем метрического характера для непрерывных дробей.

Пусть x *— иррациональное число,* $0 < x < 1$. *И пусть* $a_n = a_n(x)$ *обозначает* n*-й элемент разложения числа* x *в правильную непрерывную дробь вида*

$$x = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \dots}}}.$$

Положим

$$A_n = A_n(x) = \frac{a_1 + \dots + a_n}{n}, G(n) = \sqrt[n]{a_1 \dots a_n}.$$

Теорема 3.1. *Для любого* $\varepsilon > 0$ *и каждого иррационального* x, *за исключением, быть может, множества лебеговой меры нуль, при* $n \to \infty$ *выполняются асимптотические неравенства*

$$A_n(x) \ll n^{\varepsilon}, \overline{\lim_{n\to\infty}} G(n) \leqslant e^{e^{\sqrt{2}\ln 2}}.$$

В качестве приложения А.Я.Хинчин доказывает, что оценка В.Серпинского (1910) для любого иррационального числа при $n \to \infty$ *сумм вида*

$$\sum_{k=1}^{n} \rho(kx) = o(n), \quad \rho(t) = \frac{1}{2} - \{t\},$$

неулучшаема.

Теорема 3.2. *Пусть* $\omega(n) > 0$ *— произвольная функция натурального аргумента* n *и при* $n \to \infty$ *имеем* $\omega(n) \to 0$. *Тогда найдётся иррациональное число* x *такое, что при* $n \to \infty$ *не выполняется соотношение*

$$\sum_{k=1}^{n} \rho(kx) = O(n\omega(n)).$$

Теорема 3.3. *Для любого $\varepsilon > 0$ и для любого иррационального x, за исключением, быть может, множества лебеговой меры нуль, при $n \to \infty$ выполняется асимптотическое неравенство*

$$\sum_{k=1}^{n} \rho(kx) = O(\ln^{1+\varepsilon} n).$$

Теорема 3.4. *Для любого $\varepsilon > 0$ и для любого иррационального x, за исключением, быть может, множества лебеговой меры нуль, при $n \to \infty$ выполняется асимптотическое неравенство*

$$\sum_{k=1}^{n} \rho(kx) = \Omega(\ln n).$$

§ 5. Плотность арифмпетической последовательностипо Шнирельману

Важную теорему о плотности по Л.Г.Шнирельману суммы двух множеств доказал А.Я.Хинчин.

Пусть заданы последовательности A и B неотрицательных целых чисел

$$A = \{a_0 = 0 < a_1 < a_2 < \dots\}, \quad B = \{b_0 = 0 < b_1 < b_2 < \dots\},$$

и пусть $A(n), n \geqslant 0$, обозначает число элементов последовательности A, не превосходящих n.

Назовём, следуя Л.Г.Шнирельману, плотностью последовательности A величину

$$D(A) = \inf_{n>0} \frac{A(n) - 1}{n}.$$

Определим, далее, сумму $C = \{c_0 = 0 < c_1 < c_2 < \dots\}$ двух последовательностей A и B соотношением вида

$$C = A + B = \{c = a + b | a \in A, b \in B\}.$$

Пример. Пусть $A = B = \{0, 1, 2, 6, 7, 8, 12, \dots\}$. Тогда

$$C = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, \dots\},$$

$A(5)-1=2, D(A)=\dfrac{2}{5}, C(11)-1=9, D(C)=\dfrac{9}{11}, D(A)+D(B)=\dfrac{4}{5}<\dfrac{9}{11}=D($

Теорема 4.1. *Пусть* $D(A_1)=\cdots=D(A_k)$. *Тогда*

$$D(\sum_{r=1}^{k} A_r) \geqslant \min\{1, \sum_{r=1}^{k} D(A_r)\}.$$

В 1942 г. Г.Б.Манн распространил это утверждение на последовательности с разными плотностями.

§ 6. Хинчиновский принцип переноса

В 1926 г. А.Я.Хинчин изучил один класс линейных диофантовых приближений.

В этом исследовании А.Я.Хинчин отталкивается от известной **теоремы Л.Кронекера.** *Пусть действительные числа* $\theta_1, \theta_2, \ldots, \theta_m$ *линейно независимы над кольцом целых чисел. Тогда точки*

$$(\{n\theta_1\}, \{n\theta_2\}, \ldots, \{n\theta_n\})$$

образуют в единичном m*-мерном кубе всюду плотное множество.*

Обозначим символом $\|\theta\| = \min(\{\theta\}, 1-\{\theta\})$ *расстояние до ближайшего целого числа. Имеем, что* $\|\theta_1+\theta_2\| \leqslant \|\theta_1\|+\|\theta_2\|$ *и для любого целого* n *справедливо неравенство* $\|n\| \leqslant |n| \cdot \|\theta\|$.

Теорема 5.1. *(*А.Я.Хинчин: принцип переноса). *Пусть* $\theta_1, \theta_2, \ldots, \theta_n$ *— любые иррациональные числа, и пусть* $\omega_1 \geqslant 0, \omega_2 \geqslant 0$ *являются соответственно точными верхними гранями чисел* ω, ω' *таких, что неравенства*

$$\|u_1\theta_1+\cdots+u_n\theta_n\| \leqslant (\max_{1\leqslant j\leqslant n}|u_j|)^{-n-\omega},$$

$$\max_{1\leqslant j\leqslant n}\|x\theta_j\| \leqslant x^{-(1+\omega')/n}$$

имеют бесконечно много решений в целых числах $u_1, \ldots, u_n, x$. *Тогда*

$$\omega_1 \geqslant \omega_2 \geqslant \frac{\omega_1}{n^2+(n-1)\omega_1}.$$

§ 7. Принцип переноса для сингулярных систем линейных уравнений (1948)

Пусть задана система n линейных форм вида

$$L_j(\mathbf{x}) = \sum_{i=1}^{m} \theta_{ji} x_i \quad (1 \leqslant j \leqslant n),$$

и пусть задана транспонированная система m линейных форм вида

$$M_i(u) = \sum_{j=1}^{n} \theta_{ji} u_j \quad (1 \leqslant i \leqslant m).$$

Система из n линейных форм $L_j(\mathbf{x})$ называется *сингулярной*, если для любого $\varepsilon > 0$ найдётся $X_0 = X_0(\varepsilon)$ такое, что для всех $X > X_0$ система неравенств

$$\|L(\mathbf{x})\| < \varepsilon X^{-m/n}, |x_i| \leqslant X,$$

имеет целое решение $\mathbf{x} \neq \mathbf{0}$. В противном случае система называется *регулярной*.

Заметим, что множество коэффициентов θ_{ji} образует в mn-мерном пространстве множество лебеговой меры нуль (по лемме Бореля – Кантелли).

Теорема 6.1. *Для того, чтоб система $L_j(\mathbf{x})$ была сингулярна, необходимо и достаточно, чтобы была сингулярна транспонированная система $M_i(\mathbf{u})$.*

§ 8. Количественная концепция аппроксимационной теории Кронекера (1948)

Основной результат аппроксимационной теории Кронекера — критерий того, чтобы система неравенств

$$|\sum_{i=1}^{m} \theta_{ij} x_i - y_j - \alpha_j| < \frac{1}{t} \qquad (1 \leqslant j \leqslant n),$$

где θ_{ij} и α_j — вещественные числа, имела при любом $t > 0$ решения в целых числах x_i, y_j.

А.Я.Хинчин решает следующую задачу: найти критерий того, чтобы система неравенств

$$|\sum_{i=1}^{m} \theta_{ij} x_i - y_j - \alpha_j| < \frac{c_1}{t} \qquad (1 \leqslant j \leqslant n),$$

где θ_{ij} и α_j — вещественные числа, имела при любом $t > 0$ решения в целых числах x_i, y_j при условии, что

$$|x_i| < c_2\varphi(t) \qquad (1 \leqslant i \leqslant m),$$

причём c_1 и c_2 — некоторые положительные постоянные, а $\varphi(t)$ — любая положительная непрерывная неубывающая функция от t.

Для дальнейшего изучения теории чисел можно рекомендовать статьи и книги, приведенные в списке литературы.

Список литературы

[1] *Adleman L. M., Rivest R. L., Shamir A.* A method for obtaining digital signatures and public-key cryptosystems// Comm. ACM. 1978. V. 21. 120–126.

[2] *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел. М.: Мир, 1967.

[3] *Анохин М. И., Варновский Н. П., Сидельников В. М., Ященко В. В.* Криптография в банковском деле — М.: МИФИ, 1997. — 274 с.

[4] *Архипов Г. И., Садовничий В. А., Чубариков В. Н.* Лекции по математическому анализу. — М.: Дрофа, 2004.

[5] *Боревич З. И., Шафаревич И. Р.* Теория чисел. М.: Наука, 1985.

[6] *Бюлер В.* Гаусс. М.: Наука, 1989.

[7] *Венков Б. А.* Элементарная теория чисел. М.—Л.: ОНТИ, 1937.

[8] *Виноградов И. М.* Основы теории чисел. М.: Наука, 1982.

[9] *Виноградов И. М.* Представление нечетного числа суммою трех простых слагаемых // ДАН СССР. 1937. **15.** 291–294.

[10] *Виноградов И. М.* Элементы высшей математики (Аналитическая геометрия. Дифференциальное исчисление. Основы теории чисел). Учеб. для вузов. М.: Высшая школа, 1999.

[11] *Gardner M.* A new kind of cipher that would take millions of years to break// Sci. Amer. 1977. P. 120–124

[12] *Гаусс К. Ф.* Труды по теории чисел. М.: Изд-во АН СССР, 1959.

[13] *Гашков С. Б., Чубариков В. Н.* Арифметика. Алгоритмы. Сложность вычислений. М.: Высшая школа, 1999.

[14] *Гекке Э.* Лекции по теории алгебраических чисел. М.—Л.: ГИТТЛ, 1940.

[15] *Gelfond A. O.* Sur les nombres qui out des propriétés additives et multiplicatives données // Acta arithm. 1968. **13.** 259–265.

[16] *Делоне Б. Н.* Петербургская школа теории чисел. М.—Л.: Изд-во АН СССР, 1947.

[17] *Diffie W., Hellman M. E.* New directions in cryptography// IEEE Transactions on Information Theory. 1976. V. 22. 644–654

[18] *Дирихле Лежен П. Г.* Лекции по теории чисел. М.—Л.: ОНТИ, 1936.

[19] *Егоров Д. Ф.* Элементы теории чисел. М.—П.: ГИ, 1923.

[20] *Ингам А. Е.* Распределение простых чисел. М.—Л.: ОНТИ, 1936.

[21] *Касселс Дж. В. С.* Введение в геометрию чисел. М.: Мир, 1965.

[22] *Касселс Дж. В. С.* Введение в теорию диофантовых приближений. М.: ИЛ, 1961.
[23] *Карацуба А. А.* Основы аналитической теории чисел. М.: Наука, 1983.
[24] *Коблиц Н.* Курс теории чисел и криптографии — М.: Научное изд-во ТВП, 2001. — 254 с.
[25] *van der Corput J. G.* On de Polignac's conjecture // Simon Stevin. 1950. **27.** 99–105.
[26] *McCurley K. S.* A key distribution system equivalent to factoring// J. of Cryptology. 1988. V. 1, № 2. P. 95–105.
[27] *Nagell T.* Introduction to the number theory. 1951.
[28] *Нечаев В. И.* Элементы криптографии (Основы теории защиты информации): Учеб. пособие для ун-тов и пед. вузов — М.: Высш. шк., 1999. — 109 с.
[29] *Постников А. Г.* Введение в аналитическую теорию чисел. М.: Наука, 1971.
[30] *Постникова Л. П.* Тригонометрические суммы и теория сравнений по простому модулю. М: МГПИ, 1973.
[31] *Rankin R. A.* On the difference between consecutive prime numbers // J. London Math. Soc. 1938. **13.** 242–247.
[32] *Rankin R. A.* On the difference between consecutive prime numbers II // Proc. Cambridge Phil. Soc. 1940. **36.** 255–256.
[33] *Romanoff N. P.* Über einige Satze der additiven Zahlentheorie // Math. Ann. 1934. **109.** 668–678.
[34] *Рябко Б. Я., Фионов А. Н.* Основы современной криптографии для специалистов в информационных технологиях — М.: Научный мир, 2004. — 173 с.
[35] *Slowinski D.* Searching for the 27th Mersenne prime // J. Recreational Mathematics. 1979. **11.** 258–261.
[36] *Трост Э.* Простые числа. М: Физматлит, 1959.
[37] *Хассе Г.* Лекции по теории чисел. М: ИЛ, 1953.
[38] *Хооли К.* Применения методов решета в теории чисел. М: Наука, 1983.
[39] *Hagis, Jr., P.* A lower bound for the set off odd perfect numbers // Math. Comp. 1973. **27.** 951–953.
[40] *Hagis, Jr., P. and McDaniel W. L.* On the largest prime divisor of an odd perfect number II // Math. Comp. 1975. **29.** 922–924.
[41] *Chen J.-R.* On the representation of a large even integer as the sum a prime and the product of at most two primes // Sci. Sinica. 1973. **16.** 157–176.

[42] *Чандрасекхаран К.* Арифметические функции. М.: Наука, 1975.
[43] *Чебышёв П. Л.* Полное собрание сочинений, т. 1. М.—Л.: Изд-во АН СССР, 1944.
[44] *Чудаков Н. Г.* Введение в теорию L-функций Дирихле. М.—Л.: ГИТТЛ, 1947.
[45] *Shmuely Z.* Composite Diffie—Hellman public-key generating systems are hard to break// Comp. Sci. Dept. Tech., IIT. Febr. 1985. TR 356.
[46] *Шнирельман Л. Г.* Простые числа. М.—Л.: ГИТТЛ, 1940.
[47] *Erdös P.* On the difference of consecutive primes // Quart. J. Oxford. 1935. **6.** 124–128.
[48] *Erdös P.* On integers of the form $2^k + p$ // Summa Brasil. Math. 1950. **2.** 113–123.
[49] ГОСТ Р34.11–94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
[50] FIPS 186–2. Digital signature standart. http://csrc.nist.gov/publications/