Министерство образования и науки Российской Федерации
Сибирский федеральный университет

# ТЕОРИЯ ЧИСЕЛ

Учебное пособие

*Электронное издание*

Красноярск
СФУ
2016

УДК 511(07)
ББК 22.13я73
Т338

Составители: Осипов Николай Николаевич
Медведева Мария Ивановна

Т338 **Теория чисел** : учебное пособие [Электронный ресурс] / сост. Н.Н. Осипов, М.И. Медведева. – Электрон. дан. – Красноярск : Сиб. федер. ун-т, 2016. – 98 с. – Систем. требования: PC не ниже класса Pentium I; 128 Mb RAM; Windows 98/XP/7/8/10; Adobe Reader V8.0 и выше. – Загл. с экрана.

Учебное пособие составлено в соответствии с рабочей программой дисциплины «Теория чисел» и включает в себя следующ,ие разделы: делимость целых чисел, распределение простых чисел, сравнения по модулю, кольца классов вычетов, некоторые приложения к криптографии.

Предназначено для студентов специальности 01.03.04 «Прикладная математика».

УДК 511(07)
ББК 22.13я73



Электронное учебное издание

Подготовлено к публикации издательством
Библиотечно-издательского комплекса

Подписано в свет 10.05.2016. Заказ № 1430
Тиражируется на машиночитаемых носителях

Библиотечно-издательский комплекс
Сибирского федерального университета
660041, г. Красноярск, пр. Свободный, 82а
Тел. (391) 206-26-67; http://bik.sfu-kras.ru
E-mail: publishing_house@sfu-kras.ru

# Содержание

# Предисловие

Настоящее учебное пособие представляет собой конспект лекций, составленный в соответствии с рабочей программой дисциплины «Теория чисел» и предназначенный для студентов специальности 01.03.04 «Прикладная математика».

Основное внимание в лекциях уделяется *элементарной теории чисел*, а именно, следующим её главам: теории делимости (раздел 1) и теории сравнений (раздел 3).

Поскольку студенты уже знакомы с элементами абстрактной алгебры, у лектора появляется возможность привлекать алгебраические методы для изучения колец и полей классов вычетов (раздел 4). Эти объекты, хотя и являются алгебраическими по своей природе, естественным образом возникают в самой теории чисел и занимают в ней важное место. По мнению авторов, «родной» алгебраический взгляд на них способствует как упрощению доказательств, так и более глубокому пониманию идей, лежащих в основе некоторых классических фактов элементарной теории чисел (таких, как малая теорема Ферма, теорема Эйлера, теорема Вильсона и др.).

Раздел 5 посвящён избранным вопросам *алгоритмической теории чисел*, имеющим прикладное значение. В частности, рассказывается о приложении теории сравнений к криптографии (на примере RSA, одной из самых распространённых систем шифрования с открытым ключом).

Для реализации многих криптосистем необходимы большие простые числа, в связи с чем нельзя было не затронуть вопросы распределения простых чисел, которые традиционно относятся к *аналитической теории чисел*. Этому посвящён раздел 2, представляющий собой своеобразный мостик между элементарной теорией чисел и аналитической, использующей мощный аппарат теории функций комплексного переменного. Здесь приводится доказательство классических оценок Чебышёва для функции $\pi(x)$ и доказывается постулат Бертрана — то, что можно сделать сравнительно легко и элементарными средствами.

Каждый раздел имеет свою нумерацию «теоремоподобных» конструкций — определений, лемм, самих теорем и т. д. Решению более семи десятков упражнений, равномерно распределённых по всему тексту лекций, отводится важная роль, и этим не стоит пренебрегать даже при первом чтении лекций.

Разумеется, чтение лекций не отменяет чтение более подробно и основательно написанных руководств по теории чисел и её приложениям (см. список литературы).

# 1 Теория делимости

## 1.1 Делимость целых чисел. Наибольший общий делитель

Отношение делимости на множестве целых чисел. Деление целых чисел с остатком. Наибольший общий делитель целых чисел. Алгоритм Евклида для вычисления НОД $(a, b)$, его вычислительная сложность. Линейная форма НОД $(a, b)$. Свойства и алгоритм вычисления наибольшего общего делителя нескольких чисел.

Объектом исследования в элементарной теории чисел является *множество целых чисел*

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Как алгебраическая структура $\mathbb{Z}$ — это *коммутативное кольцо с единицей и без делителей нуля*.

На множестве $\mathbb{Z}$ можно ввести *отношение делимости*, которое играет важную роль в изучении свойств целых чисел.

**Определение 1.1.** Пусть $a,\ b \in \mathbb{Z}$. Будем говорить, что $a$ *делится на* $b$ (или $b$ *делит* $a$), если существует такое $q \in \mathbb{Z}$, что $a = bq$.

Обозначение: $b \mid a$.

Если число $a$ делится на $b$, то число $b$ называется *делителем* числа $a$, а число $a$ — *кратным* числа $b$. Число $q = a/b$ при этом называется *частным* от деления $a$ на $b$.

Перечислим теперь простейшие *свойства отношения делимости*, прямо вытекающие из определения 1.1 (ниже буквы $a$, $b$, $c$ и т. д. обозначают целые числа).

**1.** $a \mid a$ для любого $a$.

**2.** Если $b \mid a$ и $c \mid b$, то $c \mid a$.

Свойства 1 и 2 являются свойствами *рефлексивности* и *транзитивности* отношения делимости соответственно. Свойство *симметричности* (если $a$ делится на $b$, то $b$ делится на $a$) не имеет места, поэтому отношение делимости не является отношением эквивалентности на множестве $\mathbb{Z}$.

**3.** $\pm 1 \mid a,\ b \mid 0$ для любых $a$, $b$.

**4.** Если $b \mid a$, то $(\pm b) \mid (\pm a)$.

**5.** Если $b \mid a$, то $b \mid (ac)$ для любого $c$.

**6.** Если $b \mid a_1$ и $b \mid a_2$, то $b \mid (a_1 \pm a_2)$.

**7.** Если $b \mid a_1, \ldots, b \mid a_n$, то $b \mid (a_1c_1 + \ldots + a_nc_n)$ для любых $c_1, \ldots, c_n$.

**8.** Если
$$a'_1c'_1 + \ldots + a'_nc'_n = a''_1c''_1 + \ldots + a''_mc''_m + a$$
и известно, что $b \mid a'_1, \ldots, b \mid a'_n, b \mid a''_1, \ldots, b \mid a''_m$, то $b \mid a$.

**9.** Если $b \mid a$ и $a \neq 0$, то $|a| \geqslant |b|$.

**10.** Если $b \mid a$ и $a \mid b$, то $a = \pm b$.

Докажем, например, свойство 9. По определению делимости $a = bq$ для некоторого $q \in \mathbb{Z}$, при этом $q \neq 0$ (иначе было бы $a = 0$). Следовательно, $|q| \geqslant 1$ и поэтому
$$|a| = |b| \cdot |q| \geqslant |b|.$$

**Упражнение 1.1.** Докажите остальные свойства отношения делимости.

Очевидно, не любые два целых числа связаны отношением делимости (например, ни 16 не делится на 7, ни 7 не делится на 16). Однако всегда можно использовать так называемое *деление с остатком*.

**Определение 1.2.** Пусть $a, b \in \mathbb{Z}$ и $b \neq 0$. *Разделить $a$ на $b$ с остатком* — это значит представить число $a$ в виде
$$a = bq + r, \tag{1.1}$$
где $q, r \in \mathbb{Z}$ и выполнено условие $0 \leqslant r < |b|$.

В равенстве (1.1) число $a$ называют *делимым*, число $b$ — *делителем*, число $q$ — *неполным частным*, число $r$ — *остатком от деления*.

**Пример 1.1.** $16 = 7 \cdot 2 + 2$, $-41 = 5 \cdot (-9) + 4$.

**Теорема 1.1.** Для любых $a, b \in \mathbb{Z}$ и $b \neq 0$ возможно, и причём единственным образом, разделить $a$ на $b$ с остатком.

Доказательство. Пусть $b > 0$. Очевидно, существует такое $q \in \mathbb{Z}$, для которого
$$bq \leqslant a < b(q+1).$$
Положим $r = a - bq$. Тогда $a = bq + r$, при этом $0 \leqslant r < b$, т. е. $a$ можно разделить на $b$ с остатком.

Если же $b < 0$, то разделим $a$ на $(-b)$ с остатком:
$$a = (-b)q + r, \tag{1.2}$$
где $0 \leqslant r < -b = |b|$. Осталось переписать (1.2) в виде $a = b(-q) + r$.

Покажем, что деление с остатком возможно только единственным образом. Пусть
$$a = bq_1 + r_1 = bq_2 + r_2,$$
где $0 \leqslant r_i < |b|$. Отсюда $r_2 - r_1 = b(q_1 - q_2)$, т. е. $r_2 - r_1$ делится на $b$. Однако $|r_2 - r_1| < |b|$, поэтому $r_2 - r_1 = 0$, т. е. $r_2 = r_1$. Но тогда и $q_2 = q_1$. □

**Замечание 1.1.** Если $r = 0$, то говорят о *делимости нацело* (в этом случае $a$ делится на $b$ в смысле определения 1.1).

Пусть $a_1, \ldots, a_n \in \mathbb{Z}$, при этом не все эти числа равны нулю.

**Определение 1.3.** Наибольший (по величине) общий делитель чисел $a_1, \ldots, a_n$ называется их *наибольшим общим делителем*.

Обозначение: НОД $(a_1, \ldots, a_n)$.

Ясно, что

$$\text{НОД}\,(a_1, \ldots, a_n) = \text{НОД}\,(|a_1|, \ldots, |a_n|),$$

поэтому при вычислении наибольших общих делителей можно ограничиться рассмотрением только натуральных чисел.

Рассмотрим сначала случай двух чисел ($n = 2$, $a_1 = a$, $a_2 = b$).

**Лемма 1.1.** Если $a,\ b,\ q,\ r \in \mathbb{Z}$ связаны равенством

$$a = bq + r,$$

то множество общих делителей чисел $a$ и $b$ совпадает с множеством общих делителей чисел $b$ и $r$. В частности, НОД $(a, b) =$ НОД $(b, r)$.

Доказательство. Если $d$ — общий делитель $a$ и $b$, то $d$ делит $r = a - bq$, т. е. является общим делителем $b$ и $r$. Обратное утверждение столь же очевидно. □

**Лемма 1.2.** Если $a$ делится на $b > 0$, то НОД $(a, b) = b$. В частности, НОД $(0, b) = b$.

Доказательство. Действительно, все общие делители чисел $a$ и $b$ находятся среди делителей числа $b$. □

Евклид (IV — III вв. до н. э.) в книге VII своих знаменитых «Начал» изложил способ нахождения наибольшего общего делителя двух чисел, который известен теперь как способ последовательного деления с остатком или *алгоритм Евклида*.

**Теорема 1.2.** Пусть $a \geqslant b \geqslant 1$. Если $a$ делится на $b$, то

$$\text{НОД}\,(a, b) = b.$$

Иначе, полагая $r_{-1} = a$ и $r_0 = b$, для некоторого $n \geqslant 1$ будем иметь

$$r_{k-2} = r_{k-1}q_{k-1} + r_k, \quad k = 1, \ldots, n,$$
$$r_{n-1} = r_n q_n + 0,$$
$$b > r_1 > r_2 > \ldots > r_{n-1} > r_n > 0.$$

Тогда НОД $(a, b) = r_n$ — последний отличный от нуля остаток.

Доказательство. Число $n$ существует, ибо деления с остатком не могут продолжаться бесконечно (остатки убывают). Применив $n$ раз лемму 1.1 и один раз лемму 1.2, получим цепочку равенств

$$\text{НОД}\,(a, b) = \text{НОД}\,(b, r_1) = \text{НОД}\,(r_1, r_2) = \ldots = \text{НОД}\,(r_{n-1}, r_n) = r_n,$$

откуда и следует утверждение теоремы. □

Анализируя алгоритм Евклида, можно обнаружить следующее важное свойство наибольшего общего делителя двух чисел:

**1.** НОД $(a, b)$ делится на любой общий делитель чисел $a$ и $b$.

Это свойство часто принимают за определение наибольшего общего делителя.

**Пример 1.2.** Найдём $d = \text{НОД}\,(525, 231)$.
Имеем

$$525 = 231 \cdot 2 + 63, \quad 231 = 63 \cdot 3 + 42, \quad 63 = 42 \cdot 1 + 21, \quad 42 = 21 \cdot 2 + 0.$$

Таким образом, $d = 21$.

Какова *вычислительная сложность* алгоритма Евклида? Другими словами, насколько большим может оказаться число необходимых делений с остатком? (В наших обозначениях это число равно $n + 1$.)

**Лемма 1.3.** Если $a \geqslant b \geqslant 1$, то $r < a/2$, где $r$ — остаток от деления $a$ на $b$.

Доказательство. Действительно, имеем $a = bq + r$. Если предположить, что $r \geqslant a/2$, то получим

$$b \leqslant bq = a - r \leqslant a/2 \leqslant r,$$

т. е. $b \leqslant r$ — противоречие с определением остатка. □

Зафиксируем $a$ и случайным образом выберем $b \in [1, a]$. Пусть $r$ — остаток от деления $a$ на $b$. Что более вероятно: $r < b/2$ или $r \geqslant b/2$?

Оказывается, вероятность первого события почти в два раза больше, чем вероятность второго — она асимптотически равна

$$2 - 2\ln 2 \approx 61\%.$$

Действительно, количество тех $b$, для которых $r < b/2$, равно

$$\sum_{q=1}^{a} \left( \left[\frac{a}{q}\right] - \left[\frac{a}{q + 1/2}\right] \right) = 2a + 2\sum_{q=1}^{a} \left[\frac{a}{q}\right] - \sum_{q=1}^{2a} \left[\frac{2a}{q}\right].$$

Используя *формулу Дирихле* (1.16), нетрудно показать, что

$$2a + 2\sum_{q=1}^{a} \left[\frac{a}{q}\right] - \sum_{q=1}^{2a} \left[\frac{2a}{q}\right] = a(2 - 2\ln 2) + o(a)$$

при $a \to \infty$.

В следующей теореме содержится оценка сверху для числа шагов алгоритма Евклида.

**Теорема 1.3.** Если $a \geqslant b \geqslant 1$ и $a$ не делится на $b$, то

$$n < 2\log_2 b + 1,$$

где $n$ — количество делений с остатком в алгоритме Евклида.

Доказательство. По индукции с помощью леммы 1.3 легко вывести неравенства

$$r_{2s-1} < \frac{b}{2^{s-1}}, \quad r_{2s} < \frac{b}{2^s}.$$

Отсюда

$$r_k < \frac{b}{2^{(k-1)/2}}$$

для любого $k$. Положив $k = n$ и заметив, что $r_n \geqslant 1$, получим

$$1 < \frac{b}{2^{(n-1)/2}},$$

что равносильно доказываемому неравенству. □

Оценку из теоремы 1.3 можно немного улучшить. Пусть $\{F_k\}$ — *последовательность Фибоначчи*, заданная рекуррентно:

$$F_1 = F_2 = 1, \quad F_{k+1} = F_k + F_{k-1}.$$

Имеем $r_n \geqslant 1 = F_2$, $r_{n-1} \geqslant r_n + 1 \geqslant 2 = F_3$,

$$r_{n-2} = r_{n-1}q_{n-1} + r_n \geqslant r_{n-1} + r_n \geqslant F_2 + F_3 = F_4$$

и так далее до $r_0 = b \geqslant F_{n+2}$. Из *формулы Бине*

$$F_k = \frac{\Phi_+^k - \Phi_-^k}{\sqrt{5}}, \quad \Phi_\pm = \frac{1 \pm \sqrt{5}}{2},$$

следует неравенство

$$F_{n+2} > \frac{\Phi_+^{n+2}}{\sqrt{5}} - 1.$$

Таким образом, имеем

$$b > \frac{\Phi_+^{n+2}}{\sqrt{5}} - 1,$$

откуда нетрудно вывести оценку

$$n < 5 \lg b.$$

Данное неравенство в 1845 году доказал французский математик и инженер Г. Ламе (1795 — 1870). Приведённое рассуждение также показывает, что оценку из теоремы 1.3 нельзя существенно улучшена. Действительно, для пары чисел $a = F_{k+1}$, $b = F_k$ при $k \geqslant 3$ имеем

$$n = k - 2 > C \log_2 F_k,$$

где константа $C > 0$ не зависит от $k$.

Следующее утверждение известно как *теорема о линейном представлении*.

**Теорема 1.4.** Существуют такие $x_0,\ y_0 \in \mathbb{Z}$, что

$$\text{НОД}\,(a, b) = ax_0 + by_0.$$

Доказательство. Обозначим через $d$ *наименьшее* натуральное число, которое представимо в виде $ax + by$, где $x,\ y \in \mathbb{Z}$. Тогда $d = ax_0 + by_0$ для некоторых $x_0,\ y_0 \in \mathbb{Z}$.

Осталось показать, что $d = \text{НОД}\,(a, b)$. □

**Упражнение 1.2.** Закончите доказательство теоремы 1.4.

*Указание.* Достаточно убедиться в том, что $d$ — делитель $a$ и $b$. Для этого разделите, например, $a$ на $d$ с остатком: $a = dq + r$, где $0 \leqslant r < d$.

**Замечание 1.2.** Пара $(x_0, y_0)$ определяется не единственным образом: всегда можно заменить $x_0$ на $x_0 + tb$, а $y_0$ — на $y_0 - ta$.

**Пример 1.3.** Найдём линейное представление $\text{НОД}\,(525, 231)$.

Как следует из примера 1.2,

$$\begin{gathered}\text{НОД}\,(525, 231) = \boxed{\mathbf{21}} = \\ = \mathbf{63} \cdot 1 + \boxed{\mathbf{42}} \cdot (-1) = \mathbf{63} \cdot 1 + (\mathbf{231} + \mathbf{63} \cdot (-3)) \cdot (-1) = \\ = \mathbf{231} \cdot (-1) + \boxed{\mathbf{63}} \cdot 4 = \mathbf{231} \cdot (-1) + (\mathbf{525} + \mathbf{231} \cdot (-2)) \cdot 4 = \\ = \mathbf{525} \cdot 4 + \mathbf{231} \cdot (-9),\end{gathered}$$

т. е. можно положить $x_0 = 4$ и $y_0 = -9$.

**Замечание 1.3.** Можно параллельно находить наибольший общий делитель и его линейное представление. Определим пары чисел

$$(u_k, v_k), \quad k = 0,\ 1,\ \ldots,\ n,$$

рекуррентным правилом:

$$(u_k, v_k) = (u_{k-2} - q_{k-1}u_{k-1}, v_{k-2} - q_{k-1}v_{k-1})$$

при $k \geqslant 2$ и $(u_0, v_0) = (0, 1)$, $(u_1, v_1) = (1, -q_0)$. Тогда

$$r_k = au_k + bv_k, \quad k = 0,\ 1,\ \ldots,\ n.$$

При $k = n$ получим

$$\text{НОД}\,(a, b) = au_n + bv_n$$

и можно положить $x_0 = u_n$, а $y_0 = v_n$. Этот способ, известный как *расширенный алгоритм Евклида*, конструктивно доказывает теорему 1.4.

Перечислим другие свойства наибольшего общего делителя двух чисел, непосредственно вытекающие из алгоритма Евклида (далее $a$, $b$, $c$ обозначают натуральные числа).

**2.** $\text{НОД}\,(ac, bc) = c\,\text{НОД}\,(a, b)$ для любого $c$.

**3.** Если $c \mid a$ и $c \mid b$, то $\text{НОД}\,(a/c, b/c) = \text{НОД}\,(a, b)/c$.

Следует отметить, что свойство 3 представляет собой лишь другую (иногда более удобную) форму записи свойства 2.

Вернёмся к рассмотрению общего случая. Для чисел $a_1, \ldots, a_n$, среди которых есть отличные от нуля, также справедлива теорема о линейном представлении их наибольшего общего делителя.

**Упражнение 1.3.** Сформулируйте её и докажите.

*Указание.* Можно рассуждать неконструктивно (см. доказательство теоремы 1.4).

Эта теорема, в частности, позволяет распространить свойство 1 наибольшего общего делителя двух чисел на произвольное их количество.

**Теорема 1.5.** $\text{НОД}\,(a_1, \ldots, a_{n-1}, a_n) = \text{НОД}\,(\text{НОД}\,(a_1, \ldots, a_{n-1}), a_n)$.

ДОКАЗАТЕЛЬСТВО. Достаточно заметить, что множество общих делителей чисел $a_1, \ldots, a_n$ совпадает с множеством общих делителей двух чисел: $\text{НОД}\,(a_1, \ldots, a_{n-1})$ и $a_n$. □

Применяя теорему 1.5 и рассуждая по индукции, можно получить свойства наибольшего общего делителя, аналогичные указанным выше свойствам 2 и 3. Теорема 1.5 вместе с алгоритмом Евклида дают также практический способ вычисления наибольшего общего делителя нескольких чисел. Ещё один способ представлен в следующем упражнении.

**Упражнение 1.4.** Пусть на доске написаны несколько натуральных чисел. К ним применяют следующую операцию: выбирают произвольно два числа и наибольшее из них заменяют остатком от деления на наименьшее из них (если остаток равен нулю, его стирают). Докажите, что после нескольких таких операций на доске останется одно число — наибольший общий делитель исходных чисел.

*Указание.* Эта операция не меняет наибольшего общего делителя написанных на доске чисел.

**Пример 1.4.** Покажем этим способом, что $\text{НОД}\,(5, 34, 52, 15) = 1$:

$$\{\boxed{5}, 34, \boxed{52}, 15\} \to \{5, \boxed{34}, \boxed{2}, 15\} \to \{5, \boxed{2}, \boxed{15}\} \to \{\boxed{5}, 2, \boxed{1}\} \to \{\boxed{2}, \boxed{1}\} \to \{1\}.$$

## 1.2 Взаимно простые числа. Наименьшее общее кратное. Китайская теорема об остатках

Взаимно простые числа. Критерий взаимной простоты. Основные свойства взаимно простых чисел. Наименьшее общее кратное целых чисел: свойства и алгоритм вычисления. Китайская теорема об остатках.

**Определение 1.4.** Числа $a_1, \ldots, a_n$ называются *взаимно простыми*, если

$$\text{НОД}\,(a_1, \ldots, a_n) = 1.$$

Если $\text{НОД}\,(a_1, \ldots, a_n) = d$, то, как это следует из определения, числа $a_1/d, \ldots, a_n/d$ будут взаимно простыми.

Для двух чисел имеет место следующий критерий их взаимной простоты.

**Теорема 1.6.** Числа $a,\ b \in \mathbb{Z}$ взаимно просты тогда и только тогда, когда найдутся такие $x_0,\ y_0 \in \mathbb{Z}$, что

$$ax_0 + by_0 = 1.$$

Доказательство. Утверждение «тогда» очевидно, а утверждение «только тогда» является частным случаем теоремы 1.4. □

**Замечание 1.4.** Аналогичный критерий справедлив и для произвольного количества чисел $a_1, \ldots, a_n$.

Сформулируем и докажем *свойства взаимно простых чисел* (далее $a, b, c$ — произвольные целые числа).

1. Если $a \mid bc$ и $\text{НОД}\,(a, b) = 1$, то $a \mid c$.
2. Пусть $\text{НОД}\,(a, b) = 1$. Если $a \mid c$ и $b \mid c$, то $ab \mid c$.
3. Если $\text{НОД}\,(a, b) = 1$, то $\text{НОД}\,(ac, b) = \text{НОД}\,(c, b)$ для любого $c$.
4. Если $\text{НОД}\,(a, c) = 1$ и $\text{НОД}\,(b, c) = 1$, то $\text{НОД}\,(ab, c) = 1$.

Доказательство. Основная идея — использовать критерий взаимной простоты (теорема 1.6).

**1.** Для некоторых $x_0,\ y_0 \in \mathbb{Z}$ имеем

$$ax_0 + by_0 = 1.$$

Умножив на $c$, получим $acx_0 + bcy_0 = c$, откуда $a \mid c$.

**2.** Имеем $c = ac_1$ для некоторого $c_1 \in \mathbb{Z}$. Поскольку $b \mid ac_1$ и $\text{НОД}\,(a, b) = 1$, имеем $b \mid c_1$. Значит, $c_1 = bc_2$ для некоторого $c_2 \in \mathbb{Z}$. Таким образом, $c = abc_2$, а значит, $ab \mid c$.

**3.** Пусть $d$ — произвольный общий делитель чисел $ac$ и $b$. Убедимся, что $d$ — делитель $c$. Действительно, для некоторых $x_0,\ y_0 \in \mathbb{Z}$ имеем

$$ax_0 + by_0 = 1,$$

поэтому $c = acx_0 + bcy_0$ и, следовательно, $d \mid c$. Теперь понятно, что множество общих делителей чисел $ac$ и $b$ совпадает с множеством общих делителей чисел $c$ и $b$. Значит,

$$\text{НОД}\,(ac, b) = \text{НОД}\,(c, b).$$

**4.** По свойству 3 имеем

$$\text{НОД}\,(ab, c) = \text{НОД}\,(b, c) = 1.$$

Впрочем, свойство 4 нетрудно доказать и непосредственно. Обозначим $d = \text{НОД}\,(ab, c)$. Тогда $d \mid ab$ и $d \mid c$, а значит, $d \mid ac$ и, таким образом,

$$d \mid \text{НОД}\,(ab, ac) = a\,\text{НОД}\,(b, c) = a.$$

Таким образом, $d$ — общий делитель $a$ и $c$. Следовательно, $d = 1$. □

**Упражнение 1.5.** Если $\text{НОД}\,(a_i, c) = 1$ для $i = 1, \ldots, m$, то

$$\text{НОД}\,(a_1 \ldots a_m, c) = 1.$$

Докажите это утверждение (обобщение свойства 4).

**Определение 1.5.** Если $\text{НОД}\,(a_i, a_j) = 1$ для всех $i \neq j$, то числа $a_1, \ldots, a_n$ называются *попарно взаимно простыми*.

**Упражнение 1.6.** Обобщите и докажите свойство 2, используя понятие попарно взаимно простых чисел.

Пусть $a_1, \ldots, a_n \in \mathbb{Z}$, причём все эти числа отличны от нуля.

**Определение 1.6.** Аналогично определению наибольшего общего делителя, наименьшее (по величине) положительное общее кратное чисел $a_1, \ldots, a_n$ называется их *наименьшим общим кратным*.

Обозначение: $\text{НОК}\,(a_1, \ldots, a_n)$.

Если $\text{НОК}\,(a_1, \ldots, a_n) = m$, то числа $m/a_1, \ldots, m/a_n$ взаимно просты, что непосредственно следует из определения.

Имеем

$$\text{НОК}\,(a_1, \ldots, a_n) = \text{НОК}\,(|a_1|, \ldots, |a_n|),$$

поэтому всюду, где это удобно, мы будем считать числа $a_1, \ldots, a_n$ натуральными.

Рассмотрим вопрос о наименьшем общем кратном двух чисел ($n = 2$, $a_1 = a$, $a_2 = b$).

**Теорема 1.7.** Справедлива формула

$$\text{НОК}\,(a, b) = \frac{ab}{\text{НОД}\,(a, b)}. \tag{1.3}$$

Доказательство. Пусть $d = \text{НОД}\,(a, b)$ и $m = ab/d$. Докажем, что $m = \text{НОК}\,(a, b)$. Пусть $M > 0$ — произвольное общее кратное чисел $a$ и $b$, т. е.

$$M = aq_1 = bq_2,$$

где $q_1$, $q_2$ — натуральные числа. Сократив на $d$, получим

$$a_1 q_1 = b_1 q_2, \quad \text{НОД}\,(a_1, b_1) = 1.$$

По свойству 1 взаимно простых чисел отсюда следует, что, например, $q_1$ делится на $b_1$, т. е. $q_1 = b_1 q_3$ для некоторого натурального $q_3$. Но тогда

$$M = a q_1 = a b_1 q_3 = m q_3.$$

В частности, $M \geqslant m$ и, таким образом, $m = \text{НОК}\,(a, b)$. □

Доказывая формулу (1.3), мы попутно обосновали следующее важное свойство наименьшего общего кратного двух чисел.

**1.** $\text{НОК}\,(a, b)$ делит любое общее кратное чисел $a$ и $b$.

Это свойство (ср. с аналогичным свойством наибольшего общего делителя) можно было бы принять за определение наименьшего общего кратного.

**Замечание 1.5.** Свойство 1 легко доказать (и заодно распространить с двух чисел на любое их количество), если разделить с остатком произвольное общее кратное $M$ чисел $a$ и $b$ на $m = \text{НОК}\,(a, b)$:

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

Остаток $r$ также является общим кратным, а потому должен быть равен нулю.

Другое, более короткое доказательство формулы (1.3) состоит в следующем. Пусть

$$m = \text{НОК}\,(a, b), \quad d = \frac{ab}{m}.$$

Тогда $d = \text{НОД}\,(a, b)$.

**Упражнение 1.7.** Объясните, почему.
*Указание.* Число $d$ делится на любой общий делитель чисел $a$ и $b$.

Следующие далее свойства наименьшего общего кратного двух чисел немедленно вытекают из аналогичных свойств наибольшего общего делителя и формулы (1.3).

**2.** $\text{НОК}\,(ac, bc) = c\,\text{НОК}\,(a, b)$ для любого $c$.

**3.** Если $c \mid a$ и $c \mid b$, то $\text{НОК}\,(a/c, b/c) = \text{НОК}\,(a, b)/c$.

**Упражнение 1.8.** Выведите свойства 2 и 3 из свойства 1.

Перейдём к вопросу о наименьшем общем кратном нескольких чисел.

**Теорема 1.8.** $\text{НОК}\,(a_1, \ldots, a_{n-1}, a_n) = \text{НОК}\,(\text{НОК}\,(a_1, \ldots, a_{n-1}), a_n)$.

Доказательство. Аналогично доказательству теоремы 1.5. □

Теорема 1.8 в комбинации с формулой (1.3) и алгоритмом Евклида предоставляет эффективный практический способ находить наименьшее общее кратное нескольких чисел.

**Упражнение 1.9.** Распространите свойства 2 и 3 наименьшего общего кратного с двух чисел на произвольное их количество.

**Упражнение 1.10.** Докажите, что наименьшее общее кратное попарно взаимно простых чисел равно их произведению.

*Указание.* Воспользуйтесь теоремой 1.8.

**Упражнение 1.11.** Пусть $d = \text{НОД}\,(a_1, \ldots, a_n)$, $m = \text{НОК}\,(a_1, \ldots, a_n)$. Докажите равенство $\text{НОК}\,(m/a_1, \ldots, m/a_n) = m/d$.

*Решение.* Достаточно рассмотреть случай $d = 1$ (объясните, почему). Пусть $M$ — произвольное общее кратное чисел $m/a_1, \ldots, m/a_n$, т. е.

$$M = \frac{q_1 m}{a_1} = \ldots = \frac{q_n m}{a_n}$$

для некоторых целых чисел $q_1, \ldots, q_n$. Пусть $s/t$ — несократимая дробь, которой равны все дроби $q_i/a_i$. Тогда все $a_i$ должны делиться на $t$. Поскольку $d = 1$, должно быть $t = 1$. Значит, $q_i = a_i s$ и $M = ms$ делится на $m$. □

Рассмотрим задачу, известную ещё в Древнем Китае: *найти число $r$, если даны остатки $r_1, \ldots, r_k$ от его деления на заданные числа $m_1, \ldots, m_k$ соответственно*. Например: найти число $r$, дающее при делении на 3 остаток 2, при делении на 5 — остаток 3, а при делении на 7 — снова остаток 2 (Сунь Цзы, между II и VI в.).

Пусть

$$R_m = \{0, 1, 2, \ldots, m-1\}$$

— множество возможных остатков от деления на $m$. Следующая теорема известна как *китайская теорема об остатках* (для случая $k = 2$).

**Теорема 1.9.** Пусть $\text{НОД}\,(m_1, m_2) = 1$ и $m = m_1 m_2$. Тогда для любых остатков $r_1 \in R_{m_1}$, $r_2 \in R_{m_2}$ существует, и притом единственное, число $r \in R_m$, дающее при делении на $m_1$ и $m_2$ остатки $r_1$ и $r_2$ соответственно.

ДОКАЗАТЕЛЬСТВО. Рассмотрим отображение $R_m \to R_{m_1} \times R_{m_2}$, заданное правилом:

$$r \mapsto (r_1, r_2), \quad r_i \text{ — остаток от деления } r \text{ на } m_i.$$

Из условия $\text{НОД}\,(m_1, m_2) = 1$ следует, что это отображение *инъективно*. Поскольку

$$|R_m| = |R_{m_1} \times R_{m_2}|,$$

оно является и *сюръективным*. Следовательно, отображение *биективно*, что и требовалось доказать. □

**Упражнение 1.12.** Проведите подробное рассуждение.

*Указание.* При обосновании инъективности отображения используйте свойство 2 взаимно простых чисел.

**Упражнение 1.13.** Сформулируйте и докажите китайскую теорему об остатках в общем случае (для произвольного $k$).

*Указание.* Нужно потребовать, чтобы числа $m_1, \ldots, m_k$ были *попарно взаимно просты*, иначе утверждение окажется неверным.

**Замечание 1.6.** Далее (см. конец раздела 3.4) будет предложено конструктивное доказательство китайской теоремы об остатках, пригодное для практического отыскания числа $r$.

## 1.3 Простые и составные числа

Простые и составные числа. Метод Евклида доказательства бесконечности множества простых чисел. Алгоритм выписывания начального отрезка ряда простых чисел (решето Эратосфена). Характеристическое свойство простых чисел.

**Определение 1.7.** Натуральное число, большее единицы, называется *простым*, если все его натуральные делители суть единица и оно само. В противном случае это число называется *составным*.

Очевидно, любое составное число можно представить в виде произведения меньших его натуральных чисел, а простые числа этим свойством не обладают.

**Пример 1.5.** Выпишем несколько первых простых чисел: 2, 3, 5, 7, 11. Число 12 является составным, так как, например, $12 = 3 \cdot 4$.

Конечен или бесконечен ряд простых чисел? Ответ на этот вопрос был дан ещё Евклидом (см. «Начала», книга IX).

**Лемма 1.4.** Пусть $N$ — натуральное число, большее единицы. Наименьший натуральный делитель $p > 1$ числа $N$ является простым числом.

Доказательство. Действительно, иначе число $p$ имело бы натуральный делитель $p_1$, $1 < p_1 < p$, который был бы и делителем $N$, что противоречило бы определению $p$. □

Следующее утверждение известно как *теорема Евклида*.

**Теорема 1.10.** Простых чисел бесконечно много.

Доказательство. Пусть $p_1, p_2, \ldots, p_n$ — все простые числа. Рассмотрим число

$$N = p_1 p_2 \ldots p_n + 1$$

и его наименьший простой делитель $p$ (лемма 1.4). С одной стороны, $p$ — одно из простых чисел $p_i$, а с другой — ни на одно из этих чисел $N$ не делится. Противоречие. □

**Упражнение 1.14.** Используя метод Евклида, докажите, что простых чисел вида $4k - 1$ бесконечно много.

*Указание.* Пусть $p_1, p_2, \ldots, p_n$ — все простые числа такого вида. Рассмотрите число

$$N = 4p_1 p_2 \ldots p_n - 1.$$

Таким образом, ряд простых чисел неограничен, простые числа могут быть сколь угодно большими. Конкретные примеры *больших простых чисел* можно отыскать, например, на сайте `www.mersenne.org`. Приведём последний рекорд (январь 2016 года):

$$2^{74207281} - 1.$$

Десятичная запись этого числа содержит более 22 миллионов цифр.

Как выписать все простые числа, которые не превышают данного натурального числа $N$? Древнегреческий учёный Эратосфен (276 — 194 до н. э.) нашёл способ составления таблиц простых чисел, позднее названный *решетом Эратосфена*. Для обоснования этого алгоритма нам понадобится следующая

**Лемма 1.5.** Пусть $N$ — составное число. Наименьший простой делитель $p$ числа $N$ не превосходит $\sqrt{N}$.

Доказательство. Имеем $N = pN_1$, при этом $N_1 > 1$. Из определения $p$ следует неравенство $N_1 \geqslant p$. Значит, $N \geqslant p^2$, откуда $p \leqslant \sqrt{N}$. □

**Следствие 1.1.** Число $N > 1$ является простым, если оно не делится на все простые числа $p$, не превосходящие $\sqrt{N}$.

**Пример 1.6.** Число 199 является простым, так как оно не делится на 2, 3, 5, 7, 11 и 13 — последнее простое число, не превосходящее $\sqrt{199}$.

Опишем теперь сам алгоритм.

**А.** Выписать в ряд все натуральные числа от 2 до $N$.

**Б.** Обвести первое невычеркнутое в ряду число и затем вычеркнуть далее в ряду все числа, ему кратные. Делать так до тех пор, пока очередное обведённое число не окажется больше $\sqrt{N}$, после чего процесс вычеркиваний прекратить и обвести все невычеркнутые к этому моменту числа.

**В.** Обведённые числа — все простые числа, не превосходящие $N$.

Действительно, любое из обведённых чисел должно быть простым (это неочевидно только для тех из них, которые обводятся в последнюю очередь, но здесь работает лемма 1.5), а любое вычеркнутое число — очевидно, составное.

**Пример 1.7.** Найдём все простые числа, не превосходящие 60.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | [2] | [3] | 4 | [5] | 6 | [7] | 8 | 9 | 10 |
| [**11**] | 12 | [13] | 14 | 15 | 16 | [17] | 18 | [19] | 20 |
| 21 | 22 | [23] | 24 | 25 | 26 | 27 | 28 | [29] | 30 |
| [31] | 32 | 33 | 34 | 35 | 36 | [37] | 38 | 39 | 40 |
| [41] | 42 | [43] | 44 | 45 | 46 | [47] | 48 | 49 | 50 |
| 51 | 52 | [53] | 54 | 55 | 56 | 57 | 58 | [59] | 60 |

Процесс вычеркиваний следует прекратить, как только будет обведено число $11 > \sqrt{60}$.

Из определения простого числа непосредственно следует утверждение: *любое целое число либо взаимно просто с данным простым числом, либо делится на него.*

**Упражнение 1.15.** Докажите это.

Одно из возможных доказательств основной теоремы арифметики (см. далее раздел 1.4) опирается на следующее *характеристическое свойство* простых чисел.

**Лемма 1.6.** Если произведение нескольких целых чисел делится на простое число $p$, то хотя бы одно из этих чисел делится на $p$.

Доказательство. Если ни одно из этих чисел не делится на $p$, то каждое из них взаимно просто с $p$. Но тогда их произведение будет взаимно простым с $p$ (см. упражнение 1.5), а оно по условию делится на $p$. Противоречие. □

## 1.4 Основная теорема арифметики и её следствия

Основная теорема арифметики и её различные доказательства. Пример Гильберта. Каноническое разложение натурального числа. Правило вычисления НОД и НОК нескольких чисел, использующее канонические разложения.

Следующая теорема вполне заслуживает названия *основной теоремы арифметики*, ибо вскрывает структуру натуральных чисел — аддитивных образований — по отношению к «чуждой» им операции умножения.

**Теорема 1.11.** Всякое натуральное число, отличное от единицы, разлагается в произведение простых чисел. Разложение единственно с точностью до перестановки сомножителей.

Иными словами, все натуральные числа могут быть получены из простых чисел с помощью всевозможных умножений, причём в результате различных умножений получаются различные числа.

Доказательство. Рассмотрим самое длинное разложение данного числа $m > 1$ в произведение натуральных чисел, больших единицы: оно обязано состоять только из простых сомножителей. Поэтому указанное разложение существует.

Докажем единственность разложения в произведение простых чисел. Пусть

$$m = p_1 p_2 \dots p_n = q_1 q_2 \dots q_k$$

— два таких разложения. По лемме 1.6 одно из простых чисел $q_i$ (скажем, $q_1$) должно делиться на $p_1$. Но в таком случае $q_1 = p_1$, и после сокращения на общий множитель получим

$$m' = p_2 \dots p_n = q_2 \dots q_k,$$

где $m' < m$. Далее можно рассуждать по индукции. □

Отметим, что, в то время как возможность разложения непосредственно вытекает из определения простого числа, доказательство единственности разложения получается далеко не сразу. Следующий пример, принадлежащий Д. Гильберту (1862 — 1943), позволяет понять, почему эти два утверждения так отличаются друг от друга.

**Пример 1.8.** Понятие простого числа связано только с операцией умножения и не зависит от операции сложения. Рассмотрим *мультипликативно замкнутую* систему натуральных чисел вида $4k + 1$:

$$S = \{1, 5, 9, 13, 17, \dots\}.$$

Назовём *квазипростым* такое число из $S$, которое отлично от единицы и не разлагается нетривиальным образом в произведение чисел из $S$. Вот несколько первых квазипростых чисел: 5, 9, 13, 17, 21 (их ряд также бесконечен).

Ясно, что каждое число из $S$ можно разложить в произведение квазипростых чисел, однако такое разложение уже не будет, вообще говоря, однозначным. Например:

$$441 = 21^2 = 9 \cdot 49,$$

при этом числа 9, 21 и 49 — квазипростые.

Пример Гильберта также интересен тем, что даёт представление о логической структуре любого доказательства основной теоремы арифметики: такое доказательство не может опираться только на определение простого числа и свойства мультипликативных операций, оно где-то должно использовать операцию сложения или вычитания.

Вот одно из «прямых» доказательств (без скрытых излишеств типа алгоритма Евклида и его следствий), в котором аддитивная операция используется минимально возможное число раз, т. е. ровно один раз.

Заметим прежде всего, что если разложение некоторого числа на простые сомножители единственно, то каждый простой делитель этого числа должен входить в разложение. Будем доказывать единственность разложения по индукции, а именно, докажем единственность разложения числа $m$ в предположении, что для всех чисел, меньших $m$, она уже установлена. Пусть $m$ — составное число (для простого доказывать нечего), имеющее два различных разложения в произведение простых чисел:

$$m = pqr\ldots = p_1q_1r_1\ldots$$

Одно и то же простое число не может встретиться в обоих разложениях (иначе на него можно было бы сократить и прийти к противоречию с предположением индукции). Можно считать, что $p$ — наименьшее из простых чисел, встречающихся в первом разложении. Тогда $m \geqslant p^2$. Аналогично, $m \geqslant p_1^2$. Поскольку $p$ и $p_1$ не совпадают, отсюда следует неравенство $pp_1 < m$. Рассмотрим теперь число

$$m' = m - pp_1 < m.$$

Разложение этого числа в произведение простых (единственное согласно предположению индукции) должно иметь вид

$$m' = pp_1QR\ldots$$

Следовательно, число $pp_1$ делит $m = pqr\ldots$ и после сокращения на $p$ оказывается, что $p_1$ делит число $qr\ldots < m$. Однако это невозможно, ибо число $qr\ldots$ имеет по предположению индукции единственное разложение, а $p_1$ не является одним из простых множителей $q$, $r$, ... — противоречие.

**Определение 1.8.** Представление вида

$$m = p_1^{\alpha_1}\ldots p_t^{\alpha_t}, \tag{1.4}$$

где $p_i$ — различные простые числа, $\alpha_i$ — натуральные числа ($i = 1, \ldots, t$), называется *каноническим разложением* числа $m$.

**Пример 1.9.** $588000 = 2^5 \cdot 3^1 \cdot 5^3 \cdot 7^2$.

Если известно каноническое разложение (1.4) числа $m$, то можно легко перечислить все его натуральные делители. Они имеют вид

$$d = p_1^{\beta_1}\ldots p_t^{\beta_t},$$

где набор показателей $(\beta_1, \ldots, \beta_t)$ удовлетворяет ограничениям

$$0 \leqslant \beta_i \leqslant \alpha_i, \quad i = 1, \ldots, t.$$

Это утверждение вытекает из основной теоремы арифметики.

Другими следствиями являются известные правила составления НОД и НОК нескольких чисел, канонические разложения которых предполагаются известными.

1. НОД нескольких чисел равен произведению всех степеней вида $p^\alpha$, где $p$ — общий простой делитель всех данных чисел, а $\alpha$ — наименьший из показателей, с которыми $p$ входит в их канонические разложения.

2. НОК нескольких чисел равно произведению всех степеней вида $p^\alpha$, где $p$ — простой делитель хотя бы одного из данных чисел, а $\alpha$ — наибольший из показателей, с которыми $p$ входит в их канонические разложения.

**Пример 1.10.** Пусть $a = 2^2 \cdot 5^3 \cdot 7^4$ и $b = 2^5 \cdot 3^1 \cdot 7^3 \cdot 13^3$. Тогда

$$\text{НОД}\,(a, b) = 2^2 \cdot 7^3, \quad \text{НОК}\,(a, b) = 2^5 \cdot 3^1 \cdot 5^3 \cdot 7^4 \cdot 13^3.$$

Из основной теоремы арифметики можно вывести (и ещё раз осознать, взглянув с другой точки зрения) все основные факты теории делимости, установленные нами ранее из других соображений. Некоторые утверждения при этом станут очевидными. Так будет, например, со свойством 1 взаимно простых чисел (см. раздел 1.2). Действительно, если $a$ делит $bc$ и взаимно просто с $b$, то каноническое разложение $a$ входит в каноническое разложение $bc$, но не пересекается с каноническим разложением $b$ и потому должно содержаться в каноническом разложении $c$.

В терминах канонического разложения числа $m$ могут быть найдены значения многих специальных теоретико-числовых функций натурального аргумента $m$ (см. раздел 1.5). Вопрос о практическом отыскании канонического разложения данного числа мы затронем в разделе 5. Но уже сейчас сообщим, что это — сложная вычислительная задача.

## 1.5 Мультипликативные функции

Понятие мультипликативной функции. Примеры теоретико-числовых функций (число делителей, сумма делителей, функция Эйлера, функция Мёбиуса), их мультипликативность и формулы для вычисления значений. Формула обращения Мёбиуса.

**Определение 1.9.** Числовая функция $\xi(m)$ натурального аргумента $m$ называется *мультипликативной*, если

$$\xi(m_1 m_2) = \xi(m_1)\xi(m_2)$$

для любых взаимно простых натуральных чисел $m_1$, $m_2$.

**Пример 1.11.** Функция

$$\xi(m) = m^s$$

является мультипликативной при любом вещественном (и даже комплексном) значении $s$.

Перечислим простейшие свойства мультипликативных функций.

1. $\xi(1) = 1$.
2. Для любых попарно взаимно простых чисел $m_1, \ldots, m_k$ имеем

   $$\xi(m_1 \ldots m_k) = \xi(m_1) \ldots \xi(m_k).$$

   В частности, если $m = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$ — каноническое разложение числа $m$, то

   $$\xi(m) = \xi(p_1^{\alpha_1}) \ldots \xi(p_t^{\alpha_t}). \tag{1.5}$$

3. Мультипликативная функция $\xi(m)$ может быть задана следующим способом: произвольно задаём значения вида $\xi(p^\alpha)$, где $p$ — простое, $\alpha$ — натуральное, остальные значения определяем формулой (1.5).
4. Если $\xi_1(m)$ и $\xi_2(m)$ — мультипликативные функции, то их произведение

   $$\xi(m) = \xi_1(m)\xi_2(m)$$

   также будет мультипликативной функцией.

Доказательство этих свойств непосредственно вытекает из определения 1.9 и предоставляется читателю как

**Упражнение 1.16.**

В следующей теореме указан один общий способ конструирования мультипликативных функций.

**Теорема 1.12.** Пусть $\xi(m)$ — мультипликативная функция. Положим

$$\eta(m) = \sum_{d \mid m} \xi(d)$$

Тогда $\eta(m)$ — также мультипликативная функция.

Здесь и далее символ

$$\sum_{d\,|\,m}$$

означает суммирование по всем натуральным делителям $d$ числа $m$.

ДОКАЗАТЕЛЬСТВО. Пусть $m = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ — каноническое разложение числа $m$. Натуральные делители этого числа имеют вид

$$d = p_1^{\beta_1} \dots p_t^{\beta_t},$$

где $0 \leqslant \beta_i \leqslant \alpha_i$ $(i = 1, \dots, t)$. Следовательно,

$$\eta(m) = \sum_{d\,|\,m} \xi(d) =$$

$$= \sum_{\beta_1=0}^{\alpha_1} \cdots \sum_{\beta_t=0}^{\alpha_t} \xi(p_1^{\beta_1} \dots p_t^{\beta_t}) = \sum_{\beta_1=0}^{\alpha_1} \cdots \sum_{\beta_t=0}^{\alpha_t} \xi(p_1^{\beta_1}) \dots \xi(p_t^{\beta_t}) =$$

$$= \sum_{\beta_1=0}^{\alpha_1} \xi(p_1^{\beta_1}) \dots \sum_{\beta_t=0}^{\alpha_t} \xi(p_t^{\beta_t}) = \prod_{i=1}^{t} \sum_{\beta_i=0}^{\alpha_i} \xi(p_i^{\beta_i}).$$

Теперь мультипликативность функции $\eta(m)$ очевидна. □

Таким образом, если $m = p_1^{\alpha_1} \dots p_t^{\alpha_t}$, то для любой мультипликативной функции $\xi(m)$ имеет место равенство

$$\sum_{d\,|\,m} \xi(d) = \prod_{i=1}^{t} \sum_{\beta_i=0}^{\alpha_i} \xi(p_i^{\beta_i}). \tag{1.6}$$

Перейдём к рассмотрению наиболее важных примеров мультипликативных функций.

**Определение 1.10.** Функция

$$\tau(m) = \sum_{d\,|\,m} 1 \tag{1.7}$$

есть *число делителей* натурального числа $m$.

**Определение 1.11.** Функция

$$\sigma(m) = \sum_{d\,|\,m} d \tag{1.8}$$

есть *сумма делителей* натурального числа $m$.

Приведём формулы для вычисления значений этих функций:

$$\tau(m) = \prod_{i=1}^{t} (\alpha_i + 1), \quad \sigma(m) = \prod_{i=1}^{t} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1},$$

где $m = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ (это — частные случаи формулы (1.6); они получаются, если взять функции $\xi(m) = 1$ и $\xi(m) = m$ соответственно).

**Пример 1.12.** $\tau(2^3 \cdot 3^2 \cdot 5^4) = 60$, $\sigma(2^3 \cdot 3^2 \cdot 5^4) = 152295$.

**Определение 1.12.** *Функция Эйлера* $\varphi(m)$ определяется как количество чисел в ряду $0$, $1, 2, \ldots, m-1$, взаимно простых с $m$.

**Пример 1.13.** $\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$.

**Теорема 1.13.** Функция Эйлера является мультипликативной.

Доказательство. Пусть $\text{НОД}\,(m_1, m_2) = 1$ и $m = m_1 m_2$. Нетрудно видеть, что биективное соответствие между $R_m$ и $R_{m_1} \times R_{m_2}$ (см. доказательство теоремы 1.9 — китайской теоремы об остатках) обладает свойством: $\text{НОД}\,(r, m) = 1$ тогда и только тогда, когда

$$\text{НОД}\,(r_1, m_1) = \text{НОД}\,(r_2, m_2) = 1.$$

Отсюда, в частности, следует равенство

$$\varphi(m) = \varphi(m_1)\varphi(m_2),$$

которое и нужно было установить. □

Если $p$ — простое, $\alpha$ — натуральное, то по определению легко найти

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

**Упражнение 1.17.** Докажите это.

*Указание.* Подсчитайте количество чисел в ряду $1, 2, \ldots, p^\alpha$, не взаимно простых с $p^\alpha$ (т. е. с самим $p$, а значит, кратных $p$).

Пользуясь мультипликативностью, получим следующую формулу для вычисления значений функции Эйлера:

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

где $m = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$.

**Замечание 1.7.** В раскрытом виде произведение

$$\prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right) = 1 - \sum_{1 \leqslant i \leqslant t} \frac{1}{p_i} + \sum_{1 \leqslant i < j \leqslant t} \frac{1}{p_i p_j} - \ldots$$

подсказывает ещё один способ доказательства — при помощи известного из комбинаторики *правила включений и исключений*.

**Пример 1.14.** $\varphi(45000) = \varphi(2^3 \cdot 3^2 \cdot 5^4) = 12000$.

Для функции Эйлера формула (1.6), как легко видеть, примет вид

$$\sum_{d \,|\, m} \varphi(d) = m. \tag{1.9}$$

**Упражнение 1.18.** Докажите это тождество непосредственно, не обращаясь к свойству мультипликативности функции Эйлера.

*Решение*. Фиксируем произвольный делитель $d$ числа $m$ и рассмотрим все числа $x$ в ряду $0, 1, \ldots, m-1$, для которых НОД $(x, m) = d$. Их число равно $\varphi(m/d)$. Действительно, каждое из них имеет вид $x = dx_1$, где НОД $(x_1, m/d) = 1$ и $0 \leqslant x_1 < m/d$. Следовательно,

$$m = \sum_{d\,|\,m} \varphi\left(\frac{m}{d}\right) = \sum_{d\,|\,m} \varphi(d),$$

и тождество доказано. □

**Пример 1.15.** При $m = 12$ имеем

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12.$$

**Определение 1.13.** *Функция Мёбиуса* $\mu(m)$ определяется как мультипликативная функция, заданная равенствами:

$$\mu(p^\alpha) = \begin{cases} -1, & \text{если } \alpha = 1, \\ 0, & \text{если } \alpha > 1 \end{cases}$$

(здесь $p$ — простое число, $\alpha$ — натуральное число).

Иными словами, $\mu(m) = (-1)^t$, если $m$ есть произведение $t$ различных простых чисел, и $\mu(m) = 0$ во всех остальных случаях — т. е. когда $m$ не свободно от квадратов (делится на квадрат некоторого простого).

В случае функции Мёбиуса формула (1.6) принимает вид

$$\sum_{d\,|\,m} \mu(d) = \begin{cases} 1, & \text{если } m = 1, \\ 0, & \text{если } m > 1. \end{cases} \tag{1.10}$$

Следующая теорема была доказана немецким математиком и астрономом А. Ф. Мёбиусом (1790 — 1868).

**Теорема 1.14.** Пусть $f(m)$ и $F(m)$ — две числовые функции. Если

$$F(m) = \sum_{d\,|\,m} f(d), \quad m = 1, 2, \ldots, \tag{1.11}$$

то

$$f(m) = \sum_{d\,|\,m} \mu(d) F\left(\frac{m}{d}\right), \quad m = 1, 2, \ldots \tag{1.12}$$

Доказательство. Это можно проверить непосредственной подстановкой:

$$\sum_{d\,|\,m} \mu(d) F\left(\frac{m}{d}\right) = \sum_{d\,|\,m} \mu(d) \sum_{\delta\,|\,m/d} f(\delta) = \sum_{\delta\,|\,m} f(\delta) \sum_{d\,|\,m/\delta} \mu(d) = f(m).$$

На последнем этапе преобразований мы воспользовались соотношением (1.10) для функции Мёбиуса, *которое, таким образом, её характеризует*. □

**Упражнение 1.19.** Разъясните смысл фразы, выделенной курсивом.

*Решение.* Эта фраза означает: если некоторая числовая функция $f(m)$ удовлетворяет соотношению

$$\sum_{d\,|\,m} f(d) = \begin{cases} 1, & \text{если } m = 1, \\ 0, & \text{если } m > 1, \end{cases}$$

то эта функция есть функция Мёбиуса. В самом деле, равенство

$$f(m) = \mu(m), \quad m = 1,\, 2,\, \ldots,$$

является непосредственным следствие формулы (1.12). □

Формула (1.12) называется *обращением формулы* (1.11) *суммированием по делителям*.

**Пример 1.16.** Если обратить формулы (1.7), (1.8) и (1.9), то получим соответственно

$$\sum_{d\,|\,m} \mu(d)\tau\left(\frac{m}{d}\right) = 1, \quad \sum_{d\,|\,m} \mu(d)\sigma\left(\frac{m}{d}\right) = m,$$

$$\varphi(m) = m\sum_{d\,|\,m} \frac{\mu(d)}{d}.$$

После применения к последней сумме формулы (1.6) возникнет уже знакомая нам формула

$$\varphi(m) = m\prod_{i=1}^{t}\left(1 - \frac{1}{p_i}\right).$$

Тем самым она получит новое доказательство и, как следствие, ещё одним способом будет установлена мультипликативность функции Эйлера.

## 1.6 Целая и дробная часть числа

Функции целой $[x]$ и дробной $\{x\}$ части вещественного числа, их свойства. Формула Лежандра. Каноническое разложение $n$-факториала.

Помимо функций, рассмотренных в разделе 1.5, в теории чисел исключительно важную роль играют функции целой и дробной части вещественного числа.

**Определение 1.14.** *Целой частью* числа $x$ называется наибольшее целое число, не превосходящее $x$. *Дробная часть* числа $x$ — это разность между $x$ и целой частью $x$.

Обозначение: $[x]$ и $\{x\}$ — целая и дробная часть соответственно.

**Пример 1.17.** Имеем

$$[\pi] = 3, \quad \left[-\frac{22}{7}\right] = -4, \quad \left\{\frac{1+\sqrt{5}}{2}\right\} = \frac{2}{1+\sqrt{5}},$$

$$\left\{e^{\pi\sqrt{163}}\right\} = 0.9999999999992\ldots, \quad \left\{\frac{\ln 640320}{\sqrt{163}} - \frac{\pi}{3}\right\} = 0.99999999999999992\ldots$$

Последние два равенства нашёл индийский математик С. Рамануджану (1887 — 1920).

Непосредственно из определения следуют неравенства

$$[x] \leqslant x < [x] + 1, \quad 0 \leqslant \{x\} = x - [x] < 1,$$

которые также записывают в виде

$$x - 1 < [x] \leqslant x.$$

Если поделить целое число $a$ на натуральное число $m$ с остатком, то, как легко обнаружить, неполное частное будет равно $[a/m]$. Этому наблюдению можно придать следующий смысл.

**Лемма 1.7.** Пусть $m$ — натуральное число. Число положительных целых чисел, делящихся на $m$ и не превосходящих данного $x > 0$, равно $[x/m]$.

Доказательство. Речь идёт о числах $m$, $2m$, …, $qm$, при этом $q$ удовлетворяет неравенствам

$$qm \leqslant x < (q+1)m.$$

Разделив на $m$, получим $q \leqslant x/m < q + 1$, откуда $q = [x/m]$. □

**Упражнение 1.20.** При тех же $m$ и $x$ докажите, что $[x/m] = [[x]/m]$.

*Указание.* Между $[x]$ и $x$ целых чисел нет.

Некоторые другие полезные свойства функции $[x]$ представлены следующей леммой.

**Лемма 1.8.** Справедливы соотношения:

$$[x] + [y] \leqslant [x + y] \leqslant [x] + [y] + 1,$$

$$[mx] = \sum_{k=0}^{m-1} \left[x + \frac{k}{m}\right].$$

Здесь $x$, $y$ — вещественные числа, $m$ — натуральное число.

Доказательство. Указанные неравенства сводятся к паре очевидных неравенств $0 \leqslant [\{x\} + \{y\}] \leqslant 1$.

Доказательство тождества менее очевидно. Пусть

$$\frac{l}{m} \leqslant \{x\} < \frac{l+1}{m}$$

для некоторого $l = 0, 1, \ldots, m-1$. Тогда

$$[mx] = m[x] + [m\{x\}] = m[x] + l,$$

$$\left[x + \frac{k}{m}\right] = [x] + \left[\{x\} + \frac{k}{m}\right] = \begin{cases} [x], & 0 \leqslant k < m - l, \\ [x] + 1, & m - l \leqslant k < m. \end{cases}$$

Следовательно,

$$\sum_{k=0}^{m-1} \left[x + \frac{k}{m}\right] = m[x] + (m - (m - l)) = m[x] + l = [mx],$$

и тождество установлено. □

**Замечание 1.8.** Имеем $[mx] - m[x] = l$, откуда при $m = 2$ получим такое следствие:

$$[2x] - 2[x] \in \{0, 1\}$$

для любого числа $x$.

Для натурального числа $m$ и простого числа $p$ пусть $\nu_p(m)$ — показатель, с которым $p$ входит в каноническое разложение числа $m$ (если $p$ не является делителем $m$, то $\nu_p(m) = 0$). Каноническое разложение числа $m$ можно записать в виде

$$m = \prod_p p^{\nu_p(m)},$$

где (формально бесконечное, но фактически конечное) произведение распространено на все простые числа $p$.

**Теорема 1.15.** Пусть $p$ — простое число. Для любого натурального числа $n$ справедлива формула

$$\nu_p(n!) = \sum_{\alpha \geqslant 1} \left[\frac{n}{p^\alpha}\right]. \tag{1.13}$$

**Замечание 1.9.** Эта формула называется *формулой Лежандра*. Присутствующий в ней формально бесконечный ряд содержит лишь конечное число ненулевых слагаемых, поскольку $n < p^\alpha$ при всех достаточно больших $\alpha$, для которых, следовательно, $[n/p^\alpha] = 0$.

Доказательство. Можно рассуждать по индукции. Предположим, что для всех натуральных чисел, меньших данного $n > 1$, формула доказана. Докажем её для числа $n$.

При $p > n$ равенство (1.13) очевидно, поэтому считаем $p \leqslant n$. Рассмотрим в произведении $n!$ все множители, кратные $p$. По лемме 1.7 их количество есть $n_1 = [n/p]$, а сами они суть $p$, $2p$, …, $n_1 p$. Имеем

$$n! = (p \cdot 2p \cdot \ldots \cdot n_1 p)N = p^{n_1} n_1! N,$$

где $N$ — произведение всех остальных (не кратных $p$) множителей, так что НОД $(N, p) = 1$. Поскольку $n_1 < n$, по предположению индукции

$$\nu_p(n_1!) = \sum_{\alpha \geqslant 1} \left[\frac{n_1}{p^\alpha}\right] = \sum_{\alpha \geqslant 1} \left[\frac{[n/p]}{p^\alpha}\right] = \sum_{\alpha \geqslant 1} \left[\frac{n}{p^{\alpha+1}}\right]$$

(см. также упражнение 1.20). Значит,

$$\nu_p(n!) = n_1 + \nu_p(n_1!) = \left[\frac{n}{p}\right] + \sum_{\alpha \geqslant 1} \left[\frac{n}{p^{\alpha+1}}\right] = \sum_{\alpha \geqslant 1} \left[\frac{n}{p^\alpha}\right].$$

Шаг индукции сделан. □

**Упражнение 1.21.** Докажите формулу (1.13) прямым подсчётом показателя $\nu_p(n!)$.

*Решение.* Количество чисел в ряду 1, 2, …, $n$, делящихся в точности на $p^\alpha$ (т. е. кратных $p^\alpha$ и не кратных $p^{\alpha+1}$), по лемме 1.7 равно

$$\left[\frac{n}{p^\alpha}\right] - \left[\frac{n}{p^{\alpha+1}}\right].$$

Следовательно,

$$\nu_p(n!) = \sum_{\alpha \geqslant 1} \alpha \left( \left[\frac{n}{p^\alpha}\right] - \left[\frac{n}{p^{\alpha+1}}\right] \right) = \sum_{\alpha \geqslant 1} \left[\frac{n}{p^\alpha}\right].$$

См. также рассуждение на стр. 25 в книге [3]. □

**Упражнение 1.22.** Проверьте, что

$$\sum_{\alpha \geqslant 1} \left[\frac{n}{p^\alpha}\right] = \frac{n - s_p(n)}{p-1},$$

где $s_p(n) = a_\beta + \ldots + a_1 + a_0$ — сумма цифр числа

$$n = a_\beta p^\beta + \ldots + a_1 p + a_0$$

в *$p$-ичной системе счисления* (равенство верно не только для простых, но и для составных чисел $p$). Как следствие, имеет место оценка

$$\nu_p(n!) \leqslant \left[\frac{n-1}{p-1}\right].$$

Приведём примеры применения формулы Лежандра.

**Пример 1.18.** Как определить, каким количеством нулей оканчивается число

$$50! = 30414093201713378043612608166064768844377641568960512000000000000,$$

не вычисляя самого числа?

Ясно, что это количество нулей равно

$$\min\{\nu_2(50!), \nu_5(50!)\} = \nu_5(50!) = \left[\frac{50}{5}\right] + \left[\frac{50}{25}\right] = 10 + 2 = 12.$$

**Пример 1.19.** Не опираясь на комбинаторные соображения, покажем, что *биномиальный коэффициент*

$$C_n^k = \frac{n!}{k!(n-k)!}$$

является целым числом, т. е. $n!$ делится на $k!(n-k)!$.

Можно воспользоваться следующим критерием делимости: *число $A$ делится на число $B$ тогда и только тогда, когда*

$$\nu_p(A) \geqslant \nu_p(B)$$

*для любого простого числа $p$.* В нашем случае нужно проверить неравенство

$$\nu_p(n!) \geqslant \nu_p(k!(n-k)!) = \nu_p(k!) + \nu_p((n-k)!).$$

Действительно, имеем

$$\nu_p(k!) + \nu_p((n-k)!) = \sum_{\alpha \geqslant 1} \left[\frac{k}{p^\alpha}\right] + \sum_{\alpha \geqslant 1} \left[\frac{n-k}{p^\alpha}\right] =$$

$$= \sum_{\alpha \geqslant 1} \left( \left[\frac{k}{p^\alpha}\right] + \left[\frac{n-k}{p^\alpha}\right] \right) \leqslant \sum_{\alpha \geqslant 1} \left[\frac{n}{p^\alpha}\right] = \nu_p(n!)$$

(мы применили неравенство $[x] + [y] \leqslant [x+y]$, см. лемму 1.8).

Каноническое разложение $n!$ можно записать следующим образом:

$$n! = \prod_{p \leqslant n} p^{\nu_p(n!)},$$

где $\nu_p(n!)$ вычисляется по формуле (1.13). Вот ещё одна аналогичная формула:

$$\text{НОК}\,(1, 2, \ldots, n) = \prod_{p \leqslant n} p^{\nu_p(\text{НОК}\,(1,2,\ldots,n))},$$

где

$$\nu_p(\text{НОК}\,(1, 2, \ldots, n)) = \left[\frac{\ln n}{\ln p}\right].$$

**Упражнение 1.23.** Докажите последнее равенство.

*Указание.* Вспомните про правило составления наименьшего общего кратного нескольких чисел (см. раздел 1.4).

Перейдя к логарифмам, получим равенства

$$\ln n! = \sum_{p \leqslant n} \sum_{\alpha \geqslant 1} \nu_p(n!) \ln p = \sum_{p \leqslant n} \sum_{\alpha \geqslant 1} \left[\frac{n}{p^\alpha}\right] \ln p, \tag{1.14}$$

$$\ln \text{НОК}\,(1, 2, \ldots, n) = \sum_{p \leqslant n} \left[\frac{\ln n}{\ln p}\right] \ln p. \tag{1.15}$$

Этими формулами мы воспользуемся в следующем параграфе.

В заключение укажем ещё одно важное приложение функции $[x]$.

**Упражнение 1.24.** На отрезке $[a, b]$ задана положительная функция $y = f(x)$. Докажите, что число *целых точек* (точек с целочисленными координатами), лежащих в криволинейной трапеции

$$\{(x, y) \in \mathbb{R}^2 : a \leqslant x \leqslant b,\ 0 < y \leqslant f(x)\},$$

выражается формулой

$$\sum_{a \leqslant k \leqslant b} [f(k)].$$

*Указание.* $[f(k)]$ равно количеству целых чисел $y$, для которых $0 < y \leqslant f(k)$.

Так, например, число целых точек в области, ограниченной гиперболой $xy = N$ и координатными полуосями, равно

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

Для этой суммы П. Г. Лежен-Дирихле (1805 — 1859) получил в 1849 году следующую формулу:

$$S(N) = N \ln N + (2\gamma - 1)N + R, \tag{1.16}$$

где $\gamma \approx 0.5772156649$ — *постоянная Эйлера*, при этом остаточный член $R = O(\sqrt{N})$. Одной из до сих пор нерешённых проблем теории чисел является задача о точной оценке $R$. В связи с тем, что

$$S(N) = \tau(1) + \tau(2) + \ldots + \tau(N),$$

её называют также *проблемой делителей*. (Подробнее об этом см., например, в книге [1, гл. 4].)

**Упражнение 1.25.** Докажите, что

$$\sum_{k=1}^{(q-1)/2} \left[\frac{pk}{q}\right] + \sum_{l=1}^{(p-1)/2} \left[\frac{ql}{p}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2},$$

где $p$ и $q$ — нечётные взаимно простые натуральные числа.

# 2 Распределение простых чисел

## 2.1 Оценки Чебышёва

Распределение простых чисел в натуральном ряду. Функции Чебышёва $\theta(x)$ и $\psi(x)$. Центральный биномиальный коэффициент. Оценки Чебышёва для функции $\pi(x)$. Оценки для величины $n$-го простого числа. Постулат Бертрана и теорема Чебышёва.

Простые числа расположены в натуральном ряду довольно неравномерно.

С одной стороны, можно указать сколь угодно длинные отрезки натурального ряда, свободные от простых чисел. Например, все $N$ подряд идущих чисел

$$(N+1)!+2,\ (N+1)!+3,\ \ldots,\ (N+1)!+(N+1)$$

являются составными.

С другой стороны, существует много пар простых чисел, разность между которыми минимальна, например $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(41,43)$. Такие пары называются *простыми числами-близнецами*. Известны примеры очень больших простых чисел-близнецов; последний рекорд таков:

$$3756801695685 \cdot 2^{666669} \pm 1$$

(декабрь 2011 года, см. `http://primes.utm.edu`).

**Определение 2.1.** Функция

$$\pi(x) = \sum_{p \leqslant x} 1, \quad x > 0,$$

называется *функцией распределения простых чисел*.

Иными словами, $\pi(x)$ есть количество простых чисел $p$, не превосходящих данного $x > 0$. Изучение асимптотического поведения функции $\pi(x)$ является важнейшей проблемой *аналитической теории чисел*.

Первый шаг в решении этой проблемы был сделан Евклидом. Его теорему 1.10 о бесконечности множества простых чисел можно сформулировать как утверждение

$$\pi(x) \to \infty, \quad x \to \infty.$$

Л. Эйлер (1707 — 1783) заметил, что доля простых чисел в начальном отрезке натурального ряда становится исчезающе малой с увеличением длины этого отрезка:

$$\frac{\pi(x)}{x} \to 0, \quad x \to \infty.$$

Полностью это утверждение было доказано А. Лежандром (1752 — 1833). Он же, пользуясь таблицами простых чисел, эмпирически установил приближённую формулу

$$\pi(x) \approx \frac{x}{\ln x - B}, \quad B = 1,08366. \tag{2.1}$$

К. Ф. Гаусс (1777 — 1855) утверждал, что более точной является формула

$$\pi(x) \approx \int_2^x \frac{dt}{\ln t}. \tag{2.2}$$

Первый существенный успех в изучении распределения простых чисел связан с именем русского учёного П. Л. Чебышёва (1821 — 1894), который совершенно элементарными методами выяснил истинный порядок роста функции $\pi(x)$, именно: доказал существование таких положительных констант $a$ и $b$, что для всех $x \geqslant 2$ выполняются неравенства

$$a\,\frac{x}{\ln x} < \pi(x) < b\,\frac{x}{\ln x}. \tag{2.3}$$

В 1845 году французский математик Ж. Бертран, анализируя таблицы простых чисел до $3 \cdot 10^6$ в связи со своими исследованиями по теории групп, высказал предположение, с тех пор известное как

**Постулат Бертрана.** При $n \geqslant 4$ в интервале $(n, 2n-2)$ есть хотя бы одно простое число.

Вскоре этот постулат был доказан Чебышёвым в его знаменитой работе 1850 года «О простых числах» (см. ниже теорему 2.3).

**I. Предварительные результаты.**

Для доказательства оценок Чебышёва и постулата Бертрана нам потребуются некоторые вспомогательные факты и определения.

При $x > 0$ рассмотрим *функции Чебышёва*

$$\vartheta(x) = \sum_{p \leqslant x} \ln p,$$

$$\psi(x) = \sum_{p^\alpha \leqslant x} \ln p = \sum_{p \leqslant x} \left[\frac{\ln x}{\ln p}\right] \ln p.$$

Пусть также

$$T(x) = \sum_{k \leqslant x} \ln k.$$

Из формулы (1.14) следует, что

$$T(x) = T([x]) = \ln [x]! = \sum_{p \leqslant [x]} \sum_{\alpha \geqslant 1} \left[\frac{[x]}{p^\alpha}\right] \ln p = \sum_{p \leqslant x} \sum_{\alpha \geqslant 1} \left[\frac{x}{p^\alpha}\right] \ln p,$$

а из формулы (1.15) — что

$$\psi(x) = \psi([x]) = \ln \mathrm{HOK}\,(1, 2, \ldots, [x]).$$

Кроме того, справедливы неравенства

$$\theta(x) \leqslant \psi(x) \leqslant \sum_{p \leqslant x} \ln x = \pi(x) \ln x. \tag{2.4}$$

В дальнейшем изложении важную роль будут играть арифметические свойства *центрального биномиального коэффициента*

$$N = N(n) = C_{2n}^{n} = \frac{(2n)!}{n!^2} = \mathrm{e}^{T(2n)-2T(n)}. \tag{2.5}$$

Положим также

$$K = K(n) = \mathrm{НОК}\,(1, 2, \ldots, 2n) = \mathrm{e}^{\psi(2n)}.$$

**Лемма 2.1.** $K$ делится на $N$.

Доказательство. Пусть $p$ — произвольный простой делитель числа $N$. Тогда, очевидно, $p \leqslant 2n$. Положим $m_p = \nu_p(K)$. Ясно, что

$$p^{m_p} \leqslant 2n, \quad p^{m_p+1} > 2n.$$

Теперь имеем

$$\nu_p(N) = \sum_{\alpha \geqslant 1} \left( \left[ \frac{2n}{p^\alpha} \right] - 2 \left[ \frac{n}{p^\alpha} \right] \right) = \sum_{\alpha=1}^{m_p} \left( \left[ \frac{2n}{p^\alpha} \right] - 2 \left[ \frac{n}{p^\alpha} \right] \right).$$

При любом $x$ разность $[2x] - 2[x]$ равна либо 0, либо 1, поэтому

$$\nu_p(N) \leqslant \sum_{\alpha=1}^{m_p} 1 = m_p = \nu_p(K).$$

Ввиду произвольности $p$ отсюда следует делимость $K$ на $N$. □

В качестве следствия получаем неравенство $K \geqslant N$ или

$$\psi(2n) \geqslant T(2n) - 2T(n).$$

Это неравенство и будет использоваться далее.

**Лемма 2.2.** При $n \geqslant 3$ имеет место неравенство $N > 2^{n+1}$.

Доказательство. Это неравенство является довольно грубым, однако его будет достаточно при доказательстве нижней оценки для $\pi(x)$.

Доказательство можно провести индукцией по $n \geqslant 3$. Шаг индукции:

$$\frac{(2k+2)!}{(k+1)^2} = \frac{(2k)!}{k!^2} \cdot \frac{2(2k+1)}{k+1} > 2^{k+1}\,\frac{2(2k+1)}{k+1} > 2^{k+2}$$

(проверить базу индукции предоставляется читателю). □

Индукцией по $n \geqslant 1$ можно доказать более сильное неравенство

$$N > \frac{4^n}{\sqrt{4n}},$$

которое нам понадобится при обосновании постулата Бертрана. Вообще, если константа $c > \pi$, то при $n > n_0 = n_0(c)$ имеет место неравенство

$$N > \frac{4^n}{\sqrt{cn}}.$$

С другой стороны, при $n \geqslant 1$ справедливо неравенство

$$N < \frac{4^n}{\sqrt{\pi n}}.$$

Действительно, последовательность

$$x_n = \frac{C_{2n}^n \sqrt{n}}{4^n}$$

строго возрастает и имеет пределом число $1/\sqrt{\pi}$. Последнее утверждение эквивалентно классической *формуле Валлиса*:

$$\frac{3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 7 \cdot \ldots}{2 \cdot 4 \cdot 4 \cdot 6 \cdot 6 \cdot 8 \cdot \ldots} = \lim_{n\to\infty} \frac{4n((2n-1)!!)^2}{((2n)!!)^2} = \frac{4}{\pi}.$$

**II. Оценки Чебышёва для $\pi(x)$.**

Сначала докажем оценку снизу — левое неравенство в формуле (2.3).

**Теорема 2.1.** При $x \geqslant 6$ справедливо неравенство

$$\pi(x) > a\,\frac{x}{\ln x}$$

с константой $a = \frac{1}{2}\ln 2 \approx 0.34657$.

Доказательство. Подберём натуральное $n \geqslant 3$ так, чтобы

$$2n \leqslant x < 2n + 2.$$

Применив леммы 2.1 и 2.2, получим

$$\pi(x)\ln x \geqslant \pi(2n)\ln 2n \geqslant \psi(2n) \geqslant T(2n) - 2T(n) > (n+1)\ln 2 > ax.$$

Таким образом, $\pi(x)\ln x > ax$, что и требовалось доказать. □

Для доказательства оценки сверху — правого неравенства в формуле (2.3) — нам понадобится

**Лемма 2.3.** При $x \geqslant 2$ имеет место неравенство

$$\mathrm{e}^{\vartheta(x)} = \prod_{p\leqslant x} p < 4^x.$$

Доказательство. Достаточно рассмотреть случай, когда $x = n$ — натуральное число. Докажем неравенство

$$\prod_{p\leqslant n} p < 4^n$$

индукцией по $n \geqslant 2$.

Сделаем шаг индукции. Если $n > 2$ чётно, то

$$\prod_{p\leqslant n} p = \prod_{p\leqslant n-1} p < 4^{n-1} < 4^n.$$

Пусть $n > 2$ нечётно, $n = 2k+1$ $(k \geqslant 1)$. Имеем

$$\prod_{p\leqslant n} p = \prod_{p\leqslant k+1} p \prod_{k+1<p\leqslant 2k+1} p < 4^{k+1} \prod_{k+1<p\leqslant 2k+1} p.$$

Рассмотрим число

$$M = M(k) = C_{2k+1}^k = \frac{(2k+1)!}{(k+1)!k!}.$$

Если $k+1 < p \leqslant 2k+1$, то, очевидно, $\nu_p(M) \geqslant 1$. Следовательно,

$$\prod_{k+1<p\leqslant 2k+1} p \leqslant \prod_{k+1<p\leqslant 2k+1} p^{\nu_p(M)} \leqslant \prod_{p\leqslant 2k+1} p^{\nu_p(M)} = M.$$

Нетрудно установить неравенство

$$M < 4^k. \tag{2.6}$$

Таким образом,

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

и шаг индукции сделан. □

**Упражнение 2.1.** Докажите неравенство (2.6).
*Указание*. Как и при доказательстве леммы 2.2, можно применить индукцию по $k \geqslant 1$.

**Теорема 2.2.** При $x \geqslant 2$ справедливо неравенство

$$\pi(x) < b\,\frac{x}{\ln x}$$

с константой $b = 5\ln 2 \approx 3.46574$.

Доказательство. Заметим, что $\pi(x) \leqslant x/2$ при $x \geqslant 8$. Имеем

$$\vartheta(x) \geqslant \sum_{\sqrt{x}<p\leqslant x} \ln p \geqslant \sum_{\sqrt{x}<p\leqslant x} \ln\sqrt{x} = (\pi(x) - \pi(\sqrt{x})\ln\sqrt{x}.$$

Так как $\vartheta(x) \leqslant 2x\ln 2$ по лемме 2.3, то

$$\pi(x) \leqslant \frac{4x\ln 2}{\ln x} + \pi(\sqrt{x}) \leqslant \frac{4x\ln 2}{\ln x} + \frac{\sqrt{x}}{2} < b\,\frac{x}{\ln x}$$

при $x \geqslant 64$. Прямой проверкой можно убедиться, что доказываемое неравенство верно и при $2 \leqslant x < 64$. □

**Упражнение 2.2.** Пусть $p_n$ — $n$-е простое число. Докажите существование таких положительных констант $\alpha$ и $\beta$, что

$$\alpha n \ln n < p_n < \beta n \ln n$$

при всех $n \geqslant 2$.

*Указание.* При $x = p_n$ формула (2.3) принимает вид

$$a \frac{p_n}{\ln p_n} < \pi(p_n) = n < b \frac{p_n}{\ln p_n}. \tag{2.7}$$

После логарифмирования получим

$$\ln p_n - \ln\ln p_n + \ln a < \ln n < \ln p_n - \ln\ln p_n + \ln b. \tag{2.8}$$

Теперь осталось почленно перемножить (2.7) и (2.8).

### III. Доказательство постулата Бертрана.

Следующая теорема впервые была доказана П. Л. Чебышёвым.

**Теорема 2.3.** При $n \geqslant 2$ между $n$ и $2n$ есть хотя бы одно простое число.

Доказательство. Мы приведём короткое доказательство, принадлежащее П. Эрдёшу (1913 — 1996). Его идею можно кратко описать так: биномиальный коэффициент (2.5) был бы слишком мал, если бы он не имел простых делителей между $n$ и $2n$.

При $2 \leqslant n \leqslant 68$ утверждение теоремы проверяется непосредственно.

Пусть $n > 68$. Имеем

$$N = \frac{(2n)!}{n!^2} = \prod_{p \leqslant 2n} p^{\nu_p(N)} =$$

$$= \prod_{p \leqslant \sqrt{2n}} p^{\nu_p(N)} \prod_{\sqrt{2n} < p \leqslant 2n/3} p^{\nu_p(N)} \prod_{2n/3 < p \leqslant n} p^{\nu_p(N)} \prod_{n < p \leqslant 2n} p^{\nu_p(N)}.$$

Если $n < p \leqslant 2n$, то $\nu_p(N) = 1$. Следовательно,

$$\prod_{n < p \leqslant 2n} p^{\nu_p(N)} = \prod_{n < p \leqslant 2n} p.$$

Если $2n/3 < p \leqslant n$, то $\nu_p(N) = 0$ (это, по мнению автора идеи, ключевое место в доказательстве), т. е.

$$\prod_{2n/3 < p \leqslant n} p^{\nu_p(N)} = 1.$$

Если $p > \sqrt{2n}$, то $\nu_p(N) \leqslant 1$, поскольку имеем

$$p^{\nu_p(N)} \leqslant p^{\nu_p(K)} \leqslant 2n$$

(здесь, как и выше, $K = \text{НОК}(1, 2, \ldots, 2n)$). Значит,

$$\prod_{\sqrt{2n} < p \leqslant 2n/3} p^{\nu_p(N)} \leqslant \prod_{p \leqslant 2n/3} p < 4^{2n/3}$$

(см. лемму 2.3). Наконец,

$$\prod_{p\leqslant\sqrt{2n}} p^{\nu_p(N)} \leqslant (2n)^{\pi(\sqrt{2n})} \leqslant (2n)^{\sqrt{n/2}}.$$

Таким образом, имеем двойную оценку

$$\frac{4^n}{\sqrt{4n}} < N < 4^{2n/3}(2n)^{\sqrt{n/2}} \prod_{n<p\leqslant 2n} p.$$

Но она будет противоречива при $n > 68$, если предположить, что

$$\prod_{n<p\leqslant 2n} p = 1,$$

т. е. что между $n$ и $2n$ нет простых чисел. □

**A.** Сколь много простых чисел лежит между $n$ и $2n$? При $n > 68$ мы пришли к неравенству

$$P = P(n) = \prod_{n<p\leqslant 2n} p > \frac{4^{n/3}}{(2n)^{\sqrt{n/2}}\sqrt{4n}} = f(n).$$

Так как, очевидно, $P \leqslant (2n)^{\pi(2n)-\pi(n)}$, то

$$(\pi(2n) - \pi(n)) \ln 2n \geqslant \ln P > \ln f(n).$$

Отсюда следует оценка

$$\pi(2n) - \pi(n) > \frac{\ln f(n)}{\ln 2n} \sim \frac{c_1 n}{\ln n}, \quad n \to \infty,$$

где $c_1 = \frac{2}{3}\ln 2 = 0.46209$. Эта оценка не слишком груба (см. ниже упражнение 2.5).

**B.** Как доказывал постулат Бертрана сам Чебышёв? Ниже мы изложим упрощённую версию доказательства, предложенную С. Б. Стечкиным (1920 — 1995). Она полностью основана на идеях Чебышёва, главной из которых является использование тождеств

$$\psi(x) = \sum_{k\geqslant 1} \vartheta(x^{1/k}), \quad T(x) = \sum_{k\geqslant 1} \psi(x/k), \tag{2.9}$$

теперь называемых *тождествами Чебышёва*.

**Упражнение 2.3.** Докажите эти тождества.

*Решение.* Имеем

$$\sum_{k\geqslant 1} \vartheta(x^{1/k}) = \sum_{k\geqslant 1} \sum_{p\leqslant x^{1/k}} \ln p = \sum_{p\leqslant x} \sum_{k\leqslant \ln x/\ln p} \ln p = \sum_{p\leqslant x} \left[\frac{\ln x}{\ln p}\right] \ln p = \psi(x),$$

и первое тождество доказано. Второе доказывается чуть сложнее. Поскольку

$$\sum_{k\geqslant 1} \psi(x/k) = \sum_{k\geqslant 1} \sum_{p\leqslant x/k} \left[\frac{\ln (x/k)}{\ln p}\right] \ln p = \sum_{p\leqslant x} \sum_{k\leqslant x/p} \left[\frac{\ln (x/k)}{\ln p}\right] \ln p,$$

достаточно убедиться в том, что

$$\sum_{k\leqslant x/p}\left[\frac{\ln(x/k)}{\ln p}\right]=\sum_{\alpha\geqslant 1}\left[\frac{x}{p^\alpha}\right].$$

Пусть $[\ln(x/k)/\ln p]=\alpha$. Легко видеть, что это условие равносильно ограничениям

$$\frac{x}{p^{\alpha+1}}<k\leqslant\frac{x}{p^\alpha},$$

которым удовлетворяют в точности $[x/p^\alpha]-[x/p^{\alpha+1}]$ значений $k$. Следовательно,

$$\sum_{k\leqslant x/p}\left[\frac{\ln(x/k)}{\ln p}\right]=\sum_{\alpha\geqslant 1}\alpha\left(\left[\frac{x}{p^\alpha}\right]-\left[\frac{x}{p^{\alpha+1}}\right]\right)=\sum_{\alpha\geqslant 1}\left[\frac{x}{p^\alpha}\right],$$

что и требовалось. □

Доказательство постулата Бертрана состоит из нескольких этапов.

**Оценка разности $\vartheta(x)-\vartheta(x/2)$.** Рассмотрим функцию

$$U(x)=T(x)-2T(x/2).$$

Опираясь на второе из тождеств (2.9), заметим, что эта функция разлагается в знакопеременный ряд:

$$U(x)=\sum_{k\geqslant 1}(-1)^{k-1}\psi(x/k).$$

Поскольку функция $\psi(x)$ не убывает, справедливы неравенства

$$\psi(x)-\psi(x/2)\leqslant U(x)\leqslant\psi(x)-\psi(x/2)+\psi(x/3),$$

которые можно переписать в виде

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

Аналогичные соображения приводят к неравенствам

$$\psi(x)-2\psi(x^{1/2})\leqslant\vartheta(x)\leqslant\psi(x).$$

Таким образом,

$$\vartheta(x)-\vartheta(x/2)\geqslant\psi(x)-2\psi(x^{1/2})-\psi(x/2)\geqslant U(x)-\psi(x/3)-2\psi(x^{1/2}).$$

**Оценка $U(x)$.** Имеем

$$\begin{aligned}U(x)&=\sum_{k\leqslant x}\ln k-2\sum_{k\leqslant x/2}\ln k=\sum_{k\leqslant x}\ln k-2\sum_{2k\leqslant x}\ln 2k+2\left[\frac{x}{2}\right]\ln 2=\\&=\sum_{k\leqslant x}(-1)^{k-1}\ln k+2\left[\frac{x}{2}\right]\ln 2,\end{aligned}$$

откуда

$$x\ln 2-\ln x-2\ln 2\leqslant U(x)\leqslant x\ln 2+\ln x.$$

**Оценка $\psi(x)$.** Введём функцию

$$V(x) = 2x\ln 2 + \frac{1}{2\ln 2}\ln^2 x + \frac{1}{2}\ln x.$$

Имеем

$$V(x) - V(x/2) = x\ln 2 + \ln x \geqslant U(x) \geqslant \psi(x) - \psi(x/2).$$

Следовательно,

$$V(x) - \psi(x) \geqslant V(x/2) - \psi(x/2) \geqslant \ldots \geqslant V(x/2^m) - \psi(x/2^m) = \\ = V(x/2^m) \geqslant V(1),$$

где $m = [\ln x/\ln 2]$. Таким образом,

$$\psi(x) \leqslant V(x) - V(1) = 2x\ln 2 + \frac{1}{2\ln 2}\ln^2 x + \frac{1}{2}\ln x - 2\ln 2.$$

**Завершающие оценки.** Используя нижнюю оценку для $U(x)$ и верхние оценки для $\psi(x)$ и $\psi(x^{1/2})$, при $x \geqslant 4$ приходим к следующему:

$$\vartheta(x) - \vartheta(x/2) \geqslant U(x) - \psi(x/3) - 2\psi(x^{1/2}) - \ln x \geqslant \\ \geqslant \frac{\ln 2}{3}x - 4x^{1/2}\ln 2 - \frac{3}{4\ln 2}\ln^2 x - 2\ln x + 4\ln 2 = W(x).$$

Следовательно,

$$\pi(x) - \pi(x/2) \geqslant \frac{1}{\ln x}\sum_{x/2<p\leqslant x}\ln p = \frac{\vartheta(x) - \vartheta(x/2)}{\ln x} \geqslant \frac{W(x)}{\ln x} \sim \frac{c_2 x}{\ln x}, \quad x \to \infty.$$

где $c_2 = \frac{1}{3}\ln 2 = 0.23104$, поэтому $\pi(x) - \pi(x/2) > 0$ при всех достаточно больших $x$.

**С.** В своём мемуаре «О простых числах» Чебышёв фактически получил более сильный, чем постулат Бертрана, результат.

**Теорема 2.4.** Для любого $\delta > 6/5$ существует такое $n_0 = n_0(\delta)$, что для каждого $n \geqslant n_0$ интервал $(n, \delta n)$ содержит хотя бы одно простое число.

К этой теореме Чебышёв пришёл следующим образом. Он рассмотрел более сложную и специально подобранную комбинацию функций вида $T(x/k)$, именно:

$$\widetilde{U}(x) = T(x) - T(x/2) - T(x/3) - T(x/5) + T(x/30).$$

Двустороннюю оценку для функции $\widetilde{U}(x)$ можно дать с помощью хорошо известной *формулы Стирлинга*

$$n! = \sqrt{2\pi}\, n^{n+1/2}\mathrm{e}^{-n+\varepsilon_n}, \quad 0 < \varepsilon_n < \frac{1}{12n}.$$

Разложив функцию $\widetilde{U}(x)$ в знакопеременный ряд, Чебышёв доказал неравенства

$$\psi(x) - \psi(x/6) \leqslant \widetilde{U}(x) \leqslant \psi(x),$$

из которых затем вывел двустороннюю оценку для функции $\psi(x)$. Далее, исходя из неравенств

$$\psi(x) - 2\psi(x^{1/2}) \leqslant \vartheta(x) \leqslant \psi(x) - \psi(x^{1/2}),$$

он получил двустороннюю оценку для функции $\vartheta(x)$. Эта итоговая оценка такова:

$$Ax - \frac{12A}{5}\,x^{1/2} - \frac{5}{8\ln 6}\ln^2 x - \frac{15}{4}\ln x - 3 \leqslant \vartheta(x) \leqslant \frac{6A}{5}\,x - Ax^{1/2} + \frac{5}{4\ln 6}\ln^2 x + \frac{5}{2}\ln x + 2,$$

где константа

$$A = \ln\frac{2^{1/2}3^{1/3}5^{1/5}}{30^{1/30}} \approx 0.92129.$$

Следствием этой оценки и явилась теорема 2.4.

**Упражнение 2.4.** Дайте подробное доказательство теоремы 2.4.
*Указание.* Можно (и даже настоятельно рекомендуется) ознакомиться с первоисточником.

Пользуясь полученной оценкой для функции $\vartheta(x)$, Чебышёв также установил границы для функции распределения простых чисел $\pi(x)$. При этом он исходил из очевидного равенства

$$\pi(x) = \sum_{2\leqslant k\leqslant x} \frac{\vartheta(k) - \vartheta(k-1)}{\ln k}.$$

Оказалось, что неравенства (2.3) выполняются с константами

$$a \approx 0.92129, \quad b \approx 1.10555, \tag{2.10}$$

начиная с некоторого $x$.

## 2.2 Асимптотический закон распределения простых чисел

Формулировка асимптотического закона распределения простых чисел. Вывод его следствий — асимптотических формул для $n$-го простого числа, для произведения всех простых чисел, не превосходящих $n$, и для НОК $(1, 2, \ldots, n)$. Простые числа в арифметических прогрессиях.

Как доказал Чебышёв, неравенства (2.3) выполняются с константами (2.10) при достаточно больших $x$. Эти константы довольно близки к единице. Следующим шагом должно было стать доказательство *асимптотического закона распределения простых чисел*:

$$\pi(x) \sim \frac{x}{\ln x}, \quad x \to \infty. \tag{2.11}$$

В работе 1848 года «Об определении числа простых чисел, не превосходящих данной величины» Чебышёву удалось установить лишь следующее предложение: *если предел отношения*

$$\pi(x) : \frac{x}{\ln x}$$

*существует, то он равен единице*. В этой же работе он показал, что (при условии существования предела) формула Лежандра (2.1) будет точнее, если в ней положить $B = 1$. Но ещё более точной оказывается формула Гаусса (2.2), она точнее формулы Лежандра, каково бы ни было значение постоянной $B$. Отметим, что к рассмотрению *интегрального логарифма*

$$\operatorname{Li}(x) = \int\limits_2^x \frac{dt}{\ln t} \sim \frac{x}{\ln x}, \quad x \to \infty,$$

Чебышёв пришёл независимо от Гаусса, доказав, что функция $\operatorname{Li}(x)$ приближает $\pi(x)$ точнее, чем функция $x/\ln x$.

Асимптотический закон в форме

$$\pi(x) \sim \operatorname{Li}(x), \quad x \to \infty,$$

впервые был доказан в 1896 году одновременно и независимо Ж. Адамаром (1865 — 1963) и Ш. Ж. де ла Валле-Пуссеном (1866 — 1962). Доказательство использует методы теории функций комплексного переменного, которые применяются для изучения свойств специальной *дзета-функции Римана* $\zeta(s)$ — аналитической функции комплексного переменного $s$, заданной при $\Re s > 1$ рядом

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Глубокая связь между распределением простых чисел и расположением нулей функции $\zeta(s)$ ранее была обнаружена Б. Риманом (1826 — 1866). Впервые дзета-функция появилась в одной работе Эйлера 1737 года, который получил представление этой функции в виде бесконечного произведения:

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \quad \Re s > 1 \tag{2.12}$$

(*тождество Эйлера*).

Доказательство асимптотического закона распределения простых чисел выходит за рамки настоящего пособия, и мы ограничимся тем, что выведем из него некоторые асимптотические формулы.

**Теорема 2.5.** Пусть $p_n$ — $n$-е простое число. Тогда

$$p_n \sim n \ln n, \quad n \to \infty.$$

ДОКАЗАТЕЛЬСТВО. Имеем

$$n = \pi(p_n) \sim \frac{p_n}{\ln p_n}, \quad n \to \infty.$$

Это можно записать как

$$n = \frac{p_n}{\ln p_n}\,(1 + \varepsilon_n),$$

где $\varepsilon_n \to 0$ при $n \to \infty$. Тогда $\ln n = (\ln p_n - \ln\ln p_n + \ln(1+\varepsilon_n))$ и

$$n \ln n = \frac{p_n}{\ln p_n}\,(1+\varepsilon_n)(\ln p_n - \ln\ln p_n + \ln(1+\varepsilon_n)) \sim p_n, \quad n \to \infty.$$

(Ср. с решением упражнения 2.2.) □

**Пример 2.1.** Простое число $p = 1000003$ имеет номер 78499. Применив асимптотическую формулу, получим $p \approx 884750$. Относительная погрешность этого приближённого равенства составляет примерно 12%.

Отметим, что асимптотическая формула для $p_n$ допускает уточнения.

**Упражнение 2.5.** Пусть $\delta > 1$ — произвольное фиксированное число. Докажите, что при всех достаточно больших $n$ в интервале $(n, \delta n)$ содержится хотя бы одно простое число.

*Указание.* Используя (2.11), докажите оценку

$$\pi(\delta n) - \pi(n) \sim \frac{(\delta - 1)n}{\ln n}, \quad n \to \infty.$$

**Теорема 2.6.** Справедливы соотношения

$$\prod_{p \leqslant n} p = \mathrm{e}^{n(1+\delta_1(n))}, \quad \text{НОК}\,(1, 2, \ldots, n) = \mathrm{e}^{n(1+\delta_2(n))}, \tag{2.13}$$

где $\delta_i(n) \to 0$ при $n \to \infty$.

ДОКАЗАТЕЛЬСТВО. Функции $\theta(x)$, $\psi(x)$ и $\pi(x)$ связаны неравенствами (2.4), откуда

$$\frac{\theta(x)}{x} \leqslant \frac{\psi(x)}{x} \leqslant \frac{\pi(x)}{x/\ln x}.$$

Пусть $0 < \varepsilon < 1$. Имеем

$$\theta(x) = \sum_{p \leqslant x} \ln p \geqslant \sum_{x^{1-\varepsilon} < p \leqslant x} \ln p > \ln x^{1-\varepsilon}(\pi(x) - \pi(x^{1-\varepsilon})).$$

Поскольку $\pi(x^{1-\varepsilon}) < x^{1-\varepsilon}$, после преобразований получим

$$\frac{\theta(x)}{x} > (1-\varepsilon)\left(\frac{\pi(x)}{x/\ln x} - \frac{\ln x}{x^{\varepsilon}}\right).$$

Итак, имеем следующую цепочку неравенств:

$$(1-\varepsilon)\left(\frac{\pi(x)}{x/\ln x} - \frac{\ln x}{x^{\varepsilon}}\right) < \frac{\theta(x)}{x} \leqslant \frac{\psi(x)}{x} \leqslant \frac{\pi(x)}{x/\ln x}.$$

Переходя к нижним и верхним пределам отношений $\theta(x)/x$ и $\psi(x)/x$ при $x \to \infty$ и учитывая асимптотический закон распределения простых чисел (2.11), получим, что все эти пределы заключены в отрезке $[1-\varepsilon, 1]$. Но $\varepsilon$ можно выбрать сколь угодно малым, поэтому все нижние и верхние пределы должны совпадать и быть равными единице. Таким образом,

$$\lim_{x\to\infty} \frac{\theta(x)}{x} = \lim_{x\to\infty} \frac{\psi(x)}{x} = 1.$$

Поскольку имеют место равенства

$$\prod_{p\leqslant n} p = \mathrm{e}^{\vartheta(n)}, \quad \text{НОК}\,(1, 2, \ldots, n) = \mathrm{e}^{\psi(n)},$$

соотношения (2.13) можно считать доказанными. □

Важную для приложений проблему генерации больших простых чисел (см. раздел 5.1) можно решать вероятностным методом: выбрать случайным образом $k$-значное число и затем проверить его на простоту. Асимптотический закон распределения простых чисел позволяет оценить эффективность такого подхода.

Действительно, отношение

$$\frac{\pi(10^k) - \pi(10^{k-1})}{10^k - 10^{k-1}},$$

выражающее долю простых $k$-значных чисел, асимптотически равно

$$\frac{1}{k\ln 10} \approx \frac{0.43}{k}$$

(см. указание к упражнению 2.5). Так, для $k = 100$ потребуется проверить примерно 230 чисел, чтобы обнаружить хотя бы одно простое число (конечно, при дополнительном предположении о некоторой «равномерности» распределения простых чисел).

Завершим нашу краткую экскурсию в аналитическую теорию чисел обзором основных фактов о распределении простых чисел в арифметических прогрессиях — наиболее простых бесконечных подмножествах натурального ряда.

Несомненно, самым фундаментальным фактом в этой области является теорема, которую впервые доказал Дирихле в 1839 году и которая с тех пор носит его имя.

**Теорема 2.7.** В любой арифметической прогрессии

$$mk + l, \quad k = 1, 2, 3, \ldots, \tag{2.14}$$

удовлетворяющей условию НОД $(m, l) = 1$, содержится бесконечно много простых чисел.

Эта теорема впервые была сформулирована ещё Эйлером в 1783 году. В 1798 году Лежандр попытался доказать её для чётных $m$, и даже опубликовал доказательство, однако оно оказалось ошибочным.

В некоторых частных случаях теорему Дирихле удаётся доказать совершенно элементарно, применив рассуждение Евклида — см., например, упражнение 1.14. Вот ещё один пример такого рода.

**Пример 2.2.** В арифметической прогрессии $4k+1$ содержится бесконечно много простых чисел.

Пусть, от противного, $p_1, p_2, \ldots, p_n$ — все простые числа такого вида. Положим

$$N = (2p_1p_2 \ldots p_n)^2 + 1.$$

Любой простой делитель числа $N$ должен быть вида $4k+1$ (см. упражнение 3.9), но ни одно из простых чисел $p_i$ не делит $N$ — противоречие.

**Упражнение 2.6.** Докажите, что арифметическая прогрессия $8k+5$ содержит бесконечно много простых чисел.

*Указание.* Рассмотрите число $N = (p_1p_2 \ldots p_n)^2 + 4$.

Аналогичными рассуждениями можно доказать утверждение теоремы Дирихле для всех прогрессий (2.14) с $m = 8$, а также $m = 12$. Сложнее, но все ещё элементарными средствами доказывается при любом натуральном $m$ бесконечность множества простых чисел каждого из видов $mk \pm 1$. Однако к настоящему времени не найдено доказательство теоремы Дирихле с помощью элементарных рассуждений, обобщающих идею Евклида. Наиболее простое доказательство этой теоремы опирается на методы теории функций комплексной переменной и основано на рассмотрении особых теоретико-числовых функций $\chi(n)$ — *характеров по модулю* $m$, а также специальных функций

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

(так называемых *L-рядов Дирихле*) при комплексных значениях аргумента $s$.

Продемонстрируем идею доказательства на примере тех же прогрессий $4k \pm 1$. Положим

$$\chi_0(n) = \begin{cases} 0, & n \text{ чётно}, \\ 1, & n \text{ нечётно}, \end{cases} \qquad \chi_1(n) = \begin{cases} 0, & n \text{ чётно}, \\ (-1)^{(n-1)/2}, & n \text{ нечётно}, \end{cases}$$

и рассмотрим при $s > 1$ соответствующие $L$-ряды

$$L_0(s) = \sum_{n=1}^{\infty} \frac{\chi_0(n)}{n^s} = \sum_{k=0}^{\infty} \frac{1}{(2k+1)^s}, \quad L_1(s) = \sum_{n=1}^{\infty} \frac{\chi_1(n)}{n^s} = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)^s}.$$

Для этих рядов справедлив аналог тождества Эйлера (2.12):

$$L_i(s) = \prod_p \left(1 - \frac{\chi_i(p)}{p^s}\right)^{-1}, \quad i = 0, 1.$$

Отсюда можно вывести при $s \to 1$ оценки

$$\sum_p \frac{\chi_i(p)}{p^s} = \ln L_i(s) + O(1), \quad i = 0,\, 1.$$

Комбинируя их и используя определение функций $\chi_i$, получим при $s \to 1$

$$\sum\nolimits^{(1)} \frac{1}{p^s} = \frac{\ln L_0(s) + \ln L_1(s)}{2} + O(1), \quad \sum\nolimits^{(2)} \frac{1}{p^s} = \frac{\ln L_0(s) - \ln L_1(s)}{2} + O(1),$$

где первая и вторая суммы распространены на все простые $p$ вида $4k+1$ и $4k-1$ соответственно. Но тогда имеем

$$\lim_{s\to 1} \sum\nolimits^{(i)} \frac{1}{p^s} = \infty, \quad i = 1,\, 2.$$

Действительно, $L_0(s) \to \infty$ при $s \to 1$ и в то же время

$$L_1(1) \neq 0, \tag{2.15}$$

как можно непосредственно проверить. Таким образом, простых чисел каждого из видов $4k \pm 1$ не может быть конечное множество.

Интересно отметить, что при реализация этой идеи в общем случае наибольшие трудности возникают именно при доказательстве соотношений типа (2.15), ради чего, собственно, и привлекаются методы теории функций комплексного переменного.

Элементарное (т. е. не использующее теорию функций комплексного переменного) доказательство теоремы Дирихле было найдено А. Сельбергом в 1949 году. Вместе с П. Эрдёшом он дал также элементарное доказательство асимптотического закона распределения простых чисел. Оба доказательства чрезвычайно сложны.

В 1899 году Валле-Пуссен установил асимптотическую формулу для $\pi(x, m, l)$ — количества простых чисел в прогрессии (2.14), не превосходящих $x$. Оказалось, что независимо от $l$, НОД $(m, l) = 1$,

$$\pi(x, m, l) \sim \frac{1}{\varphi(m)} \operatorname{Li}(x), \quad x \to \infty, \tag{2.16}$$

т. е. простые числа распределены примерно поровну по всем $\varphi(m)$ прогрессиям вида (2.14).

Формула (2.16) показывает, что в прогрессии (2.14) имеется значительное количество простых чисел, однако ничего не говорит о том, как далеко от начала прогрессии начнут встречаться простые числа. В этой связи приведём результат Ю. В. Линника, полученный им в 1944 году: *существует такая абсолютная константа $c_0$, что наименьшее простое число в прогрессии* (2.14) *не превосходит $m^{c_0}$*.

Более подробно с вопросами распределения простых чисел можно познакомиться по книгам [1] и [4].

# 3 Теория сравнений

## 3.1 Определение и свойства сравнений

Понятие сравнимости целых чисел по модулю. Обозначение Гаусса. Основные свойства сравнений по модулю.

Мы будем рассматривать целые числа в связи с их остатками от деления на данное натуральное число $m$, которое будем называть модулем.

**Определение 3.1.** Пусть $a$, $b \in \mathbb{Z}$. Говорят, что $a$ *сравнимо с* $b$ *по модулю* $m$, если разность $a - b$ делится на $m$.

В своей знаменитой книге «Disquisitiones Arithmeticae» («Арифметические исследования»), вышедшей в 1801 году, Гаусс предложил отношение «*быть сравнимыми по модулю* $m$» записывать так:

$$a \equiv b \pmod{m}. \tag{3.1}$$

Эта запись, называемая *сравнением по модулю* $m$, оказалась исключительно удобной. Как и равенство, сравнение состоит из двух частей: левой (до знака $\equiv$) и правой (после знака $\equiv$). Но, в отличие от равенства, сравнение всегда подразумевает некоторый модуль $m$.

**Теорема 3.1.** Условие (3.1) равносильно любому из следующих условий.
(а) Числа $a$ и $b$ дают одинаковые остатки при делении на $m$.
(б) Число $a$ представимо в виде $a = b + mt$, где $t \in \mathbb{Z}$.

Доказательство. Разделим $a$ и $b$ на $m$ с остатком:

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

Ясно, что условие (3.1) равносильно делимости $r_1 - r_2$ на $m$. Но эта делимость, в силу ограничений на остатки $r_i$, означает их совпадение.
Равносильность условий (3.1) и (б) очевидна. □

Таким образом, любое из условий (а) и (б) теоремы 3.1 можно принять за определение сравнимости по модулю $m$ (обычно предпочитают условие равноостаточности (а)).

Прежде чем перейти к обсуждению свойств сравнений, заметим, что (как отношение на множестве $\mathbb{Z}$) отношение «быть сравнимыми по модулю $m$» является *отношением эквивалентности*, т. е. удовлетворяет условиям *рефлексивности*, *симметричности* и *транзитивности*.

**Упражнение 3.1.** Убедитесь в этом.

В частности, если два числа сравнимы с третьим по данному модулю, то они сравнимы между собой по этому же модулю.

Теперь сформулируем и докажем базовые свойства сравнений по модулю. Эти свойства, как правило, вполне аналогичны соответствующим свойствам равенств и составляют основу техники сравнений, полезной при решении различных теоретико-числовых задач. (Далее $a$, $b$, $c$ и т. д. обозначают целые числа.)

**1.** Если $a \equiv b \pmod m$, $c \equiv d \pmod m$, то

$$a \pm c \equiv b \pm d \pmod m, \quad ac \equiv bd \pmod m.$$

**2.** Если $a + b \equiv c \pmod m$, то $a \equiv c - b \pmod m$.

**3.** Если $a \equiv b \pmod m$, то $ak \equiv bk \pmod m$ при любом $k$.

**4.** Если $ka \equiv kb \pmod m$, причём НОД $(k, m) = 1$, то $a \equiv b \pmod m$.

**5.** Если $a \equiv b \pmod m$, то $a \equiv b + mt \pmod m$ при любом $t$.

**6.** Пусть $a \equiv b \pmod m$. Если $f(x) = c_n x^n + \ldots + c_1 x + c_0 \in \mathbb{Z}[x]$, то

$$f(a) \equiv f(b) \pmod m.$$

**7.** Если $a_i \equiv b_i \pmod m$ $(i = 1, \ldots, n)$ и $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$, то

$$f(a_1, \ldots, a_n) \equiv f(b_1, \ldots, b_n) \pmod m.$$

**8.** Если $a_i \equiv b_i \pmod m$ $(i = 1, \ldots, n)$ и многочлены с целыми коэффициентами

$$f(x_1, \ldots, x_n) = \sum A_{(k_1,\ldots,k_n)} x_1^{k_1} \ldots x_n^{k_n},$$
$$g(x_1, \ldots, x_n) = \sum B_{(k_1,\ldots,k_n)} x_1^{k_1} \ldots x_n^{k_n}$$

таковы, что $A_{(k_1,\ldots,k_n)} \equiv B_{(k_1,\ldots,k_n)} \pmod m$ для всех $(k_1, \ldots, k_n)$, то

$$f(a_1, \ldots, a_n) \equiv g(b_1, \ldots, b_n) \pmod m.$$

Доказательство. Приведём доказательства наиболее неочевидных свойств.

**1.** Имеем $a = b + mt_1$, $c = d + mt_2$, где $t_1, t_2 \in \mathbb{Z}$. Тогда

$$(a \pm c) - (b \pm d) = m(t_1 \pm t_2), \quad ac - bd = m(bt_2 + dt_1 + mt_1 t_2)$$

и утверждение доказано.

**4.** По определению, разность $ka - kb = k(a - b)$ должна делиться на $m$. Но $k$ и $m$ взаимно просты. По свойству 1 взаимно простых чисел (см. раздел 1.2) отсюда следует, что на $m$ делится $a - b$, т. е. $a \equiv b \pmod m$.

**6.** Поскольку сравнения можно перемножать (свойство 1), имеем

$$a^k \equiv b^k \pmod m, \quad k = 0, 1, 2, \ldots \tag{3.2}$$

Если умножить обе части сравнения (3.2) на $c_k$ и просуммировать по $k = 0, 1, \ldots, n$, получим $f(a) \equiv f(b) \pmod m$.

**7, 8.** Эти свойства являются обобщением свойства 6 и доказываются аналогичным образом. □

**Упражнение 3.2.** Восстановите пропущенные доказательства.

В свойствах 1 — 8 модуль сравнения оставался неизменным. В следующих дополнительных свойствах участвуют сравнения по разным модулям.

**9.** Если $a \equiv b \pmod m$ и $d \geqslant 1$ — делитель $m$, то $a \equiv b \pmod d$.

**10.** Если $a \equiv b \pmod m$, то $ak \equiv bk \pmod{mk}$ при любом $k \geqslant 1$.

**11.** Если $a \equiv b \pmod m$, а $d \geqslant 1$ — общий делитель чисел $a$, $b$, $m$, то $a/d \equiv b/d \pmod{m/d}$.

**12.** Если $a \equiv b \pmod{m_1}$ и $a \equiv b \pmod{m_2}$, то $a \equiv b \pmod m$, где $m = \text{НОК}\,(m_1, m_2)$.

**13.** Если $a \equiv b \pmod m$ и $d$ — общий делитель $a$ и $m$, то $b$ делится на $d$.

**14.** Если $a \equiv b \pmod m$, то $\text{НОД}\,(a, m) = \text{НОД}\,(b, m)$.

ДОКАЗАТЕЛЬСТВО. И здесь все утверждения почти сразу следуют из определений.

**9.** Имеет место благодаря транзитивности отношения делимости.

**10, 11.** Пусть $a - b = mt$ для некоторого целого $t$. Умножив на $k$ (разделив на $d$), получим требуемое.

**12.** Разность $a - b$ делится и на $m_1$, и на $m_2$, т. е. является общим кратных этих чисел. Но тогда она делится на $\text{НОК}\,(m_1, m_2)$ (этим наименьшее общее кратное и характеризуется).

**13.** Имеем $a = b + mt$ для некоторого целого $t$. Утверждение следует из свойства 8 отношения делимости (см. раздел 1.1).

**14.** Это утверждение является переформулировкой леммы 1.1. □

**Замечание 3.1.** Как видно из доказательства, свойство 12 можно распространить на произвольное количество модулей $m_1, \ldots, m_k$. Если эти модули к тому же попарно взаимно просты, то система сравнений

$$a \equiv b \pmod{m_i}, \quad i = 1, \ldots, k,$$

эквивалентна одному сравнению $a \equiv b \pmod m$, где $m = m_1 \ldots m_k$.

Приведём несколько простых примеров применения техники сравнений.

**Пример 3.1.** Предположим, что целые числа $x$ и $y$ дают при делении на 7 остатки 3 и 2 соответственно. Чему равен остаток от деления числа

$$A = 11x^3y - 5xy^2 + 13$$

на то же число 7?

Поскольку $x \equiv 3 \pmod 7$ и $y \equiv 2 \pmod 7$, имеем (см. свойство 8)

$$A \equiv 11 \cdot 3^3 \cdot 2 - 5 \cdot 3 \cdot 2^2 + 13 \equiv 4 \cdot 3^3 \cdot 2 + 2 \cdot 3 \cdot 2^2 - 1 = 239 \equiv 1 \pmod 7,$$

поэтому остаток будет равен 1.

**Пример 3.2.** Докажем, что число

$$A_n = 5^{2n-1} \cdot 2^{n+1} + 3^{n+1} \cdot 2^{2n-1}$$

при любом натуральном $n$ делится на 19.

Это легко доказывается по индукции, но можно ещё проще:

$$A_n = 50^{n-1} \cdot 20 + 12^{n-1} \cdot 18 \equiv$$
$$\equiv 12^{n-1} \cdot 1 + 12^{n-1} \cdot 18 = 12^{n-1} \cdot 19 \equiv 0 \pmod{19},$$

и утверждение доказано.

**Пример 3.3.** Покажем, что равенство

$$x^3 + y^3 + z^3 = 4 \tag{3.3}$$

невозможно ни при каких целых числах $x$, $y$, $z$.

Заметим, что куб целого числа сравним по модулю 9 с одним из чисел 0 и $\pm 1$. Действительно, если $a = 3q + r$, где $r \in \{0, \pm 1\}$, то

$$a^3 = (3q + r)^3 = 9(3q^3 + 3q^2 r + qr^2) + r^3 \equiv r^3 \pmod{9},$$

при этом имеем $r^3 \in \{0, \pm 1\}$.

Таким образом, сумма трёх кубов будет сравнима по модулю 9 с одним из чисел 0, $\pm 1$, $\pm 2$, $\pm 3$. Но число 4 этим свойством не обладает. Поэтому равенство (3.3) невозможно.

**Замечание 3.2.** *Метод остатков*, которым мы воспользовались в примере 3.3, не всегда эффективен при обосновании невозможности равенств с целыми числами. Так, например, равенство $x^2 - 34y^2 = -1$ невозможно, однако сравнение

$$x^2 - 34y^2 \equiv -1 \pmod{m}$$

при любом $m$ может оказаться верным (оба утверждения нетривиальны).

## 3.2 Классы вычетов. Теоремы Ферма и Эйлера

Понятие класса вычетов по модулю. Полные и приведённые системы вычетов по модулю. Малая теорема Ферма и её различные доказательства. Биномиальная формула по простому модулю. Теорема Эйлера.

Уже было отмечено, что отношение «быть сравнимыми по модулю $m$» является отношением эквивалентности на множестве целых чисел $\mathbb{Z}$. Как следствие, последнее разбивается на классы эквивалентности, которые принято называть классами вычетов по модулю $m$.

**Определение 3.2.** *Классом вычетов* по модулю $m$ с представителем $a \in \mathbb{Z}$ называется множество

$$\{x \in \mathbb{Z} : x \equiv a \pmod m\}.$$

Обозначение: $[a]_m$ или $[a]$ (при этом модуль $m$ должен быть дополнительно указан или ясен из контекста).

Очевидно, любой класс вычетов по модулю $m$ состоит из чисел, попарно сравнимых между собой по модулю $m$ (или, что то же самое, равноостаточных при делении на $m$). Равенство двух классов вычетов

$$[a_1] = [a_2]$$

по модулю $m$ означает сравнимость их представителей: $a_1 \equiv a_2 \pmod m$. Если $r$ — остаток от деления $a$ на модуль $m$, то $[a] = [r]$. Поскольку имеется в точности $m$ различных остатков от деления на $m$ (очевидно, попарно не сравнимых по модулю $m$), то все различные классы вычетов по модулю $m$ таковы:

$$[r] = \{r + mt : t \in \mathbb{Z}\}, \quad r \in \{0, 1, \ldots, m-1\}. \tag{3.4}$$

Множество всех классов вычетов по модулю $m$ обозначим $\mathbb{Z}_m$. Оно содержит, таким образом, $m$ элементов вида (3.4).

**Определение 3.3.** Наименьшее неотрицательное число, содержащееся в данном классе вычетов по модулю $m$, называется *наименьшим неотрицательным вычетом* этого класса. *Абсолютно наименьшим вычетом* называется наименьшее по абсолютной величине число из данного класса вычетов.

Для класса вычетов $[a]$ по модулю $m$ наименьшим неотрицательным вычетом будет $r$ — остаток от деления $a$ на $m$. Абсолютно наименьший вычет этого класса есть

$$\rho = \begin{cases} r & \text{при } r < m/2, \\ -(m-r) & \text{при } r > m/2 \end{cases}$$

(если $m$ чётно и $r = m/2$, то абсолютно наименьший вычет $\rho = \pm m/2$).

**Определение 3.4.** Если из каждого класса вычетов по модулю $m$ взять по одному представителю, то возникнет *полная система вычетов* по модулю $m$.

**Пример 3.4.** Числа $-14, 8, 16, -4, 18, -2, -1$ образуют полную систему вычетов по модулю $m = 7$.

Легко понять, что любая система из $m$ попарно не сравнимых по модулю $m$ чисел будет полной системой вычетов по этому модулю (действительно, эти числа принадлежат разным классам вычетов, а поскольку чисел имеется столько же, сколько и классов вычетов, то среди них найдётся представитель любого класса вычетов по модулю $m$).

Обычно используют *полную систему наименьших неотрицательных вычетов* по модулю $m$, т. е. систему возможных остатков от деления на $m$ (см., например, (3.4)). Однако для вычислений предпочтительнее *полная система абсолютно наименьших вычетов* по модулю $m$.

**Пример 3.5.** Найдем возможные остатки от деления квадратов целых чисел на $m = 7$.

Очевидно, достаточно найти остатки от деления на 7 чисел вида $\rho^2$, где $\rho$ пробегает полную систему абсолютно наименьших вычетов по модулю 7, т. е. $\rho \in \{0, \pm1, \pm2, \pm3\}$. Эти остатки таковы: 0, 1, 2, 4.

Часто бывает полезным следующее свойство полных систем вычетов по модулю $m$.

**Теорема 3.2.** Пусть $a,\ b \in \mathbb{Z}$, при этом НОД $(a, m) = 1$. Если $x$ пробегает полную систему вычетов по модулю $m$, то

$$y = ax + b$$

также пробегает полную систему вычетов по модулю $m$.

Доказательство. Заметим, что если $x_1 \not\equiv x_2 \pmod m$, то

$$y_1 = ax_1 + b \not\equiv ax_2 + b = y_2 \pmod m.$$

Действительно, иначе мы получили бы сравнение

$$ax_1 \equiv ax_2 \pmod m,$$

которое после сокращения на $a$ (корректного ввиду свойства 4 сравнений, см. раздел 3.1) привело бы к сравнению $x_1 \equiv x_2 \pmod m$. □

Теорема 3.2 позволяет дать более конструктивное доказательство китайской теоремы об остатках (см. теорему 1.9).

Пусть $m = m_1 m_2$, где НОД $(m_1, m_2) = 1$. Представим полную систему наименьших неотрицательных вычетов по модулю $m$ в виде таблицы чисел

$$r(i, j) = m_2 i + j \quad (i = 0,\ 1,\ \ldots,\ m_1 - 1;\ j = 0,\ 1,\ \ldots,\ m_2 - 1), \tag{3.5}$$

состоящей из $m_1$ строк и $m_2$ столбцов. Утверждение китайской теоремы об остатках теперь вытекает из следующих свойств этой таблицы:

(а) каждая строка таблицы — полная система вычетов по модулю $m_2$ (это очевидно);

(б) каждый столбец таблицы — полная система вычетов по модулю $m_1$ (следует из теоремы 3.2).

Действительно, число $r$ необходимо искать в столбце с номером $j = r_2$. Среди чисел этого столбца одно (и ровно одно) будет давать при делении на $m_1$ заданный остаток $r_1$.

**Упражнение 3.3.** Пусть НОД $(m_1, m_2) = 1$ и $m = m_1 m_2$. Докажите, что числа

$$x = m_2 x^{(1)} + m_1 x^{(2)},$$

где $x^{(1)}$ пробегает полную систему вычетов по модулю $m_1$, а $x^{(2)}$ — полную систему вычетов по модулю $m_2$, образуют полную систему вычетов по модулю $m$.

*Указание.* Эти числа попарно не сравнимы по модулю $m$.

Из свойства 13 сравнений (см. раздел 3.1) следует, что все числа некоторого класса вычетов по модулю $m$ либо все взаимно просты с $m$, либо все имеют с $m$ один и тот же общий нетривиальный делитель $d$. Это замечание делает корректным следующее

**Определение 3.5.** Класс вычетов $[a]$ по модулю $m$ называется *взаимно простым с модулем*, если НОД $(a, m) = 1$.

Поскольку $[a] = [r]$, где $r \in \{0, 1, \ldots, m-1\}$, количество всех взаимно простых с модулем классов вычетов равно $\varphi(m)$ — значению функции Эйлера от модуля $m$. Их множество будем обозначать $\mathbb{Z}_m^*$.

**Пример 3.6.** Имеем $\mathbb{Z}_{12}^* = \{[1], [5], [7], [11]\}$.

**Определение 3.6.** Если из каждого класса вычетов по модулю $m$, взаимно простого с $m$, взять по представителю, то возникнет *приведённая система вычетов* по модулю $m$.

**Пример 3.7.** Числа $-11$, 17, 19, 23 образуют приведённую систему вычетов по модулю $m = 12$.

Ясно, что приведённую систему вычетов по модулю $m$ образует любая система из $\varphi(m)$ попарно не сравнимых по модулю $m$ и взаимно простых с ним чисел.

**Упражнение 3.4.** Анализируя таблицу чисел (3.5), ещё раз установите свойство мультипликативности функции Эйлера.

*Решение.* Число $r(i, j)$ взаимно просто с $m = m_1 m_2$ тогда и только тогда, когда оно взаимно просто как с $m_1$, так и с $m_2$. Поэтому все числа таблицы, взаимно простые с $m$, находятся в столбцах, номера $j$ которых взаимно просты с $m_2$ (таких столбцов — $\varphi(m_2)$ штук). В каждом таком столбце, представляющем собой полную систему вычетов по модулю $m_1$, есть в точности $\varphi(m_1)$ чисел, взаимно простых с $m_1$. Следовательно, всего в таблице имеется $\varphi(m_2) \cdot \varphi(m_1)$ чисел $r(i, j)$, взаимно простых с $m$, т. е.

$$\varphi(m) = \varphi(m_1)\varphi(m_2).$$

Вот как всё это выглядит, например, при $m_1 = 4$, $m_2 = 9$:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 0 | **1** | 2 | 3 | 4 | **5** | 6 | **7** | 8 |
| 9 | 10 | **11** | 12 | **13** | 14 | 15 | 16 | **17** |
| 18 | **19** | 20 | 21 | 22 | **23** | 24 | **25** | 26 |
| 27 | 28 | **29** | 30 | **31** | 32 | 33 | 34 | **35** |

(3.6)

Отмеченные в этой таблице числа составляют приведённую систему наименьших неотрицательных вычетов по модулю $m = m_1 m_2 = 36$. □

**Упражнение 3.5.** Если в формулировке упражнения 3.3 всюду слово «полную» заменить на слово «приведённую», то получится новое верное утверждение. Докажите его и попутно установите мультипликативность функции Эйлера.

**1.** При $m_1 = 4$, $m_2 = 9$ первое доказательство мультипликативности функции Эйлера (см. доказательство теоремы 1.13) можно проиллюстрировать таблицей

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 0 | 28 | 20 | 12 | 4 | 32 | 24 | 16 | 8 |
| 9 | [1] | [29] | 21 | [13] | [5] | 33 | [25] | [17] |
| 18 | 10 | 2 | 30 | 22 | 14 | 6 | 34 | 26 |
| 27 | [19] | [11] | 3 | [31] | [23] | 15 | [7] | [35] |

(3.7)

а последнее доказательство — таблицей

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 0 | 4 | 8 | 12 | 16 | 20 | 24 | 28 | 32 |
| 9 | [13] | [17] | 21 | [25] | [29] | 33 | [1] | [5] |
| 18 | 22 | 26 | 30 | 34 | 2 | 6 | 10 | 14 |
| 27 | [31] | [35] | 3 | [7] | [11] | 15 | [19] | [23] |

(3.8)

Видно, что эти доказательства почти одинаковы (таблицы (3.7) и (3.8) получаются одна из другой перестановкой столбцов, хотя в более общей ситуации потребовалась бы ещё и перестановка строк), но существенно отличаются от предпоследнего (см. таблицу (3.6)).

**2.** Пусть $\zeta = \cos 2\pi/m + i \sin 2\pi/m$ — *первообразный корень из единицы* степени $m$. Вычислим сумму

$$S(m) = \sum_x \zeta^x,$$

где $x$ пробегает приведённую систему вычетов по модулю $m$. Это нетрудно сделать, если, используя упражнение 3.5, предварительно установить мультипликативность функции $S(m)$.

Действительно, если $m = m_1 m_2$, где НОД $(m_1, m_2) = 1$, то

$$S(m) = \sum_{x^{(1)}, x^{(2)}} \zeta^{m_2 x^{(1)} + m_1 x^{(2)}} = \sum_{x^{(1)}, x^{(2)}} \zeta_1^{x^{(1)}} \zeta_2^{x^{(2)}} = \sum_{x^{(1)}} \zeta_1^{x^{(1)}} \sum_{x^{(2)}} \zeta_2^{x^{(2)}} = S(m_1) S(m_2)$$

($\zeta_1 = \zeta^{m_2}$ и $\zeta_2 = \zeta^{m_1}$ — первообразные корни из единицы степени $m_1$ и $m_2$ соответственно). Прямое вычисление показывает, что

$$S(p^\alpha) = \begin{cases} -1, & \text{если } \alpha = 1, \\ 0, & \text{если } \alpha > 1 \end{cases}$$

(здесь $p$ — простое, а $\alpha$ — натуральное число). Но тогда $S(m)$ совпадает с функцией Мёбиуса $\mu(m)$ (см. определение 1.13).

**Теорема 3.3.** Пусть НОД $(a, m) = 1$. Если $x$ пробегает приведённую систему вычетов по модулю $m$, то

$$y = ax$$

также пробегает приведённую систему вычетов по модулю $m$.

Доказательство. Единственное отличие от доказательства аналогичной теоремы 3.2 состоит в том, что нужно предварительно заметить следующее: если $x$ взаимно просто с $m$, то $y = ax$ также взаимно просто с $m$ (это свойство 4 взаимно простых чисел, см. раздел 1.2). □

**Упражнение 3.6.** Дайте подробное доказательство теоремы 3.3.

Рассмотрим случай, когда $m = p$ — простое число. Поскольку

$$\varphi(p) = p - 1,$$

теорема 3.3 в этом случае приводит к следующему: если число $a$ не делится на $p$, то числа

$$a,\ 2a,\ \ldots,\ (p-1)a$$

образуют приведённую систему вычетов по модулю $p$. Это значит, что после замены этих чисел их остатками от деления на $p$ мы получим перестановку чисел $1, 2, \ldots, p-1$. Тогда

$$a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}. \tag{3.9}$$

Сократив обе части этого сравнения на $(p-1)!$, приходим к следующей теореме.

**Теорема 3.4.** Если $p$ — простое число, то для любого целого числа $a \not\equiv 0 \pmod{p}$ справедливо сравнение

$$a^{p-1} \equiv 1 \pmod{p}. \tag{3.10}$$

Эту теорему доказал в 1640 году П. Ферма (1601 — 1665). Теперь она известна как *малая теорема Ферма*.

**Упражнение 3.7.** Обоснуйте сокращение обеих частей сравнения (3.9) на $(p-1)!$.

Термин «малая теорема» можно объяснить тем, что есть так называемая «большая теорема» Ферма, которую мы здесь обсуждать не будем. Ввиду важности малой теоремы Ферма мы дадим ещё одно

Доказательство. Точнее, мы докажем её в альтернативной форме: для любого простого числа $p$ и любого целого числа $a$ верно сравнение

$$a^p \equiv a \pmod{p}. \tag{3.11}$$

Ясно, что для чисел $a \not\equiv 0 \pmod{p}$ сравнения (3.10) и (3.11) эквивалентны.

Сравнение (3.11) будем доказывать индукцией по натуральным $a$ (очевидно, достаточно рассмотреть только эти значения $a$). Шаг индукции:

$$(a+1)^p = a^p + \sum_{k=1}^{p-1} C_p^k a^k + 1 \equiv a + 1 \pmod{p},$$

поскольку при любом $k = 1, \ldots, p-1$ имеем $C_p^k \equiv 0 \pmod{p}$. □

**Упражнение 3.8.** Докажите последнее утверждение.

*Указание.* Число $k!C_p^k = p(p-1)\ldots(p-k+1)$ делится на $p$.

**Следствие 3.1.** Если $p$ — простое число, то для любых целых чисел $a$ и $b$ выполняется сравнение

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Доказательство. $(a+b)^p \equiv a + b \equiv a^p + b^p \pmod{p}$. □

**Замечание 3.3.** В некотрой западной учебно-методической литературе по элементарной теории чисел это следствие (эквивалентное, кстати, самой малой теореме Ферма) встречается под говорящим названием *Idiot's Binomial Theorem*. В наиболее общем виде оно выглядит как

$$(a_1 + a_2 + \ldots + a_k)^p \equiv a_1^p + a_2^p + \ldots + a_k^p \pmod{p}$$

и называется, естественно, *Idiot's Polynomial Theorem*.

**Упражнение 3.9.** Докажите, что для произвольного целого $a$ все нечётные простые делители числа $a^2 + 1$ имеют вид $4k + 1$.

*Решение.* Пусть $p$ — нечётный простой делитель этого числа, т. е.

$$a^2 + 1 \equiv 0 \pmod{p}.$$

Тогда

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

Учитывая сравнение (3.10), имеем $1 \equiv (-1)^{(p-1)/2} \pmod{p}$. Отсюда следует, что $(p-1)/2$ — чётное число, $(p-1)/2 = 2k$, откуда $p = 4k + 1$. □

В 1736 году Эйлер распространил малую теорему Ферма с простого модуля $p$ на произвольный модуль $m$. Следующая теорема известна как *теорема Эйлера*.

**Теорема 3.5.** Если НОД $(a, m) = 1$, то

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{3.12}$$

Доказательство. Пусть $x_1, x_2, \ldots, x_k$ — некоторая приведённая система вычестов по модулю $m$, где $k = \varphi(m)$. После умножения на $a$ получим другую приведённую систему вычетов $ax_1, ax_2, \ldots, ax_k$ по модулю $m$ (теорема 3.3). Как и выше, имеет место сравнение

$$ax_1 \cdot ax_2 \cdot \ldots \cdot ax_k \equiv x_1 \cdot x_2 \cdot \ldots \cdot x_k \pmod{m}.$$

После сокращения на произведение $x_1 x_2 \ldots x_k$, которое взаимно просто с $m$, получим сравнение (3.12). □

**Упражнение 3.10.** Докажите, что если $m$ не является степенью двойки и не делится на три, то

$$x_1^2 + x_2^2 + \ldots + x_k^2 \equiv 0 \pmod{m},$$

где $x_1, x_2, \ldots, x_k$ — приведённая система вычетов по модулю $m$.

*Решение.* Пусть $S = x_1^2 + x_2^2 + \ldots + x_k^2$. При нечётном $m$ имеем

$$4S = (2x_1)^2 + (2x_2)^2 + \ldots + (2x_k)^2 \equiv S \pmod{m}$$

и, таким образом, $S \equiv 0 \pmod{m}$. Случай чётного $m$ можно свести к случаю нечётного. □

**Упражнение 3.11.** Выведите теорему Эйлера из малой теоремы Ферма.

*Решение.* Пусть $p$ — любой простой делитель числа $m$. Тогда $a^{p-1} \equiv 1 \pmod{p}$. Докажем индукцией по $\alpha \geqslant 1$ сравнение

$$a^{p^{\alpha-1}(p-1)} \equiv 1 \pmod{p^\alpha}. \tag{3.13}$$

Сделаем шаг индукции. Положим $A = a^{p^{\alpha-1}(p-1)}$, тогда

$$a^{p^\alpha(p-1)} - 1 = A^p - 1 = (A-1)(A^{p-1} + A^{p-2} + \ldots + 1).$$

По предположению индукции $A \equiv 1 \pmod{p^\alpha}$. В частности, выполняется сравнение $A \equiv 1 \pmod{p}$, откуда находим

$$A^{p-1} + A^{p-2} + \ldots + 1 \equiv p \equiv 0 \pmod{p}.$$

Значит, $A^p - 1$ делится на $p^\alpha \cdot p = p^{\alpha+1}$, и шаг индукции сделан.

Таким образом, если $m = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$ — каноническое разложение числа $m$, то имеют место сравнения

$$a^{p_i^{\alpha_i-1}(p_i-1)} \equiv 1 \pmod{p_i^{\alpha_i}}, \quad i = 1, \ldots, t.$$

Теперь формула (3.12) вытекает из свойств сравнений и формулы для вычисления значений функции Эйлера $\varphi(m)$ (см. раздел 1.5). □

При $p = 2$ и $\alpha \geqslant 3$ сравнение (3.13) можно заменить более точным сравнением

$$a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$$

(благодаря тому, что при нечётном $a$ число $a^2 - 1$ делится не только на 4, но и на 8). Пусть

$$\lambda(p^\alpha) = p^{\alpha-1}(p-1)$$

для любого нечётного простого $p$ и $\alpha \geqslant 1$, а также

$$\lambda(2^\alpha) = \begin{cases} 2^{\alpha-1}, & \text{если } \alpha \in \{1, 2\}, \\ 2^{\alpha-2}, & \text{если } \alpha \geqslant 3. \end{cases}$$

Для произвольного натурального $m = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$ положим

$$\lambda(m) = \text{НОК}\,(\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_t^{\alpha_t})).$$

Функция $\lambda(m)$ называется *функцией Кармайкла*. Если НОД $(a, m) = 1$, то, как можно доказать (см. решение упражнения 3.11), имеет место сравнение

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

(это утверждение называется *теоремой Кармайкла*). Легко видеть, что всегда $\lambda(m) \mid \varphi(m)$ и, в частности, $\lambda(m) \leqslant \varphi(m)$. Можно показать, что равенство

$$\lambda(m) = \varphi(m)$$

имеет место только для $m = 2,\ 4,\ p^\alpha,\ 2p^\alpha$, где $p$ — нечётное простое число и $\alpha \geqslant 1$.

С помощью теорем Эйлера и Ферма можно понижать показатель степени при её вычислении по какому-нибудь модулю. А именно, пусть требуется найти остаток от деления числа $a^N$ на $m$, при этом показатель $N$ достаточно велик. Считая $a$ взаимно простым с $m$, представим $N$ в виде

$$N = \varphi(m)t + r, \quad 0 \leqslant r < \varphi(m).$$

Тогда

$$a^N = (a^{\varphi(m)})^t \cdot a^r \equiv a^r \pmod{m}.$$

Таким образом, показатель $N$ можно заменить его остатком $r$ от деления на $\varphi(m)$, который может оказаться не очень большим.

Для иллюстрации сказанного рассмотрим

**Пример 3.8.** Каковы три последние цифры числа $A = 1003^{2008}$?

Здесь нужно найти остаток от деления $A$ на 1000. Имеем

$$\varphi(1000) = 1000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 400.$$

Следовательно,

$$A \equiv 3^{2008} \equiv 3^8 = 6561 \equiv 561 \pmod{1000}.$$

Итак, $A = \ldots 561$.

Впрочем, в роли функции Эйлера $\varphi(m)$ иногда удобнее использовать функцию Кармайкла $\lambda(m)$, которая принимает, вообще говоря, меньшие значения.

**Упражнение 3.12.** Докажите, что 101-я степень нечётного и не кратного пяти числа оканчивается теми же тремя цифрами, что и само число.

*Указание.* $\lambda(1000) = 100$.

**Упражнение 3.13.** Пусть

$$A_1 = 2017, \quad A_{k+1} = 2017^{A_k} \quad (k = 1, 2, \ldots).$$

С помощью компьютера найдите последние $n = 50$ цифр числа $A_{2017}$.

*Указание.* Положим

$$m_0 = 10^n, \quad m_{k+1} = \lambda(m_k) \quad (k = 0, 1, \ldots, n).$$

Покажите, что $m_{n+1} = 2$. Пусть $B_k$ — наименьший неотрицательный вычет числа $A_{2017-k}$ по модулю $m_k$. Тогда $B_{n+1} = 1$ при $n \leqslant 2015$. Докажите сравнения

$$B_k \equiv 2017^{B_{k+1}} \pmod{m_k}, \quad k = 0, 1, \ldots, n.$$

*Ответ.* $A_{2017} = \ldots 12158089680652227004090466938614680363887450999777$.

Отметим также, что малая теорема Ферма лежит в основе многих *тестов псевдопростоты*, позволяющих определять составной характер числа, а теорема Эйлера находит применение в криптографии (см. раздел 5).

## 3.3 Сравнения с неизвестными

Сравнения с неизвестными. Переборный алгоритм решения сравнений с неизвестными. Сравнения с одним неизвестным по простому модулю. Понижение степени сравнения. Теорема о числе решений. Теорема Вильсона.

В этом разделе рассматриваются сравнения по модулю, содержащие неизвестные величины. Такие сравнения являются теоретико-числовым аналогом алгебраических уравнений.

**Определение 3.7.** Пусть $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$. Выражение вида

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{m} \tag{3.14}$$

называется *сравнением по модулю с неизвестными*.

Как и алгебраическое уравнение, сравнение с неизвестными вида (3.14) надо решать, т. е. находить все наборы $(a_1, \ldots, a_n)$ целочисленных значений неизвестных, ему удовлетворяющих.

Ввиду свойства 7 сравнений (см. раздел 3.1) можно понимать под *решением* сравнения (3.14) соответствующий набор $([a_1], \ldots, [a_n])$ классов вычетов по модулю $m$. Поскольку количество таких наборов равно $m^n$, любое сравнение по модулю $m$ с $n$ неизвестными имеет не более $m^n$ решений, и все они в принципе могут быть найдены полным перебором.

**Пример 3.9.** В примере 3.3 фактически речь шла о том, что сравнение

$$x^3 + y^3 + z^3 \equiv 4 \pmod{9}$$

не имеет решений.

В этом действительно можно убедиться, перебрав все $9^3 = 729$ тройки $([r_1], [r_2], [r_3])$, где $r_i$ независимо друг от друга пробегают полную систему вычетов по модулю 9, и отвергнув каждую из них.

Уже этот простой пример показывает, что при решении сравнения (3.14) алгоритм полного перебора не может быть практичным. Однако можно слегка уменьшить объем вычислительной работы, если предварительно редуцировать коэффициенты многочлена $f(x_1, \ldots, x_n)$, т. е. заменить их остатками от деления на $m$. Как следует из свойства 8 сравнений (см. раздел 3.1), это приведёт к *равносильному сравнению* (имеющему те же решения, что и исходное).

Если $m = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$ — каноническое разложение модуля $m$, то сравнение (3.14) эквивалентно системе сравнений

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p_i^{\alpha_i}}, \quad i = 1, \ldots, t. \tag{3.15}$$

Предположим, что мы решили каждое из них. Тогда с помощью китайской теоремы об остатках мы сможем покомпонентно «склеить» (см. пример 3.10) из полученных решений все решения сравнения (3.14). Всего при этом получится

$$N = N_1 \ldots N_t$$

решений, где $N_i$ — число решений $i$-го сравнения (3.15).

**Пример 3.10.** Решим сравнение $x^2 - y^4 + 1 \equiv 0 \pmod{36}$.
Сравнение $x^2 - y^4 + 1 \equiv 0 \pmod 4$ имеет четыре решения:

$$([0]_4, [1]_4),\ ([0]_4, [3]_4),\ \boxed{([2]_4, [1]_4)},\ ([2]_4, [3]_4),$$

а сравнение $x^2 - y^4 + 1 \equiv 0 \pmod 9$ — шесть решений:

$$([0]_9, [1]_9),\ ([0]_9, [8]_9),\ ([3]_9, [1]_9),\ \boxed{([3]_9, [8]_9)},\ ([6]_9, [1]_9),\ ([6]_9, [8]_9).$$

Глядя на таблицу (3.7), мы увидим, к примеру, что решение $([2]_4, [1]_4)$ и решение $([3]_9, [8]_9)$ приведут к решению $([30]_{36}, [17]_{36})$. Таким способом получаются все $4 \cdot 6 = 24$ решения исходного сравнения.

Итак, общая задача решения сравнения (3.14) сводится к случаю, когда модуль $m$ есть степень простого числа. Далее мы ограничимся изучением только сравнений с одним неизвестным, более того, будем пока считать, что $m = p$ — простое число.

Пусть дано сравнение

$$f(x) \equiv 0 \pmod p, \tag{3.16}$$

где $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$, $\deg f(x) = n$.

**Определение 3.8.** *Степенью* сравнения (3.16) называется наибольший индекс $k$, для которого $a_k \not\equiv 0 \pmod p$.

После редукции коэффициентов вполне может оказаться, что степень сравнения (3.16) меньше, чем $n$. Ещё один способ понизить степень сравнения предоставляет следующая

**Теорема 3.6.** Любое сравнение (3.16) равносильно некоторому сравнению степени не выше $p - 1$.

Доказательство. Используя процедуру «деления уголком», разделим с остатком многочлен $f(x)$ на многочлен $x^p - x$:

$$f(x) = (x^p - x)q(x) + r(x),$$

где $q(x)$, $r(x)$ — многочлены с целыми коэффициентами и $\deg r(x) \leqslant p - 1$. Применив малую теорему Ферма, получим

$$f(a) \equiv r(a) \pmod p$$

для любого $a \in \mathbb{Z}$, поэтому сравнение (3.16) равносильно сравнению

$$r(x) \equiv 0 \pmod p. \tag{3.17}$$

Ясно, что степень этого сравнения не выше $p - 1$. □

Очевидно, редукция по степени, состоящая в замене сравнения (3.16) сравнением (3.17), имеет практический смысл только при $n \geqslant p$.

**Теорема 3.7.** Число решений сравнения (3.16) не превосходит его степени.

Доказательство. Пусть степень сравнения (3.16) равна $n$, так что $a_n \not\equiv 0 \pmod{p}$.

Предположим противное: пусть $x_1, \ldots, x_n, x_{n+1}$ — представители различных классов вычетов по модулю $p$, являющихся решениями сравнения (3.16). Воспользуемся *интерполяционной формулой Ньютона*:

$$f(x) = b_n(x - x_1)\ldots(x - x_n)(x - x_{n+1}) + b_{n-1}(x - x_1)\ldots(x - x_n) + \\ + \ldots + b_1(x - x_1) + b_0,$$

в которой все коэффициенты $b_i$ — целые числа. Подставляя сюда вместо $x$ последовательно $x_1, \ldots, x_n$, обнаружим, что эти коэффициенты кратны $p$, включая и старший $b_n = a_n$.

Но это противоречит тому, что сравнение (3.16) имеет степень $n$. □

**Упражнение 3.14.** Объясните, почему: а) все коэффициенты $b_i$ — целые числа; б) все $b_i \equiv 0 \pmod{p}$.

Одним из следствий теоремы 3.7 является следующая *теорема Вильсона*.

**Теорема 3.8.** Если $p$ — простое число, то

$$(p - 1)! + 1 \equiv 0 \pmod{p}. \tag{3.18}$$

Доказательство. При $p > 2$ рассмотрим многочлен

$$f_0(x) = (x - 1)(x - 2)\ldots(x - p + 1) - (x^{p-1} - 1)$$

и соответствующее сравнение

$$f_0(x) \equiv 0 \pmod{p}.$$

Как следует из малой теоремы Ферма, все ненулевые классы вычетов по модулю $p$ будут решениями этого сравнения. Следовательно, имеется по крайней мере $p - 1$ решений. Однако $\deg f_0(x) < p - 1$, поэтому все коэффициенты многочлена $f_0(x)$ должны быть кратны $p$, в том числе и свободный коэффициент, равный $(p - 1)! + 1$. □

**Замечание 3.4.** Первое доказательство теоремы Вильсона дал в 1771 году Ж. Лагранж (1736 — 1813).

**Упражнение 3.15.** Докажите, что если натуральное число $p > 1$ удовлетворяет сравнению (3.18), то $p$ — простое число.

Таким образом, сравнение (3.18) является *критерием простоты* числа $p$. Этот критерий, однако, непрактичен при больших $p$, поскольку неизвестны быстрые способы вычисления $(p - 1)!$ по модулю $p$.

Возвращаясь к общему случаю (когда модуль сравнения есть степень простого числа), отметим, что при любом $\alpha > 1$ решение сравнения

$$f(x) \equiv 0 \pmod{p^\alpha}$$

можно свести к задаче решения сравнения (3.16). Соответствующий метод основан на так называемой *лемме Гензеля о подъёме* и напоминает *метод Ньютона* приближённого решения уравнений (подробнее см., например, в книге [1, гл. 16]). Приведём один конкретный

**Пример 3.11.** Пусть требуется решить сравнение

$$x^4 + 5x^3 - x^2 - 2 \equiv 0 \pmod{125}. \tag{3.19}$$

Очевидно, любое решение этого сравнения (как целое число, ему удовлетворяющее) будет решением каждого из сравнений

$$\begin{aligned} x^4 + 5x^3 - x^2 - 2 &\equiv 0 \pmod{25}, \\ x^4 + 5x^3 - x^2 - 2 &\equiv 0 \pmod{5}. \end{aligned} \tag{3.20}$$

Последнее сравнение, как легко видеть, имеет два решения:

$$\boxed{[2]_5 = \{2 + 5t_1 : t_1 \in \mathbb{Z}\}}, \quad [3]_5 = \{3 + 5t_1 : t_1 \in \mathbb{Z}\}.$$

Каждое из этих решений мы можем последовательно «поднять» до некоторых решений исходного сравнения (3.19). Покажем, как это делается, на примере первого решения $[2]_5$.

Подставим $x = 2 + 5t_1$ в сравнение (3.20):

$$(2 + 5t_1)^4 + 5(2 + 5t_1)^3 - (2 + 5t_1)^2 - 2 \equiv 0 \pmod{25}.$$

После редукции коэффициентов получим

$$15t_1 \equiv 0 \pmod{25}.$$

Сократив на 5 и решив получившееся сравнение, найдём

$$t_1 \equiv 0 \pmod{5},$$

т. е. $t_1 = 5t_2$, где $t_2 \in \mathbb{Z}$.

Теперь подставим $x = 2 + 5t_1 = 2 + 25t_2$ в сравнение (3.19):

$$(2 + 25t_2)^4 + 5(2 + 25t_2)^3 - (2 + 25t_2)^2 - 2 \equiv 0 \pmod{125}.$$

Редуцируя коэффициенты, получим

$$50 + 75t_2 \equiv 0 \pmod{125}.$$

Сократив на 25 и решив, найдём

$$t_2 \equiv 1 \pmod{5},$$

т. е. $t_2 = 1 + 5t_3$, где $t_3 \in \mathbb{Z}$.

Итак, $x = 2 + 25t_2 = 27 + 125t_3$, т. е. $[27]_{125}$ — одно из решений сравнения (3.19). Исходя из второго решения $[3]_5$, аналогичным образом можно найти ещё одно решение сравнения (3.19) — это $[13]_{125}$. Других решений, кроме указанных, не будет.

**Замечание 3.5.** Обратим внимание на два важных обстоятельства, имевших место в рассмотренном примере. Во-первых, «подъём на следующий этаж» каждый раз был однозначным. Во-вторых, всё, что было «внизу», удалось «поднять» на «самый верх». Так будет всегда, если для любого решения $[r]$ сравнения (3.16) выполняется условие

$$f'(r) \not\equiv 0 \pmod{p}.$$

При его нарушении как первое, так и второе обстоятельство в общем случае нельзя гарантировать.

В заключение приведём один результат о сравнениях по простому модулю с несколькими неизвестными.

**Теорема 3.9.** Пусть $\deg f(x_1, \ldots, x_n) < n$. Тогда число решений сравнения

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p} \tag{3.21}$$

кратно $p$.

Эта теорема носит название *теоремы Варнинга*. Предварительно докажем лемму, представляющую и самостоятельный интерес.

**Лемма 3.1.** Если $0 \leqslant k < p-1$, то

$$\sum r^k \equiv 0 \pmod{p},$$

где $r$ пробегает полную систему вычетов по модулю $p$.

Доказательство. Можно считать $k > 0$. Заметим, что найдётся такое не кратное $p$ число $a$, что $a^k \not\equiv 1 \pmod{p}$. Действительно, в противном случае сравнение

$$x^k - 1 \equiv 0 \pmod{p}$$

имело бы $p - 1 > k$ решений, что невозможно по теореме 3.7. Имеем

$$\sum (ar)^k \equiv \sum r^k \pmod{p},$$

откуда выводим

$$(a^k - 1) \sum r^k \equiv 0 \pmod{p}.$$

Сократив на $a^k - 1$, получим то, что требуется. □

Другое доказательство леммы 3.1 будет дано в разделе 4.4 (см. пример 4.13).

Доказательство теоремы 3.9. Пусть $F(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)^{p-1}$. Рассмотрим сумму

$$S = \sum F(r_1, \ldots, r_n),$$

в которой $r_i$ независимо друг от друга пробегают полную систему вычетов по модулю $p$. Заметим, что степень любого одночлена, входящего в многочлен $F(x_1, \ldots, x_n)$, меньше $n(p-1)$, поэтому хотя бы у одной из $n$ переменных в этом одночлене показатель будет меньше $p - 1$. Применив лемму 3.1, теперь нетрудно обнаружить, что $S \equiv 0 \pmod{p}$.

Но, с другой стороны, $S \equiv p^n - N \pmod{p}$, где $N$ — число решений сравнения (3.21). Действительно, если $([r_1], \ldots, [r_n])$ не является решением этого сравнения, то

$$F(r_1, \ldots, r_n) = f(r_1, \ldots, r_n)^{p-1} \equiv 1 \pmod{p},$$

а если является, то $F(r_1, \ldots, r_n) \equiv 0 \pmod{p}$.

Утверждение теоремы вытекает из двух полученных сравнений для $S$. □

**Следствие 3.2.** Если $\deg f(x_1, \ldots, x_n) < n$ и многочлен $f(x_1, \ldots, x_n)$ имеет нулевой свободный коэффициент, то сравнение (3.21) нетривиально разрешимо.

Утверждение следствия известно как *теорема Шевалле*. Нетривиальная разрешимость сравнения (3.21) означает наличие у него решения $([r_1], \ldots, [r_n]) \neq ([0], \ldots, [0])$.

**Пример 3.12.** Для любых целых коэффициентов $a$, $b$, $c$ существуют целые числа $x$, $y$, $z$, не все кратные $p$ и такие, что $ax^2 + by^2 + cz^2$ делится на $p$.

## 3.4 Сравнения первой степени

Сравнения первой степени с одним и многими неизвестными. Алгоритм Евклида для решения сравнений первой степени. Диофантовы уравнения первой степени.

Для некоторых типов сравнений с неизвестными существуют простые и эффективные на практике методы решения. Таковы, в первую очередь, сравнения первой степени.

**Определение 3.9.** Сравнение с неизвестными (3.14) называют *сравнением первой степени* (или *линейным сравнением*), если

$$f(x_1, \ldots, x_n) = a_1x_1 + \ldots + a_nx_n + b,$$

причём среди коэффициентов $a_i$ найдётся не кратный $m$.

Мы подробно рассмотрим случай одного неизвестного, а также покажем, как к нему можно свести случай многих неизвестных. Любое сравнение первой степени с одним неизвестным записывается в виде

$$ax \equiv b \pmod{m}, \tag{3.22}$$

где $a \not\equiv 0 \pmod{m}$.

Пусть сначала

$$\text{НОД}\,(a, m) = 1.$$

Тогда сравнение (3.22) имеет в точности одно решение $[r_0]$. Это следует, например, из свойства полных систем вычетов по модулю $m$, указанного в теореме 3.2. Более того, для представителя $r_0$ этого единственного решения можно даже дать явную формулу:

$$r_0 = a^{\varphi(m)-1}b.$$

Корректность этой формулы гарантирует теорема Эйлера:

$$ar_0 = a^{\varphi(m)}b \equiv 1 \cdot b = b \pmod{m}.$$

Однако этой формулой для $r_0$ почти не пользуются на практике. И дело здесь не в том, что степень $a^{\varphi(m)-1}$ может оказаться очень большим числом — его и не нужно находить, нужен лишь остаток от деления на $m$, вычислить который можно сравнительно легко (см. раздел 5.1). Главная причина кроется в том, что показатель этой степени содержит значение функции Эйлера $\varphi(m)$ — величину, которую, вообще говоря, трудно найти.

Правильный с практической точки зрения способ найти $r_0$ основан на алгоритме Евклида и состоит в следующем. Сначала с помощью алгоритма Евклида находим линейное представление $1 = \text{НОД}\,(a, m)$ (см. теорему 1.4, а также пример 1.3):

$$1 = ax_0 + my_0,$$

где $x_0,\ y_0 \in \mathbb{Z}$, после чего полагаем $r_0 = bx_0$. Вот проверка:

$$ar_0 = abx_0 = b - mb_0y_0 \equiv b \pmod{m}.$$

**Пример 3.13.** Решим сравнение $127x \equiv 13 \pmod{257}$.

Алгоритм Евклида даёт $\text{НОД}\,(127, 257) = 1$, а также равенство

$$1 = 127 \cdot 85 + 257 \cdot (-42).$$

Тогда $r = 13 \cdot 85 = 1105 \equiv 77 \pmod{257}$. Итак, решением будет класс вычетов $[77]$.

Рассмотрим теперь случай, когда

$$\text{НОД}\,(a, m) = d > 1.$$

В этом случае сравнение (3.22) уже может не иметь решений. Действительно, необходимым условием разрешимости является делимость $b$ на $d$, которой может и не быть.

Если $b$ всё-таки делится на $d$, то разделим все части сравнения (3.22), включая и модуль, на $d$. Тогда

$$a_1 x \equiv b_1 \pmod{m_1}, \tag{3.23}$$

где $a_1 = a/d$, $b_1 = b/d$ и $m_1 = m/d$, при этом $\text{НОД}\,(a_1, m_1) = 1$.

Из сказанного выше следует, что сравнение (3.23) имеет единственное решение, понимаемое как класс вычетов $[r_0]_{m_1}$ по модулю $m_1$. Но всякий класс вычетов по модулю $m_1$ можно представить как объединение $d$ классов вычетов по модулю $m = dm_1$:

$$[r_0]_{m_1} = \bigcup_{j=0}^{d-1} [r_0 + jm_1]_m.$$

Таким образом, в рассматриваемой ситуации сравнение (3.22) будет иметь в точности $d$ решений: это классы вычетов

$$[r_0 + jm_1]_m, \quad j = 0,\ 1,\ \ldots,\ d-1.$$

При этом если

$$d = ax_0 + my_0, \tag{3.24}$$

где $x_0,\ y_0 \in \mathbb{Z}$, то можно взять $r_0 = bx_0/d$.

**Пример 3.14.** Решим сравнение $345x \equiv 39 \pmod{597}$.

Из алгоритма Евклида следует, что

$$\text{НОД}\,(345, 597) = 3 = 345 \cdot 45 + 597 \cdot (-26).$$

Поскольку 39 кратно 3, сравнение разрешимо и имеет 3 решения. Сократив на 3, получим сравнение

$$115x \equiv 13 \pmod{199},$$

единственное решение которого есть $[13 \cdot 45]_{199} = [-12]_{199}$. Следовательно, решениями исходного сравнения будут $[-12]_{597}$, $[187]_{597}$, $[386]_{597}$.

Итак, доказана следующая

**Теорема 3.10.** Пусть $d = \text{НОД}\,(a, m)$. Если $b$ не делится на $d$, то сравнение (3.22) неразрешимо. В противном случае это сравнение имеет $d$ решений

$$\left[\frac{bx_0 + jm}{d}\right], \quad j = 0,\ 1,\ \ldots,\ d-1.$$

Здесь $x_0$ — коэффициент при $a$ в линейном представлении (3.24).

Покажем теперь, как, пользуясь теоремой 3.10, можно решать сравнения первой степени с несколькими неизвестными.

**Пример 3.15.** Решим сравнение $48x - 45y + 13 \equiv 0 \pmod{100}$.

Запишем это сравнение в виде

$$48x \equiv 45y - 13 \pmod{100}. \tag{3.25}$$

Так как НОД $(48, 100) = 4$, то должно выполняться сравнение

$$45y - 13 \equiv y - 1 \equiv 0 \pmod{4}.$$

Решив это сравнение в целых числах, получим

$$y = 1 + 4t_2,$$

где $t_2 \in \mathbb{Z}$. Подставив это в (3.25) и упростив, будем иметь

$$12x \equiv 8 + 20t_2 \pmod{25}.$$

Поскольку НОД $(12, 25) = 1$, ограничений на $t_2$ не будет. Решив последнее сравнение в целых числах, найдём

$$x = 9 + 25t_1 + 10t_2,$$

где $t_1 \in \mathbb{Z}$. Итак, все решения исходного сравнения в целых числах суть

$$(x, y) = (9 + 25t_1 + 10t_2, 1 + 4t_2), \quad t_1,\, t_2 \in \mathbb{Z}.$$

При желании это множество пар целых чисел можно «упаковать» в множество пар классов вычетов по модулю 100 (всего их окажется 100 штук, так как каждый из 25 возможных классов для $y$ приведёт к 4 классам для $x$), и мы получим ответ в виде

$$([9 + 25j_1 + 10j_2], [1 + 4j_2]),$$

где $0 \leqslant j_1 \leqslant 3$ и $0 \leqslant j_2 \leqslant 24$.

Пусть требуется решить сравнение 1-й степени с $n$ неизвестными:

$$a_1x_1 + \ldots + a_nx_n \equiv b \pmod{m},$$

где все $a_i \neq 0$. Положим $d_0 = m$ и для $i = 0,\, 1,\, \ldots,\, n-1$ вычислим

$$d_{i+1} = \text{НОД}\,(a_{i+1}, d_i) = \text{НОД}\,(a_{i+1}, \ldots, a_1, m), \quad q_i = \frac{d_i}{d_{i+1}}.$$

Если $b \not\equiv 0 \pmod{d_n}$, то решений нет, иначе положим

$$A_n = \frac{a_n}{d_n}, \quad B_n = \frac{b}{d_n}, \quad x_n = \frac{B_n}{A_n} \bmod q_{n-1} + q_{n-1}t_n$$

и для $i = n-1,\, \ldots,\, 1$ вычислим

$$A_i = \frac{a_i}{d_i}, \quad B_i = \frac{d_{i+1}B_{i+1} - a_{i+1}x_{i+1}}{d_i}, \quad x_i = \frac{B_i}{A_i} \bmod q_{i-1} + q_{i-1}t_i$$

В результате получим общее решение $(x_1, \ldots, x_n)$, «треугольно» зависящее от $n$ целочисленных параметров $t_1, \ldots, t_n$.

Теорию сравнений первой степени часто используют для решения неопределённых уравнений первой степени.

**Определение 3.10.** *Неопределённым уравнением первой степени* называется уравнение вида

$$a_1x_1 + \ldots + a_nx_n = b,$$

где $n > 1$ и все коэффициенты являются целыми числами.

Здесь предполагается, что неизвестные $x_1, \ldots, x_n$ принимают только целочисленные значения. Алгебраические уравнения

$$f(x_1, \ldots, x_n) = 0$$

с таким ограничением на неизвестные принято называть *диофантовыми* — по имени Диофанта Александрийского (III в.), автора знаменитого сочинения «Арифметика», в котором содержатся многочисленные примеры решения неопределённых уравнений.

В случае двух неизвестных решение неопределённого уравнения первой степени эквивалентно решению некоторого сравнения первой степени. Действительно, пусть дано неопределённое уравнение

$$Ax + By = C,$$

где коэффициенты $A$ и $B$ отличны от нуля. Рассмотрим сравнение

$$Ax \equiv C \pmod{|B|}.$$

Всякое решение $x_0 \in \mathbb{Z}$ этого сравнения приводит к решению $(x_0, y_0) \in \mathbb{Z}^2$ неопределённого уравнения, где

$$y_0 = \frac{C - Ax_0}{B}.$$

Обратно, если $(x_0, y_0)$ — решение неопределённого уравнения, то число $x_0$ будет удовлетворять сравнению. Таким образом, решив сравнение, мы найдём и все решения неопределённого уравнения.

**Пример 3.16.** Решим уравнение $50x - 42y = 34$.

Составив сравнение

$$50x \equiv 34 \pmod{42}$$

и решив его в целых числах, найдём $x = -1 + 21t$, где $t \in \mathbb{Z}$. Тогда

$$y = \frac{50x - 34}{42} = \frac{50(-1 + 21t) - 34}{42} = -2 + 25t.$$

Итак, все решения данного уравнения — это пары целых чисел вида

$$(x, y) = (-1 + 21t, -2 + 25t),$$

где параметр $t \in \mathbb{Z}$.

Последовательно решая подходящим образом составленные сравнения первой степени, можно решать неопределённые уравнения с любым числом неизвестных. Не излагая общего алгоритма, приведём один конкретный

**Пример 3.17.** Решим уравнение $30x + 24y - 55z = 11$.

Это уравнение эквивалентно сравнению

$$30x \equiv -24y + 11 \pmod{55}. \tag{3.26}$$

Поскольку НОД $(30, 55) = 5$, последнее разрешимо тогда и только тогда, когда

$$-24y + 11 \equiv y + 1 \equiv 0 \pmod{5},$$

откуда находим

$$y = 4 + 5t_2,$$

где $t_2 \in \mathbb{Z}$. Подставив в (3.26), после упрощений получим

$$6x \equiv 5 + 9t_2 \pmod{11}.$$

Имеем НОД $(6, 11) = 1$, поэтому никаких ограничений на $t_2$ не будет. Решив последнее сравнение, мы найдём

$$x = 10 + 11t_1 + 7t_2,$$

где $t_1 \in \mathbb{Z}$. Осталось найти неизвестное $z$:

$$z = \frac{30x + 24y - 11}{55} = \frac{30(10 + 11t_1 + 7t_2) + 24(4 + 5t_1) - 11}{55} = \\ = 7 + 6t_1 + 6t_2.$$

Таким образом, все решения данного уравнения — это тройки целых чисел вида

$$(x, y, z) = (10 + 11t_1 + 7t_2, 4 + 5t_2, 1 + 6t_1 + 6t_2),$$

где параметры $t_1,\ t_2 \in \mathbb{Z}$.

В заключение обсудим важный вопрос о конструктивном доказательстве китайской теоремы об остатках (см. теорему 1.9).

Напомним, что речь идёт о решении такой задачи: *найти число $r$, если известны остатки $r_1, \ldots, r_k$ от его деления на числа $m_1, \ldots, m_k$ соответственно.* Если данные числа $m_1$, $\ldots$, $m_k$ попарно взаимно просты, то при дополнительном ограничении

$$0 \leqslant r < m = m_1 \ldots m_k$$

эта задача имеет единственное решение для любого набора остатков $r_1, \ldots, r_k$.

Положим $M_i = m/m_i$ и для каждого $i = 1, \ldots, k$ рассмотрим сравнение

$$M_i x \equiv 1 \pmod{m_i}.$$

Поскольку

$$\text{НОД}\,(M_i, m_i) = 1, \quad i = 1, \ldots, k,$$

каждое такое сравнение имеет единственное решение, которое обозначим $[M_i^*]_{m_i}$. В качестве искомого числа $r$ можно взять наименьший неотрицательный вычет числа

$$R = M_1 M_1^* r_1 + \ldots + M_k M_k^* r_k \tag{3.27}$$

по модулю $m$. В самом деле, для любого $i = 1, \ldots, k$ имеем

$$R \equiv M_i M_i^* r_i \equiv r_i \pmod{m_i},$$

что и требуется.

**Упражнение 3.16.** Найдите все целые числа $r$, дающие при делении на 3 остаток 2, при делении на 5 — остаток 3, а при делении на 7 — снова остаток 2.

*Ответ.* $r = 23 + 105t$, где $t \in \mathbb{Z}$.

Отметим попутно, что числа $R$ вида (3.27) при $r_i$, пробегающих независимо друг от друга полные системы вычетов по модулям $m_i$ ($i = 1, \ldots, k$), образуют полную систему вычетов по модулю $m$ (случай $k = 2$ представлен в упражнении 3.3).

**Замечание 3.6.** Короткое алгебраическое доказательство китайской теоремы об остатках (и попутно свойства мультипликативности функции Эйлера) таково: отображение

$$[r]_m \to ([r]_{m_1}, [r]_{m_2})$$

задаёт *изоморфизм* кольца $\mathbb{Z}_m$ на прямую сумму колец $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$, который индуцирует изоморфизм мультипликативной группы $\mathbb{Z}_m^*$ на прямое произведение мультипликативных групп $\mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^*$.

# 4 Кольца классов вычетов

## 4.1 Кольцо $\mathbb{Z}_m$ классов вычетов по модулю $m$

Кольцо $\mathbb{Z}_m$ классов вычетов по модулю $m$. Модулярная арифметика. Делители нуля в $\mathbb{Z}_m$ и критерий их отсутствия.

В разделе 3.2 было введено множество $\mathbb{Z}_m$ всех классов вычетов по модулю $m$. Напомним, что классом вычетов по модулю $m$ с представителем $a \in \mathbb{Z}$ называется множество

$$[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}.$$

Цель этого раздела — ввести на множестве $\mathbb{Z}_m$ алгебраическую структуру кольца и изучить простейшие свойства получившегося кольца.

Прежде всего необходимо определить на $\mathbb{Z}_m$ две операции — сложение и умножение.

**Определение 4.1.** *Суммой классов вычетов* $[a]$ и $[b]$ называется класс вычетов, содержащий число $a + b$:

$$[a] + [b] = [a + b].$$

**Определение 4.2.** *Произведением классов вычетов* $[a]$ и $[b]$ называется класс вычетов, содержащий число $ab$:

$$[a] \cdot [b] = [ab].$$

Сразу возникает вопрос о корректности этих определений, поскольку складываемые (перемножаемые) классы вычетов могут быть заданы разными своими представителями.

Положительный ответ даёт

**Теорема 4.1.** Сумма и произведение классов вычетов, определенные выше, не зависят от выбора представителей классов.

Доказательство. Пусть $[a_1] = [a]$ и $[b_1] = [b]$. Тогда

$$a_1 \equiv a \pmod{m}, \quad b_1 \equiv b \pmod{m}.$$

Используя свойства сравнений (см. раздел 3.1), находим

$$a_1 + b_1 \equiv a + b \pmod{m}, \quad a_1 b_1 \equiv ab \pmod{m}.$$

Следовательно, $[a_1 + b_1] = [a + b]$ и $[a_1 b_1] = [ab]$. □

**Пример 4.1.** Рассмотрим множество

$$\mathbb{Z}_{12} = \{[0], [1], \ldots, [11]\}.$$

Приведём несколько примеров на сложение и умножение в $\mathbb{Z}_{12}$:

$$[5] + [8] = [1], \quad [5] \cdot [8] = [4], \quad [3] \cdot [8] = [0].$$

Последнее равенство выглядит особенно необычно, к нему мы ещё вернёмся.

В общем случае нетрудно заметить, что сумма классов вычетов $[a]+[b]$ содержит всевозможные суммы $a_1+b_1$, где $a_1\in[a]$ и $b_1\in[b]$. Более того, она состоит только из таких сумм:

$$[a]+[b]=\{a_1+b_1 : a_1\in[a],\ b_1\in[b]\}.$$

Действительно, если $c\in[a]+[b]=[a+b]$, то $c\equiv a+b \pmod m$, откуда $c-a\equiv b \pmod m$, т. е. $c-a\in[b]$. Таким образом, имеем $c=a+(c-a)$, где $a\in[a]$, $c-a\in[b]$.

Для произведения классов вычетов подобное утверждение уже, вообще говоря, не имеет места. Мы можем только утверждать, что

$$\{a_1b_1 : a_1\in[a],\ b_1\in[b]\}\subset[a]\cdot[b].$$

**Упражнение 4.1.** При $m=7$ покажите, что класс вычетов $[6]$ содержит элемент, не принадлежащий множеству $\{xy : x\in[2],\ y\in[3]\}$.

*Решение.* Таковым будет, например, число $13=6+7\cdot1\in[6]$. Предположим, что

$$13=(2+7t_1)(3+7t_2)$$

для некоторых $t_1,\ t_2\in\mathbb{Z}$. Так как 13 — простое число, отсюда следует

$$2+7t_1\in\{\pm1,\pm13\},$$

но это невозможно ни при каком $t_1\in\mathbb{Z}$. □

Сформулируем теперь основной результат этого параграфа.

**Теорема 4.2.** Множество $\mathbb{Z}_m$ классов вычетов по модулю $m$ с введёнными выше операциями сложения и умножения образует коммутативное кольцо с единицей.

ДОКАЗАТЕЛЬСТВО. Убедимся, что условия, определяющие коммутативное кольцо с единицей, действительно выполнены для $\mathbb{Z}_m$.

**1.** *Ассоциативность сложения.*

$$([a]+[b])+[c]=[a+b]+[c]=[(a+b)+c]=[a+(b+c)]=$$
$$=[a]+[b+c]=[a]+([b]+[c]).$$

Третье равенство в этой цепочке вытекает из свойства ассоциативности сложения целых чисел.

**2.** *Коммутативность сложения.*

$$[a]+[b]=[a+b]=[b+a]=[b]+[a].$$

Здесь мы воспользовались коммутативностью сложения целых чисел.

**3.** *Существование нулевого элемента.*

Нулевым элементом является класс вычетов $[0]$, состоящий из чисел, остаток от деления которых на $m$ равен нулю, т. е. из чисел, кратных $m$. Действительно,

$$[a]+[0]=[a+0]=[a].$$

**4.** *Существование противоположного элемента.*

Для класса вычетов $[a]$ противоположным является класс вычетов $[-a]$, содержащий число $-a$. В самом деле, имеем

$$[a] + [-a] = [a + (-a)] = [0].$$

**5.** *Ассоциативность умножения.*

$$([a] \cdot [b]) \cdot [c] = [ab] \cdot [c] = [(ab)c] = [a(bc)] = [a] \cdot [bc] = [a] \cdot ([b] \cdot [c]).$$

**6.** *Коммутативность умножения.*

$$[a] \cdot [b] = [ab] = [ba] = [b] \cdot [a].$$

**7.** *Дистрибутивность умножения по сложению.*

$$([a] + [b]) \cdot [c] = [a + b] \cdot [c] = [(a + b)c] = [ac + bc] = \\ = [ac] + [bc] = [a] \cdot [c] + [b] \cdot [c].$$

При проверке условий 5 — 7 мы использовали свойства ассоциативности, коммутативности и дистрибутивности умножения целых чисел.

**8.** *Существование единичного элемента.*

Роль единичного элемента выполняет класс вычетов $[1]$, так как

$$[a] \cdot [1] = [a \cdot 1] = [a].$$

Итак, проверена выполнимость всех условий, определяющих коммутативное кольцо с единицей. □

Кольцо $\mathbb{Z}_m$ называется *кольцом классов вычетов по модулю* $m$. Выполнение условий 1 — 4 означает, что относительно операции сложения множество $\mathbb{Z}_m$ образует абелеву группу — она называется *аддитивной группой кольца* $\mathbb{Z}_m$. В частности, мы можем стандартным образом определить операцию вычитания классов вычетов:

$$[a] - [b] = [a] + [-b].$$

Далее обычным для колец образом можно ввести операции умножения класса вычетов на целое число и возведения класса вычетов в целую неотрицательную степень.

**Определение 4.3.** Пусть $[a] \in \mathbb{Z}_m$ и $n$ — натуральное число. Тогда

$$n[a] = \underbrace{[a] + [a] + \ldots + [a]}_{n}, \quad -n[a] = n[-a], \quad 0 \cdot [a] = [0];$$

$$[a]^n = \underbrace{[a] \cdot [a] \cdot \ldots \cdot [a]}_{n}, \quad [a]^0 = [1].$$

Для любого класса вычетов $[a] \in \mathbb{Z}_m$ имеют место равенства

$$c[a] = [ca], \quad [a]^n = [a^n],$$

где $c$ и $n$ — целые числа, $n \geqslant 0$. (Классы вычетов $c[a]$ и $[ca]$ имеют общий элемент $ca$ и потому совпадают; второе равенство доказывается аналогично.)

**Определение 4.4.** Пусть $[a] \in \mathbb{Z}_m$ и $f(x) = c_0x^n + c_1x^{n-1} + \ldots + c_n \in \mathbb{Z}[x]$. Значением многочлена $f(x)$ при $x = [a]$ называется

$$f([a]) = c_0[a]^n + c_1[a]^{n-1} + \ldots + c_n[1] \in \mathbb{Z}_m.$$

Нетрудно видеть, что для любого $[a] \in \mathbb{Z}_m$ выполняется равенство

$$f([a]) = [f(a)].$$

В заключение обсудим одну особенность арифметики кольца $\mathbb{Z}_m$ (или, как обычно говорят, *модулярной арифметики*). В примере 4.1 показано, что произведение ненулевых классов вычетов может оказаться равным нулевому классу вычетов. Напомним следующее

**Определение 4.5.** Элемент $\alpha \neq 0$ кольца называется *делителем нуля*, если существует такой элемент $\beta \neq 0$ того же кольца, что $\alpha\beta = 0$.

Таким образом, кольцо $\mathbb{Z}_m$ — это кольцо, в котором, вообще говоря, могут быть делители нуля.

**Теорема 4.3.** В кольце $\mathbb{Z}_m$ отсутствуют делители нуля тогда и только тогда, когда $m = p$ — простое число.

Доказательство. Если модуль $m$ — составное число, $m = m_1m_2$, где $1 < m_i < m$, то

$$[m_1] \cdot [m_2] = [m] = [0],$$

при этом оба класса вычетов $[m_i] \neq [0]$. Значит, делители нуля есть.

Пусть теперь $m = p$ — простое число. Равенство

$$[a] \cdot [b] = [0]$$

эквивалентно сравнению $ab \equiv 0 \pmod{p}$, которое означает, что произведение $ab$ делится на $p$. Так как $p$ — простое, то один из сомножителей кратен $p$. Следовательно, $[a] = [0]$ или $[b] = [0]$, и делителей нуля нет. □

Итак, кольцо $\mathbb{Z}_m$ является *областью целостности* (т. е. коммутативным кольцом с единицей и без делителей нуля) в том и только том случае, когда $m = p$ — простое число.

Напомним (см. определение 3.5), что класс вычетов $[a] \in \mathbb{Z}_m$ называется взаимно простым с модулем, если НОД $(a, m) = 1$.

**Упражнение 4.2.** Докажите, что:

а) никакой взаимно простой с модулем класс вычетов $[a] \in \mathbb{Z}_m$ не может быть делителем нуля;

б) если НОД $(a, m) > 1$, то класс вычетов $[a] \in \mathbb{Z}_m$ является делителем нуля.

Таким образом, в кольце $\mathbb{Z}_m$ всякий класс вычетов либо взаимно прост с модулем, либо является делителем нуля.

## 4.2 Группа обратимых элементов кольца $\mathbb{Z}_m$

Обратимые классы вычетов по модулю $m$. Группа обратимых элементов кольца $\mathbb{Z}_m$. Вычисление класса вычетов, обратного к данному. Деление на обратимый класс вычетов.

Классы вычетов по модулю $m$ можно складывать, вычитать и перемножать. Можно ли определить операцию деления?

Под *делением* классов вычетов $[b],\ [a] \in \mathbb{Z}_m$ мы понимаем нахождение такого класса $[c] \in \mathbb{Z}_m$ (*частного* от деления данных классов), что

$$[b] = [a] \cdot [c].$$

**Пример 4.2.** Рассмотрим кольцо $\mathbb{Z}_{24}$.

В этом кольце можно единственным образом разделить $[16]$ на $[5]$:

$$[16] = [5] \cdot [8].$$

Деление $[12]$ на $[18]$ возможно, но не однозначно:

$$[12] = [18] \cdot [2] = [18] \cdot [6].$$

Наконец, $[9]$ нельзя разделить на $[10]$: равенство

$$[9] = [10] \cdot [x]$$

означало бы, что $9 \equiv 10x \pmod{24}$, но это сравнение неразрешимо.

Очевидно, такое разнообразие ситуаций вызвано наличием в кольце $\mathbb{Z}_{24}$ делителей нуля.

Далее мы выясним, при каких условиях деление классов вычетов возможно, причём частное определено однозначно.

**Определение 4.6.** Пусть $[a] \in \mathbb{Z}_m$. Если существует такой класс вычетов $[x] \in \mathbb{Z}_m$, что

$$[a] \cdot [x] = [1], \tag{4.1}$$

то он называется *обратным* к $[a]$. Сам же класс вычетов $[a]$ в этом случае называется *обратимым*.

Обозначение: $[x] = [a]^{-1}$.

**Упражнение 4.3.** Докажите единственность $[a]^{-1}$.

Не всякий ненулевой класс вычетов обратим. Например, любой делитель нуля $[a] \in \mathbb{Z}_m$ не имеет обратного.

**Упражнение 4.4.** Докажите это утверждение.

Оказывается, все остальные классы вычетов (а это те, которые взаимно просты с модулем) обратимы.

**Теорема 4.4.** Если класс вычетов $[a] \in \mathbb{Z}_m$ взаимно прост с модулем, то он обратим.

Доказательство. Равенство (4.1) равносильно сравнению

$$ax \equiv 1 \pmod{m}.$$

Так как НОД $(a, m) = 1$, то по теореме 3.10 это сравнение однозначно разрешимо. Его единственное решение $[r_0]$ и есть искомый обратный класс вычетов: $[a]^{-1} = [r_0]$. □

**Замечание 4.1.** В разделе 3.4 разъяснено, как следует на практике искать $r_0$. Там же приведена и явная формула для $r_0$, используя которую, мы можем записать

$$[a]^{-1} = [a^{\varphi(m)-1}], \tag{4.2}$$

где $\varphi(m)$ — функция Эйлера. Однако возможности практического применения этой формулы ограничены лишь теми значениями $m$, для которых легко вычислить $\varphi(m)$.

Из упражнений 4.2, 4.4 и теоремы 4.4 следует, что класс вычетов $[a] \in \mathbb{Z}_m$ обратим тогда и только тогда, когда он взаимно прост с модулем $m$. Напомним, что таких классов вычетов ровно $\varphi(m)$ штук, а их множество обозначается $\mathbb{Z}_m^*$.

**Упражнение 4.5.** Докажите, исходя из определения $\mathbb{Z}_m^*$, что это множество замкнуто относительно умножения.

**Пример 4.3.** Рассмотрим кольцо $\mathbb{Z}_{10}$.
Имеем $\mathbb{Z}_{10}^* = \{[1], [3], [7], [9]\}$, $\varphi(10) = 4$. По формуле (4.2) находим

$$[1]^{-1} = [1], \quad [3]^{-1} = [7], \quad [7]^{-1} = [3], \quad [9]^{-1} = [9].$$

Нетрудно заметить, что множество $\mathbb{Z}_{10}^*$ образует группу относительно умножения. На самом деле это наблюдение отражает хорошо известный алгебраический факт: обратимые элементы какого-либо кольца образуют группу (абелеву, если кольцо коммутативно), которая называется *группой обратимых элементов* этого кольца.

Итак, $\mathbb{Z}_m^*$ — группа обратимых элементов кольца $\mathbb{Z}_m$. Она, очевидно, абелева и конечна, при этом её порядок

$$|\mathbb{Z}_m^*| = \varphi(m).$$

Группу обратимых элементов $\mathbb{Z}_p^*$ при простом $p$ составляют все ненулевые классы вычетов, так как в этом случае $\varphi(p) = p - 1$.

**Пример 4.4.** Найдём три последние цифры числа $A = 1997^{1997}$.
Речь идёт о вычислении $[1997]^{1997}$ в группе $\mathbb{Z}_{1000}^*$. Имеем

$$[1997]^{1997} = [-3]^{1997} = [-3]^{5\cdot 400-3} = [-3]^{-3} = ([-3]^{-1})^3 =$$
$$= [333]^3 = [333^3] = [(333 \cdot 3)^2 \cdot 37] = [(-1)^2 \cdot 37] = [37].$$

Мы воспользовались теоремой Эйлера, согласно которой

$$(-3)^{\varphi(1000)} = (-3)^{400} \equiv 1 \pmod{1000}$$

или, по-другому, $[-3]^{400} = [1]$.
Итак, $A = \ldots 037$.

**Пример 4.5.** Используя вычисления в группе $\mathbb{Z}_p^*$ (где $p$ — нечётное простое число), дадим ещё одно доказательство теоремы Вильсона (см. теорему 3.8).

Доказательство основано на следующем наблюдении: среди всех классов вычетов $[a] \in \mathbb{Z}_p^*$ только два являются обратными к самим себе: это $[1]$ и $[p-1] = -[1]$. (Если $[a] \neq \pm[1]$, то

$$[a] \neq [a]^{-1},$$

поскольку иначе сравнение

$$x^2 - 1 \equiv 0 \pmod{p}$$

имело бы более двух решений, что невозможно.)

Но в таком случае все классы вычетов, отличные от $\pm[1]$, разбиваются на пары взаимно обратных классов, произведение которых равно, очевидно, $[1]$. Следовательно,

$$[1] \cdot [2] \cdot \ldots \cdot [p-1] = [1] \cdot [p-1] = -[1].$$

Это можно записать как $[(p-1)!] = -[1]$, что эквивалентно сравнению

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

Об этом сравнении и идёт речь в теореме Вильсона.

Вернёмся теперь к вопросу о существовании и единственности частного от деления двух классов вычетов.

**Теорема 4.5.** В кольце $\mathbb{Z}_m$ возможно, и притом единственным образом, деление на любой класс вычетов $[a] \in \mathbb{Z}_m^*$. Частное от деления $[b]$ на $[a]$ определяется по формуле

$$[c] = [b] \cdot [a]^{-1}.$$

**Упражнение 4.6.** Докажите эту теорему.

**Пример 4.6.** В кольце $\mathbb{Z}_{24}$ разделим $[18]$ на $[7]$.

Поскольку $[7] \in \mathbb{Z}_{24}^*$, это возможно. Имеем $[7]^{-1} = [7]$, поэтому

$$[18] \cdot [7]^{-1} = [18] \cdot [7] = [6],$$

т. е. частное от деления равно $[6]$.

**Упражнение 4.7.** Пусть $[a_i]$, $[b_i] \in \mathbb{Z}_m$, при этом $[a_i] \in \mathbb{Z}_m^*$, $i = 1, 2$. Докажите следующий критерий: частные от деления $[b_i]$ на $[a_i]$ равны тогда и только тогда, когда

$$b_1 a_2 \equiv b_2 a_1 \pmod{m}. \tag{4.3}$$

*Решение.* Обозначим через $[c_i]$ частное от деления $[b_i]$ на $[a_i]$. По теореме 4.5 имеем $[c_i] = [b_i] \cdot [a_i]^{-1}$. Это означает, что

$$b_i \equiv c_i a_i \pmod{m}, \quad i = 1, 2. \tag{4.4}$$

Предположим теперь, что $[c_1] = [c_2]$. Тогда

$$c_1 \equiv c_2 \pmod{m},$$
$$b_1 a_2 \equiv c_1 a_1 a_2 \equiv c_2 a_1 a_2 \equiv b_2 a_1 \pmod{m},$$

т. е. сравнение (4.3) выполняется.

Обратно, пусть имеет место сравнение (4.3). Учитывая (4.4), имеем

$$c_1 a_1 a_2 \equiv b_1 a_2 \equiv b_2 a_1 \equiv c_2 a_2 a_1 \pmod{m}, \quad c_1 a_1 a_2 \equiv c_2 a_2 a_1 \pmod{m}.$$

Сократив на $a_1 a_2$, получим $c_1 \equiv c_2 \pmod{m}$, т. е. $[c_1] = [c_2]$. □

## 4.3 Поле $\mathbb{Z}_p$ классов вычетов по простому модулю $p$

Поле $\mathbb{Z}_p$ классов вычетов по простому модулю $p$. Арифметика по простому модулю $p$. Многочлены над полем $\mathbb{Z}_p$. Теорема Вильсона как частный случай формул Виета.

Напомним следующее

**Определение 4.7.** Коммутативное кольцо с единицей, отличной от нуля, в котором каждый ненулевой элемент обратим по умножению, называется *полем*.

Когда кольцо классов вычетов $\mathbb{Z}_m$ будет полем? Ответ даёт

**Теорема 4.6.** Кольцо $\mathbb{Z}_m$ — поле тогда и только тогда, когда $m = p$ — простое число.

Доказательство. Как известно, в поле отсутствуют делители нуля, поэтому если $m$ — составное число, то $\mathbb{Z}_m$ — не поле (см. теорему 4.3).

С другой стороны, если $m = p$ — простое число, то, как уже отмечалось, группа обратимых элементов $\mathbb{Z}_p^*$ состоит из всех ненулевых классов вычетов. Следовательно, $\mathbb{Z}_p$ — поле. □

**Замечание 4.2.** Вообще, всякая конечная область целостности является полем.

**Упражнение 4.8.** Докажите это утверждение.

Таким образом, в поле классов вычетов $\mathbb{Z}_p$ по простому модулю можно выполнять все четыре арифметических действия. Рассмотрим несколько примеров использования арифметики поля $\mathbb{Z}_p$.

**Пример 4.7.** Найдём сумму

$$S = [1]^{-1} + [2]^{-1} + \ldots + [p-1]^{-1},$$

где $p$ — нечётное простое число.

Очевидно, если $x$ пробегает множество всех ненулевых элементов поля $\mathbb{Z}_p$, то $x^{-1}$ также пробегает это множество. Следовательно,

$$S = [1] + [2] + \ldots + [p-1] = [1 + 2 + \ldots + (p-1)] = \left[\frac{(p-1)p}{2}\right] = [0].$$

**Замечание 4.3.** Результат примера 4.7 можно истолковать так: если сумму дробей

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1}$$

привести к общему знаменателю, то числитель получившейся дроби будет кратен $p$. Например, при $p = 7$ имеем

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} = \frac{49}{20}$$

и 49 делится на 7.

**Упражнение 4.9.** Докажите, что если $p > 3$, то числитель будет делиться даже на $p^2$.

Следующий пример уже более близок к алгебре, чем к арифметике.

**Пример 4.8.** Натуральные числа $a$, $b$, $c$ таковы, что

$$ab + 9b + 81 \equiv 0 \pmod{101}, \quad bc + 9c + 81 \equiv 0 \pmod{101}. \tag{4.5}$$

Докажем, что число $ca + 9a + 81$ делится на 101.

Заметим, что 101 — простое число. Это позволяет нам рассматривать сравнения (4.5) как равенства

$$\alpha\beta + [9]\beta + [81] = [0], \quad \beta\gamma + [9]\gamma + [81] = [0]$$

в поле $\mathbb{Z}_{101}$, где для удобства записи введены обозначения $\alpha = [a]$, $\beta = [b]$, $\gamma = [c]$. Далее эти равенства можно исследовать алгебраически и выразить, скажем, $\alpha$ и $\gamma$ через $\beta$:

$$\alpha = -\frac{[9](\beta + [9])}{\beta}, \quad \gamma = -\frac{[81]}{\beta + [9]}$$

(здесь мы, конечно, пользуемся тем, что $\beta \neq [0]$ и $\beta \neq -[9]$). Подставив всё это в выражение

$$\gamma\alpha + [9]\alpha + [81],$$

после упрощения получим $[0]$. Осталось вернуться от классов вычетов к числам.

Специфика арифметики поля $\mathbb{Z}_p$ состоит в том, что

$$\alpha^p = \alpha \tag{4.6}$$

для всякого элемента $\alpha \in \mathbb{Z}_p$ (одна из версий малой теоремы Ферма 3.4). В некотором смысле это свойство характеризует поле $\mathbb{Z}_p$. Как следствие, получим

$$(\alpha_1 + \alpha_2 + \ldots + \alpha_k)^p = \alpha_1 + \alpha_2 + \ldots + \alpha_k$$

для любых элементов $\alpha_i \in \mathbb{Z}_p$ ($i = 1, \ldots, k$), а также

$$\alpha^{p-1} = [1], \quad \alpha^{-1} = \alpha^{p-2},$$

если $\alpha \neq [0]$.

**Пример 4.9.** Пусть $\alpha \in \mathbb{Z}_p$. Докажем, что

$$\sum_{j=1}^{p-1} j\alpha^j = \begin{cases} \dfrac{\alpha}{1-\alpha}, & \text{если } \alpha \neq [1], \\ [0], & \text{если } \alpha = [1]. \end{cases}$$

При $\alpha = [1]$ эта сумма была вычислена в примере 4.7. Пусть $\alpha \neq [1]$. Мы можем воспользоваться тождеством

$$\sum_{j=1}^{p-1} jx^j = \frac{px^p}{x-1} - \frac{x(x^p-1)}{(x-1)^2}, \quad x \neq 1,$$

справедливом в любом поле. В поле $\mathbb{Z}_p$ при $x = \alpha$ правая часть упрощается до

$$\frac{\alpha}{1-\alpha}$$

(мы учли соотношение (4.6), а также то, что $p\alpha = [0]$).

Как и над всяким полем, над полем $\mathbb{Z}_p$ можно рассматривать многочлены. Некоторые из доказанных нами ранее фактов превращаются в частные случаи общих теорем теории многочленов. Например, теорема 3.7 о том, что всякое сравнение по модулю $p$ степени $n$ имеет не более $n$ решений — частный случай хорошо известной теоремы, которая гласит: *любой многочлен с коэффициентами из некоторого поля не может иметь корней больше, чем его степень*.

Другой пример доставляет теорема Вильсона (см. теорему 3.8), которая является частным случаем *формул Виета*, выражающих элементарные симметрические функции корней многочлена через его коэффициенты. Действительно, многочлен

$$f(x) = x^{p-1} - [1]$$

над полем $\mathbb{Z}_p$ имеет в этом поле $p-1$ корней — ими являются, как легко видеть, все ненулевые элементы поля $\mathbb{Z}_p$. Но тогда произведение всех корней равно свободному коэффициенту, взятому со знаком $(-1)^{p-1}$:

$$[1] \cdot [2] \cdot \ldots \cdot [p-1] = (-1)^{p-1}(-[1]) = -[1].$$

Как уже отмечалось (см. пример 4.5), это эквивалентно утверждению теоремы Вильсона.

**Упражнение 4.10.** Пусть $p$ — простое число вида $4k+1$. Докажите, что уравнение

$$x^2 + [1] = [0] \tag{4.7}$$

разрешимо в поле $\mathbb{Z}_p$.

*Решение*. При $p = 4k+1$ равенство

$$[1] \cdot [2] \cdot \ldots \cdot [p-1] + [1] = [0]$$

преобразуется к виду

$$[(2k)!]^2 + [1] = [0],$$

поэтому можно взять $x = [(2k)!]$. □

**Замечание 4.4.** Эта формула для $x$ непригодна для больших $p$. Для практического решения уравнения (4.7) (как и любых алгебраических уравнений) над полем $\mathbb{Z}_p$ используют так называемые *вероятностные методы*. Напомним, что для $p = 4k-1$ уравнение (4.7) решений не имеет (см. упражнение 3.9).

В заключение обратим внимание на одну особенность алгебры многочленов над полем $\mathbb{Z}_p$: если $f(x)$ — произвольный многочлен с коэффициентами из $\mathbb{Z}_p$, то справедливо тождество

$$f(x)^p = f(x^p).$$

Это тождество — следствие и в то же время наиболее общая формулировка Idiot's Polynomial Theorem (см. замечание 3.3).

## 4.4 Порядок класса вычетов. Первообразные корни

Порядок обратимого класса вычетов по модулю $m$. Первообразный корень по модулю $m$. Теорема Гаусса о первообразном корне по простому модулю $p$. Критерий существования первообразного корня по модулю $m$.

В этом разделе мы продолжим изучать группу обратимых элементов $\mathbb{Z}_m^*$ кольца классов вычетов $\mathbb{Z}_m$.

**Определение 4.8.** *Порядком* класса вычетов $[a] \in \mathbb{Z}_m^*$ называется наименьшее натуральное число $\delta$ такое, что $[a]^\delta = [1]$.

Такое число $\delta$ всегда существует. Действительно, рассмотрим степени класса вычетов $[a]$ с натуральными показателями:

$$[a]^k \quad (k = 1,\ 2,\ \dots).$$

Так как все они принадлежат конечной группе $\mathbb{Z}_m^*$, то

$$[a]^k = [a]^l$$

для некоторых $k > l$. Но тогда $[a]^{k-l} = [1]$, при этом $k - l \geqslant 1$.

Более того, для порядка $\delta$ справедливо неравенство

$$\delta \leqslant \varphi(m).$$

Это следует из теоремы Эйлера (см. теорему 3.5), которую можно переформулировать так.

**Теорема 4.7.** Если $[a] \in \mathbb{Z}_m^*$, то $[a]^{\varphi(m)} = [1]$.

Определение 4.8 можно дать по-другому, сохранив его суть. Пусть НОД $(a, m) = 1$.

**Определение 4.9.** *Порядком* числа $a$ по модулю $m$ называется наименьшее натуральное число $\delta$ такое, что

$$a^\delta \equiv 1 \pmod{m}.$$

Говорят также, что число $a$ *принадлежит показателю* $\delta$ по модулю $m$. Ясно, что для всех чисел из $[a]$ показатель $\delta$, которому они принадлежат, один и тот же.

**Пример 4.10.** Найдём порядок $\delta$ класса вычетов $[7] \in \mathbb{Z}_{18}^*$.

Имеем

$$[7]^1 = [7], \quad [7]^2 = [13], \quad [7]^3 = [1],$$

поэтому $\delta = 3$.

**Теорема 4.8.** Пусть $[a] \in \mathbb{Z}_m^*$ и $k \in \mathbb{Z}$. Равенство

$$[a]^k = [1] \tag{4.8}$$

выполняется тогда и только тогда, когда $k \equiv 0 \pmod{\delta}$, где $\delta$ — порядок класса вычетов $[a]$.

Доказательство. Неочевидно лишь утверждение «только тогда». Чтобы его доказать, разделим $k$ на $\delta$ с остатком:

$$k = \delta q + r, \quad 0 \leqslant r < \delta.$$

Имеем $[a]^k = ([a]^\delta)^q [a]^r = [a]^r$. Следовательно, равенство (4.8) равносильно равенству

$$[a]^r = [1].$$

При $r > 0$ получим противоречие с определением $\delta$. Значит, $r = 0$. □

**Следствие 4.1.** Порядок любого класса вычетов из $\mathbb{Z}_m^*$ есть делитель $\varphi(m)$.

На самом деле здесь $\varphi(m)$ можно заменить на функцию Кармайкла $\lambda(m)$ (см. конец раздела 3.2), которая может быть определена как наименьшее общее кратное порядков всех классов вычетов из $\mathbb{Z}_m^*$.

**Следствие 4.2.** Для $[a] \in \mathbb{Z}_m^*$ и $k,\ l \in \mathbb{Z}$ равенство

$$[a]^k = [a]^l$$

равносильно сравнению $k \equiv l \pmod{\delta}$.

**Следствие 4.3.** Для $[a] \in \mathbb{Z}_m^*$ классы вычетов

$$[a]^k, \quad k = 0,\ 1,\ \ldots,\ \delta - 1, \tag{4.9}$$

попарно различны.

**Упражнение 4.11.** Выведите эти следствия теоремы 4.8.

**Упражнение 4.12.** Пусть порядок класса вычетов $[a] \in \mathbb{Z}_m^*$ равен $\delta$. Докажите, что порядок класса вычетов $[b] = [a]^k$, где $k \in \mathbb{Z}$, равен

$$\Delta = \frac{\delta}{\text{НОД}\,(k, \delta)}.$$

*Указание.* Воспользуйтесь определением порядка класса вычетов.

**Замечание 4.5.** Теорема 4.7 (теорема Эйлера), а также следствие 4.1 теоремы 4.8 выводятся из *теоремы Лагранжа* в теории групп, которая гласит: *порядок любой подгруппы конечной группы делит порядок этой группы*.

**Пример 4.11.** Найдём порядок класса вычетов $[7] \in \mathbb{Z}_{43}^*$.
Делителями $\varphi(43) = 42$ являются числа 1, 2, 3, 6, 7, 21 и 42. Имеем

$$[7]^1 = [7], \quad [7]^2 = [6], \quad [7]^3 = [-1], \quad [7]^6 = [1].$$

Таким образом, искомый порядок равен 6.

**Определение 4.10.** Пусть $\text{НОД}\,(g, m) = 1$. Если порядок класса вычетов $[g] \in \mathbb{Z}_m^*$ равен $\varphi(m)$, то число $g$ называется *первообразным корнем* по модулю $m$.

**Пример 4.12.** Число 3 — первообразный корень по модулю 4. Число 5 будет первообразным корнем по модулю 7. А вот по модулю 8 первообразных корней вообще нет (квадрат нечётного числа при делении на 8 всегда даёт в остатке 1).

С теоретико-групповой точки зрения вопрос о первообразных корнях по модулю $m$ — это вопрос, будет ли группа $\mathbb{Z}_m^*$ *циклической*, т. е. будет ли она состоять только из степеней какого-нибудь одного класса вычетов. Следующую теорему впервые доказал Гаусс.

**Теорема 4.9.** Если $m = p$ — простое число, то первообразные корни существуют.

На языке теории групп это звучит так: *мультипликативная группа поля из $p$ элементов является циклической*. Мы дадим два доказательства этой важной теоремы.

ПЕРВОЕ ДОКАЗАТЕЛЬСТВО. Это доказательство Гаусса.

Пусть $\delta$ — произвольный делитель числа $p-1$ и $\psi(\delta)$ — число тех классов вычетов в $\mathbb{Z}_p^*$, порядок которых равен $\delta$. Покажем, что либо $\psi(\delta) = 0$, либо $\psi(\delta) = \varphi(\delta)$.

Действительно, предположим, что $\psi(\delta) > 0$ и пусть $[a]$ — некоторый класс вычетов, порядок которого есть $\delta$. Положим

$$f_\delta(x) = x^\delta - [1]$$

и рассмотрим произвольный класс вычетов $[b]$, порядок которого также равен $\delta$. Тогда

$$[b] = [a]^k \tag{4.10}$$

для некоторого целого $k$. В самом деле, имеем

$$f_\delta([b]) = [b]^\delta - [1] = [0].$$

Но классы вычетов (4.9) попарно различны и все являются корнями многочлена $f_\delta(x)$; поскольку других корней у этого многочлена нет, должно выполняться равенство (4.10). Далее заметим, что показатель $k$ в (4.10) должен быть взаимно простым с $\delta$ числом (иначе порядок $[b]$ будет меньше $\delta$, см. упражнение 4.12). Таких показателей имеется в точности $\varphi(\delta)$ штук, а значит, классов вычетов $[b]$, чей порядок равен $\delta$, столько же, т. е. $\psi(\delta) = \varphi(\delta)$.

В частности, это рассуждение доказывает, что

$$\psi(\delta) \leqslant \varphi(\delta)$$

для любого делителя $\delta$ числа $p-1$. Но имеют место равенства

$$\sum_{\delta \,|\, p-1} \psi(\delta) = p - 1 = \sum_{\delta \,|\, p-1} \varphi(\delta)$$

(второе из них — частный случай формулы (1.9)), поэтому на самом деле

$$\psi(\delta) = \varphi(\delta)$$

для любого $\delta$. В частности, при $\delta = p-1$ получим

$$\psi(p-1) = \varphi(p-1) > 0,$$

т. е. первообразные корни действительно есть. □

Отметим, что фактически Гаусс доказал более общее утверждение: для любого делителя $\delta$ числа $p-1$ найдутся в точности $\varphi(\delta)$ классов вычетов из $\mathbb{Z}_p^*$, порядок которых равен $\delta$.

ВТОРОЕ ДОКАЗАТЕЛЬСТВО. На самом деле верно более общее утверждение: *мультипликативная группа конечного поля является циклической*. Доказательство основано на известном факте о конечных абелевых группах (ниже он сформулирован для группы $\mathbb{Z}_p^*$).

**Лемма 4.1.** Пусть $\delta_1, \ldots, \delta_\tau$ — все значения порядков классов вычетов из $\mathbb{Z}_p^*$. Тогда найдётся класс вычетов $[g] \in \mathbb{Z}_p^*$, чей порядок

$$\delta = \text{НОК}\,(\delta_1, \ldots, \delta_\tau).$$

**Упражнение 4.13.** Докажите это утверждение.

*Указание*. Пусть

$$\text{НОК}\,(\delta_1, \ldots, \delta_\tau) = \prod_{i=1}^{t} p_i^{k_i}$$

— каноническое разложение. Для каждого $i$ существует такой класс вычетов $[g_i]$, чей порядок имеет вид $p_i^{k_i} Q_i$, где $\text{НОД}\,(Q_i, p_i) = 1$. Тогда

$$[g] = \prod_{i=1}^{t} [g_i]^{Q_i}$$

— класс вычетов, имеющий требуемый порядок.

Покажем, что число $g$ из леммы 4.1 — искомый первообразный корень по модулю $p$.

Действительно, по лемме любой ненулевой класс вычетов $[a]$ является корнем многочлена $f_\delta(x)$, а корней у него может быть не более $\delta$. Отсюда $p - 1 \leqslant \delta$. С другой стороны, $\delta \leqslant p - 1$. Таким образом, $\delta = p - 1$ и всё доказано. □

**Упражнение 4.14.** Докажите критерий: число $g$ является первообразным корнем по простому модулю $p$ тогда и только тогда, когда

$$g^{(p-1)/q} \not\equiv 1 \pmod{p}$$

для любого простого делителя $q$ числа $p - 1$.

**Замечание 4.6.** Иногда первообразный корень можно указать явно. Так, если $p = 2q + 1$, где $q$ — нечётное простое число, то можно взять $g = \pm 2$ при $q \equiv \pm 1 \pmod 4$ соответственно. Ещё пример: если $p$ — простое число вида $2^n + 1$, то первообразным корнем будет $g = 3$.

Существование первообразных корней $g$ по простому модулю $p$ расширяет возможности арифметики поля $\mathbb{Z}_p$, ибо позволяет наряду с привычным аддитивным взглядом на $\mathbb{Z}_p$ как на множество

$$\{[0], [1], \ldots, [p-1]\}$$

прибегать к другой — мультипликативной — точки зрения, согласно которой $\mathbb{Z}_p$ есть объединение

$$\mathbb{Z}_p^* = \{[g]^0, [g]^1, \ldots, [g]^{p-2}\}$$

и нулевого элемента $[0]$.

Проиллюстрируем сказанное несколькими примерами.

**Пример 4.13.** В лемме 3.1 речь идёт, по существу, о сумме $k$-х степеней всех элементов поля $\mathbb{Z}_p$, где $0 < k < p-1$.

Теперь эта сумма может быть вычислена так:

$$\sum_{r=0}^{p-1}[r]^k = \sum_{j=0}^{p-2}([g]^j)^k = \sum_{j=0}^{p-2}([g]^k)^j = \frac{([g]^k)^{p-1}-[1]}{[g]^k-[1]} = \frac{([g]^{p-1})^k-[1]}{[g]^k-[1]} = [0],$$

поскольку $[g]^k \neq [1]$, а $[g]^{p-1} = [1]$.

**Пример 4.14.** Ещё раз докажем теорему Вильсона (см. теорему 3.8).

Имеем

$$\prod_{r=1}^{p-1}[r] = \prod_{j=0}^{p-2}[g]^j = [g]^{(p-2)(p-1)/2} = [g]^{(p-1)/2} = -[1].$$

Поясним последнее равенство. Если $[g]^{(p-1)/2} = [r]$, то $[r]^2 = [g]^{p-1} = [1]$. Отсюда следует, что $[r] = \pm[1]$, при этом равенство $[r] = [1]$ невозможно, так как $g$ — первообразный корень.

**Пример 4.15.** Ещё один способ решения упражнения 4.10 состоит в том, чтобы рассмотреть $x = [g]^k$. Тогда $x^2 = [g]^{2k} = [g]^{(p-1)/2} = -[1]$, что и нужно.

В заключение сформулируем теорему о тех значениях $m$, для которых есть первообразные корни. Она также впервые была получена Гауссом.

**Теорема 4.10.** Первообразные корни существуют только при

$$m = 2,\ 4,\ p^\alpha,\ 2p^\alpha,$$

где $p$ — нечётное простое число, $\alpha$ — натуральное число.

Доказательство. Если $m$ не является одним из чисел указанного вида, то, как можно убедиться,

$$\lambda(m) < \varphi(m)$$

и ввиду теоремы Кармайкла первообразных корней по модулю $m$ быть не может.

I. Если $m = 2$ или $m = 4$, то первообразные корни, очевидно, есть.

II. Пусть $p$ — нечётное простое число и $g$ — некоторый первообразный корень по модулю $p$. Покажем, как найти первообразный корень по модулю $p^\alpha$ при любом $\alpha > 1$.

Имеем

$$g^{p-1} \equiv 1 \pmod{p},$$

т. е. $g^{p-1} - 1 = pa$ для некоторого натурального числа $a$.

Предположим, что $a$ не делится на $p$. Тогда $g$ будет первообразным корнем по модулю $p^\alpha$ при любом $\alpha > 1$. Действительно, индукцией по $k \geqslant 1$ легко доказывается равенство

$$\nu_p(g^{p^{k-1}(p-1)} - 1) = k.$$

Если $\delta$ — порядок $g$ по модулю $p^\alpha$, то $\delta$ делится на $p-1$ и делит $p^{\alpha-1}(p-1)$, т. е. $\delta = p^k(p-1)$, где $0 \leqslant k \leqslant \alpha - 1$. Значит,

$$\alpha \leqslant \nu_p(g^\delta - 1) = k + 1 \leqslant \alpha,$$

откуда $k = \alpha - 1$ и $\delta = p^{\alpha-1}(p-1)$.

Если же оказалось, что $a$ кратно $p$, вместо $g$ возьмём $g+p$. Для этого числа имеем

$$(g+p)^{p-1}-1=gp+(g^{p-1}-1)+\ldots\equiv gp\ (\mathrm{mod}\ p^2),$$

т. е. $(g+p)^{p-1}-1=pa_1$, где $a_1$ уже не кратно $p$. Итак, в этом случае первообразным корнем по модулю $p^\alpha$ будет $g+p$.

III. Пусть теперь $g$ — первообразный корень по модулю $p^\alpha$. Тогда первообразным корнем по модулю $2p^\alpha$ будет то из чисел $g$ и $g+p^\alpha$, которое нечётно. □

# 5 Некоторые приложения теории сравнений

## 5.1 Система шифрования RSA

Теория чисел и криптография. Система шифрования RSA как пример криптосистемы с открытым ключом. Алгоритм быстрого возведения в степень по модулю и его практическая реализация. Генерация больших простых чисел.

В этой главе мы обсудим некоторые вопросы *алгоритмической теории чисел* — интенсивно развивающегося последние несколько десятков лет направления в теории чисел, которое имеет важные приложения в криптографии. Актуальность этого направления сильно возросла в 70-е годы прошлого века в связи с появлением криптосистем Диффи — Хеллмана и RSA. В настоящее время, по некоторым оценкам, практически весь мировой парк средств *асимметричной криптографии* в математическом плане основан на теоретико-числовых задачах.

Современная криптография совершенно немыслима без вычислительных машин и электронных средств связи. Шифрование и дешифрование текстов можно представлять себе как процессы переработки целых чисел при помощи компьютеров, а способы, которыми выполняются эти операции — как некоторые функции, определённые на множестве целых чисел. Всё это делает естественным появление в криптографии методов теории чисел.

Но возможности компьютеров небезграничны. Приходится разбивать длинную цифровую последовательность на блоки ограниченной длины и шифровать каждый такой блок отдельно. Будем предполагать в дальнейшем, что все шифруемые целые числа неотрицательны и по величине меньше некоторого заданного (скажем, техническими ограничениями) числа $m$. Таким же условиям будут удовлетворять и числа, получаемые в процессе шифрования. Это позволяет считать и те, и другие числа элементами кольца классов вычетов $\mathbb{Z}_m$. Шифрующая функция при этом может рассматриваться как некоторое взаимно однозначное отображение

$$f : \mathbb{Z}_m \to \mathbb{Z}_m,$$

а $y = f(x)$ представляет собой сообщение $x$ в зашифрованном виде.

Простейшим шифром такого рода является *шифр замены*, который соответствует отображению

$$f : x \to (x + k) \bmod m,$$

где $k$ — некоторое фиксированное целое число. Здесь и далее $a \bmod m$ обозначает остаток от деления $a$ на $m$. Подобный шифр использовал ещё Юлий Цезарь (I в. до н. э.). Конечно, не каждое отображение $f$ можно использовать с целью надёжного сокрытия информации.

В 1978 году американцы R. L. Rivest, A. Shamir, L. Adleman предложили пример функции $f$, обладающей рядом замечательных достоинств. На её основе была построена реально используемая система шифрования, получившая название по первым буквам имён авторов — система RSA. Эта функция такова, что:

1. есть быстрый алгоритм вычисления значений $f(x)$;

2. существует быстрый алгоритм вычисления значений обратной функции $f^{-1}(x)$;

3. функция $f(x)$ обладает некоторым «секретом», знание которого позволяет быстро вычислять значения $f^{-1}(x)$; в противном же случае вычисление $f^{-1}(x)$ становится трудно разрешимой в вычислительном отношении задачей.

Пусть $m$ и $e$ — некоторые натуральные числа. Функция $f$, реализующая систему RSA, устроена следующим образом:

$$f : x \to x^e \bmod m. \tag{5.1}$$

Для дешифрования сообщения $y = f(x)$ достаточно решить сравнение

$$x^e \equiv y \pmod{m}. \tag{5.2}$$

При некоторых условиях на $m$ и $e$ это сравнение имеет единственное решение $x$.

Предположим, что НОД $(e, \varphi(m)) = 1$. Тогда при условии

$$\text{НОД}\,(y, m) = 1 \tag{5.3}$$

сравнение (5.2) будет иметь единственное решение. Для того, чтобы найти его, определим целое число $d$, удовлетворяющее условиям

$$de \equiv 1 \pmod{\varphi(m)}, \quad 1 \leqslant d < \varphi(m). \tag{5.4}$$

Ясно, что такое число $d$ существует и притом только одно. Если сравнение (5.2) разрешимо, то НОД $(x, m) = 1$ и по теореме Эйлера

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

Следовательно,

$$x \equiv x^{1+t\varphi(m)} = x^{de} \equiv y^d \pmod{m}.$$

Таким образом, единственное решение сравнения (5.2) может быть найдено по формуле

$$x = y^d \bmod m. \tag{5.5}$$

**Упражнение 5.1.** Пусть число $m$ свободно от квадратов. Докажите, что сравнение (5.2) будет разрешимо и без предположения (5.3). Более того, его единственным решением будет по-прежнему (5.5).

*Решение.* Пусть выполнено сравнение (5.2) и НОД $(x, m) = r$, $m = rm'$. Имеем

$$\text{НОД}\,(r, m') = 1, \quad \text{НОД}\,(x, m') = 1.$$

Тогда $\varphi(m) = \varphi(r)\varphi(m')$, $x^{\varphi(m')} \equiv 1 \pmod{m'}$ и, как следствие,

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

Отсюда

$$y^d = x^{de} = x^{1+t\varphi(m)} \equiv x \pmod{m'}.$$

Кроме того, $y^d = x^{de} \equiv x \pmod{r}$, поскольку $x \equiv 0 \pmod{r}$. В итоге $y^d \equiv x \pmod{m}$. □

Функция (5.1), принятая в системе RSA, может быть вычислена достаточно быстро (см. ниже). Обратная функция

$$f^{-1} : y \to y^d \bmod m$$

вычисляется по тем же правилам, но с заменой показателя степени $e$ на $d$. Тем самым функция (5.1) обладает указанными выше свойствами 1 и 2.

Для вычисления функции (5.1) достаточно знать лишь числа $e$ и $m$. Они составляют *открытый ключ* для шифрования. Для вычисления обратной функции требуется знать число $d$ — это и есть тот «секрет», о котором идёт речь в свойстве 3.

Казалось бы, ничего не стоит, зная число $m$, разложить его на простые сомножители, затем вычислить $\varphi(m)$ и, наконец, определить нужное число $d$ из условия (5.4). Все шаги этого вычисления могут быть реализованы достаточно быстро, за исключением первого. Именно разложение числа $m$ на простые сомножители и составляет наиболее трудоёмкую часть вычислений. В теории чисел, несмотря на многолетнюю её историю и очень интенсивные поиски в последнее время, эффективный алгоритм разложения натуральных чисел на множители так и не был найден.

Авторы системы RSA предложили выбирать число $m$ в виде произведения двух простых сомножителей $p$ и $q$, примерно одинаковых по величине. Так как

$$\varphi(m) = \varphi(pq) = (p-1)(q-1), \tag{5.6}$$

то единственное условие на выбор показателя степени $e$ в отображении (5.1) есть

$$\text{НОД}\,(e, p-1) = \text{НОД}\,(e, q-1) = 1. \tag{5.7}$$

Итак, лицо, заинтересованное в организации шифрованной переписки с помощью системы RSA, выбирает два достаточно больших простых числа $p$ и $q$. Перемножив их, оно находит число

$$m = pq.$$

Затем выбирается число $e$, удовлетворяющее (5.7), вычисляется с помощью (5.6) число $\varphi(m)$, а с помощью (5.4) — число $d$. Числа $m$ и $e$ публикуются, число $d$ держится в секрете. Теперь любой может отправлять зашифрованные с помощью (5.1) сообщения организатору этой системы, а организатор сможет легко дешифровать их с помощью (5.5).

Естественно, нужно избегать тех сообщений $x$, для которых $\text{НОД}\,(x, m) > 1$ — иначе также окажется $\text{НОД}\,(y, m) > 1$, и злоумышленник, перехватив $y$, легко сможет разложить $m$ на множители.

**Пример 5.1.** Пусть $p = 1093$, $q = 1997$, тогда

$$m = pq = 2182721, \quad \varphi(m) = (p-1)(q-1) = 2179632.$$

Выберем в качестве открытого ключа число $e = 871531$, тогда секретный ключ

$$d = e^{-1} \bmod \varphi(m) = 1498243.$$

Допустим, нам нужно отправить сообщение $x = 362490$. В зашифрованном виде оно будет выглядеть как

$$y = x^e \bmod m = 121469.$$

Для дешифрования используем секретный ключ:

$$y^d \bmod m = 362490.$$

Видно, что получается исходное сообщение $x$.

Описанная выше система RSA ставит ряд вопросов. Например: как проводить вычисления с большими числами и, в частности, как находить большие степени по данному большому модулю.

Следующий алгоритм вычисляет

$$a^b \bmod m$$

за $O(\ln m)$ арифметических операций (т. е. не более чем за $C \ln m$ таких операций, где $C$ — константа, не зависящая от $m$). При этом предполагается, что натуральные числа $a$ и $b$ не превосходят по величине $m$.

**А.** Представим $b$ в двоичной системе счисления:

$$b = b_0 2^k + b_1 2^{k-1} + \ldots + b_{k-1} 2^1 + b_k,$$

где $b_i \in \{0, 1\}$ — цифры в двоичном представлении, $b_0 = 1$.

**Б.** Положим $a_0 = a$ и затем для $i = 1, \ldots, k$ вычислим

$$a_i = a_{i-1}^2 \cdot a^{b_i} \bmod m.$$

**В.** $a_k$ есть искомый вычет $a^b \bmod m$.

Этот алгоритм, так называемый *бинарный метод*, был известен ещё в Индии два тысячелетия тому назад. Его корректность вытекает из сравнения

$$a_i \equiv a^{b_0 2^i + \ldots + b_i} \pmod m,$$

легко доказываемого индукцией по $i$. Так как каждое вычисление на втором шаге требует не более трёх умножений по модулю $m$ и этот шаг выполняется

$$k = [\log_2 b] \leqslant \log_2 m$$

раз, то сложность алгоритма может быть оценена величиной $O(\ln m)$.

**Пример 5.2.** Вычислим $2^{340} \bmod 341$.

Имеем

$$a = 2, \quad 340 = 2^8 + 2^6 + 2^4 + 2^2 = 101010100_2, \quad k = 8.$$

Следуя алгоритму, последовательно находим

$$a_0 = 2, \quad a_1 = 4, \quad a_2 = 32, \quad a_3 = 1, \quad a_4 = 2,$$
$$a_5 = 4, \quad a_6 = 32, \quad a_7 = 1, \quad a_8 = 1.$$

Итак, $2^{340} \bmod 341 = 1$.

**Упражнение 5.2.** В рассмотренном варианте бинарного алгоритма двоичное представление числа $b$ нужно знать «слева-направо», однако получается оно «справо-налево» — сначала $b_k$, затем $b_{k-1}$, и т. д. Придумайте алгоритм вычисления $a^b \bmod m$, который использовал бы двоичные цифры сразу по их получении.

Второй важный вопрос — это вопрос о *генерации больших простых чисел*, необходимых для надёжной работы схемы RSA. Наиболее эффективные методы построения больших простых чисел основаны на различных модификациях малой теоремы Ферма.

Рассмотрим одну из таких модификаций. Пусть $N > 1$ — некоторое нечётное число и нам известно частичное разложение числа $N - 1$ на простые сомножители:

$$N - 1 = SR, \quad S = \prod_{i=1}^{l} q_i^{\alpha_i}, \quad \text{НОД}\,(R, S) = 1.$$

Это позволяет получить некоторую информацию о возможных простых делителях числа $N$, иногда достаточную для того, чтобы утверждать, что $N$ — простое число.

**Лемма 5.1.** Пусть для любого простого делителя $q_i$ числа $S$ существует такое $a_i \in \mathbb{Z}$, что

$$a_i^{N-1} \equiv 1 \pmod{N}, \quad \text{НОД}\,(a_i^{(N-1)/q_i} - 1, N) = 1. \tag{5.8}$$

Тогда любой простой делитель $p$ числа $N$ удовлетворяет сравнению

$$p \equiv 1 \pmod{S}.$$

Доказательство. Пусть

$$N - 1 = q_i^{\alpha_i} N_i,$$

где $\text{НОД}\,(q_i, N_i) = 1$. Из соотношений (5.8) следует, что

$$a_i^{N-1} \equiv 1 \pmod{p}, \quad a_i^{(N-1)/q_i} \not\equiv 1 \pmod{p}.$$

Обозначим через $d_i$ порядок $a_i$ по модулю $p$. Тогда $d_i$ делится на $q_i^{\alpha_i}$ и, как следствие, $p - 1$ также делится на $q_i^{\alpha_i}$. Так как $q_i$ — любой простой делитель $S$, то $p - 1$ делится на $S$. □

В следующей теореме приводится пример условия, гарантирующего простоту числа $N$.

**Теорема 5.1.** В условиях леммы 5.1 пусть выполнено неравенство

$$R \leqslant S + 1.$$

Тогда $N$ — простое число.

Доказательство. Действительно, пусть $p$ — наименьший простой делитель числа $N$. Если $N$ — составное число, то

$$N = pN_1 \geqslant p^2 \geqslant (S+1)^2 = S(S+2) + 1 > SR + 1 = N,$$

что невозможно. □

**Пример 5.3.** Покажем, что число

$$N = \underbrace{11111111111111111111}_{\text{23 единицы}}$$

является простым.

Перебором небольших простых делителей находим

$$N - 1 = 2 \cdot 5 \cdot 11^2 \cdot 23 \cdot 4093 \cdot 8779 \cdot R,$$

где $R = \underbrace{11111111111}_{\text{11 единиц}}$. Для каждого простого делителя

$$q_i \in \{2, 5, 11, 23, 4093, 8779\}$$

можно указать такое $a_i \in \mathbb{Z}$, что выполнено условие (5.8):

| $q_i$ | 2 | 5 | 11 | 23 | 4093 | 8779 |
|---|---|---|---|---|---|---|
| $a_i$ | 7 | 2 | 2 | 2 | 2 | 2 |

Так как $R \leqslant 1\underbrace{0000000000}_{\text{10 нулей}}11 = S + 1$, то $N$ — простое число.

**Замечание 5.1.** Если $S$ нечётно, то в условиях леммы 5.1 верно сравнение

$$p \equiv 1 \pmod{2S}.$$

В этом случае в теореме 5.1 можно требовать, чтобы $R \leqslant 4S + 2$.

Покажем, как с помощью теоремы 5.1 можно без особых вычислительных затрат строить большие простые числа.

**Пример 5.4.** Начиная с небольшого простого числа

$$S^{(0)} = 63766529,$$

взятого из таблицы простых чисел, мы последовательно находим простые числа

$$S^{(k)} = S^{(k-1)} R^{(k)} + 1.$$

Чётные числа $R^{(k)}$ при этом подбираются так, чтобы

$$R^{(k)} \leqslant 4S^{(k-1)} + 2$$

и для некоторых $a_k \in \mathbb{Z}$ были справедливы соотношения

$$a_k^{S^{(k)}-1} \equiv 1 \pmod{S^{(k)}}, \quad \text{НОД}\,(a_k^{R^{(k)}} - 1, S^{(k)}) = 1. \tag{5.9}$$

Имеем

$R^{(1)} = 70770834,$

$S^{(1)} = 4512810438615187,$

$R^{(2)} = 16595399667898434,$

$S^{(2)} = 74891892854283060614549525917159,$

$R^{(3)} = 18507193633339516211048593097738 8,$

$S^{(3)} = 13860387626215326678854874421478606308305311334707\backslash$
$747109990200693,$

$R^{(4)} = 42378727533781801960162680892611644777523641072783\backslash$
$336534883902610,$

$S^{(4)} = 58738559072398005552656622556731799674072703413590\backslash$
$63785326808519195953944340929962449243226042298109\backslash$
$51076664738559313528966508731,$

$R^{(5)} = 12817888374282574282507855019642174889455963762363\backslash$
$86323812708497876581255089773742452766244396067877\backslash$
$61625060838989198856257857196 8,$

$S^{(5)} = 75290429345620062585961289159277838795453330799438\backslash$
$86129444961628512905368666999969290917432675517124\backslash$
$66689571071799483872441239435776315998897745339218\backslash$
$16819695640973494997260310783719905034389980059085\backslash$
$22505029891693589241550796725471047933413083127845\backslash$
$83852609.$

Здесь выполнение условия (5.9) проверялось при одном и том же значении $a_k = 1999$.

**Упражнение 5.3.** Пусть $q$ — простое число, $R < q$ — натуральное число. Положим

$$N = q^2R + 1.$$

Докажите, что если $2^R \not\equiv 1 \pmod N$ и $2^{N-1} \equiv 1 \pmod N$, то $N$ — простое число.

*Решение.* Пусть $p$ — произвольный простой делитель $N$. Ясно, что $p \neq q$.

Если $p$ таков, что $2^R \equiv 1 \pmod p$, то мы имеем

$$\nu_p(N) \leqslant \nu_p(2^{N-1} - 1) = \nu_p(2^R - 1),$$

откуда $2^R \equiv 1 \pmod{p^{\nu_p(N)}}$.

Если же $2^R \not\equiv 1 \pmod p$, то верно сравнение $p \equiv 1 \pmod q$ (почему?). Отметим, что такие $p$ обязательно найдутся, так как иначе мы получили бы $2^R \equiv 1 \pmod N$.

Пусть теперь $N = N_1N_2$, где $N_1$ (соответственно $N_2$) — произведение $p^{\nu_p(N)}$ по всем $p$, для которых верно (соответственно неверно) сравнение $2^R \equiv 1 \pmod p$. Так как $N_2 \equiv 1 \pmod q$ и $N \equiv 1 \pmod q$, то $N_1 \equiv 1 \pmod q$. Положив $N_i = qR_i + 1$, получим

$$q^2R + 1 = (qR_1 + 1)(qR_2 + 1),$$

откуда $R_1 + R_2 \equiv 0 \pmod q$ и, как следствие, $R_1 + R_2 \geqslant q$. Как уже было отмечено, $R_2 > 0$. Если также $R_1 > 0$, то

$$qR = qR_1R_2 + R_1 + R_2 \geqslant q(R_1R_2 + 1) \geqslant q^2,$$

что невозможно. Таким образом, $R_1 = 0$, так что $N = N_2$. По аналогичным соображениям $N_2$ может быть только простым числом. □

## 5.2 Псевдопростые числа

Псевдопростые числа. Числа Кармайкла (абсолютно псевдопростые числа). Строго псевдопростые числа. Тест Миллера — Рабина строгой псевдопростоты и его сравнение с тестом Соловея — Штрассена псевдопростоты по Эйлеру.

Здесь мы рассмотрим вопрос о том, как отличить составное число от простого. Разумеется, речь идёт о больших по величине числах, иначе вопрос решается с помощью *алгоритма пробных делений* (см. пример 1.6).

Отправной точкой может послужить та же малая теорема Ферма. Предположим, что для данного нечётного $N > 1$ нам удалось подобрать такое $a \in \mathbb{Z}$, НОД $(a, N) = 1$, что

$$a^{N-1} \not\equiv 1 \pmod{N}.$$

Тогда, очевидно, $N$ — составное число. Если же, напротив, имеет место сравнение

$$a^{N-1} \equiv 1 \pmod{N}, \tag{5.10}$$

то число $N$ может (но не обязано!) быть простым.

Так, в древнем Китае (примерно 25 веков назад) полагали, что любое нечётное число $N > 1$ является простым, если для него выполняется сравнение

$$2^{N-1} \equiv 1 \pmod{N}.$$

Основания так считать были, поскольку для небольших $N$ этот критерий действительно справедлив. Интересно отметить, что много позже, в 1680 году, Г. Лейбниц (1664 — 1716), один из создателей математического анализа, переоткрыл эту «теорему китайцев» и даже нашёл для неё доказательство (ошибка в этом доказательстве легко обнаруживается). Только в 1819 году французский математик П. Саррюс (1798 — 1861) обнаружил первый контрпример к ней — составное число

$$N = 341 = 11 \cdot 31,$$

для которого указанное сравнение имеет место (см. выше пример 5.2).

Корректный способ обратить малую теорему Ферма предложил в 1876 году Э. Люка.

**Теорема 5.2.** Если существует такое $a \in \mathbb{Z}$, что

$$a^{N-1} \equiv 1 \pmod{N},$$

но для любого простого делителя $q$ числа $N - 1$ имеем

$$a^{(N-1)/q} \not\equiv 1 \pmod{N},$$

то $N$ — простое число.

Доказательство. Имеем $[a] \in \mathbb{Z}_N^*$, причём порядок этого класса вычетов равен $N - 1$. Но в таком случае число $N - 1$ должно быть делителем $\varphi(N)$. Так как $\varphi(N) \leqslant N - 1$, то

$$\varphi(N) = N - 1.$$

Это возможно только тогда, когда $N$ — простое число. □

**Упражнение 5.4.** Убедитесь, что условие теоремы 5.2 является не только достаточным, но и необходимым для простоты числа $N$.

*Указание.* В качестве $a$ можно взять первообразный корень $g$ по модулю $N$ (см. упражнение 4.14).

Итак, теорема Люка фактически даёт нам *критерий простоты* числа $N$. К сожалению, эффективно применить его можно только тогда, когда известны все простые делители числа $N-1$. Однако разложить на множители $N-1$, как правило, практически столь же сложно, как и само число $N$.

**Определение 5.1.** Нечётное составное число $N$ называют *псевдопростым по основанию* $a \in \mathbb{Z}$, если выполняется сравнение (5.10).

Таким образом, число 341 — псевдопростое по основанию 2. И таких чисел — контрпримеров к «теореме китайцев» — существует бесконечно много.

**Упражнение 5.5.** Докажите, что если $N$ — псевдопростое число по основанию 2, то это же справедливо и для числа $M = 2^N - 1$.

*Решение.* Так как число $N$ — составное, $N = N_1 N_2$, то число

$$M = (2^{N_1} - 1)(2^{N_1(N_2-1)} + \ldots + 2^{N_1} + 1)$$

также составное. Имеем $2^{N-1} - 1 = Nq$ для некоторого натурального $q$, поэтому

$$2^{M-1} - 1 = 2^{2^N-2} - 1 = 2^{2(2^{N-1}-1)} - 1 = 2^{2qN} - 1 =$$
$$= (2^N - 1)(2^{(2q-1)N} + \ldots + 2^N + 1) \equiv 0 \pmod{M}.$$

Значит, число $M$ — псевдопростое по основанию 2. □

Можно показать, что существует бесконечно много псевдопростых чисел по любому заданному основанию $a > 1$. Действительно, пусть $p$ — произвольное нечётное простое число, не делящее $a^2 - 1$. Тогда число

$$N = \frac{a^{2p} - 1}{a^2 - 1} = a^{2(p-1)} + \ldots + a^2 + 1$$

будет псевдопростым по основанию $a$.

**Упражнение 5.6.** Докажите это утверждение.

*Решение.* Имеем

$$N = \frac{a^p - 1}{a - 1} \cdot \frac{a^p + 1}{a + 1},$$

так что $N$ — составное число. Из определения $N$ также следует, что

$$a^{2p} \equiv 1 \pmod{N}.$$

Теперь достаточно увидеть, что $N - 1$ делится на $2p$. В самом деле,

$$N - 1 = \frac{a^{2p} - a^2}{a^2 - 1}$$

чётно (поскольку $N$ нечётно) и делится на $p$ по малой теореме Ферма. □

При $a = 2$ и $p = 5$ получим $N = 341$ — первое псевдопростое число по основанию 2.

Заметим, что число 341, будучи псевдопростым по основанию 2, не будет псевдопростым, например, по основанию 3, поскольку

$$3^{340} \equiv 56 \not\equiv 1 \pmod{341}.$$

**Упражнение 5.7.** Найдите наименьшее псевдопростое число по основанию 3.
*Ответ.* 91.

Итак, мы можем пытаться обосновать непростоту числа $N$, варьируя основание $a$. Увы, такой подход не всегда приводит к успеху. Как оказывается, существуют нечётные составные числа $N$, которые удовлетворяют сравнению (5.10) при любом $a \in \mathbb{Z}$, НОД $(a, N) = 1$.

**Определение 5.2.** Эти числа называются *числами Кармайкла*, или *абсолютно псевдопростыми числами*.

Первый (и наименьший) пример абсолютно псевдопростого числа предложил сам Кармайкл в 1910 году: это число

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

В корректности этого примера легко убедиться с помощью малой теоремы Ферма, заметив, что $560 = 561 - 1$ делится на $2 = 3 - 1$, на $10 = 11 - 1$ и на $16 = 17 - 1$.

Другие примеры абсолютно псевдопростых чисел:

$$1105 = 5 \cdot 13 \cdot 17, \quad 1729 = 7 \cdot 13 \cdot 19.$$

Оказывается, любое число Кармайкла имеет вид

$$N = \prod_{i=1}^{t} p_i,$$

где $t \geqslant 3$ и простые числа $p_i$ различны, причём $N - 1$ делится на каждую разность $p_i - 1$.

**Упражнение 5.8.** Докажите это утверждение, известное как *критерий Корсельта*.
*Решение.* Пусть $p$ — простое число,

$$N = p^{\alpha} N_1, \quad \text{НОД}\,(N_1, p) = 1,$$

причём $\alpha \geqslant 2$. Положим $a = 1 + pN_1$. Из сравнения (5.10) следует, что

$$1 \equiv (1 + pN_1)^{N-1} \equiv 1 + (N-1)pN_1 \pmod{p^2},$$

откуда $(N-1)N_1 \equiv 0 \pmod{p}$, что невозможно.

Итак, если $N$ — число Кармайкла, то оно обязано быть свободно от квадратов. Пусть теперь $p$ — произвольный простой делитель числа $N$. Поскольку

$$\text{НОД}\,(p, N/p) = 1,$$

можно найти такой первообразный корень $a$ по модулю $p$, который взаимно прост с $N/p$. Из сравнения (5.10) следует, что

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

Порядок $a$ по модулю $p$ равен $p - 1$, поэтому $N - 1$ делится на $p - 1$. □

**Упражнение 5.9.** Докажите, что если $N$ — число Кармайкла, то

$$a^N \equiv a \pmod{N}$$

для любого $a \in \mathbb{Z}$.

*Указание.* Докажите, что $a^N \equiv a \pmod{p}$ для любого простого делителя $p$ числа $N$.

Относительно недавно (1995 год) было доказано, что чисел Кармайкла существует бесконечно много.

В 1976 году Миллер предложил вместо (5.10) проверять несколько иное условие. Если $N$ — нечётное простое число,

$$N - 1 = 2^l R,$$

где $R$ нечётно, то для каждого $a \in \mathbb{Z}$ с условием НОД $(a, N) = 1$ в произведении

$$(a^R - 1)\prod_{i=0}^{l-1}(a^{2^i R} + 1) = a^{N-1} - 1 \equiv 0 \pmod{N}$$

по крайней мере один из сомножителей делится на $N$. Обращение этого свойства можно использовать, чтобы отличать составные числа от простых.

**Определение 5.3.** Нечётное составное число $N$ называют *строго псевдопростым по основанию* $a \in \mathbb{Z}$, если либо

$$a^R \equiv 1 \pmod{N}, \tag{5.11}$$

либо для некоторого $i = 0, 1, \ldots, l-1$ имеем

$$a^{2^i R} \equiv -1 \pmod{N}. \tag{5.12}$$

**Пример 5.5.** Число $3277 = 29 \cdot 113$ является строго псевдопростым по основанию 2.
Действительно, имеем $3276 = 2^2 \cdot 819$. Тогда

$$2^{819} \equiv 128 \not\equiv \pm 1 \pmod{3277}, \quad 2^{2\cdot 819} \equiv 128^2 \equiv -1 \pmod{3277}.$$

Кстати, наименьшее строго псевдопростое число по основанию 2 — это $2047 = 23 \cdot 89$.

**Упражнение 5.10.** Проверьте этот факт.

Как доказал Рабин в 1980 году, если $N$ — нечётное составное число, то количество тех оснований $a$, $1 \leqslant a \leqslant N-1$, по которым оно окажется строго псевдопростым, не превосходит $(N-1)/4$ (доказательство можно найти, например, в книге [2], стр. 38).

Следующий вероятностный алгоритм, отличающий составные числа от простых, известен как *тест Миллера — Рабина*.

**А.** Выберем случайным образом основание $a$, $1 \leqslant a \leqslant N-1$, и проверим, будут ли выполнены сравнение (5.11) и сравнения (5.12).

**Б.** Если ни одно из них не имеет места, то число $N$ — составное.

**В.** Если хотя бы одно из сравнений верно, возвращаемся к шагу А.

Из сказанного выше следует, что составное число не будет определено как составное после однократного выполнения шагов А — В с вероятностью $< 4^{-1}$. А вероятность не определить его как составное после $k$ итераций будет $< 4^{-k}$, т. е. с ростом $k$ убывает очень быстро.

Опишем ещё один классический вероятностный тест, который основан на другом понятии псевдопростоты.

**Определение 5.4.** Нечётное составное число $N$ называется *псевдопростым числом Эйлера по основанию* $a \in \mathbb{Z}$, НОД $(a, N) = 1$, если

$$a^{(N-1)/2} \equiv (a/N) \pmod{N}. \tag{5.13}$$

Это понятие было введено Робинсоном в 1957 году. Здесь $(a/N)$ — так называемый *символ Якоби*, который может быть быстро вычислен (см., например, [3, гл. 5]). Для простых $N$ символ Якоби превращается в *символ Лежандра* и сравнение (5.13) выполняется по *критерию Эйлера* (см. там же).

Следующий вероятностный алгоритм называется *тест Соловея — Штрассена*.

**А.** Выберем случайное основание $a$, $1 \leqslant a \leqslant N-1$, и проверим сравнение (5.13).

**Б.** Если оно не выполнено, то число $N$ — составное.

**В.** Если сравнение (5.13) имеет место, возвращаемся к шагу А.

Авторы теста доказали, что если $N$ — нечётное составное число, то число тех оснований $a$, $1 \leqslant a \leqslant N-1$, по которым оно будет псевдопростым числом Эйлера, не превосходит $\varphi(N)/2$ (доказательство см. в книге [2], стр. 37). Таким образом, если тест Соловея — Штрассена применить к составному числу $k$ раз, то вероятность ошибки (не определить его как составное) будет $< 2^{-k}$.

На практике оба теста работают очень хорошо (в частности, они оба справляются с числами Кармайкла). Отметим, что второй тест слабее первого: если составное число прошло один цикл теста Миллера — Рабина и не определилось как составное, то тест Соловея — Штрассена даст тот же результат. Другими словами, справедлива следующая

**Теорема 5.3.** Если $N$ — строго псевдопростое число по основанию $a$, то $N$ — псевдопростое число Эйлера по основанию $a$.

Доказательство теоремы 5.3 можно найти в статье [9]. Читателю, желающему более основательно познакомиться с проблемами алгоритмической теории чисел, а также её приложениями к криптографии, рекомендуется обратиться к книгам [2], [5] и [7].

# Заключение

По разным причинам за рамками настоящего учебного пособия остались такие традиционно излагаемые разделы элементарной теории чисел как «Квадратичные вычеты» и «Непрерывные дроби» (последний тесно связан с алгоритмом Евклида). Кроме этого, тема «Первообразные корни» обычно подразумевает и рассказ об индексах (дискретных логарифмах).

В планируемом более полном учебном пособии по курсу теории чисел авторы надеются восполнить эти пробелы, а сейчас отсылают читателя к классическим учебникам [1] и [3], где указанные разделы присутствуют (см. также учебное пособие [6] или, весьма оригинальное по стилю изложения, учебное пособие [8]).

# Список литературы


[1] *Бухштаб А.А.* Теория чисел. М.: Просвещение, 1966.

[2] *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2006.

[3] *Виноградов И.М.* Основы теории чисел. М.: Наука, 1981.

[4] *Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б.* Введение в теорию чисел. М.: Изд-во МГУ, 1995.

[5] *Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В.* Введение в теоретико-числовые методы криптографии. СПб.: Изд-во «Лань», 2011.

[6] *Нестеренко Ю.В.* Теория чисел. М.: Академия, 2008.

[7] *Ростовцев А.Г., Маховенко Е.Б.* Теоретическая криптография. СПб.: Изд-во «Профессионал», 2005.

[8] *Сизый С.В.* Лекции по теории чисел. М.: ФИЗМАТЛИТ, 2007.

[9] *Monier L.* Evaluation and comparison of two efficient probabilistic primality testing algorithms // Theor. Comput. Sci. 1980. V. 12. P. 97 — 108.