ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ КОСМИЧЕСКИХ И ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ

Н. Н. Осипов

ТЕОРИЯ ЧИСЕЛ

Красноярск, 2008

ТЕОРИЯ ЧИСЕЛ

Конспект лекций

Красноярск, 2008

УДК 511.2

Н. Н. Осипов

Конспект лекций составлен в соответствии с учебной программой дисциплины «Теория чисел» и включает следующие разделы: теория делимости, теория сравнений, кольца классов вычетов, некоторые приложения теории сравнений.

Предназначен для студентов направления 220900.62 Прикладная математика.

Эта книга не для тех студентов, которые хотели бы «побыстрее выучить, чтобы сдать». Побыстрее не получится, поскольку автор заставляет читателя буквально продираться сквозь многочисленные упражнения. Более шестидесяти упражнений сопровождают изложение. Этот учебник для тех, кто хотел бы овладеть идеями и методами теории чисел; для таких читателей решение упражнений стало бы хорошей школой усвоения материала. [...]

В процессе чтения читатель порой уводится далеко за пределы собственно элементарной теории чисел и попадает в область высшей алгебры, математического анализа и теории функций комплексного переменного. [...]

Автор не довольствуется одним доказательством какого-нибудь теоретико-числового факта, демонстрируя разные точки зрения на этот факт и предоставляя элементарные и совсем не элементарные методы его доказательства. Видно, что автор не отказывает себе в удовольствии сообщить читателю короткие «культурные» доказательства некоторых классических теорем элементарной теории чисел, которые, правда, требуют большего багажа общематематических знаний и, в целом, большей математической культуры. [...]

Из рецензии профессора С. В. Ларина.

Содержание

Предисловие 6

I. Теория делимости 8

§1. Делимость целых чисел. Наибольший общий делитель 8
§2. Взаимно простые числа. Наименьшее общее кратное. Китайская теорема об остатках 15
§3. Простые и составные числа 19
§4. Основная теорема арифметики и её следствия 22
§5. Мультипликативные функции 25
§6. Целая и дробная часть числа 31
§7. Оценки Чебышёва 37
§8. Асимптотический закон распределения простых чисел 47

II. Теория сравнений 54

§1. Определение и свойства сравнений 54
§2. Классы вычетов. Теоремы Ферма и Эйлера 59
§3. Сравнения с неизвестными 69
§4. Сравнения первой степени 75

III. Кольца классов вычетов 82

§1. Кольцо Z_m классов вычетов по модулю m 82
§2. Группа обратимых элементов кольца Z_m 87
§3. Поле Z_p классов вычетов по простому модулю p 91
§4. Порядок класса вычетов. Первообразные корни 95

IV. Некоторые приложения теории сравнений 101

§1. Система шифрования RSA 101
§2. Псевдопростые числа 109

Заключение 116

Список литературы 117

Предисловие

Настоящий конспект лекций составлен в соответствии с учебной программой дисциплины «Теория чисел» и предназначен для студентов направления 220900.62 Прикладная математика.

Учебная программа курса теории чисел составлена с учётом того, что этот курс будет читаться студентам во 2-м семестре. Поэтому основное внимание в лекциях уделяется *элементарной теории чисел*, а именно, следующим её главам: теории делимости (1-й раздел) и теории сравнений (2-й раздел).

Поскольку параллельно студенты знакомятся с элементами высшей алгебры, у лектора появляется возможность привлекать алгебраические методы для изучения колец и полей классов вычетов (3-й раздел). Эти объекты, хотя и являются алгебраическими по своей природе, естественным образом возникают в теории чисел и занимают в ней важное место. По мнению автора, «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.).

4-й раздел посвящён некоторым вопросам *алгоритмической теории чисел*, имеющим прикладное значение. В частности, рассматривается приложение теории сравнений к криптографии. В связи с этим невозможно было не затронуть вопросы распределения простых чисел, традиционно относящиеся к *аналитической теории чисел*. Этому посвящены последние две лекции 1-го раздела, представляющие 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 чем шести десятков упражнений, равномерно распределённых по всему тексту лекций, отводится важная роль, и этим не стоит пренебрегать даже при

первом чтении лекций.

Автор выражает свою искреннюю благодарность доктору физико-математических наук, профессору Ю. В. Нестеренко, чьи лекции по теории чисел автор, ещё будучи студентом, с большим интересом прослушал. Автор весьма признателен профессору С. В. Ларину за многочисленные полезные обсуждения различных учебно-методических вопросов, связанных с курсом теории чисел, и тщательное прочтение первоначального текста рукописи, приведшее, в частности, к устранению многих мелких неточностей и опечаток.

I. Теория делимости

§ 1. Делимость целых чисел. Наибольший общий делитель

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

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

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

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. 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 (см. определение 1) называется *частным* от деления a на b.

Перечислим теперь простейшие *свойства отношения делимости*, непосредственно вытекающие из определения 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* $c \mid a$.

Замечание. 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.

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. Имеем $a = bq$ для некоторого $q \in \mathbb{Z}$. Так как $a \neq 0$, то и $q \neq 0$. Следовательно, $|q| \geqslant 1$ и поэтому

$$|a| = |b| \cdot |q| \geqslant |b|.$$

Упражнение 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 можно использовать так называемое *деление с остатком*.

Определение 2. Пусть $a,\ b \in \mathbb{Z}$, $b \neq 0$. *Разделить* a *на* b *с остатком* — это значит представить число a в виде

$$a = bq + r, \tag{1}$$

где $q,\ r \in \mathbb{Z}$ и выполнено условие $0 \leqslant r < |b|$.

В равенстве (1) число a называют *делимым*, число b — *делителем*, число q — *неполным частным*, число r — *остатком от деления*.

Пример 1. $16 = 7 \cdot 2 + 2$, $-41 = 5 \cdot (-9) + 4$.

Теорема 1. *Для любых* $a,\ b \in \mathbb{Z}$, $b \neq 0$, *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:

$$a = (-b)q + r, \tag{2}$$

где $0 \leqslant r < -b = |b|$. Осталось переписать (2) в виде $a = b(-q) + r$.

Покажем теперь, что деление с остатком возможно только единственным образом. Пусть

$$a = \boxed{bq_1 + r_1 = bq_2 + r_2},$$

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. Но $|r_2 - r_1| < |b|$, поэтому $r_2 - r_1 = 0$, т. е. $r_2 = r_1$, а значит, и $q_2 = q_1$. □

Замечание. Если остаток от деления равен нулю, то говорят о *делимости нацело* (в этом случае a делится на b в смысле определения 1).

Пусть $a_1, \ldots, a_n \in \mathbb{Z}$ и не все равны нулю.

Определение 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 НОД $(a_1, \ldots, a_n) =$ 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. *Если a, b, q, $r \in \mathbb{Z}$ связаны соотношением $a = bq + r$, 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. Вытекает из свойств отношения делимости: если d — общий делитель a и b, то d делит и $r = a - bq$, т. е. является общим делителем b и r; обратное утверждение столь же очевидно. □

Лемма 2. *Если a делится на $b > 0$, то* НОД $(a, b) = b$. *В частности,* НОД $(0, b) = b$.

Доказательство. Утверждение леммы очевидно. □

Упражнение 2. Тем не менее, проведите формальное доказательство леммы 2 (очевидно то, что очевидно доказывается).

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

Теорема 2. *Пусть* $a \geqslant b \geqslant 1$. *Если* a *делится на* b, *то* НОД $(a, b) = b$. *Иначе, считая* $r_{-1} = a$, $r_0 = b$, *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. Применяя n раз лемму 1 и один раз лемму 2, получим следующую цепочку равенств:

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

Для завершения доказательства нужно ещё объяснить, почему указанное в формулировке число n действительно найдётся (деления с остатком не могут продолжаться бесконечно). □

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

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

Таким образом, $d = 21$.

Обсудим вопрос о *вычислительной сложности* алгоритма Евклида.

Лемма 3. *Пусть $a \geqslant b \geqslant 1$. Тогда остаток от деления a на b удовлетворяет неравенству $r < a/2$.*

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. □

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

Теорема 3. *Пусть $a \geqslant b \geqslant 1$. Если a не делится на b, то для количества делений с остатком в алгоритме Евклида справедливо неравенство*

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

Доказательство. Рассуждая по индукции (шаг индукции делается на основе леммы 3), получим

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

В частности, для любого $k = 1, \ldots, n$ выполняется неравенство

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

Полагая $k = n$ и учитывая очевидное неравенство $r_n \geqslant 1$, будем иметь

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

что равносильно доказываемому неравенству. □

Замечание. Пусть $\{F_k\}$ — *последовательность Фибоначчи*, определяемая рекуррентным правилом:

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

Если применить алгоритм Евклида к паре чисел

$$a = F_{k+1}, \quad b = F_k,$$

где $k \geqslant 3$, то, как легко убедиться, получим $n = k - 2$. Из *формулы Бине*

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

следует неравенство $F_k < C\Phi_+^k$, где константа C не зависит от k. Следовательно,

$$n = k - 2 > \log_{\Phi_+} \frac{b}{C} - 2 \geqslant C_1 \log_2 b,$$

где константа C_1 не зависит от b. Таким образом, оценка для параметра n, указанная в теореме 3, *неулучшаема по порядку*, т. е. не слишком груба. Тем не менее, её можно улучшить до

$$n < 5 \lg b.$$

Это утверждение в 1845 году доказал французский математик и инженер Г. Ламе (1795 — 1870).

Следующее утверждение известно под названием *теоремы о линейном представлении*.

Теорема 4. *Существуют такие* $x_0,\ y_0 \in \mathbb{Z}$, *что*

$$\text{НОД}\,(a, b) = ax_0 + by_0.$$

Доказательство. Пусть d — *наименьшее* натуральное число, которое можно представить в виде $ax + by$, где $x,\ y \in \mathbb{Z}$. По определению, $d = ax_0 + by_0$ для некоторых $x_0,\ y_0 \in \mathbb{Z}$.

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

Упражнение 3. Закончите доказательство теоремы 4.

Указание. Нужно 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. Пара (x_0, y_0) определяется неоднозначно: всегда можно заменить x_0 на $x_0 + tb$, а y_0 — на $y_0 - ta$.

Пример 3. Найдём линейное представление $\text{НОД}\,(525, 231)$.

Как следует из примера 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 $y_0 = -9$. (Здесь мы фактически изложили другое — *конструктивное* — доказательство теоремы 4.)

Перечислим другие свойства наибольшего общего делителя двух чисел, непосредственно вытекающие из алгоритма Евклида (далее a, b и 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* $\text{НОД}\,(a/c, b/c) = \text{НОД}\,(a, b)/c$.

Замечание. Свойство 3 — лишь иная форма записи свойства 2.

Вернемся 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 4. Сформулируйте её и докажите.

Указание. Можно рассуждать неконструктивно (см. доказательство теоремы 4).

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

Теорема 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 5 и рассуждая по индукции, можно получить свойства наибольшего общего делителя, аналогичные указанным выше свойствам 2 и 3. Теорема 5 вместе с алгоритмом Евклида дают также практический способ вычисления наибольшего общего делителя нескольких чисел. Ещё один способ представлен в следующем упражнении.

Упражнение 5. Пусть на доске написаны несколько натуральных чисел. К ним применяют такую операцию: выбирают произвольно два числа и *наибольшее* из них заменяют *остатком* от деления на *наименьшее* из них (если остаток равен нулю, его затем 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 4. Покажем этим способом, что НОД $(5, 34, 52, 15) = 1$:

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

§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 (НОК) целых чисел: свойства и алгоритм вычисления. Китайская теорема об остатках.

Определение 4. Если НОД $(a_1, \ldots, a_n) = 1$, то числа $a_1, \ldots, a_n$ называются *взаимно простыми*.

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

Для двух чисел имеет место следующий *критерий взаимной простоты*.

Теорема 6. *Числа $a,\ b \in \mathbb{Z}$ взаимно просты тогда и только тогда, когда существуют такие $x_0,\ y_0 \in \mathbb{Z}$, что*

$$ax_0 + by_0 = 1.$$

Доказательство. Утверждение «только тогда» является частным случаем теоремы 4. Утверждение «тогда» очевидно. □

Замечание. Аналогичный критерий верен и для произвольного количества чисел $a_1, \ldots, a_n$.

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

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

2. *Пусть* НОД $(a, b) = 1$. *Если $a \mid c$ и $b \mid c$, то $ab \mid c$.*

3. *Если* НОД $(a, b) = 1$, *то* НОД $(ac, b) =$ НОД (c, b) *для любого c.*

4. *Если* НОД $(a, c) = 1$ *и* НОД $(b, c) = 1$, *то* НОД $(ab, c) = 1$.

Доказательство. Идея доказательства — воспользоваться критерием взаимной простоты (теорема 6).

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

$$ax_0 + by_0 = 1.$$

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

2. Имеем $c = ac_1$ для некоторого $c_1 \in \mathbb{Z}$. Так как $b \mid ac_1$ и НОД $(a, b) = 1$, то $b \mid c_1$ (свойство 1), т. е. $c_1 = bc_2$ 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, НОД $(ac, b) =$ НОД (c, b).

4. По свойству 3 имеем НОД $(ab, c) =$ НОД $(b, c) = 1$. Впрочем, свойство 4 нетрудно доказать и непосредственно. Обозначим $d =$ 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 6. Если 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 5. Если НОД $(a_i, a_j) = 1$ для всех $i \neq j$, то числа $a_1, \ldots, a_n$ называются *попарно взаимно простыми*.

Упражнение 7. Обобщите и докажите свойство 2, используя понятие попарно взаимно простых чисел.

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

Определение 6. Аналогично определению наибольшего общего делителя, наименьшее (по величине) положительное общее кратное чисел $a_1, \ldots, a_n$ называется их *наименьшим общим кратным*.

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

Если $m = \text{НОК}(a_1, \ldots, a_n)$, то числа $m/a_1, \ldots, m/a_n$ взаимно просты. Это утверждение вытекает непосредственно 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.

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

Теорема 7. *Справедлива формула*

$$\text{НОК}(a, b) = \frac{ab}{\text{НОД}(a, b)}. \tag{3}$$

Доказательство. Пусть $d = \text{НОД}(a, b)$ и $m = ab/d$. Нужно доказать равенство $m = \text{НОК}(a, b)$.

Пусть $M > 0$ — *произвольное* общее кратное чисел a и b, т. е.

$$M = aq_1 = bq_2,$$

где q_1, q_2 — натуральные числа. Сокращая 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, например, что q_1 делится на b_1, т. е. $q_1 = b_1 q_3$ для некоторого натурального q_3. Но тогда

$$M = aq_1 = ab_1 q_3 = mq_3.$$

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

Между прочим, доказывая формулу (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 также можно принять за определение наименьшего общего кратного (ср. с аналогичным свойством наибольшего общего делителя).

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

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

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

Другое, более короткое доказательство формулы (3) состоит в следующем. Пусть $m = \text{НОК}(a, b)$ и $d = ab/m$. Тогда $d = \text{НОД}(a, b)$.

Упражнение 8. 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 (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 9. Выведите свойства 2 и 3 из свойства 1.

Перейдём к вопросу о наименьшем общем кратном нескольких чисел.

Теорема 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 5. □

Теорема 8 в комбинации с формулой (3) и алгоритмом Евклида позволяет практически находить наименьшее общее кратное нескольких чисел.

Упражнение 10. Распространите свойства 2 и 3 наименьшего общего кратного с двух чисел на произвольное их количество.

Упражнение 11. Докажите, что наименьшее общее кратное попарно взаимно простых чисел равно их произведению.

Рассмотрим одну задачу, популярную в Древнем Китае: *найти число* r, *если известны 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 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.

Доказательство. Рассмотрим отображение множества R_m в множество $R_{m_1} \times R_{m_2}$, заданное правилом:

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

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

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

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

Упражнение 12. Проведите подробное рассуждение.

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

Упражнение 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. В конце § 4 раздела II будет предложено конструктивное доказательство китайской теоремы об остатках, пригодное для практического отыскания числа r.

§3. Простые и составные числа

Понятие простого и составного целого числа. Метод Евклида доказательства бесконечности множества простых чисел и его приложения. Алгоритм выписывания начального отрезка ряда простых чисел (решето Эратосфена). Характеристическое свойство простых чисел.

Определение 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 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 Евклидом (см. «Начала», книга IX).

Лемма 4. *Пусть N — натуральное число, большее единицы. Наименьший натуральный делитель $p > 1$ числа N является простым числом.*

Доказательство. Действительно, иначе у p найдется натуральный делитель p_1, $1 < p_1 < p$, который будет и делителем N. Это противоречит определению p. □

Следующее утверждение известно как *теорема Евклида*.

Теорема 10. *Простых чисел бесконечно много.*

Доказательство. Допустим противное и 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 (см. лемму 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 14. Методом 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 один из последних рекордов (август 2008 года):

$$2^{43112609} - 1.$$

Десятичная запись этого монстра содержит почти 13 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 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. *Если $N > 1$ не делится на все простые числа $p \leqslant \sqrt{N}$, то N — простое число.*

Пример 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 *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 помогает лемма 5), а любое вычеркнутое число — очевидно, составное.

Пример 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

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

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

Упражнение 15. Докажите это.

Одно из возможных доказательств основной теоремы арифметики (см. § 4) опирается на следующее *характеристическое свойство* простых чисел.

Лемма 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 и их произведение будет взаимно простым с p (см. упражнение 6), а оно по условию делится на p. □

§4. Основная теорема арифметики и её следствия

Основная теорема арифметики и её различные доказательства. Пример Гильберта, или почему нужно доказывать основную теорему арифметики. Каноническое разложение целого 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 11. *Всякое натуральное число, отличное от единицы, разлагается в произведение простых чисел. Разложение единственно с точностью до порядка сомножителей.*

Иными словами, все натуральные числа получаются из простых чисел с помощью всевозможных умножений, причем в результате различных умножений получаются различные числа.

Доказательство. Нетрудно понять, почему указанное разложение *существует*. Для этого достаточно рассмотреть *самое длинное* разложение данного числа $m > 1$ в произведение натуральных чисел, больших единицы: оно обязано состоять только из простых сомножителей.

Сложнее доказать *единственность* разложения в произведение простых. Пусть

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

— два таких разложения. По лемме 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 получаем

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

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 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 больше 1 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.

Этот пример проливает свет на логическую структуру *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 множители 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 двух 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

$$m' = pp_1QR\ldots$$

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

Определение 8. Представление вида

$$m = p_1^{\alpha_1}\ldots p_t^{\alpha_t}, \tag{4}$$

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

Пример 9. $588000 = 2^5 \cdot 3^1 \cdot 5^3 \cdot 7^2$.

Если известно каноническое разложение (4) числа m, то можно легко указать *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 хорошо известные правила составления НОД и НОК нескольких чисел, канонические разложения которых предполагаются известными.

1. НОД нескольких чисел равен произведению степеней вида p^α, где p — простой делитель *всех* этих чисел, а α — *наименьший* из показателей, с которыми p входит в их канонические разложения.

2. НОК нескольких чисел равно произведению степеней вида p^α, где p — простой делитель *хотя бы одного* из этих чисел, а α — *наибольший* из показателей, с которыми p входит в их канонические разложения.

Пример 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

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

Замечание. Из основной теоремы арифметики можно вывести (и ещё раз осознать, взглянув с иной 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. § 2): 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 содержится в каноническом разложении c.

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

§ 5. Мультипликативные функции

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

Определение 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 11. Функция

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

является мультипликативной при любом вещественном (или 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

$$\xi(m) = \xi(p_1^{\alpha_1}) \ldots \xi(p_t^{\alpha_t}). \qquad (5)$$

3. Мультипликативная функция $\xi(m)$ может быть задана следующим способом: произвольно задаём значения вида $\xi(p^\alpha)$, где p — простое, α — натуральное, остальные значения определяем формулой (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 9 и предоставляется читателю как

Упражнение 16.

В следующей теореме указан ещё один способ конструирования мультипликативных функций.

Теорема 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

$$\sum_{d \mid m}$$

означает суммирование чего-либо 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,

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

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

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

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

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

$$\sum_{d \mid m} \xi(d) = \prod_{i=1}^{t} \sum_{\beta_i=0}^{\alpha_i} \xi(p_i^{\beta_i}). \tag{6}$$

Перейдём к рассмотрению наиболее важных примеров мультипликативных функций.

Определение 10. Функция

$$\tau(m) = \sum_{d \mid m} 1 \tag{7}$$

есть *число делителей* натурального числа m.

Определение 11. Функция

$$\sigma(m) = \sum_{d \mid m} d \tag{8}$$

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 (6); они получаются, если взять функции $\xi(m) = 1$ и $\xi(m) = m$ соответственно).

Пример 12. $\tau(2^3 \cdot 3^2 \cdot 5^4) = 60$, $\sigma(2^3 \cdot 3^2 \cdot 5^4) = 152295$.

Определение 12. *Функция Эйлера* $\varphi(m)$ определяется как количество чисел в ряду $0, 1, 2, \dots, m-1$, *взаимно простых* с m.

Пример 13. $\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$.

Теорема 13. *Функция Эйлера является мультипликативной.*

Доказательство. Пусть 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 9 — китайской теоремы об остатках) обладает свойством: 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, α — натуральное, то по определению легко найти

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

Упражнение 17. Докажите это.

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

Пользуясь мультипликативностью, получаем 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 $m = p_1^{\alpha_1} \dots p_t^{\alpha_t}$.

Замечание. В раскрытом виде произведение

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

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

Пример 14. $\varphi(45000) = \varphi(2^3 \cdot 3^2 \cdot 5^4) = 12000$.

Для функции Эйлера формула (6), как легко видеть, примет вид

$$\sum_{d\,|\,m} \varphi(d) = m. \tag{9}$$

Упражнение 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 количество 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 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 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, α — натуральное).

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 (6) принимает вид

$$\sum_{d\,|\,m} \mu(d) = \begin{cases} 1, & \text{если } m = 1, \\ 0, & \text{если } m > 1. \end{cases} \tag{10}$$

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

Теорема 14. *Пусть $f(m)$ и $F(m)$ — две числовые функции. Если*

$$F(m) = \sum_{d\,|\,m} f(d), \quad m = 1, 2, \ldots, \tag{11}$$

то

$$f(m) = \sum_{d\,|\,m} \mu(d) F\left(\frac{m}{d}\right), \quad m = 1, 2, \ldots \tag{12}$$

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 (10) для функции Мёбиуса, *которое, таким образом, её характеризует*. □

Упражнение 19. Каков смысл фразы, выделенной курсивом?

Решение. «Пусть числовая функция $f(m)$ удовлетворяет соотношению

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

Тогда $f(m)$ — функция Мёбиуса.» В самом деле, равенство $f(m) = \mu(m)$ — следствие формулы (12). □

Формула (12) называется *обращением формулы* (11) *суммированием по делителям*.

Пример 16. Если обратить формулы (7), (8) и (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 (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.

§6. Целая и дробная часть числа

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

Кроме функций, рассмотренных в § 5, в теории чисел исключительно важную роль играют функции *целой* и *дробной части* вещественного числа.

Определение 14. *Целой частью* числа x называется наибольшее целое число, не превосходящее x. *Дробная часть* числа x — это разность между x и его целой частью.

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

Пример 17. Имеем

$$[\pi] = 3, \quad \left[-\frac{22}{7}\right] = -4, \quad \left\{\frac{1+\sqrt{5}}{2}\right\} = \frac{2}{1+\sqrt{5}},$$
$$\left\{e^{\pi\sqrt{163}}\right\} = 0.9999999999992\ldots,$$
$$\left\{\frac{\ln 640320}{\sqrt{163}} - \frac{\pi}{3}\right\} = 0.99999999999999992\ldots$$

Последние две формулы принадлежат индийскому математику С. Рамануджану (1887 — 1920).

Непосредственно из определения следуют неравенства

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

которые иногда записывают в виде

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

Деля целое число a на натуральное число d с остатком, нетрудно обнаружить, что неполное частное выражается формулой

$$q = \left[\frac{a}{d}\right].$$

Этому наблюдению можно придать следующий смысл.

Лемма 7. *Пусть d — натуральное число. Количество положительных целых чисел, делящихся на d и не превосходящих данного $x > 0$, равно $[x/d]$.*

Доказательство. Указанные числа имеют вид $d, 2d, \ldots, kd$, где

$$kd \leqslant x < (k+1)d.$$

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

Упражнение 20. При тех же d и x докажите равенство $[x/d] = [[x]/d]$.
Указание. Между $[x]$ и x целых чисел нет.

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

Лемма 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. Пара неравенств эквивалентна паре очевидных неравенств $0 \leqslant [\{x\} + \{y\}] \leqslant 1$. Докажем тождество. 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. Имеем $[mx] - m[x] = l$, откуда при $m = 2$ получаем такое следствие: *выражение* $[2x] - 2[x]$ *принимает только два значения* — 0 *и* 1.

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

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

где (лишь формально бесконечное) произведение распространено на все простые числа p.

Теорема 15. *Пусть* p *— простое число. Для любого натурального числа* n *справедлива формула*

$$\nu_p(n!) = \sum_{\alpha \geqslant 1} \left[\frac{n}{p^\alpha} \right]. \tag{13}$$

Замечание. 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 α.

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

Если $p > n$, то доказывать нечего, поэтому считаем $p \leqslant n$. Рассмотрим в произведении $n!$ все множители, кратные p. По лемме 7 их количество есть $q = [n/p]$, а сами они суть p, $2p$, …, qp. Имеем

$$n! = (p \cdot 2p \cdot \ldots \cdot qp)N = p^q q! N,$$

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

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

(см. также упражнение 20). Значит,

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

Шаг индукции сделан. □

Упражнение 21. Докажите формулу (13) прямым подсчётом показателя $\nu_p(n!)$.

Решение. Количество чисел в ряду $1, 2, \ldots, n$, делящихся *в точности на* p^α (т. е. кратных p^α и не кратных $p^{\alpha+1}$), по лемме 7 равно

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

Следовательно,

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

Сравните с классическим рассуждением (см. [1], стр. 25): «Действительно, число сомножителей произведения $n!$, кратных p, равно $[n/p]$, среди них число кратных p^2 равно $[n/p^2]$, среди последних число кратных p^3 равно $[n/p^3]$, и т. д. Сумма (13) и даст искомый показатель, так как каждый сомножитель произведения $n!$, кратный p^m, но не p^{m+1}, нами сосчитан точно m раз, как кратный p, p^2, p^3, …, наконец, p^m.». □

Приведём примеры применения формулы Лежандра.

Пример 18. Как определить, каким количеством нулей оканчивается число

$$40! = 815915283247897734345611269596115894272000000000,$$

не вычисляя самого этого числа? Это количество равно

$$\nu_5(40!) = \left[\frac{40}{5}\right] + \left[\frac{40}{25}\right] = 8 + 1 = 9.$$

Упражнение 22. Поясните, почему.

Указание. Числа, кратные пяти, встречаются в натуральном ряду реже, чем числа, кратные двум.

Пример 19. Покажем, что *биномиальный коэффициент*

$$\frac{n!}{k!(n-k)!}$$

является целым числом (не зная, что это C_n^k — *число сочетаний из n по k*, т. е. количество k-элементных подмножеств n-элементного множества). Для этого можно воспользоваться следующим очевидным критерием: *натуральное число A делится на натуральное число B тогда и только тогда, когда*

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

для любого простого числа p.

Таким образом, требуется 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 воспользовались неравенством $[x] + [y] \leqslant [x+y]$, см. лемму 8).

Итак, каноническое разложение $n!$ выглядит следующим образом:

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

Вот ещё одна формула такого типа:

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

где показатель

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

Упражнение 23. Проверьте последнее равенство.

Указание. Воспользуйтесь правилом составления наименьшего общего кратного нескольких чисел (см. § 4).

Перейдя к логарифмам, получим

$$\ln n! = \sum_{p\leqslant n}\sum_{\alpha\geqslant 1}\nu_p(n!)\ln p = \sum_{p\leqslant n}\sum_{\alpha\geqslant 1}\left[\frac{n}{p^\alpha}\right]\ln p, \tag{14}$$

$$\ln \mathrm{HOK}\,(1,2,\ldots,n) = \sum_{p\leqslant n}\left[\frac{\ln n}{\ln p}\right]\ln p. \tag{15}$$

Этими формулами мы воспользуемся в следующем параграфе.

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

Упражнение 24. Пусть на отрезке $a \leqslant x \leqslant b$ задана некоторая неотрицательная и непрерывная функция $y = f(x)$. Число *целых точек* (x, y) (т. е. точек, имеющих целочисленные координаты), лежащих в криволинейной трапеции $\{(x, y) \in \mathbb{R}^2 : a \leqslant x \leqslant b,\ 0 < y \leqslant f(x)\}$, равно

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

Указание. $[f(k)]$ равно количеству целых чисел y, удовлетворяющих условию $0 < y \leqslant f(k)$.

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

$$S(N) = \sum_{k=1}^{N}\left[\frac{N}{k}\right] \approx N\ln N + (2\gamma - 1)\ln N, \quad N \to \infty,$$

где $\gamma = 0.5772156649\ldots$ — так называемая *постоянная Эйлера*. Одной из задач теории чисел, до сих пор не получившей окончательного решения, является задача об оценке погрешности этого приближённого равенства. 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 25. Пусть P и Q — положительные нечётные взаимно простые числа. Докажите, что

$$\sum_{0<x<Q/2}\left[\frac{Px}{Q}\right] + \sum_{0<y<P/2}\left[\frac{Qy}{P}\right] = \frac{P-1}{2}\cdot\frac{Q-1}{2}.$$

§7. Оценки Чебышёва

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

Простые числа расположены в натуральном ряду весьма неравномерно. С одной стороны, можно указать сколь угодно длинные отрезки натурального ряда, свободные от простых чисел, например вида

$$N!+2,\ N!+3,\ \ldots,\ N!+N.$$

С другой — существует много пар простых чисел, разность между которыми равна двум (их называют *простыми числами-близнецами*), например $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(41,43)$ и др. Известны примеры пар очень больших простых чисел-близнецов; последний рекорд таков:

$$2003663613 \cdot 2^{195000} \pm 1$$

(январь 2007 года, см. `www.primes.utm.edu`).

Определение 15. 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 теории чисел.

Первый шаг в решении этой проблемы был сделан Евклидом. Его теорему о бесконечности множества простых чисел (см. §3) можно сформулировать как утверждение

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

Л. Эйлер (1707 — 1783) высказал следующую теорему: доля простых чисел в начальном отрезке натурального ряда становится исчезающе мала с увеличением длины этого отрезка, т. е.

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

Полностью эта теорема была доказана А. Лежандром (1752 — 1833). Он же, пользуясь таблицами простых чисел, эмпирически установил приближённую формулу

$$\pi(x) \approx \frac{x}{\ln x - B}, \quad B = 1,08366. \tag{16}$$

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

$$\pi(x) \approx \int_2^x \frac{dt}{\ln t}. \tag{17}$$

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

$$a\,\frac{x}{\ln x} < \pi(x) < b\,\frac{x}{\ln x}. \tag{18}$$

В 1845 году французский математик Ж. Бертран, анализируя таблицы простых чисел $\leqslant 3\,000\,000$ в связи со своими исследованиями по теории групп, высказал предположение, с тех пор известное как

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

Вскоре этот постулат был доказан Чебышёвым в его знаменитой работе «О простых числах» («Memoire sur les nombres premiers», 1850 год).

А. 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 (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 (15) — что

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

Кроме того, справедливы неравенства

$$\theta(x) \leqslant \psi(x) \leqslant \sum_{p \leqslant x} \ln x = \pi(x) \ln x. \tag{19}$$

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

$$N = N(n) = C_{2n}^n = \frac{(2n)!}{n!^2} = \mathrm{e}^{T(2n) - 2T(n)}. \tag{20}$$

Положим также

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

Лемма 9. *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 10. *При $n \geqslant 3$ имеет место неравенство $N > 2^{n+1}$.*

Доказательство. Это неравенство является довольно грубым, однако при доказательстве нижней оценки для $\pi(x)$ нам будет его достаточно. Доказать его можно, например, индукцией по $n \geqslant 3$. Шаг индукции:

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

Проверку базы индукции предоставим читателю. □

Замечание. 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 стремится к пределу $1/\sqrt{\pi}$; последнее утверждение эквивалентно классической *формуле Валлиса*:

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

Б. Оценки Чебышёва для $\pi(x)$.

Сначала докажем *оценку снизу* — левое неравенство в формуле (18).

Теорема 16. *При $x \geqslant 6$ справедливо неравенство*

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

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

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

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

Применяя леммы 9 и 10, будем иметь

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

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

Для доказательства *оценки сверху* — правого неравенства в формуле (18) — нам понадобится

Лемма 11. *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 доказать (например, индукцией по $k \geqslant 1$) неравенство

$$M < 4^k.$$

Итак,

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

Шаг индукции сделан. □

Теорема 17. *При $x \geqslant 2$ справедливо неравенство*

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

с константой $b = 5\ln 2 = 3.46574$.

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 $\vartheta(x) \leqslant 2x\ln 2$ (см. лемму 11), 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 $x \geqslant 64$. Но доказываемое неравенство также верно и при $2 \leqslant x < 64$, что можно проверить при помощи таблиц простых чисел. □

Упражнение 26. Пусть p_n — n-е простое число. Докажите существование таких положительных констант α и β, что при всех $n \geqslant 2$

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

Указание. При $x = p_n$ формула (18) принимает вид

$$a\,\frac{p_n}{\ln p_n} < \pi(p_n) = n < b\,\frac{p_n}{\ln p_n}. \tag{21}$$

Логарифмируя, получим

$$\ln p_n - \ln\ln p_n + \ln a < \ln n < \ln p_n - \ln\ln p_n + \ln b. \tag{22}$$

Теперь почленно перемножьте (21) и (22).

В. Доказательство постулата Бертрана.

Следующая теорема впервые была доказана П. Л. Чебышёвым.

Теорема 18. *При $n \geqslant 2$ между n и $2n$ есть хотя бы одно простое число.*

Доказательство. Мы приведём изящное доказательство, принадлежащее П. Эрдёшу (1913 — 1996). Его идею можно описать так: биномиальный коэффициент (20) был бы «слишком мал», если бы 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 11). 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 противоречива при $n > 68$, если предположить, что

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

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

1. 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 29).

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

$$\psi(x) = \sum_{k\geqslant 1} \vartheta(x^{1/k}), \quad T(x) = \sum_{k\geqslant 1} \psi(x/k), \tag{23}$$

теперь называемых *тождествами Чебышёва*.

Упражнение 27. 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.

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

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

Опираясь на второе из тождеств (23), замечаем, что эта функция разлагается в *знакопеременный ряд*:

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

Поскольку функция $\psi(x)$ — *неубывающая*, 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,

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

II. Оценка $U(x)$**.** Имеем

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

откуда

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

III. 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,

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

IV. Завершение доказательства. 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.

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

Теорема 19. *Для любого* $\delta > 6/5$ *в интервале* $(n, \delta n)$ *содержится хотя бы одно простое число, если* $n \geqslant n_0 = n_0(\delta)$.

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 $\widetilde{U}(x)$ нетрудно дать при помощи 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:

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

где константа

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

Следствием этой оценки и явилась теорема 19.

Упражнение 28. Попробуйте дать подробное доказательство теоремы 19.

Указание. Можно (и даже настоятельно рекомендуется) ознакомиться с первоисточником.

Кроме этого, пользуясь полученной оценкой для $\vartheta(x)$, Чебышёв установил границы для функции распределения простых чисел. 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 (18) выполняются с константами

$$a = 0.92129, \quad b = 1.10555, \tag{24}$$

начиная с некоторого x.

§8. 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 (18) выполняются с константами (24) при достаточно больших x. Эти константы близки к единице. Следующим шагом должно было стать доказательство *асимптотического закона распределения простых чисел*, который выражается формулой

$$\pi(x) \sim \frac{x}{\ln x}, \quad x \to \infty. \tag{25}$$

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 (16) будет точнее, если в ней положить $B = 1$. Но ещё более точной оказывается формула Гаусса (17), она точнее формулы Лежандра (16), каково бы ни было значение постоянной B. Отметим, что к рассмотрению *интегрального логарифма*

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

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

Асимптотический закон в форме

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

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 *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 уже 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:

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \quad \Re s > 1 \tag{26}$$

(*тождество Эйлера*).

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

Теорема 20. *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 26.) □

Пример 20. Простое число $p = 1000003$ имеет номер 78499. Применяя асимптотическую формулу, получим $p \approx 884750$. Относительная погрешность этого приближенного равенства составляет примерно 12%.

Упражнение 29. 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 (25), докажите оценку

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

Теорема 21. *Справедливы соотношения*

$$\prod_{p \leqslant n} p \sim \text{НОК}(1, 2, \ldots, n) \sim \mathrm{e}^n, \quad n \to \infty. \tag{27}$$

Доказательство. Функции $\theta(x)$, $\psi(x)$ и $\pi(x)$ связаны неравенствами (19), 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 получаем

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

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 сначала к *нижним*, а затем и к *верхним* пределам отношений $\theta(x)/x$ и $\psi(x)/x$ при $x \to \infty$ и учитывая асимптотический закон распределения простых чисел (25), получим, что все эти пределы заключены между $1-\varepsilon$ и 1. Но ε можно выбрать сколь угодно малым, поэтому все нижние и верхние пределы совпадают и равны 1. 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 (27) можно считать доказанными. □

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 в 1839 году П. Г. Лежен-Дирихле (1805 — 1859) и которая с тех пор носит его имя.

Теорема Дирихле. *В любой арифметической прогрессии*

$$mk + l, \quad k = 1, 2, 3, \ldots, \tag{28}$$

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, применяя рассуждение Евклида — см., например, упражнение 14. Вот ещё один пример такого рода.

Пример 21. Докажем, что арифметическая прогрессия $4k+1$ содержит бесконечно много простых чисел.

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

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

Любой его простой делитель имеет вид $4k+1$ (см. упражнение 9 из раздела II), но ни одно из простых чисел p_i не делит N — противоречие.

Упражнение 30. Докажите, что в арифметической прогрессии $8k+5$ содержится бесконечно много простых чисел.

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

Аналогичными рассуждениями можно доказать утверждение теоремы Дирихле для прогрессий

$$8k \pm 1, \quad 8k \pm 3, \quad 12k \pm 1, \quad 12k \pm 5.$$

Несколько сложнее, но все ещё элементарными методами доказывается бесконечность множества простых чисел вида $mk \pm 1$ для любого натурального m. 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 рядов

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

(*L-функций 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-функции — 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 (26):

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

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 χ_i, получим при $s \to 1$

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

где первая сумма распространена на все простые p вида $4k+1$, а вторая — на все простые p вида $4k-1$. Но тогда для каждой из этих сумм имеем

$$\lim_{s \to 1} \sum \frac{1}{p^s} = +\infty,$$

поскольку $L_0(s) \to +\infty$ при $s \to 1$ и в то же время

$$L_1(1) \neq 0, \qquad (*)$$

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 неравенств типа $(*)$. Ради этого, собственно, и привлекаются методы теории функций комплексного переменного.

Замечание. Элементарное (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 (28), не превосходящих x. Оказалось, что независимо от l, НОД $(m, l) = 1$,

$$\pi(x, m, l) \sim \frac{1}{\varphi(m)} \operatorname{Li}(x), \quad x \to \infty, \qquad (29)$$

т. е. простые числа распределены *примерно поровну* по всем $\varphi(m)$ прогрессиям вида (28).

Формула (29) показывает, что в прогрессии (28) 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* (28) *не превосходит* m^{c_0}.

Более подробно с вопросами, обсуждаемыми в этом и предыдущем параграфах, можно познакомиться по книгам [2] и [3].

II. Теория сравнений

§1. Определение и свойства сравнений

Понятие (числового) сравнения по модулю. Обозначение Гаусса. Эквивалентность различных определений. Основные свойства сравнений.

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

Определение 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:

$$a \equiv b \pmod{m}. \tag{1}$$

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 конкретный модуль m.

Теорема 1. *Условие* (1) *равносильно любому из следующих условий.*

(1а) *Числа* a *и* b *дают одинаковые остатки при делении на* m.

(1б) *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 (1) равносильно делимости $r_1 - r_2$ на m. Но эта делимость, в силу ограничений на остатки r_i, означает их совпадение.

Равносильность условий (1) и (1б) станет самоочевидной, если равенство $a = b + mt$ переписать в виде $a - b = mt$. □

Таким образом, любое из условий (1а) и (1б) теоремы 1 может быть принято за определение сравнимости по модулю m (обычно предпочитают условие *равноостаточности* (1а)).

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 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*

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

Сравнения можно почленно складывать, вычитать и перемножать.

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

Из одной части сравнения можно перенести слагаемое в другую его часть, изменив знак.

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

Обе части сравнения можно умножить на одно и то же целое число.

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

Обе части сравнения можно разделить на их общий делитель, если он взаимно прост с модулем.

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

К любой части сравнения можно добавить число, кратное модуля.

6. *Пусть* $a \equiv b \pmod m$. *Если* $f(x) = c_n x^n + \ldots + c_1 x + c_0$ — *произвольный многочлен с целыми коэффициентами, то*

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

7. *Если* $a_1 \equiv b_1 \pmod m$, …, $a_n \equiv b_n \pmod m$ *и* $f(x_1, \ldots, x_n)$ — *многочлен с целыми коэффициентами, то*

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

8. *Если* $a_1 \equiv b_1 \pmod m$, …, $a_n \equiv b_n \pmod m$ *и многочлены с целыми коэффициентами*

$$f(x_1, \ldots, x_n) = \sum A_{(t_1,\ldots,t_n)} x_1^{t_1} \ldots x_n^{t_n},$$
$$g(x_1, \ldots, x_n) = \sum B_{(t_1,\ldots,t_n)} x_1^{t_1} \ldots x_n^{t_n}$$

таковы, что $A_{(t_1,\ldots,t_n)} \equiv B_{(t_1,\ldots,t_n)} \pmod m$ *для всех* $(t_1, \ldots, t_n)$, *то*

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

Доказательство. Приведём лишь доказательства чуть менее очевидных свойств.

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

$$(a \pm c) - (b \pm d) = m(t_1 \pm t_2), \quad ac - bd = m(bt_2 + dt_1 + mt_1t_2)$$

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. § 2 раздела I) отсюда следует, что на m делится $a - b$, т. е. $a \equiv b \pmod m$.

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

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

Если умножить обе части сравнения (2) на c_k и просуммировать по всем $k = 0,\ 1,\ \ldots,\ n$, получим $f(a) \equiv f(b) \pmod m$.

7 (8). Это свойство обобщает свойство 6 (7) и доказывается аналогичным образом. □

Упражнение 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 *— натуральный делитель модуля* m*, то* $a \equiv b \pmod{d}$.

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

11. *Если* $a \equiv b \pmod{m}$*,* d *— общий натуральный делитель чисел* a*,* b *и модуля* 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 имеет место сравнение* $a \equiv b \pmod{m}$*, где* $m = \text{НОК}(m_1, m_2)$.

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

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

Доказательство. И здесь всё и сразу (или почти сразу) следует из определений.

9. Если разность $a - b$ делится на m, то она делится и на d — делитель m (транзитивность отношения делимости).

10 (11). Пусть $a - b = mt$, где $t \in \mathbb{Z}$. Умножим на k (или разделим на d) и получим то, что нужно.

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. Это утверждение — иная формулировка леммы 1 из раздела I.

14. Имеем $a = b + mt$, где $t \in \mathbb{Z}$. Утверждение является частным случаем свойства 8 отношения делимости (см. § 1 раздела I). □

Замечание. 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 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 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. Покажем, что равенство

$$x^3 + y^3 + z^3 = 4$$

невозможно ни при каких целых x, y, z.

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

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

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

Таким образом, сумма трёх кубов будет сравнима по модулю 9 с одним из чисел 0, ± 1, ± 2, ± 3. А число 4, как легко видеть, этим свойством не обладает. Поэтому $x^3 + y^3 + z^3 \neq 4$ для любых целых чисел x, y, z.

Замечание. *Метод остатков*, которым мы воспользовались в примере 3, не всегда эффективен при обосновании невозможности равенств. Так, например, можно показать, что $x^2 - 34y^2 \neq -1$ при любых целых x, y, однако сравнение

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

разрешимо по *любому* модулю m.

§2. Классы вычетов. Теоремы Ферма и Эйлера

Понятие класса вычетов по модулю. Полные и приведённые системы вычетов по модулю и их свойства. Малая теорема Ферма и её различные доказательства. Биномиальная формула по простому модулю. Теорема Эйлера. Применение теоремы Эйлера для вычисления степеней целых чисел по модулю.

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

Определение 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 просто $[a]$ (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:

$$[r] = \{r + mt : t \in \mathbb{Z}\}, \quad r \in \{0, 1, \ldots, m-1\}. \tag{3}$$

Множество всех классов вычетов по модулю m обозначим Z_m. Оно содержит, таким образом, m элементов вида (3).

Определение 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 принимает два значения: $\rho = \pm m/2$).

Определение 4. Если из каждого класса вычетов по модулю m взять по одному представителю, то возникнет *полная система вычетов* по модулю m.

Пример 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)). Однако для вычислений предпочтительнее *полная система абсолютно наименьших вычетов* по модулю m.

Пример 5. Найдем возможные остатки от деления квадратов целых чисел на $m = 7$.

Очевидно, достаточно найти остатки от деления на 7 чисел вида ρ^2, где ρ пробегает полную систему абсолютно наименьших вычетов по модулю 7, т. е. $\rho \in \{0, \pm 1, \pm 2, \pm 3\}$. Эти остатки таковы: 0, 1, 2, 4.

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

Теорема 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. Утверждение теоремы является непосредственным следствием такого факта: если $x_1 \not\equiv x_2 \pmod m$, то

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

Этот факт можно обосновать рассуждением от противного: иначе мы получили бы сравнение

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

которое после сокращения на a (корректного ввиду свойства 4 сравнений, см. § 1) привело бы к $x_1 \equiv x_2 \pmod m$. □

Опираясь на теорему 2, можно дать несколько более конструктивное доказательство китайской теоремы об остатках (теорема 9 раздела I).

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

$$r(i, j) = m_2 i + j \quad (i = 0, 1, \ldots, m_1 - 1;\ j = 0, 1, \ldots, m_2 - 1), \qquad (4)$$

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 2).

Действительно, число r нужно 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. 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. § 1) следует, что все числа некоторого класса вычетов по модулю m либо все взаимно просты с m, либо все имеют с m общий делитель $d > 1$. Это замечание делает корректным следующее

Определение 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 Z_m^*.

Пример 6. Имеем $Z_{12}^* = \{[1], [5], [7], [11]\}$.

Определение 6. Если из каждого класса вычетов по модулю m, взаимно простого с m, взять по одному представителю, то возникнет *приведённая система вычетов* по модулю m.

Пример 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 4. Анализируя таблицу чисел (4), ещё раз установите свойство мультипликативности функции Эйлера.

Решение. Число $r = r(i, j)$ взаимно просто с $m = m_1 m_2$ тогда и только тогда, когда r взаимно просто с m_1 и взаимно просто 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, 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**

(5)

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

Упражнение 5. Если в формулировке упражнения 3 слово «полную» заменить на слово «приведённую», то получится новое верное утверждение. Докажите его, а заодно в $(N+1)$-й раз осознайте, что функция Эйлера — мультипликативна.

Контрольный вопрос. Чему равно N?

Ответ. Если Вы — внимательный читатель, то для Вас $N = 4$.

1. При $m_1 = 4$, $m_2 = 9$ первое доказательство мультипликативности функции Эйлера (см. теорему 13 раздела I) 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

(6)

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

(7)

Видно, что эти доказательства почти одинаковы (таблицы (6) и (7) получаются одна из другой *перестановкой столбцов*, хотя в более общей ситуации потребовалась бы ещё и *перестановка строк*), но существенно отличаются от предпоследнего (см. таблицу (5)).

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 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). Далее, прямое вычисление показывает, что

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

(здесь p — простое, α — натуральное). Но тогда $S(m) = \mu(m)$ — функция Мёбиуса (см. определение 13 раздела I).

Теорема 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 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. § 1 раздела I). □

Упражнение 6. Дайте подробное доказательство теоремы 3.

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

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

теорема 3 в этом случае приводит к такому результату: *если число a не кратно 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* исходной системы $1, 2, \ldots, p - 1$. Отсюда, в частности, следует сравнение

$$a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}. \tag{8}$$

После сокращения на общий множитель $(p - 1)!$ мы приходим к теореме, доказанной в 1640 году П. Ферма (1601 — 1665) и известной теперь как

Малая теорема Ферма. *Если p — простое число, a целое число a не кратно p, то справедливо сравнение*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{9}$$

Упражнение 7. Объясните, почему сокращение обеих частей сравнения (8) на $(p - 1)!$ законно.

Термин «малая теорема» объясняется тем, что есть и «большая теорема» Ферма, которую мы здесь обсуждать не будем. Ввиду важности малой теоремы Ферма мы дадим ей ещё одно

Доказательство. Точнее, мы докажем её в следующей форме: для любого простого числа p и любого целого числа a верно сравнение

$$a^p \equiv a \pmod{p}. \tag{10}$$

Ясно, что для чисел a, не кратных на p, сравнения (9) и (10) будут эквивалентны.

Сравнение (10) будем доказывать индукцией по *натуральным* a (очевидно, достаточно рассмотреть только такие 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 $1 \leqslant k \leqslant p-1$ биномиальные коэффициенты суть нули по модулю p: $C_p^k \equiv 0 \pmod{p}$. □

Упражнение 8. Докажите последнее утверждение.
Указание. Число $k!C_p^k = p(p-1)\ldots(p-k+1)$ делится на p.

Следствие. *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. В западной учебно-методической литературе, посвящённой теории чисел, это следствие (эквивалентное, кстати, самой малой теореме Ферма) иногда 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 9. Докажите, что все нечётные простые делители числа $a^2 + 1$ имеют вид $4k + 1$.

Решение. Пусть p — нечётный простой делитель этого числа, т. е.

$$a^2 + 1 \equiv 0 \pmod{p}.$$

Перенося единицу вправо и возводя в степень $(p-1)/2$, получим

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

Учитывая сравнение (9), имеем $1 \equiv (-1)^{(p-1)/2} \pmod{p}$. Отсюда следует, что $(p-1)/2$ — чётное число, $(p-1)/2 = 2k$, т. е. $p = 4k+1$. □

В 1736 году Эйлер распространил малую теорему Ферма с простого модуля p на произвольный модуль m.

Теорема Эйлера. *Если* НОД $(a, m) = 1$, *то*

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{11}$$

Доказательство. Рассмотрим какую-нибудь приведённую систему вычетов $x_1, x_2, \ldots, x_k$ по модулю m, так что $k = \varphi(m)$. После умножения на a получим другую приведённую систему вычетов $ax_1, ax_2, \ldots, ax_k$ по модулю m (теорема 3). Как и выше, имеет место сравнение

$$ax_1 \cdot ax_2 \cdot \ldots \cdot ax_k \equiv x_1 \cdot x_2 \cdot \ldots \cdot x_k \pmod{m}.$$

Собирая множители a в степень и сокращая на произведение $x_1 x_2 \ldots x_k$, взаимно простое с m, получим сравнение (11). □

Упражнение 10. Пусть НОД $(m, 6) = 1$. Докажите, что

$$x_1^2 + x_2^2 + \ldots + x_k^2 \equiv 0 \pmod{m},$$

где $x_1, x_2, \ldots, x_k$ — приведённая система вычетов по модулю m.

Решение. Пусть $S = x_1^2 + x_2^2 + \ldots + x_k^2$. Тогда

$$4S = (2x_1)^2 + (2x_2)^2 + \ldots + (2x_k)^2 \equiv S \pmod{m},$$

откуда $3S \equiv 0 \pmod{m}$ и $S \equiv 0 \pmod{m}$. □

Упражнение 11. Выведите теорему Эйлера из малой теоремы Ферма.

Решение. Пусть p — произвольный простой делитель числа m. Тогда $a^{p-1} \equiv 1 \pmod{p}$. Докажем индукцией по $\alpha \geqslant 1$ сравнение

$$a^{p^{\alpha-1}(p-1)} \equiv 1 \pmod{p^\alpha}. \tag{12}$$

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 разность $A - 1$ делится на p^α. 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 (11) вытекает из свойств сравнений и формулы для $\varphi(m)$ (см. § 5 раздела I). □

Замечание. При $p = 2$ и $\alpha \geqslant 3$ сравнение (12) можно уточнить:

$$a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$$

(следствие того, что при нечётном a число $a^2 - 1$ делится не только на 4, но и на 8). Положим $\lambda(p^\alpha) = p^{\alpha-1}(p-1)$ для любого нечётного простого числа p,

$$\lambda(2^\alpha) = \begin{cases} 2^{\alpha-1}, & \text{если } \alpha = 1,\ 2, \\ 2^{\alpha-2}, & \text{если } \alpha \geqslant 3. \end{cases}$$

Если $m = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$, то пусть

$$\lambda(m) = \text{НОК}\,(\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_t^{\alpha_t})).$$

Так определённая функция $\lambda(m)$ называется *функцией Кармайкла*. Если НОД $(a, m) = 1$, то, как следует из решения упражнения,

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

Основное предназначение теорем Эйлера и Ферма — понижать показатель степени при её вычислении по какому-нибудь модулю. Более точно, пусть требуется найти остаток от деления числа a^N на m, причём число N достаточно велико. Считая a взаимно простым с m и представляя показатель N в виде

$$N = \varphi(m)t + r, \quad 0 \leqslant r < \varphi(m),$$

будем иметь

$$a^N = (a^{\varphi(m)})^t \cdot a^r \equiv a^r \pmod{m}.$$

Таким образом, показатель N можно заменить его остатком r от деления на $\varphi(m)$, который может оказаться не очень большим.

Пример 8. Найдём три последние цифры числа $A = 1003^{2008}$.

Фактически требуется 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 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 13. («Хвост зверя») Пусть

$$A_1 = 2009, \quad A_{k+1} = 2009^{A_k} \quad (k = 1, 2, \ldots).$$

Используя компьютер, найдите *последние* 40 цифр числа A_{2009}.

Указание. Положим

$$m_0 = 10^{40}, \quad m_{k+1} = \lambda(m_k) \quad (k = 0, 1, \ldots),$$

и пусть B_k — наименьший неотрицательный вычет числа A_{2009-k} по модулю m_k. Докажите, что справедливы сравнения

$$B_k \equiv 2009^{B_{k+1}} \pmod{m_k}, \quad k = 0, 1, \ldots, 2007.$$

Ответ. $A_{2009} = \ldots 4882433483045575722353334513087881963289$.

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 IV).

§3. Сравнения с неизвестными

Определение сравнения по модулю с неизвестными. Переборный алгоритм решения. Сравнения с одним неизвестным по простому модулю. Редукция по степени сравнения. Теорема о числе решений. Теорема Вильсона.

В этом параграфе мы будем изучать сравнения по модулю, содержащие неизвестные — теоретико-числовой аналог алгебраических уравнений.

Определение 7. Пусть $f(x_1, \ldots, x_n)$ — многочлен от переменных x_1, $\ldots$, x_n с целыми коэффициентами. Выражение вида

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{m} \tag{13}$$

называется *сравнением по модулю с неизвестными*.

Как и алгебраическое уравнение, сравнение с неизвестными вида (13) надлежит *решать*, т. е. находить *все наборы* $(a_1, \ldots, a_n)$ целочисленных значений неизвестных, ему удовлетворяющих.

Ввиду свойства 7 сравнений (см. § 1) можно понимать под *решением* сравнения (13) 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 перебором.

Пример 9. В примере 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 (13) 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. § 1), это приведёт к *равносильному сравнению* (имеющему те же решения, что и исходное).

Если $m = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ — каноническое разложение модуля m, то сравнение (13) эквивалентно системе сравнений

$$f(x_1, \dots, x_n) \equiv 0 \pmod{p_i^{\alpha_i}}, \quad i = 1, \dots, t. \tag{14}$$

Предположим, что мы решили каждое из них. Тогда, опираясь на китайскую теорему об остатках, мы сможем покомпонентно «склеить» из полученных решений все решения сравнения (13). Всего при этом получится $N = N_1 \dots N_t$ решений, где N_i — число решений i-го сравнения (14).

Пример 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:

$$([0]_9, [1]_9),\ ([0]_9, [8]_9),\ ([3]_9, [1]_9),\ \boxed{([3]_9, [8]_9)},\ ([6]_9, [1]_9),\ ([6]_9, [8]_9).$$

«Склеив», например, решение $([2]_4, [1]_4)$ с решением $([3]_9, [8]_9)$, получим решение $([30]_{36}, [17]_{36})$ (см. таблицу (6)). Таким способом можно получить все $4 \cdot 6 = 24$ решения исходного сравнения.

Итак, общая задача решения сравнения (13) 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

$$f(x) \equiv 0 \pmod p, \tag{15}$$

где $f(x) = a_n x^n + \dots + a_1 x + a_0$ — многочлен с целыми коэффициентами, $\deg f(x) = n$.

Определение 8. *Степенью* сравнения (15) называется *наибольший индекс* k, для которого $a_k \not\equiv 0 \pmod p$.

После редукции коэффициентов вполне может оказаться, что степень сравнения (15) меньше, чем $\deg f(x)$. Ещё один способ понизить степень сравнения предоставляет следующая

Теорема 4. *Любое сравнение* (15) *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, $\deg r(x) \leqslant p-1$. По малой теореме Ферма имеем

$$f(a) \equiv r(a) \pmod{p}$$

для любого $a \in \mathbb{Z}$, поэтому сравнение (15) равносильно сравнению

$$r(x) \equiv 0 \pmod{p}. \tag{16}$$

Ясно, что степень этого сравнения не выше $p-1$. □

Очевидно, *редукция по степени*, состоящая в замене сравнения (15) сравнением (16), имеет практический смысл только при $n \geqslant p$.

Теорема 5. *Сравнение* (15) *имеет решений не более, чем его степень.*

Доказательство. Будем считать, что степень сравнения (15) равна n, т. е. $a_n \not\equiv 0 \pmod{p}$.

Предположим противное: пусть $x_1, \ldots, x_n, x_{n+1}$ — представители *различных* классов вычетов по модулю p, являющихся решениями сравнения (15). 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 — некоторые 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 (15) имеет степень n. □

Упражнение 14. Объясните, почему: а) все коэффициенты b_i — целые числа; б) все $b_i \equiv 0 \pmod{p}$.

Одним из следствий теоремы 5 является следующая

Теорема Вильсона. *Если p — простое число, то*

$$(p-1)! + 1 \equiv 0 \pmod{p}. \tag{17}$$

Доказательство. При $p > 2$ положим

$$f_0(x) = (x-1)(x-2)\dots(x-p+1) - (x^{p-1}-1)$$

и рассмотрим 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 не менее $p-1$ решений. Но $\deg f_0(x) < p-1$, поэтому *все коэффициенты многочлена $f_0(x)$ должны быть кратны p*, в том числе и свободный коэффициент, равный $(p-1)!+1$. □

Замечание. Первое доказательство теоремы Вильсона дал в 1771 году Ж. Лагранж (1736 — 1813).

Упражнение 15. Если натуральное число $p > 1$ удовлетворяет сравнению (17), то p — простое число. Докажите это.

Таким образом, сравнение (17) является *критерием простоты* числа p. Этот критерий, однако, непрактичен ввиду большой величины факториала $(p-1)!$.

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 (15). Соответствующий метод основан на так называемой *лемме Гензеля о подъёме* и весьма напоминает *метод Ньютона* приближённого решения уравнений (подробнее см., например, в книге [2, гл. 16]). Приведём один конкретный

Пример 11. Пусть требуется решить сравнение

$$x^4 + 5x^3 - x^2 - 2 \equiv 0 \pmod{125}. \tag{18}$$

Очевидно, любое решение этого сравнения (как *целое число*, ему удовлетворяющее) будет и решением каждого из сравнений

$$\begin{aligned} x^4 + 5x^3 - x^2 - 2 &\equiv 0 \pmod{25}, \\ x^4 + 5x^3 - x^2 - 2 &\equiv 0 \pmod{5}. \end{aligned} \tag{19}$$

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 (18). Покажем, как это делается, на примере первого решения $[2]_5$.

Подставим $x = 2 + 5t_1$ в сравнение (19):

$$(2 + 5t_1)^4 + 5(2 + 5t_1)^3 - (2 + 5t_1)^2 - 2 \equiv 0 \pmod{25}.$$

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 (18):

$$(2 + 25t_2)^4 + 5(2 + 25t_2)^3 - (2 + 25t_2)^2 - 2 \equiv 0 \pmod{125}.$$

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 (18). Исходя из второго решения $[3]_5$, аналогичным образом можно найти ещё одно решение сравнения (18) — $[13]_{125}$. Других решений, кроме указанных, не будет.

Замечание. 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». Можно показать, что так будет всегда, если для любого решения $[r]$ сравнения (15) 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 6. *Пусть* $\deg f(x_1, \ldots, x_n) < n$. *Тогда число решений сравнения*

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p} \tag{20}$$

кратно p.

Эта теорема носит название *теоремы Варнинга*. Предварительно докажем лемму, представляющую и самостоятельный интерес.

Лемма 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 5. Имеем

$$\sum (ar)^k \equiv \sum r^k \pmod{p},$$

откуда выводим

$$(a^k - 1) \sum r^k \equiv 0 \pmod{p}.$$

Сокращая на $a^k - 1$, получим то, что требуется. □

Другое доказательство леммы 1 будет дано в § 4 раздела III (см. пример 13).

Доказательство теоремы 6. Положим $F(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)^{p-1}$ и 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 состав $F(x_1, \ldots, x_n)$, меньше $n(p-1)$, поэтому хотя бы у одной из n переменных в этом одночлене показатель будет меньше $p-1$. Применяя лемму 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 (20). 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. *Если* $\deg f(x_1, \ldots, x_n) < n$ *и многочлен* $f(x_1, \ldots, x_n)$ *имеет нулевой свободный коэффициент, то сравнение* (20) *нетривиально разрешимо.*

Утверждение следствия известно как *теорема Шевалле*. Нетривиальная разрешимость сравнения (20) означает наличие у него решения $([r_1], \ldots, [r_n]) \neq ([0], \ldots, [0])$.

Пример 12. Для любых целых чисел 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.

§4. Сравнения первой степени

Сравнения первой степени с одним неизвестным, различные методы решения. Эффективный алгоритм решения, основанный на алгоритме Евклида. Диофантовы уравнения первой степени с двумя неизвестными.

В этом параграфе мы рассмотрим один тип сравнений с неизвестными, который допускает сравнительно простое исследование. Речь идёт о так называемых *линейных сравнениях*, или *сравнениях первой степени*.

Определение 9. Сравнение (13) называется *линейным*, или *первой степени*, если $\deg f(x_1, \ldots, x_n) = 1$, т. е.

$$f(x_1, \ldots, x_n) = a_1x_1 + \ldots + a_nx_n + b,$$

где все коэффициенты — целые числа, причём среди a_i найдётся не кратный m.

Мы подробно рассмотрим случай одного неизвестного, а также покажем, как к нему можно свести случай многих неизвестных.

Очевидно, сравнение первой степени с одним неизвестным можно записать в виде

$$ax \equiv b \pmod{m}, \tag{21}$$

где $a \not\equiv 0 \pmod{m}$.

Пусть сначала

$$\text{НОД}\,(a, m) = 1.$$

Тогда сравнение (21) имеет в точности одно решение. Это следует, например, из свойства полных систем вычетов по модулю m (см. теорему 2). Более того, для представителя r_0 этого единственного решения $[r_0]$ можно дать явную формулу:

$$r_0 = a^{\varphi(m)-1}b.$$

Корректность гарантируется теоремой Эйлера:

$$ar_0 = a^{\varphi(m)}b \equiv 1 \cdot b = b \pmod{m}.$$

Однако этой формулой почти не пользуются на практике. И дело здесь даже 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. § 1 раздела IV). Главная причина в том, что показатель этой степени содержит значение функции Эйлера $\varphi(m)$ — величину, которую, вообще говоря, трудно вычислить.

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 4 и пример 3 раздела I):

$$1 = ax_0 + my_0,$$

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 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 $r = 13 \cdot 85 = 1105 \equiv 77 \pmod{257}$. Таким образом, решением будет класс вычетов $[77]$.

Рассмотрим теперь случай, когда

$$\text{НОД}\,(a, m) = d > 1.$$

В этом случае сравнение (21) уже может не иметь решений. Действительно, необходимым условием разрешимости является, как нетрудно видеть, делимость b на d, а она не всегда имеет место.

Если b всё-таки делится на d, то разделим все части сравнения (21), включая модуль, на d:

$$a_1x \equiv b_1 \pmod{m_1}, \tag{22}$$

где $a_1 = a/d$, $b_1 = b/d$ и $m_1 = m/d$, при этом $\text{НОД}\,(a_1, m_1) = 1$. Полученное сравнение (22) имеет единственное решение — 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 (21) будет иметь в точности d решений: это классы вычетов

$$[r_0 + jm_1]_m, \quad j = 0,\ 1,\ \ldots,\ d-1.$$

При этом если

$$d = ax_0 + my_0, \tag{23}$$

где $x_0,\ y_0 \in \mathbb{Z}$, то можно взять $r_0 = bx_0/d$.

Пример 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. Сокращая 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, мы доказали следующую теорему.

Теорема 7. *Пусть* $d = \text{НОД}\,(a, m)$. *Если* b *не делится на* d, *то сравнение* (21) *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* (23).

Покажем теперь, как, пользуясь теоремой 7, можно решать сравнения первой степени с несколькими неизвестными.

Пример 15. Решим сравнение $48x - 45y + 13 \equiv 0 \pmod{100}$.

Запишем это сравнение в виде

$$48x \equiv 45y - 13 \pmod{100}. \tag{24}$$

Так как $\text{НОД}\,(48, 100) = 4$, то должно выполняться сравнение

$$45y - 13 \equiv 0 \pmod{4}.$$

Решая это сравнение в *целых числах*, получим

$$y = 1 + 4t_1,$$

где $t_1 \in \mathbb{Z}$. Подставим в (24) и после сокращения на 4 будем иметь

$$12x \equiv 45t_1 + 8 \pmod{25}.$$

Поскольку НОД $(12, 25) = 1$, ограничений на t_1 нет. Решая опять в целых числах, найдем

$$x = 9 + 10t_1 + 25t_2,$$

где $t_2 \in \mathbb{Z}$. Итак, все решения исходного сравнения в целых числах суть

$$(x, y) = (9 + 10t_1 + 25t_2, 1 + 4t_1), \quad t_1,\, t_2 \in \mathbb{Z}.$$

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 приведет к 4 классам для x), и мы получим ответ в виде

$$([9 + 10j_1 + 25j_2], [1 + 4j_1]),$$

где $0 \leqslant j_1 \leqslant 24$ и $0 \leqslant j_2 \leqslant 4$.

Теория сравнений первой степени оказывается полезной при решении неопределённых уравнений первой степени.

Определение 10. Уравнение вида

$$a_1x_1 + \ldots + a_nx_n = b,$$

где $n > 1$ и все коэффициенты — целые числа, называется *неопределённым уравнением первой степени*.

Предполагается, что неизвестные $x_1, \ldots, x_n$ могут принимать 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

$$Ax \equiv C \pmod{|B|}.$$

Любое решение $x_0 \in \mathbb{Z}$ этого сравнения приводит к решению $(x_0, y_0) \in \mathbb{Z}^2$ неопределённого уравнения, при этом

$$y_0 = \frac{C - Ax_0}{B}.$$

Обратно, если (x_0, y_0) — некоторое решение неопределённого уравнения, то число x_0 будет удовлетворять сравнению. Таким образом, решив сравнение, мы найдём и все решения неопределённого уравнения.

Пример 16. Решим уравнение $50x - 42y = 34$.

Составляя сравнение

$$50x \equiv 34 \pmod{42}$$

и решая его в целых числах, найдём $x = 20 + 21t$, где $t \in \mathbb{Z}$. Тогда

$$y = \frac{50x - 34}{42} = \frac{50(20 + 21t) - 34}{42} = 23 + 25t.$$

Итак, все решения данного уравнения — это пары целых чисел вида

$$(x, y) = (20 + 21t, 23 + 25t), \quad t \in \mathbb{Z}.$$

Оказывается, последовательно решая подходящим образом составленные сравнения первой степени, можно решать неопределённые уравнения с любым числом неизвестных. Вот соответствующий

Пример 17. Решим уравнение $30x + 24y - 55z = 11$.

Это уравнение эквивалентно сравнению

$$30x \equiv -24y + 11 \pmod{55}. \tag{25}$$

Поскольку НОД $(30, 55) = 5$, последнее разрешимо тогда и только тогда, когда

$$24y \equiv 11 \pmod{5}.$$

Решив это сравнение, найдём

$$y = 4 + 5t_1,$$

где $t_1 \in \mathbb{Z}$. Подставив в (25), после упрощений получим

$$6x \equiv -17 - 24t_1 \pmod{11}.$$

Имеем НОД $(6, 11) = 1$, поэтому никаких ограничений на t_1 не будет. Решая последнее сравнение, мы находим

$$x = -34 - 48t_1 + 11t_2,$$

где $t_2 \in \mathbb{Z}$. Осталось найти неизвестное z:

$$z = \frac{30x + 24y - 11}{55} = \frac{30(-34 - 48t_1 + 11t_2) + 24(4 + 5t_1) - 11}{55} = \\ = -17 - 24t_1 + 6t_2.$$

Таким образом, все решения данного уравнения — это тройки целых чисел вида

$$(x, y, z) = (-34 - 48t_1 + 11t_2, 4 + 5t_1, -17 - 24t_1 + 6t_2), \quad t_1, t_2 \in \mathbb{Z}.$$

В заключение обсудим вопрос о *конструктивном доказательстве* китайской теоремы об остатках (теорема 9 раздела I).

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 (это и есть утверждение китайской теоремы об остатках).

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 будет иметь единственное решение, которое мы обозначим $[M_i^*]_{m_i}$. Теперь в качестве искомого числа r мы можем взять наименьший неотрицательный вычет числа

$$R = M_1 M_1^* r_1 + \ldots + M_k M_k^* r_k \tag{26}$$

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 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 (26) при r_i, пробегающих полные системы вычетов по модулям m_i, $i = 1, \ldots, k$, образуют полную систему вычетов по модулю m — см. упражнение 3, где $k = 2$.

Замечание. Короткое «культурное» доказательство китайской теоремы об остатках и свойства мультипликативности функции Эйлера таково: *отображение*

$$[r]_m \to ([r]_{m_1}, [r]_{m_2})$$

является изоморфизмом колец Z_m и $Z_{m_1} \times Z_{m_2}$, который индуцирует изоморфизм их мультипликативных групп Z_m^* и $Z_{m_1}^* \times Z_{m_2}^*$.

III. Кольца классов вычетов

§ 1. Кольцо Z_m классов вычетов по модулю m

Конструкция кольца Z_m классов вычетов по модулю m. Арифметика по модулю m. Делители нуля в Z_m и критерий их отсутствия.

В § 2 раздела II было введено множество Z_m всех классов вычетов по модулю m. Напомним, что классом вычетов по модулю m с представителем $a \in \mathbb{Z}$ называется множество

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

Основная цель этого параграфа — ввести на множестве Z_m алгебраическую структуру кольца.

Прежде всего, необходимо определить на Z_m две операции — сложение и умножение.

Определение 1. *Суммой классов вычетов* $[a]$ и $[b]$ называется класс вычетов, содержащий число $a + b$:

$$[a] + [b] = [a + b].$$

Определение 2. *Произведением классов вычетов* $[a]$ и $[b]$ называется класс вычетов, содержащий число ab:

$$[a] \cdot [b] = [ab].$$

Сразу возникает вопрос о корректности этих определений, а именно, однозначным ли образом определяются сумма и произведение двух данных классов — ведь они могут быть заданы разными представителями.

В качестве ответа приводим следующее утверждение.

Теорема 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. § 1 раздела II), 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 1. Рассмотрим множество

$$Z_{12} = \{[0], [1], \ldots, [11]\}.$$

Приведём несколько примеров на сложение и умножение:

$$[5] + [8] = [1], \quad [5] \cdot [8] = [4], \quad [3] \cdot [8] = [0].$$

Последнее равенство выглядит особенно необычно, к нему мы вернёмся в конце параграфа.

В общем случае нетрудно заметить, что сумма классов $[a] + [b]$ 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 подобное утверждение уже, вообще говоря, не имеет места. Мы можем только утверждать, что

$$\{a_1 b_1 : a_1 \in [a],\ b_1 \in [b]\} \subset [a] \cdot [b].$$

Упражнение 1. Пусть $m = 7$. Покажите, что класс вычетов $[6]$ содержит элемент, не принадлежащий множеству $\{xy : x \in [2],\ y \in [3]\}$.

Решение. Таковым будет, например, число $13 = 6 + 7 \cdot 1 \in [6]$. 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

$$2 + 7t_1 \in \{\pm 1, \pm 13\},$$

но это невозможно ни при каком $t_1 \in \mathbb{Z}$. □

Сформулируем теперь основной результат этого параграфа.

Теорема 2. *Множество Z_m классов вычетов по модулю m с операциями сложения и умножения образует коммутативное кольцо с единицей.*

Доказательство. Убедимся, что условия, определяющие коммутативное кольцо с единицей, выполнены в случае 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 $[0]$, 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 $[a]$ противоположным является класс $[-a]$, содержащий число $-a$. В самом деле,

$$[a]+[-a]=[a+(-a)]=[0].$$

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 $[1]$, так как

$$[a]\cdot[1]=[a\cdot 1]=[a].$$

Итак, проверена выполнимость всех условий, определяющих коммутативное кольцо с единицей. □

Кольцо Z_m называется *кольцом классов вычетов по модулю* m. Выполнение условий 1 — 4 означает, что относительно операции сложения множество Z_m образует абелеву группу — она называется *аддитивной группой кольца* Z_m. В частности, мы можем стандартным образом определить операцию вычитания классов:

$$[a]-[b]=[a]+[-b].$$

Далее, обычным для колец образом можно ввести операции умножения класса на целое число и возведения класса в целую неотрицательную степень.

Определение 3. Пусть $[a]\in Z_m$ 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 $[a]\in Z_m$ имеют место равенства

$$c[a]=[ca],\quad [a]^n=[a^n],$$

где c и n — целые числа, $n\geqslant 0$. (Действительно, классы $c[a]$ и $[ca]$ имеют общий элемент ca и потому совпадают; второе равенство доказывается аналогично.)

Определение 4. Пусть $[a] \in Z_m$ и $f(x) = c_0x^n + c_1x^{n-1} + \ldots + c_n$ — произвольный многочлен с целыми коэффициентами. Значением многочлена $f(x)$ при $x = [a]$ называется

$$f([a]) = c_0[a]^n + c_1[a]^{n-1} + \ldots + c_n[1] \in Z_m.$$

Нетрудно видеть, что для любого $[a] \in Z_m$ выполняется равенство

$$f([a]) = [f(a)].$$

В заключение обсудим одну особенность арифметики кольца Z_m, или *арифметики по модулю* m. Из примера 1 видно, что произведение двух ненулевых классов $[a]$ и $[b]$ может оказаться равным нулевому классу $[0]$. Напомним следующее

Определение 5. Элемент $\alpha \neq 0$ кольца называется *делителем нуля*, если существует элемент $\beta \neq 0$ этого же кольца такой, что $\alpha\beta = 0$.

Таким образом, кольцо Z_m — это кольцо, в котором, вообще говоря, могут быть делители нуля.

Теорема 3. *В кольце Z_m классов вычетов по модулю m нет делителей 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 $[m_i] \neq [0]$ и потому являются делителями нуля.

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 множителей кратен p. Следовательно, $[a] = [0]$ или $[b] = [0]$, и делителей нуля нет. □

Итак, кольцо Z_m является *областью целостности* (коммутативным кольцом с единицей и без делителей нуля) в том и только том случае, когда $m = p$ — простое число.

Напомним (см. § 2 раздела II), что класс вычетов $[a] \in Z_m$ называется взаимно простым с модулем, если НОД $(a, m) = 1$.

Упражнение 2. Докажите, что:

а) никакой взаимно простой с модулем класс вычетов $[a] \in Z_m$ не может быть делителем нуля;

б) если НОД $(a, m) > 1$, то класс вычетов $[a] \in Z_m$ является делителем нуля.

Из упражнения 2 следует, что в кольце Z_m всякий класс вычетов либо взаимно прост с модулем, либо является делителем нуля.

§2. Группа обратимых элементов кольца Z_m

Обратимые классы вычетов по модулю m. Группа обратимых элементов кольца 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 $[b]$, $[a] \in Z_m$ мы понимаем нахождение такого класса $[c] \in Z_m$ (*частного* от деления данных классов), что

$$[b] = [c] \cdot [a].$$

Пример 2. Рассмотрим кольцо Z_{24} классов вычетов по модулю 24.

В этом кольце можно *единственным образом* разделить класс $[16]$ на класс $[5]$:

$$[16] = [8] \cdot [5].$$

Деление класса $[12]$ на класс $[18]$ *возможно, но не однозначно*:

$$[12] = [2] \cdot [18] = [6] \cdot [18].$$

Наконец, класс $[9]$ *нельзя* разделить на класс $[10]$: равенство

$$[9] = [x] \cdot [10]$$

означало бы, что $9 \equiv 10x \pmod{24}$, но это невозможно ни при каком целом x. Очевидно, такое разнообразие ситуаций вызвано наличием в кольце Z_{24} делителей нуля.

Далее мы рассмотрим вопрос о том, когда операция деления классов вычетов возможна, причём частное определено однозначно.

Определение 6. Если для данного класса $[a] \in Z_m$ существует такой класс $[x] \in Z_m$, что

$$[a] \cdot [x] = [1], \tag{1}$$

то он называется *обратным* к $[a]$. Сам же класс $[a]$ в этом случае называется *обратимым*.

Обозначение: $[x] = [a]^{-1}$.

Упражнение 3. Докажите *единственность* обратного класса вычетов.

Не всякий класс вычетов обратим: например, можно показать, что делители нуля $[a] \in Z_m$ не имеют обратных.

Упражнение 4. Докажите это утверждение.

Оказывается, все остальные классы вычетов обратимы.

Теорема 4. *Если класс вычетов $[a] \in Z_m$ взаимно прост с модулем, то он обратим.*

Доказательство. Равенство (1) равносильно сравнению

$$ax \equiv 1 \pmod{m}.$$

Поскольку НОД $(a, m) = 1$, по теореме 7 раздела II это сравнение однозначно разрешимо. Его единственное решение $[r_0]$ и есть искомый обратный класс: $[a]^{-1} = [r_0]$. □

Замечание. В § 4 раздела II разъяснено, как следует на практике искать r_0. Там же приведена и явная формула для r_0, используя которую, мы можем записать

$$[a]^{-1} = [a^{\varphi(m)-1}]. \tag{2}$$

Однако возможности практического применения этой формулы ограничены лишь небольшими значениями модуля m.

Таким образом, класс вычетов $[a] \in Z_m$ обратим тогда и только тогда, когда этот класс взаимно прост с модулем m. Напомним, что таких классов всего имеется $\varphi(m)$ штук, где $\varphi(m)$ — функция Эйлера, а их множество обозначается Z_m^*.

Упражнение 5. Докажите, исходя из определения Z_m^*, что это множество замкнуто относительно умножения.

Пример 3. Рассмотрим кольцо Z_{10}.

Имеем $Z_{10}^* = \{[1], [3], [7], [9]\}$, $\varphi(10) = 4$. По формуле (2) находим

$$[1]^{-1} = [1], \quad [3]^{-1} = [7], \quad [7]^{-1} = [3], \quad [9]^{-1} = [9].$$

Видно, что множество 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, Z_m^* — группа обратимых элементов кольца Z_m. Она, очевидно, абелева и конечна; её порядок, т. е. число элементов, равен $\varphi(m)$. Если модуль m есть простое число p, то группу обратимых элементов Z_p^* составляют *все* ненулевые классы (так как $\varphi(p) = p - 1$).

Пример 4. Найдём три последние цифры числа $A = 1997^{1997}$.

Речь идёт о вычислении $[1997]^{1997}$ в группе 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:

$$[-3]^{\varphi(1000)} = [-3]^{400} = [1],$$

а также равенством $333^3 = (333 \cdot 3)^2 \cdot 37$.

Итак, $A = \ldots 037$.

Пример 5. Используя вычисления в группе Z_p^*, дадим ещё одно доказательство теоремы Вильсона (см. § 3 раздела II).

Это доказательство основано на следующем наблюдении: среди всех классов вычетов $[a] \in Z_p^*$ только два класса являются обратными к самим себе: это $[1]$ и $[p-1] = -[1]$. В самом деле, если $[a] \neq \pm[1]$, то

$$[a] \neq [a]^{-1},$$

так как иначе сравнение

$$x^2 - 1 \equiv 0 \pmod{p}$$

имело бы более двух решений, что невозможно.

Но в таком случае все классы вычетов $[a] \in Z_p^*$, 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. □

Вернемся теперь к вопросу, которым мы задавались в начале параграфа — о существовании и единственности частного двух классов.

Теорема 5. *В кольце Z_m возможно, и притом единственным образом, деление на любой класс $[a] \in Z_m^*$. Частное от деления класса $[b]$ на $[a]$ определяется по формуле*

$$[c] = [b] \cdot [a]^{-1}.$$

Упражнение 6. Докажите эту теорему.

Пример 6. В кольце Z_{24} разделим класс $[18]$ на класс $[7]$.

Поскольку $[7] \in Z_{24}^*$, это возможно. Имеем $[7]^{-1} = [7]$, поэтому единственное частное равно

$$[18] \cdot [7]^{-1} = [18] \cdot [7] = [6].$$

Упражнение 7. Пусть $[a_i]$, $[b_i] \in Z_m$, при этом $[a_i] \in Z_m^*$ для $i = 1, 2$. Докажите, что частные от деления $[b_i]$ на $[a_i]$ равны тогда и только тогда, когда

$$b_1 a_2 \equiv b_2 a_1 \pmod{m}. \tag{3}$$

Решение. Обозначим через $[c_i]$ частное от деления $[b_i]$ на $[a_i]$. По теореме 5 имеем $[c_i] = [b_i] \cdot [a_i]^{-1}$. Это означает, что

$$b_i \equiv c_i a_i \pmod{m}, \quad i = 1, 2. \tag{4}$$

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 (3) выполняется.

Обратно, пусть имеет место сравнение (3). Учитывая (4), имеем

$$c_1a_1a_2 \equiv b_1a_2 \equiv b_2a_1 \equiv c_2a_2a_1 \pmod{m},$$
$$c_1a_1a_2 \equiv c_2a_2a_1 \pmod{m}.$$

Сокращая на a_1a_2, получим $c_1 \equiv c_2 \pmod{m}$, т. е. $[c_1] = [c_2]$. □

§3. Поле Z_p классов вычетов по простому модулю p

Поле Z_p классов вычетов по простому модулю p. Арифметика по простому модулю p. Многочлены над Z_p. Теорема Вильсона как частный случай формул Виета.

Напомним следующее

Определение 7. Коммутативное кольцо с единицей, отличной от нуля, в котором каждый ненулевой элемент обратим по умножению, называется *полем*.

Когда кольцо классов вычетов Z_m является полем? Ответ даёт

Теорема 6. *Кольцо Z_m является полем тогда и только тогда, когда $m = p$ — простое число.*

Доказательство. Как известно, в поле отсутствуют делители нуля, поэтому если m — составное число, то Z_m — не поле (см. теорему 3).

С другой стороны, если $m = p$ — простое число, то, как уже отмечалось, группа обратимых элементов Z_p^* состоит из всех ненулевых классов вычетов. Следовательно, Z_p — поле. □

Замечание. Вообще, *всякая конечная область целостности является полем*.

Упражнение 8. Докажите это утверждение.

Таким образом, в поле классов вычетов Z_p по простому модулю можно выполнять все четыре арифметических действия. Рассмотрим несколько примеров, в которых так или иначе задействована арифметика поля Z_p.

Пример 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 Z_p, то x^{-1} также пробегает это множество. Следовательно,

$$S = [1] + [2] + \ldots + [p-1] = [1 + 2 + \ldots + (p-1)] = \\ = [(p-1)p/2] = [0].$$

Замечание. Полученный результат допускает следующее толкование: 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:

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{25}{12}$$

и 25 делится на 5.

Упражнение 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 8. Натуральные числа a, b, c таковы, что

$$ab + 9b + 81 \equiv 0 \pmod{101}, \quad bc + 9c + 81 \equiv 0 \pmod{101}. \qquad (5)$$

Докажем, что число $ca + 9a + 81$ делится на 101.

Заметим, что 101 — простое число. Это позволяет нам рассматривать сравнения (5) как *равенства*

$$\alpha\beta + [9]\beta + [81] = [0], \quad \beta\gamma + [9]\gamma + [81] = [0]$$

в поле Z_{101}, где введены обозначения $\alpha = [a]$, $\beta = [b]$, $\gamma = [c]$. Далее эти равенства можно исследовать *алгебраически* и выразить, скажем, α и γ через β:

$$\alpha = -\frac{[9](\beta + [9])}{\beta}, \quad \gamma = -\frac{[81]}{\beta + [9]}$$

(здесь мы, конечно, пользуемся тем, что $\beta \neq [0]$ и $\beta \neq -[9]$). Если теперь всё это подставить в выражение

$$\gamma\alpha + [9]\alpha + [81],$$

то после упрощения получится тождественный $[0]$. Осталось вернуться от классов вычетов к числам.

Специфика арифметики поля Z_p (или *арифметики по простому модулю* p) состоит в том, что

$$\alpha^p = \alpha \tag{6}$$

для любого элемента $\alpha \in Z_p$ (так можно истолковать утверждение малой теоремы Ферма, см. § 2 раздела II). Можно показать, что это свойство *характеризует* поле Z_p, т. е. присуще только этому полю. Как следствие, получаем

$$(\alpha_1 + \alpha_2 + \ldots + \alpha_k)^p = \alpha_1 + \alpha_2 + \ldots + \alpha_k$$

для любых элементов $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_k \in Z_p$, а также

$$\alpha^{p-1} = [1], \quad \alpha^{-1} = \alpha^{p-2},$$

если $\alpha \neq [0]$.

Пример 9. Пусть $\alpha \in Z_p$. 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 уже была вычислена в примере 7. Пусть теперь $\alpha \neq [1]$. Мы можем воспользоваться тождеством

$$\sum_{j=1}^{p-1} ja^j = \frac{pa^p}{a-1} - \frac{a(a^p-1)}{(a-1)^2}, \quad a \neq 1,$$

справедливом в любом поле. В поле Z_p правая часть этого тождества редуцируется до

$$\frac{\alpha}{1-\alpha}$$

(мы учли соотношение (6), а также то, что $p\alpha = [0]$).

Как и над всяким полем, над полем Z_p можно рассматривать многочлены. Некоторые из доказанных нами ранее фактов превращаются в частные случаи общих теорем теории многочленов. Например, теорема о том, что всякое сравнение по модулю p степени n имеет не более n решений (теорема 5 раздела II) — частный случай хорошо известной теоремы, которая гласит: *любой многочлен с коэффициентами из некоторого поля не может иметь корней больше, чем его степень*.

Другой пример: теорема Вильсона (см. § 3 раздела II) на самом деле является частным случаем *формул Виета*, выражающих элементарные симметрические функции корней многочлена через его коэффициенты. Действительно, многочлен

$$f(x) = x^{p-1} - [1]$$

над Z_p имеет в этом поле $p-1$ корней — как легко видеть, ими являются все элементы $[a] \neq [0]$ поля 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 5), это эквивалентно утверждению теоремы Вильсона.

Упражнение 10. Пусть p — простое число вида $4k+1$. Докажите, что уравнение $x^2 + [1] = [0]$ разрешимо в поле 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 $x = [(2k)!]$. □

На практике этой формулой можно пользоваться только когда p невелико. Например, при $p = 13$ находим $x = [6!] = [720] = [5]$.

Контрольный вопрос. Разрешимо ли это уравнение, если p имеет вид $4k-1$?

Ответ. Нет, см. упражнение 9 раздела II.

В заключение обратим внимание на одну особенность алгебры многочленов над полем Z_p: если $f(x)$ — произвольный многочлен с коэффициентами из 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. § 2 раздела II).

§4. Порядок класса вычетов. Первообразные корни

Порядок обратимого класса вычетов по модулю m. Теорема Эйлера — частный случай теоремы Лагранжа. Понятие первообразного корня по модулю m. Теорема Гаусса о существовании первообразного корня по простому модулю p и её различные доказательства. Критерий существования первообразного корня по модулю m.

Теорему Эйлера можно сформулировать следующим образом.

Теорема 7. *Если* $[a] \in Z_m^*$ *— обратимый класс вычетов, то*

$$[a]^{\varphi(m)} = [1].$$

Определение 8. *Порядком* класса вычетов $[a] \in Z_m^*$ называется *наименьшее* натуральное число δ такое, что $[a]^\delta = [1]$.

То, что такое число δ существует, вытекает, например, из теоремы 7, которая даже гарантирует неравенство

$$\delta \leqslant \varphi(m),$$

но может быть доказано и следующим простым рассуждением. Рассмотрим степени класса вычетов $[a]$ с произвольными натуральными показателями:

$$[a]^k, \quad k = 1, 2, \ldots$$

Так как все они принадлежат *конечной* группе Z_m^*, то

$$[a]^k = [a]^l$$

для некоторых $k > l$. Но тогда $[a]^{k-l} = [1]$, при этом $k - l \geqslant 1$.

Определение 8 можно сформулировать в следующих терминах. Пусть НОД $(a, m) = 1$. Порядком числа a по модулю m называется наименьшее натуральное число δ такое, что

$$a^\delta \equiv 1 \pmod{m}.$$

Говорят также, что число a *принадлежит показателю* δ по модулю m. Ясно, что для всех чисел из $[a]$ показатель δ, которому они принадлежат, один и тот же.

Пример 10. Найдём порядок класса вычетов $[7] \in Z_{18}^*$.

Имеем

$$[7]^1 = [7], \quad [7]^2 = [13], \quad [7]^3 = [1],$$

поэтому $\delta = 3$.

Теорема 8. *Пусть δ — порядок класса вычетов $[a] \in Z_m^*$. Равенство*

$$[a]^k = [1] \tag{7}$$

имеет место тогда и только тогда, когда $k \equiv 0 \pmod{\delta}$.

Доказательство. Неочевидным здесь является лишь утверждение «только тогда». Чтобы его доказать, разделим k на δ с остатком:

$$k = \delta q + r, \quad 0 \leqslant r < \delta.$$

Имеем $[a]^k = ([a]^\delta)^q [a]^r = [a]^r$. Следовательно, равенство (7) равносильно равенству

$$[a]^r = [1].$$

Если допустить, что $r > 0$, то получим противоречие с определением δ как наименьшего натурального числа, для которого $[a]^\delta = [1]$. □

Следствие 1. *Порядок любого класса вычетов из Z_m^* является делителем $\varphi(m)$.*

Следствие 2. *Равенство*

$$[a]^k = [a]^l$$

равносильно сравнению $k \equiv l \pmod{\delta}$.

Следствие 3. *Все классы вычетов*

$$[a]^k, \quad k = 0, 1, \ldots, \delta - 1, \tag{8}$$

попарно различны.

Упражнение 11. Выведите эти следствия теоремы 8.

Упражнение 12. Пусть порядок класса вычетов $[a] \in Z_m^*$ равен δ. Докажите, что при любом целом k порядок класса вычетов $[b] = [a]^k$ равен

$$\frac{\delta}{\text{НОД}\,(k, \delta)}.$$

Следует отметить, что теорема Эйлера, сформулированная в виде теоремы 7, а также следствие 1 теоремы 8 являются частными случаями хорошо известной в теории групп *теоремы Лагранжа*, которая гласит: *порядок элемента конечной группы делит порядок самой группы*.

Пример 11. Найдём порядок класса вычетов $[7] \in Z_{43}^*$.

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, $\delta = 6$.

Определение 9. Пусть НОД $(g, m) = 1$. Если порядок класса вычетов $[g] \in Z_m^*$ равен $\varphi(m)$, то число g называется *первообразным корнем по модулю* m.

Пример 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 наличии первообразных корней по модулю m — это вопрос о том, будет ли группа Z_m^* *циклической*, т. е. будет ли она состоять из целых степеней какого-нибудь *одного* класса вычетов. Следующая теорема впервые была доказана Гауссом.

Теорема 9. *Если модуль m есть простое число p, то первообразные корни существуют.*

Теорема Гаусса может быть сформулирована так: *мультипликативная группа поля из p элементов является циклической*.

Мы дадим два доказательства этой важной теоремы.

1-Е ДОКАЗАТЕЛЬСТВО. Оно принадлежит самому Гауссу.

Пусть δ — произвольный делитель $p - 1$ и $\psi(\delta)$ — количество классов вычетов в Z_p^*, порядок каждого из которых равен δ. Тогда либо $\psi(\delta) = 0$, либо $\psi(\delta) = \varphi(\delta)$.

Действительно, допустим, что $\psi(\delta) > 0$ и $[a]$ — некоторый класс вычетов, порядок которого есть δ. Обозначим

$$f_\delta(x) = x^\delta - [1]$$

и рассмотрим произвольный класс вычетов $[b]$, порядок которого также равен δ. Покажем, что

$$[b] = [a]^k \tag{9}$$

для некоторого целого k. В самом деле, имеем

$$f_\delta([b]) = [b]^\delta - [1] = [0].$$

Но классы вычетов (8) попарно различны и все являются корнями многочлена $f_\delta(x)$; поскольку других корней у этого многочлена нет, должно выполняться равенство (9). Далее заметим, что показатель k в (9) должен быть взаимно простым с δ числом (иначе порядок $[b]$ будет меньше δ, см. упражнение 12). Таких показателей имеется в точности $\varphi(\delta)$ штук, а значит, классов вычетов $[b]$, чей порядок равен δ, столько же, т. е. $\psi(\delta) = \varphi(\delta)$.

Итак, во всяком случае доказано, что для любого δ — делителя $p-1$ — справедливо неравенство

$$\psi(\delta) \leqslant \varphi(\delta).$$

Но имеют место равенства (второе из них — частный случай формулы (9) § 5 раздела I)

$$\sum_{\delta \,|\, p-1} \psi(\delta) = p - 1 = \sum_{\delta \,|\, p-1} \varphi(\delta),$$

поэтому на самом деле

$$\psi(\delta) = \varphi(\delta)$$

для любого δ. В частности, при $\delta = p-1$ получаем

$$\psi(p-1) = \varphi(p-1) > 0,$$

т. е. первообразные корни действительно есть. □

Замечание. Попутно мы доказали, что для любого делителя δ числа $p-1$ найдётся в точности $\varphi(\delta)$ классов вычетов, порядок которых равен этому δ.

2-Е ДОКАЗАТЕЛЬСТВО. Фактически это доказательство следующего общего утверждения: *мультипликативная группа конечного поля является циклической*. В основе рассуждения лежит один факт из теории конечных абелевых групп.

Пусть $\delta_1, \ldots, \delta_\tau$ — все значения порядков всех ненулевых классов вычетов по модулю p. Тогда найдётся такой класс вычетов $[g]$, чей порядок δ будет равен НОК $(\delta_1, \ldots, \delta_\tau)$.

Упражнение 13. Докажите это утверждение.

Указание. Пусть

$$\text{НОК}\,(\delta_1, \ldots, \delta_\tau) = \prod_{i=1}^{t} p_i^{k_i} \tag{10}$$

— каноническое разложение. Для каждого i существует такой класс вычетов $[g_i]$, чей порядок имеет вид $p_i^{k_i}Q_i$, где НОД $(Q_i, p_i) = 1$. Тогда

$$[g] = \prod_{i=1}^{t} [g_i]^{Q_i}$$

— искомый класс вычетов.

Покажем теперь, что число g и есть искомый первообразный корень.

Действительно, поскольку δ есть (10), *любой* ненулевой класс вычетов $[a]$ является корнем многочлена $f_\delta(x)$, а корней у этого многочлена может быть не более δ. Поэтому $p - 1 \leqslant \delta$. Но, с другой стороны, $\delta \leqslant p - 1$, так что $\delta = p - 1$, и всё доказано. □

Упражнение 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 $p - 1$.

Существование первообразных корней g по простому модулю p расширяет возможности арифметики поля Z_p, ибо позволяет наряду с привычным *аддитивным* взглядом на Z_p как на множество

$$\{[0], [1], \ldots, [p-1]\}$$

прибегать там, где это удобно, к другой — *мультипликативной* — точки зрения, согласно которой Z_p есть объединение

$$Z_p^* = \{[g]^0, [g]^1, \ldots, [g]^{p-2}\}$$

и нулевого элемента $[0]$.

Пример 13. В лемме 1 раздела II речь идёт, по существу, о сумме k-х $(0 < k < p - 1)$ степеней всех элементов поля Z_p.

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 14. Ещё раз докажем теорему Вильсона (см. § 3 раздела II). Имеем

$$\prod_{r=1}^{p-1}[r]=\prod_{j=0}^{p-2}[g]^j=[g]^{0+1+2+\ldots+(p-2)}=[g]^{(p-2)(p-1)/2}=[g]^{(p-1)/2}=-[1].$$

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 15. Ещё один способ решения упражнения 10: достаточно положить $x=[g]^k$.

Действительно, $x^2=[g]^{2k}=[g]^{(p-1)/2}=-[1]$. □

В заключение приведём без доказательства теорему, в которой перечисляются все значения m, для которых есть первообразные корни.

Теорема 10. *Первообразные корни существуют только при*

$$m=2,\ 4,\ p^\alpha,\ 2p^\alpha,$$

где p — нечётное простое число, α — натуральное число.

Пример 16. Пусть p — нечётное простое число и g — первообразный корень по модулю p. Найдём первообразный корень по модулю p^α.

Имеем $g^{p-1}\equiv 1 \pmod p$, т. е. $g^{p-1}-1=pa$. Предположим, что a не делится на p. Тогда g будет первообразным корнем по модулю p^α при любом натуральном α.

Упражнение 15. Докажите это утверждение индукцией по $\alpha\geqslant 1$.

Если оказалось так, что a кратно p, вместо числа g рассмотрим $g+p$. Для этого числа имеем

$$(g+p)^{p-1}-1=gp+(g^{p-1}-1)+\ldots\equiv gp \pmod{p^2},$$

т. е. $(g+p)^{p-1}-1=pA$, где число A не делится на p. Итак, в этом случае первообразным корнем по модулю p^α будет $g+p$. □

IV. Некоторые приложения теории сравнений

§ 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.

В этом и следующем параграфах мы обсудим некоторые вопросы *алгоритмической теории чисел* — интенсивно развивающегося последние тридцать лет направления в теории чисел, которое имеет важные приложения в криптографии. Актуальность этого направления неизмеримо увеличилась 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 имеют определённые границы. Приходится разбивать длинную цифровую последовательность на блоки ограниченной длины и шифровать каждый такой блок отдельно. Мы 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 Z_m. Шифрующая функция при этом может рассматриваться как некоторое взаимно однозначное отображение

$$f : Z_m \to Z_m,$$

а $a = f(x)$ 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 запись

$$a \bmod m$$

означает взятие остатка от деления a на m.) Подобный шифр использовал ещё Юлий Цезарь (I в. до н. э.). Конечно, не каждое отображение f подходит для целей надежного 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 достаточно быстрый алгоритм вычисления значений $f(x)$;
2. существует достаточно 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 схему RSA, устроена следующим образом:

$$f : x \to x^e \bmod m. \tag{1}$$

Для расшифровки сообщения $a = f(x)$ достаточно решить сравнение

$$x^e \equiv a \pmod m. \tag{2}$$

При некоторых условиях на m и e это сравнение имеет единственное решение x.

Если показатель степени e в сравнении (2) взаимно прост с $\varphi(m)$, то при условии

$$\text{НОД}\,(a, m) = 1 \tag{3}$$

сравнение (2) имеет единственное решение. Для того, чтобы найти его, определим целое число d, удовлетворяющее условиям

$$de \equiv 1 \pmod{\varphi(m)}, \quad 1 \leqslant d < \varphi(m). \tag{4}$$

Очевидно, такое число существует, и притом единственное. Если сравнение (2) разрешимо, то $\text{НОД}\,(x, m) = 1$ и по теореме Эйлера

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

Следовательно,

$$x \equiv x^{de} \equiv a^d \pmod{m}.$$

Таким образом, единственное решение сравнения (2) может быть найдено по формуле

$$x = a^d \bmod m. \tag{5}$$

Упражнение 1. Пусть число m свободно от квадратов. Докажите, что сравнение (2) будет разрешимо и без предположения (3), при этом его единственным решением будет по-прежнему (5).

Решение. Пусть $\text{НОД}\,(x, m) = r$ и $m = rm'$. Имеем

$$\text{НОД}\,(r, m') = 1, \quad \text{НОД}\,(x, m') = 1.$$

Так как $\varphi(m) = \varphi(r)\varphi(m')$, то

$$a^d = x^{ed} \equiv x \pmod{m'}, \quad a^d = x^{ed} \equiv x \pmod{r}$$

(поскольку $x \equiv 0 \pmod{r}$). Следовательно, $a^d \equiv x \pmod{m}$. □

Функция (1), принятая в системе RSA, может быть вычислена достаточно быстро (см. ниже). Обратная к $f(x)$ функция

$$f^{-1} : x \to x^d \bmod m$$

вычисляется по тем же правилам, что и $f(x)$, лишь с заменой показателя степени e на d. Таким образом, для функции (1) будут выполнены указанные выше свойства 1 и 2.

Для вычисления функции (1) достаточно знать лишь числа e и m. Они составляют *открытый ключ* для шифрования. Но вот для вычисления обратной функции требуется знать число d, которое и является «секретом», о котором идёт речь в пункте 3.

Казалось бы, ничего не стоит, зная число m, разложить его на простые сомножители, вычислить затем с помощью известных правил значение $\varphi(m)$ и, наконец, с помощью (4) определить нужное число d. Все шаги этого вычисления могут быть реализованы достаточно быстро, за исключением первого. Именно разложение числа m на простые множители и составляет наиболее трудоемкую часть вычислений. В теории чисел, несмотря на многолетнюю её историю и очень интенсивные поиски в течение последних 30 лет, эффективный алгоритм разложения натуральных чисел на множители так и не найден.

Авторы схемы RSA предложили выбирать число m в виде произведения двух простых сомножителей p и q, примерно одинаковых по величине. Так как

$$\varphi(m) = \varphi(pq) = (p-1)(q-1), \tag{6}$$

то единственное условие на выбор показателя степени e в отображении (1) есть

$$\text{НОД}\,(e, p-1) = \text{НОД}\,(e, q-1) = 1. \tag{7}$$

Итак, лицо, заинтересованное в организации шифрованной переписки с помощью схемы RSA, выбирает два достаточно больших простых числа p и q. Перемножая их, оно находит число

$$m = pq.$$

Затем выбирается число e, удовлетворяющее (7), вычисляется с помощью (6) число $\varphi(m)$ и с помощью (4) — число d. Числа m и e публикуются, число d держится в секрете. Теперь любой может отправлять зашифрованные с помощью (1) сообщения организатору этой системы, а организатор сможет легко дешифровать их с помощью (5).

Пример 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 требуется отправить сообщение $x = 362490$. В зашифрованном виде оно будет выглядеть как

$$a = x^e \bmod m = 121469.$$

Для дешифрования используем секретный ключ:

$$a^d \bmod m = 362490.$$

Видно, что получается исходное сообщение x.

Описанная выше схема RSA ставит ряд вопросов. Например: *как проводить вычисления с большими числами* и, в частности, 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, цифры в двоичном представлении, равны 0 или 1, $b_0 = 1$.

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 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 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 них.

Пусть $N > 1$ — нечётное число, и нам известно *частичное разложение* числа $N - 1$ на простые множители:

$$N - 1 = SR, \quad S = \prod_{i=1}^{l} q_i^{\alpha_i}, \quad \text{НОД}\,(R, S) = 1.$$

Это позволяет получить некоторую информацию о возможных простых делителях числа N, иногда достаточную для того, чтобы утверждать, что N — простое число.

Предложение. *Пусть для любого простого делителя q_i числа S существует такое $a_i \in \mathbb{Z}$, что*

$$a_i^{N-1} \equiv 1 \pmod{N}, \quad \text{НОД}\,(a_i^{(N-1)/q_i} - 1, N) = 1. \tag{8}$$

Тогда любой простой делитель p числа N удовлетворяет сравнению

$$p \equiv 1 \pmod{S}.$$

Доказательство. Пусть

$$S = q_i^{\alpha_i} S_i, \quad \text{НОД}\,(S_i, q_i) = 1.$$

Обозначим $Q_i = (N-1)/q_i$. Из соотношений (8) следует, что

$$a_i^{N-1} = 1, \quad a_i^{Q_i} \neq 1$$

в поле Z_p. Так как, кроме того, $a_i^{p-1} = 1$ в Z_p, то $a_i^d = 1$ в Z_p, где

$$d = \text{НОД}\,(p-1, N-1) = \text{НОД}\,(p-1, q_i^{\alpha_i} S_i R).$$

Положим $d = q_i^{\beta_i} d_i$, где $\beta_i \leqslant \alpha_i$, а d_i — делитель $S_i R$.

Если предположить, что $\beta_i \leqslant \alpha_i - 1$, то d будет делить $Q_i = q_i^{\alpha_i - 1} S_i R$ и, как следствие, получим $a_i^{Q_i} = 1$ в Z_p — противоречие. Значит,

$$\beta_i = \alpha_i, \quad d = q_i^{\alpha_i} d_i$$

и, таким образом, $q_i^{\alpha_i}$ — делитель $p-1$. Поскольку q_i — произвольный простой делитель S, то S делит $p-1$. □

Из доказанного вытекает следующая

Теорема 1. *В условиях предложения пусть выполнено неравенство*

$$R \leqslant S + 1.$$

Тогда N — простое число.

Доказательство. Действительно, пусть p — наименьший простой делитель числа N. Если N — составное, то

$$N = pN_1 \geqslant p^2 \geqslant (S+1)^2 = S(S+2) + 1 > SR + 1 = N,$$

что невозможно. □

Пример 3. Покажем, что число

$$N = \underbrace{11111111111111111111111}_{\text{23 единицы}}$$

является простым. Пусть мы знаем, что

$$N - 1 = 2 \cdot 5 \cdot 11^2 \cdot 23 \cdot 4093 \cdot 8779 \cdot R,$$

где $R = \underbrace{11111111111}_{11 \text{ единиц}}$. Для каждого простого делителя

$$q_i \in \{2, 5, 11, 23, 4093, 8779\}$$

мы можем найти такое a_i, что выполнено условие (8):

q_i	2	5	11	23	4093	8779
a_i	7	2	2	2	2	2

Так как $R < \sqrt{N}$ и, следовательно, $R \leqslant S + 1$, то N — простое число.

Замечание. Если S нечётно, то в условиях леммы справедливо более сильное сравнение

$$p \equiv 1 \pmod{2S}.$$

В этом случае в теореме 1 достаточно требовать, чтобы $R \leqslant 4S + 2$.

Покажем, как с помощью теоремы 1 можно без особых вычислительных затрат строить большие простые числа.

Пример 4. Начиная с небольшого простого числа

$$S^{(0)} = 63766529,$$

взятого из таблицы простых чисел, мы находим последовательно 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

$$a_k^{S^{(k)}-1} \equiv 1 \pmod{S^{(k)}}, \quad \text{НОД}\,(a_k^{R^{(k)}} - 1, S^{(k)}) = 1. \tag{9}$$

Имеем

$R^{(1)} = 70770834,$

$S^{(1)} = 4512810438615187,$

$R^{(2)} = 16595399667898434,$

$S^{(2)} = 74891892854283060614549525917159,$

$$R^{(3)} = 185071936333395162110485930977388,$$

$$S^{(3)} = 13860387626215326678854874421478606308305311334707\backslash 747109990200693,$$

$$R^{(4)} = 42378727533781801960162680892611644777523641072783\backslash 336534883902610,$$

$$S^{(4)} = 58738559072398005552656622556731799674072703413590\backslash 63785326808519195953944340929962449243226042298109\backslash 51076664738559313528966508731,$$

$$R^{(5)} = 12817888374282574282507855019642174889455963762363\backslash 86323812708497876581255089773742452766244396067877\backslash 61625060838989198856257857196 8,$$

$$S^{(5)} = 75290429345620062585961289159277838795453330799438\backslash 86129444961628512905368666999969290917432675517124\backslash 66689571071799483872441239435776315998897745339218\backslash 16819695640973494997260310783719905034389980059085\backslash 22505029891693589241550796725471047933413083127845\backslash 83852609.$$

Следующее простое число $S^{(6)}$ будет иметь уже более 500 десятичных знаков. Условия (9) выполняются для $a_k = 1999$, $k = 1, 2, \ldots, 5$.

При написании этого параграфа автор существенно опирался на материалы статьи Ю. В. Нестеренко «Алгоритмические проблемы теории чисел» в книге [5].

§2. Псевдопростые числа

Псевдопростые числа или как отличить составное число от простого. Числа Кармайкла, или абсолютно 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 тривиально решается при помощи *алгоритма пробных делений* (см. пример 6 раздела I).

Отправной точкой может служить та же малая теорема Ферма. Предположим, что для данного нечётного $N > 1$ нам удалось подобрать число $a \in Z_N^*$, такое, что

$$a^{N-1} \not\equiv 1 \pmod{N}.$$

Тогда, очевидно, N — составное число. Если же, напротив, имеет место сравнение

$$a^{N-1} \equiv 1 \pmod{N}, \tag{10}$$

то число N, возможно, простое.

Так, например, в Древнем Китае (примерно 25 веков назад) полагали, что нечётное число $N > 1$ является простым, если для него выполняется сравнение

$$2^{N-1} \equiv 1 \pmod{N}.$$

Основания так считать были, поскольку для *не слишком больших* N это действительно правда. Интересно отметить, что много позже, в 1680 году, Г. Лейбниц (1664 — 1716), один из создателей математического анализа, «переоткрыл» эту китайскую «теорему», и только в 1819 году французский математик П. Сарю обнаружил первый контрпример к ней — составное число

$$N = 341 = 11 \cdot 31,$$

для которого указанное сравнение имело место (см. пример 2).

Корректный способ обратить малую теорему Ферма впервые предложил в 1876 году Э. Люка (E. Lucas).

Теорема 2. *Если существует такое* $a \in \mathbb{Z}$, *что*

$$a^{N-1} \equiv 1 \pmod{N},$$

но для любого простого делителя q_i *числа* $N - 1$ *имеем*

$$a^{(N-1)/q_i} \not\equiv 1 \pmod{N},$$

то N *— простое число.*

Доказательство. Из условия теоремы следует, что порядок a как элемента группы Z_N^* равен $N - 1$.

Действительно, каждый нетривиальный делитель d числа $N - 1$ является делителем одного из чисел $(N - 1)/q_i$, поэтому из равенства $a^d = 1$ следовало бы $a^{(N-1)/q_i} = 1$, что неверно.

По теореме Эйлера $N-1$ делит $\varphi(N)$. Так как $\varphi(N) \leqslant N-1$, то

$$\varphi(N) = N-1.$$

Но это возможно только тогда, когда N — простое число. □

Упражнение 3. Убедитесь, что условие теоремы 2 является *необходимым* для простоты числа N.

Указание. В качестве a можно взять первообразный корень g по модулю N (см. упражнение 14 раздела III).

Итак, теорема Люка фактически даёт нам *критерий простоты* числа N. К сожалению, эффективно применить этот критерий можно только тогда, когда известны все простые делители числа $N-1$. Однако разложить на множители это число, как правило, практически столь же сложно, как и само число N.

Определение 1. Нечётное составное число N называют *псевдопростым по основанию* $a \in Z_N^*$, если выполняется сравнение (10).

Таким образом, число 341 — псевдопростое по основанию 2. И таких чисел — контрпримеров к китайской «теореме» — существует бесконечно много.

Упражнение 4. Докажите, что если N — псевдопростое число по основанию $a > 1$, то это же справедливо и для числа $M = a^N - 1$.

Решение. Так как N — составное, то M — тоже. Имеем $a^{N-1}-1 = Nq$ для некоторого натурального q. Тогда

$$a^{M-1} - 1 = a^{2(2^{N-1}-1)} - 1 = a^{2qN} - 1 =$$
$$= (a^N - 1)(a^{(2q-1)N} + \ldots + a^N + 1) \equiv 0 \pmod{M}.$$

Значит, число M — псевдопростое по основанию a. □

Однако число 341 уже не будет псевдопростым, например, по основанию 3, так как

$$3^{340} \equiv 56 \pmod{341}.$$

Упражнение 5. Найдите наименьшее псевдопростое число по основанию 3.

Ответ. 91.

Итак, мы можем пытаться обосновать непростоту числа N, варьируя основания a. Увы, но такой подход не всегда даёт то, что хотелось бы. Как оказывается, существуют нечётные составные числа N, которые удовлетворяют сравнению (10) *при любом* $a \in Z_N^*$.

Определение 2. Эти числа называются *числами Кармайкла*, или *абсолютно псевдопростыми числами*.

Рассмотрим, например, число

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

Так как 560 делится на каждое из чисел 2, 10, 16, то с помощью малой теоремы Ферма легко проверить, что 561 есть число Кармайкла. Другие примеры абсолютно псевдопростых чисел:

$$1105 = 5 \cdot 13 \cdot 17, \quad 1729 = 7 \cdot 13 \cdot 19.$$

Можно доказать (R. D. Carmichael, 1912 год), что любое из таких чисел имеет вид

$$N = \prod_{i=1}^{t} p_i,$$

где $t \geqslant 3$ и все простые числа p_i различны, причем $N - 1$ делится на каждую разность $p_i - 1$.

Упражнение 6. Докажите это утверждение.

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 (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 должно 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 (10) следует, что

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

В частности, $N - 1$ делится на $p - 1$. □

Упражнение 7. Докажите, что если N — число Кармайкла, то

$$a^N \equiv a \pmod{N}$$

для всех $a \in \mathbb{Z}$.

Указание. Установите сравнение $a^N \equiv a \pmod{p_i}$ для любого простого делителя p_i числа N.

Относительно недавно, в 1995 году, было доказано, что чисел Кармайкла существует *бесконечно много*.

В 1976 году Миллер предложил вместо (10) проверять несколько иное условие. Если N — нечётное простое число,

$$N - 1 = 2^l R,$$

где R нечётно, то для каждого $a \in Z_N^*$ по крайней мере один из сомножителей в произведении

$$(a^R - 1)\prod_{i=0}^{l-1}(a^{2^i R} + 1) = a^{N-1} - 1 \equiv 0 \pmod{N}$$

делится на N. Обращение этого свойства можно использовать, чтобы отличать составные числа от простых.

Определение 3. Нечётное составное число N называют *строго псевдопростым по основанию* $a \in Z_N^*$, если либо

$$a^R \equiv 1 \pmod{N}, \tag{11}$$

либо для некоторого i, $0 \leqslant i \leqslant l - 1$,

$$a^{2^i R} \equiv -1 \pmod{N}. \tag{12}$$

Пример 5. Покажем, что число $3277 = 29 \cdot 113$ является строго псевдопростым по основанию 2.

Действительно, имеем $3276 = 2^2 \cdot 819$,

$$2^{819} \equiv 128 \not\equiv \pm 1 \pmod{3277}, \quad 2^{2\cdot 819} \equiv 128^2 \equiv -1 \pmod{3277}.$$

Кстати, наименьшее строго псевдопростое число по основанию 2 — это $2047 = 23 \cdot 89$.

Упражнение 8. Проверьте это.

Как доказал Рабин в 1980 году, если N — нечётное составное число, то количество оснований a, по которым оно окажется строго псевдопростым (т. е. будет выполнено либо сравнение (11), либо одно из сравнений (12)), будет меньше, чем $(N-1)/4$.

Следующий вероятностный алгоритм, отличающий составные числа от простых, носит название *теста Миллера — Рабина*.

А. Выберем случайным образом $a \in Z_N^*$ и проверим, будут ли выполнены сравнение (11) и сравнения (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 меньшей 4^{-1}. А вероятность не определить его как составное после k итераций будет меньше 4^{-k}, т. е. убывает очень быстро.

Опишем ещё один классический вероятностный тест, который основан на понятии псевдопростоты по Эйлеру.

Определение 4. Нечётное составное число N называется *псевдопростым числом Эйлера по основанию* $a \in Z_N^*$, если

$$a^{(N-1)/2} \equiv (a/N) \pmod{N}. \tag{13}$$

Это понятие было введено Робинсоном в 1957 году. Здесь (a/N) — так называемый *символ Якоби*, принимающий лишь два значения ± 1 и который можно вычислить эффективно (см. [1, гл. 5]). Для простых N символ Якоби превращается в *символ Лежандра* и сравнение (13) выполняется по *критерию Эйлера* (см. там же).

Следующий вероятностный алгоритм называется *тестом Соловея — Штрассена*.

А. Выберем случайным образом $a \in Z_N^*$ и проверим сравнение (13).

Б. Если оно не выполнено, то число N — составное.

В. Если сравнение (13) имеет место, возвращаемся к шагу А.

Авторы этого теста доказали, что если N — нечётное составное число, то количество оснований a, по которым оно окажется псевдопростым числом Эйлера, не превосходит $\varphi(N)/2$. Таким образом, если тест Соловея — Штрассена применить к составному числу k раз, то вероятность не определить его как составное будет меньше 2^{-k}.

На практике оба теста работают очень хорошо и, в частности, справляются с числами Кармайкла. Тест Соловея — Штрассена *слабее* теста Миллера — Рабина в следующем смысле: если составное число прошло один цикл теста Миллера — Рабина и не определилось как составное, то с тестом Соловея — Штрассена будет та же история. Другими словами, справедлива следующая

Теорема 3. *Если N — строго псевдопростое число по основанию a, то N — псевдопростое число Эйлера по основанию a.*

Доказательство этой теоремы мы приводить не будем.

Читателю, желающему более основательно познакомиться с проблемами алгоритмической теории чисел и её приложениями к криптографии, рекомендуем обратиться к монографии [6] (см. также учебник [7]).

Заключение

По разным причинам за рамками настоящего курса лекций остались такие традиционно излагаемые разделы элементарной теории чисел как квадратичные вычеты (включая закон взаимности) и аппарат непрерывных дробей, непосредственно связанный с алгоритмом Евклида. Кроме этого, тема «Первообразные корни» обычно подразумевает и рассказ об индексах (дискретных логарифмах).

В планируемом учебном пособии по курсу теории чисел автор надеется восполнить эти пробелы, а сейчас отсылает читателя к классическим учебникам [1], [2], где указанные разделы присутствуют (см. также недавно вышедшее и оригинальное по стилю изложения учебное пособие [4]).

Список литературы

1. *Виноградов И.М.* Основы теории чисел. М.: Наука, 1981.
2. *Бухштаб А.А.* Теория чисел. М.: Просвещение, 1966.
3. *Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б.* Введение в теорию чисел. М.: Изд-во МГУ, 1995.
4. *Сизый С.В.* Лекции по теории чисел. М.: ФИЗМАТЛИТ, 2007.
5. Введение в криптографию / Под общ. ред. В. В. Ященко. М.: МЦНМО, 1999.
6. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2006.
7. *Черемушкин А.В.* Лекции по арифметическим алгоритмам в криптографии. М.: МНЦМО, 2002.