Е. Б. Маховенко

# Теоретико-числовые методы в криптографии

| Номер шага | $u(x)$ | | | | | | $v(x)$ | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $x^5$ | $x^4$ | $x^3$ | $x^2$ | $x^1$ | $x^0$ | $x^5$ | $x^4$ | $x^3$ | $x^2$ | $x^1$ | $x^0$ | |
| 1 | 1 | 3 | 3 | 2 | 0 | 0 | 1 | 2 | 2 | 1 | 0 | | $g(x) = 1$ |
| 2 | | 1 | 3 | 3 | 2 | 0 | | 1 | 2 | 2 | 1 | | $g(x) = x$ |
| 4.1 | | | 1 | 3 | 3 | 2 | | | | | | | |
| 4.3 | $u(x) = -(u(x) - 2 \cdot v(x))$ | | | | | | | | | | | | |
| | | | 1 | 1 | 1 | 0 | | | | | | | |
| 4.1 | | | | 1 | 1 | 1 | | | | | | | |
| 4.3 | $v(x) = v(x) - u(x)$ | | | | | | | | | | | | |
| | | | | | | | | 1 | 1 | 1 | 0 | | |
| 4.2 | | | | | | | | | 1 | 1 | 1 | | |
| 4.3 | $u(x) = u(x) - v(x)$ | | | | | | | | | | | | |
| | | | | | | 0 | | | | | | | |

Гелиос АРВ

Е. Б. МАХОВЕНКО

# ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

*Допущено Учебно-методическим объединением вузов по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям группы «Информационная безопасность»*

Москва
**«Гелиос АРВ»**
2006

УДК [00.3.26:004.056](075.8)

ББК 32.973.202-01я73-1

М42

Рецензенты:

*Яковлев В. А.* — доктор технических наук, профессор кафедры Военного университета связи,

*Шехунова Н. А.* — кандидат технических наук, профессор кафедры информационных систем Санкт-Петербурского государственного университета аэрокосмического приборостроения.

**Маховенко Е. Б.**

М42 Теоретико-числовые методы в криптографии: Учебное пособие / Е. Б. Маховенко. — М.: Гелиос АРВ, 2006. — 320 с., ил.

ISBN 5-85438-143-5

В учебном пособии излагаются методы решения алгебраических и теоретико-числовых задач, возникающих при разработке и исследовании криптографических методов и средств защиты информации. Изучаются алгоритмы арифметики больших целых чисел и полиномов, проверки чисел на простоту и разложения на множители. Исследуется безопасность криптосистем RSA, Диффи–Хеллмана, ранцевых криптосистем.

Приведены примеры практических заданий по реализации ряда алгоритмов.

Для студентов, обучающихся по специальности «Компьютерная безопасность».

ББК 32.973.202-01я73-1

© Маховенко Е. Б., 2006

ISBN 5-85438-143-5

© Оформление. Издательство «Гелиос АРВ», 2006

# ВВЕДЕНИЕ

Учебное пособие предназначено для подготовки математиков по специальности 090102 «Компьютерная безопасность» и обеспечивает дисциплину «Теоретико-числовые методы в криптографии», предусмотренную Государственным образовательным стандартом высшего профессионального образования. Дисциплина ставит своей целью обучение студентов принципам и методам численного решения алгебраических и теоретико-числовых задач, возникающих при разработке и исследовании криптографических методов и средств защиты информации.

Книга подготовлена на основе курса лекций, читаемых с 1998 года на кафедре «Информационная безопасность компьютерных систем» Санкт-Петербургского государственного политехнического университета для студентов специальностей 090102 «Компьютерная безопасность» и 090105 «Комплексное обеспечение информационной безопасности автоматизированных систем». Курс охватывает основные математические задачи, положенные в основу безопасности криптосистем с открытым ключом: задачу разложения числа на множители, задачу дискретного логарифмирования, задачу об укладке ранца, а также базовые вычислительные алгоритмы в кольце целых чисел.

Представленный материал дает начальное представление о высшей алгебре и теории чисел и доступен студентам младших курсов технических вузов. Полученные знания и навыки используются в дальнейшем при изучении дисциплин «Алгебра», «Криптографические методы защиты информации», «Криптографические протоколы».

Пособие включает в себя восемь глав. В главе 1 вводится понятие кольца целых чисел и его основные свойства. Практическая составляющая этой главы представлена алгоритмами вычисления наибольшего общего делителя.

В главе 2 рассматриваются свойства простых чисел и сравнений, символы Лежандра и Якоби, а также методы решения сравнений первой и второй степени.

В главе 3 рассматриваются конечные и бесконечные непрерывные дроби, изучаются соотношения между подходящими дробями, приводятся примеры использования непрерывных дробей для решения уравнений.

В главе 4 изучаются основные арифметические операции над целыми числами и полиномами. Приведены различные способы умножения: в классах вычетов, с помощью быстрого преобразования Фурье, а также метод Монтгомери модульного умножения.

Алгоритмы проверки чисел на простоту и разложения на множители, рассматриваемые в главах 5 и 6, разделены на вероятностные, использующие генераторы случайных чисел, и детерминированные. В главе 6 изучается также криптографическая система RSA и простейшие методы ее анализа.

В главе 7 сформулирована задача дискретного логарифмирования в конечном поле и приведены некоторые методы ее решения. Приводятся протоколы Диффи–Хеллмана и Месси–Омуры и устанавливается их связь с задачей дискретного логарифмирования.

В главе 8 приведены основные понятия теории решеток и алгоритм Ленстры–Ленстры–Ловаша, используемый для минимизации базиса решетки при исследовании ранцевых криптоалгоритмов.

Большинство определений, теорем и алгоритмов иллюстрируется примерами. В конце каждой главы приведены упражнения, закрепляющие теоретический материал. В приложение включены лабораторные работы, позволяющие получить практические навыки реализации и анализа вычислительных алгоритмов.

Пособие может использоваться при подготовке студентов по специальностям, входящим в группу «Информационная безопасность».

## Глава 1

# ДЕЛИМОСТЬ В КОЛЬЦЕ ЦЕЛЫХ ЧИСЕЛ

Определение 1.1. Множество $\mathbb{N}$ *натуральных чисел* определяется с использованием *аксиом Пеано*:

1. $1 \in \mathbb{N}$ (единица — натуральное число).
2. Для любого $a \in \mathbb{N}$ существует единственное последующее $a^+ \in \mathbb{N}$.
3. Для любого $a \in \mathbb{N}$ выполняется неравенство $a^+ \neq 1$ (единица — наименьшее натуральное число).
4. Если $a^+ = b^+$, то $a = b$ (каждое последующее число обладает единственным предыдущим).
5. Если некоторое подмножество $N \subseteq \mathbb{N}$ содержит единицу и для каждого натурального числа $a \in N$ выполняется $a^+ \in N$, то $N = \mathbb{N}$ (принцип индукции).

Таким образом,

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}.$$

На основании этих аксиом строится арифметика натуральных чисел, включающая следующие операции сложения и умножения. Каждой паре натуральных чисел $a$, $b$ можно единственным образом сопоставить их *сумму* — натуральное число $a + b = (\ldots(a^+)^+\ldots)^+$ ($b$ раз) так, чтобы выполнялись условия для любых натуральных чисел $a$, $b$, $c$:

1) $a + 1 = a^+$;
2) ассоциативность сложения: $(a + b) + c = a + (b + c)$;
3) коммутативность сложения: $a + b = b + a$;
4) если $a + b = a + c$, то $b = c$.

Упражнение. Доказать равенства 2–4, исходя из аксиом Пеано.

Каждой паре натуральных чисел $a$, $b$ можно единственным образом сопоставить их *произведение* — натуральное число

$a \cdot b = (\ldots(a + a) + \ldots + a)$ ($b$ раз) так, чтобы выполнялись условия для любых натуральных чисел $a$, $b$, $c$:

1) $a \cdot 1 = a$;

2) $a \cdot b^{+} = a \cdot b + a$;

3) ассоциативность умножения: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

4) коммутативность умножения: $a \cdot b = b \cdot a$;

5) дистрибутивность умножения относительно сложения: $a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$;

6) если $a \cdot b = a \cdot c$, то $b = c$.

Упражнение. Доказать равенства 5, 6, исходя из аксиом Пеано и свойств сложения.

Из аксиом Пеано 2–4 следует, что множество натуральных чисел *линейно упорядочено*: для любых $a, b \in \mathbb{N}$ выполняется ровно одно из трех условий:

$$a > b,\ a < b,\ a = b.$$

Отношение «<» (как и отношение «>») транзитивно, то есть из неравенств $a < b$ и $b < c$ следует, что $a < c$. Если для $a, b \in \mathbb{N}$ выполняется одно из соотношений $a > b$ или $a = b$, то записывают $a \leq b$ или $b \geq a$.

Определение 1.2. Множество $\mathbb{Z}$ *целых чисел* определим как объединение множеств натуральных чисел, отрицательных натуральных чисел и нуля: $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N}) \cup \{0\}$, таким образом

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

На множестве $\mathbb{Z}$ целых чисел операции сложения и умножения задаются теми же правилами, что и для натуральных чисел.

## 1.1. Делимость в кольце целых чисел

Определение 1.3. Пусть над некоторым множеством $\Omega$ произвольной природы определены операции сложения «+» и умножения «·». Множество $\Omega$ называется *кольцом*, если выполняются следующие условия:

1) сложение коммутативно: $a + b = b + a$ для любых $a, b \in \Omega$;
2) сложение ассоциативно: $(a + b) + c = a + (b + c)$ для любых $a$, $b$, $c \in \Omega$;
3) существует *нулевой* элемент $0 \in \Omega$ такой, что $a + 0 = a$ для любого $a \in \Omega$;
4) для каждого элемента $a \in \Omega$ существует *противоположный* элемент $-a \in \Omega$ такой, что $(-a) + a = 0$;
5) умножение дистрибутивно относительно сложения:

$$a \cdot (b + c) = a \cdot b + a \cdot c, (a + b) \cdot c = a \cdot c + b \cdot c$$

для любых $a, b, c \in \Omega$.

Если в кольце $\Omega$ умножение коммутативно: $a \cdot b = b \cdot a$ для любых $a, b \in \Omega$, то кольцо называется *коммутативным*.

Если в кольце $\Omega$ умножение ассоциативно: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ для любых $a, b, c \in \Omega$, то кольцо называется *ассоциативным*.

Если в кольце $\Omega$ существует *единичный* элемент $e$ такой, что $a \cdot e = e \cdot a = a$ для любого $a \in \Omega$, то кольцо называется *кольцом с единицей*.

Если в ассоциативном, коммутативном кольце $\Omega$ с единицей для каждого ненулевого элемента $a$ существует *обратный* элемент $a^{-1} \in \Omega$ такой, что $a \cdot a^{-1} = a^{-1} \cdot a = e$, то кольцо называется *полем*.

Пример 1.1. Множество $\mathbb{Z}$ целых чисел является коммутативным, ассоциативным кольцом с единицей. Нулевым элементом является

число 0, единичным элементом — число 1. Для каждого целого числа $a$ противоположным элементом является число $-a$. □

Пример 1.2. Множество $2\mathbb{Z}$ четных чисел является коммутативным, ассоциативным кольцом без единицы. □

Пример 1.3. Множество квадратных матриц, элементами которых являются рациональные числа, с обычной операцией сложения матриц и операцией йорданова умножения: $A \cdot B = \frac{1}{2}(AB + BA)$, где в скобках — обычное умножение матриц, является неассоциативным, коммутативным кольцом с единицей. □

Пример 1.4. Множество подмножеств некоторого множества с операциями симметрической разности («сложение») и пересечения («умножение») является ассоциативным, коммутативным кольцом с единицей. □

Пример 1.5. Множество $\mathbb{Q}$ рациональных чисел и множество $\mathbb{R}$ вещественных чисел являются полями. □

Определение 1.4. Говорят, что целое число $a$ *делится* (нацело) на целое число $b > 0$ (или что целое число $b > 0$ делит целое число $a$), если существует такое целое число $c$, что $a = bc$. Число $a$ называют *кратным* числа $b$, число $b$ — *делителем* числа $a$, число $c$ — *частным* от деления $a$ на $b$.

Пример 1.6. $38 = 19 \cdot 2$ (38 делится на 19, 19 делит 38), $-24 = (-6) \cdot 4$ (–24 делится на –6, –6 делит –24), $0 = 5 \cdot 0$ (0 делится на 5, 5 делит 0). □

Отношение делимости обладает следующими свойствами.

1. Нуль делится на любое целое число.
2. Если $a_1$ делится на $b$, $a_2$ делится на $b$, то $a_1 \pm a_2$ делится на $b$.

2′. Если $a_1 \pm a_2$ делится на $b$ и $a_1$ делится на $b$, то $a_2$ делится на $b$.

3. Если $a$ делится на $b$ и $x$ — произвольное целое число, то $xa$ делится на $b$.
4. Любое целое число делится на 1.
5. Если $a$ делится на $b$ и $b$ делится на $c$, то $a$ делится на $c$.
6. Если 1 делится на $a$, то $a = \pm 1$.

Упражнение. Доказать свойства делимости.

Определение 1.5. Пусть числа $a$ и $b$ целые и $b \neq 0$. *Разделить $a$ на $b$ с остатком* — значит представить $a$ в виде $a = qb + r$, где $q, r \in \mathbb{Z}$ и $0 \leq r < |b|$. Число $q$ называется *неполным частным*, число $r$ — остатком от деления $a$ на $b$.

Пример 1.7. Для $b = 15$ имеем

$$45 = 3 \cdot 15 + 0,\ 0 \leq 0 < 15;$$

$$123 = 8 \cdot 15 + 3,\ 0 \leq 3 < 15;$$

$$-105 = (-7) \cdot 15 + 0,\ 0 \leq 0 < 15;$$

$$-169 = (-12) \cdot 15 + 11,\ 0 \leq 11 < 15. \qquad \square$$

Пример 1.8. Для $b = -11$ имеем

$$44 = (-4) \cdot (-11) + 0,\ 0 \leq 0 < 11;$$

$$119 = (-10) \cdot (-11) + 9,\ 0 \leq 9 < 11;$$

$$-253 = 23 \cdot (-11) + 0,\ 0 \leq 0 < 11;$$

$$-228 = 21 \cdot (-11) + 3,\ 0 \leq 3 < 11. \qquad \square$$

Теорема 1.1 (о делении с остатком). Для любых $a, b \in \mathbb{Z}$, $b \neq 0$, существует единственная пара таких чисел $q, r \in \mathbb{Z}$, что $a = qb + r$; $0 \leq r < |b|$.

*Доказательство*. Сначала докажем теорему для случая $a \geq 0$, $b > 0$. Рассмотрим множество

$$N = \{n \in \mathbb{N} \cup \{0\} \mid nb \le a\}.$$

Множество $N$ непусто, поскольку $0 \in N$. Кроме того, для любого $n \in N$ выполняется неравенство $n \le nb$, а значит, $n \le a$. Таким образом, все элементы множества $N$ ограничены сверху числом $a$, и в множестве $N$ существует наибольший элемент $q$. Но тогда $qb \le a < (q + 1)b$. Обозначим $r = a - qb$, тогда получаем требуемое неравенство для $r$:

$$0 \le r = a - qb < (q + 1)b - qb = b.$$

Теперь найдем требуемую пару чисел $q$ и $r$ для $a < 0$, $b > 0$. Согласно предыдущему случаю, для $-a > 0$ и $b$ существуют целые числа $q'$, $r'$ такие, что $-a = q'b + r'$. При $r' = 0$ полагаем $q = -q'$, $r = 0$. При $r' > 0$ полагаем $q = -(q' + 1)$, $r = b - r'$.

При $b < 0$ нужно разделить с остатком $a$ на $|b|$ согласно одному из рассмотренных случаев: $a = q'|b| + r$, а затем положить $q = -q'$.

Единственность докажем от противного. Пусть существуют две такие пары целых чисел $q_1$, $r_1$, $q_2$, $r_2$, что

$$a = q_1 b + r_1 = q_2 b + r_2,$$

где $0 \le r_1, r_2 < |b|$. Тогда

$$(q_1 - q_2)b = -(r_1 - r_2),$$

откуда следует

$$|q_1 - q_2| \cdot |b| = |r_1 - r_2| < |b|,$$

$$0 \le |q_1 - q_2| < 1,$$

а так как числа $q_1$ и $q_2$ целые, то

$$|q_1 - q_2| = 0$$

и

$$q_1 = q_2, r_1 = r_2. \qquad \square$$

## 1.2. Наибольший общий делитель и наименьшее общее кратное

Определение 1.6. Целое число $d \neq 0$ называется *наибольшим общим делителем* целых чисел $a_1, a_2, \ldots, a_k$ (обозначается $d = \text{НОД}(a_1, a_2, \ldots, a_k)$), если выполняются следующие условия:

1) каждое из чисел $a_1, a_2, \ldots, a_k$ делится на $d$;
2) если $d_1 \neq 0$ — другой общий делитель чисел $a_1, a_2, \ldots, a_k$, то $d$ делится на $d_1$.

Пример 1.9. НОД(12345, 24690) = 12345; НОД(12345, 54321) = = 3; НОД(12345, 12541) = 1. □

Ненулевые целые числа $a$ и $b$ называются *ассоциированными* (обозначается $a \sim b$), если $a$ делится на $b$ и $b$ делится на $a$.

Теорема 1.2 (об ассоциированных числах). Числа $a$ и $b$ ассоциированы тогда и только тогда, когда $a = \pm b$.

*Доказательство.* Пусть $a$ делится на $b$, тогда существует такое целое число $c$, что $a = b \cdot c$. Поскольку $|c| \geq 1$, получаем $|a| = |b| \cdot |c| \geq |b| \cdot 1 = |b|$, то есть $|a| \geq |b|$.

В то же время $b$ делится на $a$. Проводя аналогичные выкладки, получаем $|b| \geq |a|$. Таким образом, $|a| = |b|$, то есть $a = \pm b$. □

Теорема 1.3 (о единственности наибольшего общего делителя). Пусть числа $a_1, a_2, \ldots, a_k$ целые и $d_1$ — их наибольший общий делитель. Целое число $d_2$ является наибольшим общим делителем чисел $a_1, a_2, \ldots, a_k$ тогда и только тогда, когда $d_2 \sim d_1$.

*Доказательство.* Число $d_1$ — наибольший общий делитель чисел $a_1, a_2, \ldots, a_k$, а $d_2$ — общий делитель этих чисел. Значит, по определению наибольшего общего делителя, $d_1$ делится на $d_2$. Точно так же, если рассматривать $d_2$ как наибольший общий делитель чисел $a_1, a_2, \ldots, a_k$, а $d_1$

— как общий делитель этих чисел, то $d_2$ делится на $d_1$. Таким образом, $d_1 \sim d_2$. Необходимость доказана.

Теперь докажем достаточность. Пусть $d_2 \sim d_1$. Тогда, по определению наибольшего общего делителя, каждое из чисел $a_1, a_2, \ldots, a_k$ делится на $d_1$. Кроме того, числа $d_1$ и $d_2$ ассоциированы, поэтому $d_1$ делится на $d_2$. Значит, каждое из чисел $a_1, a_2, \ldots, a_k$ делится на $d_2$. Таким образом, $d_2$ — общий делитель чисел $a_1, a_2, \ldots, a_k$. Покажем теперь, что он наибольший.

Пусть $\delta$ — некоторый общий делитель чисел $a_1, a_2, \ldots, a_k$. По условию $d_1 = \text{НОД}(a_1, a_2, \ldots, a_k)$, тогда $d_1$ делится на $\delta$. А раз $d_2 \sim d_1$, то $d_2$ делится на $d_1$, значит, $d_2$ делится на $\delta$ и $d_2 = \text{НОД}(a_1, a_2, \ldots, a_k)$. □

Учитывая теоремы 1.2, 1.3, далее для определенности наибольший общий делитель целых чисел будем считать положительным числом.

Теорема 1.4 (о существовании и линейном представлении наибольшего общего делителя). Для любых целых чисел $a_1, a_2, \ldots, a_k$ существует наибольший общий делитель $d$, и его можно представить в виде линейной комбинации этих чисел: $d = c_1a_1 + c_2a_2 + \ldots + c_ka_k$, где $c_i \in \mathbb{Z}$.

*Доказательство* [1]. Пусть $A = \{c_1a_1 + c_2a_2 + \ldots + c_ka_k \mid c_i \in \mathbb{Z}\}$ — множество всевозможных целочисленных линейных комбинаций чисел $a_1, a_2, \ldots, a_k$. Будем считать, что не все числа $a_1, a_2, \ldots, a_k$ нулевые, тогда в множестве $A$ существует наименьший положительный элемент. Обозначим его $d$. Покажем, что множество $A$ совпадает с множеством всех целых чисел, кратных $d$. Поскольку число $d$ может быть представлено в виде линейной комбинации чисел $a_1, a_2, \ldots, a_k$, то и любое число вида $x_id$, где $x_i \in \mathbb{Z}$, может быть представлено в виде линейной комбинации этих чисел.

Обратно, любая линейная комбинация чисел $a_1, a_2, \ldots, a_k$ делится на $d$. Действительно, применим к числу $d$ и произвольному элементу $y \in A$ теорему о делении с остатком: существуют такие целые числа $q$ и $r$, что $y = qd + r$, причем $0 \le r < d$. Число $r = y - qd$ является элементом множества $A$, поскольку $y \in A$ и $d \in A$. Но $d$ — наименьший неотрицательный элемент множества $A$, значит, $r = 0$ и $y = qd$. Таким образом, $A = \{x_i d \mid x_i \in \mathbb{Z}\}$.

Осталось доказать, что $d$ — это наибольший общий делитель чисел $a_1, a_2, \ldots, a_k$. Каждое из этих чисел имеет вид $x_i d$, где $x_i \in \mathbb{Z}$ (достаточно рассмотреть линейную комбинацию вида $0 \cdot a_1 + 0 \cdot a_2 + \ldots + 0 \cdot a_{i-1} + 1 \cdot a_i + 0 \cdot a_{i+1} + \ldots + 0 \cdot a_k$). Таким образом, $d$ — общий делитель чисел $a_1, a_2, \ldots, a_k$.

Пусть $c$ — любой другой делитель этих чисел. Тогда по свойству 2 делимости $c$ делит каждую линейную комбинацию вида $c_1 a_1 + c_2 a_2 + \ldots + c_k a_k$, в том числе и ту, которая равна $d$. □

Пример 1.10. Наибольший общий делитель чисел 91, 105, 154 равен 7. В качестве линейного представления можно взять, например,

$$7 = 7 \cdot 91 + (-6) \cdot 105 + 0 \cdot 154$$

или

$$7 = 4 \cdot 91 + 1 \cdot 105 - 3 \cdot 154.$$ □

Определение 1.7. Целые числа $a_1, a_2, \ldots, a_k$ называются *взаимно простыми в совокупности*, если НОД$(a_1, a_2, \ldots, a_k) = 1$. Целые числа $a$ и $b$ называются *взаимно простыми*, если НОД$(a, b) = 1$.

Определение 1.8. Целые числа $a_1, a_2, \ldots, a_k$ называются *попарно взаимно простыми*, если НОД$(a_i, a_j) = 1$ для всех $1 \le i \ne j \le k$.

Пример 1.11. Числа 3, 6, 8 взаимно просты в совокупности, так как НОД$(3, 6, 8) = 1$. Числа 3, 5, 8 попарно взаимно просты. □

Взаимно простые числа обладают следующими свойствами.

1. Для того чтобы целые числа $a_1, a_2, \ldots, a_k$ были взаимно простыми в совокупности, необходимо и достаточно, чтобы существовали такие целые числа $c_1, c_2, \ldots, c_k$, что $c_1a_1 + c_2a_2 + \ldots + c_ka_k = 1$.

*Доказательство*. Необходимость следует из теоремы о существовании и линейном представлении наибольшего общего делителя. Докажем достаточность. Пусть целые числа $c_1, c_2, \ldots, c_k$ таковы, что $c_1a_1 + c_2a_2 + \ldots + c_ka_k = 1$ и пусть $d = \text{НОД}(a_1, a_2, \ldots, a_k)$. Тогда, по определению наибольшего общего делителя, каждое из чисел $a_1, a_2, \ldots, a_k$ делится на $d$. Значит, по свойству 2 делимости, и сумма $c_1a_1 + c_2a_2 + \ldots + c_ka_k$ делится на $d$, то есть 1 делится на $d$, следовательно, по свойству 6 делимости, $d = 1$. Таким образом, $1 = \text{НОД}(a_1, a_2, \ldots, a_k)$ и числа $a_i$ взаимно просты в совокупности. □

1′. Для того чтобы целые числа $a$, $b$ были взаимно простыми, необходимо и достаточно, чтобы существовали такие целые числа $m$, $n$, что $ma + nb = 1$.

2. Пусть произведение $ab$ делится на $c$ и $\text{НОД}(a, c) = 1$. Тогда $b$ делится на $c$.

*Доказательство*. Числа $a$ и $c$ взаимно просты, тогда, по свойству 1′, существуют такие целые числа $m$, $n$, что $ma + nc = 1$. Домножим обе части последнего равенства на $b$:

$$mab + ncb = b.$$

Первое слагаемое в левой части равенства делится на $c$ по условию. Второе слагаемое, очевидно, делится на $c$. Значит, и $b$ делится на $c$.

□

3. Если $\text{НОД}(a, b) = 1$, $\text{НОД}(a, c) = 1$, то $\text{НОД}(a, bc) = 1$.

*Доказательство*. Числа $a$ и $b$ взаимно просты, поэтому по свойству 1′ число 1 можно представить в виде $1 = ma + nb$, где числа $m$ и $n$ целые. Умножим обе части этого равенства на $c$, получим

$$c = mac + nbc.$$

Пусть $d$ — наибольший общий делитель чисел $a$ и $bc$. Тогда оба слагаемых в правой части равенства делятся на $d$, а значит и число $c$ делится на $d$. Но 1 — наибольший общий делитель чисел $a$ и $c$, то есть 1 делится на $d$ и $d = 1$. □

4. Если НОД$(a, b_1) = 1$, НОД$(a, b_2) = 1$, …, НОД$(a, b_k) = 1$, то НОД$(a, b_1b_2\ldots b_k) = 1$.

5. Пусть целые числа $a_1, a_2, \ldots, a_l, b_1, b_2, \ldots, b_k$ таковы, что НОД$(a_i, b_j) = 1$ для всех $1 \le i \le l$, $1 \le j \le k$. Тогда НОД$(a_1a_2\ldots a_l, b_1b_2\ldots b_k) = 1$.

6. Пусть целое число $a$ делится на $b_1$ и на $b_2$, НОД$(b_1, b_2) = 1$. Тогда $a$ делится на произведение $b_1b_2$.

*Доказательство*. Число $a$ делится на $b_1$, поэтому существует такое целое число $c$, что $a = cb_1$.

Так как $a$ делится на $b_2$, то произведение $cb_1$ делится на $b_2$. Но поскольку НОД$(b_1, b_2) = 1$, значит, по свойству 2 взаимно простых чисел, $c$ делится на $b_2$, то есть существует такое целое число $d$, что $c = db_2$. Отсюда $a = cb_1 = db_1b_2$, то есть $a$ делится на $b_1b_2$. □

7. Если $a$ делится на каждое из попарно взаимно простых чисел $b_1, b_2, \ldots, b_k$, то $a$ делится на произведение $b_1b_2\ldots b_k$.

Упражнение. Методом математической индукции доказать свойства 4, 5, 7.

Определение 1.9. Целое число $M$ называется *наименьшим общим кратным* целых чисел $a_1, a_2, \ldots, a_k$, $a_i \neq 0$ для $i = 1, 2, \ldots, k$, (обо-

значается $M = \text{НОК}(a_1, a_2, \ldots, a_k)$), если выполняются следующие условия:

1) $M$ делится на каждое из чисел $a_1, a_2, \ldots, a_k$;
2) если $M_1$ — другое общее кратное чисел $a_1, a_2, \ldots, a_k$, то $M_1$ делится на $M$.

Пример 1.12. НОК(12345, 24690) = 24690; НОК(12345, 54321) = = 223530915; НОК(12345, 12541) = 154818645. □

Наибольший общий делитель и наименьшее общее кратное двух положительных целых чисел связаны соотношением:

$$\text{НОД}(a, b) \cdot \text{НОК}(a, b) = ab.$$

Пример 1.13. НОД(12345, 24690) · НОК(12345, 24690) = 12345 × × 24690 = 304798050; НОД(12345, 54321) · НОК(12345, 54321) = 3 × × 223530915 = 670592745 = 12345 · 54321; НОД(12345, 12541) · НОК(12345, 12541) = 1 · 154818645 = 12345 · 12541. □

## 1.3. Вычисление наибольшего общего делителя

### 1.3.1. Алгоритм Евклида

Для вычисления наибольшего общего делителя двух целых чисел применяется способ повторного деления с остатком, называемый *алгоритмом Евклида*.

Алгоритм 1.1. Алгоритм Евклида.

*Вход*. Целые числа $a$, $b$; $0 < b \le a$.

*Выход*. $d = \text{НОД}(a, b)$.

1. Положить $r_0 \leftarrow a$, $r_1 \leftarrow b$, $i \leftarrow 1$.
2. Найти остаток $r_{i+1}$ от деления $r_{i-1}$ на $r_i$.

3. Если $r_{i+1} = 0$, то положить $d \leftarrow r_i$. В противном случае положить $i \leftarrow i + 1$ и вернуться на шаг 2.

4. Результат: $d$. □

Сложность алгоритма Евклида равна $O(\log^2 a)$.

Для доказательства корректности алгоритма Евклида нам понадобятся две леммы.

Лемма 1.5. Если числа $a$ и $b$ целые и $a$ делится на $b$, то $b = \text{НОД}(a, b)$.

*Доказательство.* Пусть $d = \text{НОД}(a, b)$, тогда по теореме 1.4 существуют такие целые числа $m$, $n$, что $d = ma + nb$. Поскольку $a$ делится на $b$, то сумма в правой части равенства делится на $b$, а значит и $d$ делится на $b$. В то же время $b$ делится на $d$ как на наибольший общий делитель. Таким образом, числа $d$ и $b$ ассоциированы и равны с точностью до знака. □

Лемма 1.6. Для любых целых чисел $a$, $b$, $c$ выполняется равенство $\text{НОД}(a + cb, b) = \text{НОД}(a, b)$.

*Доказательство.* Пусть $d = \text{НОД}(a, b)$. Тогда $a$ делится на $d$, $b$ делится на $d$, значит, по свойству 2 делимости, и сумма $a + cb$ делится на $d$, то есть $d$ — общий делитель чисел $a + cb$ и $b$.

Пусть $d_1$ — произвольный общий делитель чисел $a + cb$ и $b$. Тогда число $a = (a + cb) - cb$ делится на $d_1$, то есть $d_1$ — общий делитель чисел $a$ и $b$. А так как делитель $d$ наибольший, то $d$ делится на $d_1$, и $d$ — наибольший общий делитель чисел $a + cb$ и $b$. □

Пример 1.14. Используя алгоритм Евклида, найдем такие целые числа $n$, для которых дробь $\dfrac{3n+4}{8n+5}$ несократима [4]. Дробь несократима, если ее числитель и знаменатель взаимно просты. Построим последовательность наибольших общих делителей, используя лемму 1.6:

$$\text{НОД}(3n+4,\ 8n+5) = \text{НОД}(3n+4,\ 2\cdot(3n+4)+2n-3) =$$

$$= \text{НОД}(3n+4,\ 2n-3) = \text{НОД}(2n-3+n+7,\ 2n-3) =$$

$$= \text{НОД}(n+7,\ 2n-3) = \text{НОД}(n+7,\ 2\cdot(n+7)-17) = \text{НОД}(n+7,\ -17) =$$

$$= \text{НОД}(n+7,\ 17).$$

Таким образом, чтобы дробь была несократима, нужно, чтобы число $n+7$ не делилось на 17, то есть чтобы $n$ имело вид $17q+r$, где $0 \le r \le 16$, $r \ne 10$. Действительно, при $r = 10$ получаем

$$\frac{3(17q+10)+4}{8(17q+10)+5} = \frac{3\cdot 17q+34}{8\cdot 17q+85} = \frac{17(3q+2)}{17(8q+5)} = \frac{3q+2}{8q+5}. \qquad \square$$

Теорема 1.7. Для любых $a$, $b > 0$ алгоритм Евклида останавливается и выдаваемое им число $d$ является наибольшим общим делителем чисел $a$ и $b$.

*Доказательство.* По теореме о делении с остатком для любого $i \ge 1$ имеем $r_{i-1} = q_i r_i + r_{i+1}$, где $0 \le r_{i+1} < r_i$. Получаем монотонно убывающую последовательность неотрицательных целых чисел $r_1 > r_2 > r_3 > \ldots \ge 0$, ограниченную снизу. Такая последовательность не может быть бесконечной, следовательно, алгоритм Евклида останавливается.

Докажем теперь, что число $d$ — наибольший общий делитель для чисел $r_1, r_2, \ldots, r_k$, где $r_{k-1}$ делится на $r_k$. С учетом леммы 1.6 можем записать:

$$\text{НОД}(a, b) = \text{НОД}(r_0, r_1) = \text{НОД}(q_1 r_1 + r_2, r_1) = \text{НОД}(r_1, r_2) =$$

$$= \text{НОД}(r_2, r_3) = \ldots = \text{НОД}(r_{k-1}, r_k).$$

А по лемме 1.5 получаем $\text{НОД}(r_{k-1}, r_k) = r_k = d$. $\square$

Посмотрим, для каких целых чисел алгоритм Евклида выполняет больше всего итераций.

Напомним, что *последовательностью Фибоначчи* $\{F_k\}$, где $k \in \mathbb{N}$, называется последовательность, элементы которой связаны соотношением: $F_{k+1} = F_k + F_{k-1}$ для $k \geq 2$, при этом $F_1 = F_2 = 1$:

$$1, 1, 2, 3, 5, 8, 13, \ldots$$

Найдем наибольший общий делитель для чисел Фибоначчи $F_{k+2}$ и $F_{k+1}$: НОД$(F_{k+2}, F_{k+1})$ = по определению чисел Фибоначчи = НОД$(F_{k+1} + F_k, F_{k+1})$ = по лемме 1.6 = НОД$(F_{k+1}, F_k) = \ldots =$ НОД$(F_2, F_1) =$ = НОД$(1, 1) = 1$. Таким образом, для вычисления наибольшего общего делителя требуется ровно $k$ итераций. □

Пример 1.15. Пусть $a = F_6 = 8$, $b = F_5 = 5$. Тогда за четыре шага: $8 = 1 \cdot 5 + 3$, $5 = 1 \cdot 3 + 2$, $3 = 1 \cdot 2 + 1$, $2 = 2 \cdot 1 + 0$ — находим НОД$(a, b) = 1$. □

Лемма 1.8. При $k \geq 2$ справедливо неравенство $F_k \geq \phi^{k-2}$, где $\phi = \dfrac{1+\sqrt{5}}{2}$ — корень квадратного уравнения $x^2 - x - 1 = 0$ («золотое сечение»).

*Доказательство* [5] проведем методом математической индукции. При $k = 2$ имеем $F_2 = 1 \geq \phi^0 = 1$.

Индукционный переход:

$$F_{k+1} = F_k + F_{k-1} \geq \phi^{k-2} + \phi^{k-3} = \phi^{k-3}(\phi + 1) = \phi^{k-3}\phi^2 = \phi^{k-1}. \quad \square$$

Теорема 1.9 (Ламэ). Для целых чисел $a$, $b$, $N$ таких, что $0 < b < a \leq N$, число итераций в алгоритме Евклида для $a$ и $b$ не превосходит $1 + \left[\log_\phi N\right]$.

*Доказательство* [5]. Пусть НОД$(a, b)$ = НОД$(r_0, r_1)$ = НОД$(r_1, r_2)$ = $= \ldots =$ НОД$(r_{k-1}, r_k) = r_k$. Сначала индукцией по $i$ докажем, что $F_i \leq r_{k-(i-1)}$ для $i = 1, 2, \ldots, k + 1$. При $i = 1$ имеем $F_1 = 1 \leq$ НОД$(a, b) = r_k$; при $i = 2$ —

$F_2 = 1 \le$ НОД$(a, b) = r_k < r_{k-1}$. Индукционный переход — делим с остатком $r_{k-i}$ на $r_{k+1-i}$:

$$r_{k-i} = q_{k-(i-1)} r_{k-(i-1)} + r_{k-(i-2)} \ge r_{k-(i-1)} + r_{k-(i-2)} \ge F_i + F_{i-1} = F_{i-1}.$$

Отсюда

$$N \ge a = r_0 \ge F_{k+1} \ge \phi^{k-1}$$

(в последнем неравенстве мы воспользовались леммой 1.8). Логарифмируя неравенство $\phi^{k-1} \le N$, получаем требуемую оценку числа итераций в алгоритме Евклида: $k \le 1 + \left[\log_\phi N\right]$. □

### 1.3.2. Бинарный алгоритм Евклида

Этот вариант алгоритма Евклида оказывается более быстрым при реализации на компьютере, поскольку использует двоичное представление чисел $a$ и $b$. *Бинарный алгоритм Евклида* основан на следующих свойствах наибольшего общего делителя (считаем, что $0 < b \le a$):

1) если оба числа $a$ и $b$ четные, то НОД$(a, b) = 2 \cdot$ НОД$\left(\frac{a}{2}, \frac{b}{2}\right)$;

2) если число $a$ нечетное, число $b$ четное, то НОД$(a, b) =$ НОД$\left(a, \frac{b}{2}\right)$;

3) если оба числа $a$ и $b$ нечетные, $a > b$, то НОД$(a, b) =$ НОД$(a - b, b)$;

4) если $a = b$, то НОД$(a, b) = a$.

Пример 1.16. Вычислим наибольший общий делитель чисел $a = 30 = (11110)_2$, $b = 20 = (10100)_2$, используя двоичную систему счисления. Оба числа четные, поэтому, согласно свойству 1, НОД$(a, b) =$ $=$ НОД$((10100)_2, (11110)_2) = 2 \cdot$ НОД$((1010)_2, (1111)_2)$. Теперь первое число четное, второе — нечетное, поэтому, согласно свойству 2, НОД$(a, b) = 2 \cdot$ НОД$((101)_2, (1111)_2) =$ по свойству 3 $= 2 \cdot$ НОД$((101)_2, (1010)_2) =$ по свойству 2 $= 2 \cdot$ НОД$((101)_2, (101)_2)$. Наконец, по свойству 4

получаем: НОД($(101)_2$, $(101)_2$) = $(101)_2$ = 5. Таким образом, НОД($a$, $b$) = $= 2 \cdot 5 = 10$. □

Алгоритм 1.2. Бинарный алгоритм Евклида [6].

*Вход*. Целые числа $a$, $b$; $0 < b \le a$.

*Выход*. $d$ = НОД($a$, $b$).

1. Положить $g \leftarrow 1$.
2. Пока оба числа $a$ и $b$ четные, выполнять $a \leftarrow \frac{a}{2}$, $b \leftarrow \frac{b}{2}$, $g \leftarrow 2g$ до получения хотя бы одного нечетного значения $a$ или $b$.
3. Положить $u \leftarrow a$, $v \leftarrow b$.
4. Пока $u \ne 0$, выполнять следующие действия.

   4.1. Пока $u$ четное, полагать $u \leftarrow \frac{u}{2}$.

   4.2. Пока $v$ четное, полагать $v \leftarrow \frac{v}{2}$.

   4.3. При $u \ge v$ положить $u \leftarrow u - v$. В противном случае положить $v \leftarrow v - u$.
5. Положить $d \leftarrow gv$.
6. Результат: $d$. □

Сложность этого алгоритма равна $O(\log^2 a)$.

Аналогичный алгоритм можно построить для полиномов $a(x)$, $b(x)$ с целыми коэффициентами от одной переменной $x$, только вместо деления на 2 следует использовать деление на $x$, а условие $a \ge b$ заменить условием $\deg(a) \ge \deg(b)$ для степеней полиномов.

Пример 1.17. Пусть $a(x) = x^5 + 3x^4 + 3x^3 + 2x^2$, $b(x) = x^4 + 2x^3 + 2x^2 + x$. Найдем $d(x)$ = НОД($a(x)$, $b(x)$).

Применяем алгоритм 1.2 (записываем только коэффициенты):

| Номер шага | $u(x)$ | | | | | | $v(x)$ | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $x^5$ | $x^4$ | $x^3$ | $x^2$ | $x^1$ | $x^0$ | $x^5$ | $x^4$ | $x^3$ | $x^2$ | $x^1$ | $x^0$ | |
| 1 | 1 | 3 | 3 | 2 | 0 | 0 | | 1 | 2 | 2 | 1 | 0 | $g(x) = 1$ |
| 2 | | 1 | 3 | 3 | 2 | 0 | | | 1 | 2 | 2 | 1 | $g(x) = x$ |
| 4.1 | | | 1 | 3 | 3 | 2 | | | | | | | |
| 4.3 | $u(x) = -(u(x) - 2 \cdot v(x))$ | | | | | | | | | | | | |
| | | | 1 | 1 | 1 | 0 | | | | | | | |
| 4.1 | | | | 1 | 1 | 1 | | | | | | | |
| 4.3 | $v(x) = v(x) - u(x)$ | | | | | | | | | | | | |
| | | | | | | | | 1 | 1 | 1 | 0 | | |
| 4.2 | | | | | | | | | 1 | 1 | 1 | | |
| 4.3 | $u(x) = u(x) - v(x)$ | | | | | | | | | | | | |
| | | | | | | 0 | | | | | | | |

Таким образом, $d(x) = \text{НОД}(a(x), b(x)) = x(x^2 + x + 1)$. □

### 1.3.3. Расширенный алгоритм Евклида

Пример 1.18. Найдем наибольший общий делитель чисел $a = 861$, $b = 798$:

$$861 = 1 \cdot 798 + 63,$$

$$798 = 12 \cdot 63 + 42,$$

$$63 = 1 \cdot 42 + 21,$$

$$42 = 2 \cdot 21 + 0.$$

Таким образом, $21 = \text{НОД}(861, 798)$. Теперь найдем представление числа 21 в виде целочисленной линейной комбинации чисел 861 и 798. Выражаем остатки:

$$21 = 63 - 1 \cdot 42,$$

$$42 = 798 - 12 \cdot 63,$$

$$63 = 861 - 1 \cdot 798$$

и подставляем последовательно эти выражения друг в друга:

$$21 = 63 - 1 \cdot 42 = 63 - 1 \cdot (798 - 12 \cdot 63) = 13 \cdot 63 - 1 \cdot 798 =$$

$$= 13 \cdot (861 - 1 \cdot 798) - 1 \cdot 798 = 13 \cdot 861 - 14 \cdot 798.$$

Таким образом, $21 = 13 \cdot 861 + (-14) \cdot 798$. □

Расширенный алгоритм Евклида находит наибольший общий делитель $d$ чисел $a$ и $b$ и его линейное представление, то есть целые числа $x$ и $y$, для которых $ax + by = d$, и не требует «возврата», как в рассмотренном примере.

Алгоритм 1.3. Расширенный алгоритм Евклида.

*Вход*. Целые числа $a$, $b$; $0 < b \le a$.

*Выход*. $d =$ НОД$(a, b)$; такие целые числа $x$, $y$, что $ax + by = d$.

1. Положить $r_0 \leftarrow a$, $r_1 \leftarrow b$, $x_0 \leftarrow 1$, $x_1 \leftarrow 0$, $y_0 \leftarrow 0$, $y_1 \leftarrow 1$, $i \leftarrow 1$.
2. Разделить с остатком $r_{i-1}$ на $r_i$: $r_{i-1} = q_i r_i + r_{i+1}$.
3. Если $r_{i+1} = 0$, то положить $d \leftarrow r_i$, $x \leftarrow x_i$, $y \leftarrow y_i$. В противном случае положить $x_{i+1} \leftarrow x_{i-1} - q_i x_i$, $y_{i+1} \leftarrow y_{i-1} - q_i y_i$, $i \leftarrow i + 1$ и вернуться на шаг 2.
4. Результат: $d$, $x$, $y$. □

Сложность этого алгоритма равна $O(\log^2 a)$.

Корректность определения чисел $x$ и $y$, вычисляемых алгоритмом 1.2, показывает следующая лемма.

Лемма 1.10. На каждой итерации алгоритма 1.3 выполняется равенство $ax_i + by_i = r_i$ при $i \ge 0$.

*Доказательство* [2]. Воспользуемся методом математической индукции.

Для $i = 0$ и $i = 1$ требуемое равенство имеет место в силу шага 1 алгоритма 1.3. Допустим, что оно справедливо для $i - 1$ и для $i$. Тогда на шаге 3 получаем $x_{i+1} = x_{i-1} - q_i x_i$ и $y_{i+1} = y_{i-1} - q_i y_i$. Следовательно,

$$ax_{i+1} + by_{i+1} = a(x_{i-1} - q_i x_i) + b(y_{i-1} - q_i y_i) =$$

$$= ax_{i-1} + by_{i-1} - q_i(ax_i + by_i) = r_{i-1} - q_i r_i = r_{i+1}. \qquad \square$$

Соотношение леммы 1.10 используется в некоторых алгоритмах разложения чисел на множители и дискретного логарифмирования.

Пример 1.19. Найдем наибольший общий делитель чисел $a = 1092$, $b = 988$ и его линейное представление алгоритмом 1.3. Промежуточные результаты сведем в таблицу:

| $i$ | $r_i$ | $x_i$ | $y_i$ | $q_i$ |
|---|---|---|---|---|
| 1 | 1092 | 1 | 0 | |
| 2 | 988 | 0 | 1 | 1 |
| 3 | 104 | 1 | –1 | 9 |
| 4 | **52** | **–9** | **10** | 2 |

Таким образом, НОД(1092, 988) = 52 = $1092 \cdot (-9) + 988 \cdot 10$. $\square$

Расширенный алгоритм Евклида можно реализовать и в двоичном виде.

Алгоритм 1.4. Расширенный бинарный алгоритм Евклида [6].

*Вход*. Целые числа $a$, $b$; $0 < b \le a$.

*Выход*. $d$ = НОД($a$, $b$); такие целые числа $x$, $y$, что $ax + by = d$.

1. Положить $g \leftarrow 1$.
2. Пока оба числа $a$ и $b$ четные, выполнять $a \leftarrow \frac{a}{2}$, $b \leftarrow \frac{b}{2}$, $g \leftarrow 2g$ до получения хотя бы одного нечетного значения $a$ или $b$.
3. Положить $u \leftarrow a$, $v \leftarrow b$, $A \leftarrow 1$, $B \leftarrow 0$, $C \leftarrow 0$, $D \leftarrow 1$.

4. Пока $u \neq 0$, выполнять следующие действия.

4.1. Пока $u$ четное:

4.1.1. Положить $u \leftarrow \frac{u}{2}$.

4.1.2. Если оба числа $A$ и $B$ четные, то положить $A \leftarrow \frac{A}{2}$, $B \leftarrow \frac{B}{2}$. В противном случае положить $A \leftarrow \frac{A+b}{2}, B \leftarrow \frac{B-a}{2}$.

4.2. Пока $v$ четное:

4.2.1. Положить $v \leftarrow \frac{v}{2}$.

4.2.2. Если оба числа $C$ и $D$ четные, то положить $C \leftarrow \frac{C}{2}$, $D \leftarrow \frac{D}{2}$. В противном случае положить $C \leftarrow \frac{C+b}{2}, D \leftarrow \frac{D-a}{2}$.

4.3. При $u \geq v$ положить $u \leftarrow u - v$, $A \leftarrow A - C$, $B \leftarrow B - D$. В противном случае положить $v \leftarrow v - u$, $C \leftarrow C - A$, $D \leftarrow D - B$.

5. Положить $d \leftarrow gv, x \leftarrow C, y \leftarrow D$.

6. Результат: $d, x, y$. □

Сложность этого алгоритма равна $O(\log^2 a)$. Здесь по аналогии с леммой 1.10 на каждом шаге выполняются соотношения $u = aA + bB$ и $v = aC + bD$. Если все три числа $u$, $A$ и $B$ четные, то обе части равенства $u = aA + bB$ можно разделить на 2 (первое условие шага 4.1.2). Если же при четном $u$ хотя бы одно из чисел $A$, $B$ нечетное, то соотношение $u = aA + bB$ преобразуется в $u = aA + bB + ab - ab = a(A + b) + b(B - a)$ (второе условие шага 4.1.2). То же справедливо и для чисел $v$, $C$, $D$.

Пример 1.20. Найдем наибольший общий делитель чисел $a = 1092$, $b = 988$ и его линейное представление алгоритмом 1.4.

На шаге 1 полагаем $g = 1$. Шаг 2 выполняем два раза, получаем $a = 273$, $b = 247$, $g = 4$. Последовательность дальнейших шагов алгоритма 1.4 сведем в таблицу:

| Шаг | $u$ | $v$ | $A$ | $B$ | $C$ | $D$ |
|---|---|---|---|---|---|---|
| 3 | 273 | 247 | 1 | 0 | 0 | 1 |
| 4.3 | 26 | | 1 | −1 | | |
| 4.1 | 13 | | 124 | −137 | | |
| 4.3 | | 234 | | | −124 | 138 |
| 4.2 | | 117 | | | −62 | 69 |
| 4.3 | | 104 | | | −186 | 206 |
| 4.2 | | 52 | | | −93 | 103 |
| 4.2 | | 26 | | | 77 | −85 |
| 4.2 | | 13 | | | 162 | −179 |
| 4.3 | 0 | | −38 | 42 | | |

На шаге 5 полагаем $d = 4 \cdot 13 = 52$, $x = 162$, $y = -179$.

Проверка: $1092 \cdot 162 + 988 \cdot (-179) = 176904 - 176852 = 52$. □

Как видно из примеров, линейное представление $ax + by = \text{НОД}(a, b)$ не единственно. Выведем общий вид коэффициентов $x$ и $y$. Пусть есть другое представление $ax' + by' = \text{НОД}(a, b)$. Тогда $a(x' - x) + b(y' - y) = 0$. Найдем такие целые числа $s$, $t$, для которых $as = bt$. Запишем $a = a_1 \cdot \text{НОД}(a, b)$, $b = b_1 \cdot \text{НОД}(a, b)$, где $\text{НОД}(a_1, b_1) = 1$. Отсюда $a_1 s = b_1 t$, и это равенство выполняется для $s = b_1 k$, $t = a_1 k$, где $k$ — произвольное целое число. Получаем

$$x' = x + \frac{bk}{\text{НОД}(a,b)}, \quad y' = y - \frac{ak}{\text{НОД}(a,b)},$$

для произвольного целого числа $k$.

В примере 1.19 $a = 1092$, $b = 988$, НОД$(a, b) = 52$, $x = -9$, $y = 10$. Тогда значения $x'$, $y'$ определяются равенствами

$$x' = -9 + 19k, y' = 10 - 21k.$$

Значения $x' = 162$, $y' = -179$ из примера 1.20 получаем при $k = 9$.

## 1.4. Простые числа

Определение 1.10. Пусть $a$ — целое число. Числа $1, -1, a, -a$ называются *тривиальными делителями* числа $a$.

Определение 1.11. Целое число $p \in \mathbb{Z} \setminus \{0\}$ называется *простым*, если оно не является делителем единицы и не имеет других делителей, кроме тривиальных. В противном случае число $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$ называется *составным*.

Пример 1.21. Числа $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 17, \pm 19, \pm 23, \pm 29, \pm 7927, \pm 7933, \pm 7937, \pm 7949, \pm 7951, \pm 7963, \pm 7993, \pm 8009, \pm 8011, \pm 8017, \pm 857577350159748432833953074357386668492904846040851678209$ являются простыми. □

Пример 1.22. Числа

$$-17647 = -7 \cdot 2521,\ 1752458619827 = 4133 \cdot 5851 \cdot 72469,$$

$$916941942360412139468515338546876825319747546525 9 =$$

$$= 857577350158321091012200932964 3 \cdot 1069223600869509313$$

являются составными. □

### 1.4.1. Свойства простых чисел

1. Если числа $p$ и $q$ простые и $p$ делится на $q$, то $p \sim q$.

*Доказательство*. Из определения простого числа и того, что $p$ делится на $q$, следует, что $q \in \{\pm 1, \pm p\}$.

Если $q = \pm 1$, то $q$ не простое; если $q = \pm p$, то $p \sim q$. □

2. Если число $p$ простое и число $a$ целое, то либо $a$ делится на $p$, либо НОД$(a, p) = 1$.

*Доказательство*. Пусть НОД$(a, p) = d > 1$. Тогда $a$ делится на $d$ и $p$ делится на $d$, но так как число $p$ простое, то либо $d = \pm 1$ (что противоречит предположению), либо $d = \pm p$. □

3. Если число $p$ простое и произведение $ab$ делится на $p$, то либо $a$ делится на $p$, либо $b$ делится на $p$.

*Доказательство*. Пусть $a$ не делится на $p$. Тогда по предыдущему свойству НОД$(a, p) = 1$. Следовательно, по свойству 2 наибольшего общего делителя, $b$ делится на $p$. □

4. Если число $p$ простое и произведение $a_1a_2\ldots a_k$ делится на $p$, то хотя бы одно из чисел $a_1, a_2, \ldots, a_k$ делится на $p$.

5. Если числа $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_l$ простые и выполняется равенство для произведений $p_1p_2\ldots p_k = q_1q_2\ldots q_l$, то $l = k$ и числа $q_1, q_2, \ldots, q_l$ можно перенумеровать так, что $p_1 \sim q_1, p_2 \sim q_2, \ldots, p_k \sim q_k$.

Упражнение. Методом математической индукции доказать свойства 4, 5.

Пример 1.23. Найдем все простые числа $p$, для которых числа $p + 2$ и $p + 5$ одновременно являются простыми.

При $p = 2$ получаем $p + 2 = 4$ — составное число, при $p = -2$ получаем $p + 2 = 0$.

Все остальные простые числа — нечетные и имеют вид $p = 2k + 1$. Тогда $p + 5 = 2k + 1 + 5 = 2(k + 3)$. Это число четное и может быть простым лишь тогда, когда оно равно 2 или $-2$. В первом случае получаем $k + 3 = 1$, $k = -2$, $p = -3$. Но тогда $p + 2 = -1$ — не простое число.

Во втором случае получаем $k+3=-1$, $k=-4$, $p=-7$. Тогда $p+2=-5$ — простое число.

Таким образом, число $p=-7$ является единственным решением нашей задачи. □

Учитывая свойство 1 простых чисел, под простыми числами обычно понимают только положительные простые числа.

Теорема 1.11 (основная теорема арифметики). Всякое число $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ можно представить в виде $n = \varepsilon p_1 p_2 \ldots p_r$, где $\varepsilon = \pm 1$ и $p_1, p_2, \ldots, p_r$ — простые числа (не обязательно различные), $r \geq 1$. Это представление единственно с точностью до порядка сомножителей.

*Доказательство.* Сначала докажем, что разложение существует. Пусть $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Доказывать будем индукцией по $|n|$. Если $|n| = 2$, то $n = \varepsilon \cdot 2$, где $\varepsilon = \pm 1$, — база индукции. Пусть для всех чисел $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$, $|a| < |n|$, уже доказано существование нужного представления. Докажем, что для $n$ такое представление тоже возможно.

Если $|n|$ — простое число, то, обозначив его $|n| = p_1$, получим $n = \pm|n| = \pm\varepsilon p_1$, где $\varepsilon = \pm 1$.

Пусть теперь число $n$ составное, $|n| > 1$, то есть существует нетривиальный делитель $a$ ($a \neq \pm 1$, $a \neq \pm n$) числа $n$. Тогда существует такое целое число $b$, что $n = ab$, где $b \neq \pm 1$, $b \neq \pm n$. Поскольку $|n| > 1$, справедливо равенство для абсолютных величин: $|n| = |ab| = |a| \cdot |b| > |a|$.

Аналогично $|n| > |b|$, поэтому к числам $a$ и $b$ применимо предположение индукции:

$$a = \varepsilon_1 p_1 p_2 \ldots p_k, \quad b = \varepsilon_2 q_1 q_2 \ldots q_l,$$

где числа $p_i$, $q_j$ простые, $\varepsilon_1, \varepsilon_2 = \pm 1$.

Произведение $ab$ дает требуемое представление. Существование представления доказано.

Теперь докажем единственность.

Пусть $n = \varepsilon_1 p_1 p_2 \ldots p_k = \varepsilon_2 q_1 q_2 \ldots q_l$, где числа $p_i$, $q_j$ простые, $\varepsilon_1 = \pm 1$, $\varepsilon_2 = \pm 1$. Тогда $\varepsilon_1 = \varepsilon_2 = 1$ при $n > 0$, $\varepsilon_1 = \varepsilon_2 = -1$ при $n < 0$.

Далее, $p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_l$, тогда по свойству 5 простых чисел $k = l$ и числа $q_1, q_2, \ldots, q_l$ можно перенумеровать так, что $p_1 = q_1$, $p_2 = q_2$, ..., $p_k = q_l$. □

Представление числа $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ в виде $n = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, где $\varepsilon = \pm 1$, $p_1, p_2, \ldots, p_s$ — различные простые числа, $\alpha_i \geq 1$ для $i = 1, 2, \ldots, s$, $s \geq 1$, называется *каноническим разложением* числа $n$.

Пример 1.24. Каноническое разложение числа 12345876 имеет вид $2^2 \cdot 3^2 \cdot 17 \cdot 20173$; каноническое разложение числа –2345679 имеет вид $(-1) \cdot 3^5 \cdot 7^2 \cdot 197$. □

### 1.4.2. Распределение простых чисел

Следующие две теоремы называются теоремами Евклида о простых числах.

Теорема 1.12. Простых чисел бесконечно много.

*Доказательство* проведем от противного. Пусть утверждение неверно и $p_1, p_2, \ldots, p_s$ — все простые числа. Составим новое число: $n = p_1 p_2 \ldots p_s + 1$ и представим его в виде $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$. Перенумеруем простые числа так, чтобы $\alpha_1 \neq 0$. Тогда число $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s} = p_1 p_2 \ldots p_s + 1$ делится на $p_1$, то есть, по свойству 2′ делимости, число 1 делится на $p_1$. Отсюда $p_1 = 1$ — не простое число. Противоречие доказывает теорему. □

Теорема 1.13. Существуют сколь угодно длинные отрезки натурального ряда, не содержащие простых чисел, то есть для любого $k \geq 1$ существует такое $n \in \mathbb{N}$, что числа $n + 1, n + 2, \ldots, n + k$ составные.

*Доказательство.* Рассмотрим число $n = (k+1)! + 1$. При $k \geq 1$ выполняется неравенство $n \geq 3$. Тогда $n + 1 = (k+1)! + 2 = 1 \cdot 2 \cdot \ldots \cdot (k+1) + 2$ делится на 2 (и не равно 2), $n + 2 = (k+1)! + 3 = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (k+1) + 3$ делится на 3 (и не равно 3) и т. д. Число $n + k = (k+1)! + (k+1) = 1 \cdot 2 \cdot \ldots \cdot (k+1) + (k+1)$ делится на $k+1$ (и не равно $k+1$). □

Пример 1.25. При $k = 3$ полагаем $n = 4! + 1 = 25$. Тогда числа $n + 1 = 26$, $n + 2 = 27$, $n + 3 = 28$ составные. □

Пример 1.26. При $k = 10$ имеем $n = 11! + 1 = 39916801$, тогда

$n + 1 = 39916802 = 2 \cdot 19958401$, $n + 2 = 39916803 = 3 \cdot 13305601$,

$n + 3 = 39916804 = 4 \cdot 9979201$, $n + 4 = 39916805 = 5 \cdot 7983361$,

$n + 5 = 39916806 = 6 \cdot 6652801$, $n + 6 = 39916807 = 7 \cdot 5702401$,

$n + 7 = 39916808 = 8 \cdot 4989601$, $n + 8 = 39916809 = 9 \cdot 4435201$,

$n + 9 = 39916810 = 10 \cdot 3991681$, $n + 10 = 39916811 = 11 \cdot 3628801$.

□

Если выписать подряд все простые числа, то можно заметить, что относительная плотность их убывает: от 1 до 10 — четыре простых числа, то есть 40 % целых чисел являются простыми, от 1 до 100 — 25 простых чисел (25 %), от 1 до 100 — 168 простых чисел (17 %), от 1 до $10^5$ — 9 592 простых числа (менее 10 %).

Обозначим $\pi(x)$ число всех простых чисел, не превосходящих $x$. Из первой теоремы Евклида о простых числах следует, что $\pi(x) \to \infty$ при $x \to \infty$. Еще в XVIII веке Л. Эйлер установил, что простых чисел «много» в том смысле, что $\pi(x) > \ln x - 1$, и в то же время большинство натуральных чисел — составные, поскольку $\dfrac{\pi(x)}{x} \underset{x \to \infty}{\to} 0$.

В 1851–52 году П.Л. Чебышев показал, что функция $\pi(x)$ растет так же, как функция $\frac{x}{\ln x}$, а именно, что существуют такие постоянные $a > \frac{1}{2}\ln 2$ и $A < 2\ln 2$, что для любого $x \geq 2$ выполняется неравенство

$$a\frac{x}{\ln x} < \pi(x) < A\frac{x}{\ln x}.$$

В 1896 году Ж. Адамаром и Ш. Ла Валле Пуссеном независимо был получен *асимптотический закон распределения простых чисел*:

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\ln x} = 1.$$

Пример 1.27. Для $x = 10^5$ имеем $\frac{x}{\ln x} \approx 8686$, $\pi(x) = 9592$; для $x = 10^{10}$ имеем $\frac{x}{\ln x} \approx 434294481$, $\pi(x) = 455052511$. Для любых $x \geq 17$ справедлива нижняя оценка $\pi(x) > \frac{x}{\ln x}$; для всех $x > 1$ справедлива верхняя оценка $\pi(x) < 1{,}25506\frac{x}{\ln x}$ (см., например, [6]). □

## Упражнения к главе 1

1. Доказать, что если целое число $n$ не делится на 7, то на 7 делится либо $n^3 - 1$, либо $n^3 + 1$.

2. Натуральное число $n > 1$ не делится на 2 и на 3. Доказать, что число $n^2 - 1$ делится на 24.

3. Доказать, что число $\frac{n!}{2^n}$ нецелое.

4. Доказать, что для любых целых чисел $a$, $b$, $c$ справедливо равенство НОД($a$, $b$, $c$) = НОД(НОД($a$, $b$), $c$).

5. Доказать, что для любых целых чисел $a$, $b$, $c$ справедливо равенство НОД($ac$, $bc$) = $c \cdot$ НОД($a$, $b$).

6. Для взаимно простых чисел $m$, $n$ найти а) НОД($m + n$, $m - n$); б) НОД($mn$, $m^2 + n^2$).

7. При каких натуральных $m$, $n$ число $n^4 + 4m^4$ простое?

8. Доказать, что простых чисел вида $4m + 3$ бесконечно много.

## Литература к главе 1


1. *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел. — М.: Мир, 1987.
2. *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов. — М.: Мир, 1979.
3. *Виноградов И. М.* Основы теории чисел. — М.: Наука, 1981.
4. *Гашков С. Б., Чубариков В. Н.* Арифметика, алгоритмы, сложность вычислений. — М.: Высшая школа, 2000.
5. *Черемушкин А. В.* Лекции по арифметическим алгоритмам в криптографии. — М.: МЦНМО, 2002. Доступно с http://www.cryptography.ru/.
6. *Menezes A., van Oorschot P., Vanstone S.* Handbook of applied cryptography. CRC Press, 1997. Доступно с http://www.cacr.math.uwaterloo.ca/hac/.

## Глава 2

# СРАВНЕНИЯ С ОДНИМ НЕИЗВЕСТНЫМ

## 2.1. Отношение сравнимости

Многие свойства чисел, а также вопросы разрешимости уравнений в целых числах удобно описывать в терминах сравнений.

Определение 2.1. Пусть $m \in \mathbb{N}$, $m > 1$. Целые числа $a$ и $b$ называются *сравнимыми по модулю* $m$ (обозначается $a \equiv b \pmod{m}$), если разность $a - b$ делится на $m$.

Отношение сравнимости обладает следующими свойствами.

1. *Рефлексивность*: $a \equiv a \pmod{m}$.

2. *Симметричность*: если $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$.

3. *Транзитивность*: если $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$.

4. Сравнения можно почленно складывать (вычитать): если $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, то $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$.

*Доказательство*. Из определения отношения сравнимости имеем: $a_1 - b_1$ делится на $m$, $a_2 - b_2$ делится на $m$. Тогда, по свойству 2 делимости, сумма и разность $(a_1 - b_1) \pm (a_2 - b_2)$ делятся на $m$, откуда $(a_1 \pm a_2) - (b_1 \pm b_2)$ делится на $m$. □

5. Сравнения можно почленно перемножать: если $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, то $a_1a_2 \equiv b_1b_2 \pmod{m}$.

*Доказательство*. Покажем, что разность $a_1a_2 - b_1b_2$ делится на $m$. Прибавим к этому выражению и вычтем из него число $a_1b_2$. Получим: $a_1a_2 - b_1b_2 = a_1a_2 - a_1b_2 + a_1b_2 - b_1b_2 = a_1(a_2 - b_2) + (a_1 - b_1)b_2$. Так как оба слагаемых в последней сумме делятся на $m$, то и вся сумма делится на $m$.

□

6. Обе части сравнения и модуль можно разделить на их общий делитель: если $ac \equiv bc \pmod{mc}$, где $c \neq 0$, то $a \equiv b \pmod{m}$.

*Доказательство.* Выражение $ac \equiv bc \pmod{mc}$ означает, что разность $ac - bc$ делится на $mc$, то есть, по определению делимости, существует такое целое число $d$, что $ac - bc = mcd$. Вынесем общий множитель $c$ за скобки: $(a - b)c = mcd$. Тогда $a - b = md$, то есть $a - b$ делится на $m$. □

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

*Доказательство.* Пусть $a \equiv b \pmod{m}$, где $a = a_1 d$, $b = b_1 d$, НОД$(d, m) = 1$. По определению отношения сравнимости разность $a - b = (a_1 - b_1)d$ делится на $m$. Числа $d$ и $m$ взаимно просты, значит, по свойству 2 взаимно простых чисел, разность $a_1 - b_1$ делится на $m$. □

8. Если $m_1$ — делитель числа $m$ и $a \equiv b \pmod{m}$, то $a \equiv b \pmod{m_1}$.

9. Если $f(x)$ — полином с целыми коэффициентами и $a \equiv b \pmod{m}$, то $f(a) \equiv f(b) \pmod{m}$.

Отношение, обладающее свойствами рефлексивности, симметричности и транзитивности, называется *отношением эквивалентности*. Таким образом, отношение сравнимости является отношением эквивалентности на множестве $\mathbb{Z}$ целых чисел.

Отношение эквивалентности разбивает множество, на котором оно определено, на *классы эквивалентности*. Любые два класса эквивалентности либо не пересекаются, либо совпадают.

Классы эквивалентности, определяемые отношением сравнимости, называются *классами вычетов по модулю m*. Класс вычетов, содержащий число $a$, обозначается $a \pmod{m}$ или $\bar{a}$ и представляет собой множество чисел вида $a + km$, где $k \in \mathbb{Z}$; число $a$ называется *представителем* этого класса вычетов.

Множество классов вычетов по модулю $m$ обозначается $\mathbb{Z}/m\mathbb{Z}$, состоит ровно из $m$ элементов и относительно операций сложения и умножения является *кольцом классов вычетов* по модулю $m$.

Пример 2.1. Если $m = 2$, то $\mathbb{Z}/2\mathbb{Z} = \{0 \pmod 2, 1 \pmod 2\}$, где $0 \pmod 2 = 2\mathbb{Z}$ — множество всех четных чисел, $1 \pmod 2 = 2\mathbb{Z} + 1$ — множество всех нечетных чисел. □

Пример 2.2. При $m = 15$ отношение сравнимости разбивает множество $\mathbb{Z}$ на 15 классов вычетов: $\mathbb{Z}/15\mathbb{Z} = \{0 \pmod{15}, 1 \pmod{15}, \ldots, 14 \pmod{15}\}$, где $0 \pmod{15} = \{\ldots, -30, -15, 0, 15, 30, \ldots\}$, $1 \pmod{15} = \{\ldots, -29, -14, 1, 16, 31, \ldots\}$, ..., $14 \pmod{15} = \{\ldots, -16, -1, 14, 29, 44, \ldots\}$. □

Определение 2.2. *Полной системой вычетов* по модулю $m$ называется совокупность $m$ целых чисел, содержащая точно по одному представителю из каждого класса вычетов по модулю $m$. Совокупность чисел $0, 1, 2, \ldots, m-1$ называется *системой наименьших неотрицательных вычетов*. Совокупность чисел

$$0, \pm 1, \ldots, \pm\frac{m-1}{2} \text{ при нечетном } m;$$

$$-\frac{m}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{m}{2} \text{ при четном } m$$

называется *системой абсолютно наименьших вычетов* по модулю $m$. Каждый из абсолютно наименьших вычетов по абсолютной величине не превосходит половины модуля. Часть полной системы вычетов, состоящая из чисел, взаимно простых с модулем, называется *приведенной системой вычетов*.

Пример 2.3. Найдем различные системы вычетов по модулю $m = 6$.

Полная система вычетов: $\{0, 1, 2, 3, 4, 5\}$, или $\{6, -5, 14, 9, -14, -19\}$, или $\{0, 1, 2, -3, -2, -1\}$.

Система наименьших неотрицательных вычетов: $\{0, 1, 2, 3, 4, 5\}$.

Система абсолютно наименьших вычетов: $\{-2, -1, 0, 1, 2, 3\}$.

Приведенная система вычетов: $\{1, 5\}$. □

Определение 2.3. Функция $\varphi: \mathbb{N} \to \mathbb{N}$, ставящая в соответствие каждому натуральному числу $m$ количество $\varphi(m)$ натуральных чисел, меньших $m$ и взаимно простых с $m$, называется *функцией Эйлера*. При этом полагают $\varphi(1) = 1$.

Таким образом, функция Эйлера $\varphi(m)$ задает число элементов приведенной системы вычетов по модулю $m$.

Пример 2.4. $\varphi(2) = 1$ (единственное число, меньшее 2 и взаимно простое с ним, — это 1); $\varphi(3) = 2$ (числа 1, 2), $\varphi(6) = 2$ (числа 1, 5), $\varphi(9) = 6$ (числа 1, 2, 4, 5, 7, 8). □

Функция Эйлера обладает свойством *мультипликативности*: если НОД$(m, n) = 1$, то $\varphi(mn) = \varphi(m)\varphi(n)$.

Пример 2.5. Пусть $m = 3$, $n = 4$. Вычислим $\varphi(3)$, $\varphi(4)$ и $\varphi(3 \cdot 4) = \varphi(12)$. Имеем: $\varphi(3) = 2$ (числа 1, 2); $\varphi(4) = 2$ (числа 1, 3); $\varphi(12) = 4$ (числа 1, 5, 7, 11), то есть, действительно, $\varphi(12) = \varphi(3) \cdot \varphi(4)$. □

Теорема 2.1 (Эйлер). Пусть число $m > 1$ натуральное. Тогда для любого целого числа $a$, взаимно простого с $m$, выполняется сравнение $a^{\varphi(m)} \equiv 1 \pmod{m}$.

*Доказательство* [2]. Пусть $r_1, r_2, \ldots, r_{\varphi(m)}$ — приведенная система вычетов по модулю $m$, составленная из наименьших неотрицательных вычетов. Сопоставим каждому из чисел $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ его наименьший неотрицательный вычет $\rho_i$, где $i = 1, 2, \ldots, \varphi(m)$, то есть $\rho_1 \equiv ar_1 \pmod{m}$, $\rho_2 \equiv ar_2 \pmod{m}$, $\ldots$, $\rho_{\varphi(m)} \equiv ar_{\varphi(m)} \pmod{m}$, и покажем, что сис-

темы вычетов $\rho_1, \rho_2, \ldots, \rho_{\varphi(m)}$ и $r_1, r_2, \ldots, r_{\varphi(m)}$ совпадают с точностью до порядка элементов.

Действительно, поскольку НОД$(a, m) = 1$ (по условию теоремы) и НОД$(r_i, m) = 1$ для всех $i = 1, 2, \ldots, \varphi(m)$ (по определению приведенной системы вычетов), то по свойству 3 взаимно простых чисел НОД$(ar_i, m) = 1$ для всех $i = 1, 2, \ldots, \varphi(m)$. Из сравнения $\rho_i \equiv ar_i \pmod m$ следует существование такого целого числа $z_i$, что $\rho_i = ar_i + mz_i$, где $i = 1, 2, \ldots, \varphi(m)$. Тогда, согласно лемме 1.6, НОД$(\rho_i, m) =$ НОД$(ar_i + mz_i, m) =$ $=$ НОД$(ar_i, m) = 1$, то есть наименьшие неотрицательные вычеты $\rho_i$ взаимно просты с числом $m$. Значит, каждому из чисел $\rho_i$ соответствует некоторое число $r_j$.

Осталось показать, что все числа $\rho_1, \rho_2, \ldots, \rho_{\varphi(m)}$ различны. Действительно, если выполняется равенство $\rho_i = \rho_k$, то $ar_i \equiv ar_k \pmod m$. Числа $a$ и $m$ взаимно просты, поэтому можем поделить обе части сравнения на $a$. Получим $r_i \equiv r_k \pmod m$. Но $r_i$ и $r_k$ — наименьшие неотрицательные вычеты, тогда должно выполняться равенство $r_i = r_k$, а это не так. Значит, и среди чисел $\rho_1, \rho_2, \ldots, \rho_{\varphi(m)}$ нет одинаковых, и эти две системы вычетов совпадают.

Перемножаем: $\rho_1\rho_2\ldots\rho_{\varphi(m)} \equiv a^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} \pmod m$. Поскольку $\rho_1\rho_2\ldots\rho_{\varphi(m)} \equiv r_1 r_2 \ldots r_{\varphi(m)} \pmod m$, поделим обе части предыдущего сравнения на одно и то же число (а это сделать можно, так как система приведенная, и произведение взаимно просто с $m$), получаем $a^{\varphi(m)} \equiv 1 \pmod m$. □

Пример 2.6. Пусть $a = 2$, $m = 35$. Вычислим функцию Эйлера: $\varphi(35) = \varphi(5 \cdot 7) = \varphi(5) \cdot \varphi(7) = 4 \cdot 6 = 24$. Тогда $2^{24} = (2^5)^4 \cdot 2^4 \equiv 3^4 \cdot 2^4 \equiv$ $\equiv (6^2)^2 \equiv 1 \pmod{35}$. □

Замечание. Умножив обе части сравнения $a^{\varphi(m)} \equiv 1 \pmod m$ на $a$, получим сравнение

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

которое будет выполняться уже для любого числа $a$, не обязательно взаимно простого с $m$.

Пример 2.7. Пусть $a = 18$, $m = 42$. Вычислим функцию Эйлера:

$$\varphi(42) = \varphi(2 \cdot 3 \cdot 7) = \varphi(2) \cdot \varphi(3) \cdot \varphi(7) = 1 \cdot 2 \cdot 6 = 12.$$

Тогда

$$18^{13} = (18^3)^4 \cdot 18 \equiv (2 \cdot 18)^4 \cdot 18 = 2^4 \cdot 18^3 \cdot 18^2 \equiv 2^5 \cdot 18^3 \equiv 2^6 \cdot 18 =$$

$$= 2^7 \cdot 9 \equiv 2 \cdot 9 = 18 \pmod{42}. \qquad \square$$

Если число $p$ простое, то $\varphi(p) = p - 1$. Отсюда получаем частный случай теоремы Эйлера.

Теорема 2.2 (малая теорема Ферма). Пусть число $p$ простое, число $a$ целое, $a$ не делится на $p$. Тогда $a^{p-1} \equiv 1 \pmod{p}$.

Пример 2.8. Используя малую теорему Ферма, найдем младший разряд числа $7^{1000000}$ в системе счисления с основанием 13.

В этой системе счисления $7^{1000000} = a_n \cdot 13^n + a_{n-1} \cdot 13^{n-1} + \ldots + a_1 \cdot 13 + a_0$, где $0 \le a_i < 13$, для всех $i = 0, 1, \ldots, n$. Тогда $7^{1000000} \equiv a_0 \pmod{13}$, то есть для решения задачи нужно вычислить $7^{1000000} \pmod{13}$. Числа 7 и 13 взаимно просты, поэтому в обозначениях малой теоремы Ферма $a = 7$, $p = 13$ и $7^{12} \equiv 1 \pmod{13}$. Используя теорему о делении с остатком, находим представление $1000000 = 12 \cdot 83333 + 4$. Отсюда $7^{1000000} = 7^{12 \cdot 83333 + 4} = (7^{12})^{83333} \cdot 7^4 \equiv 7^4 \equiv 9 \pmod{13}$, то есть $a_0 = 9$. $\square$

Рассмотрим способ вычисления функции Эйлера.

Теорема 2.3. Если число $p$ простое, число $n$ натуральное, то $\varphi(p^n) = p^n - p^{n-1}$.

*Доказательство*. Число $p$ простое, тогда любое число $a$, не превосходящее $p^n$ и не взаимно простое с $p^n$, делится на $p$, то есть является элементом множества $P = \{p, 2p, \ldots, p^n\}$. Функция Эйлера $\varphi(p^n)$ будет задавать число элементов множества $\{1, 2, \ldots, p^n\} \setminus P$. Это число равно $p^n - p^{n-1}$. □

Из свойства мультипликативности функции Эйлера и теоремы 2.3 следует, что если число $n > 1$ и $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ — его каноническое разложение, то

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_s^{\alpha_s}) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_s}\right).$$

Эту формулу называют *формулой Эйлера*. С ее помощью можно дать еще одно доказательство первой теоремы Евклида о простых числах (теорема 1.12). Как и ранее, предположим, что $p_1, p_2, \ldots, p_s$ — все простые числа, и составим число $N = p_1 p_2 \ldots p_s$. Тогда должно выполняться равенство $\varphi(N) = 1$ (все числа, не превосходящие $N$, должны делиться хотя бы на одно из простых чисел $p_1, p_2, \ldots, p_s$). Но по формуле Эйлера

$$\varphi(N) = N\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_s}\right) = (p_1-1)(p_2-1)\ldots(p_s-1) \neq 1.$$

Пример 2.9. Вычислим $\varphi(283500)$. Находим каноническое разложение: $283500 = 2^2 \cdot 3^4 \cdot 5^3 \cdot 7$. Тогда по формуле Эйлера:

$$\varphi(283500) = 283500 \cdot \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) =$$

$$= 283500 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = 64800.$$ □

## 2.2. Решение сравнений

Сравнение с одним неизвестным $x$ имеет вид

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{m}, \qquad (2.1)$$

где $m \in \mathbb{N}$, $m > 1$. Если $a_n$ не делится на $m$, то $n$ называется *степенью* сравнения (2.1).

*Решением* сравнения (2.1) называется всякое целое число $x_0$, для которого $a_n x_0^n + a_{n-1}x_0^{n-1} + \ldots + a_0 \equiv 0 \pmod{m}$. Если $x_0$ удовлетворяет сравнению (2.1), то, согласно свойству 9 сравнений, этому сравнению будут удовлетворять все целые числа, сравнимые с $x_0$ по модулю $m$. Поэтому все решения сравнения (2.1), принадлежащие одному классу вычетов по модулю $m$, будем рассматривать как одно решение. Таким образом, сравнение (2.1) имеет столько решений, сколько элементов полной системы вычетов ему удовлетворяет.

Сравнения, множества решений которых совпадают, называются *равносильными*.

### 2.2.1. Сравнения первой степени

Сравнение первой степени с одним неизвестным $x$ имеет вид

$$ax \equiv b \pmod{m}. \qquad (2.2)$$

Теорема 2.4. Для того чтобы сравнение (2.2) имело хотя бы одно решение, необходимо и достаточно, чтобы число $b$ делилось на НОД($a$, $m$).

*Доказательство.* Сначала докажем необходимость. Пусть $d$ = НОД($a$, $m$) и $x_0$ — решение сравнения (2.2). Тогда $ax_0 \equiv b \pmod{m}$, то есть разность $ax_0 - b$ делится на $m$. Значит, существует такое целое число $q$, что $ax_0 - b = qm$. Отсюда $b = ax_0 - qm$. А поскольку $d$, как общий делитель, делит числа $a$ и $m$, то уменьшаемое и вычитаемое делятся на $d$, а значит и $b$ делится на $d$.

Теперь докажем достаточность. Пусть $d$ — наибольший общий делитель чисел $a$ и $m$, и $b$ делится на $d$. Тогда по определению делимости существуют такие целые числа $a_1$, $b_1$, $m_1$, что $a = a_1d$, $b = b_1d$, $m = m_1d$.

Расширенным алгоритмом Евклида найдем линейное представление числа 1 = НОД($a_1$, $m_1$):

$$1 = a_1x_0 + m_1y_0$$

для некоторых $x_0, y_0 \in \mathbb{Z}$. Домножим обе части последнего равенства на $b_1d$:

$$b_1d = a_1b_1dx_0 + m_1b_1dy_0$$

или, что то же самое,

$$b = ab_1x_0 + mb_1y_0,$$

то есть $ab_1x_0 \equiv b \pmod{m}$, и $b_1x_0$ — решение сравнения (2.2). □

Пример 2.10. Сравнение $9x \equiv 6 \pmod{12}$ имеет решение, так как НОД(9, 12) = 3 и 6 делится на 3. □

Пример 2.11. Сравнение $6x \equiv 9 \pmod{12}$ не имеет решений, так как НОД(6, 12) = 6, а 9 не делится на 6. □

Теорема 2.5. Пусть сравнение (2.2) разрешимо и $d$ = НОД($a$, $m$). Тогда множество решений сравнения (2.2) состоит из $d$ классов вычетов по модулю $m$, а именно, если $x_0$ — одно из решений, то все другие решения — это $x_0 + m_1$, $x_0 + 2m_1$, …, $x_0 + (d-1)m_1$, где $m_1 = \dfrac{m}{d}$.

*Доказательство*. Пусть $x_0$ — решение сравнения (2.2), то есть $ax_0 \equiv b \pmod{m}$ и $a = a_1d$, $m = m_1d$. Значит, существует такое $q \in \mathbb{Z}$, что $ax_0 - b = qm$. Подставляя теперь в последнее равенство вместо $x_0$ произвольное решение вида $x_0 + km_1$, где $1 \le k \le d-1$, получаем выражение

$$a(x_0 + km_1) - b = ax_0 + akm_1 - b = ax_0 - b + akm_1 =$$

$$= qm + a_1dkm_1 = (q + a_1k)m,$$

делящееся на $m$. □

Пример 2.12. Сравнение $9x \equiv 6 \pmod{12}$ имеет ровно три решения, так как НОД(9, 12) = 3. Эти решения: $x_0 = 2$, $x_0 + 4 = 6$, $x_0 + 2 \cdot 4 = 10$. □

Пример 2.13. Сравнение $11x \equiv 2 \pmod{15}$ имеет единственное решение $x_0 = 7$, так как НОД(11, 15) = 1. □

Покажем, как решать сравнение первой степени. Не умаляя общности, будем считать, что НОД$(a, m) = 1$. Тогда решение сравнения (2.2) можно искать, например, по алгоритму Евклида. Действительно, используя расширенный алгоритм Евклида, представим число 1 в виде линейной комбинации чисел $a$ и $m$:

$$1 = aq + mr.$$

Умножим обе части этого равенства на $b$, получим: $b = abq + mrb$, откуда $abq - b = -mrb$, то есть $a \cdot (bq) \equiv b \pmod{m}$ и $bq$ — решение сравнения (2.2).

Еще один путь решения — использовать теорему Эйлера. Опять считаем, что НОД$(a, m) = 1$. Применяем теорему Эйлера: $a^{\varphi(m)} \equiv 1 \pmod{m}$. Умножим обе части сравнения на $b$: $a^{\varphi(m)}b \equiv b \pmod{m}$. Переписывая последнее выражение в виде $a(a^{\varphi(m)-1}b) \equiv b \pmod{m}$, получаем, что $a^{\varphi(m)-1}b$ — решение сравнения (2.2).

Пусть теперь НОД$(a, m) = d > 1$. Тогда $a = a_1d$, $m = m_1d$, где НОД$(a_1, m_1) = 1$. Кроме того, необходимо $b = b_1d$, для того чтобы сравнение было разрешимо. Если $x_0$ — решение сравнения $a_1x \equiv b_1 \pmod{m_1}$, причем единственное, поскольку НОД$(a_1, m_1) = 1$, то $x_0$ будет решением и сравнения $a_1dx \equiv b_1d \pmod{m_1d}$, то есть исходного сравнения (2.2). Остальные $d - 1$ решений находим по теореме 2.5.

Пример 2.14. Решим сравнение $12x \equiv 9 \pmod{21}$. Вычисляем НОД(12, 21) = 3. Число 9 делится на 3, поэтому сравнение разрешимо, и у него три решения. Поделим обе части сравнения и модуль на их наибольший общий делитель: $4x \equiv 3 \pmod 7$. Поскольку НОД(4, 7) = 1, можем воспользоваться теоремой Эйлера: $x_0 = 4^{\varphi(7)-1} \cdot 3 \equiv 4^5 \cdot 3 \equiv 6 \pmod 7$. Таким образом, 6 — это одно из решений сравнения $12x \equiv 9 \pmod{21}$. Находим остальные решения:

$$6 + \frac{21}{3} = 6 + 7 = 13, \quad 6 + 2 \cdot \frac{21}{3} = 6 + 14 = 20.$$

Проверка: $12 \cdot 6 - 9 = 63 = 21 \cdot 3$; $12 \cdot 13 - 9 = 147 = 21 \cdot 7$; $12 \cdot 20 - 9 = 231 = 21 \cdot 11$. □

Замечание. Следует особо отметить сравнение первой степени вида $ax \equiv 1 \pmod m$. Оно разрешимо тогда и только тогда, когда НОД$(a, m) = 1$, и при условии разрешимости имеет единственное решение. Это решение $x_0$ обозначается $a^{-1}$ и называется *мультипликативно обратным* к числу $a$ по модулю $m$. Таким образом, число $a^{-1}$, мультипликативно обратное к $a$ по модулю $m$, — это такое число, при умножении которого на $a$ получается единица по модулю $m$.

Пример 2.15. Найдем число, мультипликативно обратное к 26 по модулю 49. Числа 26 и 49 взаимно просты, значит, искомое число существует. Реализуем расширенный алгоритм Евклида для чисел 26 и 49, промежуточные результаты занесем в таблицу:

| $i$ | $r_i$ | $x_i$ | $y_i$ | $q_i$ |
|---|---|---|---|---|
| 1 | 49 | 1 | 0 | |
| 2 | 26 | 0 | 1 | 1 |
| 3 | 23 | 1 | −1 | 1 |
| 4 | 3 | −1 | 2 | 7 |

| $i$ | $r_i$ | $x_i$ | $y_i$ | $q_i$ |
|---|---|---|---|---|
| 5 | 2 | 8 | −15 | 1 |
| 6 | 1 | −9 | 17 | |

Таким образом, $49 \cdot (-9) + 26 \cdot 17 = 1$. Приводим обе части этого равенства по модулю 49: $26 \cdot 17 \equiv 1 \pmod{49}$. Таким образом, число 17 является мультипликативно обратным к числу 26 по модулю 49, то есть $26^{-1} \equiv 17 \pmod{49}$. Точно так же число 26 является мультипликативно обратным к числу 17 по модулю 49, то есть $17^{-1} \equiv 26 \pmod{49}$. □

Отметим, что если число $p$ простое, то сравнение $ax \equiv 1 \pmod{p}$ разрешимо для любого числа $a$, не делящегося на $p$, то есть для любого такого $a$ существует мультипликативно обратное по модулю $p$. Значит, кольцо классов вычетов $\mathbb{Z}/p\mathbb{Z}$ является полем. Это поле часто обозначают $\mathbb{F}_p$ и называют *конечным полем из p элементов* (см. главу 7).

### 2.2.2. Китайская теорема об остатках

Рассмотрим систему сравнений первой степени:

$$x \equiv a_1 \pmod{m_1},\ x \equiv a_2 \pmod{m_2},\ \ldots,\ x \equiv a_r \pmod{m_r}, \qquad (2.3)$$

где числа $m_1, m_2, \ldots, m_r$ попарно взаимно простые, и найдем значение $x_0 \in \mathbb{Z}$, удовлетворяющее всем $r$ сравнениям.

Теорема 2.6 (китайская теорема об остатках). Пусть числа $m_1, m_2, \ldots, m_r$ попарно взаимно простые и числа $a_1, a_2, \ldots, a_r$ произвольные целые. Тогда существует такое целое число $x_0$, что $0 \le x_0 < m_1 m_2 \ldots m_r$ и $x_0 \equiv a_1 \pmod{m_1}$, $x_0 \equiv a_2 \pmod{m_2}$, $\ldots$, $x_0 \equiv a_r \pmod{m_r}$.

*Доказательство.* Докажем теорему для $r = 2$. Пусть $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, НОД$(m_1, m_2) = 1$.

Пусть $x_0 \in \mathbb{Z}$ — решение первого сравнения, то есть $x_0 = a_1 + m_1 u$ для некоторого целого числа $u$. Найдем такое $u$, чтобы $x_0$ было решением и второго сравнения. Подставляем выражение для $x_0$ во второе сравнение: $a_1 + m_1 u \equiv a_2 \pmod{m_2}$. Получаем сравнение первой степени $m_1 u \equiv a_2 - a_1 \pmod{m_2}$ относительно неизвестного $u$. Числа $m_1$ и $m_2$ взаимно просты, поэтому по теореме 2.5 это сравнение имеет единственное решение. Найдем его по теореме Эйлера:

$$u_0 \equiv m_1^{\varphi(m_2)-1}(a_2 - a_1) \pmod{m_2}$$

или

$$u_0 = m_1^{\varphi(m_2)-1}(a_2 - a_1) + vm_2$$

для некоторого целого $v$.

Подставляем найденное решение в выражение для $x_0$:

$$x_0 = a_1 + m_1^{\varphi(m_2)}(a_2 - a_1) + vm_1 m_2,$$

то есть

$$x_0 \equiv a_1 + m_1^{\varphi(m_2)}(a_2 - a_1) \pmod{m_1 m_2}. \qquad (2.4)$$

□

Упражнение. Доказать теорему в общем случае методом математической индукции, используя доказанное утверждение в качестве базы индукции.

Замечание. Приведем выражение (2.4) к симметричному виду. Для этого сначала покажем, что $m_1^{\varphi(m_2)} + m_2^{\varphi(m_1)} \equiv 1 \pmod{m_1 m_2}$. Действительно, так как числа $m_1$, $m_2$ взаимно просты, можем применить к ним теорему Эйлера: $m_1^{\varphi(m_2)} \equiv 1 \pmod{m_2}$, то есть разность $m_1^{\varphi(m_2)} - 1$ делится на $m_2$. Но точно так же $m_2^{\varphi(m_1)} \equiv 1 \pmod{m_1}$, то есть разность $m_2^{\varphi(m_1)} - 1$ делится на $m_1$. Тогда выражение $m_1^{\varphi(m_2)} + m_2^{\varphi(m_1)} - 1$ делится на $m_1 m_2$.

Раскроем скобки в формуле (2.4) и воспользуемся только что доказанным соотношением:

$$x_0 \equiv -a_1(m_1^{\varphi(m_2)} - 1) + a_2 m_1^{\varphi(m_2)} \equiv a_1 m_2^{\varphi(m_1)} + a_2 m_1^{\varphi(m_2)} =$$
$$= a_1 m_2 m_2^{\varphi(m_1)-1} + a_2 m_1 m_1^{\varphi(m_2)-1} \pmod{m_1 m_2}$$

или, в другой записи,

$$x_0 \equiv a_1 m_2 (m_2^{-1} \pmod{m_1}) + a_2 m_1 (m_1^{-1} \pmod{m_2}) \pmod{m_1 m_2}.$$

В общем случае получаем *целочисленный аналог интерполяционной формулы Лагранжа*:

$$x_0 \equiv \sum_{i=1}^{r} a_i M_i N_i \pmod{m_1 m_2 \ldots m_r}, \tag{2.5}$$

где $M_i = m_1 \ldots m_{i-1} m_{i+1} \ldots m_r$ и $N_i \equiv M_i^{-1} \pmod{m_i}$.

Пример 2.16. Решим систему сравнений $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 6$, $x \equiv 4 \pmod 7$.

Вычисляем: $M_1 = 6 \cdot 7 = 42$, $M_2 = 5 \cdot 7 = 35$, $M_3 = 5 \cdot 6 = 30$. Находим мультипликативно обратные числа:

$$N_1 \equiv 42^{-1} \equiv 2^{-1} \equiv 3 \pmod 5;$$

$$N_2 \equiv 35^{-1} \equiv 5^{-1} \equiv 5 \pmod 6;$$

$$N_3 \equiv 30^{-1} \equiv 2^{-1} \equiv 4 \pmod 7.$$

Подставляем значения в формулу (2.5):

$$x_0 \equiv 2 \cdot 42 \cdot 3 + 3 \cdot 35 \cdot 5 + 4 \cdot 30 \cdot 4 =$$

$$= 252 + 525 + 480 = 1257 \equiv 207 \pmod{210}.$$

Проверка: $207 - 2 = 205 = 5 \cdot 41$, то есть $207 \equiv 2 \pmod 5$; $207 - 3 = 204 = 6 \cdot 34$, то есть $207 \equiv 3 \pmod 6$; $207 - 4 = 203 = 7 \cdot 29$, то есть $207 \equiv 4 \pmod 7$. □

Определение 2.4. Пусть $f(x_1, x_2, \ldots, x_n)$ — полином $n$-й степени с целыми коэффициентами от переменных $x_1, x_2, \ldots, x_n$. Уравнение вида $f(x_1, x_2, \ldots, x_n) = 0$, которое нужно решить в целых (или рациональных) числах, называется *диофантовым*.

Следствие. Диофантово уравнение $f(x_1, x_2, \ldots, x_n) = 0$ разрешимо в целых числах тогда и только тогда, когда оно разрешимо по модулю любого простого числа.

Пример 2.17. Покажем, что уравнение $x^2 - 7y^3 = 3$ не имеет целочисленных решений, то есть не существует пары целых чисел $x$, $y$, удовлетворяющих данному уравнению.

Приведем обе части уравнения по модулю 7, получим

$$x^2 \equiv 3 \pmod 7,$$

то есть если пара целых чисел $(x_0, y_0)$ — решение исходного уравнения, то $x_0^2 \equiv 3 \pmod 7$. Заметим, что число $x_0$ имеет вид $x_0 = 7q + r$, где число $q$ целое и $r \in \{0, 1, 2, 3, 4, 5, 6\}$. Тогда

$$x_0^2 = (7q + r)^2 = 49q^2 + 14qr + r^2 \equiv r^2 \pmod 7.$$

Число $r^2$ при делении на 7 дает остатки 0, 1, 4, 2, 4, 1. Таким образом, ни для какого целого числа $x_0$ сравнение $x_0^2 \equiv 3 \pmod 7$ не выполнено, а значит, и исходное уравнение $x^2 - 7y^3 = 3$ не имеет целочисленных решений. □

### 2.2.3. Сравнения произвольной степени по простому модулю

Теорема 2.7. Сравнение

$$f(x) \equiv 0 \pmod p, \tag{2.6}$$

где $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ и число $p$ простое, равносильно сравнению степени не выше $p - 1$.

*Доказательство* [2]. Разделим $f(x)$ с остатком на $x^p - x$, получим

$$f(x) = (x^p - x)q(x) + r(x),$$

где $0 \le \deg r(x) \le p - 1$. Согласно малой теореме Ферма, $x^p - x \equiv 0 \pmod p$, поэтому $f(x) \equiv r(x) \pmod p$. □

Пример 2.18. Найдем сравнение степени ниже 7, которому равносильно сравнение

$$f(x) = 2x^{11} + 5x^{10} + 2x^9 + 4x^8 + 2x^7 + 3x^6 + x^4 + 5x^3 + 3x^2 + 3x + 5 \equiv 0 \pmod 7.$$

Делим $f(x)$ с остатком на $x^7 - x$: $f(x) = (x^7 - x)q(x) + r(x)$, где

$$q(x) = 2x^4 + 5x^3 + 2x^2 + 4x + 2, \quad r(x) = 3x^6 + 2x^5 + 6x^4 + 7x^3 + 7x^2 + 5x + 5.$$

Приводя коэффициенты полинома $r(x)$ по модулю 7, получаем:

$$f(x) \equiv 3x^6 + 2x^5 + 6x^4 + 5x + 5 \pmod 7.$$ □

Теорема 2.8. Если сравнение (2.6) имеет больше чем $n$ решений, то $a_i \equiv 0 \pmod p$ для $i = 0, 1, \ldots, n$.

*Доказательство* [2]. Пусть $x_1, x_2, \ldots, x_n, x_{n+1}$ — различные решения сравнения (2.6). Тогда полином $f(x)$ можно представить в виде

$$f(x) = b_n(x - x_1)(x - x_2)\ldots(x - x_{n-1})(x - x_n) +$$

$$+ b_{n-1}(x - x_1)(x - x_2)\ldots(x - x_{n-1}) + \ldots + b_1(x - x_1) + b_0,$$

где $b_n = a_n$, $b_{n-t} = a_{n-t} + \sum_{j=1}^{t}\left(a_{n-t+j}\sum_{i_1\ldots i_j=1}^{n-t+1} x_{i_1}x_{i_2}\ldots x_{i_j}\right)$, $1 \le t \le n$.

Вычисляем: $f(x_1) = b_0$, но $x_1$ — решение сравнения (2.6), значит, $f(x_1) \equiv 0 \pmod p$ и $b_0 \equiv 0 \pmod p$.

Далее: $f(x_2) = b_0 + b_1(x_2 - x_1) \equiv b_1(x_2 - x_1) \equiv 0 \pmod p$. Поскольку $x_1 \ne x_2 \pmod p$, получаем $b_1 \equiv 0 \pmod p$. Продолжая процесс, получаем, что $b_i \equiv 0 \pmod p$ для всех $0 \le i \le n$. А значит, и $a_i \equiv 0 \pmod p$ для всех $0 \le i \le n$. □

## 2.3. Сравнения второй степени

Будем рассматривать сравнения второй степени вида

$$x^2 \equiv a \pmod{m}, \tag{2.7}$$

где $m \in \mathbb{N}$, $m > 1$, числа $a$ и $m$ взаимно просты. Целое число $a$ представляет соответствующий класс вычетов по модулю $m$.

Определение 2.5. Если сравнение (2.7) разрешимо, то число $a$ называется *квадратичным вычетом по модулю $m$*, в противном случае $a$ называется *квадратичным невычетом по модулю $m$*.

Пример 2.19. Число 5 является квадратичным вычетом по модулю 11, поскольку сравнение $x^2 \equiv 5 \pmod{11}$ имеет очевидное решение $x \equiv 4 \pmod{11}$: $4^2 = 16 \equiv 5 \pmod{11}$. □

Пример 2.20. Число 21 является квадратичным вычетом по модулю $m = 541 \cdot 547 \cdot 563 \cdot 571 \cdot 587$, поскольку сравнение $x^2 \equiv 21 \pmod{m}$ имеет решение $x \equiv 10208002722743 \pmod{m}$. □

Пример 2.21. Число 3 является квадратичным невычетом по модулю 7, поскольку ни одно из чисел $1^2 = 1$, $2^2 = 4$, $3^2 = 9 \equiv 2 \pmod{7}$, $4^2 = 16 \equiv 2 \pmod{7}$, $5^2 = 25 \equiv 4 \pmod{7}$, $6^2 = 36 \equiv 1 \pmod{7}$ не сравнимо с 3 по модулю 7, то есть сравнение $x^2 \equiv 3 \pmod{7}$ не имеет решений. □

### 2.3.1. Символы Лежандра и Якоби

Определение 2.6. Рассмотрим сравнение

$$x^2 \equiv a \pmod{p}, \tag{2.8}$$

где число $p$ простое, $p \neq 2$, $a$ не делится на $p$. Определим для таких $a$ и $p$ *символ Лежандра*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если сравнение (2.8) разрешимо,} \\ -1, & \text{если сравнение (2.8) неразрешимо.} \end{cases}$$

Таким образом, если $\left(\frac{a}{p}\right)=1$, то $a$ — квадратичный вычет по модулю $p$, если $\left(\frac{a}{p}\right)=-1$, то $a$ — квадратичный невычет по модулю $p$.

Замечание. Понятие символа Лежандра можно обобщить и на случай, когда $a$ делится на $p$. Тогда полагают $\left(\frac{a}{p}\right)=0$.

Символ Лежандра обладает следующими свойствами для любых целых чисел $a$, $b$, не делящихся на простое число $p \neq 2$.

1. $\left(\frac{a+kp}{p}\right)=\left(\frac{a}{p}\right)$ для любого $k \in \mathbb{Z}$.

*Доказательство*. Равенство выполняется, поскольку $a+kp \equiv a \pmod{p}$ для любого $k \in \mathbb{Z}$. Таким образом, если $a \equiv b \pmod{p}$, то $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$. □

2. $\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right)$.

*Доказательство*. Так как НОД$(b, p) = 1$, существует $b^{-1} \pmod{p}$. Тогда сравнения $x^2 \equiv ab^2 \pmod{p}$ и $(b^{-1}x)^2 \equiv a \pmod{p}$ разрешимы или не разрешимы одновременно. □

3. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. В частности, $\left(\frac{1}{p}\right)=1$ для любого простого $p \neq 2$, $\left(\frac{-1}{p}\right)=1$ при $p \equiv 1 \pmod 4$ и $\left(\frac{-1}{p}\right)=-1$ при $p \equiv 3 \pmod 4$.

*Доказательство* [2]. Согласно малой теореме Ферма, $a^{p-1} \equiv 1 \pmod{p}$. Тогда $a^{p-1}-1=(a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1) \equiv 0 \pmod{p}$. Оба сомножителя в этом сравнении на $p$ делиться не могут, так как иначе их разность, рав-

ная 2, делилась бы на $p$. Таким образом, для каждого $a$, $1 \le a < p$, выполняется ровно одно из сравнений

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p, \tag{2.9}$$

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p. \tag{2.10}$$

Если $a$ — квадратичный вычет по модулю $p$, то существует такое число $c$, что $a \equiv c^2 \pmod p$. Возводя обе части этого сравнения в степень $\frac{p-1}{2}$ и воспользовавшись малой теоремой Ферма, получаем $a^{\frac{p-1}{2}} \equiv c^{p-1} \equiv 1 \pmod p$, то есть любой квадратичный вычет удовлетворяет сравнению (2.9). При этом, согласно теореме 2.8, сравнение $y^{\frac{p-1}{2}} \equiv 1 \pmod p$ не может иметь более $\frac{p-1}{2}$ решений. Следовательно, квадратичные невычеты удовлетворяют сравнению (2.10). □

4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

*Доказательство.* Дважды применяя свойство 3, получаем

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

Таким образом, разность $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ делится на $p$. Число $p$ простое, а символ Лежандра принимает значения $-1$, $1$, значит, делимость возможна лишь в том случае, когда $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. □

5. Лемма 2.9 (Гаусс). $\left(\frac{a}{p}\right)=(-1)^{\mu}$, где $\mu$ — число отрицательных вычетов среди абсолютно наименьших вычетов чисел $a, 2\cdot a, \ldots, \frac{p-1}{2}\cdot a$.

*Доказательство* [1]. Пусть $\pm m_k$ — абсолютно наименьший вычет, соответствующий числу $ka$, где $m_k > 0$. При изменении значения $k$ от 1 до $\frac{p-1}{2}$ число $\mu$ — это число знаков «–» при $m_k$. Покажем, что $m_k \neq m_l$, если $k \neq l$ и $1 \le k, l \le \frac{p-1}{2}$. Действительно, равенство $m_k = m_l$ означает, что $ka \equiv \pm la \pmod p$. Поскольку $a$ не делится на $p$, можем разделить обе части сравнения на $a$. Получим $k \equiv \pm l \pmod p$, то есть $k \pm l \equiv 0 \pmod p$. Но это невозможно, поскольку $|k \pm l| \le k + l \le p - 1$ и, кроме того, $k \neq l$. Значит, все элементы множества $\{m_1, m_2, \ldots, m_{(p-1)/2}\}$ различны, и это множество совпадает с множеством $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$. Перемножая сравнения $a \equiv \pm m_1 \pmod p$, $2a \equiv \pm m_2 \pmod p$, ..., $\frac{p-1}{2}\cdot a \equiv \pm m_{(p-1)/2} \pmod p$, получаем

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

Поскольку число $((p-1)/2)!$ не делится на $p$, поделим на него обе части сравнения: $a^{\frac{p-1}{2}} \equiv (-1)^{\mu} \pmod p$. Применяя свойство 3 и учитывая, что символ Лежандра принимает только значения 1 и $-1$, получаем требуемое равенство. □

Пример 2.22. Вычислим символ Лежандра $\left(\frac{5}{13}\right)$, используя лемму Гаусса. Составляем систему абсолютно наименьших вычетов: 5,

$2\cdot 5=10\equiv -3 \pmod{13}$, $3\cdot 5=15\equiv 2 \pmod{13}$, $4\cdot 5=20\equiv -6 \pmod{13}$, $5\cdot 5=25\equiv -1 \pmod{13}$, $6\cdot 5=30\equiv 4 \pmod{13}$. Получили три отрицательных значения, значит, $\left(\frac{5}{13}\right)=(-1)^3=-1$. □

6. $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$, то есть $\left(\frac{2}{p}\right)=1$ при $p\equiv \pm 1 \pmod 8$; $\left(\frac{2}{p}\right)=-1$ при $p\equiv \pm 3 \pmod 8$.

*Доказательство*. Рассмотрим систему вычетов $2\cdot 1$, $2\cdot 2$, ..., $2\cdot\frac{p-1}{2}$ по модулю $p$. В обозначениях леммы Гаусса число $\mu$ равно числу тех элементов этой системы, которые больше, чем $\frac{p-1}{2}$. Зададим целое число $m$ двойным неравенством: $\frac{p-1}{2}-2<2m\le\frac{p-1}{2}$. Тогда $\mu=\frac{p-1}{2}-m$.

Дальнейшие выкладки для всех возможных значений $p$ запишем в таблицу:

| $p$ | $\frac{p-1}{2}$ | $\frac{p-1}{2}-2<2m\le\frac{p-1}{2}$ | $m$ | $\mu$ | $\left(\frac{2}{p}\right)=(-1)^{\mu}$ |
|---|---|---|---|---|---|
| $8k+1$ | $4k$ | $4k-2<2m\le 4k$ | $2k$ | $2k$ | 1 |
| $8k+7$ | $4k+3$ | $4k+1<2m\le 4k+3$ | $2k+1$ | $2k+2$ | 1 |
| $8k+3$ | $4k+1$ | $4k-1<2m\le 4k+1$ | $2k$ | $2k+1$ | $-1$ |
| $8k+5$ | $4k+2$ | $4k<2m\le 4k+2$ | $2k+1$ | $2k+1$ | $-1$ |

□

7. При изменении $a$ от 1 до $p-1$ символ Лежандра принимает значения 1 и $-1$ одинаково часто.

*Доказательство.* Квадратичными вычетами по модулю $p$ являются те и только те числа, которые сравнимы с $1^2, 2^2, \ldots, ((p-1)/2)^2$. Все эти числа различны. Действительно, из $a^2 \equiv b^2 \pmod{p}$ для $0 < a < b \le \frac{p-1}{2}$ следует, что $a \equiv b \pmod{p}$ или $a \equiv -b \equiv p - b \pmod{p}$. Остальные $\frac{p-1}{2}$ чисел являются квадратичными невычетами по модулю $p$. □

Теорема 2.10 (квадратичный закон взаимности Гаусса). Пусть $p$ и $q$ — различные простые числа, $p \ne 2$, $q \ne 2$. Тогда

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

Другими словами, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, если $p \equiv q \equiv 3 \pmod{4}$, и $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ в противном случае.

*Доказательство* [3]. Определим функции $f$ и $g$, сопоставляющие каждому целому числу $m$ его абсолютно наименьший вычет по модулю $p$ и $q$ соответственно:

$$f(m) \equiv m \pmod{p},$$

$$g(m) \equiv m \pmod{q}.$$

Согласно китайской теореме об остатках, для каждого целого числа $m$ из интервала $\left[-\frac{pq-1}{2}, \frac{pq-1}{2}\right]$ существует единственная пара абсолютно наименьших вычетов $(f(m), g(m))$, и наоборот. Пусть $P$ — множество таких пар абсолютно наименьших вычетов, которым соответствуют целые числа $m$ из интервала $\left[1, \frac{pq-1}{2}\right]$. Обозначим

$$P^{++} = \{(x, y) \in P \mid x > 0, y > 0\},$$

$$P^{-+} = \{(x, y) \in P \mid x < 0, y \geq 0\},$$

$$P^{+-} = \{(x, y) \in P \mid x \geq 0, y < 0\},$$

и пусть $N^{++}$, $N^{-+}$, $N^{+-}$ — число элементов множества $P^{++}$, $P^{-+}$, $P^{+-}$ соответственно.

Существует ровно $\frac{p-1}{2}$ точек $(x, y)$ множества $P$, для которых $y = 0$, — это точки вида $(f(mq), 0)$, где $m = 1, 2, \ldots, \frac{p-1}{2}$. Пусть $u$ — число таких точек, для которых $f(mq) < 0$. Аналогично, существует ровно $\frac{q-1}{2}$ точек $(x, y)$ множества $P$, для которых $x = 0$, — это точки вида $(0, g(np))$, где $n = 1, 2, \ldots, \frac{q-1}{2}$. Пусть $v$ — число таких точек, для которых $g(mp) < 0$.

В множестве $P$ ровно $\frac{p-1}{2}\left(\frac{q-1}{2}+1\right)$ точек, для которых $f(m) > 0$, — это точки $(f(m), g(m))$, соответствующие числам $m = k + lp$, где $1 \leq k \leq \frac{p-1}{2}$, $0 \leq l \leq \frac{q-1}{2}$. Значит,

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

Аналогично $N^{++} + N^{-+} = \frac{p-1}{2} \cdot \frac{q-1}{2} + u + v$.

Функции $f$ и $g$ нечетные: $f(-m) = -f(m)$, $g(-m) = -g(m)$, поэтому для любой пары таких целых чисел $x \neq 0$, $y \neq 0$, что $x \in \left[-\frac{p-1}{2}, \frac{p-1}{2}\right]$, $y \in \left[-\frac{q-1}{2}, \frac{q-1}{2}\right]$, только одна из точек $(x, y)$ или $(-x, -y)$ принадлежит множеству $P$. А значит

$$N^{+-} + N^{-+} = \frac{p-1}{2} \cdot \frac{q-1}{2} + u + v.$$

Отсюда

$$2(N^{++}+N^{+-}+N^{-+})=3\left(\frac{p-1}{2}\cdot\frac{q-1}{2}+u+v\right).$$

Приведем обе части этого равенства по модулю 2, получим

$$0\equiv\frac{p-1}{2}\cdot\frac{q-1}{2}+u+v\pmod 2,$$

то есть

$$\frac{p-1}{2}\cdot\frac{q-1}{2}\equiv u+v\pmod 2$$

и

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}=(-1)^u(-1)^v,$$

а по лемме Гаусса $(-1)^u=\left(\frac{q}{p}\right),(-1)^v=\left(\frac{p}{q}\right)$. □

Пример 2.23. Вычислим символ Лежандра $\left(\frac{88}{347}\right)$. Разложим число 88 на множители: $88=2^3\cdot 11$. Значит, согласно свойству 4,

$$\left(\frac{88}{347}\right)=\left(\frac{2^3\cdot 11}{347}\right)=\left(\frac{2^3}{347}\right)\left(\frac{11}{347}\right).$$

По свойству 2 имеем: $\left(\frac{2^3}{347}\right)=\left(\frac{2\cdot 2^2}{347}\right)=\left(\frac{2}{347}\right)$. Поскольку $347\equiv 3 \pmod 8$, по свойству 6 получаем $\left(\frac{2}{347}\right)=-1$.

Для вычисления $\left(\frac{11}{347}\right)$ воспользуемся квадратичным законом взаимности: $\left(\frac{11}{347}\right)=(-1)^{\frac{11-1}{2}\cdot\frac{347-1}{2}}\left(\frac{347}{11}\right)=(-1)^{5\cdot 173}\left(\frac{347}{11}\right)=-\left(\frac{347}{11}\right)$.

Поскольку $347 = 11 \cdot 31 + 6$, по свойству 1 получаем $\left(\frac{347}{11}\right) = \left(\frac{6}{11}\right)$.

Снова применяем свойство 4: $\left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right)$. Вычисляем по свойству 6: $\left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = (-1)^{15} = -1$, по свойству 3: $\left(\frac{3}{11}\right) \equiv 3^{\frac{11-1}{2}} = 3^5 = 243 \equiv 1 \pmod{11}$. Таким образом, $\left(\frac{11}{347}\right) = -(-1 \cdot 1) = 1$ и $\left(\frac{88}{347}\right) = -1 \cdot 1 = -1$. □

Пример 2.24. Используя квадратичный закон взаимности, найдем такие простые числа $p$, для которых 5 является квадратичным вычетом. Запишем символ Лежандра

$$\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2}\frac{p-1}{2}}\left(\frac{p}{5}\right) = (-1)^{2\cdot\frac{p-1}{2}}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)$$

и определим, при каких значениях $p$ он равен 1. По свойству 3 символа Лежандра имеем:

$$\left(\frac{p}{5}\right) \equiv p^{\frac{5-1}{2}} = p^2 \pmod 5.$$

Таким образом, нужно найти такие простые числа $p$, для которых $p^2 \equiv 1 \pmod 5$. Простое число $p \neq 5$ при делении на 5 может давать в остатке 1, 2, 3 или 4, при этом $1^2 \equiv 4^2 \equiv 1 \pmod 5$. Значит, число 5 является квадратичным вычетом по модулю простых чисел вида $5k + 1$ и $5k + 4$, где число $k$ целое. Другими словами, число $p$, заданное в десятичной системе счисления, должно оканчиваться на 1 или на 9. Это, например, числа 11, 19, 29, 31 и т. д. □

Обобщением понятия символа Лежандра является символ Якоби.

Определение 2.7. Пусть $m, n \in \mathbb{Z}$, где $n = p_1 p_2 \ldots p_r$ и числа $p_i \neq 2$ простые (не обязательно различные). *Символ Якоби* $\left(\frac{m}{n}\right)$ определяется равенством

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)\left(\frac{m}{p_2}\right)\ldots\left(\frac{m}{p_r}\right).$$

Если число $n$ — простое, то символ Якоби является символом Лежандра.

Символ Якоби обладает следующими свойствами.

1. $\left(\frac{a}{n}\right)$ принимает значения 0, 1 или $-1$, причем $\left(\frac{a}{n}\right) = 0$ тогда и только тогда, когда НОД$(a, n) \neq 1$. Полагают $\left(\frac{a}{\pm 1}\right) = 1$.

2. $\left(\frac{a + kn}{n}\right) = \left(\frac{a}{n}\right)$ для всех $a, k \in \mathbb{Z}$.

3. $\left(\frac{ab^2}{n}\right) = \left(\frac{a}{n}\right)$ для всех $a, b \in \mathbb{Z}$, НОД$(b, n) = 1$.

4. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ для всех $a, b \in \mathbb{Z}$.

5. $\left(\frac{1}{n}\right) = 1$; $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$. Следовательно, $\left(\frac{-1}{n}\right) = 1$ при $n \equiv 1 \pmod 4$; $\left(\frac{-1}{n}\right) = -1$ при $n \equiv -1 \pmod 4$.

*Доказательство* [2]. Равенство $\left(\frac{1}{n}\right) = 1$ выполняется по определению символа Якоби. Для доказательства второго равенства отметим, что для нечетных чисел $p_1 = 2k_1 + 1$, $p_2 = 2k_2 + 1$ выполняется сравнение

$$\frac{p_1 p_2 - 1}{2} \equiv \frac{p_1 - 1}{2} + \frac{p_2 - 1}{2} \pmod 2.$$

Действительно, $(p_1-1)(p_2-1)=2k_1\cdot 2k_2=4k_1k_2\equiv 0 \pmod 4$, поэтому $p_1p_2-1=(p_1-1)(p_2-1)+p_1+p_2-2\equiv(p_1-1)+(p_2-1) \pmod 4$. Поделив крайние части и модуль этого сравнения на 2, получим требуемое соотношение. По индукции получаем

$$\sum_{i=1}^{r}\frac{p_i-1}{2}\equiv\frac{p_1p_2\ldots p_r-1}{2} \pmod 2.$$

Тогда $\left(\frac{-1}{n}\right)=\prod_{i=1}^{r}\left(\frac{-1}{p_i}\right)=\prod_{i=1}^{r}(-1)^{\frac{p_i-1}{2}}=(-1)^{\sum_{i=1}^{r}\frac{p_i-1}{2}}=(-1)^{\frac{p_1p_2\ldots p_r-1}{2}}=(-1)^{\frac{n-1}{2}}$. □

6. $\left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}$. Следовательно, $\left(\frac{2}{n}\right)=1$ при $n\equiv\pm1\pmod 8$; $\left(\frac{2}{n}\right)=-1$ при $n\equiv\pm3 \pmod 8$.

*Доказательство* [2]. Отметим, что для нечетных чисел $p_1$, $p_2$ выполняется сравнение

$$\frac{p_1^2p_2^2-1}{8}\equiv\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8} \pmod 2.$$

Действительно, каждое из чисел $p_1^2-1$ и $p_2^2-1$ делится на 4, то есть $(p_1^2-1)(p_2^2-1)\equiv 0 \pmod{16}$, поэтому $p_1^2p_2^2-1\equiv(p_1^2-1)+(p_2^2-1) \pmod{16}$. Поделив обе части сравнения и модуль на 8, получим требуемое соотношение. По индукции получаем

$$\sum_{i=1}^{r}\frac{p_i^2-1}{8}\equiv\frac{p_1^2p_2^2\ldots p_r^2-1}{8} \pmod 2.$$

Тогда $\left(\frac{2}{n}\right)=\prod_{i=1}^{r}\left(\frac{2}{p_i}\right)=\prod_{i=1}^{r}(-1)^{\frac{p_i^2-1}{8}}=(-1)^{\sum_{i=1}^{r}\frac{p_i^2-1}{8}}=(-1)^{\frac{p_1^2p_2^2\ldots p_r^2-1}{8}}=(-1)^{\frac{n^2-1}{8}}$. □

7. Для нечетных целых чисел $m$, $n$ справедливо равенство $\left(\frac{m}{n}\right)=(-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right)$.

*Доказательство* [2]. Если $m = p_1p_2\ldots p_r$, $n = q_1q_2\ldots q_s$, то с учетом свойства 4, определения символа Якоби и квадратичного закона взаимности имеем $\left(\frac{m}{n}\right) = (-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}\left(\frac{n}{m}\right)$. Сумму в показателе степени достаточно вычислить по модулю 2. Получаем

$$\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2} \equiv \frac{m-1}{2}\sum_{j=1}^{s}\frac{q_j-1}{2} \equiv \frac{m-1}{2}\cdot\frac{n-1}{2} \pmod 2,$$

то есть числа $\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}$ и $\frac{m-1}{2}\cdot\frac{n-1}{2}$ имеют одинаковую четность, и $(-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}} = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$. □

Из свойств символа Якоби следует, что если $n$ — нечетное целое число и $a = 2^k a_1$, где число $a_1$ нечетное, то

$$\left(\frac{a}{n}\right) = \left(\frac{2^k}{n}\right)\left(\frac{a_1}{m}\right) = \left(\frac{2}{n}\right)^k\left(\frac{n \pmod{a_1}}{a_1}\right)(-1)^{\frac{(a_1-1)(n-1)}{4}}.$$

Отсюда получаем алгоритм вычисления символа Якоби [4].

Алгоритм 2.1. Вычисление символа Якоби.

*Вход*. Нечетное целое число $n \geq 3$, целое число $a$, $0 \leq a < n$.

*Выход*. Символ Якоби $\left(\frac{a}{n}\right)$.

1. Положить $g \leftarrow 1$.
2. При $a = 0$ результат: 0.
3. При $a = 1$ результат: $g$.
4. Представить $a$ в виде $a = 2^k a_1$, где число $a_1$ нечетное.
5. При четном $k$ положить $s \leftarrow 1$. При нечетном $k$ положить $s \leftarrow 1$, если $n \equiv \pm 1 \pmod 8$; положить $s \leftarrow -1$, если $n \equiv \pm 3 \pmod 8$.
6. При $a_1 = 1$ результат: $g \cdot s$.

7. Если $n \equiv 3 \pmod 4$ и $a_1 \equiv 3 \pmod 4$, то $s \leftarrow -s$.

8. Положить $a \leftarrow n \pmod{a_1}$, $n \leftarrow a_1$, $g \leftarrow g \cdot s$ и вернуться на шаг 2. □

Сложность алгоритма равна $O(\log^2 n)$.

Пример 2.25. Вычислим символ Якоби $\left(\frac{532}{2739}\right)$. Полагаем $g = 1$.

Первая итерация. Находим представление числа $a$: $532 = 2^2 \cdot 133$, $a_1 = 133$. Число $k = 2$ четное, поэтому $s = 1$. Полагаем $a = 2739 \equiv 79 \pmod{133}$, $n = 133$, $g = 1 \cdot 1 = 1$.

Вторая итерация. Находим представление числа $a$: $79 = 2^0 \cdot 79$, $a_1 = 79$. Число $k = 0$ четное, поэтому $s = 1$. Полагаем $a = 133 \equiv 54 \pmod{79}$, $n = 79$, $g = 1 \cdot 1 = 1$.

Третья итерация. Находим представление числа $a$: $54 = 2^1 \cdot 27$, $a_1 = 27$. Число $k = 1$ нечетное и $n = 79 \equiv -1 \pmod 8$, поэтому $s = 1$. Кроме того, $n \equiv 3 \pmod 4$ и $a_1 \equiv 3 \pmod 4$, поэтому $s = -1$. Полагаем $a = 79 \equiv 25 \pmod{27}$, $n = 27$, $g = 1 \cdot (-1) = -1$.

Четвертая итерация. Находим представление числа $a$: $25 = 2^0 \cdot 25$, $a_1 = 25$. Число $k = 0$ четное, поэтому $s = 1$. Полагаем $a = 27 \equiv 2 \pmod{25}$, $n = 25$, $g = (-1) \cdot 1 = -1$.

Пятая итерация. Находим представление числа $a$: $2 = 2^1 \cdot 1$, $a_1 = 1$. Число $k = 1$ нечетное и $n \equiv 1 \pmod 8$, поэтому $s = 1$.

Поскольку $a_1 = 1$, алгоритм заканчивает работу на шаге 6 с результатом: $-1 \cdot 1 = -1$. □

### 2.3.2. Случаи простого модуля

Рассмотрим сравнение

$$x^2 \equiv a \pmod p, \tag{2.11}$$

где число $p \neq 2$ простое и целое число $a$ не делится на $p$.

Для того чтобы узнать, разрешимо ли сравнение, достаточно вычислить символ Лежандра $\left(\frac{a}{p}\right)$. При $\left(\frac{a}{p}\right) = -1$ сравнение (2.11) решений не имеет.

При $\left(\frac{a}{p}\right) = 1$ сравнение (2.11) разрешимо и имеет ровно два решения. Действительно, если $\left(\frac{a}{p}\right) = 1$, то по определению символа Лежандра сравнение (2.11) имеет хотя бы одно решение $x_1 \pmod p$. Пусть $x_2$ — другое решение сравнения (2.11). Тогда $x_1^2 \equiv a \pmod p$, $x_2^2 \equiv a \pmod p$, то есть $x_1^2 - x_2^2 \equiv 0 \pmod p$. Значит хотя бы одно из выражений $x_1 - x_2$, $x_1 + x_2$ должно делиться на $p$. В первом случае получаем уже имеющееся решение $x_1$, во втором случае — решение $x_2 \equiv -x_1 \pmod p$. При этом значения $x_1$ и $-x_1$ различны, в противном случае выполнялось бы соотношение $2x_1 \equiv 0 \pmod p$, что невозможно, поскольку $p \neq 2$ и НОД$(x_1, p)$ = НОД$(a, p)$ = 1. Кроме того, согласно теореме 2.8, сравнение (2.11) не может иметь более двух решений.

Рассмотрим некоторые способы решения сравнения (2.11) в зависимости от вида модуля.

Пусть $p \equiv 3 \pmod 4$, то есть $p = 4m + 3$, где $m \in \mathbb{Z}$. Разрешимость сравнения (2.11) означает, что $\left(\frac{a}{p}\right) = 1$. По свойству 3 символа Лежандра $1 = \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} = a^{2m+1} \pmod p$. Тогда

$$(a^{m+1})^2 = a^{2m+2} = a^{2m+1} \cdot a \equiv a \pmod p.$$

Таким образом, решение имеет вид $x \equiv \pm a^{m+1} \pmod p$.

Пример 2.26. Решим сравнение $x^2 \equiv 7 \pmod{31}$. Вычисляем символ Лежандра: $\left(\frac{7}{31}\right)=1$, значит, сравнение разрешимо. Число 31 представляем в виде $31 = 4 \cdot 7 + 3$, то есть $m = 7$. Находим решение: $x \equiv \pm 7^8 = \pm 7^3 7^3 7^2 \equiv \pm 2 \cdot 2 \cdot 18 \equiv \pm 10 \pmod{31}$.

Проверка: $(\pm 10)^2 - 7 = 100 - 7 = 93 = 31 \cdot 3$. □

Пусть $p \equiv 5 \pmod 8$, то есть $p = 8m + 5$, где $m \in \mathbb{Z}$. Разрешимость сравнения (2.11) означает, что $\left(\frac{a}{p}\right)=1$. По свойству 3 символа Лежандра $1=\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} = a^{4m+2} = (a^{2m+1})^2 \pmod p$. Отсюда $a^{2m+1} \equiv 1 \pmod p$ или $a^{2m+1} \equiv -1 \pmod p$. В первом случае, умножая обе части сравнения на $a$, получаем $a^{2m+2} \equiv a \pmod p$, то есть решение имеет вид $x \equiv \pm a^{m+1} \pmod p$.

При $a^{2m+1} \equiv -1 \pmod p$ ситуация немного сложнее. Заметим, что при $p \equiv 5 \pmod 8$ число 2 является квадратичным невычетом по модулю $p$. Действительно, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{64m^2+80m+24}{8}} = (-1)^{8m^2+10m+3} = -1$. По свойству 3 символа Лежандра $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} = 2^{4m+2} = (2^{2m+1})^2 \pmod p$. Таким образом, $(2^{2m+1})^2 \equiv -1 \pmod p$. Тогда

$$a^{2m+1} \cdot (2^{2m+1})^2 \equiv 1 \pmod p.$$

Умножая обе части этого сравнения на $a$, получаем решение сравнения (2.11): $x \equiv \pm a^{m+1} \cdot 2^{2m+1} \pmod p$.

Здесь вместо числа 2 можно брать любой другой квадратичный невычет по модулю $p$.

Пример 2.27. Решим сравнение $x^2 \equiv 10 \pmod{53}$. Вычисляем символ Лежандра: $\left(\frac{10}{53}\right)=1$, значит, сравнение разрешимо. Число 53 представляем в виде $53 = 8 \cdot 6 + 5$, то есть $m = 6$. Поскольку $10^{2\cdot 6+1} \equiv 1 \pmod{53}$, находим решение: $x \equiv \pm 10^7 \equiv \pm 13 \pmod{53}$.

Проверка: $(\pm 13)^2 - 10 = 169 - 10 = 159 = 53 \cdot 3$. □

Пример 2.28. Решим сравнение $x^2 \equiv 11 \pmod{37}$. Вычисляем символ Лежандра: $\left(\frac{11}{37}\right)=1$, значит, сравнение разрешимо. Число 37 представляем в виде $37 = 8 \cdot 4 + 5$, то есть $m = 4$. Поскольку $11^{2\cdot 4+1} \equiv -1 \pmod{37}$, находим решение: $x \equiv \pm 11^5 \cdot 2^9 \equiv \pm 14 \pmod{37}$.

Проверка: $(\pm 14)^2 - 11 = 196 - 11 = 185 = 37 \cdot 5$. □

Пусть $p \equiv 1 \pmod 8$. Представим $p$ в виде $p = 2^k \cdot h + 1$, где $k \geq 3$, число $h$ нечетное. Разрешимость сравнения (2.11) означает, что $\left(\frac{a}{p}\right)=1$. По свойству 3 символа Лежандра $1=\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} = a^{2^{k-1}\cdot h} \pmod p$. Отсюда $a^{2^{k-2}\cdot h} \equiv \pm 1 \pmod p$. Пусть $N$ — произвольный квадратичный невычет по модулю $p$, то есть $-1=\left(\frac{N}{p}\right) \equiv N^{2^{k-1}\cdot h} \pmod p$. Тогда при некотором целом $s_2 \geq 0$ получим $a^{2^{k-2}\cdot h} \cdot N^{2^{k-1}\cdot s_2} \equiv 1 \pmod p$, откуда $a^{2^{k-3}\cdot h} \cdot N^{2^{k-2}\cdot s_2} \equiv \pm 1 \pmod p$. Далее, при некотором целом $s_3 \geq 0$ получим $a^{2^{k-3}\cdot h} \cdot N^{2^{k-2}\cdot s_3} \equiv 1 \pmod p$, откуда $a^{2^{k-4}\cdot h} \cdot N^{2^{k-3}\cdot s_3} \equiv \pm 1 \pmod p$ и т. д. Получив сравнение $a^h \cdot N^{2s_k} \equiv 1 \pmod p$ для некоторого целого $s_k \geq 0$ и умножив обе его части на $a$, получаем решение $x \equiv \pm a^{\frac{h+1}{2}} \cdot N^{s_k} \pmod p$.

Алгоритм 2.2. Решение сравнения второй степени по модулю простого числа [4].

*Вход*. Простое число $p \neq 2$; такие целые числа $a$ и $N$, что $\left(\frac{a}{p}\right) = -\left(\frac{N}{p}\right) = 1$.

*Выход*. Решение сравнения $x^2 \equiv a \pmod p$.

1. Представить число $p$ в виде $p = 2^k \cdot h + 1$, где число $h$ нечетное.
2. Положить $a_1 \leftarrow a^{\frac{h+1}{2}} \pmod p$, $a_2 \leftarrow a^{-1} \pmod p$, $N_1 \leftarrow N^h \pmod p$, $N_2 \leftarrow 1, j \leftarrow 0$.
3. Для $i = 0, 1, \ldots, k-2$ выполнять следующие действия.
   3.1. Положить $b \leftarrow a_1 N_2 \pmod p$.
   3.2. Вычислить $c \leftarrow a_2 b^2 \pmod p$.
   3.3. Вычислить абсолютно наименьший вычет $d \leftarrow c^{2^{k-2-i}} \pmod p$. При $d = 1$ положить $j_i \leftarrow 0$, при $d = -1$ положить $j_i \leftarrow 1$.
   3.4. Положить $N_2 \leftarrow N_2 N_1^{2^i j_i} \pmod p$.
4. Результат: $\pm a_1 N_2 \pmod p$. □

Сложность этого алгоритма равна $O(\log^4 p)$.

Пример 2.29. Решим сравнение $x^2 \equiv 14 \pmod{193}$. Вычисляем символ Лежандра: $\left(\frac{14}{193}\right) = 1$, значит, сравнение разрешимо. Выбираем $N = 5$, $\left(\frac{5}{193}\right) = -1$. Находим представление $193 = 2^6 \cdot 3 + 1$, то есть $k = 6$, $h = 3$.

Полагаем $a_1 = 14^2 \equiv 3 \pmod{193}$, $a_2 = 14^{-1} \equiv 69 \pmod{193}$, $N_1 = 5^3 \equiv 125 \pmod{193}$, $N_2 = 1, j = 0$.

Результаты вычислений сведем в таблицу:

| $i$ | $b \equiv a_1 N_2$ | $c \equiv a_2 b^2$ | $d \equiv c^{2^{4-i}}$ | $j_i$ | $N_2$ |
|---|---|---|---|---|---|
| 0 | 3 | 42 | −1 | 1 | 125 |
| 1 | 182 | 50 | −1 | 1 | 158 |
| 2 | 88 | 112 | 1 | 0 | 158 |
| 3 | 88 | 112 | −1 | 1 | 39 |
| 4 | 117 | 192 | −1 | 1 | 122 |

Тогда решением сравнения будет $x = \pm 3 \cdot 122 \equiv \pm 173 \pmod{193}$.

Проверка: $(\pm 173)^2 - 14 = 29929 - 14 = 29915 = 193 \cdot 155$. □

### 2.3.3. Случаи составного модуля

Теорема 2.11. Пусть число $p$ простое, $p \neq 2$, целое число $a$ не делится на $p$ и $n \in \mathbb{N}$, $n \geq 1$. Для того чтобы сравнение

$$x^2 \equiv a \pmod{p^n} \tag{2.12}$$

было разрешимо, необходимо и достаточно, чтобы было разрешимо сравнение

$$x^2 \equiv a \pmod{p}. \tag{2.13}$$

*Доказательство*. Если сравнение (2.12) разрешимо и $x_n \in \mathbb{Z}$ — его решение, то есть $x_n^2 \equiv a \pmod{p^n}$, то разность $x_n^2 - a$ делится на $p^n$, а значит и на $p$, и $x_n$ является решением сравнения (2.13).

Пусть теперь разрешимо сравнение (2.13) и $x \equiv x_1 \pmod{p}$ — его решение. Тогда $x = x_1 + pk_1$ для некоторого целого $k_1$. Подставляя это значение $x$ в сравнение $x^2 \equiv a \pmod{p^2}$, получаем

$$x_1^2 + 2x_1 p k_1 \equiv a \pmod{p^2},$$

а так как разность $x_1^2 - a$ делится на $p$, получаем

$$2x_1 k_1 \equiv \frac{-(x_1^2 - a)}{p} \pmod{p}. \tag{2.14}$$

Числа $a$ и $p$ взаимно просты, поэтому числа $x_1$ и $p$ тоже взаимно просты; кроме того, $p \neq 2$. Поэтому НОД$(2x_1, p) = 1$, то есть целое число $\dfrac{x_1^2 - a}{p}$ делится на НОД$(2x_1, p)$ и по теореме 2.5 сравнение (2.14) имеет единственное решение $k_1 \equiv k_1' \pmod p$, $k_1 = k_1' + pk_2$ для некоторого целого $k_2$. Тогда $x = x_1 + pk_1 = x_1 + pk_1' + p^2k_2 = x_2 + p^2k_2$. Подставляя это значение в сравнение $x^2 \equiv a \pmod{p^3}$, получаем

$$x_2^2 + 2x_2p^2k_2 \equiv a \pmod{p^3},$$

$$2x_2k_2 \equiv \frac{-(x_2^2 - a)}{p^2} \pmod p. \qquad (2.15)$$

Здесь НОД$(x_2, p) =$ НОД$(x_1 + pk_1', p) =$ НОД$(x_1, p) = 1$, поэтому сравнение (2.15) имеет единственное решение $k_2 \equiv k_2' \pmod p$, $k_2 = k_2' + pk_3$ для некоторого целого $k_3$. Тогда

$$x = x_2 + p^2k_2 = x_2 + p^2k_2' + p^3k_3 = x_3 + p^3k_3.$$

Продолжая аналогичные рассуждения, получаем решение $x \equiv x_n \pmod{p^n}$ сравнения (2.12), где $x_n \equiv x_1 \pmod p$.

Второе решение сравнения (2.12) имеет вид $-x_n \equiv -x_1 \pmod p$. □

Покажем, что теоремой 2.11 определяются все решения сравнения (2.12).

Определение 2.8. *Порядком* числа $a$, $1 \le a < m$, НОД$(a, m) = 1$, по модулю $m$ называется наименьшее натуральное число $d$, для которого $a^d \equiv 1 \pmod m$.

Определение 2.9. Число $a$, $1 \le a < m$, порядка $\varphi(m)$ по модулю $m$ называется *первообразным корнем по модулю m*.

Лемма 2.12. Для числа $a$, имеющего порядок $d$ по модулю $m$, сравнение $a^{\gamma_1} \equiv a^{\gamma_2} \pmod m$ выполняется тогда и только тогда, когда $\gamma_1 \equiv \gamma_2 \pmod d$.

*Доказательство* [2]. Разделим $\gamma_1$ и $\gamma_2$ с остатком на $d$: $\gamma_1 = dq_1 + r_1$, $\gamma_2 = dq_2 + r_2$ для некоторых целых $q_1$, $q_2$, $r_1$, $r_2$. Тогда, с учетом того, что $a^d \equiv 1 \pmod m$, получаем

$$a^{\gamma_1} \equiv a^{dq_1+r_1} \equiv a^{r_1} \pmod m, \quad a^{\gamma_2} \equiv a^{dq_2+r_2} \equiv a^{r_2} \pmod m,$$

то есть $a^{\gamma_1} \equiv a^{\gamma_2} \pmod m$ равносильно сравнению $a^{r_1} \equiv a^{r_2} \pmod m$. Тогда $a^{r_1-r_2} \equiv 1 \pmod m$. Из условия $0 \le r_1, r_2 < d$ и определения порядка получаем, что $r_1 = r_2$, а значит, $\gamma_1 = dq_1 + r_2 = \gamma_2 - dq_2 \equiv \gamma_2 \pmod d$. □

Лемма 2.13. Если число $a$ имеет порядок $d_1d_2$ по модулю $m$, то число $a^{d_1}$ имеет порядок $d_2$ по модулю $m$.

*Доказательство* [2]. Пусть $\delta$ — порядок числа $a^{d_1}$ по модулю $m$. Тогда $(a^{d_1})^\delta \equiv 1 \pmod m$. По лемме 2.12 $d_1\delta$ делится на $d_1d_2$ и $\delta$ делится на $d_2$.

Так как $d_1d_2$ — порядок числа $a$, выполняется сравнение $1 \equiv a^{d_1d_2} \equiv (a^{d_1})^{d_2} \pmod m$, значит, по лемме 2.12 $d_2$ делится на $\delta$. Поэтому $d_2 = \delta$. □

Лемма 2.14. Если числа $a_1$, $a_2$ имеют по модулю $m$ порядки $d_1$, $d_2$ соответственно, причем НОД$(d_1, d_2) = 1$, то число $a_1a_2$ имеет по модулю $m$ порядок $d_1d_2$.

*Доказательство* [2]. Пусть $\delta$ — порядок числа $a_1a_2$ по модулю $m$. Тогда $(a_1a_2)^\delta \equiv 1 \pmod m$. Возводя обе части этого сравнения в степень $d_1$ и учитывая, что $a_1^{d_1} \equiv 1 \pmod m$, получаем $a_1^{d_1\delta}a_2^{d_1\delta} \equiv a_2^{d_1\delta} \equiv 1 \pmod m$. Согласно лемме 2.12, произведение $d_1\delta$ делится на $d_2$, а так как НОД$(d_1, d_2) = 1$, получаем, что $\delta$ делится на $d_2$. Аналогично получаем, что $\delta$ делится на $d_1$. А так как $\delta$ делится на взаимно простые числа $d_1$ и

$d_2$, значит, $\delta$ делится и на их произведение $d_1d_2$ (см. п. 1.2, свойство 6 взаимно простых чисел).

Возводя сравнения $a_1^{d_1} \equiv 1 \pmod m$, $a_2^{d_2} \equiv 1 \pmod m$ в степени $d_2$, $d_1$ соответственно и перемножая их, получаем $(a_1a_2)^{d_1d_2} \equiv 1 \pmod m$. Но $\delta$ — наименьшее такое число, что $(a_1a_2)^{\delta} \equiv 1 \pmod m$. Следовательно, $d_1d_2$ делится на $\delta$. Поэтому $\delta = d_1d_2$. □

Теорема 2.15. Для любого простого $p \neq 2$ существует первообразный корень по модулю $p$.

*Доказательство* [2]. Пусть $d_1, d_2, \ldots, d_r$ — все различные порядки по модулю $p$ чисел $1, 2, \ldots, p-1$. Обозначим $M = \text{НОК}(d_1, d_2, \ldots, d_r)$ и найдем каноническое разложение числа $M$:

$$M = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s}.$$

Каждое из чисел $q_i^{\alpha_i}$ является делителем хотя бы одного $d_j$, то есть $d_j = cq_i^{\alpha_i}$ для некоторого целого числа $c$. Пусть число $a_j$, $1 \le a_j \le p-1$, имеет порядок $d_j$. Тогда по лемме 2.13 число $b_j = a_j^c$ имеет порядок $q_i^{\alpha_i}$, а по лемме 2.14 число $g = b_1b_2\ldots b_s$ имеет порядок $q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_s^{\alpha_s} = M$. Согласно малой теореме Ферма, $g^{p-1} \equiv 1 \pmod p$, значит, $p-1$ делится на $M$.

Из сравнения $a_j^{d_j} \equiv 1 \pmod p$ и того, что $M$ делится на $d_j$, следует, что $a_j$ является решением сравнения $x^M \equiv 1 \pmod p$, то есть корнями полинома $x^M - 1$ по модулю $p$ являются все числа $1, 2, \ldots, p-1$. Из теоремы 2.8 получаем $p-1 \le M$, значит, $p-1 = M$ и $g$ — первообразный корень по модулю $p$. □

Пример 2.30. Число 2 является первообразным корнем по модулю 13, поскольку $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16 \equiv 3 \pmod{13}$, $2^5 \equiv 6$

(mod 13), $2^6 \equiv 12 \pmod{13}$, $2^7 \equiv 11 \pmod{13}$, $2^8 \equiv 9 \pmod{13}$, $2^9 \equiv 5 \pmod{13}$, $2^{10} \equiv 10 \pmod{13}$, $2^{11} \equiv 7 \pmod{13}$, $2^{12} \equiv 1 \pmod{13}$ и $\varphi(13) = 12$.□

Теорема 2.16. Для любого простого $p \neq 2$ существует первообразный корень по модулю $p^2$.

*Доказательство* [2]. По теореме 2.15 существует первообразный корень $g$ по модулю $p$. Кроме того, если $g$ — первообразный корень по модулю $p$, то $g + p$ — тоже первообразный корень по модулю $p$ и выполняется хотя бы одно из сравнений

$$g^{p-1} \quad 1 \pmod{p^2} \tag{2.16}$$

или

$$(g+p)^{p-1} \quad 1 \pmod{p^2}. \tag{2.17}$$

Действительно, если $g^{p-1} \equiv 1 \pmod{p^2}$, то

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \equiv 1 + (p-1)g^{p-2}p \quad 1 \pmod{p^2}.$$

Положим $g_1 = g$ (если выполняется сравнение (2.16)) или $g_1 = g + p$ (если выполняется сравнение (2.17)) и покажем, что число $g_1$ является первообразным корнем по модулю $p^2$. Запишем $g_1^{p-1} = 1 + zp$ для некоторого целого $z$, не делящегося на $p$. Пусть $d$ — порядок числа $g_1$ по модулю $p^2$, тогда, возводя сравнение $g_1^d \equiv 1 \pmod{p^2}$ в степень $p - 1$, получаем

$$1 \equiv (g_1^d)^{p-1} = (g_1^{p-1})^d = (1+zp)^d \pmod{p^2}.$$

Число $1 + zp$ имеет порядок $p$ по модулю $p^2$, поэтому $d$ делится на $p$ по лемме 2.12, то есть существует такое $t \in \mathbb{Z}$, что $d = pt$. Тогда

$$g_1^d = g_1^{pt} = (g_1^p)^t \equiv g_1^t \pmod{p},$$

поскольку $g_1$ — первообразный корень по модулю $p$. Из условия $g_1^d \equiv 1 \pmod{p^2}$ следует, что $g_1^d \equiv 1 \pmod{p}$, значит, и $g_1^t \equiv 1 \pmod{p}$. А

так как $g_1$ — первообразный корень по модулю $p$, получаем, что $t$ делится на $p-1$, $t=(p-1)c$, где $c \in \mathbb{Z}$, и $d=p(p-1)c$. Но $p(p-1)=\varphi(p^2)$, значит, $g_1$ — первообразный корень по модулю $p^2$. □

Пример 2.31. Число 3 является первообразным корнем по модулю 7 и $3^6=729 \equiv 43 \quad 1 \pmod{7^2}$. Значит, согласно доказательству теоремы 2.16, число 3 является первообразным корнем по модулю $7^2$. Проверяем: $3^1=3$, $3^2=9$, $3^3=27$, $3^4 \equiv 32 \pmod{7^2}$, ..., $3^{21} \equiv 48 \equiv -1 \pmod{7^2}$, ..., $3^{39} \equiv 20 \pmod{7^2}$, $3^{40} \equiv 11 \pmod{7^2}$, $3^{41} \equiv 33 \pmod{7^2}$, $3^{42} \equiv 1 \pmod{7^2}$. □

Теорема 2.17. Если сравнение (2.12) разрешимо, то оно имеет ровно два решения.

*Доказательство* [2]. Согласно теореме 2.15, существует первообразный корень $g$ по модулю $p$. Числа $1, g, g^2, \ldots, g^{p-1}$ пробегают все множество $\{1, 2, \ldots, p-1\}$, поэтому существуют такие целые числа $u$, $v$, что $a \equiv g^u \pmod{p^n}$, $x \equiv g^v \pmod{p^n}$. Тогда сравнение (2.12) равносильно сравнению $g^{2v} \equiv g^u \pmod{p^n}$. Последнее сравнение равносильно сравнению

$$2v \equiv u \pmod{p^n - p^{n-1}}. \tag{2.16}$$

Согласно теоремам 2.4, 2.5, это сравнение разрешимо тогда и только тогда, когда $u$ делится на НОД$(2, p^n - p^{n-1}) = 2$, и в случае разрешимости имеет ровно два решения.

Таким образом, сравнения (2.12) и (2.16) разрешимы или нет одновременно, и в случае разрешимости имеют ровно по два решения. □

Следствие. Число квадратичных вычетов по модулю $p^n$, где $p$ — простое число, $p \neq 2$, равно числу квадратичных невычетов по модулю $p^n$.

Пример 2.32. Решим сравнение $x^2 \equiv 3 \pmod{11^3}$. Оно разрешимо, поскольку $\left(\frac{3}{11}\right)=1$ и сравнение $x^2 \equiv 3 \pmod{11}$ разрешимо. Поскольку $11 \equiv 3 \pmod 4$, находим решение сравнения $x^2 \equiv 3 \pmod{11}$ как $x \equiv 3^{2+1} = 27 \equiv 5 \pmod{11}$, то есть $x = 5 + 11k_1$. Вычисляем: $x^2 = 25 + 2 \cdot 5 \cdot 11k_1 \equiv 3 \pmod{11^2}$. Отсюда

$$2 \cdot 5 \cdot 11k_1 \equiv -22 \pmod{11^2},$$

$$2 \cdot 5 \cdot k_1 \equiv -2 \pmod{11},$$

$$k_1 \equiv -2 \cdot (2 \cdot 5)^{-1} \equiv -2 \cdot (-1)^{-1} \equiv -2 \cdot (-1) = 2 \pmod{11},$$

то есть $k_1 = 2 + 11k_2$, $x = 5 + 11 \cdot 2 + 11^2k_2 = 27 + 11^2k_2$.

Ищем коэффициент $k_2$. Возводим $x$ в квадрат по модулю $11^3$: $x^2 = 27^2 + 2 \cdot 27 \cdot 11^2k_2 \equiv 3 \pmod{11^3}$. Отсюда

$$2 \cdot 27 \cdot 11^2k_2 \equiv -726 \pmod{11^3},$$

$$2 \cdot 27 \cdot k_2 \equiv -6 \pmod{11},$$

$$k_2 \equiv -6 \cdot (2 \cdot 27)^{-1} \equiv -6 \cdot (-1)^{-1} \equiv -6 \cdot (-1) = 6 \pmod{11},$$

то есть $k_2 = 6 + 11k_3$, $x_3 = 27 + 11^2 \cdot 6 + 11^3k_3 \equiv 753 \pmod{11^3}$.

Второе решение: $-753 \equiv 578 \pmod{11^3}$. Это же решение получается, если строить $x_3$ из начального значения $x \equiv 6 \pmod{11}$ — второго решения сравнения $x^2 \equiv 3 \pmod{11}$.

Проверка:

$753^2 - 3 = 567006 = 11^3 \cdot 426$, $578^2 - 3 = 334081 = 11^3 \cdot 251$. □

Теорема 2.18. Пусть число $a$ нечетное. Справедливы следующие утверждения.

1. Сравнение $x^2 \equiv a \pmod 2$ разрешимо при любом $a$.

2. Сравнение $x^2 \equiv a \pmod{2^2}$ разрешимо тогда и только тогда, когда $a \equiv 1 \pmod 4$.

3. Сравнение $x^2 \equiv a \pmod{2^n}$, где $n \geq 3$, разрешимо тогда и только тогда, когда $a \equiv 1 \pmod 8$.

*Доказательство* [2]. Если число $a$ нечетное, то $a \equiv 1 \pmod 2$, и сравнение из п. 1 имеет вид $x^2 \equiv 1 \pmod 2$. Это сравнение имеет единственное решение $x \equiv 1 \pmod 2$.

Если $a \equiv 1 \pmod 4$, то есть $a = 4k + 1$, то сравнение вида $x^2 \equiv 4k + 1 \equiv 1 \pmod 4$ имеет два решения: $x \equiv \pm 1 \pmod 4$. Обратно, пусть $c$ — решение сравнения $x^2 \equiv a \pmod 4$. Нечетное число $a$ имеет вид $a = 2k + 1$, где $k \in \mathbb{Z}$. Кроме того, так как число $a$ нечетное, то $c$ тоже нечетное, $c = 2l + 1$. Отсюда

$$(2l + 1)^2 \equiv 2k + 1 \pmod 4,$$

$$0 \equiv 2k \pmod 4,$$

то есть $k \equiv 0 \pmod 2$, и $a \equiv 1 \pmod 4$.

Осталось рассмотреть случай $n \geq 3$. Здесь решение тоже будет нечетным числом. Пусть $c = 2l + 1$ — решение сравнения. Аналогично предыдущему случаю получаем $a \equiv 1 \pmod 4$, то есть $a = 4k + 1$, где $k \in \mathbb{Z}$. Тогда

$$(2l + 1)^2 \equiv 4k + 1 \pmod{2^n},$$

$$4l^2 + 4l \equiv 4k \pmod{2^n},$$

$$l(l + 1) \equiv k \pmod{2^{n-2}},$$

где $n \geq 3$. Произведение в левой части сравнения является четным числом, тогда и число $k$ четное, и $a \equiv 1 \pmod 8$.

Пусть теперь $a = 8k + 1$. При $n = 3$ решениями сравнения $x^2 \equiv a \pmod 8$ будут $x \equiv \pm 1$ и $x \equiv \pm 3 \pmod 8$. Найдем решения сравнения $x^2 \equiv a \pmod{2^n}$ для $n \geq 4$. Решение этого сравнения — нечетное число, то есть сравнимо с 1 или с 3 по модулю 4 и имеет вид $x = \pm(1 + 4t_3)$, где $t_3 \in \mathbb{Z}$. Тогда

$$(1 + 4t_3)^2 \equiv 8k + 1 \pmod{2^n},$$

$$8t_3 + 16t_3^2 \equiv 8k \pmod{2^n},$$

в частности,

$$8t_3 \equiv 8k \pmod{2^4},$$

$$t_3 \equiv k \pmod 2,$$

то есть $t_3 = t_3' + 2t_4$ для $t_3' \in \{0, 1\}$, $t_4 \in \mathbb{Z}$, и $x = \pm(1 + 4t_3' + 8t_4) = \pm(x_4 + 8t_4)$. Рассматривая сравнение по модулю $2^5$, получаем

$$(x_4 + 8t_4)^2 \equiv 8k + 1 \pmod{2^5},$$

$$16k^2 + 16t_4 \equiv 0 \pmod{2^5},$$

$$t_4 \equiv k^2 \pmod 2,$$

то есть $t_4 = t_4' + 2t_5$ для $t_4' \in \{0, 1\}$, $t_5 \in \mathbb{Z}$, и $x = \pm(1 + 4t_3' + 8t_4' + 16t_5) = \pm(x_5 + 16t_5)$. Продолжаем, пока не получим

$$x = \pm(x_n + 2^{n-1}t_n),$$

где $t_n \in \mathbb{Z}$. Целые числа с четным значением $t_n$ дают два решения: $x \equiv \pm x_n \pmod{2^n}$, целые числа с нечетным значением $t_n$ — еще два решения: $x \equiv \pm(x_n + 2^{n-1}) \pmod{2^n}$. При этом $x_n \equiv x_n + 2^{n-1} \equiv 1 \pmod 4$, $-x_n \equiv -(x_n + 2^{n-1}) \equiv 3 \pmod 4$. □

Пример 2.33. Решим сравнение $x^2 \equiv 41 \pmod{64}$, то есть $n = 6$. Поскольку $41 \equiv 1 \pmod 8$, сравнение разрешимо. Представляем решение в виде $x = \pm(1 + 4t_3)$. Тогда

$$(1 + 4t_3)^2 \equiv 41 \pmod{2^4},$$

$$2 \cdot 4t_3 \equiv 40 \pmod{2^4},$$

$$t_3 \equiv 1 \pmod 2,$$

то есть $t_3 = 1 + 2t_4$ и $x = \pm(5 + 8t_4)$.

Далее,

$$(5 + 8t_4)^2 \equiv 41 \pmod{2^5},$$

$$2 \cdot 5 \cdot 8t_4 \equiv -16 \pmod{2^5},$$

$$t_4 \equiv 1 \pmod 2,\ t_4 = 1 + 2t_5,\ x = \pm(13 + 16t_5);$$

$$(13 + 16t_5)^2 \equiv 41 \pmod{2^5},$$

$$2 \cdot 13 \cdot 16t_5 \equiv -128 \pmod{2^5},$$

$$t_5 \equiv 0 \pmod 2,\ t_5 = 2t_6,\ x = \pm(13 + 32t_6).$$

Отсюда получаем четыре решения: $x \equiv \pm 13$, $x \equiv \pm 45 \pmod{64}$.

Проверка: $(\pm 13)^2 - 41 = 169 - 41 = 128 = 64 \cdot 2$; $(\pm 45)^2 - 41 = 2025 - 41 = 1984 = 64 \cdot 31$. □

Теорема 2.19. Пусть $m = m_1 m_2 \ldots m_r$, где числа $m_1, m_2, \ldots, m_r$ попарно взаимно просты. Для того чтобы сравнение (2.7) было разрешимо, необходимо и достаточно, чтобы были разрешимы все сравнения $x^2 \equiv a \pmod{m_1}$, $x^2 \equiv a \pmod{m_2}$, …, $x^2 \equiv a \pmod{m_r}$.

*Доказательство.* Если $c$ — решение сравнения (2.7), то разность $c^2 - a$ делится на произведение $m_1 m_2 \ldots m_r$, а значит, и на каждое из чисел $m_1, m_2, \ldots, m_r$.

Пусть теперь $u_1, u_2, \ldots, u_r$ — решения сравнений по соответствующим модулям, то есть $u_i^2 \equiv a \pmod{m_i}$ для $i = 1, 2, \ldots, r$. Числа $m_1, m_2, \ldots, m_r$ попарно взаимно просты, значит, по китайской теореме об остатках, существует такое целое число $u$, что $u \equiv u_i \pmod{m_i}$ для всех $i = 1, 2, \ldots, r$. Тогда $u^2 \equiv u_i^2 \equiv a \pmod{m_i}$ для всех $i = 1, 2, \ldots, r$, то есть разность $u^2 - a$ делится на каждое из чисел $m_1, m_2, \ldots, m_r$, а значит, по свойству 7 наибольшего общего делителя, и на произведение $m_1 m_2 \ldots m_r = m$. □

Пример 2.34. Сравнение $x^2 \equiv 13 \pmod{35}$ не имеет решений, хотя

$$\left(\frac{13}{35}\right)=(-1)^{\frac{13-1}{2}\cdot\frac{35-1}{2}}\left(\frac{35}{13}\right)=(-1)^{6\cdot 17}\left(\frac{9}{13}\right)=\left(\frac{9}{13}\right)=\left(\frac{3^2}{13}\right)=\left(\frac{1}{13}\right)=1.$$

Представим этот символ Якоби в виде $\left(\frac{13}{35}\right)=\left(\frac{13}{5}\right)\left(\frac{13}{7}\right)$. Вычисляя символы Лежандра в правой части равенства, получаем

$$\left(\frac{13}{5}\right)=\left(\frac{3}{5}\right)=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)=-1,$$

$$\left(\frac{13}{7}\right)=\left(\frac{6}{7}\right)=\left(\frac{2}{7}\right)\left(\frac{3}{7}\right)=1\cdot(-1)\left(\frac{7}{3}\right)=-\left(\frac{7}{3}\right)=-1\cdot 1=-1,$$

то есть число 13 является квадратичным невычетом по модулям 5 и 7. □

Следствие 1. Пусть $m=2^n p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_s^{\alpha_s}$ — каноническое разложение целого числа $m$ и целое число $a$ взаимно просто с $m$. Сравнение $x^2\equiv a \pmod m$ разрешимо тогда и только тогда, когда $a\equiv 1 \pmod 4$ при $n=2$, $a\equiv 1 \pmod 8$ при $n\geq 3$ и $\left(\frac{a}{p_1}\right)=\left(\frac{a}{p_2}\right)=\ldots=\left(\frac{a}{p_s}\right)=1$. Это сравнение имеет $2^s$ решений при $n=0$ или $n=1$; $2^{s+1}$ решений при $n=2$; $2^{s+2}$ решений при $n\geq 3$.

Следствие 2. Если целое число $m$ имеет хотя бы два взаимно простых делителя, то число квадратичных вычетов по модулю $m$ строго меньше, чем число квадратичных невычетов. Для заданного нечетного числа $m=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_s^{\alpha_s}$ произвольное наугад взятое число $a$, взаимно простое с $m$, будет квадратичным вычетом с вероятностью $\frac{1}{2^s}$.

*Доказательство* следует из свойства 7 символа Лежандра, согласно которому для каждого из чисел $p_1, p_2, \ldots, p_s$ число $a$ будет квадратичным вычетом с вероятностью $\frac{1}{2}$. □

Пример 2.35. Решим сравнение $x^2\equiv 1033 \pmod{2^4\cdot 3^3\cdot 19}$.

Это сравнение разрешимо, поскольку $1033 \equiv 1 \pmod 8$ и выполняются равенства для символов Лежандра $\left(\frac{1033}{3}\right)=\left(\frac{1033}{19}\right)=1$.

В обозначениях следствия 1 $s=2$, $n=4$, значит, сравнение имеет $2^{2+2}=16$ решений.

Решаем сравнение по модулю 19: $x^2 \equiv 1033 \equiv 7 \pmod{19}$. Так как $19 \equiv 3 \pmod 4$, по способу п. 2.3.2 решением будет $x \equiv \pm 7^5 \equiv \pm 8 \pmod{19}$.

Решаем сравнение по модулю $3^3$: $x^2 \equiv 1033 \equiv 7 \pmod{3^3}$. Ищем решение в виде $x_0 + 3k_1 + 9k_2$. Находим $x_0 \equiv 1 \pmod 3$ — решение сравнения $x^2 \equiv 7 \equiv 1 \pmod 3$. Далее, $(1+3k_1)^2 \equiv 1 + 6k_1 \equiv 7 \pmod{3^2}$, $k_1 \equiv 1 \pmod 3$; $(4+9k_2)^2 \equiv 16 + 72k_2 \equiv 7 \pmod{3^3}$, $k_2 \equiv 1 \pmod 3$. Таким образом, нашли решение $x \equiv \pm 13 \pmod{3^3}$.

Решаем сравнение по модулю $2^4$: $x^2 \equiv 1033 \equiv 9 \pmod{2^4}$. Отсюда очевидные решения: $x \equiv \pm 3 \pmod{2^4}$, $x \equiv \pm 5 \pmod{2^4}$.

Восстанавливаем решения исходного сравнения по китайской теореме об остатках. Решаем систему $x \equiv 8 \pmod{19}$, $x \equiv 13 \pmod{3^3}$, $x \equiv 3 \pmod{2^4}$:

$$x \equiv 8 \cdot 3^3 \cdot 2^4 \cdot (3^{-3} \cdot 2^{-4} \pmod{19}) + 13 \cdot 19 \cdot 2^4 \cdot (19^{-1} \cdot 2^{-4} \pmod{3^3}) +$$

$$+ 3 \cdot 19 \cdot 3^3 \cdot (19^{-1} \cdot 3^{-3} \pmod{2^4}) \equiv 3456 \cdot 15 + 3952 \cdot 4 + 1539 \cdot 1 \equiv$$

$$\equiv 3523 \pmod{2^4 \cdot 3^3 \cdot 19}.$$

Аналогично находим еще семь решений:

| $x \pmod{19}$ | $x \pmod{3^3}$ | $x \pmod{2^4}$ | $x \pmod{2^4 \cdot 3^3 \cdot 19}$ |
|---|---|---|---|
| 8 | 13 | 5 | 4549 |
| 8 | −13 | 3 | 4739 |
| 8 | −13 | 5 | 5765 |
| −8 | 13 | 3 | 6547 |
| −8 | 13 | 5 | 7573 |

| $x \pmod{19}$ | $x \pmod{3^3}$ | $x \pmod{2^4}$ | $x \pmod{2^4 \cdot 3^3 \cdot 19}$ |
|---|---|---|---|
| $-8$ | $-13$ | $3$ | $7763$ |
| $-8$ | $-13$ | $5$ | $581$ |

Остальные восемь решений противоположны найденным по знаку.

Итак, окончательный результат: $x \equiv \pm 445, 581, \pm 635, \pm 1661, \pm 2443, \pm 3469, \pm 3523, \pm 3659 \pmod{2^4 \cdot 3^3 \cdot 19}$.

Проверка:

$(\pm 445)^2 - 1033 = 196992 = 2^4 \cdot 3^3 \cdot 19 \cdot 24,$

$(\pm 581)^2 - 1033 = 336528 = 2^4 \cdot 3^3 \cdot 19 \cdot 41,$

$(\pm 635)^2 - 1033 = 402192 = 2^4 \cdot 3^3 \cdot 19 \cdot 49,$

$(\pm 1661)^2 - 1033 = 2757888 = 2^4 \cdot 3^3 \cdot 19 \cdot 336,$

$(\pm 2443)^2 - 1033 = 5967216 = 2^4 \cdot 3^3 \cdot 19 \cdot 727,$

$(\pm 3469)^2 - 1033 = 12032928 = 2^4 \cdot 3^3 \cdot 19 \cdot 1466,$

$(\pm 3523)^2 - 1033 = 12410496 = 2^4 \cdot 3^3 \cdot 19 \cdot 1512,$

$(\pm 3659)^2 - 1033 = 13387248 = 2^4 \cdot 3^3 \cdot 19 \cdot 1631.$ □

## Упражнения к главе 2

1. Образуют ли числа $2^0, 2^1, \ldots, 2^{12}$ полную систему вычетов по модулю 13?

2. Представляя целое число в системе счисления с основанием 100, вывести признак делимости на 101.

3. Вычислить функцию Эйлера: а) $\varphi(7^3)$; б) $\varphi(8!)$; в) $\varphi(240240)$.

4. Решить сравнение: а) $13x \equiv 10 \pmod{15}$; б) $16x \equiv 7 \pmod{26}$; в) $12x \equiv 18 \pmod{22}$; г) $12x \equiv 8 \pmod{24}$.

5. Доказать, что уравнение $3x^2 + 2 = y^2$ неразрешимо в целых числах.

6. Используя китайскую теорему об остатках, решить систему сравнений: а) $x \equiv 3 \pmod 5$, $x \equiv 1 \pmod 7$, $x \equiv 4 \pmod 9$; б) $x \equiv 2 \pmod 5$,

$x \equiv 3 \pmod{11}$, $x \equiv 4 \pmod{17}$; в) $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 4 \pmod 5$, $x \equiv 3 \pmod 7$; г) $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 4$, $x \equiv 6 \pmod 7$, $x \equiv 5 \pmod{11}$.

7. Составить таблицу всех квадратичных вычетов и невычетов по модулю 7, 11, 13, 17.

8. Вычислить символы Лежандра $\left(\frac{401}{757}\right), \left(\frac{215}{761}\right), \left(\frac{113}{997}\right), \left(\frac{514}{1093}\right)$.

9. Доказать, что число 3 является квадратичным вычетом по модулю любого простого числа вида $2^p - 1$, где $p$ — простое, $p \geq 3$.

10. Используя квадратичный закон взаимности, найти простые числа $p$, по модулю которых а) число 7 является квадратичным вычетом; б) число 15 является квадратичным вычетом.

11. Пусть число $p \neq 2$ простое, числа $a$, $b$, $c$ целые, и $a$ не делится на $p$. Доказать, что а) число решений сравнения $x^2 \equiv b \pmod p$ равно $1 + \left(\frac{b}{p}\right)$; б) число решений сравнения $ax^2 + bx + c \equiv 0 \pmod p$ равно $1 + \left(\frac{b^2 - 4ac}{p}\right)$.

12. Используя лемму Гаусса, вычислить символы Лежандра $\left(\frac{5}{7}\right), \left(\frac{3}{11}\right), \left(\frac{6}{13}\right), \left(\frac{-1}{p}\right)$.

13. Решить сравнение: а) $x^2 \equiv 7 \pmod{19}$; б) $x^2 \equiv 6 \pmod{23}$; в) $x^2 \equiv 14 \pmod{31}$.

14. Решить сравнение: а) $x^2 \equiv 7 \pmod{37}$; б) $x^2 \equiv 13 \pmod{53}$; в) $x^2 \equiv 19 \pmod{61}$.

15. Решить сравнение: а) $x^2 \equiv 28 \pmod{3^5}$; б) $x^2 \equiv 31 \pmod{5^4}$; в) $x^2 \equiv 102 \pmod{7^3}$.

16. Решить сравнение: а) $x^2 \equiv 17 \pmod{2^6}$; б) $x^2 \equiv 57 \pmod{2^8}$; в) $x^2 \equiv 129 \pmod{2^9}$.

17. Решить сравнение: а) $x^2 \equiv 14 \pmod{5 \cdot 11}$; б) $x^2 \equiv 41 \pmod{2^3 \cdot 5 \cdot 23}$; в) $x^2 \equiv 161 \pmod{2^2 \cdot 17^2 \cdot 19}$.

## Литература к главе 2


1. *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел. — М.: Мир, 1987.
2. *Виноградов И. М.* Основы теории чисел. — М.: Наука, 1981.
3. *Hammik L.* A simple proof of the quadratic reciprocity law. 31 May 2002.
4. *Menezes A., van Oorschot P., Vanstone S.* Handbook of applied cryptography. CRC Press, 1997. Доступно с http://www.cacr.math.uwaterloo.ca/hac/.

## Глава 3

# ОСНОВЫ ТЕОРИИ НЕПРЕРЫВНЫХ ДРОБЕЙ

### 3.1. Определение непрерывной дроби

Пример 3.1. Используя алгоритм Евклида, найдем наибольший общий делитель чисел 46 и 62:

$$62 = 1 \cdot 46 + 16,$$

$$46 = 2 \cdot 16 + 14,$$

$$16 = 1 \cdot 14 + 2,$$

$$14 = 7 \cdot 2 + 0.$$

Поделим эти равенства на 46, 16, 14 и 2 соответственно. Получим

$$\frac{62}{46} = 1 + \frac{16}{46} = 1 + \frac{1}{46/16} = 1 + \frac{1}{2 + \frac{14}{16}} = 1 + \frac{1}{2 + \frac{1}{16/14}} = 1 + \frac{1}{2 + \frac{1}{1 + \frac{2}{14}}} =$$

$$= 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{14/2}}} = 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{7}}}.$$

Последнее выражение представляет собой разложение числа $\frac{62}{46}$ в непрерывную дробь. □

Определение 3.1. *Непрерывной* (или *цепной*) дробью называется выражение вида

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \ddots}}} = \left[a_0; \frac{b_1}{a_1}, \frac{b_2}{a_2}, \frac{b_3}{a_3}, \ldots\right], \tag{3.1}$$

где элементы $a_k$ и $b_k$ могут быть вещественными или комплексными числами, а также функциями одной или нескольких переменных. Дроби $a_0 = \frac{a_0}{1}$, $\frac{b_k}{a_k}$, где $k = 1, 2, \ldots$, называются *звеньями* непрерывной дроби (соответственно нулевым, первым и т. д.). Будем предполагать, что $a_k \neq 0$ при $k > 0$. Следует отметить, что в сокращенной записи (3.1) звенья $\frac{b_k}{a_k}$ сокращать нельзя.

Если число звеньев непрерывной дроби (3.1) конечное, то она называется *конечной* и сокращенно обозначается $\left[a_0; \frac{b_k}{a_k}\right]_1^n$. Конечная непрерывная дробь отождествляется с рациональным числом, которое получается в результате выполнения указанных действий.

Пример 3.2. Рассмотрим непрерывную дробь $\left[1; \frac{1}{2}, \frac{1}{1}, \frac{1}{7}\right]$ из примера 3.1. «Свернем» эту дробь, последовательно выполняя умножение и «переворачивая» дроби:

$$1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{7}}} = 1 + \cfrac{1}{2 + \cfrac{1}{8/7}} = 1 + \cfrac{1}{2 + \cfrac{7}{8}} = 1 + \frac{1}{23/8} = 1 + \frac{8}{23} = \frac{31}{23}.$$

Заметим, что полученное рациональное число — это то же число $\frac{62}{46}$, но уже с взаимно простыми числителем и знаменателем. □

Обобщим рассуждения примера 3.1. Перепишем последовательность равенств, получаемых в алгоритме Евклида:

$$a = bq_0 + r_1,\ b = r_1q_1 + r_2,\ r_1 = r_2q_2 + r_3,\ \ldots,\ r_{k-2} = r_{k-1}q_{k-1} + r_k,\ r_{k-1} = r_kq_k,$$

в виде равносильной цепочки равенств:

$$\frac{a}{b}=q_0+\frac{r_1}{b},\quad \frac{b}{r_1}=q_1+\frac{r_2}{r_1},\quad \frac{r_1}{r_2}=q_2+\frac{r_3}{r_2},\ldots,\frac{r_{k-2}}{r_{k-1}}=q_{k-1}+\frac{r_k}{r_{k-1}},\quad \frac{r_{k-1}}{r_k}=q_k.$$

Используя эти соотношения, выразим дробь $\frac{a}{b}$ через $q_0, q_1, \ldots, q_k$:

$$\frac{a}{b}=q_0+\cfrac{1}{q_1+\cfrac{1}{q_2+\ddots+\cfrac{1}{q_{k-1}+\cfrac{1}{q_k}}}}. \tag{3.2}$$

Таким образом, алгоритм Евклида позволяет представить каждое рациональное число в виде конечной непрерывной дроби.

Определение 3.2. Непрерывная дробь вида $\left[a_0;\frac{1}{a_1},\frac{1}{a_2},\ldots\right]$ (обозначается также $[a_0;\ a_1,\ a_2,\ \ldots]$), где $a_i\in\mathbb{N}$, называется *обыкновенной.*

Замечание. Если в представлении (3.2) записать $q_k=(q_k-1)+1$ (при $q_k>1$), то получится другое представление числа $\frac{a}{b}$ в виде непрерывной дроби:

$$\frac{a}{b}=q_0+\cfrac{1}{q_1+\cfrac{1}{q_2+\ddots+\cfrac{1}{q_{k-1}+\cfrac{1}{(q_k-1)+\cfrac{1}{1}}}}}=q_0'+\cfrac{1}{q_1'+\cfrac{1}{q_2'+\ddots+\cfrac{1}{q_{k-1}'+\cfrac{1}{q_k'+\cfrac{1}{q_{k+1}'}}}}},$$

где $q_{k+1}'=1$. Поэтому для однозначности представления в конечной обыкновенной непрерывной дроби $[a_0;\ a_1,\ \ldots,\ a_n]$ всегда будем считать $a_n>1$.

Непрерывная дробь (3.1) с бесконечным числом звеньев называется *бесконечной* и сокращенно обозначается $\left[a_0; \frac{b_k}{a_k}\right]_1^{\infty}$. Каждое положительное иррациональное число можно разложить в бесконечную обыкновенную непрерывную дробь, причем это разложение единственно [5].

Пример 3.3. Разложим в непрерывную дробь число $\alpha = \sqrt{47}$. Целая часть числа $\sqrt{47}$ равна 6, поэтому $\sqrt{47} = 6 + \frac{1}{a_1}$. Отсюда

$$a_1 = \frac{1}{\sqrt{47} - 6} = \frac{6 + \sqrt{47}}{11}.$$

Целая часть числа $a_1$ равна 1, поэтому $a_1 = 1 + \frac{1}{a_2}$ и

$$a_2 = \frac{1}{a_1 - 1} = \frac{11}{\sqrt{47} - 5} = \frac{5 + \sqrt{47}}{2} = 5 + \frac{1}{a_3}.$$

Продолжаем разложение:

$$a_3 = \frac{1}{a_2 - 5} = \frac{2}{\sqrt{47} - 5} = \frac{5 + \sqrt{47}}{11} = 1 + \frac{1}{a_4},$$

$$a_4 = \frac{1}{a_3 - 1} = \frac{11}{\sqrt{47} - 6} = \frac{6 + \sqrt{47}}{1} = 12 + \frac{1}{a_5},$$

$$a_5 = \frac{1}{a_4 - 12} = \frac{1}{\sqrt{47} - 6} = \frac{6 + \sqrt{47}}{11} = 1 + \frac{1}{a_6}.$$

Поскольку $a_5 = a_1$, дальше элементы непрерывной дроби будут повторяться. Последовательно подставляя полученные выражения друг в друга, получаем разложение

$$\sqrt{47} = 6 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{12 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{12 + \ddots}}}}}}}}. \qquad \square$$

## 3.2. Подходящие дроби

Определение 3.3. Отрезок $\frac{P_k}{Q_k} = \left[a_0; \frac{b_1}{a_1}, \frac{b_2}{a_2}, \ldots, \frac{b_k}{a_k}\right]$ непрерывной дроби (конечной или бесконечной) называют $k$-й *подходящей дробью*, при этом полагают $P_{-1} = 1$, $Q_{-1} = 0$; $P_0 = a_0$; $Q_0 = 1$. Число $k$ называют *порядком* подходящей дроби $\frac{P_k}{Q_k}$.

Теорема 3.1 (закон составления подходящих дробей). Числа $P_k$, $Q_k$, $k = -1, 0, 1, \ldots$, определяемые из соотношений

$$P_k = a_k P_{k-1} + b_k P_{k-2};\ Q_k = a_k Q_{k-1} + b_k Q_{k-2}, \tag{3.3}$$

где

$$P_{-1} = 1, Q_{-1} = 0, P_0 = a_0, Q_0 = 1, \tag{3.4}$$

являются соответственно числителями и знаменателями подходящих дробей $\frac{P_k}{Q_k}$ непрерывной дроби (3.1).

*Доказательство*. Обозначим $R_k$ подходящие дроби непрерывной дроби (3.1) и докажем, что $R_k = \frac{P_k}{Q_k}$ для $k = 1, 2, \ldots$ .

Воспользуемся методом математической индукции.

База индукции: при $k = 1$ для подходящей дроби $R_1$ имеем

$$R_1 = a_0 + \frac{b_1}{a_1} = \frac{a_0 a_1 + b_1}{a_1}.$$

Из соотношений (3.3) с учетом (3.4) находим

$$P_1 = a_1 P_0 + b_1 P_{-1} = a_1 \cdot a_0 + b_1 \cdot 1 = a_0 a_1 + b_1,$$

$$Q_1 = a_1 Q_0 + b_1 Q_{-1} = a_1 \cdot 1 + b_1 \cdot 0 = a_1.$$

Следовательно, $R_1 = \frac{P_1}{Q_1}$ и для $k = 1$ утверждение теоремы справедливо.

Пусть теперь теорема верна для всех натуральных чисел, не превосходящих $k$. Покажем, что она справедлива и для очередного натурального числа $k + 1$. Из соотношений (3.3) получаем

$$P_{k+1} = a_{k+1} P_k + b_{k+1} P_{k-1}, \quad Q_{k+1} = a_{k+1} Q_k + b_{k+1} Q_{k-1}.$$

По индукционному предположению

$$R_k = \frac{P_k}{Q_k} = \frac{a_k P_{k-1} + b_k P_{k-2}}{a_k Q_{k-1} + b_k Q_{k-2}}.$$

По определению подходящая дробь $R_{k+1}$ получается из подходящей дроби $R_k$ путем замены $a_k$ суммой $a_k + \frac{b_{k+1}}{a_{k+1}}$. Поэтому

$$R_{k+1} = \frac{\left(a_k + \frac{b_{k+1}}{a_{k+1}}\right) P_{k-1} + b_k P_{k-2}}{\left(a_k + \frac{b_{k+1}}{a_{k+1}}\right) Q_{k-1} + b_k Q_{k-2}} = \frac{a_{k+1}(a_k P_{k-1} + b_k P_{k-2}) + b_{k+1} P_{k-1}}{a_{k+1}(a_k Q_{k-1} + b_k Q_{k-2}) + b_{k+1} Q_{k-1}} =$$

$$= \frac{a_{k+1} P_k + b_{k+1} P_{k-1}}{a_{k+1} Q_k + b_{k+1} P_{k-1}} = \frac{P_{k+1}}{Q_{k+1}}. \qquad \square$$

Следствие. Для непрерывной дроби с положительными элементами числители $P_k$ образуют монотонно возрастающую последовательность при $k \geq 0$; знаменатели $Q_k$ образуют монотонно возрастающую последовательность при $k \geq 1$.

Для удобства вычислений подходящих дробей по формулам (3.3) обычно пользуются следующей таблицей:

| $k$ | $-1$ | $0$ | $1$ | $2$ | $3$ | ... |
|---|---|---|---|---|---|---|
| $b_k$ | | | $b_1$ | $b_2$ | $b_3$ | ... |
| $a_k$ | | $a_0$ | $a_1$ | $a_2$ | $a_3$ | ... |
| $P_k$ | $1$ | $a_0$ | $P_1$ | $P_2$ | $P_3$ | ... |
| $Q_k$ | $0$ | $1$ | $Q_1$ | $Q_2$ | $Q_3$ | ... |

Пример 3.4. Найдем все подходящие дроби для непрерывной дроби $\left[0; \frac{1}{2}, \frac{3}{4}, \frac{5}{6}\right]$. Заполняем таблицу:

| $k$ | $-1$ | $0$ | $1$ | $2$ | $3$ |
|---|---|---|---|---|---|
| $b_k$ | | | $1$ | $3$ | $5$ |
| $a_k$ | | $0$ | $2$ | $4$ | $6$ |
| $P_k$ | $1$ | $0$ | $1$ | $4$ | $29$ |
| $Q_k$ | $0$ | $1$ | $2$ | $11$ | $76$ |

Отсюда $\frac{P_0}{Q_0} = \frac{0}{1}$, $\frac{P_1}{Q_1} = \frac{1}{2}$, $\frac{P_2}{Q_2} = \frac{4}{11}$, $\frac{P_3}{Q_3} = \frac{29}{76}$. □

При вычислении подходящих дробей для обыкновенной непрерывной дроби вторую строку в таблице, как правило, не пишут.

Пример 3.5. Найдем все подходящие дроби для обыкновенной непрерывной дроби [2; 1, 2, 1, 3, 1, 4]. Заполняем таблицу:

| $k$ | $-1$ | $0$ | $1$ | $2$ | $3$ | $4$ | $5$ | $6$ |
|---|---|---|---|---|---|---|---|---|
| $a_k$ | | $2$ | $1$ | $2$ | $1$ | $3$ | $1$ | $4$ |
| $P_k$ | $1$ | $2$ | $3$ | $8$ | $11$ | $41$ | $52$ | $249$ |
| $Q_k$ | $0$ | $1$ | $1$ | $3$ | $4$ | $15$ | $19$ | $91$ |

Отсюда

$$\frac{P_0}{Q_0}=\frac{2}{1},\ \frac{P_1}{Q_1}=\frac{3}{1},\ \frac{P_2}{Q_2}=\frac{8}{3},\ \frac{P_3}{Q_3}=\frac{11}{4},\ \frac{P_4}{Q_4}=\frac{41}{15},\ \frac{P_5}{Q_5}=\frac{52}{19},\ \frac{P_6}{Q_6}=\frac{249}{91}. \quad \square$$

Лемма 3.2. Для соседних подходящих дробей $\frac{P_{k-1}}{Q_{k-1}}$, $\frac{P_k}{Q_k}$ непрерывной дроби (3.1) при $k \geq 1$ справедливо соотношение

$$P_kQ_{k-1} - P_{k-1}Q_k = (-1)^{k-1}b_1b_2\ldots b_k. \tag{3.5}$$

*Доказательство.* Обозначим $\Delta_k = \begin{vmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{vmatrix}$ и распишем элементы первого столбца по закону составления подходящих дробей. Тогда

$$\Delta_k = \begin{vmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{vmatrix} = \begin{vmatrix} a_kP_{k-1} + b_kP_{k-2} & P_{k-1} \\ a_kQ_{k-1} + b_kQ_{k-2} & Q_{k-1} \end{vmatrix} = \begin{vmatrix} b_kP_{k-2} & P_{k-1} \\ b_kQ_{k-2} & Q_{k-1} \end{vmatrix} = b_k \begin{vmatrix} P_{k-2} & P_{k-1} \\ Q_{k-2} & Q_{k-1} \end{vmatrix} =$$

$$= -b_k \begin{vmatrix} P_{k-1} & P_{k-2} \\ Q_{k-1} & Q_{k-2} \end{vmatrix} = -b_k\Delta_{k-1}.$$

Проводя аналогичные выкладки для $\Delta_{k-1}$, $\Delta_{k-2}$, …, получаем:

$$\Delta_k = (-b_k)(-b_{k-1})\ldots(-b_1)\Delta_0 = (-1)^k b_1b_2\ldots b_k\Delta_0,$$

где

$$\Delta_0 = \begin{vmatrix} P_0 & P_{-1} \\ Q_0 & Q_{-1} \end{vmatrix} = \begin{vmatrix} a_0 & 1 \\ 1 & 0 \end{vmatrix} = a_0 \cdot 0 - 1 \cdot 1 = -1.$$

Отсюда $P_kQ_{k-1} - P_{k-1}Q_k = \Delta_k = (-1)^{k+1}b_1b_2\ldots b_k = (-1)^{k-1}b_1b_2\ldots b_k$. $\square$

Для подходящих дробей обыкновенной непрерывной дроби соотношение (3.5) имеет вид

$$P_kQ_{k-1} - P_{k-1}Q_k = (-1)^{k-1}. \tag{3.6}$$

Следствие. Для обыкновенной непрерывной дроби числитель и знаменатель любой подходящей дроби взаимно просты.

*Доказательство.* Пусть $d = \text{НОД}(P_k, Q_k)$. Тогда оба слагаемых в левой части равенства (3.6) делятся на $d$, а значит и $(-1)^{k-1}$ делится на $d$, то есть $d = \pm 1$. □

Лемма 3.3. Для подходящих дробей $\frac{P_{k-2}}{Q_{k-2}}, \frac{P_k}{Q_k}$ непрерывной дроби (3.1) при $k \geq 2$ справедливо соотношение

$$P_k Q_{k-2} - P_{k-2} Q_k = (-1)^k b_1 b_2 \ldots b_{k-1} a_k. \tag{3.7}$$

*Доказательство.* Воспользуемся методом математической индукции. Составляем базу индукции:

$$P_2 Q_0 - P_0 Q_2 = (a_2 P_1 + b_2 P_0) \cdot 1 - a_0 (a_2 Q_1 + b_2 Q_0) =$$

$$= a_2 (a_1 P_0 + b_1 P_{-1}) + b_2 a_0 - a_0 (a_2 (a_1 Q_0 + b_1 Q_{-1}) + b_2) =$$

$$= a_0 a_1 a_2 + a_2 b_1 + a_0 b_2 - a_0 a_1 a_2 - a_0 b_2 = b_1 a_2 = (-1)^2 b_1 a_2.$$

Тогда

$$P_{k+1} Q_{k-1} - P_{k-1} Q_{k+1} = (a_{k+1} P_k + b_{k+1} P_{k-1}) Q_{k-1} - P_{k-1} (a_{k+1} Q_k + b_{k+1} Q_{k-1}) =$$

$$= a_{k+1} (P_k Q_{k-1} - P_{k-1} Q_k) = a_{k+1} (-1)^{k-1} b_1 b_2 \ldots b_k = (-1)^{k+1} b_1 b_2 \ldots b_k a_{k+1}.$$ □

Теорема 3.4. Для непрерывной дроби с положительными элементами справедливы следующие утверждения.

1. Подходящие дроби четного порядка образуют монотонно возрастающую последовательность, а подходящие дроби нечетного порядка — монотонно убывающую последовательность.

2. Любая подходящая дробь четного порядка меньше любой подходящей дроби нечетного порядка.

3. Число, выражаемое этой непрерывной дробью, содержится между двумя соседними подходящими дробями (рис. 3.1).

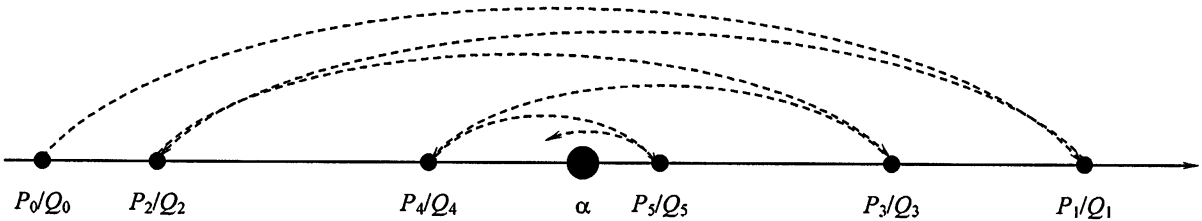



***Рис. 3.1.*** *Последовательности, образованные подходящими дробями*

*Доказательство* [3]. Пусть $\alpha = \left[a_0; \frac{b_1}{a_1}, \frac{b_2}{a_2}, \ldots\right]$ — конечная или бесконечная непрерывная дробь, где $a_k > 0$, $b_k > 0$, и $\frac{P_k}{Q_k}$ $(k = 0, 1, \ldots)$ — ее последовательные подходящие дроби. Очевидно, что $P_k > 0$ и $Q_k > 0$.

Для $k = 2m$ по лемме 3.3 получаем $\frac{P_{2m}}{Q_{2m}} - \frac{P_{2m-2}}{Q_{2m-2}} > 0$, учитывая, что $a_k > 0$ и $b_i > 0$ для $i = 1, 2, \ldots, 2m$. Следовательно,

$$\frac{P_{2m-2}}{Q_{2m-2}} < \frac{P_{2m}}{Q_{2m}}$$

для $m = 1, 2, \ldots$, или

$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \frac{P_4}{Q_4} < \ldots$$

Аналогично для $k = 2m + 1$ получаем

$$\frac{P_{2m-1}}{Q_{2m-1}} > \frac{P_{2m+1}}{Q_{2m+1}}$$

для $m = 1, 2, \ldots$, или

$$\frac{P_1}{Q_1} > \frac{P_3}{Q_3} > \frac{P_5}{Q_5} > \ldots$$

Первое утверждение доказано.

Применяя лемму 3.2 при $k = 2m$, получаем

$$\frac{P_{2m-1}}{Q_{2m-1}} > \frac{P_{2m}}{Q_{2m}},$$

то есть всякая подходящая дробь нечетного порядка больше соседней подходящей дроби четного порядка. Покажем, что любая подходящая дробь нечетного порядка больше любой подходящей дроби четного по-

рядка. Для произвольных подходящих дробей $\frac{P_{2s-1}}{Q_{2s-1}}, \frac{P_{2s}}{Q_{2s}}, \frac{P_{2m-1}}{Q_{2m-1}}, \frac{P_{2m}}{Q_{2m}}$ имеем:

$$\frac{P_{2s-1}}{Q_{2s-1}} \geq \frac{P_{2m-1}}{Q_{2m-1}} > \frac{P_{2m}}{Q_{2m}},$$

если $s \leq m$, и

$$\frac{P_{2s-1}}{Q_{2s-1}} > \frac{P_{2s}}{Q_{2s}} > \frac{P_{2m}}{Q_{2m}},$$

если $s > m$. Следовательно, при любых $s$ и $m$ справедливо неравенство

$$\frac{P_{2s-1}}{Q_{2s-1}} > \frac{P_{2m}}{Q_{2m}}.$$

Докажем утверждение 3. Из способа построения непрерывной дроби имеем соотношения

$$\alpha > \frac{P_0}{Q_0}, \quad \alpha < \frac{P_1}{Q_1}, \quad \alpha > \frac{P_2}{Q_2}, \ldots$$

Следовательно, $\frac{P_k}{Q_k} < \alpha \leq \frac{P_{k+1}}{Q_{k+1}}$ при четном $k$ и $\frac{P_k}{Q_k} > \alpha \geq \frac{P_{k+1}}{Q_{k+1}}$ при нечетном $k$. Если число $\alpha$ задано конечной непрерывной дробью $\left[a_0; \frac{b_1}{a_1}, \frac{b_2}{a_2}, \ldots, \frac{b_n}{a_n}\right]$, то при $k = n$ достигается равенство. □

Следствие. Если $\frac{P_k}{Q_k}, \frac{P_{k+1}}{Q_{k+1}}$ — подходящие дроби для числа $\alpha$, заданного обыкновенной непрерывной дробью, то выполняется неравенство

$$\left|\alpha - \frac{P_k}{Q_k}\right| \leq \frac{1}{Q_k Q_{k+1}},$$

а при $\alpha \neq \frac{P_{k+1}}{Q_{k+1}}$ — строгое неравенство

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \frac{1}{Q_k Q_{k+1}}.$$

Подходящая дробь $\frac{P_k}{Q_k}$, где $k \geq 2$, является *наилучшим приближением* числа $\alpha$, выраженного обыкновенной непрерывной дробью, то есть для любых положительных целых чисел $P$, $Q$, таких, что $0 < Q \leq Q_k$ и $\frac{P}{Q} \neq \frac{P_k}{Q_k}$, выполняется неравенство $|Q_k\alpha - P_k| < |Q\alpha - P|$.

Определение 3.4. Бесконечная непрерывная дробь $\left[a_0; \frac{b_k}{a_k}\right]_1^\infty$ называется *сходящейся*, если существует конечный предел

$$\alpha = \lim_{k\to\infty} \frac{P_k}{Q_k},$$

где $\frac{P_k}{Q_k}$ — подходящие дроби, $k = 1, 2, \ldots$; при этом число $\alpha$ принимается за значение этой непрерывной дроби. Если такой предел не существует, то бесконечная непрерывная дробь называется *расходящейся*, и ей не приписывается никакого числового значения.

Пример 3.6. Решим уравнение $x^2 - 5x + 4 = 0$, используя непрерывные дроби. Перепишем его в виде $x^2 = 5x - 4$, отсюда $x = 5 - \frac{4}{x}$, то есть

$$x = 5 - \cfrac{4}{5 - \cfrac{4}{5 - \ddots}}.$$

Вычислим подходящие дроби к $x$:

$$\frac{5}{1}, \frac{21}{5}, \frac{85}{21}, \frac{341}{85}, \ldots, \frac{4^{k+1}-1}{4^k-1} = 4 + \frac{3}{4^k-1},$$

где $k \geq 1$. Эта последовательность монотонно убывает и стремится к 4 при $k \to \infty$ (рис. 3.2 на стр. 96), то есть $x = 4$ — корень уравнения.

Аналогично ищем второй корень. Записываем уравнение в виде $4 = 5x - x^2$, откуда $x = \frac{4}{5-x}$, то есть

$$x = \cfrac{4}{5 - \cfrac{4}{5 - \ddots}}.$$

Вычисляем подходящие дроби:

$$\frac{4}{5}, \frac{20}{21}, \frac{84}{85}, \frac{340}{341}, \ldots, \frac{4^k-4}{4^k-1} = 1 - \frac{3}{4^k-1},$$

где $k \geq 2$. Предел этой монотонно возрастающей последовательности равен 1 при $k \to \infty$, то есть $x = 1$ — второй корень уравнения. □

Теорема 3.5. Если все элементы $a_k$, $b_k$ ($k = 0, 1, \ldots$) бесконечной непрерывной дроби положительны, причем

$$b_k \leq a_k, \quad a_k \geq d > 0 \ (k = 1, 2, \ldots),$$

то бесконечная непрерывная дробь сходится.

*Доказательство* [3]. Подходящие дроби $\frac{P_{2k}}{Q_{2k}}$ ($k = 0, 1, 2, \ldots$) четного порядка образуют монотонно возрастающую последовательность, ограниченную сверху (например, числом $\frac{P_1}{Q_1}$). Значит, существует конечный предел $\lim\limits_{k\to\infty} \frac{P_{2k}}{Q_{2k}} = \alpha$.

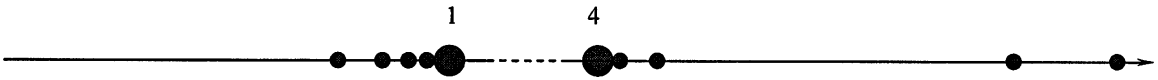



***Рис. 3.2.*** *Подходящие дроби, определяющие корни квадратного уравнения*

Аналогично подходящие дроби $\frac{P_{2k+1}}{Q_{2k+1}}$ $(k = 0, 1, 2,\ldots)$ нечетного порядка образуют монотонно убывающую последовательность, ограниченную снизу (например, числом $\frac{P_0}{Q_0}$). Следовательно, существует конечный предел $\lim\limits_{k\to\infty}\frac{P_{2k+1}}{Q_{2k+1}} = \beta$.

Согласно утверждению 2 теоремы 3.4, для любого $k \geq 0$ выполняется неравенство

$$\frac{P_{2k}}{Q_{2k}} < \alpha \leq \beta < \frac{P_{2k+1}}{Q_{2k+1}},$$

откуда, воспользовавшись леммой 3.2, получаем

$$0 \leq \beta - \alpha < \frac{P_{2k+1}}{Q_{2k+1}} - \frac{P_{2k}}{Q_{2k}} = \frac{b_1 b_2 \ldots b_{2k+1}}{Q_{2k} Q_{2k+1}} = \gamma_k.$$

Покажем, что $\gamma_k \underset{k\to\infty}{\to} 0$.

Согласно закону составления подходящих дробей, имеем при $k \geq 2$

$$Q_{k-1} = a_{k-1}Q_{k-2} + b_{k-1}Q_{k-3}.$$

По условию теоремы $a_{k-1} \geq d > 0$, $b_{k-1} > 0$, значит,

$$Q_{k-1} \geq dQ_{k-2}.$$

Аналогично, поскольку $a_k \geq b_k$, получаем

$$Q_k = a_kQ_{k-1} + b_kQ_{k-2} \geq b_kQ_{k-1} + b_kQ_{k-2} = b_k(Q_{k-1} + Q_{k-2}).$$

Подставляем в это неравенство оценку для $Q_{k-1}$:

$$Q_k \geq b_k(1 + d)Q_{k-2}.$$

Отсюда последовательно получаем

$$Q_{2k} \geq b_{2k}(1 + d)Q_{2k-2} \geq \ldots \geq b_{2k}b_{2k-2}\ldots b_2(1 + d)^kQ_0 = b_2b_4\ldots b_{2k}(1 + d)^k.$$

Точно так же для подходящих дробей нечетного порядка имеем

$$Q_{2k+1} \geq b_{2k+1}(1+d)Q_{2k-1} \geq \ldots \geq b_{2k+1}b_{2k-1}\ldots b_3(1+d)^k Q_1 = b_1 b_3 \ldots b_{2k+1}(1+d)^k.$$

Перемножая полученные оценки, находим

$$Q_{2k}Q_{2k+1} \geq b_1 b_2 \ldots b_{2k+1}(1+d)^{2k},$$

и, значит,

$$\gamma_k = \frac{b_1 b_2 \ldots b_{2k+1}}{Q_{2k}Q_{2k+1}} \leq \frac{1}{(1+d)^{2k}} \underset{k\to\infty}{\to} 0,$$

откуда $0 \leq \beta - \alpha \leq 0$, то есть

$$\alpha = \beta = \lim_{k\to\infty} \frac{P_k}{Q_k},$$

и, следовательно, бесконечная непрерывная дробь сходится. □

Следствие. Обыкновенная непрерывная дробь всегда сходится.

Пример 3.7. Найдем число, задаваемое бесконечной непрерывной дробью [1; 1, 1, 1, ...].

Из выражения

$$\alpha = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}$$

получаем $\alpha = 1 + \dfrac{1}{\alpha}$, то есть $\alpha^2 - \alpha - 1 = 0$. Это уравнение имеет два решения:

$$\alpha_{1,2} = \frac{1 \pm \sqrt{5}}{2}.$$

Все элементы непрерывной дроби [1; 1, 1, 1, ...] положительны, поэтому $\alpha = \dfrac{1+\sqrt{5}}{2}$. □

## 3.3. Квадратичные иррациональности

Определение 3.5. Бесконечная обыкновенная непрерывная дробь $\alpha = [a_0; a_1, a_2, \ldots]$ называется *периодической*, если существуют такие натуральные числа $k_0$ и $t$, что для любого $k > k_0$ выполняется равенство $a_{k+t} = a_k$, то есть последовательность $\{a_k\}$, начиная с некоторого места, является периодической:

$$\alpha = [a_0; a_1, \ldots, a_{k_0-1}, a_{k_0}, a_{k_0+1}, \ldots, a_{k_0+t}, a_{k_0+1}, \ldots, a_{k_0+t}, \ldots] =$$
$$= [a_0; a_1, \ldots, a_{k_0}, \{a_{k_0+1}, \ldots, a_{k_0+t}\}].$$

Пример 3.8. Следующие числа раскладываются в периодические непрерывные дроби:

$\sqrt{17} = [4; \{8\}]$ — период равен 1;

$\dfrac{\sqrt{35}+6}{11} = [1; 12, \{130, 13\}]$ — период равен 2;

$\sqrt{21} = [4; \{1, 1, 2, 1, 1, 8\}]$ — период равен 6;

$\dfrac{8\sqrt{29}}{13} = [3; \{3, 5, 2, 1, 1, 22, 3, 1, 3, 22, 1, 1, 2, 5, 3, 6\}]$ — период равен 16;

$812\sqrt{2} = [1148; \{2, 1, 13, 11, 1, 1, 1, 4, 2, 1, 2, 1, 1, 46, 3, 2, 2, 1, 1, 573, 1, 1, 2, 2, 3, 46, 1, 1, 2, 1, 2, 4, 1, 1, 1, 11, 13, 1, 2, 2296\}]$ — период равен 40.

Отметим, что при разложении в непрерывную дробь квадратного корня из целого положительного числа, не являющегося полным квадратом, период всегда начинается с первого звена. □

Пример 3.9. Следующие числа раскладываются в непериодические непрерывные дроби:

$\sqrt[3]{2} = [1; 3, 1, 5, 1, 1, 4, 1, 1, 8, 1, 14, 1, 10, 2, 1, 4, 12, 2, 3, 2, \ldots]$;

$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2, 1, \ldots]$;

$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, 14, \ldots]$;

$\ln 2 = [0; 1, 2, 3, 1, 6, 3, 1, 1, 2, 1, 1, 1, 1, 3, 10, 1, 1, 1, 2, 1, \ldots]$;

$2^{\sqrt{2}} = [2; 1, 1, 1, 72, 3, 4, 1, 3, 2, 1, 1, 1, 14, 1, 2, 1, 1, 3, 1, 3, \ldots]$. □

Определение 3.6. Число называется *квадратичной иррациональностью*, если оно является корнем квадратного уравнения $ax^2 + bx + c = 0$ с целыми коэффициентами $a$, $b$, $c$. Это уравнение определено однозначно, если потребовать, чтобы числа $a$, $b$, $c$ были взаимно просты в совокупности и $a \geq 0$.

Пример 3.10. Числа $\sqrt{3}$, $3\sqrt{2}+5$, $\dfrac{1+\sqrt{15}}{2}$, $\dfrac{1+\sqrt{15}}{7-4\sqrt{15}}$ являются квадратичными иррациональностями; числа $\sqrt[3]{5}$, $2\sqrt[5]{7}+3$, $e$, $\pi$ не являются квадратичными иррациональностями. □

Любая квадратичная иррациональность имеет вид $u+v\sqrt{N}$, где числа $u$, $v$ рациональные и $N$ не является полным квадратом. Квадратичная иррациональность вида $u-v\sqrt{N}$ называется *сопряженной* к иррациональности $u+v\sqrt{N}$.

Теорема 3.6 (Лагранж). Квадратичные иррациональности и только они могут быть представлены в виде бесконечной периодической обыкновенной непрерывной дроби.

*Доказательство* [4]. Сначала докажем достаточность. Рассмотрим бесконечную периодическую обыкновенную непрерывную дробь

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}.$$

Назовем число

$$r_k = a_k + \cfrac{1}{a_{k+1} + \cfrac{1}{a_{k+2} + \ddots}}$$

остатком непрерывной дроби $\alpha$, тогда

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \cfrac{\ddots}{a_{k-1} + \cfrac{1}{r_k}}}}.$$

Для остатков периодической непрерывной дроби выполняется соотношение $r_{k+t} = r_k$, где $k \geq k_0$ и $t$ — период последовательности $\{a_k\}$. По способу составления подходящих дробей имеем

$$\alpha = \frac{r_k P_{k-1} + P_{k-2}}{r_k Q_{k-1} + Q_{k-2}} = \frac{r_{k+t} P_{k+t-1} + P_{k+t-2}}{r_{k+t} Q_{k+t-1} + Q_{k+t-2}} = \frac{r_k P_{k+t-1} + P_{k+t-2}}{r_k Q_{k+t-1} + Q_{k+t-2}},$$

откуда

$$\frac{r_k P_{k-1} + P_{k-2}}{r_k Q_{k-1} + Q_{k-2}} = \frac{r_k P_{k+t-1} + P_{k+t-2}}{r_k Q_{k+t-1} + Q_{k+t-2}},$$

то есть $r_k$ является корнем квадратного уравнения

$$(P_{k-1}Q_{k+t-1} - P_{k+t-1}Q_{k-1})r^2 + (P_{k-1}Q_{k+t-2} + P_{k-2}Q_{k+t-1} -$$

$$- P_{k+t-1}Q_{k-2} - P_{k+t-2}Q_{k-1})r + (P_{k-2}Q_{k+t-2} - P_{k+t-2}Q_{k-2}) = 0$$

с целыми коэффициентами. Значит, $r_k$ — квадратичная иррациональность. Тогда и

$$\alpha = \frac{r_k P_{k-1} + P_{k-2}}{r_k Q_{k-1} + Q_{k-2}}$$

— квадратичная иррациональность.

Теперь докажем необходимость. Пусть число $\alpha$ является корнем квадратного уравнения с целыми коэффициентами

$$a\alpha^2 + b\alpha + c = 0. \tag{3.8}$$

Разложим число $\alpha$ в обыкновенную непрерывную дробь и выразим его через некоторый остаток $r_k$ непрерывной дроби:

$$\alpha = \frac{r_k P_{k-1} + P_{k-2}}{r_k Q_{k-1} + Q_{k-2}}.$$

Подставляя это выражение в формулу (3.8) и проводя ряд преобразований, снова получаем квадратное уравнение

$$A_k r_k^2 + B_k r_k + C_k = 0 \tag{3.9}$$

относительно $r_k$ с целыми коэффициентами

$$A_k = aP_{k-1}^2 + bP_{k-1}Q_{k-1} + cQ_{k-1}^2,$$
$$B_k = 2aP_{k-1}P_{k-2} + b\left(P_{k-1}Q_{k-2} + P_{k-2}Q_{k-1}\right) + 2cQ_{k-1}Q_{k-2},$$
$$C_k = aP_{k-2}^2 + bP_{k-2}Q_{k-2} + cQ_{k-2}^2.$$

Заметим, что $C_k = A_{k-1}$ и

$$B_k^2 - 4A_kC_k = (b^2 - 4ac)(P_{k-1}Q_{k-2} + P_{k-2}Q_{k-1})^2 =$$
$$= (b^2 - 4ac)(-1)^{2(k-2)} = b^2 - 4ac,$$

то есть дискриминанты уравнений (3.8) и (3.9) совпадают при любом $k$.

Из неравенства $\left|\alpha - \frac{P_{k-1}}{Q_{k-1}}\right| < \frac{1}{Q_{k-1}^2}$ получаем, что

$$P_{k-1} = \alpha Q_{k-1} + \frac{\varepsilon_{k-1}}{Q_{k-1}}$$

при некотором $\varepsilon_{k-1}$, таком, что $|\varepsilon_{k-1}| < 1$. Тогда

$$A_k = aP_{k-1}^2 + bP_{k-1}Q_{k-1} + cQ_{k-1}^2 =$$
$$= a\left(\alpha Q_{k-1} + \frac{\varepsilon_{k-1}}{Q_{k-1}}\right)^2 + b\left(\alpha Q_{k-1} + \frac{\varepsilon_{k-1}}{Q_{k-1}}\right)Q_{k-1} + cQ_{k-1}^2 =$$
$$= (a\alpha^2 + b\alpha + c)Q_{k-1}^2 + 2\alpha\varepsilon_{k-1} + a\frac{\varepsilon_{k-1}^2}{Q_{k-1}^2} + b\varepsilon_{k-1} =$$
$$= 0 \cdot Q_{k-1}^2 + 2\alpha\varepsilon_{k-1} + a\frac{\varepsilon_{k-1}^2}{Q_{k-1}^2} + b\varepsilon_{k-1} = 2\alpha\varepsilon_{k-1} + a\frac{\varepsilon_{k-1}^2}{Q_{k-1}^2} + b\varepsilon_{k-1}.$$

Значит,

$$|A_k| = \left|2a\alpha\varepsilon_{k-1} + a\frac{\varepsilon_{k-1}^2}{Q_{k-1}^2} + b\varepsilon_{k-1}\right| < 2|a\alpha| + |a| + |b|,$$

$$|C_k| = |A_{k-1}| < 2|a\alpha| + |a| + |b|$$

для любого натурального $k$. Таким образом, целые коэффициенты $A_k$ и $C_k$ уравнения (3.9) ограничены по абсолютной величине и, следовательно, при изменении $k$ могут принимать лишь конечное число различных значений. Дискриминанты уравнений (3.8) и (3.9) совпадают, поэтому коэффициент $B_k$ может принимать лишь конечное число различных значений. Значит, при $k = 1, 2, \ldots$ существует лишь конечное число различных уравнений вида (3.9), то есть лишь конечное число различных остатков $r_k$. Следовательно, найдутся два одинаковых остатка $r_k$ и $r_{k+t}$ с разными номерами, что и означает периодичность непрерывной дроби. □

Пример 3.11. Разложим в непрерывную дробь число $1+2\sqrt{3}$:

$$1+2\sqrt{3} = [4;\ \{2,\ 6\}].$$

Эта непрерывная дробь периодическая, и все $a_k$ равны либо 2, либо 6 при $k \geq 1$. Действительно, обозначим через $x$ бесконечную непрерывную дробь [0; 2, 6, 2, 6, ...]. Тогда $x = \dfrac{1}{2+\dfrac{1}{6+x}}$. Упрощая выражение, получаем, что $x$ является корнем уравнения

$$x^2 + 6x - 3 = 0,$$

откуда $x = -3 + 2\sqrt{3}$ и $4 + x = 1 + 2\sqrt{3}$. □

### 3.4. Использование непрерывных дробей для решения задач

Рассмотрим некоторые примеры использования непрерывных дробей.

### 3.4.1. Простейшие диофантовы уравнения и сравнения первой степени

Предположим, что $\frac{P_k}{Q_k}$ — последняя подходящая дробь в представлении непрерывной дробью рационального числа $\frac{a}{b}$, где НОД$(a, b) = 1$. Тогда $a = P_k$, $b = Q_k$. Перепишем выражение (3.6) для соседних подходящих дробей: $a \cdot (-1)^{k-1} Q_{k-1} - b \cdot (-1)^{k-1} P_{k-1} = 1$. Получаем одно решение диофантова уравнения $ax - by = 1$: $x_0 = (-1)^{k-1} Q_{k-1}$, $y_0 = (-1)^{k-1} P_{k-1}$.

Остальные решения имеют вид

$$x = (-1)^{k-1} Q_{k-1} + bt, y = (-1)^{k-1} P_{k-1} + at, \ t \in \mathbb{Z}.$$

В общем случае диофантово уравнение $ax - by = c$ разрешимо, если число $c$ делится на НОД$(a, b)$; решение имеет вид

$$x = (-1)^{k-1} \frac{c}{\text{Í Î Ä}(a,b)} Q_{k-1} + bt, \quad y = (-1)^{k-1} \frac{c}{\text{Í Î Ä}(a,b)} P_{k-1} + at, \quad t \in \mathbb{Z}.$$

Пример 3.12. Решим диофантово уравнение $31x - 23y = 11$. Поскольку 11 делится на НОД$(31, 23) = 1$, решение существует. Заполняем таблицу:

| $k$ | $-1$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|
| $a_k$ | | 1 | 2 | 1 | 7 |
| $P_k$ | 1 | 1 | 3 | 4 | 31 |
| $Q_k$ | 0 | 1 | 2 | 3 | 23 |

Значит, $k = 3$, $\frac{P_2}{Q_2} = \frac{4}{3}$. Находим решение: $x = (-1)^2 \cdot 11 \cdot 3 + 23t = 33 + 23t$, $y = (-1)^2 \cdot 11 \cdot 4 + 31t = 44 + 31t$, где $t \in \mathbb{Z}$.

Проверка: $31 \cdot (33 + 23t) - 23 \cdot (44 + 31t) = 31 \cdot 33 + 31 \cdot 23t - 23 \cdot 44 - 23 \cdot 31t = 31 \cdot 33 - 23 \cdot 44 = 11$. □

Пример 3.13. Решим диофантово уравнение $655x - 115y = 700$. Поскольку 700 делится на НОД(655, 115) = 5, решение существует. Заполняем таблицу:

| $k$ | $-1$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|---|
| $a_k$ | | 5 | 1 | 2 | 3 | 2 |
| $P_k$ | 1 | 5 | 6 | 17 | 57 | 131 |
| $Q_k$ | 0 | 1 | 1 | 3 | 10 | 23 |

Значит, $k = 4$, $\frac{P_3}{Q_3} = \frac{57}{10}$. Находим решение:

$$x = (-1)^3 \cdot 140 \cdot 10 + 115t = -1400 + 115t,$$

$$y = (-1)^3 \cdot 140 \cdot 57 + 655t = -7980 + 655t,$$

где $t \in \mathbb{Z}$.

Проверка: $655 \cdot (-1400 + 115t) - 115 \cdot (-7980 + 655t) = -655 \cdot 1400 + 655 \cdot 115t + 115 \cdot 7980 - 115 \cdot 655t = -917000 + 917700 = 700$. □

Аналогично решаются сравнения первой степени вида $ax \equiv b \pmod{m}$. Для этого достаточно взять обе части диофантова уравнения $ax - my = b$ по модулю $m$. Как уже говорилось в главе 1, это сравнение разрешимо только тогда, когда $b$ делится на НОД($a$, $m$). Решение имеет вид

$$x \equiv (-1)^{k-1} \frac{b}{\text{Í Î Ä}(a, m)} Q_{k-1} \pmod{m}.$$

### 3.4.2. Уравнение Пелля

Определение 3.7. *Уравнением Пелля* называется диофантово уравнение вида

$$x^2 - Ny^2 = 1, \tag{3.10}$$

где натуральное число $N$ свободно от квадратов.

Теорема 3.7. Для данного иррационального числа $\alpha$ существует бесконечно много пар таких взаимно простых целых чисел $x, y$, что $\left|\frac{x}{y}-\alpha\right|<\frac{1}{y^2}, y>0$.

*Доказательство* [1]. Разобьем полуинтервал [0, 1) на $n$ равных полуинтервалов:

$$[0,1)=\left[0,\frac{1}{n}\right)\cup\left[\frac{1}{n},\frac{2}{n}\right)\cup\ldots\cup\left[\frac{n-1}{n},1\right).$$

Дробная часть $\{\alpha\}$ числа $\alpha$, $\{\alpha\}=\alpha-[\alpha]$, лежит ровно в одном из этих полуинтервалов. Рассмотрим дробные части 0, $\{\alpha\}$, $\{2\alpha\}$, ..., $\{n\alpha\}$. По крайней мере две из них должны лежать в одном и том же полуинтервале $\left[\frac{i}{n},\frac{i+1}{n}\right)$, то есть существуют такие целые числа $k$, $j$, $0\le j<k\le n$, что

$$\left|k\alpha-[k\alpha]-(j\alpha-[j\alpha])\right|<\frac{1}{n}.$$

Полагая $x=[j\alpha]-[k\alpha], y=k-j$, получаем $|x-y\alpha|<\frac{1}{n}$. Числа $x$ и $y$ можно считать взаимно простыми, так как в противном случае получим более сильное неравенство. Поделив обе его части на $y$, получим

$$\left|\frac{x}{y}-\alpha\right|<\frac{1}{ny}<\frac{1}{y^2},$$

так как $0<y<n$.

Неравенство $j<k$ обеспечивает нам $\left|\frac{x}{y}-\alpha\right|\ne 0$. Выберем целое число $n_1>\frac{1}{|(x/y)-\alpha|}$. Тогда, разбивая полуинтервал [0, 1) на $n_1$ равных

полуинтервалов, находим пару таких взаимно простых целых чисел $x_1$, $y_1$, что

$$\left|\frac{x_1}{y_1}-\alpha\right|<\frac{1}{n_1 y_1}<\left|\frac{x}{y}-\alpha\right|, \quad 0<y_1<n_1.$$

Повторяя рассуждения, получаем бесконечное число пар $x_i$, $y_i$, для которых $\left|\frac{x_i}{y_i}-\alpha\right|<\frac{1}{y_i^2}$. □

Лемма 3.8. Если натуральное число $N$ свободно от квадратов, то существует такое число $c>0$, что неравенство $\left|x^2-Ny^2\right|<c$ имеет бесконечно много целочисленных решений $(x, y)$.

*Доказательство* [1]. Запишем $x^2-Ny^2=(x-y\sqrt{N})(x+y\sqrt{N})$. Полагая в теореме 3.7 $\alpha=\sqrt{N}$, получаем, что существует бесконечно много пар таких взаимно простых целых чисел $x, y$, что $\left|x-y\sqrt{N}\right|<\frac{1}{y}$, где $y>0$. Тогда

$$\left|x+y\sqrt{N}\right|=\left|x-y\sqrt{N}+2y\sqrt{N}\right|<\left|x-y\sqrt{N}\right|+2y\sqrt{N}<\frac{1}{y}+2y\sqrt{N}.$$

Отсюда

$$\left|x^2-Ny^2\right|=\left|x-y\sqrt{N}\right|\cdot\left|x+y\sqrt{N}\right|<\frac{1}{y}\cdot\left(\frac{1}{y}+2y\sqrt{N}\right)\le 1+2\sqrt{N}.$$

Полагая $c=1+2\sqrt{N}$, получаем утверждение леммы. □

Теорема 3.9. Уравнение (3.10) имеет бесконечно много решений в целых числах. Кроме того, существует такое решение $(x_1, y_1)$, что каждое другое решение $(x_k, y_k)$ задается соотношением

$$x_k+y_k\sqrt{N}=\pm(x_1+y_1\sqrt{N})^k. \tag{3.11}$$

*Доказательство* [1]. Согласно лемме 3.8, существует такое целое число $m$, что равенство $x^2 - Ny^2 = m$ выполняется для бесконечного числа пар целых чисел $x$, $y$, где $y > 0$. Будем предполагать, что все значения $x$ различны. Поскольку число классов вычетов по модулю $|m|$ конечно, найдутся такие пары $(x_1, y_1)$, $(x_2, y_2)$, что $x_1 \equiv x_2 \pmod{|m|}$, $y_1 \equiv y_2 \pmod{|m|}$.

Рассмотрим частные

$$\frac{x_2 \pm y_2\sqrt{N}}{x_1 \pm y_1\sqrt{N}} = \frac{(x_1 \mp y_1\sqrt{N})(x_2 \pm y_2\sqrt{N})}{x_1^2 - Ny_1^2} = \frac{(x_1x_2 - Ny_1y_2) \pm (x_1y_2 - x_2y_1)\sqrt{N}}{m}.$$

Заметим, что

$$x_1x_2 - Ny_1y_2 \equiv x_1^2 - Ny_1^2 \equiv 0 \pmod{|m|}, \quad x_1y_2 - x_2y_1 \equiv 0 \pmod{|m|},$$

значит, $x = \dfrac{x_1x_2 - Ny_1y_2}{m}$, $y = \dfrac{x_1y_2 - x_2y_1}{m}$ — целые числа.

Тогда

$$x^2 - Ny^2 = (x - y\sqrt{N})(x + y\sqrt{N}) = \frac{x_2 - y_2\sqrt{N}}{x_1 - y_1\sqrt{N}} \cdot \frac{x_2 + y_2\sqrt{N}}{x_1 + y_1\sqrt{N}} =$$
$$= \frac{x_2^2 - Ny_2^2}{x_1^2 - Ny_1^2} = \frac{m}{m} = 1.$$

Таким образом, пара $(x, y)$ является решением уравнения Пелля.

Проверим, что $y \neq 0$. Действительно, при $y = 0$ получаем $x = \pm 1$ и

$$(x_1 - y_1\sqrt{N})(x_2 + y_2\sqrt{N}) = \pm m.$$

Умножая обе части этого равенства на $x_2 - y_2\sqrt{N}$, получаем

$$(x_1 - y_1\sqrt{N}) \cdot m = \pm m \cdot (x_2 - y_2\sqrt{N}),$$
$$x_1 - y_1\sqrt{N} = \pm(x_2 - y_2\sqrt{N}),$$

то есть $x_1 = x_2$. Противоречие.

Упорядочим множество решений уравнения Пелля: будем говорить, что решение $(x, y)$ больше, чем решение $(u, v)$, если

$x+y\sqrt{N}>u+v\sqrt{N}$. Пусть $(x_1, y_1)$ — наименьшее решение с положительными $x_1$, $y_1$ (оно называется *фундаментальным*). Покажем, что для любого другого решения $(u, v)$ с положительными $u$, $v$ выполняется равенство $u+v\sqrt{N}=(x_1+y_1\sqrt{N})^k$ для некоторого целого числа $k$. Выберем целое число $k$ так, чтобы

$$(x_1+y_1\sqrt{N})^k<u+v\sqrt{N}<(x_1+y_1\sqrt{N})^{k+1}.$$

Тогда

$$1<(x_1-y_1\sqrt{N})^k(u+v\sqrt{N})<x_1+y_1\sqrt{N},$$

поскольку $x_1-y_1\sqrt{N}=\dfrac{1}{x_1+y_1\sqrt{N}}$.

Обозначим $U+V\sqrt{N}=(x_1-y_1\sqrt{N})^k(u+v\sqrt{N})$. Пара $(U, V)$ является решением уравнения Пелля, причем $1<U+V\sqrt{N}<x_1+y_1\sqrt{N}$. Так как $U+V\sqrt{N}>0$ и $U-V\sqrt{N}=\dfrac{1}{U+V\sqrt{N}}>0$, получаем $U>0$. Кроме того, $U-V\sqrt{N}=\dfrac{1}{U+V\sqrt{N}}<1$, то есть $V\sqrt{N}>U-1\geq 0$ и $V>0$. Получили решение $(U, V)$ с положительными $U$, $V$, меньшее, чем фундаментальное. Противоречие.

Если решение $(u, v)$ уравнения Пелля таково, что $u>0$, $v<0$, то

$$\frac{1}{u+v\sqrt{N}}=u-v\sqrt{N}=(x_1+y_1\sqrt{N})^k$$

для некоторого целого $k$ (поскольку $-v>0$) и $u+v\sqrt{N}=(x_1+y_1\sqrt{N})^{-k}$.

При $u<0$, $v>0$ и $u<0$, $v<0$ получаем $-(x_1+y_1\sqrt{N})^{\pm k}$ для $k\in\mathbb{Z}$. □

Фундаментальное решение можно найти, раскладывая $\sqrt{N}$ в непрерывную дробь (*метод Браункера*) [2]: если $\frac{P_k}{Q_k}$ — подходящие дроби для непрерывной дроби

$$\sqrt{N} = [a_0; \{a_1, a_2, \ldots, a_n, 2a_0\}],$$

то при нечетном $n$ решением будет пара $(P_n, Q_n)$, при четном $n$ — пара $(P_{2n+1}, Q_{2n+1})$.

Пример 3.14. Решим уравнение $x^2 - 34y^2 = 1$. Раскладываем число $\sqrt{34}$ в непрерывную дробь:

$$\sqrt{34} = 5 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{10 + \ddots}}}},$$

то есть $a_0 = 5$, $a_1 = 1$, $a_2 = 4$, $a_3 = 1$ и $n = 3$ — нечетное число. Вычисляем подходящие дроби: $\frac{P_0}{Q_0} = \frac{5}{1}$, $\frac{P_1}{Q_1} = \frac{6}{1}$, $\frac{P_2}{Q_2} = \frac{29}{5}$, $\frac{P_3}{Q_3} = \frac{35}{6}$. Значит, $x_1 = 35$, $y_1 = 6$.

Проверка: $35^2 - 34 \cdot 6^2 = 1225 - 1224 = 1$.

Решениями будут также пары (2449, 420), (171395, 29394), (11995201, 2057160), (839492675, 143971806), ..., определяемые из соотношения (3.11). □

Пример 3.15. Решим уравнение $x^2 - 29y^2 = 1$. Раскладываем число $\sqrt{29}$ в непрерывную дробь:

$$\sqrt{29} = 5 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{10 + \ddots}}}}},$$

то есть $a_0 = 5$, $a_1 = 2$, $a_2 = a_3 = 1$, $a_4 = 2$ и $n = 4$ — четное число, $2n + 1 = 9$. Вычисляем подходящие дроби:

$$\frac{P_0}{Q_0} = \frac{5}{1}, \quad \frac{P_1}{Q_1} = \frac{11}{2}, \quad \frac{P_2}{Q_2} = \frac{16}{3}, \quad \frac{P_3}{Q_3} = \frac{27}{5}, \quad \frac{P_4}{Q_4} = \frac{70}{13}, \quad \frac{P_5}{Q_5} = \frac{727}{135},$$
$$\frac{P_6}{Q_6} = \frac{1524}{283}, \quad \frac{P_7}{Q_7} = \frac{2251}{418}, \quad \frac{P_8}{Q_8} = \frac{3775}{701}, \quad \frac{P_9}{Q_9} = \frac{9801}{1820}.$$

Значит, $x_1 = 9801$, $y_1 = 1820$.

Проверка: $9801^2 - 29 \cdot 1820^2 = 96059601 - 96059600 = 1$.

Решениями будут также пары

(192119201, 35675640),

(3765920568201, 699313893460),

(73819574785756801, 13707950903927280),

(1447011301184484245001, 268703252919468649100), ...,

определяемые из соотношения (3.11). □

### 3.4.3. Представление числа в виде суммы квадратов

Теорема 3.10 (Эрмит). Любой делитель $d$ числа $a^2 + 1$, где $a \in \mathbb{Z}$, можно представить в виде суммы двух квадратов.

*Доказательство* [4]. Разложим рациональное число $\frac{a}{d}$ в обыкновенную непрерывную дробь. Согласно следствию из теоремы 3.1, последовательность знаменателей подходящих дробей $1 = Q_1 < Q_2 < \ldots < Q_n = d$ монотонно возрастает (последнее равенство выполняется, поскольку числа $a$ и $d$ взаимно простые). Пусть число $k$, $1 \le k \le n$, таково, что

$$Q_k \le \sqrt{d} \le Q_{k+1}, \tag{3.12}$$

причем хотя бы одно из этих неравенств строгое.

Согласно следствию из теоремы 3.4, справедливо неравенство

$$\left|\frac{a}{d} - \frac{P_k}{Q_k}\right| \le \frac{1}{Q_k Q_{k+1}},$$

то есть существует такое число $\varepsilon \le 1$, что $\left|\frac{a}{d} - \frac{P_k}{Q_k}\right| = \frac{\varepsilon}{Q_k Q_{k+1}}$. Перепишем последнее равенство:

$$|aQ_k - dP_k| = \frac{\varepsilon d}{Q_{k+1}}.$$

Оценивая $Q_{k+1}$ по формуле (3.12), получаем

$$|aQ_k - dP_k| \le \frac{\varepsilon d}{\sqrt{d}} = \varepsilon\sqrt{d} \le \sqrt{d},$$

значит, $(aQ_k - dP_k)^2 \le d$.

Оценивая $Q_k$ по формуле (3.12), получаем $Q_k^2 \le d$, причем хотя бы одно из двух последних неравенств строгое. Складывая их, получаем строгое неравенство

$$0 < (aQ_k - dP_k)^2 + Q_k^2 = (a^2+1)Q_k^2 - 2adP_kQ_k + d^2P_k^2 < 2d.$$

Сумма $(a^2+1)Q_k^2 - 2adP_kQ_k + d^2P_k^2$ делится на $d$ (поскольку каждое ее слагаемое делится на $d$) и строго меньше $2d$, а значит, в точности равна $d$. Отсюда

$$(aQ_k - dP_k)^2 + Q_k^2 = d$$

— представили делитель в виде суммы двух квадратов. □

Пример 3.16. Пусть $a = 7949$, тогда

$$a^2 + 1 = 63186602 = 2 \cdot 37 \cdot 853873.$$

Пусть $d = 853873$. Раскладываем рациональное число $\frac{a}{d}$ в обыкновенную непрерывную дробь:

$$\frac{7949}{853873} = [0; 107, 2, 2, 1, 1, 2, 2, 107].$$

Вычисляем подходящие дроби, пока не получим выполнение условия (3.12) для $\sqrt{d} = \sqrt{853873} \approx 924{,}052$:

$$\frac{P_1}{Q_1} = \frac{0}{1}, \quad \frac{P_2}{Q_2} = \frac{1}{107}, \quad \frac{P_3}{Q_3} = \frac{2}{215}, \quad \frac{P_4}{Q_4} = \frac{5}{537}, \quad \frac{P_5}{Q_5} = \frac{7}{752}, \quad \frac{P_6}{Q_6} = \frac{19}{2041}.$$

Таким образом, $k = 5$ и искомое представление имеет вид

$$853873 = (aQ_5 - dP_5)^2 + Q_5^2 =$$

$$= (7949 \cdot 752 - 853873 \cdot 7)^2 + 752^2 = 537^2 + 752^2.$$

Аналогично получаем для других делителей числа 63186602:

| $d$ | $\frac{a}{d}$ | $k$ | $P_k$ | $Q_k$ | $Q_{k+1}$ | $(aQ_k - dP_k)^2 + Q_k^2$ |
|---|---|---|---|---|---|---|
| 2 | [3974; 2] | 1 | 3974 | 1 | 2 | $1^2 + 1^2$ |
| 37 | [214; 1, 5, 6] | 2 | 1289 | 6 | 37 | $1^2 + 6^2$ |
| $2 \cdot 37$ | [107; 2, 2, 1, 1, 2, 2] | 4 | 752 | 7 | 12 | $(-5)^2 + 7^2$ |
| $2 \cdot 853873$ | [0; 214, 1, 5, 5, 1, 214] | 4 | 6 | 1289 | 6660 | $(-215)^2 + 1289^2$ |
| $37 \cdot 853873$ | [0; 3974, 1, 1, 3974] | 3 | 1 | 3975 | 7949 | $3974^2 + 3975^2$ |

□

### 3.5. Разложение функций в непрерывные дроби

Непрерывные дроби можно использовать для представления и вычисления функций.

По аналогии с рациональными числами рациональные функции раскладываются в конечные непрерывные дроби. Разложим в непрерывную дробь рациональную функцию

$$f(x)=\frac{c_{10}+c_{11}x+c_{12}x^2+\ldots+c_{1n}x^n}{c_{00}+c_{01}x+c_{02}x^2+\ldots+c_{0n}x^n}.$$

Производя элементарные преобразования, получаем:

$$f(x)=\frac{1}{\dfrac{c_{00}}{c_{10}}+\dfrac{c_{00}+c_{01}x+c_{02}x^2+\ldots+c_{0n}x^n}{c_{10}+c_{11}x+c_{12}x^2+\ldots+c_{1n}x^n}-\dfrac{c_{00}}{c_{10}}}=\frac{c_{10}}{c_{00}+xf_1(x)},$$

где

$$f_1(x)=\frac{c_{20}+c_{21}x+c_{22}x^2+\ldots+c_{2n}x^n}{c_{10}+c_{11}x+c_{12}x^2+\ldots++c_{1n}x^n}$$

и

$$c_{2k}=c_{10}c_{0,k+1}-c_{00}c_{1,k+1},\quad k=0,\,1,\,\ldots.$$

Аналогично

$$f_1(x)=\frac{c_{20}}{c_{10}+xf_2(x)},$$

где

$$f_2(x)=\frac{c_{30}+c_{31}x+c_{32}x^2+\ldots+c_{3n}x^n}{c_{20}+c_{21}x+c_{22}x^2+\ldots+c_{2n}x^n}$$

и

$$c_{3k}=c_{20}c_{1,k+1}-c_{10}c_{2,k+1},\quad k=0,\,1,\,\ldots,$$

и т. д. Таким образом,

$$f(x)=\cfrac{c_{10}}{c_{00}+\cfrac{c_{20}x}{c_{10}+\cfrac{c_{30}x}{c_{20}+\ddots+c_{n-1,0}+\cfrac{c_{n0}x}{c_{n-1,0}}}}}=\left[0;\frac{c_{10}}{c_{00}},\frac{c_{20}x}{c_{10}},\frac{c_{30}x}{c_{20}},\ldots,\frac{c_{n0}x}{c_{n-1,0}}\right].$$

Коэффициенты $c_{jk}$ можно вычислять как определитель

$$c_{jk}=-\begin{vmatrix}c_{j-2,0} & c_{j-2,k+1}\\ c_{j-1,0} & c_{j-1,k+1}\end{vmatrix},\quad j\geq 2.$$

Пример 3.17. Разложим в непрерывную дробь функцию

$$f(x)=\frac{1-3x+2x^2}{1+4x+5x^2-6x^3}.$$

Коэффициенты $c_{jk}$ запишем в таблицу:

| | $k$ | | | |
|---|---|---|---|---|
| $j$ | 0 | 1 | 2 | 3 |
| 0 | 1 | 4 | 5 | –6 |
| 1 | 1 | –3 | 2 | 0 |
| 2 | 7 | 3 | –6 | 0 |
| 3 | –24 | 20 | 0 | 0 |
| 4 | –212 | 144 | 0 | 0 |
| 5 | –784 | 0 | 0 | 0 |
| 6 | –112896 | 0 | 0 | 0 |

Следовательно,

$$\frac{1-3x+2x^2}{1+4x+5x^2-6x^3}=\left[0;\frac{1}{1},\frac{7x}{1},\frac{-24x}{7},\frac{-212x}{-24},\frac{-784x}{-212},\frac{-112896x}{-784}\right]=$$

$$=\cfrac{1}{1+\cfrac{7x}{1-\cfrac{24x}{7-\cfrac{212x}{-24-\cfrac{784x}{-212+144x}}}}}. \qquad \square$$

Если функция $f(x)$ раскладывается в бесконечную непрерывную дробь, то в общем случае нужно доказать сходимость этой дроби и убедиться, что предельное значение подходящих дробей равно $f(x)$.

Раскладывая функцию в непрерывную дробь, можно вычислять приближенное значение этой функции.

Пример 3.18. Для функции $e^x$ известно разложение в непрерывную дробь, полученное Эйлером:

$$e^x = \left[0; \frac{1}{1}, \frac{-2x}{2+x}, \frac{x^2}{6}, \frac{x^2}{10}, \ldots, \frac{x^2}{4n+2}, \ldots\right],$$

сходящееся для любого $x$, вещественного или комплексного [3].

Вычислим для этой функции подходящие дроби:

$$\frac{P_1}{Q_1} = \frac{1}{1}, \quad \frac{P_2}{Q_2} = \frac{2+x}{2-x}, \quad \frac{P_3}{Q_3} = \frac{12+6x+x^2}{12-6x+x^2}, \quad \frac{P_4}{Q_4} = \frac{120+60x+12x^2+x^3}{120-60x+12x^2-x^3},$$

$$\frac{P_5}{Q_5} = \frac{1680+840x+180x^2+20x^3+x^4}{1680-840x+180x^2-20x^3+x^4}, \ldots$$

При $x = 1$ пятая подходящая дробь дает $e \approx \frac{2721}{1001} = 2{,}71828\ldots$ □

## Упражнения к главе 3

1. Разложить в непрерывную дробь числа: $\frac{1}{3}$; $\frac{2}{3}$; 3,14159; 3,14160; $\frac{51}{11}$; $\frac{1725}{1193}$; $\frac{1193}{1725}$; $-\frac{1193}{1725}$; $\frac{30031}{16579}$; $\frac{1103}{87}$. Для каждого разложения найти подходящие дроби.

2. Разложить в непрерывную дробь числа $\sqrt{5}$, $\frac{1}{\sqrt{5}}$, $2-\frac{1}{\sqrt{5}}$. Для каждого разложения найти первые пять подходящих дробей.

3. Разложить в непрерывную дробь числа $\sqrt{n^2+1}$, $\sqrt{n^2+2}$, где число $n$ натуральное.

4. Доказать, что для обыкновенной непрерывной дроби $[0; a, a, \ldots, a]$ справедливо тождество $P_n^2 + P_{n+1}^2 = P_{n-1}P_{n+1} + P_nP_{n+2}$.

5. Доказать, что если обыкновенная непрерывная дробь $[a_0; a_1, a_2, \ldots, a_n]$ является симметрической ($a_0 = a_n$, $a_1 = a_{n-1}$, …), то $P_{n-1} = Q_n$.

6. Доказать, что разложение числа $\frac{F_{n-3}}{F_n}$, где $F_n$ — число Фибоначчи, в непрерывную дробь имеет вид $\left[0; \frac{1}{4}, \frac{1}{4}, \ldots, a_k\right]$, где $k = m + 1$, $a_k = 0$, если $n = 3m$; $a_k = \frac{1}{3}$, если $n = 3m + 1$; $a_k = \frac{1}{5}$, если $n = 3m + 2$.

7. С помощью непрерывных дробей найти все целые решения уравнения: а) $85x - 53y = 5$; б) $41x - 11y = 7$.

8. Решить уравнение Пелля $x^2 - Ny^2 = 1$ для $N = 5, 6, 8, 11, 12, 13, 31, 83$.

9. Доказать тождества:

$$\text{а)}\ \left(\frac{1}{1+\frac{1}{1+\ddots}}\right)^3 = \frac{1}{4+\frac{1}{4+\ddots}};\ \text{б)}\ \left(\frac{1}{1+\frac{1}{1+\ddots}}\right)^2 = \frac{1}{3-\frac{1}{3-\ddots}}.$$

10. Разложить в непрерывную дробь функцию:

$$\text{а)}\ \frac{2+x}{1-3x+5x^2};\ \text{б)}\ \frac{1-2x+3x^2}{1+2x-x^2+x^3};\ \text{в)}\ \frac{3+x+4x^2+x^3}{1-2x+x^2-x^3+2x^4}.$$

## Литература к главе 3


1. *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел. — М.: Мир, 1987.
2. *Гашков С. Б., Чубариков В. Н.* Арифметика, алгоритмы, сложность вычислений. — М.: Высшая школа, 2000.
3. *Демидович Б. П., Марон И. А.* Основы вычислительной математики. — М.: Наука, 1970.
4. *Сизый С. В.* Лекции по теории чисел: Учебное пособие для математических специальностей. — Екатеринбург: Уральский государственный университет им. А. М. Горького, 1999. Доступно с http://virlib.eunnet.net/books/numbers/.
5. *Хинчин А. Я.* Цепные дроби. — М.: Наука, 1978.

## Глава 4

# АРИФМЕТИЧЕСКИЕ ОПЕРАЦИИ НАД ЦЕЛЫМИ ЧИСЛАМИ И ПОЛИНОМАМИ

Алгоритмы арифметики целых чисел и полиномов во многом похожи, поскольку представление целого числа $a$ в системе счисления с основанием $B$ в виде $a = a_{n-1}B^{n-1} + a_{n-2}B^{n-2} + \ldots + a_1B + a_0$, где $0 \le a_i < B$, аналогично представлению полинома $a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0$ с коэффициентами $0 \le u_i < B$.

## 4.1. Сложение и вычитание

Операции сложения и вычитания для чисел и полиномов выполняются практически одинаково. Отличие заключается в том, что при сложении (вычитании) чисел возникает перенос в следующий разряд, а при операциях над полиномами перенос отсутствует.

Пусть неотрицательные целые числа $a$ и $b$ заданы в системе счисления с основанием $B$:

$$a = (a_{n-1}, a_{n-2}, \ldots, a_0)_B = a_{n-1}B^{n-1} + a_{n-2}B^{n-2} + \ldots + a_1B + a_0,$$

$$b = (b_{n-1}, b_{n-2}, \ldots, b_0)_B = b_{n-1}B^{n-1} + b_{n-2}B^{n-2} + \ldots + b_1B + b_0,$$

где $0 \le a_i, b_i < B$. Для удобства считаем, что оба числа имеют равную длину, при необходимости старшие разряды меньшего числа заполняем нулями.

Сложение выполняется «в столбик».

Алгоритм 4.1. Сложение целых чисел [2].

*Вход*. Целые числа $a = (a_{n-1}, a_{n-2}, \ldots, a_0)_B$, $b = (b_{n-1}, b_{n-2}, \ldots, b_0)_B$.

*Выход*. Сумма $c = a + b = (c_n, c_{n-1}, \ldots, c_0)_B$.

1. Положить $s \leftarrow 0$.
2. Для $i = 0, 1, \ldots, n-1$ выполнить следующие действия.

2.1. Вычислить $t \leftarrow a_i + b_i + s$.

2.2. Положить $s \leftarrow \left[\frac{t}{B}\right]$, $c_i \leftarrow t \pmod B$.

3. Положить $c_n \leftarrow s$.

4. Результат: $c = (c_n, c_{n-1}, \ldots, c_0)_B$. □

Переменная $s$ означает перенос в старший разряд и всегда принимает значение 0 (при $a_i + b_i + s < b$) или 1 (при $a_i + b_i + s \geq b$). На шаге 2.1 может произойти не более одного переноса. Действительно,

$$a_i + b_i + 1 \leq (B - 1) + (B - 1) + 1 = 2B - 1 < 2B.$$

Сложность алгоритма 4.1 равна $O(n)$.

Пример 4.1. Вычислим сумму чисел

$$a = (\text{abc8071d})_{16},\ b = (\text{7835e39f})_{16}.$$

В обозначениях алгоритма 4.1 имеем $B = 16$, $n = 8$. Промежуточные выкладки сведем в таблицу:

| $i$ | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|---|
| $a_i$ | | $a_{16}$ | $b_{16}$ | $c_{16}$ | $8_{16}$ | $0_{16}$ | $7_{16}$ | $1_{16}$ | $d_{16}$ |
| $b_i$ | | $7_{16}$ | $8_{16}$ | $3_{16}$ | $5_{16}$ | $e_{16}$ | $3_{16}$ | $9_{16}$ | $f_{16}$ |
| $t$ | | $12_{16}$ | $13_{16}$ | $f_{16}$ | $d_{16}$ | $e_{16}$ | $a_{16}$ | $b_{16}$ | $1c_{16}$ |
| $s$ | | $1_{16}$ | $1_{16}$ | $0_{16}$ | $0_{16}$ | $0_{16}$ | $0_{16}$ | $0_{16}$ | $1_{16}$ |
| $c_i$ | $1_{16}$ | $2_{16}$ | $3_{16}$ | $f_{16}$ | $d_{16}$ | $e_{16}$ | $a_{16}$ | $b_{16}$ | $c_{16}$ |

Таким образом, искомая сумма $c = (\text{123fdeabc})_{16}$. □

Алгоритм сложения полиномов с целыми коэффициентами аналогичен, но переносов здесь нет, и степень полинома, задающего сумму, совпадает со степенью слагаемых.

Пример 4.2. Найдем сумму полиномов

$$a(x) = 7x^5 + 2x^3 - 3x^2 + x + 5,\ b(x) = -2x^3 + 5x^2 - 4x - 2.$$

Поскольку $\deg(b) < \deg(a)$, представим полином $b(x)$ в виде $b(x) = 0x^5 + 0x^4 - 2x^3 + 5x^2 - 4x - 2$. Тогда суммой будет полином

$$c(x) = 7x^5 + 0x^4 + 0x^3 + 2x^2 - 3x + 3 = 7x^5 + 2x^2 - 3x + 3. \qquad \square$$

Алгоритмы вычисления разности целых чисел и полиномов похожи на соответствующие алгоритмы вычисления суммы.

Алгоритм 4.2. Вычитание целых чисел [2].

*Вход*. Целые числа $a = (a_{n-1}, a_{n-2}, \ldots, a_0)_B$, $b = (b_{n-1}, b_{n-2}, \ldots, b_0)_B$, $0 < b \le a$.

*Выход*. Разность $c = a - b = (c_{n-1}, c_{n-2}, \ldots, c_0)_B$.

1. Положить $s \leftarrow 0$.
2. Для $i = 0, 1, \ldots, n-1$ выполнить следующие действия.
   2.1. Вычислить $t \leftarrow a_i - b_i + s$.
   2.2. Положить $s \leftarrow \left[\dfrac{t}{B}\right]$, $c_i \leftarrow t \pmod B$.
3. Результат: $c = (c_{n-1}, c_{n-2}, \ldots, c_0)_B$. $\square$

Переменная $s$ принимает значение $-1$ или $0$ в зависимости от того, «занимаем» ли мы из старшего разряда (то есть выполняется ли неравенство $a_i - b_i + s < 0$). По окончании работы алгоритма должно выполняться равенство $s = 0$ (равенство $s = -1$ возможно тогда и только тогда, когда $a < b$, что противоречит условию).

Сложность алгоритма 4.2 равна $O(n)$.

Пример 4.3. Найдем разность чисел

$$a = (\text{abc8071d})_{16},\ b = (7835\text{e}39\text{f})_{16}.$$

В обозначениях алгоритма 4.2 $B = 16$, $n = 8$. Промежуточные выкладки сведем в таблицу:

| | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| $a_i$ | $a_{16}$ | $b_{16}$ | $c_{16}$ | $8_{16}$ | $0_{16}$ | $7_{16}$ | $1_{16}$ | $d_{16}$ |
| $b_i$ | $7_{16}$ | $8_{16}$ | $3_{16}$ | $5_{16}$ | $e_{16}$ | $3_{16}$ | $9_{16}$ | $f_{16}$ |
| $t$ | $3_{16}$ | $3_{16}$ | $9_{16}$ | $2_{16}$ | $-e_{16}$ | $3_{16}$ | $-9_{16}$ | $-2_{16}$ |
| $s$ | $0_{16}$ | $0_{16}$ | $0_{16}$ | $0_{16}$ | $-1_{16}$ | $0_{16}$ | $-1_{16}$ | $-1_{16}$ |
| $c_i$ | $3_{16}$ | $3_{16}$ | $9_{16}$ | $2_{16}$ | $2_{16}$ | $3_{16}$ | $7_{16}$ | $e_{16}$ |

Таким образом, искомая разность $c = (3392237e)_{16}$. □

Вычитание полиномов выполняется аналогично.

## 4.2. Умножение

Операция умножения является одной из наиболее трудоемких и вместе с функцией деления определяет время работы многих вычислительных алгоритмов.

### 4.2.1. Умножение «в столбик». Возведение в квадрат

Пусть неотрицательные целые числа $a$ и $b$ заданы в системе счисления с основанием $B$:

$$a = (a_{n-1}, a_{n-2}, \ldots, a_0)_B = a_{n-1}B^{n-1} + a_{n-2}B^{n-2} + \ldots + a_1B + a_0,$$

$$b = (b_{n-1}, b_{n-2}, \ldots, b_0)_B = b_{n-1}B^{n-1} + b_{n-2}B^{n-2} + \ldots + b_1B + b_0,$$

где $0 \le a_i < B$, $0 \le b_i < B$.

Самый очевидный способ умножения — умножение «в столбик».

Алгоритм 4.3. Умножение целых чисел «в столбик» [2].

*Вход*. Целые числа $a = (a_{n-1}, a_{n-2}, \ldots, a_0)_B$, $b = (b_{n-1}, b_{n-2}, \ldots, b_0)_B$, $0 < b \le a$.

*Выход*. Произведение $c = ab = (c_{2n-1}, c_{2n-2}, \ldots, c_0)_B$.

1. Для $i = 0, 1, \ldots, n-1$ положить $c_i \leftarrow 0$.
2. Для $i = 0, 1, \ldots, n-1$ выполнить следующие действия.

2.1. Для $j = 0, 1, \ldots, n-1$:

2.1.1. Положить $s \leftarrow 0$.

2.1.2. Вычислить $t \leftarrow c_{i+j} + a_i b_j + s$, $c_{i+j} \leftarrow t \pmod B$, $s \leftarrow \left[\frac{t}{B}\right]$.

2.2. Положить $c_{i+n} \leftarrow s$.

3. Результат: $c = (c_{2n-1}, c_{2n-2}, \ldots, c_0)_B$. □

Во внешнем цикле этого алгоритма вычисляются частичные произведения $a_i(b_{n-1}, b_{n-2}, \ldots, b_0)_B$, а во внутреннем — произведения $a_i b_j$, где $j = 0, 1, \ldots, n-1$. Текущий разряд произведения равен $t \pmod B$, а очередной перенос: $s \leftarrow \left[\frac{t}{B}\right]$. При этом на шаге 2.1.2 выполняется неравенство

$$c_{i+j} + a_i b_j + s \le B - 1 + (B-1)(B-1) + B - 1 =$$

$$= (B-1)B + B - 1 = B^2 - 1 < B^2.$$

Сложность умножения «в столбик» равна $O(n^2)$.

Пример 4.4. Найдем произведение чисел $a = (1, 129, 205)_{256}$, $b = (0, 91, 160)_{256}$, заданных в системе счисления с основанием 256. В обозначениях алгоритма 4.3 имеем $B = 256$, $n = 3$. Результаты вычислений запишем в таблицу:

| $i$ | $j$ | $t$ | $c_{i+j}$ | $s$ | $c_{i+n}$ |
|---|---|---|---|---|---|
| 0 | 0 | $c_0 + a_0 b_0 + s = (128, 32)_{256}$ | $(\mathbf{32})_{256}$ | $(128)_{256}$ | |
| | 1 | $c_1 + a_0 b_1 + s = (73, 95)_{256}$ | $(95)_{256}$ | $(73)_{256}$ | |
| | 2 | $c_2 + a_0 b_2 + s = (73)_{256}$ | $(73)_{256}$ | $0_{256}$ | $0_{256}$ |
| 1 | 0 | $c_1 + a_1 b_0 + s = (80, 255)_{256}$ | $(\mathbf{255})_{256}$ | $(80)_{256}$ | |
| | 1 | $c_2 + a_1 b_1 + s = (46, 116)_{256}$ | $(116)_{256}$ | $(46)_{256}$ | |

| $i$ | $j$ | $t$ | $c_{i+j}$ | $s$ | $c_{i+n}$ |
|---|---|---|---|---|---|
| | 2 | $c_3 + a_1b_2 + s = (46)_{256}$ | $(46)_{256}$ | $0_{256}$ | $0_{256}$ |
| 2 | 0 | $c_2 + a_2b_0 + s = (1, 20)_{256}$ | $(\mathbf{20})_{256}$ | $1_{256}$ | |
| | 1 | $c_3 + a_2b_1 + s = (138)_{256}$ | $(\mathbf{138})_{256}$ | $0_{256}$ | |
| | 2 | $c_4 + a_2b_2 + s = 0_{256}$ | $0_{256}$ | $0_{256}$ | $0_{256}$ |

Таким образом, $c = ab = (138, 20, 255, 32)_{256}$. □

При возведении числа в квадрат с использованием алгоритма умножения «в столбик» для числа $a = (a_{n-1}, a_{n-2}, \ldots, a_0)_B$ получаем

$$c = a^2 = \sum_{i,j=0}^{n-1} a_i a_j B^{i+j} = 2\sum_{i=0}^{n-2}\sum_{j=i+1}^{n-1} a_i a_j B^{i+j} + \sum_{j=0}^{n-1} a_i^2 B^{2i},$$

то есть число элементарных умножений по сравнению с алгоритмом умножения сокращается с $n^2$ до $\dfrac{n(n+1)}{2}$.

Алгоритм 4.4. Возведение целого числа в квадрат [2].

*Вход*. Целое положительное число $a = (a_{n-1}, a_{n-2}, \ldots, a_0)_B$.

*Выход*. Значение $c = a^2 = (c_{2n-1}, c_{2n-2}, \ldots, c_0)_B$.

1. Для $i = 0, 1, \ldots, n-1$ положить $c_i \leftarrow 0$.
2. Для $i = 0, 1, \ldots, n-1$ выполнить следующие действия.

   2.1. Положить $t \leftarrow c_{2i} + a_i^2$, $c_{2i} \leftarrow t \pmod B$ и $s \leftarrow \left[\dfrac{t}{B}\right]$.

   2.2. Для $j = i+1,\ i+2,\ \ldots,\ n-1$ вычислить $t \leftarrow c_{i+j} + 2a_ia_j + s$, $c_{i+j} \leftarrow t \pmod B$ и $s \leftarrow \left[\dfrac{t}{B}\right]$.

   2.3. Положить $c_{i+n} \leftarrow s$.
3. Результат: $c = (c_{2n-1}, c_{2n-2}, \ldots, c_0)_B$. □

На шаге 2.2 алгоритма выполняется неравенство

$$c_{i+j} + 2a_ia_j + s \le (B-1) + 2(B-1)^2 + (B-1) = 2B^2 - 2B < 2B^2 - 1,$$

то есть величина $t$ может занимать более двух разрядов в системе счисления с основанием $B$.

Пример 4.5. Возведем в квадрат число $a = (8bca)_{16}$. В обозначениях алгоритма 4.4 $B = 16$, $n = 4$. Результаты вычислений запишем в таблицу (разряды $c_i$, которые на последующих шагах не меняются, выделены):

| $i$ | $j$ | $t$ | $c_{2i}$ | $c_{i+j}$ | $s$ | $c_{i+n}$ |
|---|---|---|---|---|---|---|
| 0 | | $c_0 + a_0^2 = (64)_{16}$ | $4_{16}$ | | $6_{16}$ | |
| | 1 | $c_1 + 2a_0a_1 + s = (f6)_{16}$ | | $6_{16}$ | $f_{16}$ | |
| | 2 | $c_2 + 2a_0a_2 + s = (eb)_{16}$ | | $b_{16}$ | $e_{16}$ | |
| | 3 | $c_3 + 2a_0a_3 + s = (ae)_{16}$ | | $e_{16}$ | $a_{16}$ | $a_{16}$ |
| 1 | | $c_2 + a_1^2 = (9b)_{16}$ | $b_{16}$ | | $9_{16}$ | |
| | 2 | $c_3 + 2a_1a_2 + s = (11f)_{16}$ | | $f_{16}$ | $(11)_{16}$ | |
| | 3 | $c_4 + 2a_1a_3 + s = (db)_{16}$ | | $b_{16}$ | $d_{16}$ | $d_{16}$ |
| 2 | | $c_4 + a_2^2 = (84)_{16}$ | $4_{16}$ | | $8_{16}$ | |
| | 3 | $c_5 + 2a_2a_3 + s = (c5)_{16}$ | | $5_{16}$ | $c_{16}$ | $c_{16}$ |
| 3 | | $c_6 + a_3^2 = (4c)_{16}$ | $c_{16}$ | | $4_{16}$ | $4_{16}$ |

Таким образом, $c = a^2 = (4c54fb64)_{16}$. □

### 4.2.2. Умножение методом Карацубы–Офмана

Этот метод был впервые предложен А.А. Карацубой в 1962 году для умножения полиномов. Пусть $a(x)$ и $b(x)$ — полиномы степени не более $2n-1$ с целыми коэффициентами. Для умножения этих полиномов представим их в виде

$$a(x) = a_1(x)x^n + a_0(x),\ b(x) = b_1(x)x^n + b_0(x),$$

где $\deg(a_1), \deg(a_0), \deg(b_1), \deg(b_0) \le n-1$.

При обычном умножении «в столбик» получаем:

$$a(x)b(x) = a_1(x)b_1(x)x^{2n} + (a_1(x)b_0(x) + a_0(x)b_1(x))x^n + a_0(x)b_0(x),$$

то есть требуется четыре умножения полиномов степени не выше $n-1$. Перепишем это же произведение иначе:

$$a(x)b(x) = a_1(x)b_1(x)x^{2n} +$$

$$+ ((a_1(x) + a_0(x))(b_1(x) + b_0(x)) - a_1(x)b_1(x) - a_0(x)b_0(x))x^n + a_0(x)b_0(x).$$

Здесь нужно всего лишь три умножения полиномов степени не выше $n-1$. Умножение полинома на $x^n$ выполняется сдвигом массива коэффициентов и имеет линейную от $n$ сложность. Асимптотическая сложность алгоритма при умножении полиномов степени $n$ равна $O(3^{[\log_2 n+1]}) = O(n^{\log_2 3}) \approx O(n^{1,585})$.

Умножение целых чисел происходит аналогично: вместо переменной $x$ нужно подставить $B$ — основание системы счисления, а при сложении чисел учитывать переносы.

Пример 4.6. Вычислим произведение чисел $a = (20, 226)_{256}$, $b = (24, 145)_{256}$ методом Карацубы–Офмана. Здесь $a_1 = 20$, $a_0 = 226$, $b_1 = 24$, $b_0 = 145$. Вычисляем: $a_0b_0 = 32770$, то есть младший разряд произведения равен 2, разряд переноса — 128. Далее: $(a_1 + a_0)(b_1 + b_0) = 246 \cdot 169 = 41574$, разряд произведения равен 102, разряд переноса — 162; $a_1b_1 = 20 \cdot 24 = 480$, разряд произведения равен 224, разряд переноса — 1. Получаем:

$$ab = (224 + 1 \cdot 256) \cdot 256^2 + ((102 + 162 \cdot 256) - (224 + 1 \cdot 256) -$$

$$- (2 + 128 \cdot 256)) \cdot 256 + (2 + 128 \cdot 256) =$$

$$= 1 \cdot 256^3 + (1 + 1 \cdot 256) \cdot 256^2 + 4 \cdot 256 + 2 = (2, 1, 4, 2)_{256}. \qquad \square$$

### 4.2.3. Умножение в классах вычетов

Алгоритм умножения в классах вычетов, предложенный А. Шенхаге (A. Schönhage), использует китайскую теорему об остатках.

Если целые числа $m_0, m_1, \ldots, m_{k-1}$ попарно взаимно просты, то каждому целому числу $a$, $0 \le a < M$, где $M = m_0 m_1 \ldots m_{k-1}$, единственным образом можно сопоставить набор элементов $a_0, a_1, \ldots, a_{k-1}$ классов вычетов по модулям $m_i$, где $a_i \equiv a \pmod{m_i}$, $0 \le i < k$.

Сумме, разности и произведению чисел по модулю $M$ соответствуют суммы, разности и произведения по модулям $m_i$. Если $a = (a_0, a_1, \ldots, a_{k-1})$, $b = (b_0, b_1, \ldots, b_{k-1})$, то $a + b \pmod{M} = (c_0, c_1, \ldots, c_{k-1})$, $a - b \pmod{M} = (d_0, d_1, \ldots, d_{k-1})$, $ab \pmod{M} = (e_0, e_1, \ldots, e_{k-1})$, где $c_i \equiv a_i + b_i \pmod{m_i}$, $d_i \equiv a_i - b_i \pmod{m_i}$, $e_i \equiv a_i b_i \pmod{m_i}$, $i = 0, 1, \ldots, k-1$.

Пример 4.7. Пусть $m_0 = 5$, $m_1 = 9$, $m_2 = 17$. Тогда $M = 765$. Пусть $a = 221 = (1, 5, 0)$, $b = 562 = (2, 4, 1)$.

Вычисляем сумму: $221 + 562 = 783 \equiv 18 \pmod{M}$ и

$$221 + 562 = (1 + 2, 5 + 4, 0 + 1) = (3, 0, 1).$$

Действительно, $18 \equiv 3 \pmod 5$, $18 \equiv 0 \pmod 9$, $18 \equiv 1 \pmod{17}$.

Вычисляем разность: $221 - 562 = -341 \equiv 424 \pmod{M}$ и

$$221 - 562 = (1 - 2, 5 - 4, 0 - 1) = (4, 1, 16).$$

Проверяем: $424 \equiv 4 \pmod 5$, $424 \equiv 1 \pmod 9$, $424 \equiv 16 \pmod{17}$.

Вычисляем произведение: $221 \cdot 562 = 124202 \equiv 272 \pmod{M}$ и

$$221 \cdot 562 = (1 \cdot 2, 5 \cdot 4, 0 \cdot 1) = (2, 2, 0).$$

Проверяем: $272 \equiv 2 \pmod 5$, $272 \equiv 2 \pmod 9$, $272 \equiv 0 \pmod{17}$. □

Наиболее трудоемкой операцией при вычислениях в классах вычетов является представление числа в классах вычетов и обратное восстановление по китайской теореме об остатках.

Таблица чисел $m_i$ фиксирована, поэтому можно заранее вычислить вспомогательные величины (см. формулу (2.5) в главе 2)

$$M_i = m_0 m_1 \ldots m_{i-1} m_{i+1} \ldots m_{k-1},$$

$$N_i \equiv M_i^{-1} \pmod{m_i}.$$

На практике число $k$ удобно выбирать так, чтобы оно было степенью двойки. Нахождение вычетов по модулям $m_i$ можно ускорить следующим образом: сначала вычислить произведения $m_0m_1$, $m_2m_3$, ..., $m_{k-2}m_{k-1}$, после этого — произведения $m_0m_1m_2m_3$, $m_4m_5m_6m_7$, ..., $m_{k-4}m_{k-3}m_{k-2}m_{k-1}$ и т. д., пока не получатся числа

$$m_0m_1\ldots m_{\frac{k}{2}-1}, \quad m_{\frac{k}{2}}m_{\frac{k}{2}+1}\ldots m_{k-1}.$$

Для нахождения $a = (a_0, a_1, \ldots, a_{k-1})$, где $a_i \equiv a \pmod{m_i}$, вычисляем

$$a_{0,1,\ldots,\frac{k}{2}-1} \equiv a \pmod{m_0m_1\ldots m_{\frac{k}{2}-1}},$$
$$a_{\frac{k}{2},\frac{k}{2}+1,\ldots,k-1} \equiv a \pmod{m_{\frac{k}{2}}m_{\frac{k}{2}+1}\ldots m_{k-1}},$$

затем

$$a_{0,1,\ldots,\frac{k}{4}-1} \equiv a_{0,1,\ldots,\frac{k}{2}-1} \pmod{m_0m_1\ldots m_{\frac{k}{4}-1}},$$
$$a_{\frac{k}{4},\frac{k}{4}+1,\ldots,\frac{k}{2}-1} \equiv a_{0,1,\ldots,\frac{k}{2}-1} \pmod{m_{\frac{k}{4}}m_{\frac{k}{4}+1}\ldots m_{\frac{k}{2}-1}},$$
$$a_{\frac{k}{2},\frac{k}{2}+1,\ldots,\frac{3k}{4}-1} \equiv a_{\frac{k}{2},\frac{k}{2}+1,\ldots,k-1} \pmod{m_{\frac{k}{2}}m_{\frac{k}{2}+1}\ldots m_{\frac{3k}{4}-1}},$$
$$a_{\frac{3k}{4},\frac{3k}{4}+1,\ldots,k-1} \equiv a_{\frac{k}{2},\frac{k}{2}+1,\ldots,k-1} \pmod{m_{\frac{3k}{4}}m_{\frac{3k}{4}+1}\ldots m_{k-1}}$$

и т. д., пока не получим

$$a_0 \equiv a_{01} \pmod{m_0},\ a_1 \equiv a_{01} \pmod{m_1},\ \ldots,$$

$$a_{k-2} \equiv a_{k-2,k-1} \pmod{m_{k-2}},\ a_{k-1} \equiv a_{k-2,k-1} \pmod{m_{k-1}}.$$

Пример 4.8. Пусть $m_0 = 3$, $m_1 = 23$, $m_2 = 7$, $m_3 = 17$, $m_4 = 5$, $m_5 = 19$, $m_6 = 11$, $m_7 = 13$. Вычисляем $m_0m_1 = 69$, $m_2m_3 = 119$, $m_4m_5 = 95$, $m_6m_7 = 143$; $m_0m_1m_2m_3 = 69 \cdot 119 = 8211$, $m_4m_5m_6m_7 = 95 \cdot 143 = 13585$.

Представим число $a = 12345678$ в классах вычетов по модулям $m_i$. Находим

$$a_{0123} \equiv a \equiv 4545 \pmod{8211},\ a_{4567} \equiv a \equiv 10498 \pmod{13585},$$

$$a_{01} \equiv a_{0123} \equiv 60 \pmod{69},\ a_{23} \equiv a_{0123} \equiv 23 \pmod{119},$$

$$a_{45} \equiv a_{4567} \equiv 48 \pmod{95},\ a_{67} \equiv a_{4567} \equiv 59 \pmod{143},$$

$$a_0 \equiv a_{01} \equiv 0 \pmod{3},\ a_1 \equiv a_{01} \equiv 14 \pmod{23},$$

$$a_2 \equiv a_{23} \equiv 2 \pmod{7},\ a_3 \equiv a_{23} \equiv 6 \pmod{17},$$

$$a_4 \equiv a_{45} \equiv 3 \pmod{5},\ a_5 \equiv a_{45} \equiv 10 \pmod{19},$$

$$a_6 \equiv a_{67} \equiv 4 \pmod{11},\ a_7 \equiv a_{67} \equiv 7 \pmod{13}.$$

Таким образом, 12345678 = (0, 14, 2, 6, 3, 10, 4, 7). □

При восстановлении числа $a$ из классов вычетов $(a_0, a_1, \ldots, a_{k-1})$ по китайской теореме об остатках: $a \equiv \sum_{i=0}^{k-1} a_i M_i N_i \pmod{M}$, где $a_i \equiv a \pmod{m_i}$, слагаемые $a_i M_i N_i$ для разных $i$ имеют много общих делителей. Например, все эти слагаемые имеют общий делитель $m_0 m_1 \ldots m_{\frac{k}{2}-1}$ при $i \geq \frac{k}{2}$ и $m_{\frac{k}{2}} m_{\frac{k}{2}+1} \ldots m_{k-1}$ при $i < \frac{k}{2}$. Поэтому

$$a \equiv \left( \sum_{i=0}^{\frac{k}{2}-1} a_i M_{1i} N_i \right) \prod_{r=\frac{k}{2}}^{k-1} m_r + \left( \sum_{j=\frac{k}{2}}^{k-1} a_j M_{2j} N_j \right) \prod_{s=0}^{\frac{k}{2}-1} m_s \pmod{M},$$

где $M_{1i} = m_0 m_1 \ldots m_{i-1} m_{i+1} \ldots m_{\frac{k}{2}-1}$, $M_{2j} = m_{\frac{k}{2}} m_{\frac{k}{2}+1} \ldots m_{j-1} m_{j+1} \ldots m_{k-1}$.

Данное разбиение дает возможность применить тот же метод, что и при нахождении остатков по модулю $m_i$. Обозначим $x_{ij} = m_i m_{i+1} \ldots m_{i+2^j-1}$ произведение $2^j$ подряд идущих модулей, начиная с $m_i$. Найдем целые числа

$$y_{ij} = \sum_{r=i}^{i+2^j-1} a_r \frac{x_{ij}}{m_r} N_r .$$

Вычисляя значения $y_{ij}$ по рекуррентной формуле

$$y_{i0} = a_i N_i,$$

$$y_{ij} = y_{i,j-1} x_{i+2^{j-1},j-1} + y_{i+2^{j-1},j-1} x_{i,j-1},\ \ j \geq 1,$$

получаем $a \equiv y_{0,\log_2 k} \pmod M$.

Пример 4.9. Пусть $a = (0, 14, 2, 6, 3, 10, 4, 7)$ и значения $m_i$ такие же, как в предыдущем примере, то есть $k = 8$ и

$$M = 3 \cdot 23 \cdot 7 \cdot 17 \cdot 5 \cdot 19 \cdot 11 \cdot 13.$$

Пусть уже вычислены значения

$$N_0 \equiv 1 \pmod 3,\ N_1 \equiv 17 \pmod{23},\ N_2 \equiv 6 \pmod 7,\ N_3 \equiv 11 \pmod{17},$$

$$N_4 \equiv 3 \pmod 5,\ N_5 \equiv 9 \pmod{19},\ N_6 \equiv 3 \pmod{11},\ N_7 \equiv 1 \pmod{13}.$$

Находим

$$y_{00} = 0,\ y_{10} = 238,\ y_{20} = 12,\ y_{30} = 66,\ y_{40} = 9,\ y_{50} = 90,\ y_{60} = 12,\ y_{70} = 7;$$

$$y_{01} = y_{00}x_{10} + y_{10}x_{00} = 0 \cdot 23 + 238 \cdot 3 = 714,$$

$$y_{21} = y_{20}x_{30} + y_{30}x_{20} = 12 \cdot 17 + 66 \cdot 7 = 666,$$

$$y_{41} = y_{40}x_{50} + y_{50}x_{40} = 9 \cdot 19 + 90 \cdot 5 = 621,$$

$$y_{61} = y_{60}x_{70} + y_{70}x_{60} = 12 \cdot 13 + 7 \cdot 11 = 233;$$

$$y_{02} = y_{01}x_{21} + y_{21}x_{01} = 714 \cdot 119 + 666 \cdot 69 = 130920,$$

$$y_{42} = y_{41}x_{61} + y_{61}x_{41} = 621 \cdot 143 + 233 \cdot 95 = 110938;$$

$$y_{03} = y_{02}x_{42} + y_{42}x_{02} = 130920 \cdot 13585 + 110938 \cdot 8211 = 2689460118.$$

Тогда $a \equiv y_{03} = 2689460118 \equiv 12345678 \pmod M$. □

Асимптотическая сложность алгоритма умножения чисел в классах вычетов равна $O(k \log k)$. Практически данный метод умножения эффективнее, чем умножение «в столбик», лишь тогда, когда длина сомножителей превышает разрядность процессора в десятки раз. Модули $m_i$ удобно выбирать в виде $2^s \pm c$, где число $c$ мало. Если выполняется подряд несколько умножений небольших сомножителей без восстановления промежуточных произведений по китайской теореме об остатках,

то необходимо принять меры, исключающие «переполнение», при котором произведение превышает модуль $M$.

Этот подход можно применять и для умножения полиномов одной переменной.

## 4.3. Умножение с помощью быстрого преобразования Фурье

Преобразование Фурье используется во многих областях математики и теоретической физики. Мы рассмотрим *дискретное* преобразование Фурье, на основе которого разработан асимптотически самый быстрый алгоритм умножения целых чисел (алгоритм Шенхаге–Штрассена).

### 4.3.1. Дискретное преобразование Фурье

Определение 4.1. Пусть числа $m$, $n$ натуральные, $m > 1$. Элемент $\omega \in \mathbb{Z}/m\mathbb{Z}$, обладающий свойствами: 1) $\omega \not\equiv 1 \pmod{m}$; 2) $\omega^n \equiv 1 \pmod{m}$; 3) $\sum_{j=0}^{n-1} \omega^{ij} \equiv 0 \pmod{m}$ для любого $i$, $1 \le i < n$, называется *примитивным корнем степени n из единицы*. Элементы $\omega^0$, $\omega^1$, ..., $\omega^{n-1}$ называются корнями степени $n$ из единицы.

Пример 4.10. В кольце $\mathbb{Z}/103\mathbb{Z}$ классов вычетов по модулю 103:

- числа 46 и 56 являются примитивными корнями степени 3 из единицы;
- числа 8, 9, 13, 14, 23, 30, 34, 61, 64, 66, 72, 76, 79, 81, 93, 100 являются примитивными корнями степени 17 из единицы;
- числа 2, 4, 7, 15, 16, 17, 18, 19, 25, 26, 28, 29, 32, 33, 36, 38, 41, 49, 50, 52, 55, 58, 59, 60, 63, 68, 82, 83, 91, 92, 97, 98 являются примитивными корнями степени 51 из единицы;

числа 5, 6, 11, 12, 20, 21, 35, 40, 43, 44, 45, 48, 51, 53, 54, 62, 65, 67, 70, 71, 74, 75, 77, 78, 84, 85, 86, 87, 88, 96, 99, 101 являются примитивными корнями степени 102 из единицы. □

Замечание. Перепишем условие 2 для примитивного корня: $\omega \cdot \omega^{n-1} \equiv 1 \pmod{m}$. Таким образом, для элемента $\omega$ существует мультипликативно обратный элемент $\omega^{-1} \equiv \omega^{n-1} \pmod{m}$, то есть $\omega \cdot \omega^{-1} \equiv 1 \pmod{m}$.

Лемма 4.1. Для любого целого числа $a$ и натурального $k$ выполняется равенство

$$\sum_{i=0}^{2^k-1} a^i = \prod_{j=0}^{k-1}(1+a^{2^j}). \tag{4.1}$$

*Доказательство.* Воспользуемся методом математической индукции. При $k = 1$ получаем: $a^0 + a^1 = 1 + a$ — нужное равенство выполнено. Пусть равенство (4.1) справедливо для $k$, докажем его для $k + 1$. Заметим, что

$$\sum_{i=0}^{2^{k+1}-1} a^i = (1+a)\sum_{i=0}^{2^k-1}(a^2)^i.$$

Воспользовавшись индукционным предположением и подставив $a^2$ вместо $a$, получим

$$\sum_{i=0}^{2^k-1}(a^2)^i = \prod_{j=0}^{k-1}(1+(a^2)^{2^j}) = \prod_{j=0}^{k-1}(1+a^{2^{j+1}}) = \prod_{j=1}^{k}(1+a^{2^j}),$$

откуда

$$\sum_{i=0}^{2^{k+1}-1} a^i = (1+a)\sum_{i=0}^{2^k-1}(a^2)^i = (1+a)\prod_{j=1}^{k}(1+a^{2^j}) = \prod_{j=0}^{k}(1+a^{2^j}),$$

что и требовалось доказать. □

Лемма 4.2. Пусть $m = \omega^{\frac{n}{2}} + 1$, где $n = 2^k$ и $\omega \in \mathbb{N}$. Тогда для любого $i$, $1 \le i < n$, выполняется сравнение

$$\sum_{j=0}^{n-1}\omega^{ij} \equiv 0 \pmod{m}.$$

*Доказательство*. Полагая в обозначениях предыдущей леммы $a = \omega^i$, где $i$ — произвольное целое число, $1 \le i < n$, имеем:

$$\sum_{j=0}^{n-1}\omega^{ij} = \prod_{t=0}^{k-1}(1+\omega^{i2^t}),$$

то есть нужно показать, что для любого $i$ из указанного интервала найдется такое $t$, что

$$1+\omega^{i2^t} \equiv 0 \pmod{m}.$$

Представим $i$ в виде $i = 2^s r$, где число $r$ нечетное, и положим $t = k-1-s$ (при $0 \le s \le k-1$ имеем $0 \le t \le k-1$). Тогда, учитывая, что $\omega^{\frac{n}{2}} \equiv -1 \pmod{m}$, получаем

$$1+\omega^{i2^t} = 1+\omega^{2^{k-1}r} = 1+\omega^{\frac{n}{2}\cdot r} \equiv 1+(-1)^r \equiv 0 \pmod{m},$$

поскольку число $r$ нечетное. □

Теорема 4.3 (о существовании примитивного корня). Если $n = 2^k$ и $\omega = 2^q$, где $q > 1$, то при $m = \omega^{\frac{n}{2}}+1$ число $\omega$ как элемент кольца $\mathbb{Z}/m\mathbb{Z}$ является примитивным корнем степени $n$ из единицы. Кроме того, существует элемент $n^{-1}$, мультипликативно обратный к $n$ по модулю $m$, то есть $n \cdot n^{-1} \equiv 1 \pmod{m}$.

*Доказательство*. По условию $\omega = 2^q \not\equiv 1 \pmod{m}$ при $q > 1$ — первое условие для примитивного корня выполнено. Поскольку $\omega^{\frac{n}{2}} \equiv -1 \pmod{m}$, получаем $\omega^n \equiv 1 \pmod{m}$ — второе условие выполнено. Третье условие выполняется согласно лемме 4.2. Первое утверждение доказано.

Числа $n = 2^k$ и $m = \omega^{\frac{n}{2}}+1 = 2^{2^{k-1}q}+1$ взаимно просты, поэтому элемент $n$ имеет обратный по модулю $m$. Поскольку $n \cdot n^{-1} \equiv 1 \pmod{m}$, а

$1 \equiv -\omega^{\frac{n}{2}} \pmod m$, получаем: $n \cdot n^{-1} \equiv -\omega^{\frac{n}{2}} \pmod m$, то есть $2^k \cdot n^{-1} \equiv -2^{\frac{qn}{2}} \pmod m$, откуда $n^{-1} \equiv -2^{2^{k-1}q-k} \pmod m$. □

Пример 4.11. Пусть $k = 4$, $q = 2$, то есть $n = 2^4 = 16$, $\omega = 2^2 = 4$ и $m = \omega^{\frac{n}{2}} + 1 = 4^8 + 1 = 65537$. Тогда $\omega = 4 \quad 1 \pmod{65537}$, $\omega^n = 4^{16} \equiv 1 \pmod{65537}$ и для любого $i$, $1 \le i < 2^4$,

$$\sum_{j=0}^{15} 4^{ij} \equiv 0 \pmod{65537},$$

то есть 4 является примитивным корнем степени 16 из единицы в кольце $\mathbb{Z}/65537\mathbb{Z}$.

Вычисляем: $n^{-1} \equiv -2^{2^3 \cdot 2-4} \equiv -2^{12} \equiv 61441 \pmod{65537}$. □

Определение 4.2. Пусть вектор $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})^{\mathrm{T}}$, где $a_i \in \mathbb{Z}/m\mathbb{Z}$ для некоторого целого числа $m$, НОД$(m, n) = 1$ и $\omega$ — примитивный корень степени $n$ из единицы в кольце $\mathbb{Z}/m\mathbb{Z}$. Пусть элементы квадратной матрицы $A$ размера $n$ имеют вид $\omega^{ij} \pmod m$, где $0 \le i, j < n$. *Дискретным преобразованием Фурье* по модулю $m$ вектора $\mathbf{a}$ называется вектор $F(\mathbf{a}) = A\mathbf{a}$, $i$-я координата которого равна $\sum_{j=0}^{n-1} a_j \omega^{ij} \pmod m$, $0 \le i < n$.

Лемма 4.4. Пусть $\omega$ — примитивный корень степени $n$ из единицы в кольце $\mathbb{Z}/m\mathbb{Z}$ и НОД$(m, n) = 1$. Пусть элементы квадратной матрицы $A$ размера $n$ имеют вид $\omega^{ij}$, где $0 \le i, j < n$. Тогда существует обратная матрица $A^{-1}$ с элементами $n^{-1}\omega^{-ij} \pmod m$, где $0 \le i, j < n$.

*Доказательство.* Достаточно показать, что $A \cdot A^{-1} = E$ (единичная матрица), если суммы и произведения элементов матриц рассматривать по модулю $m$. Элементы $e_{ij}$ матрицы произведения имеют вид

$$e_{ij} \equiv n^{-1}\sum_{k=0}^{n-1}\omega^{ik}\omega^{-kj} = n^{-1}\sum_{k=0}^{n-1}\omega^{(i-j)k} \pmod m, \tag{4.2}$$

где $0 \le i, j < n$ (элемент $n^{-1} \pmod m$ существует, так как числа $m$ и $n$ взаимно просты). При $i = j$ получаем $e_{ij} \equiv n^{-1}\sum_{k=0}^{n-1}1 = n^{-1}\cdot n \equiv 1 \pmod m$.

Пусть теперь $i \ne j$. Разность $i - j$ принимает значения от $-n$ до $n$ и не равна 0. При $i > j$ по третьему условию для примитивного корня сумма в выражении (4.2) равна 0, и значит, $e_{ij} \equiv 0 \pmod m$. Если же $i < j$, то, умножая крайние части сравнения (4.2) на $\omega^{n(j-i)} \equiv 1^{(j-i)} = 1 \pmod m$, получаем:

$$e_{ij} \equiv n^{-1}\sum_{k=0}^{n-1}\omega^{(j-i)(n-k)} = n^{-1}\sum_{k=0}^{n-1}\omega^{(j-i)k} \pmod m,$$

где сумма в правой части снова равна 0. □

Определение 4.3. *Обратным дискретным преобразованием Фурье* вектора **a** называется вектор $F^{-1}(\mathbf{a}) = A^{-1}\mathbf{a}$, $i$-я координата которого равна $n^{-1}\sum_{j=0}^{n-1}a_j\omega^{-ij} \pmod m$, где $0 \le i < n$.

Если применить обратное преобразование Фурье $F^{-1}$ к вектору $F(\mathbf{a})$, то получится сам вектор **a**, то есть $F^{-1}(F(\mathbf{a})) = \mathbf{a}$.

Преобразование Фурье непосредственно связано с интерполяцией полиномов. Любой полином $a(x) = \sum_{i=0}^{n-1}a_i x^i$ степени $n - 1$ можно однозначно представить набором коэффициентов $a_0, a_1, \ldots, a_{n-1}$ и набором значений в $n$ различных точках $x_0, x_1, \ldots, x_{n-1}$. Преобразование Фурье вектора $(a_0, a_1, \ldots, a_{n-1})^{\mathrm{T}}$ переводит вектор коэффициентов полинома $a(x)$ в вектор его значений в точках $\omega^0, \omega^1, \ldots, \omega^{n-1}$. Обратное преобразование Фурье представляет собой интерполяцию полинома $a(x)$ по его значениям в корнях степени $n$ из единицы.

Определение 4.4. *Сверткой* $\mathbf{a} * \mathbf{b}$ векторов $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})^{\mathrm{T}}$ и $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})^{\mathrm{T}}$ называется такой вектор $\mathbf{c} = (c_0, c_1, \ldots, c_{2n-1})^{\mathrm{T}}$, что $c_i = \sum_{j=0}^{n-1} a_j b_{i-j}$, $0 \le i < 2n$. При этом полагают $a_j = b_j = 0$, если $j < 0$ или $j \ge n$.

Таким образом,

$$c_0 = a_0 b_0,\ c_1 = a_0 b_1 + a_1 b_0,\ c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$

и т. д., при этом всегда $c_{2n-1} = 0$. Отметим, что коэффициенты произведения двух полиномов $a(x) = \sum_{i=0}^{n-1} a_i x^i$, $b(x) = \sum_{i=0}^{n-1} b_i x^i$ — это в точности компоненты свертки векторов $\mathbf{a}$ и $\mathbf{b}$, составленных из коэффициентов исходных полиномов:

$$a(x)b(x) = \sum_{i=0}^{2n-2} \left( \sum_{j=0}^{i} a_j b_{i-j} \right) x^i .$$

Если полиномы $a(x)$ и $b(x)$ степени $n-1$ представлены своими коэффициентами, то, чтобы определить коэффициенты их произведения $a(x)b(x)$, можно вычислить свертку векторов их коэффициентов. Обратно, если полиномы $a(x)$ и $b(x)$ представлены своими значениями в корнях степени $n$ из единицы, то, перемножая покоординатно векторы значений, получаем представление полинома $a(x)b(x)$ в корнях степени $n$ из единицы.

Но произведение $a(x)b(x)$ — это полином степени $2n-2$, то есть для его однозначного представления требуются значения в $2n-2$ различных точках. Для этого будем рассматривать полиномы $a(x)$ и $b(x)$ степени $n-1$ как полиномы степени $2n-1$, у которых коэффициенты при $x^{2n-1}, x^{2n-2}, \ldots, x^n$ равны нулю.

Теорема 4.5 (о свертке). Пусть $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}, 0, 0, \ldots, 0)^{\mathrm{T}}$, $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1}, 0, 0, \ldots, 0)^{\mathrm{T}}$ — векторы длины $2n$,

$F(\mathbf{a}) = (a'_0, a'_1, \ldots, a'_{2n-1})^{\mathrm{T}}$, $F(\mathbf{b}) = (b'_0, b'_1, \ldots, b'_{2n-1})^{\mathrm{T}}$ — их преобразования Фурье. Тогда $\mathbf{a} * \mathbf{b} = F^{-1}(F(\mathbf{a}) \cdot F(\mathbf{b}))$.

*Доказательство* [1]. По определению преобразования Фурье

$$a'_s = \sum_{u=0}^{2n-1} a_u \omega^{su}, \quad b'_s = \sum_{v=0}^{2n-1} b_v \omega^{sv},$$

но $a_k = b_k = 0$ при $n \le k < 2n$, поэтому верхние пределы суммирования в обеих суммах можно понизить до $n-1$. Следовательно, при $0 \le s < 2n$ получаем координаты вектора $F(\mathbf{a}) \cdot F(\mathbf{b})$:

$$a'_s b'_s = \sum_{u=0}^{n-1} \sum_{v=0}^{n-1} a_u b_v \omega^{s(u+v)}.$$

Обозначим $\mathbf{a} * \mathbf{b} = (c_0, c_1, \ldots, c_{2n-1})^{\mathrm{T}}$, $F(\mathbf{a} * \mathbf{b}) = (c'_0, c'_1, \ldots, c'_{2n-1})^{\mathrm{T}}$, при этом $c'_s = \sum_{k=0}^{2n-1} c_k \omega^{sk}$. По определению свертки $c_k = \sum_{u=0}^{2n-1} a_u b_{k-u}$, поэтому

$$c'_s = \sum_{k=0}^{2n-1} \sum_{u=0}^{2n-1} a_u b_{k-u} \omega^{sk}.$$

Меняем порядок суммирования и делаем замену индексов $v = k - u$:

$$c'_s = \sum_{u=0}^{2n-1} \sum_{k=0}^{2n-1} a_u b_{k-u} \omega^{sk} = \sum_{u=0}^{2n-1} \sum_{v=-u}^{2n-1-u} a_u b_v \omega^{s(u+v)}.$$

Поскольку $b_v = 0$ при $v < 0$ и $a_u = 0$ при $u \ge n$, можно повысить нижний предел во внутренней сумме до 0 и понизить верхний предел во внешней сумме до $n-1$:

$$c'_s = \sum_{u=0}^{n-1} \sum_{v=0}^{2n-1-u} a_u b_v \omega^{s(u+v)}.$$

Кроме того, при $0 \le u \le n-1$ верхний предел во внутренней сумме изменяется от $2n-1$ до $n$, а при таких значениях $v$ имеем $b_v = 0$, то есть

$$c'_s = \sum_{u=0}^{n-1} \sum_{v=0}^{n-1} a_u b_v \omega^{s(u+v)} = a'_s b'_s .$$

Таким образом, $F(\mathbf{a} * \mathbf{b}) = F(\mathbf{a}) \cdot F(\mathbf{b})$, откуда $\mathbf{a} * \mathbf{b} = F^{-1}(F(\mathbf{a}) \cdot F(\mathbf{b}))$.□

Определение 4.5. *Положительно обернутой сверткой* векторов $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})^{\mathrm{T}}$ и $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})^{\mathrm{T}}$ назовем такой вектор $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})^{\mathrm{T}}$, что

$$c_i = \sum_{j=0}^{i} a_j b_{i-j} + \sum_{j=i+1}^{n-1} a_j b_{n+i-j}, \; 0 \le i < n.$$

*Отрицательно обернутой сверткой* векторов $\mathbf{a}$ и $\mathbf{b}$ назовем такой вектор $\mathbf{d} = (d_0, d_1, \ldots, d_{n-1})^{\mathrm{T}}$, что

$$d_i = \sum_{j=0}^{i} a_j b_{i-j} - \sum_{j=i+1}^{n-1} a_j b_{n+i-j}, \; 0 \le i < n.$$

Пусть $\mathbf{a}$ и $\mathbf{b}$ — векторы коэффициентов полиномов $a(x)$ и $b(x)$ степени $n-1$. Положительно обернутая свертка векторов $\mathbf{a}$ и $\mathbf{b}$ эквивалентна вычислению остатка от деления произведения $a(x)b(x)$ на полином $x^n - 1$, отрицательно обернутая свертка — на $x^n + 1$ (рис. 4.1 на стр. 138). Если вычислить значения полиномов $a(x)$ и $b(x)$ степени $n-1$ в корнях степени $n$ из единицы: $a(\omega^0)$, $b(\omega^0)$, $a(\omega^1)$, $b(\omega^1)$, …, $a(\omega^{n-1})$, $b(\omega^{n-1})$, то по $n$ произведениям $a(\omega^0)b(\omega^0)$, $a(\omega^1)b(\omega^1)$, …, $a(\omega^{n-1})b(\omega^{n-1})$ можно однозначно интерполировать полином степени $n-1$. Вектор коэффициентов этого полинома будет положительно обернутой сверткой векторов коэффициентов полиномов $a(x)$ и $b(x)$.

Теорема 4.6. Пусть $m$ и $n$ — взаимно простые целые числа, $m > 1$, векторы $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})^{\mathrm{T}}$ и $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})^{\mathrm{T}}$ таковы, что $a_i$, $b_i \in \mathbb{Z}/m\mathbb{Z}$, $0 \le i < n$, $\omega$ — примитивный корень степени $n$ из единицы и $\psi^2 \equiv \omega \pmod{m}$. Тогда справедливы следующие утверждения.

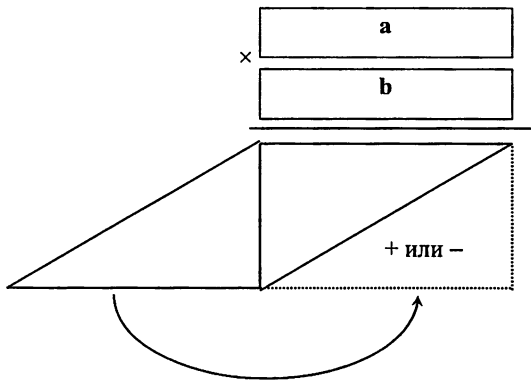



*Рис. 4.1. Положительно (отрицательно) обернутая свертка*

1. Положительно обернутая свертка векторов **a** и **b** равна $F^{-1}(F(\mathbf{a})\cdot F(\mathbf{b}))$.

2. Если вектор $\mathbf{d}=(d_0,\ d_1,\ \ldots,\ d_{n-1})^{\mathrm{T}}$ — отрицательно обернутая свертка векторов **a** и **b**, $\mathbf{a}'=(a_0,\ \psi a_1,\ \ldots,\ \psi^{n-1}a_{n-1})^{\mathrm{T}}$, $\mathbf{b}'=(b_0,\ \psi b_1,\ \ldots,\ \psi^{n-1}b_{n-1})^{\mathrm{T}}$, $\mathbf{d}'=(d_0,\ \psi d_1,\ \ldots,\ \psi^{n-1}d_{n-1})^{\mathrm{T}}$, то $\mathbf{d}'=F^{-1}(F(\mathbf{a}')\cdot F(\mathbf{b}'))$.

*Доказательство*. Докажем второе утверждение. Пусть

$$F(\mathbf{a}')=(a'_0,a'_1,\ldots,a'_{n-1})^{\mathrm{T}},\quad F(\mathbf{b}')=(b'_0,b'_1,\ldots,b'_{n-1})^{\mathrm{T}}$$

— преобразования Фурье по модулю $m$, где

$$a'_s\equiv\sum_{u=0}^{n-1}\psi^u a_u\omega^{su}\pmod m,\quad b'_s\equiv\sum_{v=0}^{n-1}\psi^v b_v\omega^{sv}\pmod m.$$

Тогда

$$a'_s b'_s\equiv\sum_{u=0}^{n-1}\sum_{v=0}^{n-1}\psi^{u+v}a_u b_v\omega^{s(u+v)}\pmod m.$$

Пусть $F(\mathbf{d}')=(d'_0,d'_1,\ldots,d'_{n-1})^{\mathrm{T}}$ — преобразование Фурье по модулю $m$ вектора $\mathbf{d}'$, где

$$d'_s\equiv\sum_{i=0}^{n-1}\psi^i d_i\omega^{si}\pmod m.$$

Но по определению отрицательно обернутой свертки

$$d_i\equiv\sum_{u=0}^{i}a_u b_{i-u}-\sum_{u=i+1}^{n-1}a_u b_{n+i-u}\pmod m,$$

тогда

$$d'_s\equiv\sum_{i=0}^{n-1}\sum_{u=0}^{i}\psi^i a_u b_{i-u}\omega^{si}-\sum_{i=0}^{n-1}\sum_{u=i+1}^{n-1}\psi^i a_u b_{n+i-u}\omega^{si}\pmod m.$$

Повышаем верхний предел суммирования во внутренней сумме первого слагаемого до $n-1$, понижаем нижний предел суммирования во внутренней сумме второго слагаемого до 0 и меняем порядок суммирования:

$$d'_s \equiv \sum_{u=0}^{n-1}\sum_{i=0}^{n-1}\psi^i a_u b_{i-u}\omega^{si} - \sum_{u=0}^{n-1}\sum_{i=0}^{n-1}\psi^i a_u b_{n+i-u}\omega^{si} \pmod m.$$

Делая замену индексов $v = i - u$ в первом слагаемом, $w = n + i - u$ во втором слагаемом и учитывая, что $\psi^n \equiv -1 \pmod m$, получаем

$$d'_s \equiv \sum_{u=0}^{n-1}\sum_{v=-u}^{n-1-u}\psi^{u+v}a_u b_v \omega^{s(u+v)} + \sum_{u=0}^{n-1}\sum_{w=n-u}^{2n-1-u}\psi^{u+w}a_u b_w \omega^{s(u+w-n)} \equiv$$

$$\equiv \sum_{u=0}^{n-1}\left(\sum_{v=0}^{n-u-1}\psi^{u+v}a_u b_v \omega^{s(u+v)} + \sum_{w=n-u}^{n-1}\psi^{u+w}a_u b_w \omega^{s(u+w-n)}\right) \pmod m.$$

Поскольку $\omega^{-n} = (\omega^n)^{-1} \equiv 1 \pmod m$, имеем

$$d'_s \equiv \sum_{u=0}^{n-1}\sum_{v=0}^{n-1}\psi^{u+v}a_u b_v \omega^{s(u+v)} \equiv a'_s b'_s \pmod m. \qquad \square$$

Упражнение. Доказать утверждение 1 теоремы 4.6.

### 4.3.2. Алгоритм быстрого преобразования Фурье

Для вычисления прямого и обратного преобразования Фурье по модулю $m$ вектора **a** длины $n$ требуется $O(n^2)$ операций умножения по модулю $m$, если просто умножать матрицу $A$ на вектор **a**. Однако если $n$ — степень числа 2, то вычисления можно ускорить. Далее будем считать, что $n = 2^k$, где $k \in \mathbb{Z}$.

Преобразование Фурье $A\mathbf{a}$, где $\mathbf{a} = (a_{n-1}, a_{n-2}, \ldots, a_0)^{\mathrm{T}}$, переводит вектор **a** коэффициентов полинома $a(x) = \sum_{i=0}^{n-1} a_i x^i$ в вектор его значений $(a(\omega^0), a(\omega^1), \ldots, a(\omega^{n-1}))^{\mathrm{T}}$. Чтобы вычислить значение полинома $a(x)$ в точке $x = \omega^i$, нужно найти остаток от деления полинома $a(x)$ на $x - \omega^i$ для $i = 0, 1, \ldots, n-1$.

Метод последовательного деления полинома $a(x)$ на каждый из полиномов $x - \omega^i$ имеет сложность $O(n^2)$. Полиномы $x - \omega^i$ попарно взаимно просты, а их произведение равно $x^n - 1$. Поэтому в случае $n = 2^k$

для ускорения вычислений можно воспользоваться тем же приемом, что и при умножении в классах вычетов.

Поскольку $\omega^{\frac{n}{2}} \equiv -1 \pmod{m}$, имеем

$$x^n - 1 = (x^{\frac{n}{2}} - 1)(x^{\frac{n}{2}} + 1) \equiv (x^{\frac{n}{2}} - 1)(x^{\frac{n}{2}} - \omega^{\frac{n}{2}}) \pmod{m}.$$

Аналогично

$$x^{\frac{n}{2}} - 1 \equiv (x^{\frac{n}{4}} - 1)(x^{\frac{n}{4}} - \omega^{\frac{n}{2}}) \pmod{m}, \quad x^{\frac{n}{4}} - \omega^{\frac{n}{2}} \equiv (x^{\frac{n}{4}} - \omega^{\frac{n}{4}})(x^{\frac{n}{4}} - \omega^{\frac{3n}{4}}) \pmod{m}$$

и т. д., пока в правой части не получатся полиномы первой степени $x - \omega^i$. Этот процесс можно описать деревом высоты $k$, где полином $x^n - 1$ является корнем, а линейные полиномы $x - \omega^i$ — листьями (рис. 4.2 на стр. 142). Из каждой вершины, не являющейся листом, выходят два ребра, соответствующие разложению на два сомножителя.

Теперь для вычисления остатка от деления полинома $a(x)$ на каждый из полиномов $x - \omega^0$, $x - \omega^1$, ..., $x - \omega^{n-1}$ сначала делим $a(x)$ с остатком на $x^{\frac{n}{2}} - 1$ и $x^{\frac{n}{2}} - \omega^{\frac{n}{2}}$, каждый из полученных остатков делим с остатком на полиномы вида $x^{\frac{n}{4}} - \omega^{\frac{m}{4}}$ и т. д.

Лемма 4.7. Пусть $a(x) = \sum_{j=0}^{2t-1} a_j x^j$ и $C$ — некоторая константа. Тогда остаток от деления полинома $a(x)$ на $x^t - C$ равен

$$r(x) = \sum_{j=0}^{t-1} (a_j + C a_{j+t}) x^j .$$

*Доказательство.* Представляя $a(x)$ в виде

$$a(x) = \left( \sum_{j=0}^{t-1} a_{j+t} x^j \right)(x^t - C) + r(x),$$

получаем требуемое выражение для остатка $r(x)$. □

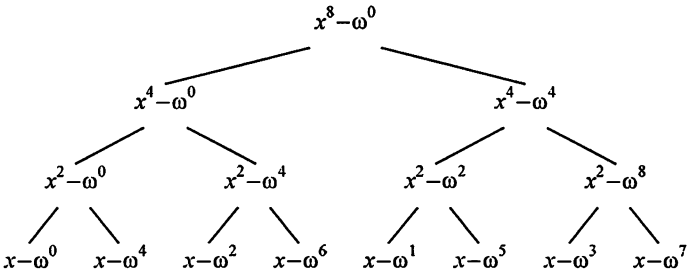



***Рис. 4.2.*** *Разложение полинома* $x^8 - \omega^0$

Лемма 4.7 показывает, что для вычисления остатка от деления произвольного полинома степени $2t-1$ на $x^t - C$ требуется $O(t)$ элементарных операций.

Лемма 4.8. Пусть $n = 2^k$ и $\omega$ — примитивный корень степени $n$ из единицы. Пусть $(d_{k-1}, d_{k-2}, \ldots, d_0)_2$ — двоичное представление целого числа $j$, где $0 \le j < 2^k$ (то есть $j = \sum_{i=0}^{k-1} d_i 2^i$), а $\mathrm{rev}(j)$ — целое число с двоичным представлением $(d_0, d_1, \ldots, d_{k-1})_2$. Тогда

$$\prod_{j=l}^{l+2^s-1} (x - \omega^{\mathrm{rev}(j)}) \equiv x^{2^s} - \omega^{\mathrm{rev}(l/2^s)} \pmod m,$$

где $0 \le s \le k$, число $l$ кратно $2^s$, $0 \le l < n-1$.

*Доказательство* проведем индукцией по $s$. При $s = 0$ имеем $\prod_{j=l}^{l+2^s-1} (x - \omega^{\mathrm{rev}(j)}) = x - \omega^{\mathrm{rev}(l)}$, и утверждение леммы справедливо. Пусть лемма верна для всех $s \le m$, докажем ее для $s = m+1$. Запишем

$$\prod_{j=l}^{l+2^{m+1}-1} (x - \omega^{\mathrm{rev}(j)}) = \prod_{j=l}^{l+2^m-1} (x - \omega^{\mathrm{rev}(j)}) \cdot \prod_{j=l+2^m}^{l+2^m+2^m-1} (x - \omega^{\mathrm{rev}(j)}) =$$

$$= \prod_{j=l}^{l+2^m-1} (x - \omega^{\mathrm{rev}(j)}) \cdot \prod_{j=u}^{u+2^m-1} (x - \omega^{\mathrm{rev}(u+2^m)}).$$

Тогда по индукционному предположению

$$\prod_{j=l}^{l+2^{m+1}-1} (x - \omega^{\mathrm{rev}(j)}) \equiv (x^{2^m} - \omega^{\mathrm{rev}(l/2^m)})(x^{2^m} - \omega^{\mathrm{rev}(l/2^m+1)}) \pmod m.$$

Пусть число $t$ четное, $0 \le t < n-1$, тогда

$$t = (t_{k-1}, t_{k-2}, \ldots, t_1, 0)_2,$$

$$t + 1 = (t_{k-1}, t_{k-2}, \ldots, t_1, 1)_2,$$

$$t/2 = (0, t_{k-1}, t_{k-2}, \ldots, t_1)_2,$$

$$\mathrm{rev}(t) = (0, t_1, \ldots, t_{k-2}, t_{k-1})_2,$$

$$\mathrm{rev}(t+1) = (1, t_1, \ldots, t_{k-2}, t_{k-1})_2 = \mathrm{rev}(t) + 2^{k-1}, \tag{4.3}$$

$$\mathrm{rev}(t/2) = (t_1, t_2, \ldots, t_{k-1}, 0)_2 = 2 \cdot \mathrm{rev}(t). \tag{4.4}$$

Учитывая, что $\omega^{2^{k-1}} = \omega^{\frac{n}{2}} \equiv -1 \pmod m$, и воспользовавшись соотношением (4.3), получаем

$$\omega^{\mathrm{rev}(l/2^m+1)} = \omega^{\mathrm{rev}(l/2^m)} \cdot \omega^{2^{k-1}} \equiv -\omega^{\mathrm{rev}(l/2^m)} \pmod m.$$

Тогда, с учетом соотношения (4.4),

$$\prod_{j=l}^{l+2^{m+1}-1} (x - \omega^{\mathrm{rev}(j)}) \equiv (x^{2^m} - \omega^{\mathrm{rev}(l/2^m)})(x^{2^m} + \omega^{\mathrm{rev}(l/2^m)}) =$$

$$= x^{2^{m+1}} - \omega^{2\,\mathrm{rev}(l/2^m)} = x^{2^{m+1}} - \omega^{\mathrm{rev}(l/2^{m+1})} \pmod m. \qquad \square$$

Лемма 4.8 задает порядок появления степеней $i$ в полиномах $x^i - \omega^i$ при составлении попарных произведений так, чтобы все произведения имели вид $x^{2^s} - \omega^i$.

Алгоритм 4.5. Быстрое преобразование Фурье [1].

*Вход*. Вектор $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})^{\mathrm{T}}$, где $n = 2^k$, $a_i \in \mathbb{Z}/m\mathbb{Z}$.

*Выход*. Вектор $\mathbf{b} = F(\mathbf{a}) = (b_0, b_1, \ldots, b_{n-1})^{\mathrm{T}}$, где $b_i \equiv \sum_{j=0}^{n-1} a_j \omega^{ij} \pmod m$ для $0 \le i < n$.

1. Положить $r_{0,k} \leftarrow \sum_{j=0}^{n-1} a_j x^j$.

2. Для $s = k-1, k-2, \ldots, 0$ выполнить следующие действия.

   2.1. Положить $t \leftarrow 0$.

   2.2. Пока $t < n-1$:

      2.2.1. Представить полином $r_{t,s+1}(x)$ в виде $\sum_{j=0}^{2^{s+1}-1} a_j x^j$.

      2.2.2. Положить $e \leftarrow \mathrm{rev}(t/2^s)$.

2.2.3. Положить $r_{t,s}(x) \leftarrow \sum_{j=0}^{2^s-1}(a_j + \omega^e a_{j+2^s})x^j \pmod m$.

2.2.4. Положить $r_{t+2^s,s}(x) \leftarrow \sum_{j=0}^{2^s-1}(a_j + \omega^{e+\frac{n}{2}} a_{j+2^s})x^j \pmod m$.

2.3. Положить $t \leftarrow t + 2^{s+1}$ и вернуться на шаг 2.2.

3. Для $i = 0, 1, \ldots, n-1$ положить $b_{\mathrm{rev}(i)} \leftarrow r_{i,0}$.

4. Результат: $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})^{\mathrm{T}}$. □

Сложность алгоритма 4.5 равна $O(n \log_2 n)$.

Пример 4.12. Вычислим быстрое преобразование Фурье вектора $\mathbf{a} = (0, 1, 2, 3, 4, 5, 6, 7)^{\mathrm{T}}$ в кольце $\mathbb{Z}/65537\mathbb{Z}$. Таким образом, $n = 2^3$, $k = 3$.

Находим $\omega = 16$ — примитивный корень степени 8 из 1 по модулю 65537.

Полагаем

$$r_{0,3}(x) = x + 2x^2 + 3x^3 + 4x^4 + 5x^5 + 6x^6 + 7x^7.$$

Все вычисления с коэффициентами полиномов выполняем по модулю 65537:

| $s$ | $t$ | $e$ | $r_{t,s}(x)$, $r_{t+2^s,s}(x)$ |
|---|---|---|---|
| 2 | 0 | 0 | $r_{0,2}(x) = (0 + 4) + (1 + 5)x + (2 + 6)x^2 + (3 + 7)x^3 =$<br>$= 4 + 6x + 8x^2 + 10x^3$,<br>$r_{4,2}(x) = (0 + 4\omega^4) + (1 + 5\omega^4)x + (2 + 6\omega^4)x^2 + (3 + 7\omega^4)x^3 =$<br>$= 65533 + 65533x + 65533x^2 + 65533x^3$ |
| 1 | 0 | 0 | $r_{0,1}(x) = (4 + 8) + (6 + 10)x = 12 + 16x$,<br>$r_{2,1}(x) = (4 + 8\omega^4) + (6 + 10\omega^4)x = 65533 + 65533x$ |
| | 4 | 2 | $r_{4,1}(x) = (65533 + 65533\omega^2) + (65533 + 65533\omega^2)x =$<br>$= 64509 + 64509x$,<br>$r_{6,1}(x) = (65533 + 65533\omega^6) + (65533 + 65533\omega^6)x =$ |

| $s$ | $t$ | $e$ | $r_{t,s}(x)$, $r_{t+2^s,s}(x)$ |
|---|---|---|---|
| | | | $= 1020 + 1020x$ |
| 0 | 0 | 0 | $r_{0,0}(x) = 12 + 16 = 28$,<br>$r_{1,0}(x) = 12 + 16\omega^4 = 65533$ |
| | 2 | 2 | $r_{2,0}(x) = 65533 + 65533\omega^2 = 64509$,<br>$r_{3,0}(x) = 65533 + 65533\omega^6 = 1020$ |
| | 4 | 1 | $r_{4,0}(x) = 64509 + 64509\omega = 48061$,<br>$r_{5,0}(x) = 64509 + 64509\omega^5 = 15420$ |
| | 6 | 3 | $r_{6,0}(x) = 1020 + 1020\omega^3 = 50109$,<br>$r_{7,0}(x) = 1020 + 1020\omega^7 = 17468$ |

На шаге 3 получаем $b_0 = r_{0,0}$, $b_4 = r_{1,0}$, $b_2 = r_{2,0}$, $b_6 = r_{3,0}$, $b_1 = r_{4,0}$, $b_5 = r_{5,0}$, $b_3 = r_{6,0}$, $b_7 = r_{7,0}$. то есть $\mathbf{b} = (28, 48061, 64509, 50109, 65533, 15420, 1020, 17468)^{\mathrm{T}}$. □

Для вычисления обратного преобразования Фурье по модулю $m$ используется этот же алгоритм, но $\omega$ везде меняем на $\omega^{-1}$ (mod $m$), а на шаге 3 полагаем $b_{\mathrm{rev}(i)} \leftarrow n^{-1} \cdot r_{i,0}$ (mod $m$).

### 4.3.3. Алгоритм Шенхаге–Штрассена для умножения целых чисел

Идея быстрого умножения целых чисел длины $n = 2^k$ битов заключается в следующем. Сомножители нужно представить в виде чисел длины $2n$ (добавив $n$ нулей в старших разрядах, как мы это делали в теореме о свертке) — это делается для того, чтобы не было переполнения. Полученные векторы преобразования Фурье перемножаются покоординатно по модулю $2^{2l} + 1$ (обычно удобно выбирать число $2l$ равным разрядности процессора), и после этого выполняется обратное преобразование Фурье, то есть вычисляется отрицательно обернутая свертка. При этом необходимо принять меры, исключающие влияние переносов, возникающих при целочисленном сложении $d = 2n/l$ слагаемых (умноже-

ние целых чисел отличается от умножения полиномов тем, что появляются переносы). Для этого А. Шенхаге и Ф. Штрассен (V. Strassen) предложили использовать «разреженные» слагаемые, содержащие достаточное число нулей в старших разрядах. При этом, естественно, длина каждого слагаемого возрастает в несколько раз.

Алгоритм 4.6. Алгоритм Шенхаге–Штрассена [1].

*Вход.* Числа $a=\sum_{i=0}^{d-1} a_i 2^{li}$, $b=\sum_{i=0}^{d-1} b_i 2^{li}$ длины $n$ бит, где $d=2n/l$, $0 \le a_i < 2^l$, $0 \le b_i < 2^l$ для $0 \le i < d/2$, $a_i = b_i = 0$ для $d/2 \le i < d$; $\psi$ — примитивный корень степени $2d$ из единицы по модулю $2^{2l}+1$, $\omega = \psi^2$ — примитивный корень степени $d$ из единицы по модулю $2^{2l}+1$.

*Выход.* Произведение $c = ab$, $c \equiv \sum_{i=0}^{d-1} c_i 2^{li} \pmod{2^{2n+1}}$.

1. Выполнить быстрое преобразование Фурье по модулю $2^{2l}+1$ векторов $\mathbf{a}' = (a_0,\ \psi a_1 \pmod{2^{2l}+1},\ \ldots,\ \psi^{\frac{d}{2}-1} a_{\frac{d}{2}-1} \pmod{2^{2l}+1},\ 0,\ 0, \ldots, 0)^{\mathrm{T}}$, $\mathbf{b}' = (b_0,\ \psi b_1 \pmod{2^{2l}+1},\ \ldots,\ \psi^{\frac{d}{2}-1} b_{\frac{d}{2}-1} \pmod{2^{2l}+1},\ 0,\ 0, \ldots, 0)^{\mathrm{T}}$ длины $d$.
2. Вычислить покомпонентное произведение векторов $F(\mathbf{a}')$ и $F(\mathbf{b}')$ и выполнить обратное преобразование Фурье $F^{-1}(F(\mathbf{a}') \cdot F(\mathbf{b}'))$ по модулю $2^{2l}+1$.
3. Найти вектор $\mathbf{c}'' = (c_0'', c_1'', \ldots, c_{d-1}'')^{\mathrm{T}}$, где $c_i'' \equiv c_i \pmod{2^{2l}+1}$, для чего умножить каждую $i$-ю координату вектора, полученного на шаге 2, на $\psi^{-i} \pmod{2^{2l}+1}$, $0 \le i < d$.
4. Вычислить коэффициенты $c_i' \equiv c_i \pmod{d}$ следующим образом.

   4.1. Найти числа $a' \leftarrow \sum_{i=0}^{d-1} a_i' 2^{(3\log_2 d)i}$, $b' \leftarrow \sum_{i=0}^{d-1} b_i' 2^{(3\log_2 d)i}$, где $a_i' \equiv a_i \pmod{d}$, $b_i' \equiv b_i \pmod{d}$ для $0 \le i \le d-1$.

4.2. Вычислить произведение $v \leftarrow a'b' = \sum_{i=0}^{2d-1} v_i 2^{(3\log_2 d)i}$, где

$v_i = \sum_{j=0}^{2d-1} a'_j b'_{i-j}$ алгоритмом Карацубы–Офмана.

4.3. Для $i = 0, 1, \ldots, d-1$ положить $c'_i \equiv v_i - v_{d+i} \pmod d$.

5. Каждую из координат $c_i$ вектора произведения восстановить по китайской теореме об остатках для взаимно простых модулей $2^{2l}+1$ и $d$, при этом $-(d-1-i)\cdot 2^{2l} \le c_i \le (i+1)\cdot 2^{2l}$, $0 \le i < d$.

6. Вычислить точное значение произведения $c \equiv \sum_{i=0}^{d-1} c_i 2^{li} \pmod{2^{2n}+1}$.

7. Результат: $c$. □

Сложность алгоритма 4.6 равна $O(n \log n \log\log n)$.

Пример 4.13. Вычислим алгоритмом Шенхаге–Штрассена произведение чисел $a = 1979678689$ и $b = 3988965357$.

Здесь $n = 32$, то есть $k = 5$. Выбираем $2l = 16$, тогда $l = 8$, $d = 8$. Представляем числа $a$ и $b$ в системе счисления с основанием $2^l = 2^8 = 256$:

$$a = (117)_{256}\cdot(2^8)^3 + (255)_{256}\cdot(2^8)^2 + (127)_{256}\cdot(2^8)^1 + (225)_{256}\cdot(2^8)^0,$$

$$b = (237)_{256}\cdot(2^8)^3 + (194)_{256}\cdot(2^8)^2 + (199)_{256}\cdot(2^8)^1 + (237)_{256}\cdot(2^8)^0$$

и полагаем

$$\mathbf{a} = ((225)_{256}, (127)_{256}, (255)_{256}, (117)_{256}, 0_{256}, 0_{256}, 0_{256}, 0_{256})^{\mathrm{T}},$$

$$\mathbf{b} = ((237)_{256}, (199)_{256}, (194)_{256}, (237)_{256}, 0_{256}, 0_{256}, 0_{256}, 0_{256})^{\mathrm{T}}.$$

Для $i = 0, 1, \ldots, d-1$ умножаем $i$-ю координату векторов $\mathbf{a}$ и $\mathbf{b}$ на $\psi = 4$ — примитивный корень степени $2d = 16$ из единицы (согласно теореме о существовании примитивного корня, $m = 2^{16}+1 = \psi^d + 1 = \psi^8 + 1$, откуда $\psi = 2^2 = 4$):

$$\mathbf{a}' = ((225)_{256}, \psi\cdot(127)_{256}, \psi^2\cdot(255)_2, \psi^3\cdot(117)_2, 0, 0, 0, 0)^{\mathrm{T}}$$

и

$$\mathbf{b}' = ((237)_{256}, \psi \cdot (199)_{256}, \psi^2 \cdot (194)_{256}, \psi^3 \cdot (237)_{256}, 0, 0, 0, 0)^{\mathrm{T}}$$

и вычисляем преобразование Фурье по модулю $2^{2l} + 1 = 2^{16} + 1$ векторов $\mathbf{a}'$ и $\mathbf{b}'$, используя в качестве примитивного корня степени $d = 8$ из единицы $\omega = \psi^2 = 16$. Получаем

$$F(\mathbf{a}') = (12301, 3773, 44301, 42192, 61846, 53990, 13526, 32019)^{\mathrm{T}},$$

$$F(\mathbf{b}') = (19305, 20205, 53510, 21700, 52914, 62166, 6293, 27951)^{\mathrm{T}}.$$

Покомпонентное произведение этих векторов равно (все произведения берем по модулю $2^{2l} + 1$)

$$F(\mathbf{a}') \cdot F(\mathbf{b}') = (30254, 13934, 7683, 14510, 60223, 61496, 52092, 55334)^{\mathrm{T}}.$$

Обратным преобразованием Фурье этого вектора будет вектор

$$F^{-1}(F(\mathbf{a}') \cdot F(\mathbf{b}')) = (53325, 37348, 38081, 50344, 49775, 61166, 2363, 0)^{\mathrm{T}}.$$

Для $i = 0, 1, \ldots, d - 1$ умножаем $i$-ю координату на $\psi^{-i} \pmod{2^{2l} + 1}$:

$$\mathbf{c}'' = (53325, 9337, 63821, 25363, 37315, 17596, 27729, 0)^{\mathrm{T}}$$

— отрицательно обернутая свертка векторов $\mathbf{a}$ и $\mathbf{b}$, согласно теореме 4.6.

Теперь вычислим коэффициенты $c_i' \equiv c_i \pmod{d}$. Учитывая, что $3 \log_2 d = 9$, $2^9 = 512$, находим

$$a' = (0, 0, 0, 0, 5, 7, 7, 1)_{512},$$

$$b' = (0, 0, 0, 0, 5, 2, 7, 5)_{512},$$

откуда

$$v = (0, 0, 0, 0, 0, 0, 0, 0, 0, 25, 45, 84, 93, 86, 42, 5)_{512}.$$

Тогда $\mathbf{c}' = (5, 2, 6, 5, 4, 5, 1, 0)^{\mathrm{T}}$.

Восстанавливаем координаты вектора произведения из $\mathbf{c}'$ и $\mathbf{c}''$ по китайской теореме об остатках:

$$\mathbf{c} = (53325, 74874, 129358, 156437, 102852, 83133, 27729, 0)^{\mathrm{T}}.$$

Находим точное значение произведения:

$$c = 53325 \cdot (2^8)^0 + 74874 \cdot (2^8)^1 + 129358 \cdot (2^8)^2 + 156437 \cdot (2^8)^3 +$$

$$+ 102852 \cdot (2^8)^4 + 83133 \cdot (2^8)^5 + 27729 \cdot (2^8)^6 + 0 \cdot (2^8)^7 =$$

$$= 7896869708412176973.$$

Таким образом, $1979678689 \cdot 3988965357 = 7896869708412176973$.□

## 4.4. Модульное умножение

Модульное умножение — наиболее часто встречающаяся операция в алгоритмах криптографии с открытым ключом. Обычно приходится выполнять умножение целых чисел по простому или составному модулю или умножение полиномов по модулю неприводимого полинома.

Если выполнять модульное умножение непосредственно, сначала перемножая целые числа (полиномы), а потом вычисляя остаток от деления (см. п. 4.5), то сложность алгоритма будет определяться процедурой нахождения остатка. Рассмотрим методы модульного умножения, не требующие деления.

Наиболее просто выполняется умножение по модулю чисел $p$ вида $p = 2^n \pm 1$. Для этого нужно вычислить целочисленное произведение сомножителей и представить его в виде $2^n A + B$, где $B$ — младшие $n$ бит произведения. Произведение по модулю $p$ будет равно $B \mp A \pmod p$.

Обобщением этого метода является умножение по модулю чисел $p = 2^n \pm c$ для малого $c$. В этом случае, если $ab = 2^n A + B$, где $B < 2^n$, то $ab \equiv B \mp cA \pmod p$. При необходимости применяется рекурсия.

### 4.4.1. Метод Монтгомери

Этот метод, предложенный П. Монтгомери (P. Montgomery) в 1985 году, не требует выполнения операции деления [7].

Определение 4.6. Пусть $N$ — нечетное число, по модулю которого выполняется операция умножения. Выберем число $R$, равное сте-

пени числа 2 и превышающее $N$. Определим *N-вычет* числа $a$ по модулю $N$ как $aR \pmod N$ и *произведение Монтгомери* чисел $a$ и $b$ по модулю $N$ как

$$MP(a, b, N, R) \equiv abR^{-1} \pmod N.$$

Для вычисления вычета $TR^{-1} \pmod N$ по заданному числу $T$ воспользуемся *преобразованием Монтгомери*, которое выполняется следующим алгоритмом.

Алгоритм 4.7. Вычисление преобразования Монтгомери.

*Вход.* $T = (t_{2n-1}, t_{2n-2}, \ldots, t_0)_B$, $B = 2^m$ (процессор оперирует со словами длины $m$ битов), $R = B^n$, $N = (N_{n-1}, N_{n-2}, \ldots, N_0)_B$, $N < R$, $N' \equiv -N^{-1} \pmod B$ ($N'$ — одиночное слово).

*Выход.* $TR^{-1} \pmod N$.

1. Положить $U \leftarrow T$, $U = (u_{2n-1}, u_{2n-2}, \ldots, u_0)_B$.
2. Для $i = 0, 1, \ldots, n-1$ вычислить $v_i \leftarrow u_i N' \pmod B$, $U \leftarrow U + v_i N B^i$.
3. $U \leftarrow \dfrac{U}{R}$.
4. Если $U \geq N$, то $U \leftarrow U - N$.
5. Результат: $U$. □

Корректность алгоритма обосновывается следующей теоремой.

Теорема 4.9. Пусть $N$ и $R$ — взаимно простые положительные целые числа, $N' \equiv -N^{-1} \pmod R$. Тогда для любого целого $0 \leq T \leq RN$ и $M \equiv TN' \pmod R$ число $t = \dfrac{T + MN}{R}$ — целое и $TR^{-1} \pmod N = t$ или $t - N$.

*Доказательство.* Запишем цепочку сравнений:

$$T + MN \equiv T + T\,N'N \equiv T + T(-N^{-1})N \equiv T - T \equiv 0 \pmod R,$$

то есть сумма $T + MN$ делится на $R$.

Теперь оценим значение $TR^{-1} \pmod N$. Поскольку $tR = T + MN$, выполняется сравнение $tR \equiv T \pmod N$, то есть $t \equiv TR^{-1} \pmod N$. Всегда можно считать $0 \le M < R$, поэтому $0 \le T + MN < RN + RN$, то есть $0 \le t < 2N$, и вычитание на шаге 4 алгоритма 4.7 дает величину, меньшую $N$. □

Для вычисления произведения Монтгомери $MP(a, b, N, R)$ достаточно перемножить операнды $a$ и $b$ как целые числа, а затем выполнить преобразование Монтгомери. Но можно действовать исключительно в терминах $N$-вычетов. Для вычисления произведения $ab \pmod N$ сначала переводят числа $a$ и $b$ в $N$-вычеты, вычисляя $MP(a, R^2 \pmod N, N, R) \equiv$ $\equiv aR \pmod N$, $bR = MP(b, R^2 \pmod N, N, R) \equiv bR \pmod N$. Затем находят произведение $N$-вычетов:

$$MP(aR, bR, N, R) \equiv (aR)(bR)R^{-1} \equiv (ab)R \pmod N.$$

И, наконец, выполняют обратное преобразование $N$-вычета в число: $MP((ab)R, 1, N, R) \equiv ((ab)R)R^{-1} \equiv ab \pmod N$.

Алгоритм 4.8. Умножение $N$-вычетов.

*Вход.* $N$-вычеты $aR \pmod N = (a_{n-1}, a_{n-2}, \ldots, a_0)_B$, $bR \pmod N = (b_{n-1}, b_{n-2}, \ldots, b_0)_B$, где $B = 2^m$, $R = B^n$, $N' \equiv -N^{-1} \pmod B$.

*Выход.* $N$-вычет $c \equiv (ab)R \pmod N$.

1. Положить $c \leftarrow 0$, $c = (c_{n-1}, c_{n-2}, \ldots, c_0)_B$.
2. Для $i = 0, 1, \ldots, n-1$ выполнить следующие действия.
   2.1. Положить $u_i \leftarrow (c_0 + a_i b_0) N' \pmod B$.
   2.2. Вычислить $c = \dfrac{c + a_i\left(bR \left(\bmod N\right)\right) + u_i N}{B}$.
3. При $c \ge N$ положить $c \leftarrow c - N$.
4. Результат: $c$. □

Заметим, что сумма $N$-вычетов также является $N$-вычетом:

$$AR + BR \equiv (A + B)R \pmod N,$$

поэтому множество $N$-вычетов с операциями умножения по Монтгомери и сложения является кольцом.

Пример 4.14. Найдем произведение чисел $a = 30000$ и $b = 45678$ методом Монтгомери.

Исходные данные: $N = 64553$, $R = 65536 = 2^{16}$, $B = 16 = 2^4$.

Вычисляем вспомогательные параметры: $N' = 7$, $R^2 \equiv 62547 \pmod N$.

Алгоритмом 4.8 переводим числа $a$ и $b$ в $N$-вычеты, перемножаем эти $N$-вычеты и выполняем обратное преобразование. Результаты вычислений сведем в таблицу:

| Произведение Монтгомери | $i$ | $u_i \pmod{16}$ | $C$ |
|---|---|---|---|
| $MP(a, R^2 \pmod N, N, R)$ | 0 | 0 | 0 |
| | 1 | 15 | 7693 |
| | 2 | 4 | 36165 |
| | 3 | 6 | **53832** |
| $MP(B, R^2 \pmod N, N, R)$ | 0 | 6 | 14383 |
| | 1 | 7 | 52596 |
| | 3 | 6 | 35313 |
| | 4 | 14 | **37139** |
| $MP(aR, bR, N, R)$ | 0 | 8 | 50846 |
| | 1 | 6 | 36670 |
| | 2 | 12 | 55349 |
| | 3 | 4 | **49773** |
| $MP((ab)R, 1, N, R)$ | 0 | 11 | 44381 |
| | 1 | 5 | 22947 |
| | 2 | 3 | 13538 |
| | 3 | 2 | **8916** |

Таким образом, $aR \equiv 53832 \pmod N$, $bR \equiv 37139 \pmod N$, $(ab)R \equiv$ $\equiv 49773 \pmod N$, $ab \equiv 8916 \pmod N$. □

В арифметике Монтгомери можно выполнять не только умножение, но также сложение и возведение в степень. При этом нет необходимости переводить промежуточные результаты из $N$-вычетов в обычное представление.

Асимптотическая сложность алгоритма умножения Монтгомери такая же, как и у алгоритма, выполняющего сначала умножение операндов «в столбик», а затем деление с остатком. Однако, если требуется не одиночное умножение, а цепочка умножений и сложений, то случае можно исключить преобразование произведения из $N$-вычета в обычную форму и преобразование операндов в $N$-вычеты. Тогда сложность умножения алгоритмом Монтгомери составляет $2n(n + 1)$ обычных умножений слов.

Алгоритм Монтгомери можно применять и для модульного умножения полиномов. Если нужно вычислить произведение полиномов по модулю $N(x)$, то следует выбрать вспомогательный полином $R(x)$ удобного вида, например, $R(x) = x^{n+1}$, $\deg(R) > \deg(N)$, найти расширенным алгоритмом Евклида такие полиномы $R^{-1}(x)$, $N'(x)$, что $R(x)R^{-1}(x) -$ $- N(x)N'(x) = 1$, а затем выполнить вычисления, аналогичные алгоритму 4.8. Отличие заключается в том, что на последнем шаге после деления на $R(x)$ всегда получается $\deg(U) < \deg(N)$, поэтому операция вычитания $N(x)$ не требуется.

### 4.4.2. Модульное возведение в степень

Многие криптографические протоколы (RSA, протокол Диффи–Хеллмана, см. главы 6, 7), а также соответствующие методы анализа требуют модульного возведения целого числа $a$ в произвольную степень $n \geq 3$. При обычном рекурсивном способе: $a^0 = 1$, $a^n \equiv (a^{n-1}) \cdot a \pmod m$

требуется $n-1$ операций возведения в степень по модулю $m$, то есть $O(m^2)$ операций модульного умножения. Если же предварительно представить показатель $n$ в двоичном виде: $n = 2^k n_k + 2^{k-1} n_{k-1} + \ldots + 2n_1 + n_0$, то есть $n = (n_k, n_{k-1}, \ldots, n_0)_2$, где $k = [\log_2 n]$, $n_i \in \{0, 1\}$, то $a^n = (a^{2^k})^{n_k} (a^{2^{k-1}})^{n_{k-1}} \ldots (a^2)^{n_1} a^{n_0}$, где $a^{2^k} = (a^{2^{k-1}})^2 \pmod m$. При таком способе вычисления потребуется $k$ модульных возведений в квадрат и $\delta(n) - 1$ модульных умножений, где $\delta(n) = \sum_{i=0}^{k} n_i$ — число единиц в двоичном представлении показателя $n$. Учитывая, что каждый разряд принимает значение 0 или 1 равновероятно, можно считать, что $\delta(n) = \frac{k}{2}$ и в среднем требуется 1,5 $\log m$ модульных умножений.

Отсюда получаем следующий алгоритм модульного возведения в степень.

Алгоритм 4.9. Модульное возведение в степень [2].

*Вход.* Целое число $a$, $1 \le a < m$; показатель степени $n \ge 2$, $n = (n_k, n_{k-1}, \ldots, n_0)_2$.

*Выход.* $c \equiv a^n \pmod m$.

1. Положить $c \leftarrow a^{n_k}$.
2. Для $i = k-1, k-2, \ldots, 0$ выполнить следующие действия.
   2.1. Вычислить $c \leftarrow c^2 \pmod m$.
   2.2. При $n_i = 1$ вычислить $c \leftarrow ca \pmod m$.
3. Результат: $c$. □

Пример 4.15. Возведем $a = 583$ в степень $n = 3571$ по модулю $m = 13129651$. Находим двоичное представление показателя: $n = (110111110011)_2$, то есть $k = 11$. На шаге 1 полагаем $c = 583$. Дальнейшие вычисления сведем в таблицу:

| $k$ | $c \equiv c^2 \pmod m$ | $n_k$ | $c \equiv ca \pmod m$ |
|---|---|---|---|

| $k$ | $c \equiv c^2 \pmod m$ | $n_k$ | $c \equiv ca \pmod m$ |
|---|---|---|---|
| 10 | 339889 | 1 | 1210522 |
| 9 | 2553327 | 0 | |
| 8 | 3083483 | 1 | 12038053 |
| 7 | 4717099 | 1 | 5971658 |
| 6 | 2577971 | 1 | 6176879 |
| 5 | 579862 | 1 | 9818271 |
| 4 | 9471750 | 1 | 7576830 |
| 3 | 4223480 | 0 | |
| 2 | 10147263 | 0 | |
| 1 | 8631198 | 1 | 3332101 |
| 0 | 4650816 | 1 | 6717622 |

Таким образом, $583^{3571} \equiv 6717622 \pmod{13129651}$. □

Этот метод возведения в степень иногда называют *бинарным*. Обобщением его является *B-арный* метод, в котором показатель $n$ раскладывается уже не по степеням двойки, а по степеням произвольного числа $B$: $n = \sum_{i=0}^{k} n_i B^i$, где $0 \le n_i < B$, $i = 0, 1, \ldots, k$.

Алгоритм 4.10. $B$-арное модульное возведение в степень [2].

*Вход*. Целое число $a$, $1 \le a < m$; показатель степени $n \ge 2$, $n = (n_k, n_{k-1}, \ldots, n_0)_B$.

*Выход*. $c \equiv a^n \pmod m$.

1. Составить таблицу предвычислений: $a^2 \pmod m$, $a^3 \pmod m$, …, $a^{B-1} \pmod m$.
2. Положить $c \leftarrow a^{n_k}$.
3. Для $i = k-1, k-2, \ldots, 0$ выполнить следующие действия.

   3.1. Вычислить $c \leftarrow c^B \pmod m$.

3.2. При $n_i > 0$ выбрать из таблицы значение $a^{n_i} \pmod m$ и положить $c \leftarrow ca^{n_i} \pmod m$.

4. Результат: $c$. □

В качестве основания $B$ обычно выбирают степень числа 2, чтобы максимально сократить число выполнений шага 3.2.

Пример 4.16. Снова возведем $a = 583$ в степень $n = 3571$ по модулю $m = 13129651$, теперь уже представляя показатель степени в системе счисления с основанием 16. Тогда $n = (\mathrm{df3})_{16}$, то есть $k = 2$. Таблица предвычислений имеет вид:

| $i$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| $a^i$ | 339889 | 1210522 | 9862823 | 12368322 | 2553327 | 4939078 | 4088905 |

| $i$ | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|
| $a^i$ | 7364784 | 273195 | 1716873 | 3083483 | 12038053 | 6951265 | 8654987 |

Из таблицы берем значение $c \equiv a^{13} \equiv 12038053 \pmod m$. Далее, при $i = 1$, $c \equiv 4160635 \pmod m$, $n_1 = \mathrm{f}_{16}$ полагаем $c = 4160635 \cdot a^{15} = 4160635 \cdot 8654987 \equiv 7576830 \pmod m$; при $i = 0$, $c \equiv 4789459 \pmod m$, $n_0 = 3_{16}$ вычисляем $c = 4789459 \cdot a^3 = 4789459 \cdot 1210522 \equiv 6717622 \pmod m$. □

## 4.5. Целочисленное деление с остатком

Операция взятия целого числа $a$ по модулю $p$ представляет собой, по сути, целочисленное деление с остатком $a$ на $p$ и определяет скорость алгоритмов модульной арифметики.

### 4.5.1. Схема Горнера

Пусть $a(x)=\sum_{i=0}^{n} a_i x^i$ — полином с вещественными или комплексными коэффициентами. Обозначим $P_i(x)=\sum_{j=i}^{n} a_j x^{j-i}$. Тогда

$$P_0(x)=\sum_{j=0}^{n} a_j x^j = a(x), \quad P_n(x)=a_n$$

и для $i \geq 0$ выполняется соотношение

$$P_i(x)=\sum_{j=i}^{n} a_j x^{j-i} = a_i + \sum_{j=i+1}^{n} a_j x^{j-i} = a_i + x\sum_{j=i+1}^{n} a_j x^{j-(i+1)} = a_i + xP_{i+1}(x).$$

Обозначая $q_i = P_i(x_0)$ для некоторого $x_0$, получаем алгоритм Горнера для вычисления значения полинома $a(x)$ в точке $x = x_0$.

Алгоритм 4.11. Схема Горнера.

*Вход*. Полином $a(x)=\sum_{i=0}^{n} a_i x^i$, $x_0$.

*Выход*. $b = a(x_0)$.

1. Положить $q_n \leftarrow a_n$.
2. Для $i = n-1, n-2, \ldots, 0$ полагать $q_i \leftarrow a_i + x_0 \cdot q_{i+1}$.
3. Результат: $b \leftarrow q_0$. □

Сложность алгоритма 4.11 равна $O(n)$.

Теорема 4.10. Полином $q(x)=\sum_{i=0}^{n-1} q_{i+1} x^i$ является неполным частным от деления полинома $a(x)$ на $x - x_0$.

*Доказательство*. Запишем

$$q(x)\cdot(x-x_0)+a(x_0)=\sum_{i=0}^{n-1}q_{i+1}x^i\cdot(x-x_0)+q_0=$$

$$=\sum_{i=0}^{n-1}q_{i+1}x^{i+1}-\sum_{i=0}^{n-1}x_0q_{i+1}x^i+q_0=\sum_{i=1}^{n}q_ix^i-\sum_{i=0}^{n-1}x_0q_{i+1}x^i+q_0=$$

$$=q_nx^n+\sum_{i=0}^{n-1}q_ix^i-\sum_{i=0}^{n-1}x_0q_{i+1}x^i=a_nx^n+\sum_{i=0}^{n-1}(q_i-x_0q_{i+1})x^i=$$

$$=a_nx^n+\sum_{i=0}^{n-1}a_ix^i=a(x).$$ □

Схему Горнера можно использовать и для деления целого $n$-разрядного числа $a=(a_{n-1}, a_{n-2}, \ldots, a_0)_B$ на одноразрядное число $b$, $0<b<B$, при этом полагаем $a_n=0$.

Алгоритм 4.12. Деление на одноразрядное число.

*Вход*. Целые числа $a=(a_{n-1}, a_{n-2}, \ldots, a_0)_B$ и $b$, где $0<b<B$.

*Выход*. Такие целые числа $q=(q_{n-1}, q_{n-2}, \ldots, q_0)_B$ и $r$, что $a=qb+r$, $0\le r<B$.

1. Положить $r\leftarrow 0$.
2. Для $i=n-1, n-2, \ldots, 0$ выполнить следующие действия.
   2.1. Вычислить $t\leftarrow a_i+r\cdot B$.
   2.2. Положить $q_i\leftarrow\left[\dfrac{t}{b}\right]$, $r\leftarrow t \pmod b$.
3. Результат: $q=(q_{n-1}, q_{n-2}, \ldots, q_0)_B$, $r$. □

Пример 4.17. Разделим с остатком число

$$a=29876543212345678=(106, 36, 142, 201, 73, 217, 78)_{256}$$

на $b=19$. В обозначениях алгоритма 4.12 имеем $B=256$, $n=7$. Результаты вычислений запишем в таблицу:

| $i$ | $t$ | $q_i$ | $r$ |
|---|---|---|---|
| 6 | $a_6+r\cdot B=(0, 106)_{256}=106$ | $5_{256}$ | $(11)_{256}$ |
| 5 | $a_5+r\cdot B=(11, 36)_{256}=2852$ | $(150)_{256}$ | $2_{256}$ |

| $i$ | $t$ | $q_i$ | $r$ |
|---|---|---|---|
| 4 | $a_4 + r \cdot B = (2, 142)_{256} = 654$ | $(34)_{256}$ | $8_{256}$ |
| 3 | $a_3 + r \cdot B = (8, 201)_{256} = 2249$ | $(118)_{256}$ | $7_{256}$ |
| 2 | $a_2 + r \cdot B = (7, 73)_{256} = 1865$ | $(98)_{256}$ | $3_{256}$ |
| 1 | $a_1 + r \cdot B = (3, 217)_{256} = 985$ | $(51)_{256}$ | $(16)_{256}$ |
| 0 | $a_0 + r \cdot B = (16, 78)_{256} = 4174$ | $(219)_{256}$ | $(13)_{256}$ |

Получили неполное частное $q = (5, 150, 34, 118, 98, 51, 219)_{256} =$ $= 1572449642755035$ и остаток $r = (13)_{256} = 13$. □

### 4.5.2. Деление на $2^m - c$

Просто выполняется деление и в том случае, когда делитель имеет вид $2^m - c$, где число $c$ мало.

Алгоритм 4.13. Вычисление остатка о деления на $2^m - c$.

*Вход*. Делимое $a$, делитель $p = 2^m - c$.

*Выход*. $a \pmod p$.

1. Представить число $a$ в системе счисления с основанием $B = 2^m$: $a = (a_k, a_{k-1}, \ldots, a_0)_B$.
2. Если $k = 0$, то при $a_0 \geq p$ положить $a_0 \leftarrow a_0 - p$. Результат: $a_0$.
3. Положить $t \leftarrow a_k$.
4. Для $i = k - 1, k - 2, \ldots, 0$ выполнить следующие действия.
   4.1. Положить $t \leftarrow tc + a_i$.
   4.2. Пока $t > B$, выполнять: $t_0 \leftarrow t \pmod B$, $t_1 \leftarrow \dfrac{t - t_0}{B}$, $t \leftarrow t_1 c + t_0$.
5. При $t \geq p$ положить $t \leftarrow t - p$.
6. Результат: $t$. □

Пример 4.18. Пусть $p = 2^{32} - 522279 = (\text{fff807d9})_{16}$, $c = 522279 =$ $= (7f827_{16})$. Найдем остаток от деления на $p$ числа

$$a = (\text{fedcba098765432ffeeddccbbaabcdef})_{16}.$$

Представляем $a$ в системе счисления с основанием $2^{32}$:

$$a = ((\text{fedcba09})_{16}, (\text{8765432f})_{16}, (\text{feeddccb})_{16}, (\text{baabcdef})_{16})_{2^{32}}$$

и полагаем $t = (\text{fedcba09})_{16}$.

Результаты вычислений на шаге 4 запишем в таблицу:

| $i$ | $t = tc + a_i$ | $t_0 \pmod{2^{32}}$ | $t_1$ | $t = t_1c + t_0$ | $t > B$ |
|---|---|---|---|---|---|
| 2 | $(\text{7ef16457d528e})_{16}$ | $(\text{457d528})\text{e}_{16}$ | $(\text{7ef16})_{16}$ | $(\text{3f7fea0ee8})_{16}$ | Да |
| | | $(\text{7fea0ee8})_{16}$ | $(\text{3f})_{16}$ | $(\text{81e02081})_{16}$ | Нет |
| 1 | $(\text{40b06cb16c872})_{16}$ | $(\text{cb16c872})_{16}$ | $(\text{40b06})_{16}$ | $(\text{21038c465c})_{16}$ | Да |
| | | $(\text{38c465c})_{16}$ | $(\text{21})_{16}$ | $(\text{4934363})_{16}$ | Нет |
| 0 | $(\text{2476ee17fa04})_{16}$ | $(\text{ee17fa04})_{16}$ | $(\text{2476})_{16}$ | $(\text{210a9d7fe})_{16}$ | Да |
| | | $(\text{10a9d7fe})_{16}$ | $2_{16}$ | $(\text{10b9c84c})_{16}$ | Нет |

Результат: $a \equiv (\text{10b9c84c})_{16} \pmod{2^{32} - 522279}$. □

Аналогично можно реализовать и алгоритм деления на разреженный полином.

### 4.5.3. Общий случай

Для деления в общем случае используем алгоритм Д. Кнута [3]. Будем делить «в столбик» число $a = (a_{m+n-1}, a_{m+n-2}, \ldots, a_0)_B$ на число $b = (b_{n-1}, b_{n-2}, \ldots, b_0)_B$. Найдем такое частное $q = (q_m, q_{m-1}, \ldots, q_0)_B$ и остаток $r = (r_{n-1}, r_{n-2}, \ldots, r_0)_B$, что $a = qb + r$ (см. теорему 1.1).

При делении на каждом шаге находим частное $Q = \left[\frac{R}{b}\right]$ от деления некоторого $(n+1)$-разрядного числа $R = (R_n, R_{n-1}, \ldots, R_0)_B$ на $b$, где $0 \le \frac{R}{b} < B$. Неравенство $\frac{R}{b} < B$ эквивалентно неравенству $\frac{R}{B} < b$, откуда

$$(b_{n-1}, b_{n-2}, \ldots, b_0)_B = b > \left[\frac{R}{B}\right] = \left[\frac{(R_n, R_{n-1}, \ldots, R_0)_B}{B}\right] = (R_n, R_{n-1}, \ldots, R_1)_B.$$

Полагая $R = R - Qb$, получаем $0 \le R < b$.

Для определения числа $Q$ будем использовать аппроксимацию

$$\tilde{q} = \min\left(\left[\frac{R_n B + R_{n-1}}{b_{n-1}}\right], B-1\right). \tag{4.5}$$

При $R_n = b_{n-1}$ получаем $\frac{R_n B + R_{n-1}}{b_{n-1}} = \frac{b_{n-1}B + R_{n-1}}{b_{n-1}} = B + \frac{R_{n-1}}{b_{n-1}} \ge B$ и $\tilde{q} = B-1$, то есть определение наименьшего из двух чисел в выражении (4.5) сводится к проверке равенства $R_n = b_{n-1}$.

Теорема 4.11. Пусть $R = (R_n, R_{n-1}, \ldots, R_0)_B$, $b = (b_{n-1}, b_{n-2}, \ldots, b_0)_B$. Если $b_{n-1} \ge \left[\frac{B}{2}\right]$, то значение $Q = \left[\frac{R}{b}\right]$ удовлетворяет неравенству

$$\tilde{q} - 2 \le Q \le \tilde{q}, \tag{4.6}$$

где $\tilde{q}$ определяется из соотношения (4.5).

*Доказательство.* Поскольку $Q \le \frac{R}{b} \le B-1$, при $\tilde{q} = B-1$ неравенство $Q \le \tilde{q}$ выполнено. Предположим, что $\tilde{q} = \left[\frac{R_n B + R_{n-1}}{b_{n-1}}\right]$. Запишем

$$R = R_n B^n + R_{n-1}B^{n-1} + \alpha, \quad b = b_{n-1}B^{n-1} + \beta,$$

где $0 \le \alpha < B^{n-1}$, $0 \le \beta < B^{n-1}$.

По определению целой части числа выполняется неравенство $R_n B + R_{n-1} - \tilde{q} b_{n-1} \le b_{n-1} - 1$, тогда

$$\begin{aligned} R - \tilde{q}b &= R_n B^n + R_{n-1}B^{n-1} + \alpha - \tilde{q}(b_{n-1}B^{n-1} + \beta) = \\ &= (R_n B + R_{n-1} - \tilde{q}b_{n-1})B^{n-1} + \alpha - \tilde{q}\beta \le \\ &\le (b_{n-1} - 1)B^{n-1} + \alpha - \tilde{q}\beta < b_{n-1}B^{n-1} - \tilde{q}\beta \le b_{n-1}B^{n-1} < b. \end{aligned}$$

Отсюда $\frac{R}{b} < \tilde{q}+1$ и $Q \le \tilde{q}$, и правая часть неравенства (4.6) выполняется для любого $\tilde{q}$.

Предположим теперь, что $\tilde{q} \ge Q+3$. Из соотношения (4.5) имеем неравенство

$$\tilde{q} \le \frac{R_n B + R_{n-1}}{b_{n-1}} = \frac{R_n B^n + R_{n-1} B^{n-1}}{b_{n-1} B^{n-1}} \le \frac{R}{b_{n-1} B^{n-1}} < \frac{R}{b - B^{n-1}}$$

(знаменатель в последней дроби не равен нулю, поскольку иначе получили бы $\tilde{q} = q$).

Учитывая, что $Q \le \frac{R}{b} < Q+1$, получаем

$$3 \le \tilde{q} - Q < \frac{R}{b - B^{n-1}} - \frac{R}{b} + 1 = \frac{RB^{n-1}}{b(b - B^{n-1})} + 1 = \frac{R}{b} \cdot \frac{1}{\frac{b}{B^{n-1}} - 1} + 1 \le \frac{R}{b} \cdot \frac{1}{b_{n-1} - 1} + 1,$$

то есть

$$\frac{R}{b} > 2(b_{n-1} - 1) \ge 2 \cdot \left( \left[ \frac{B}{2} \right] - 1 \right) > 2 \cdot \left( \frac{B}{2} - 2 \right) = B - 4.$$

Но $\tilde{q} \le B - 1$, тогда $\frac{R}{b} > B - 4 \ge \tilde{q} - 3 \ge Q \ge \frac{R}{b}$. Получили противоречие, то есть $\tilde{q} < Q+3$. □

Лемма 4.12. Если в обозначениях, введенных выше, выполняется неравенство $b_{n-2}\tilde{q} \le (R_n B + R_{n-1} - \tilde{q} b_{n-1})B + R_{n-2}$ и $b_{n-1} > 0$, то $Q \ge \tilde{q} - 1$.

*Доказательство.* Запишем

$$R = R_n B^n + R_{n-1} B^{n-1} + R_{n-2} B^{n-2} \alpha, \quad b = b_{n-1} B^{n-1} + b_{n-2} B^{n-2} + \beta,$$

где $0 \le \alpha < B^{n-2}$, $0 \le \beta < B^{n-2}$.

Тогда

$$R - \tilde{q} b = R_n B^n + R_{n-1} B^{n-1} + R_{n-2} B^{n-2} - \tilde{q} b_{n-1} B^{n-1} - \tilde{q} b_{n-2} B^{n-2} + \alpha - \tilde{q}\beta =$$
$$= (R_n B^2 + R_{n-1} B + R_{n-2} - \tilde{q} b_{n-1} B - \tilde{q} b_{n-2}) B^{n-2} + \alpha - \tilde{q}\beta =$$

$$= (((R_n B + R_{n-1} - \tilde{q} b_{n-1}) B + R_{n-2}) - \tilde{q} b_{n-2}) B^{n-2} + \alpha - \tilde{q}\beta \geq$$
$$\geq (\tilde{q} b_{n-2} - \tilde{q} b_{n-2}) B^{n-2} + \alpha - \tilde{q}\beta \geq$$
$$\geq \alpha - \tilde{q}\beta \geq -\tilde{q}\beta > -B \cdot \beta = B \cdot (-\beta) > -B^{n-1} > -b_{n-1} B^{n-1} \geq -b.$$

Отсюда $\dfrac{R}{b} > \tilde{q} - 1$ и $Q \geq \tilde{q} - 1$. □

Приведем теперь алгоритм деления с остатком. Чтобы старший разряд делителя удовлетворял условию теоремы 4.11, числа $a$ и $b$ нужно умножить на некоторое целое число $d > 0$, такое, что $\tilde{b}_{n-1} \geq \left[\dfrac{B}{2}\right]$, где

$$\tilde{a} = a \cdot d = (\tilde{a}_{m+n}, \tilde{a}_{m+n-1}, \ldots, \tilde{a}_0)_B, \quad \tilde{b} = b \cdot d = (\tilde{b}_{n-1}, \tilde{b}_{n-2}, \ldots, \tilde{b}_0)_B.$$

Частное при этом не изменится: $\left[\dfrac{\tilde{a}}{\tilde{b}}\right] = \left[\dfrac{a}{b}\right]$. Число разрядов в $\tilde{b}$ не должно превышать число разрядов в $b$; число разрядов в $\tilde{a}$ может быть на единицу больше, чем в $a$ (если это не так, полагаем $a_{m+n} = 0$). Удобно выбирать $d$ равным степени двойки, так как умножение на $d$ в этом случае выполняется сдвигом.

Алгоритм 4.14. Деление «в столбик».

*Вход*. Неотрицательные целые числа $a = (a_{m+n-1}, a_{m+n-2}, \ldots, a_0)_B$, $b = (b_{n-1}, b_{n-2}, \ldots, b_0)_B$, $b \neq 0$; таблица деления 2-разрядного числа на 1-разрядное.

*Выход*. Целые числа $q = (q_m, q_{m-1}, \ldots, q_0)_B$, $r = (r_{n-1}, r_{n-2}, \ldots, r_0)_B$, такие, что $a = qb + r$, $0 \leq r < b$.

1. Определить такое целое число $d > 0$, что $\tilde{b}_{n-1} \geq \left[\dfrac{B}{2}\right]$, где $(\tilde{b}_{n-1}, \tilde{b}_{n-2}, \ldots, \tilde{b}_0)_B = (b_{n-1}, b_{n-2}, \ldots, b_0)_B \cdot d$.
2. Положить $(r_{m+n}, r_{m+n-1}, r_{m+n-2}, \ldots, r_0)_B \leftarrow (0, a_{m+n-1}, a_{m+n-2}, \ldots, a_0)_B$.
3. Для $i = m + n, m + n - 1, \ldots, n$ выполнить следующие действия.

3.1. Если $\tilde{r}_i = \tilde{b}_{n-1}$, то положить $\tilde{q} \leftarrow B-1$; в противном случае определить по таблице $\tilde{q} \leftarrow \left[\dfrac{\tilde{r}_i B + \tilde{r}_{i-1}}{\tilde{b}_{n-1}}\right]$, где $(\tilde{r}_i, \tilde{r}_{i-1}, \ldots, \tilde{r}_{i-n})_B = (r_i, r_{i-1}, \ldots, r_{i-n})_B \cdot d$.

3.2. Пока $\tilde{b}_{n-2}\tilde{q} > (\tilde{r}_i B + \tilde{r}_{i-1} - \tilde{q}\tilde{b}_{n-1})B + \tilde{r}_{i-2}$, полагать $\tilde{q} \leftarrow \tilde{q} - 1$.

3.3. При $(r_i, r_{i-1}, \ldots, r_{i-n})_B - b\tilde{q} < 0$ положить $\tilde{q} \leftarrow \tilde{q} - 1$.

3.4. Вычислить $(r_i, r_{i-1}, \ldots, r_{i-n})_B \leftarrow (r_i, r_{i-1}, \ldots, r_{i-n})_B - b\tilde{q}$ и $q_{i-n} \leftarrow \tilde{q}$.

4. Результат: $q = (q_m, q_{m-1}, \ldots, q_0)_B$, $r = (r_{n-1}, r_{n-2}, \ldots, r_0)_B$. □

Сложность алгоритма деления «в столбик» равна $O(mn)$.

Пример 4.19. Разделим с остатком $a = 212550433 = (\text{cab}4321)_{16}$ на $b = 1110 = (456)_{16}$. Здесь $n = 3$, $m = 4$, $B = 16$.

Выбираем $d = 2$, тогда $\tilde{b} = (\tilde{b}_2, \tilde{b}_1, \tilde{b}_0)_{16} = (8\text{ac})_{16}$. На шаге 2 полагаем $(r_7, r_6, \ldots, r_0)_{16} = (0\text{cab}4321)_{16}$.

Для $i = m + n = 7$ полагаем $(\tilde{r}_7, \tilde{r}_6, \tilde{r}_5, \tilde{r}_4)_{16} = (1956)_{16}$. Поскольку $\tilde{r}_7 = 1 \neq 8 = \tilde{b}_2$, полагаем $\tilde{q} = \left[\dfrac{\tilde{r}_7 \cdot 16 + \tilde{r}_6}{\tilde{b}_2}\right] = \left[\dfrac{1 \cdot 16 + 9}{8}\right] = \left[\dfrac{25}{8}\right] = 3$.

Вычисляем $\tilde{b}_{n-2}\tilde{q} = \tilde{b}_1\tilde{q} = 10 \cdot 3 = 30$, $(\tilde{r}_7 \cdot 16 + \tilde{r}_6 - \tilde{q}\tilde{b}_{n-1}) \cdot 16 + \tilde{r}_5 = (1 \cdot 16 + 9 - 3 \cdot 8) \cdot 16 + 5 = 21 < 30$, тогда уменьшаем $\tilde{q}$ на 1: $\tilde{q} = 2$. Повторная проверка дает $\tilde{b}_1\tilde{q} = 20 < (\tilde{r}_7 \cdot 16 + \tilde{r}_6 - \tilde{q}\tilde{b}_{n-1}) \cdot 16 + \tilde{r}_5 = 149$.

На шаге 3.4 полагаем $(r_7, r_6, r_5, r_4)_{16} = (r_7, r_6, r_5, r_4)_{16} - b\tilde{q} = (0\text{cad})_{16} - (8\text{ac})_{16} \cdot 3_{16} = (03\text{ff})_{16}$ и $q_{i-n} = q_m = q_4 = 2_{16}$.

Результаты дальнейших вычислений запишем в таблицу:

| $i$ | $(\tilde{r}_i, \tilde{r}_{i-1}, \ldots, \tilde{r}_{i-3})_{16}$ | $\tilde{q}$ | $\tilde{b}_1\tilde{q}$ | $(\tilde{r}_i \cdot 16 + \tilde{r}_{i-1} - \tilde{q}\tilde{b}_2) \cdot 16 + \tilde{r}_{i-2}$ | $(r_i, r_{i-1}, \ldots, r_{i-3})_{16} - b\tilde{q} < 0$ |
|---|---|---|---|---|---|
| 6 | $(7\text{fe}8)_{16}$ | $\text{f}_{16}$ | $(96)_{16}$ | $(7\text{e})_{16}$ | |
| | | $\text{e}_{16}$ | $(8\text{c})_{16}$ | $(\text{fe})_{16}$ | Нет |

| $i$ | $(\tilde{r}_i, \tilde{r}_{i-1}, \ldots, \tilde{r}_{i-3})_{16}$ | $\tilde{q}$ | $\tilde{b}_1\tilde{q}$ | $(\tilde{r}_i \cdot 16 + \tilde{r}_{i-1} - -\tilde{q}\tilde{b}_2) \cdot 16 + \tilde{r}_{i-2}$ | $(r_i, r_{i-1}, \ldots, r_{i-3})_{16} - b\tilde{q} < 0$ |
|---|---|---|---|---|---|
| | $(r_6, r_5, r_4, r_4)_{16} = (3\text{ff}4)_{16} - (8\text{ac})_{16} \cdot \text{e}_{16} = (0340)_{16}$, $q_3 = \text{e}_{16}$ | | | | |
| 5 | $(6806)_{16}$ | $\text{d}_{16}$ | $(82)_{16}$ | $0_{16}$ | |
| | | $\text{c}_{16}$ | $(78)_{16}$ | $(80)_{16}$ | Да |
| | | $\text{b}_{16}$ | | | |
| | $(r_5, r_4, r_3, r_2)_{16} = (3403)_{16} - (8\text{ac})_{16} \cdot \text{b}_{16} = (0451)_{16}$, $q_2 = \text{b}_{16}$ | | | | |
| 4 | $(8\text{a}24)_{16}$ | $\text{f}_{16}$ | $(78)_{16}$ | $(122)_{16}$ | Нет |
| | $(r_4, r_3, r_2, r_1)_{16} = (4512)_{16} - (8\text{ac})_{16} \cdot \text{f}_{16} = (0408)_{16}$, $q_1 = \text{f}_{16}$ | | | | |
| 3 | $(8102)_{16}$ | $\text{f}_{16}$ | $(78)_{16}$ | $(90)_{16}$ | Да |
| | | $\text{e}_{16}$ | | | |
| | $(r_3, r_2, r_1, r_0)_{16} = (4081)_{16} - (8\text{ac})_{16} \cdot \text{e}_{16} = (03\text{cd})_{16}$, $q_0 = \text{e}_{16}$ | | | | |

Получили $q = (q_4, q_3, q_2, q_1, q_0) = (2\text{ebfe})_{16} = 191486$, $r = (r_2, r_1, r_0) = (3\text{cd})_{16} = 973$ и $212550433 = 191486 \cdot 1110 + 973$. □

## Упражнения к главе 4

1. Предложить метод распараллеливания вычислений при умножении больших чисел в предположении, что умножение слов выполняется значительно медленнее сложения слов.

2. Что собой представляет матрица быстрого преобразования Фурье? Найти вторую и четвертую степени этой матрицы над кольцами $\mathbb{Z}/p\mathbb{Z}$, где $p$ — простое число, и $\mathbb{Z}/2^m\mathbb{Z}$.

3. Назовем циклической разностью $\Delta\mathbf{a}$ вектора $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})^{\mathrm{T}}$ вектор $(a_0 - a_{n-1}, a_1 - a_0, a_2 - a_1, \ldots, a_{n-1} - a_{n-2})^{\mathrm{T}}$. Пусть $F(\mathbf{a}) = (a'_0, a'_1, \ldots, a'_{n-1})^{\mathrm{T}}$. Найти $F(\Delta\mathbf{a})$.

4. Тройка целых чисел ($\omega$, $n$, $m$) называется *допустимой*, если числа $\omega$ и $n$ имеют обратные по модулю $m$ и $\omega$ — примитивный корень $n$-й степени из единицы по модулю $m$. Какие из следующих троек допустимы: (4, 6, 7); (3, 11, 23); (2, 10, 11)?

5. С помощью теоремы о свертке вычислить произведение по модулю 15 полиномов $6x^7 + 3x^5 + x^2 + 9x + 1$ и $5x^7 + 10x^6 + 11x^4 + 6x + 1$.

6. Алгоритмом Шенхаге–Штрассена найти произведение чисел $(1b936cd8d1effec9fe1bea54e1c19)_{16}$, $(1df9e4f2a5b4fccdb7a41a9a2f447)_{16}$.

7. Алгоритмом Монтгомери найти произведение чисел $a = 13234082374087103405$, $b = 17133492303093114193$ по модулю $N = 18340912473405432173$.

8. Используя схему Горнера, вычислить значение полинома $a(x) = x^{10} + 2x^9 + 3x^8 + 12x^7 + x^5 + x^3 + 1$ в точке $x = 3$; $x = 12$; $x = 20$.

9. Найти $a \pmod p$: а) $a = (81bfca06db34219a328afccdeab312ba)_{16}$, $p = 2^{32} - 107$; б) $a = (ac7edbf620946af48ebad93cc23943)_{16}$, $p = 2^{32} - 76583$; в) $a = (92abdec2964ab349e520ab49dceab37253ccdea1)_{16}$, $p = 2^{64} - 323$.

10. Разделить с остатком а) 212550433 на 2345; б) 90824757298347 на 2345234953459; в) 42945828529348140931 на 1740133342343.

## Литература к главе 4


1. *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов. — М.: Мир, 1979.
2. *Вельшенбах М.* Криптография на Си и С++ в действии. — М.: ТРИУМФ, 2004.
3. *Кнут Д.* Искусство программирования. Т. 2. Получисленные алгоритмы. — М.–СПб.–Киев: Вильямс, 2000.

4. *Ноден П.*, *Китте К.* Алгебраическая алгоритмика. — М.: Мир, 1999.

5. *Ростовцев А. Г.* Алгебраические основы криптографии. — СПб.: Мир и Семья, Интерлайн, 2000.

6. *Menezes A.*, *van Oorschot P.*, *Vanstone S.* Handbook of applied cryptography. CRC Press, 1997. Доступно с http://www.cacr.math.uwaterloo.ca/hac/.

7. *Montgomery P. L.* Modular multiplication without trial division // Mathematics of Computation. 1985. Vol. 44. No. 170. P. 519–521.

# Глава 5

# ПРОВЕРКА ЧИСЕЛ НА ПРОСТОТУ

Проверка чисел на простоту является составной частью алгоритмов генерации простых чисел, используемых в криптографии с открытым ключом. Алгоритмы проверки на простоту можно разделить на вероятностные и детерминированные.

*Детерминированный* алгоритм всегда действует по одной и той же схеме и гарантированно решает поставленную задачу (или не дает никакого ответа). *Вероятностный* алгоритм использует генератор случайных чисел и дает не гарантированно точный ответ. Вероятностные алгоритмы в общем случае не менее эффективны, чем детерминированные (если используемый генератор случайных чисел всегда дает набор одних и тех же чисел, возможно, зависящих от входных данных, то вероятностный алгоритм становится детерминированным).

## 5.1. Вероятностные алгоритмы проверки чисел на простоту

Для того чтобы проверить вероятностным алгоритмом, является ли целое число $n$ простым, выбирают случайное число $a$, $1 < a < n$, и проверяют условие алгоритма. Если число $n$ не проходит тест по основанию $a$, то алгоритм выдает результат «Число $n$ составное», и число $n$ действительно является составным (рис. 5.1 на стр. 170).

Если же $n$ проходит тест по основанию $a$, ничего нельзя сказать о том, действительно ли число $n$ является простым. Последовательно проведя ряд проверок таким тестом для разных $a$ и получив для каждого из них ответ «Число $n$, вероятно, простое», можно утверждать, что число $n$ является простым с вероятностью, близкой к 1. После $t$ независимых

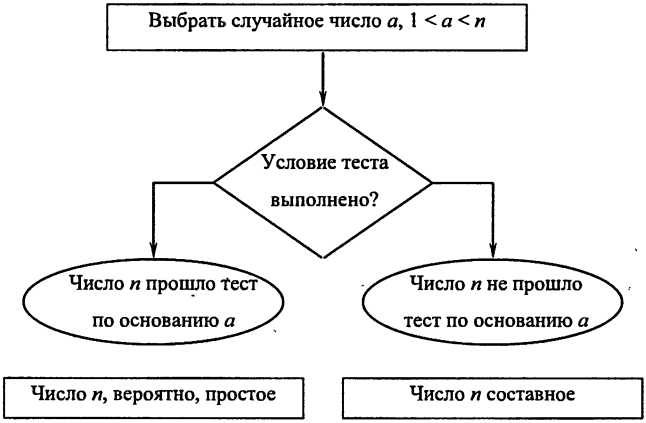



***Рис. 5.1.*** *Схема вероятностного алгоритма проверки числа на простоту*

выполнений теста вероятность того, что составное число $n$ будет $t$ раз объявлено простым (вероятность ошибки), не превосходит $\frac{1}{2^t}$.

### 5.1.1. Тест Ферма

Согласно малой теореме Ферма для простого числа $p$ и произвольного целого числа $a$, $1 \le a \le p-1$, выполняется сравнение

$$a^{p-1} \equiv 1 \pmod{p}. \tag{5.1}$$

Следовательно, если для нечетного $n$ существует такое целое $a$, что $1 \le a < n$, НОД$(a, n) = 1$ и $a^{n-1} \quad 1 \pmod{n}$, то число $n$ составное. Отсюда получаем следующий вероятностный алгоритм проверки числа на простоту.

Алгоритм 5.1. Тест Ферма.

*Вход*. Нечетное целое число $n \ge 5$.

*Выход*. «Число $n$, вероятно, простое» или «Число $n$ составное».

1. Выбрать случайное целое число $a$, $2 \le a \le n-2$.
2. Вычислить $r \leftarrow a^{n-1} \pmod{n}$.
3. При $r = 1$ результат: «Число $n$, вероятно, простое». В противном случае результат: «Число $n$ составное». □

На шаге 1 алгоритма мы не рассматриваем числа $a = 1$ и $a = n-1$, поскольку $1^{n-1} \equiv 1 \pmod{n}$ для любого целого $n$ и $(n-1)^{n-1} \equiv (-1)^{n-1} \equiv 1 \pmod{n}$ для любого нечетного $n$.

Сложность теста Ферма равна $O(\log^3 n)$ при умножении «в столбик» и $O(t \log^2 n \log\log n)$ при умножении алгоритмом Шенхаге–Штрассена.

Определение 5.1. Пусть число $n > 0$ нечетное составное и число $a$ произвольное целое, взаимно простое с $n$, $1 \le a \le n-1$. Число $n$

называется *псевдопростым по основанию a*, если выполняется сравнение (5.1), то есть если для числа $n$ алгоритм 5.1 выдает результат «Число $n$, вероятно, простое».

Пример 5.1. Число $n = 527 = 17 \cdot 31$ является псевдопростым по основаниям 1, 154, 373, 526, поскольку $1^{526} \equiv 154^{526} \equiv 373^{526} \equiv 526^{526} \equiv 1 \pmod{527}$. □

Пример 5.2. Число $n = 629 = 17 \cdot 37$ является псевдопростым по основаниям 1, 38, 149, 154, 186, 191, 290, 302, 327, 339, 438, 443, 475, 480, 591, 628. □

Пример 5.3. В интервале от 8 до 10000 псевдопростыми по основанию 7 являются числа

$$25 = 5^2,\quad 325 = 5^2 \cdot 13,\quad 561 = 3 \cdot 11 \cdot 17,\quad 703 = 19 \cdot 37,$$
$$817 = 19 \cdot 43,\quad 1105 = 5 \cdot 13 \cdot 17,\quad 1825 = 5^2 \cdot 73,\quad 2101 = 11 \cdot 191,$$
$$2353 = 13 \cdot 181,\quad 2465 = 5 \cdot 17 \cdot 29,\quad 3277 = 29 \cdot 113,\quad 4525 = 5^2 \cdot 181,$$
$$4825 = 5^2 \cdot 193,\quad 6697 = 37 \cdot 181,\quad 8321 = 53 \cdot 157.$$ □

Теорема 5.1. Для нечетного составного числа $n > 0$ справедливы следующие утверждения.

1. Число $n$ является псевдопростым по основанию $a$ тогда и только тогда, когда $n - 1$ делится на порядок числа $a$ по модулю $n$.

2. Если число $n$ псевдопростое по основаниям $a$ и $b$, то $n$ псевдопростое по основаниям $ab \pmod n$, $ab^{-1} \pmod n$ и $a^{-1}b \pmod n$.

3. Если число $n$ не является псевдопростым хотя бы по одному основанию $a$, то $n$ является псевдопростым не более чем по $\dfrac{\varphi(n)}{2}$ основаниям, где $\varphi$ — функция Эйлера.

*Доказательство.* Если $d$ — порядок числа $a$ по модулю $n$ и $n - 1 = kd$ для некоторого целого числа $k$, то, возводя обе части сравнения $a^d \equiv 1 \pmod n$ в степень $k$, получаем соотношение (5.1).

Обратно, пусть число $n$ псевдопростое по основанию $a$, то есть $a^{n-1} \equiv 1 \pmod{n}$, и $d$ — порядок числа $a$ по модулю $n$. Разделим $n-1$ с остатком на $d$: $n-1 = qd + r$ для некоторых целых неотрицательных чисел $q$ и $r$, тогда

$$1 \equiv a^{n-1} = a^{qd+r} = (a^d)^q \cdot a^r \equiv a^r \pmod{n}.$$

Но $d$ — наименьшая степень, в которой $a$ сравнимо с 1 по модулю $n$. Значит, $r = 0$ и $n-1$ делится на $d$. Первое утверждение доказано.

Если $a^{n-1} \equiv 1 \pmod{n}$ и $b^{n-1} \equiv 1 \pmod{n}$, то, перемножая почленно эти сравнения, получаем $(ab)^{n-1} \equiv 1 \pmod{n}$. А из сравнения $a^{n-1} \equiv b^{n-1} \pmod{n}$ получаем $(ab^{-1})^{n-1} \equiv (a^{-1}b)^{n-1} \equiv 1 \pmod{n}$. Второе утверждение доказано.

Докажем утверждение 3. Пусть $\{a_1, a_2, \ldots, a_k\}$ — множество всех тех оснований, по которым число $n$ является псевдопростым, то есть $1 \le a_i \le n-1$, НОД$(a_i, n) = 1$ и $a_i^{n-1} \equiv 1 \pmod{n}$ для $1 \le i \le k$ (это множество непусто, поскольку хотя бы числа 1 и $n-1$ ему принадлежат). Пусть $a$ — такое основание, по которому $n$ не является псевдопростым, то есть $1 \le a \le n-1$, НОД$(a, n) = 1$ и $a^{n-1} \not\equiv 1 \pmod{n}$. Рассмотрим числа $b_1 \equiv aa_1 \pmod{n}$, $b_2 \equiv aa_2 \pmod{n}$, $\ldots$, $b_k \equiv aa_k \pmod{n}$ и предположим, что число $n$ является псевдопростым по основанию $b_i$ хотя бы для одного $i$, $1 \le i \le k$. Тогда, согласно утверждению 2, число $n$ является псевдопростым и по основанию $ba_i^{-1} \equiv (aa_i)a_i^{-1} \equiv a \pmod{n}$, а это не так. Следовательно, число $n$ не является псевдопростым ни по одному из $k$ различных оснований $b_1$, $b_2$, $\ldots$, $b_k$. Таким образом, чисел, удовлетворяющих сравнению (5.1), по крайней мере не больше, чем чисел, которые этому сравнению не удовлетворяют, а из условия НОД$(a_i, n) = 1$ получаем, что их не больше, чем $\frac{\varphi(n)}{2}$. □

Из утверждения 3 следует, что если число $n$ не является псевдопростым хотя бы по одному основанию, то оно не является псевдопростым по крайней мере по $\frac{n-1}{2}$ основаниям.

Для любого числа $a > 1$ существует бесконечно много чисел, псевдопростых по основанию $a$.

Пример 5.4. Покажем, что если число $n$ псевдопростое по основанию 2, то число $2^n - 1$ тоже псевдопростое по основанию 2. Действительно, пусть $2^{n-1} \equiv 1 \pmod{n}$, то есть $2^{n-1} - 1 = kn$ для некоторого целого числа $k$. Тогда

$$2^{2^n-2} = 2^{2(2^{n-1}-1)} = 2^{2kn} = (2^n)^{2k} \equiv 1^{2k} = 1 \pmod{2^n - 1}.$$

Таким образом, существует бесконечно много чисел, псевдопростых по основанию 2. □

Определение 5.2. Нечетные составные числа $n$, для которых сравнение (5.1) выполняется при любом $a$, $1 \le a \le n-1$, взаимно простом с $n$, называются *числами Кармайкла* (R.D. Carmichael). Для этих чисел тест Ферма всегда выдает результат «Число $n$, вероятно, простое».

Пример 5.5. Самое маленькое число Кармайкла — $561 = 3 \cdot 11 \cdot 17$. Еще несколько чисел Кармайкла: $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, $6601 = 7 \cdot 23 \cdot 41$, $29341 = 13 \cdot 37 \cdot 61$, $41041 = 7 \cdot 11 \cdot 13 \cdot 41$, $278545 = 5 \cdot 17 \cdot 29 \cdot 113$, $949803513811921 = 17 \cdot 31 \cdot 191 \cdot 433 \cdot 21792241$, $651693055693681 = 72931 \cdot 87517 \cdot 102103$. □

Теорема 5.2 (критерий Корселта). Нечетное составное число $n$ является числом Кармайкла тогда и только тогда, когда:

1) $n$ свободно от квадратов;

2) для каждого простого делителя $p$ числа $n$ число $n-1$ делится на $p-1$.

*Доказательство.* Сначала докажем, что число, удовлетворяющее указанным свойствам, является числом Кармайкла. Пусть $n = p_1 p_2 \ldots p_k$ — каноническое разложение числа $n$ (все простые числа $p_i$ различны, так как выполняется свойство 1), и пусть $a$ — произвольное целое число, $1 \le a \le n-1$, взаимно простое с $n$. Согласно малой теореме Ферма, $a^{p_i - 1} \equiv 1 \pmod{p_i}$ для каждого $i$, $1 \le i \le k$. Из свойства 2 следует, что $n-1$ делится на $p_i - 1$, то есть $n - 1 = (p_i - 1)q_i$ для некоторого целого числа $q_i$. Тогда

$$a^{n-1} = a^{(p_i-1)q_i} \equiv 1 \pmod{p_i},$$

то есть разность $a^{n-1} - 1$ делится на $p_i$ для всех делителей $p_i$ числа $n$. А так как все числа $p_i$ различны, то по свойству 7 взаимно простых чисел $a^{n-1} - 1$ делится и на произведение $p_1 p_2 \ldots p_k = n$. Число $a$ мы выбирали произвольно, поэтому $a^{n-1} \equiv 1 \pmod{n}$ для любого $a$, $1 \le a \le n-1$, и, значит, $n$ является числом Кармайкла.

Теперь докажем, что всякое число Кармайкла $n$ удовлетворяет свойству 2. Пусть $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ — каноническое разложение числа $n$. Согласно теореме 2.15, для каждого $p_i$ найдется число $a_i$ порядка $p_i - 1$. Тогда из условия $a_i^{n-1} \equiv 1 \pmod{n}$ следует, что $n-1$ делится на $p_i - 1$.

Осталось доказать, что число Кармайкла $n$ свободно от квадратов. Пусть $n = p^t r$, где $t \ge 2$. Для любого $a$, взаимно простого с $n$, выполняется сравнение $a^{n-1} \equiv 1 \pmod{n}$, тогда $a^{n-1} \equiv 1 \pmod{p^2}$. Возьмем в качестве $a$ первообразный корень по модулю $p^2$ (см. теорему 2.5), то есть число порядка $p(p-1)$. Тогда $n-1$ должно делиться на $p(p-1)$, то есть $n-1$ должно делиться на $p$. А это противоречит тому, что $n$ делится на $p$. □

Следствие. Любое число Кармайкла является произведением не менее трех различных простых чисел.

*Доказательство.* Из теоремы 5.2 мы знаем, что простые делители числа Кармайкла должны быть различны. Посмотрим, может ли число Кармайкла $n$ иметь ровно два простых делителя. Итак, пусть $n = pq$, где числа $p$ и $q$ простые, $p < q$. Тогда $n - 1$ делится на $q - 1$, то есть $n - 1 \equiv 0 \pmod{q - 1}$. В то же время

$$n - 1 = pq - 1 = p(q - 1 + 1) - 1 = p(q - 1) + p - 1 \equiv p - 1 \pmod{q - 1}.$$

Но $p - 1 \quad 0 \pmod{q - 1}$, поскольку $0 < p - 1 < q - 1$. Получили противоречие. □

Замечание. Условие 2 в теореме 5.2 можно переписать так: число $n - 1$ должно делиться на НОК$(p_1 - 1, p_2 - 1, \ldots, p_s - 1)$. Отсюда получаем следующий способ генерации чисел Кармайкла.

Пример 5.6. Рассмотрим простые числа вида $p_1 = 6k + 1$, $p_2 = 12k + 1$, $p_3 = 18k + 1$ (например, при $k = 1$ получаем $p_1 = 7$, $p_2 = 13$, $p_3 = 19$). Докажем, что число $n = p_1p_2p_3$ является числом Кармайкла.

Согласно малой теореме Ферма, для любого числа $a$, взаимно простого с $p_1$, выполняется сравнение $a^{6k} \equiv 1 \pmod{p_1}$. Аналогично, $a^{12k} \equiv 1 \pmod{p_2}$, $a^{18k} \equiv 1 \pmod{p_3}$. Число $36k$ является наименьшим общим кратным чисел $6k$, $12k$ и $18k$, тогда по китайской теореме об остатках $a^{36k} \equiv 1 \pmod{n}$ для всех чисел $a$, взаимно простых с $n$. Но $n - 1 = 1296k^2 + 396k + 36k = 36k(36k^2 + 11k + 1)$, значит, $a^{n-1} \equiv 1 \pmod{n}$ для всех чисел $a$, взаимно простых с $n$. □

Для генерации чисел Кармайкла общего вида можно воспользоваться следующим алгоритмом [7].

Алгоритм 5.2. Алгоритм Эрдеша (1956).

*Вход.* Сильно составное число $m > 0$.

*Выход*. Число Кармайкла.

1. Составить множество $S$ простых чисел $p$, для которых $m$ делится на $p-1$ и НОД$(m, p) = 1$.
2. Из множества $S$ выбрать такие числа $p_1, p_2, \ldots, p_r$, $r \geq 3$, для которых $p_1p_2\ldots p_r \equiv 1 \pmod{m}$.
3. Положить $n \leftarrow p_1p_2\ldots p_r$.
4. Результат: $n$. □

Пример 5.7. Пусть $m = 120 = 2^3 \cdot 3 \cdot 5$. Составляем множество $S = \{7, 11, 13, 31, 41, 61\}$. Чем больше множество $S$, тем больше чисел Кармайкла, возможно, нам удастся построить. Перебирая всевозможные произведения элементов множества $S$, получаем:

$$41041 = 7 \cdot 11 \cdot 13 \cdot 41 \equiv 1 \pmod{120},$$

$$172081 = 7 \cdot 13 \cdot 31 \cdot 61 \equiv 1 \pmod{120},$$

$$852841 = 11 \cdot 31 \cdot 41 \cdot 61 \equiv 1 \pmod{120},$$

— числа Кармайкла. □

Наиболее трудоемким в алгоритме Эрдеша является шаг 2. Следующая модификация этого шага, предложенная в 1994 году У. Альфордом (W. Alford), делает этот алгоритм пригодным для практического использования.

3.1. Найти такое подмножество $P \subseteq S$, что для любого числа $a$, $1 \leq a \leq m$, взаимно простого с $m$, найдутся числа $p_1, p_2, \ldots, p_r \in P$, для которых $p_1p_2\ldots p_r \equiv a \pmod{m}$.

3.2. Для любых чисел $q_1, q_2, \ldots, q_t \in S \setminus P$ вычислить $a \equiv (q_1q_2\ldots q_t)^{-1} \pmod{m}$. Тогда $p_1p_2\ldots p_rq_1q_2\ldots q_t$ — число Кармайкла.

Выбор множества $P$ на шаге 3.1 можно выполнить так. Пусть элементы множества $S$ упорядочены по возрастанию: $p_1 < p_2 < \ldots$ . Обозначим $R_j$ множество всевозможных произведений чисел $p_1, p_2, \ldots, p_j$ по мо-

дулю $m$. Множества $R_j$ задаются рекуррентным соотношением $R_{j+1} = R_j \cup \{sp_{j+1} \pmod m \mid s \in R_j\}$. Тогда в качестве $P$ нужно взять то множество $R_j$, которое представляет собой приведенную систему вычетов по модулю $m$: $R_j = \{a \mid 1 \le a \le m, \text{НОД}(a, m) = 1\}$.

На шаге 3.2 получаем $p_1p_2\ldots p_r \equiv a \equiv (q_1q_2\ldots q_t)^{-1} \pmod m$, откуда $p_1p_2\ldots p_rq_1q_2\ldots q_t \equiv 1 \pmod m$ — число Кармайкла, согласно шагу 2 алгоритма Эрдеша. Рассмотренный алгоритм позволяет найти $2^{\#(S\setminus P)} - 1$ чисел Кармайкла.

Приведем без доказательства еще один интересный критерий распознавания чисел Кармайкла. Нечетное составное число $n$, свободное от квадратов, является числом Кармайкла тогда и только тогда, когда оно делит знаменатель числа Бернулли $B_{n-1}$ (числа Бернулли определяются из рекуррентного соотношения: $B_0 = 1$, $\sum_{k=0}^{n-1} \frac{n!}{k!(n-k)!} B_k = 0$ при $n \ge 1$). Например, для числа Кармайкла $n = 1105$ число Бернулли $B_{1104}$ отрицательно, числитель имеет длину 2012 десятичных знаков, знаменатель равен

$$83985438810 = 1105 \cdot 76004922.$$

Числа Кармайкла встречаются довольно редко. От 1 до $10^5$ всего 16 чисел Кармайкла: 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361. От 1 до $2{,}5 \cdot 10^{10}$ всего 2163 чисел Кармайкла; от 1 до $10^{15}$ всего 105212 чисел Кармайкла.

В то же время чисел Кармайкла бесконечно много: для любого достаточно большого $n$ справедливо неравенство

$$n^{\frac{2}{7}} < C(n) < n\exp\left(-\frac{\ln n \ln\ln\ln n}{\ln\ln n}\right),$$

где $C(n)$ — количество чисел Кармайкла, меньших $n$ [6].

Если $n$ является числом Кармайкла и все его простые делители достаточно велики, то с большой вероятностью тест Ферма объявит $n$ простым даже при большом числе итераций. Если в тесте Ферма использовать не случайные, а заранее определенные основания $a$, то его можно «обмануть» выбором соответствующего числа Кармайкла. Этот недостаток теста Ферма устраняется следующими тестами с более жесткими критериями.

### 5.1.2. Тест Соловэя–Штрассена

В основе этого теста лежит следующая теорема.

Теорема 5.3 (критерий Эйлера). Нечетное число $n$ является простым тогда и только тогда, когда для любого целого числа $a$, $1 \le a \le n-1$, взаимно простого с $n$, выполняется сравнение

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) (\mathrm{mod}\, n). \qquad (5.2)$$

*Доказательство.* Если число $n$ простое, то сравнение (5.2) — это свойство 3 символа Лежандра. Пусть теперь сравнение выполнено, и число $n$ составное. Тогда

$$a^{n-1} = \left(a^{\frac{n-1}{2}}\right)^2 \equiv \left(\frac{a}{n}\right)^2 = 1\,(\mathrm{mod}\, n).$$

Таким образом, для любого числа $a$, удовлетворяющего условиям теоремы, выполняется сравнение (5.1), и $n$ является числом Кармайкла. Согласно свойству 2 из теоремы 5.2, каноническое разложение числа $n$ имеет вид $n = p_1 p_2 \ldots p_s$ (все числа $p_i$ различны). Пусть $b$ — квадратичный невычет по модулю $p_1$, то есть $\left(\frac{b}{p_1}\right) = -1$. По китайской теореме об остатках найдем такое число $a$, что

$$a \equiv b\ (\mathrm{mod}\, p_1),\ a \equiv 1\ (\mathrm{mod}\, p_2),\ \ldots,\ a \equiv 1\ (\mathrm{mod}\, p_s). \qquad (5.3)$$

Вычислим символ Якоби:

$$\left(\frac{a}{n}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\ldots\left(\frac{a}{p_s}\right)=\left(\frac{b}{p_1}\right)\left(\frac{1}{p_2}\right)\ldots\left(\frac{1}{p_s}\right)=\left(\frac{b}{p_1}\right)=-1.$$

Подставляя это значение в сравнение (5.2), получаем, что $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$, а значит, $a^{\frac{n-1}{2}} \equiv -1 \pmod{p_i}$ для всех $i$, $1 \le i \le s$, что противоречит условию (5.3). □

Критерий Эйлера лежит в основе следующего вероятностного теста простоты [10].

Алгоритм 5.3. Тест Соловэя–Штрассена.

*Вход*. Нечетное целое число $n \ge 5$.

*Выход*. «Число $n$, вероятно, простое» или «Число $n$ составное».

1. Выбрать случайное целое число $a$, $2 \le a \le n-2$.
2. Вычислить $r \leftarrow a^{\frac{n-1}{2}} \pmod{n}$.
3. При $r \ne 1$ и $r \ne n-1$ результат: «Число $n$ составное».
4. Вычислить символ Якоби $s \leftarrow \left(\frac{a}{n}\right)$.
5. При $r \quad s \pmod{n}$ результат: «Число $n$ составное». В противном случае результат: «Число $n$, вероятно, простое». □

На шаге 1 мы снова не рассматриваем числа 1 и $n-1$, поскольку в силу свойства 3 символа Лежандра сравнение (5.2) для этих чисел выполняется при любом нечетном $n$. Если $d = \text{НОД}(a, n) > 1$, то $d$ делит и число $r$, вычисляемое на шаге 2. Таким образом, при проверке неравенства $r \ne 1$ на шаге 3 автоматически проверяется условие $\text{НОД}(a, n) \ne 1$.

Сложность теста Соловэя–Штрассена определяется сложностью вычисления символа Якоби и равна $O(\log^3 n)$.

Определение 5.3. Пусть число $n$ нечетное составное и число $a$ произвольное целое, взаимно простое с $n$, $2 \le a \le n-1$. Число $n$ называется *эйлеровым псевдопростым по основанию* $a$, если выполняется сравнение (5.2), то есть если для числа $n$ алгоритм 5.3 выдает результат «Число $n$, вероятно, простое».

Теорема 5.3 показывает, что для теста Соловэя–Штрассена не существует чисел, подобных числам Кармайкла, то есть составных чисел, которые были бы эйлеровыми псевдопростыми по всем основаниям $a$. Этот результат был независимо получен Д. Лемером (D. Lehmer) в 1976 году и Р. Соловэем (R. Solovay), Ф. Штрассеном в 1977 году.

Пример 5.8. Число $n = 527 = 17 \cdot 31$ является эйлеровым псевдопростым по основаниям 1 и 526, поскольку $1^{263} \equiv 526^{263} \equiv 1 \pmod{527}$ и $\left(\frac{1}{527}\right) = \left(\frac{526}{527}\right) = 1$. □

Пример 5.9. Число $n = 629 = 17 \cdot 37$ является эйлеровым псевдопростым по основаниям 1, 186, 191, 302, 327, 438, 443, 628, поскольку

$$1^{314} \equiv 186^{314} \equiv 443^{314} \equiv 628^{314} \equiv 1 \pmod{629},$$

$$\left(\frac{1}{629}\right) = \left(\frac{186}{629}\right) = \left(\frac{443}{629}\right) = \left(\frac{628}{629}\right) = 1$$

и

$$191^{314} \equiv 302^{314} \equiv 327^{314} \equiv 438^{314} \equiv 628 \pmod{629},$$

$$\left(\frac{191}{629}\right) = \left(\frac{302}{629}\right) = \left(\frac{327}{629}\right) = \left(\frac{438}{629}\right) = -1.$$ □

Пример 5.10. В интервале от 8 до 10000 эйлеровыми псевдопростыми по основанию 7 являются числа 25, 325, 703, 2101, 2353, 2465, 3277, 4525. □

Пример 5.11. Для числа $n = 561$ тест Ферма выдает результат «Число $n$, вероятно, простое» для всех $320 = \varphi(561)$ оснований $a$. Тест

Соловэя–Штрассена для этого числа выдает такой же результат лишь для $80 = \frac{\varphi(561)}{4}$ оснований $a$. Например, при $a = 5$ получаем $a^{\frac{n-1}{2}} = 5^{280} \equiv 67 \pmod{n}$ и результат «Число $n$ составное» на шаге 3; при $a = 13$ получаем $a^{\frac{n-1}{2}} = 13^{280} \equiv 1 \pmod{n}$, но $\left(\frac{13}{561}\right) = -1$ и результат «Число $n$ составное» на шаге 5. □

Теорема 5.4. Для нечетного составного числа $n$ справедливы следующие утверждения.

1. Если число $n$ эйлерово псевдопростое по основанию $a$ и не является таковым по основанию $b$, то оно не эйлерово псевдопростое по основанию $ab \pmod{n}$.

2. Если число $n$ эйлерово псевдопростое по основаниям $a$ и $b$, то $n$ псевдопростое по основаниям $ab \pmod{n}$, $ab^{-1} \pmod{n}$ и $a^{-1}b \pmod{n}$.

3. Если число $n$ не является эйлеровым псевдопростым хотя бы по одному основанию $a$, то $n$ является эйлеровым псевдопростым не более чем по $\frac{\varphi(n)}{2}$ основаниям, где $\varphi$ — функция Эйлера.

4. Если число $n$ является эйлеровым псевдопростым по основанию $a$, то оно является и псевдопростым по основанию $a$.

*Доказательство.* Первое утверждение докажем от противного. Пусть сравнение (5.2) выполнено для $a$ и для $ab$ и не выполнено для $b$. Обозначим $l_a = \left(\frac{a}{n}\right)$. Тогда

$$(ab)^{\frac{n-1}{2}} - l_{ab} = a^{\frac{n-1}{2}} b^{\frac{n-1}{2}} - l_a l_b = a^{\frac{n-1}{2}} b^{\frac{n-1}{2}} - a^{\frac{n-1}{2}} l_b + a^{\frac{n-1}{2}} l_b - l_a l_b =$$
$$= a^{\frac{n-1}{2}} (b^{\frac{n-1}{2}} - l_b) + (a^{\frac{n-1}{2}} - l_a) l_b.$$

Разность $(ab)^{\frac{n-1}{2}} - l_{ab}$ делится на $n$ по предположению, разность $a^{\frac{n-1}{2}} - l_a$ делится на $n$ по условию теоремы, тогда и число $a^{\frac{n-1}{2}}(b^{\frac{n-1}{2}} - l_b)$ должно делиться на $n$. Но $a$ взаимно просто с $n$, и разность в скобках не делится на $n$. Противоречие.

Утверждения 2 и 3 доказываются аналогично утверждениям 2 и 3 теоремы 5.1.

Для доказательства четвертого утверждения возводим в квадрат обе части сравнения (5.2) и получаем сравнение (5.1). □

Вероятность того, что тест Соловэя–Штрассена объявит нечетное составное число $n$ простым, меньше, чем $\frac{1}{2^t}$.

### 5.1.3. Тест Миллера–Рабина

На сегодняшний день для проверки чисел на простоту чаще всего используется тест Миллера–Рабина, основанный на следующем наблюдении. Пусть число $n$ нечетное и $n - 1 = 2^s r$, где $r$ — нечетное. Если $n$ простое, то для любого $a \geq 2$, взаимно простого с $n$, выполняется условие (5.1). Разложим число $a^{n-1}$ на множители:

$$a^{n-1} - 1 = a^{2^s r} - 1 = (a^{2^{s-1}r} - 1)(a^{2^{s-1}r} + 1) =$$

$$= (a^{2^{s-2}r} - 1)(a^{2^{s-2}r} + 1)(a^{2^{s-1}r} + 1) = \ldots =$$

$$= (a^{2r} - 1)(a^{2r} + 1)\ldots(a^{2^{s-2}r} + 1)(a^{2^{s-1}r} + 1) =$$

$$= (a^r - 1)(a^r + 1)(a^{2r} + 1)\ldots(a^{2^{s-2}r} + 1)(a^{2^{s-1}r} + 1).$$

Тогда в последнем произведении хотя бы одна из скобок делится на $n$, то есть либо $a^r \equiv 1 \pmod{n}$, либо среди чисел $a^r$, $a^{2r}$, …, $a^{2^{s-1}r}$ найдется сравнимое с $-1$ по модулю $n$.

Обращение этого свойства и лежит в основе теста Миллера–Рабина.

Алгоритм 5.4. Тест Миллера–Рабина.

*Вход*. Нечетное целое число $n \geq 5$.

*Выход*. «Число $n$, вероятно, простое» или «Число $n$ составное».

1. Представить $n - 1$ в виде $n - 1 = 2^s r$, где число $r$ нечетное.
2. Выбрать случайное целое число $a$, $2 \leq a \leq n - 2$.
3. Вычислить $y \leftarrow a^r \pmod n$.
4. При $y \neq 1$ и $y \neq n - 1$ выполнить следующие действия.
   - 4.1. Положить $j \leftarrow 1$.
   - 4.2. Если $j \leq s - 1$ и $y \neq n - 1$, то
     - 4.2.1. Положить $y \leftarrow y^2 \pmod n$.
     - 4.2.2. При $y = 1$ результат: «Число $n$ составное».
     - 4.2.3. Положить $j \leftarrow j + 1$.
   - 4.3. При $y \neq n - 1$ результат: «Число $n$ составное».
5. Результат: «Число $n$, вероятно, простое». □

В результате выполнения теста для простого числа $n$ в последовательности $a^r \pmod n$, $a^{2r} \pmod n$, ..., $a^{2^{s-1}r} \pmod n$ обязательно перед 1 должна появиться $-1$ (или, что то же самое, $n - 1 \pmod n$). Это означает, что для простого числа $n$ единственными решениями сравнения $y^2 \equiv 1 \pmod n$ являются $y \equiv \pm 1 \pmod n$. Если число $n$ составное и имеет $k > 1$ различных простых делителей (то есть не является степенью простого числа), то по китайской теореме об остатках существует $2^k$ решений сравнения $y^2 \equiv 1 \pmod n$. Действительно, для любого простого делителя $p_i$ числа $n$ существует два решения указанного сравнения: $y \equiv \pm 1 \pmod{p_i}$. Поэтому $k$ таких сравнений дают $2^k$ наборов решений по модулям $p_i$, содержащих элементы $\pm 1$.

Сложность алгоритма 5.4 равна $O((\log n)^3)$.

Определение 5.4. Пусть число $n$ нечетное простое, $n-1=2^s r$, где $r$ — нечетное, и $a$ — произвольное целое число, $1 \le a \le n-1$, взаимно простое с $n$. Число $n$ называется *сильно псевдопростым по основанию* $a$, если $a^r \equiv 1 \pmod n$ или если существует такое целое $j$, $0 \le j \le s-1$, что $a^{2^j r} \equiv -1 \pmod n$.

Пример 5.12. Для числа $n = 105 = 3 \cdot 5 \cdot 7$ имеем: $n-1 = 2^3 \cdot 13$, то есть $s=3$, $r=13$. Число 105 является сильно псевдопростым только по основаниям 1 и 104.

Более того, любое целое число $n$, являющееся произведением первых $k \ge 2$ нечетных чисел, является сильно псевдопростым только по двум основаниям, а именно, 1 и $n-1$. □

Пример 5.13. Для числа $n = 629 = 17 \cdot 37$ имеем: $n-1 = 2^2 \cdot 157$, то есть $s=2$, $r=157$, $2r=314$. Число 629 является сильно псевдопростым по основаниям 1, 191, 302, 327, 438, 628 поскольку

$$1^{157} \equiv 1 \pmod{629}, \quad 628^{157} \equiv -1 \pmod{629},$$

$$191^{314} \equiv 302^{314} \equiv 327^{314} \equiv 438^{314} \equiv -1 \pmod{629}.$$ □

Пример 5.14. В интервале от 8 до 10000 сильно псевдопростыми по основанию 7 являются числа 25, 325, 703, 2101, 2353, 4525:

| $n$ | $s$ | $r$ | $7^r \pmod n$ | $7^{2r} \pmod n$ |
|---|---|---|---|---|
| 25 | 3 | 3 | 18 | −1 |
| 325 | 2 | 81 | 307 | −1 |
| 703 | 1 | 351 | 1 | |
| 2101 | 2 | 525 | −1 | |
| 2353 | 4 | 147 | 343 | −1 |
| 4525 | 2 | 1131 | 343 | −1 |

□

Пример 5.15. Покажем, что число Кармайкла $2465 = 5 \cdot 17 \cdot 29$ не является сильно псевдопростым по основанию 3. Находим представление $2465 - 1 = 2^5 \cdot 77$, то есть $s = 5$, $r = 77$. Рассмотрим значения $2^{2^j r}$ для $j = 0, 1, \ldots, 5$ по модулю каждого из делителей числа 2465:

| | mod 5 | mod 17 | mod 29 | mod 2465 |
|---|---|---|---|---|
| $3^{77}$ | 3 | 12 | 17 | 2018 |
| $(3^{77})^2$ | $-1$ | 8 | $-1$ | 144 |
| $(3^{77})^{2^2}$ | 1 | 13 | 1 | 1016 |
| $(3^{77})^{2^3}$ | 1 | $-1$ | 1 | 1886 |
| $(3^{77})^{2^4}$ | 1 | 1 | 1 | 1 |
| $(3^{77})^{2^5}$ | 1 | 1 | 1 | 1 |

В последнем столбце значение $-1$ можем получить только в том случае, если все вычеты в соответствующей строке равны $-1$. Поскольку значения вычетов по разным модулям не зависят друг от друга, вероятность получить $-1$ по всем модулям достаточно мала. □

Вероятность того, что тест Миллера–Рабина объявит нечетное составное число $n$, не являющееся степенью простого числа, простым, меньше, чем $\frac{1}{4}$. Для большинства нечетных составных чисел $n$ оснований, по которым $n$ является сильно псевдопростым, на самом деле гораздо меньше, чем $\frac{\varphi(n)}{4}$.

Пример 5.16. Для составных чисел $n$ вида $(2p + 1)(4p + 1)$, где $2p + 1$, $4p + 1$ — простые числа, $p$ — положительное нечетное, и чисел Кармайкла, состоящих из трех сомножителей, оснований, по которым $n$ является сильно псевдопростым, ровно $\frac{\varphi(n)}{4}$ [8, 11].

Например, для $n = 88831 = 211 \cdot 421$ существует 22050 чисел $a$, $1 \le a < n$, взаимно простых с $n$, для которых выполняется сравнение $a^r \equiv \pm 1 \pmod n$, где $r = 44415 = \frac{n-1}{2}$, при этом $\varphi(n) = 210 \cdot 420 = 88200 = 4 \cdot 22050$. □

Замечание. Если число $n$ является сильно псевдопростым по основаниям $a$ и $b$, то, как правило, $n$ будет сильно псевдопростым и по основанию $ab \pmod n$. Поэтому на шаге 2 теста Миллера–Рабина можно выбирать не случайные числа $a$, а первые несколько простых чисел.

Пусть $p_1, p_2, \ldots, p_t$ — первые $t$ простых чисел. Обозначим $\psi_t$ наименьшее положительное составное число, которое является псевдопростым по каждому из оснований $p_1, p_2, \ldots, p_t$. Тогда для проверки на простоту произвольного целого числа $n < \psi_t$ тестом Миллера–Рабина достаточно взять в качестве $a$ первые $t$ простых чисел $p_1, p_2, \ldots, p_t$. В этом случае тест всегда дает верный результат. Например, при $n < 2\,047$ достаточно выполнить тест для числа $a = 2$; при $n < 1\,373\,653$ — для чисел 2 и 3; при $n < 25\,326\,001$ — для чисел 2, 3, 5 и т. д.

Лемма 5.5. Пусть для некоторого целого $a$ выполняется сравнение $a^{2^{s-1}r} \equiv -1 \pmod n$, где $n - 1 = 2^s r$, $p$ — произвольный простой делитель числа $n$, $p - 1 = 2^{s'} r'$, число $r'$ нечетное. Тогда

$$\left(\frac{a}{p}\right) = \begin{cases} -1 & \text{при } s' = s, \\ 1 & \text{при } s' > s. \end{cases}$$

*Доказательство* [2]. Возведем обе части сравнения $a^{2^{s-1}r} \equiv -1 \pmod n$ в нечетную степень $r'$: $(a^{2^{s-1}r})^{r'} \equiv -1 \pmod n$. Это же сравнение справедливо и по модулю любого простого делителя числа $n$, в том числе и по модулю $p$. Если предположить, что $s' < s$, то $a^{2^{s'}r'}$ не

может быть сравнимо с 1 по модулю $p$, а это противоречит малой теореме Ферма. Таким образом, возможен лишь случай $s' \geq s$.

При $s' = s$ получаем

$$\left(\frac{a}{p}\right)=\left(\frac{a}{p}\right)^r \equiv \left(a^{\frac{p-1}{2}}\right)^r = (a^{2^{s'-1}r'})^r = (a^{2^{s-1}r'})^r \equiv -1 \pmod p.$$

При $s' > s$, возводя обе части сравнения $(a^{2^{s-1}r})^{r'} \equiv -1 \pmod p$ в степень $2^{s'-s}$, получаем

$$1 \equiv ((a^{2^{s-1}r})^{r'})^{2^{s'-s}} = (a^{2^{s'-1}r'})^r = \left(\frac{a}{p}\right)^r = \left(\frac{a}{p}\right) \pmod p. \qquad \square$$

Лемма 5.6. Пусть для некоторого целого $a$ и некоторого целого $j$ выполняется сравнение $a^{2^{j-1}r} \equiv -1 \pmod n$, где $n-1=2^s r$, $1 \leq j \leq s-1$, $p$ — произвольный простой делитель числа $n$, $p-1=2^{s'}r'$, число $r'$ нечетное. Тогда

$$\left(\frac{a}{p}\right)=\begin{cases} -1 & \text{при } s'=j, \\ 1 & \text{при } s'>j. \end{cases}$$

*Доказательство* проводится аналогично предыдущей лемме [2].

Теорема 5.7. Если число $n$ является сильно псевдопростым по основанию $a$, то оно является эйлеровым псевдопростым по основанию $a$.

*Доказательство* [2]. Запишем $n-1$ в виде $n-1=2^s r$, где число $r$ нечетное. Рассмотрим три случая.

Случай 1. Пусть $a^r \equiv 1 \pmod n$. Тогда $a^{\frac{n-1}{2}} = a^{2^{s-1}r} = (a^r)^{2^{s-1}} \equiv 1 \pmod n$. Чтобы выполнялось сравнение (5.2), число $a$ должно быть квадратичным вычетом по модулю $n$. По свойствам символа Якоби получаем последовательность равенств

$$1=\left(\frac{1}{n}\right)=\left(\frac{a^r}{n}\right)=\left(\frac{a}{n}\right)^r=\left(\frac{a}{n}\right),$$

поскольку число $r$ нечетное.

Случай 2. Пусть $a^{\frac{n-1}{2}}=a^{2^{s-1}r}\equiv -1 \pmod n$. Теперь число $a$ должно быть квадратичным невычетом по модулю $n$. Разложим число $n$ на простые множители: $n=p_1p_2\ldots p_m$, где числа $p_i$ не обязательно различны, и представим $p_i-1=2^{s_i}r_i$, где числа $r_i$ нечетные. Пусть $k$ — количество тех чисел $p_i$, для которых $s_i=s$ (сомножители $p_i$ считаются с учетом кратности). Согласно лемме 5.5, для всех $i$ выполняется неравенство $s_i\geq s$, откуда $\left(\frac{a}{n}\right)=\prod_i\left(\frac{a}{p_i}\right)=(-1)^k$.

Кроме того, $p_i=2^{s_i}r_i+1=2^sr_i+1\equiv 2^s+1 \pmod{2^{s+1}}$ при $s_i=s$, $p_i=2^{s_i}r_i+1\equiv 1 \pmod{2^{s+1}}$ при $s_i>s$ и $n=2^sr+1\equiv 2^s+1 \pmod{2^{s+1}}$. Тогда

$$2^s+1\equiv n=p_1p_2\ldots p_m\equiv(2^s+1)^k\equiv k2^s+1 \pmod{2^{s+1}},$$

откуда $k\equiv 1 \pmod 2$, то есть число $k$ нечетное и $\left(\frac{a}{n}\right)=(-1)^k=-1$.

Осталось рассмотреть случай, когда $a^{2^{j-1}r}\equiv -1 \pmod n$ для некоторого $j$, $1\leq j\leq s-1$. Возводя обе части сравнения в нужную степень двойки, получаем $a^{\frac{n-1}{2}}\equiv 1 \pmod n$. Таким образом, для того чтобы число $n$ было эйлеровым псевдопростым, число $a$ должно быть квадратичным вычетом по модулю $n$. Так же, как в случае 2, получаем, что $\left(\frac{a}{n}\right)=(-1)^k$. Воспользовавшись теперь леммой 5.6 и проводя рассуждения, аналогичные предыдущему случаю, получаем $n=2^sr+1\equiv 1 \pmod{2^{j+1}}$ и

$$1\equiv n=p_1p_2\ldots p_m\equiv(2^j+1)^k\equiv k2^j+1 \pmod{2^{j+1}},$$

откуда $k \equiv 0 \pmod 2$, то есть число $k$ четное и $\left(\frac{a}{n}\right) = (-1)^k = 1$. □

Таким образом, если число $n$ сильно псевдопростое по основанию $a$, то $n$ — эйлерово псевдопростое по основанию $a$. Если число $n$ эйлерово псевдопростое по основанию $a$, то $n$ — псевдопростое по основанию $a$ (рис. 5.2).

Посмотрим, когда условия эйлеровой и сильной псевдопростоты эквивалентны.

Теорема 5.8. Число $n \equiv 3 \pmod 4$ является сильно псевдопростым по основанию $a$ тогда и только тогда, когда $n$ является эйлеровым псевдопростым по основанию $a$.

*Доказательство.* Пусть число $n = 3 + 4k$, где $k \in \mathbb{Z}$, сильно псевдопростое по основанию $a$. Запишем $n - 1 = 2 + 4k = 2 \cdot (2k + 1)$, то есть, по определению сильно псевдопростого числа, $s = 1$, $r = 2k + 1$ и $a^{\frac{n-1}{2}} = a^r \equiv \pm 1 \pmod n$. Докажем, что число $\pm 1$ в правой части сравнения совпадает с символом Якоби $\left(\frac{a}{n}\right)$. Вычисляем:

$$\left(\frac{1}{n}\right) = 1, \quad \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = (-1)^{2k+1} = -1,$$

то есть $\left(\frac{\pm 1}{n}\right) = \pm 1$. Тогда

$$\left(\frac{a}{n}\right) = \left(\frac{a \cdot (a^{(n-3)/4})^2}{n}\right) = \left(\frac{a^{(n-1)/2}}{n}\right) = \left(\frac{\pm 1}{n}\right) = \pm 1 \equiv a^{\frac{n-1}{2}} \pmod n,$$

и число $n$ эйлерово псевдопростое по основанию $a$.

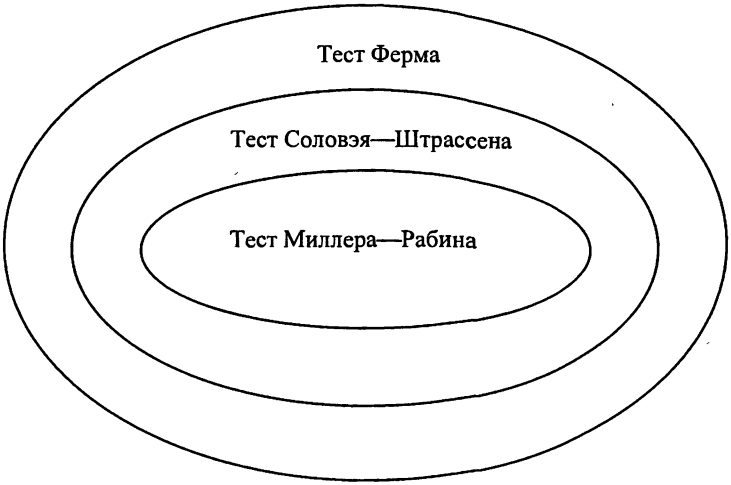



***Рис. 5.2.*** *Соотношение между основаниями, по которым данное число n проходит вероятностные тесты проверки на простоту*

Обратно, пусть число $n = 3 + 4k$, где $k \in \mathbb{Z}$, эйлерово псевдопростое по основанию $a$. Для того чтобы $n$ было сильно псевдопростым, должно выполняться либо сравнение $a^r = a^{\frac{n-1}{2}} \equiv 1 \pmod{n}$, либо при $j = 0$ сравнение $a^{2^j r} = a^{2^0 r} = a^r = a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$, то есть должно быть $a^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}$. А для эйлеровых псевдопростых чисел это имеет место по определению. □

### 5.1.4. Генерация простого числа

Существуют различные алгоритмы генерации простых чисел (см., например, работы [1, 5]). Многие из них вырабатывают числа, обладающие специальными свойствами. Рассмотрим способ генерации, использующий вероятностные алгоритмы проверки чисел на простоту.

Алгоритм 5.5. Генерация простого числа.

*Вход*. Разрядность $k$ искомого числа $p$; параметр $t \geq 1$.

*Выход*. Число $p$, простое с вероятностью не менее $1 - \frac{1}{4^t}$.

1. Сгенерировать случайное $k$-битное число $p = (b_{k-1}b_{k-2}\ldots b_0)_2$.
2. Положить $b_{k-1} = 1$, $b_0 = 1$.
3. Проверить, что $p$ не делится на простые числа 3, 5, 7, … .
4. Для $i = 1, 2, \ldots, t$ выполнить следующие действия.
   4.1. Выбрать случайное число $a$, $2 \leq a \leq p - 2$.
   4.2. Проверить число $p$ тестом Миллера–Рабина для основания $a$. Если число $p$ прошло тест, то вернуться на шаг 4.1. В противном случае вернуться на шаг 1.
5. Результат: $p$. □

Равенство $b_{k-1} = 1$ на шаге 2 гарантирует, что длина числа $p$ в точности равна $k$ бит, равенство $b_0 = 1$ обеспечивает нечетность числа $p$.

Число проверок на шаге 3 на практике варьируется от 256 до 2000. При проверке чисел 3, 5, 7 отбраковываются 54% нечетных составных чисел, при проверке простых чисел, меньших 100, — 76%, при проверке простых чисел, меньших 256, — 80%. Однако чем больше $n$ и чем больше чисел мы проверяем, тем дольше шаг 3.

## 5.2. Детерминированные алгоритмы проверки чисел на простоту

Детерминированные тесты можно назвать тестами, *доказывающими* простоту. Эти тесты вычислительно более сложны, чем вероятностные, поэтому, прежде чем проверять число детерминированным тестом, необходимо проверить его, например, тестом Миллера–Рабина.

Всякий детерминированный тест, по сути, представляет собой доказательство теоремы о достаточном условии простоты числа. Поэтому числа, которые считаются простыми на основании прохождения ими детерминированного теста, называются *доказуемо простыми*.

Детерминированные тесты можно использовать и для генерации простых чисел. Для этого выбирают некоторую последовательность чисел специального вида, среди которых нужно найти простое число, и к каждому из этих чисел применяют детерминированный тест.

В некоторых детерминированных тестах используются случайные числа. Однако, в отличие от тестов Ферма, Соловэя–Штрассена или Миллера–Рабина, эти тесты дают ответ «Число $n$ простое» или «Число $n$, вероятно, составное». Поэтому при проверке чисел на простоту можно параллельно выполнять какой-либо вероятностный и детерминированный тест до тех пор, пока один из них не даст определенный ответ.

### 5.2.1. Проверка чисел Мерсенна

Определение 5.5. Пусть $s \geq 2$ — целое число. *Числом Мерсенна* называется целое число $M_s = 2^s - 1$, где число $s$ простое. Если число $2^s - 1$ простое, то оно называется *простым числом Мерсенна*.

Критерием простоты чисел Мерсенна служит следующее утверждение.

Теорема 5.9 (Люка–Лемер). Число Мерсенна $M_s = 2^s - 1$, где $s \geq 3$ — нечетное число, является простым тогда и только тогда, когда

1) число $s$ простое;

2) выполняется сравнение $L_{s-2} \equiv 0 \pmod{M_s}$, где последовательность $\{L_k\}$ формируется по следующему правилу: $L_0 = 4$, $L_{k+1} \equiv L_k^2 - 2 \pmod{M_s}$ при $k \geq 0$.

*Доказательство* см., например, в работах [3, 4].

Это условие простоты числа Мерсенна было открыто Э. Люка в конце 1890-х годов, а в данной формулировке приведено около 1930 года в работах Д. Лемера. Теорема 5.9 положена в основу следующего алгоритма проверки числа Мерсенна на простоту.

Алгоритм 5.6. Алгоритм Люка–Лемера.

*Вход*. Число Мерсенна $M_s = 2^s - 1$, $s \geq 3$.

*Выход*. «Число $M_s$ простое» или «Число $M_s$ составное».

1. Методом пробного деления проверить, есть ли у числа $s$ делители от 2 до $\left[\sqrt{s}\right]$. Если есть, то результат: «Число $M_s$ составное».

2. Положить $L = 4$.

3. Для $k = 1, 2, \ldots, s - 2$ вычислять $L \leftarrow L^2 - 2 \pmod{M_s}$.

4. При $L = 0$ результат: «Число $M_s$ простое». В противном случае результат: «Число $M_s$ составное». □

Пример 5.16. Пусть $s = 11$ — простое число. Проверим, будет ли простым число $2^{11} - 1 = 2047$.

Строим последовательность $L_i$:

$L_0 = 4$, $L_1 = 4^2 - 2 = 14$, $L_2 = 14^2 - 2 = 194$,

$L_3 = 194^2 - 2 \equiv 788 \pmod{2047}$, $L_4 = 788^2 - 2 \equiv 701 \pmod{2047}$,

$L_5 = 701^2 - 2 \equiv 119 \pmod{2047}$, $L_6 = 119^2 - 2 \equiv 1877 \pmod{2047}$,

$L_7 = 1877^2 - 2 \equiv 240 \pmod{2047}$, $L_8 = 240^2 - 2 \equiv 282 \pmod{2047}$,

$L_9 = 282^2 - 2 \equiv 1736 \quad 0 \pmod{2047}$.

Значит, число 2047 составное. И в самом деле, $2047 = 23 \cdot 89$. □

Пример 5.17. Пусть $s = 13$ — простое число. Проверим, будет ли простым число $2^{13} - 1 = 8191$.

Строим последовательность $L_i$:

$L_0 = 4$, $L_1 = 4^2 - 2 = 14$, $L_2 = 14^2 - 2 = 194$,

$L_3 = 194^2 - 2 \equiv 4870 \pmod{8191}$, $L_4 = 4870^2 - 2 \equiv 3953 \pmod{8191}$,

$L_5 = 3953^2 - 2 \equiv 5970 \pmod{8191}$, $L_6 = 5970^2 - 2 \equiv 1857 \pmod{8191}$,

$L_7 = 1857^2 - 2 \equiv 36 \pmod{8191}$, $L_8 = 36^2 - 2 = 1294$,

$L_9 = 1294^2 - 2 \equiv 3470 \pmod{8191}$, $L_{10} = 3470^2 - 2 \equiv 128 \pmod{8191}$,

$L_{11} = 128^2 - 2 = 16382 \equiv 0 \pmod{8191}$.

Значит, число 8191 простое. □

В настоящее время неизвестно, конечно ли число простых чисел Мерсенна. В таблице 4.1 приведены известные на сегодняшний день простые числа Мерсенна ($d_p$ означает число десятичных разрядов в числе $M_p$; 39?–42? означает, что неизвестно, есть ли еще простые числа Мерсенна между $2^{6972593} - 1$ и этими числами; см. также www.mersenne.org).

Таблица 5.1

**Простые числа Мерсенна**

| № п/п | $p$ | $d_p$ | Год открытия | Автор и год опубликования | Компьютер |
|---|---|---|---|---|---|
| 1 | 2 | 1 | – | – | |
| 2 | 3 | 1 | – | – | |
| 3 | 5 | 2 | – | – | |
| 4 | 7 | 3 | – | – | |
| 5 | 13 | 4 | 1456[1] | Reguis, 1536; Pietro Cataldi, 1603 | |
| 6 | 17 | 6 | 1588 | Pietro Cataldi, 1603 | |
| 7 | 19 | 6 | 1588 | Pietro Cataldi, 1603 | |
| 8 | 31 | 10 | 1750 | Leonhard Euler, 1772 | |
| 9 | 61 | 19 | 1883 | Иван Михеевич Первушин 1883; Paul P. Seelhoff, 1886 | |
| 10 | 89 | 27 | 1911 | Raymond E. Powers, 1911 | |
| 11 | 107 | 33 | 1913 | Raymond E. Powers, 1914 | |
| 12 | 127 | 39 | 1876 | François Lucas, 1876 | |
| 13 | 521 | 157 | 1952 | Raphael M. Robinson, 1952 | SWAC |
| 14 | 607 | 183 | 1952 | Derrick H. Lehmer, 1952–53; Raphael M. Robinson, 1952 | SWAC |
| 15 | 1279 | 386 | 1952 | Derrick H. Lehmer, | SWAC |

[1] По другим источникам, 1461 г.

| № п/п | $p$ | $d_p$ | Год открытия | Автор и год опубликования | Компьютер |
|---|---|---|---|---|---|
| | | | | 1952–53; Raphael M. Robinson, 1952 | |
| 16 | 2203 | 664 | 1952 | Derrick H. Lehmer, 1952–53; Raphael M. Robinson, 1952 | SWAC |
| 17 | 2281 | 687 | 1952 | Derrick H. Lehmer, 1952–53; Raphael M. Robinson, 1952 | SWAC |
| 18 | 3217 | 969 | 1957 | Hans Riesel, 1957 | BESK |
| 19 | 4253 | 1281 | 1961 | Alexander Hurwitz, John L. Selfridge, 1961 | IBM 7090 |
| 20 | 4423 | 1332 | 1961 | Alexander Hurwitz, John L. Selfridge, 1961 | IBM 7090 |
| 21 | 9689 | 2917 | 1963 | Donald B. Gillies, 1964 | ILLIAC 2 |
| 22 | 9941 | 2993 | 1963 | Donald B. Gillies, 1964 | ILLIAC 2 |
| 23 | 11213 | 3376 | 1963 | Donald B. Gillies, 1964 | ILLIAC 2 |
| 24 | 19937 | 6002 | 1971 | Bryant Tuckerman, 1971 | IBM 360/91 |
| 25 | 21701 | 6533 | 1978 | Landon C. Noll, Laura A. Nickel, 1980 | Cyber 174 |
| 26 | 23209 | 6987 | 1979 | Landon C. Noll, 1980 | Cyber 174 |
| 27 | 44497 | 13395 | 1979 | Harry L. Nelson, David Slowinski, 1979 | Cray 1 |
| 28 | 86243 | 25962 | 1982 | David Slowinski, 1982 | Cray 1 |
| 29 | 110503 | 33265 | 1988 | Walter N. Colquitt, Luther Welsh, Jr., 1991 | SGI |

| № п/п | $p$ | $d_p$ | Год открытия | Автор и год опубликования | Компьютер |
|---|---|---|---|---|---|
| 30 | 132049 | 39751 | 1983 | David Slowinski, 1988 | Cray X-MP |
| 31 | 216091 | 65050 | 1985 | David Slowinski, 1989 | Cray X-MP |
| 32 | 756839 | 227832 | 1992 | David Slowinski, Paul Gage, 1992 | Cray 2 |
| 33 | 859433 | 258716 | 1994 | David Slowinski, Paul Gage, 1994 | Cray C90 |
| 34 | 1257787 | 378632 | 1996 | David Slowinski, Paul Gage | Cray T94 |
| 35 | 1398269 | 420921 | 1996 | Joel Armengaud, George F. Woltman и др. (GIMPS) | Pentium 90 |
| 36 | 2976221 | 895932 | 1997 | Gordon Spence, George F. Woltman и др. (GIMPS) | Pentium 100 |
| 37 | 3021377 | 909526 | 1998 | Roland Clarkson, George F. Woltman, Scott Kurowski и др. (GIMPS, PrimeNet) | Pentium 200 |
| 38 | 6972593 | 2098960 | 1999 | Nayan Hajratwala, George F. Woltman, Scott Kurowski и др. (GIMPS, PrimeNet) | Pentium II 350 |
| 39? | 13466917 | 4053946 | 2001 | Michael Cameron, George F. Woltman, Scott Kurowski и др. (GIMPS, PrimeNet) | AMD T-Bird 800 |
| 40? | 20996011 | 6320430 | 2003, | Michael Shafer, | Pentium 4, |

| № п/п | $p$ | $d_p$ | Год открытия | Автор и год опубликования | Компьютер |
|---|---|---|---|---|---|
| | | | 19 ноября | George F. Woltman, Scott Kurowski и др. (GIMPS, PrimeNet) | 2 ГГц |
| 41? | 24036583 | 7235733 | 2004, 1 июня | Josh Findley и др. (GIMPS, PrimeNet) | Pentium 4, 2,4 ГГц |
| 42? | 25964951 | 7816230 | 2005, 18 февраля | Martin Nowak, George F. Woltman, Scott Kurowski и др. (GIMPS, PrimeNet) | Pentium 4, 2,4 ГГц |

Числа Мерсенна $M_s$ обладают тем свойством, что число $M_s + 1$ является сильно составным. Следующая теорема позволяет проверять на простоту произвольное число $n$, для которого известно разложение числа $n + 1$.

Теорема 5.10. Пусть целые числа $p$ и $q$ взаимно просты и пусть последовательность $\{U_i\}$ определяется соотношениями $U_0 = 0$, $U_1 = 1$, $U_{i+1} = pU_i - qU_{i-1}$ при $i \geq 1$. Положительное нечетное число $n$ является простым, если выполнены следующие условия:

1) $p^2 - 4q$ — квадратичный невычет по модулю $n$;

2) $U_{n+1} \equiv 0 \pmod{n}$;

3) $U_{(n+1)/r} \not\equiv 0 \pmod{n}$ для всех простых делителей $r$ числа $n + 1$.

*Доказательство* см. в работе [5].

Пример 5.18. Пусть $n = 350657$. Разложим на множители число $n + 1$:

$$350658 = 2 \cdot 3^2 \cdot 7 \cdot 11^2 \cdot 23.$$

Выберем $p=3$, $q=5$, то есть $p^2-4q=3^2-4\cdot 5=-11$, тогда $\left(\frac{-11}{n}\right)=-1$, и первое условие теоремы выполнено.

Строим последовательность $\{U_i\}$: $U_0=0$, $U_1=1$, $U_2=3$, ..., $U_{n-1}\equiv 280525 \pmod n$, $U_n\equiv 350656 \pmod n$, $U_{n+1}\equiv 0 \pmod n$. Второе условие теоремы выполнено.

Проверяем третье условие:

$$U_{(n+1)/2}\equiv 7281 \pmod n,\quad U_{(n+1)/3}\equiv 155139 \pmod n,$$
$$U_{(n+1)/7}\equiv 299210 \pmod n,\quad U_{(n+1)/11}\equiv 306723 \pmod n,$$
$$U_{(n+1)/23}\equiv 51824 \pmod n.$$

Следовательно, число 350657 простое. □

### 5.2.2. Проверка с использованием разложения числа $n-1$

Ряд критериев проверки на простоту основан на знании частичного или полного разложения числа $n-1$.

Лемма 5.11. Пусть целое число $n\geq 3$ имеет вид $n=q^sR+1$, где число $q$ простое и $R$ не делится на $q$. Если существует такое $a$, что $a^{n-1}\equiv 1 \pmod n$ и НОД$(a^{(n-1)/q}-1,n)=1$, то для любого простого делителя $p$ числа $n$ выполняется сравнение $p\equiv 1 \pmod{q^s}$.

*Доказательство*. Пусть $p$ — простой делитель числа $n$. Тогда из $a^{n-1}\equiv 1 \pmod n$ следует, что $a^{n-1}\equiv 1 \pmod p$, то есть число $n-1=q^sR$ делится на порядок $d$ числа $a$ по модулю $p$.

Условие НОД$(a^{(n-1)/q}-1,n)=1$ означает, что $a^{(n-1)/q}\not\equiv 1 \pmod p$. Следовательно, число $q^{s-1}R$ на $d$ не делится. Значит, $d$ делится на $q^s$.

Согласно малой теореме Ферма, $a^{p-1}\equiv 1 \pmod p$, то есть $p-1$ делится на $d$, а значит, и на $q^s$. □

Теорема 5.12 (Поклингтон). Пусть целое число $n \geq 3$ имеет вид $n = QR + 1$, где НОД$(Q, R) = 1$, $R < Q$ и $Q = \prod_{j=1}^{t} q_j^{\alpha_j}$ — каноническое разложение числа $Q$. Если для каждого $q_j$ существует целое число $a_j$, для которого $a_j^{n-1} \equiv 1 \pmod{n}$ и НОД$(a_j^{(n-1)/q_j} - 1, n) = 1$, то число $n$ простое.

*Доказательство*. Пусть число $n$ составное и $p$ — его простой делитель. По лемме 5.11 и китайской теореме об остатках для любого простого делителя $p$ числа $n$ выполняется сравнение $p \equiv 1 \pmod{Q}$. Значит, $p > Q \geq \sqrt{n}$. Противоречие. □

Для случайно выбранного числа $b$, $1 \leq b \leq n - 1$, вероятность того, что $b^{n-1} \equiv 1 \pmod{n}$ и НОД$(b^{(n-1)/q_j} - 1, n) = 1$, равна $\prod_{j=1}^{t}\left(1 - \frac{1}{q_j}\right) \geq 1 - \sum_{j=1}^{t} \frac{1}{q_j}$.

Пример 5.19. Покажем, как можно генерировать простые числа, используя теорему Поклингтона [1]. Пусть нужно найти простое число длины 8 десятичных знаков.

Выберем произвольное простое число $q_1 \geq 5$, например $q_1 = 19$, и выберем четное число $R$ из интервала $[2, q_1 - 3] = [2, 16]$. Пусть $R = 12$. Положим $n = q_1 R + 1 = 19 \cdot 12 + 1 = 229$. Тогда, согласно теореме Поклингтона, чтобы $n$ было простым, достаточно найти одно целое число $a$, для которого $a^{n-1} \equiv 1 \pmod{n}$ и НОД$(a^R - 1, n) = 1$. Этим условиям удовлетворяет, например, $a = 2$.

Обозначим $q_2 = n = 229$. Выберем четное число $R$ из интервала $[2, q_2 - 3] = [2, 226]$. Пусть $R = 224$. Положим $n = q_2 R + 1 = 229 \cdot 224 + 1 = 51297$. Но при $a = 2$ получаем $a^{n-1} \equiv 4 \pmod{n}$. Это означает, что число $n$ составное и нужно выбрать другое $R$. При $R = 222$ получаем $n = 50839$ и условия теоремы выполнены.

Полагаем $q_3 = n = 50839$. При $R = 300$ получаем $n = q_3R + 1 = 50839 \cdot 300 + 1 = 15251701$. Условия теоремы выполнены, и число 15251701 — простое, требуемой длины.

Отметим, что здесь на каждом шаге неравенство $q_i \geq \sqrt{n}$ выполнено, поскольку

$$n = q_iR + 1 \leq q_i(q_i - 3) + 1 = q_i^2 - 3q_i + 1 \leq q_i^2 - 3 \cdot 5 + 1 < q_i^2. \qquad \square$$

Приведем без доказательства еще один критерий [5, 9], позволяющий судить о простоте числа $n$, зная разложение делителя числа $n - 1$. Пусть $n \geq 3$ — целое число вида $n = 2QR + 1$, где $Q = \prod_{j=1}^{t} q_j^{\alpha_j} \geq \sqrt[3]{n}$, $2R = xQ + y$, $x \geq 0$, $0 \leq y < Q$ и число $y^2 - 4x \neq 0$ не является полным квадратом. Если найдется целое число $a$, для которого $a^{n-1} \equiv 1 \pmod{n}$ и $\text{НОД}(a^{(n-1)/q_j} - 1, n) = 1$ для всех $1 \leq j \leq t$, то число $n$ простое.

Пример 5.20. Пусть $n = 15486433 = 2QR + 1$, где $Q = 624 = 2^4 \cdot 3 \cdot 13 \geq \sqrt[3]{n} \approx 249{,}26$, $R = 12409$. Поделив с остатком $2R$ на $Q$, получим $24818 = 39 \cdot 624 + 482$, то есть $x = 39$, $y = 482$.

Вычисляем $y^2 - 4x = 482^2 - 4 \cdot 39 = 232168$ — делится на $2^3$, а значит, не является полным квадратом.

При $a = 5$ получаем $a^{n-1} \equiv 1 \pmod{n}$ и

$$\text{НОД}(a^{7743216} \pmod{n}, n) = \text{НОД}(15486432, n) = 1,$$

$$\text{НОД}(a^{5162144} \pmod{n}, n) = \text{НОД}(8511400, n) = 1,$$

$$\text{НОД}(a^{1191264} \pmod{n}, n) = \text{НОД}(6618795, n) = 1,$$

значит, число 15486433 простое. $\square$

Другой класс чисел специального вида — *числа Ферма* $F_k = 2^{2^k} + 1$. Еще в 1640 году П. Ферма предположил, что все такие числа являются

простыми. Однако на сегодняшний день известно лишь пять простых чисел Ферма: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$.

Теорема 5.13 (Пепин). При $k \geq 1$ число Ферма $F_k$ является простым тогда и только тогда, когда $3^{\frac{F_k-1}{2}} \equiv -1 \pmod{F_k}$.

*Доказательство.* Если число $F_k$ простое, то по свойству 3 символа Лежандра

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

Вычисляем

$$\left(\frac{3}{F_k}\right) = (-1)^{\frac{F_k-1}{2}}\left(\frac{F_k}{3}\right) = \left(\frac{2^{2^k}+1}{3}\right) = \left(\frac{(-1)^{2^k}+1}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Чтобы доказать достаточность, полагаем в теореме Поклингтона $Q = 2^{2^k}$, $R = 1$ и $a = 3$. □

Заметим, что вместо числа 3 в условиях теоремы 5.13 можно взять любой квадратичный невычет по модулю $F_k$, например 5 или 10.

## Упражнения к главе 5

1. Доказать, что для любого простого числа $p \neq 2$, и любого $a$ такого, что НОД$(a^2 - 1, p) = 1$, число $\dfrac{a^{2p}-1}{a^2-1}$ является псевдопростым по основанию $a$.

2. а) Для каждого из чисел 15; 91; 703 найти все основания, по которым эти числа являются псевдопростыми.

б) Доказать, что если числа $p$ и $2p-1$ простые, то их произведение $n=p(2p-1)$ является псевдопростым ровно по $\frac{\varphi(n)}{2}$ основаниям $a$, а именно по тем основаниям, для которых $\left(\frac{a}{2p-1}\right)=1$.

3. Найти наименьшее псевдопростое число а) по основанию 2; б) по основанию 3; в) по основанию 5.

4. Доказать, что следующие числа являются числами Кармайкла, если все сомножители в скобках — простые числа:

а) $(12k+5)(36k+13)(48k+17)$;

б) $(30k+7)(60k+13)(150k+31)$;

в) $(180k+7)(300k+11)(360k+13)(1200k+41)$.

5. Найти составное число $n$ и основание $a$, для которых $a^{(n-1)/2}\equiv\pm1 \pmod{n}$, но $n$ не является эйлеровым псевдопростым по основанию $a$.

6. Доказать, что если числа $p$ и $2p-1$ простые, то их произведение $n=p(2p-1)$ является эйлеровым псевдопростым ровно по $\frac{\varphi(n)}{4}$ основаниям $a$.

7. Пусть $n=(6k+1)(12k+1)(18k+1)$, где числа $6k+1$, $12k+1$, $18k+1$ — простые. Доказать, что: а) если $k$ нечетное, то $n$ является эйлеровым псевдопростым ровно по $\frac{\varphi(n)}{2}$ основаниям $a$; б) если $k$ четное, то $n$ является эйлеровым псевдопростым ровно по $\frac{\varphi(n)}{4}$ основаниям $a$.

8. Доказать, что если число $n$ псевдопростое по основанию 2, то число $2^n-1$ а) эйлерово псевдопростое по основанию 2; б) сильно псевдопростое по основанию 2.

9. Доказать, что если число $n$ сильно псевдопростое по основанию $a$, то $n$ сильно псевдопростое по основанию $a^k$ для любого целого $k$.

10. Пусть число $n$ является псевдопростым, но не является сильно псевдопростым по основанию $a$. Найти нетривиальный делитель числа $n$.

## Литература к главе 5


1. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. — М.: МЦНМО, 2003.
2. *Коблиц Н.* Курс теории чисел и криптографии / Пер. с англ. М. А. Михайловой и В. Е. Тараканова под ред. *А. М. Зубкова.* — М.: Научное изд-во ТВП, 2001.
3. *Кнут Д.* Искусство программирования. Т. 2. Получисленные алгоритмы. — М.–СПб.–Киев: Вильямс, 2000.
4. *Ноден П.*, *Китте К.* Алгебраическая алгоритмика. — М.: Мир, 1999.
5. *Черемушкин А. В.* Лекции по арифметическим алгоритмам в криптографии. — М.: МЦНМО, 2002. Доступно с http://www.cryptography.ru/.
6. *Alford W. R.*, *Granville A.*, *Pomerance C.* There are infinitely many Carmichael numbers // Annals of Mathematics. 1994. Vol. 139. N. 3. P. 703–722. Доступно с http://citeseer.ist.psu.edu/alford93there.html.
7. *Granville A.* Primality testing and Carmichael numbers // Notices of the American Mathematical Society. 1992. Vol. 39. P. 696–700. Доступно с http://www.dms.umontreal.ca/~andrew/agpapers.html.
8. *Higgins B. C.* The Rabin-Miller probabilistic primality test: some results on the number of non-witnesses to compositeness // Electronic Proceedings of the Allegheny Mountain Section of the Mathematical Association of America. 1996. Vol. 1. Доступно с http://www.ma.iup.edu/MAA/proceedings/vol1/higgins.pdf.

9. *Menezes A.*, *van Oorschot P.*, *Vanstone S.* Handbook of applied cryptography. CRC Press, 1997. Доступно с http://www.cacr.math.uwaterloo.ca/hac/.

10. *Solovay R.*, *Strassen V.* A fast Monte-Carlo test for primality // SIAM Journal on Computing. 1977. Vol. 6. N. 1. P. 84–86.

11. *Smith W.* On Carmichael numbers with 3 factors and the strong pseudoprime test. 1997. Доступно с http://citeseer.ist.psu.edu/smith97carmichael.html.

# Глава 6

# РАЗЛОЖЕНИЕ ЧИСЕЛ НА МНОЖИТЕЛИ И КРИПТОСИСТЕМА RSA

Задача разложения на множители — одна из первых задач, использованных для построения криптосистем с открытым ключом.

Определение 6.1. *Задача разложения составного числа на множители* формулируется так: для данного положительного целого числа $n$ найти его каноническое разложение $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, где $p_i$ — попарно различные простые числа, $\alpha_i \geq 1$.

Задача разложения является более сложной, чем задача проверки числа на простоту, поэтому, прежде чем раскладывать число на множители, его проверяют одним из тестов, рассмотренных в предыдущей главе.

Заметим, что на практике не обязательно находить каноническое разложение числа $n$. Достаточно найти его разложение на два *нетривиальных сомножителя*: $n = pq$, $1 < p \leq q < n$. Далее будем понимать задачу разложения именно в этом смысле.

## 6.1. Метод пробного деления

Самый очевидный метод разложения представляет собой «обращение» решета Эратосфена. Пусть $n$ — нечетное составное число. Перебирая по очереди простые числа $p_i = 3, 5, 7, \ldots$, пытаемся разделить $n$ нацело на $p_i$. Если попытка удалась, полагаем $n \leftarrow \dfrac{n}{p_i}$ и повторяем процедуру до тех пор, пока не получим каноническое разложение числа $n$.

Процесс можно немного ускорить, если заранее вычислить произведения простых чисел. Тогда вместо целочисленного деления нужно вычислить алгоритмом Евклида наибольший общий делитель $d$ числа $n$

и этих произведений и положить $n \leftarrow \frac{n}{d}$, повторяя процедуру до тех пор, пока не получится каноническое разложение числа $n$.

Пример 6.1. Разложим на множители число $n = 84257901$ методом пробного деления.

Составим базу данных из произведений простых чисел по три: $q_1 = 3 \cdot 5 \cdot 7 = 105$; $q_2 = 11 \cdot 13 \cdot 17 = 2431$; $q_3 = 19 \cdot 23 \cdot 29 = 12673$.

Вычисляем $d_{11} = \text{НОД}(n, q_1) = \text{НОД}(84257901, 105) = 21$. Значит, $n$ делится на 3 и на 7. Полагаем $n = \frac{n}{d_{11}} = \frac{84257901}{21} = 4012281$. Далее вычисляем:

$$d_{12} = \text{НОД}(n, q_1) = \text{НОД}(4012281, 105) = 21, \; n = \frac{n}{d_{12}} = 191061;$$

$$d_{13} = \text{НОД}(n, q_1) = \text{НОД}(191061, 105) = 3, \; n = \frac{n}{d_{13}} = 63687;$$

$$d_{14} = \text{НОД}(n, q_1) = \text{НОД}(63687, 105) = 3, \; n = \frac{n}{d_{14}} = 21229.$$

Значит, 84257901 делится на $3^4$ и на $7^2$.

Аналогично,

$$d_{21} = \text{НОД}(n, q_2) = \text{НОД}(21229, 2431) = 13, \; n = \frac{n}{d_{21}} = \frac{21229}{13} = 1633;$$

$$d_{31} = \text{НОД}(n, q_3) = \text{НОД}(1633, 12673) = 23, \quad n = \frac{n}{d_{31}} = \frac{1633}{23} = 71 \; —$$

простое число.

Таким образом, $84257901 = 3^4 \cdot 7^2 \cdot 13 \cdot 23 \cdot 71$. □

«Малость» простых делителей определяется либо размером числа $n$, либо объемом памяти компьютера. Перебрав все простые числа, меньшие $\sqrt{n}$, мы найдем каноническое разложение числа $n$. В наихудшем случае, то есть когда $n$ представляет собой произведение двух про-

стых чисел примерно одинакового размера, для этого потребуется примерно $\sqrt{n}$ делений. В общем случае, если делители, получаемые на каждом шаге, проверяются на простоту, то полное разложение числа $n$ методом пробного деления требует $O(p + \log n)$ операций деления, где $p$ — второй по величине делитель числа $n$.

## 6.2. ρ-Метод Полларда

Пусть $n$ — нечетное составное число, $S = \{0, 1, \ldots, n-1\}$ и $f: S \to S$ — случайное отображение, обладающее сжимающими свойствами, например $f(x) \equiv x^2 + 1 \pmod{n}$. Основная идея метода состоит в следующем. Выбираем случайный элемент $x_0 \in S$ и строим последовательность $x_0, x_1, x_2, \ldots$, определяемую рекуррентным соотношением

$$x_{i+1} = f(x_i),$$

где $i \geq 0$, до тех пор, пока не найдем такие числа $i, j$, что $i < j$ и $x_i = x_j$. Поскольку множество $S$ конечно, такие индексы $i, j$ существуют (последовательность «зацикливается»). Последовательность $\{x_i\}$ будет состоять из «*хвоста*» $x_0, x_1, \ldots, x_{i-1}$ длины $O(\sqrt{\pi n/8})$ и *цикла* $x_i = x_j, x_{i+1}, \ldots, x_{j-1}$ той же длины [2].

Если $p$ — простой делитель числа $n$ и $x_i \equiv x_j \pmod{p}$, то разность $x_i - x_j$ делится на $p$ и НОД$(x_i - x_j, n) > 1$. Число $p$ нам нужно найти, поэтому все вычисления в алгоритме будем проводить по модулю $n$ и на каждом шаге вычислять $d =$ НОД$(x_i - x_j, n)$. Нетривиальный наибольший общий делитель $1 < d < n$ (когда числа $x_i$ и $x_j$ принадлежат одному классу вычетов по модулю $p$, но разным классам вычетов по модулю $n$) как раз и будет искомым делителем $p$ числа $n$. Случай $d = n$ имеет место с пренебрежимо малой вероятностью.

Если последовательно вычислять значения $x_{i+1} = f(x_i)$, запоминать их и искать равные, то число шагов алгоритма в среднем равно $\sqrt{\pi n/2}$.

Кроме того, временная и емкостная сложности равны $O(\sqrt{n})$. Необходимость хранения большого количества информации устраняется, если применить *алгоритм Флойда* [10]: начиная с $i = 1$, рекурсивно вычислять $(x_i, x_{2i})$ из $(x_{i-1}, x_{2i-2})$, пока не найдется такое число $k$, что $x_m = x_{2m}$.

Обозначим длину «хвоста» последовательности через $\lambda$, длину цикла через $\mu$ и оценим максимальное число шагов $m$ до входа в цикл. Понятно, что $x_k = x_i$ при $k \geq i$ тогда и только тогда, когда разность $k - i$ делится на $\mu$ (от $x_i$ до $x_k$ необходимо пройти хотя бы один цикл). Кроме того, должно выполняться неравенство $i \geq \lambda$, поскольку два значения из «хвоста» совпасть не могут — только из цикла. При использовании алгоритма Флойда получаем $x_{2i} = x_i$ тогда и только тогда, когда $i$ делится на $\mu$ и $i \geq \lambda$.

Найдем верхнюю оценку для минимального значения $i_{\min}$, при котором выполняется равенство $x_{2i} = x_i$. Перенумеруем все элементы цикла последовательности $\{x_i\}$ числами от 0 до $\mu - 1$. После $\lambda$ шагов расстояние между точками $x_\lambda$ и $x_{2\lambda}$ будет равно $l \equiv \lambda \pmod{\mu}$: по «одиночной» траектории $\{x_i\}$ сделали $\lambda$ шагов, по «двойной» траектории $\{x_{2i}\}$ — $2\lambda$ шагов. На каждом шаге расстояние между точками «одиночной» и «двойной» траектории увеличивается на 1: после первого шага оно равно $l + 1$, после второго шага $l + 2$, ..., после произвольного числа $s$ шагов — $l + s$. Для совпадения точек двух траекторий необходимо, чтобы $l + s = \mu$, то есть $s = \mu - l = \mu - (\lambda \pmod{\mu})$, где вычитаемое — наименьший неотрицательный вычет по модулю $\mu$. Учитывая, что предварительно до цикла нужно еще пройти весь «хвост» длины $\lambda$, получаем следующие границы:

$$\lambda \leq i_{\min} \leq \lambda + \mu - \lambda \pmod{\mu}.$$

Замечание. Графически последовательность $\{x_i\}$ можно изобразить так, что ее «хвост» и цикл будут образовывать греческую букву «ρ» (рис. 6.1 на стр. 212). Отсюда и название метода.

Алгоритм 6.1. ρ-Метод Полларда.

*Вход*. Число $n$, начальное значение $c$, функция $f$, обладающая сжимающими свойствами.

*Выход*. Нетривиальный делитель $p$ числа $n$.

1. Положить $a \leftarrow c$, $b \leftarrow c$.
2. Вычислить $a \leftarrow f(a) \pmod n$, $b \leftarrow f(b) \pmod n$, $b \leftarrow f(b) \pmod n$.
3. Найти $d \leftarrow$ НОД$(a - b, n)$.
4. Если $1 < d < n$, то положить $p \leftarrow d$ и результат: $p$. При $d = n$ результат: «Делитель не найден»; при $d = 1$ вернуться на шаг 2. □

Пример 6.2. Найдем ρ-методом Полларда нетривиальный делитель числа $n = 1359331$. Положим $c = 1$ и $f(x) \equiv x^2 + 5 \pmod n$. Работа алгоритма иллюстрируется следующей таблицей:

| $i$ | $a$ | $b$ | $d =$ НОД$(a - b, n)$ |
|---|---|---|---|
| | 1 | 1 | |
| 1 | 6 | 41 | 1 |
| 2 | 41 | 123939 | 1 |
| 3 | 1686 | 391594 | 1 |
| 4 | 123939 | 438157 | 1 |
| 5 | 435426 | 582738 | 1 |
| 6 | 391594 | 1144026 | 1 |
| 7 | 1090062 | 885749 | 1181 |

Таким образом, 1181 является нетривиальным делителем числа 1359331 (действительно, $1359331 = 1181 \cdot 1151$). □

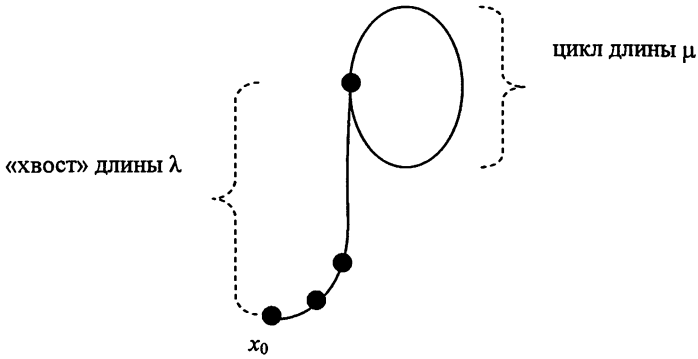



***Рис. 6.1.*** *Случайная последовательность в ρ-методе Полларда*

Пример 6.3. Найдем нетривиальный делитель числа $n = 1373503$. Положим $c = 2$ и $f(x) \equiv x^2 - 2 \pmod{n}$. На первой итерации получаем $a = b = 2$ (неподвижная точка) и $d = 1373503 = n$. Меняя отображение на $f(x) \equiv x^2 - 22 \pmod{n}$, за пять итераций получаем $a = 777096$, $b = 742847$ и $d = 1181$ (действительно, $1373503 = 1181 \cdot 1163$). □

В предположении, что функция $f$ ведет себя как случайная, алгоритм 6.1 требует для нахождения делителя $p$ числа $n$ порядка $O(\sqrt{p})$ модульных умножений. Следовательно, для нахождения нетривиального делителя числа $n$ требуется $O(\sqrt[4]{n})$ модульных умножений.

## 6.3. ($p$ – 1)-Метод Полларда

Пусть $n$ — нечетное составное число и $p$ — его нетривиальный делитель. ($p$ – 1)-Метод особенно эффективен при разложении таких чисел $n$, для которых число $p - 1$ сильно составное [10, 11].

Определение 6.2. Пусть $B = \{p_1, p_2, \ldots, p_s\}$ — множество различных простых чисел. Назовем множество $B$ *базой разложения*. Целое число назовем *B-гладким*, если все его простые делители являются элементами множества $B$.

Идея метода такова. Пусть $n = pq$ и пусть каноническое разложение числа $p - 1$ имеет вид $p - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$. Найдем максимальные показатели $l_1, l_2, \ldots, l_s$, для которых $p_i^{l_i} \le n$. Прологарифмируем обе части этого неравенства: $l_i \ln p_i \le \ln n$, откуда $l_i \le \left[\dfrac{\ln n}{\ln p_i}\right]$. Вычислим

$$M = p_1^{\left[\frac{\ln n}{\ln p_1}\right]} p_2^{\left[\frac{\ln n}{\ln p_2}\right]} \ldots p_s^{\left[\frac{\ln n}{\ln p_s}\right]},$$

тогда $M = (p - 1) \cdot z$ для некоторого целого числа $z$.

Согласно малой теореме Ферма, выполняется сравнение $a^{p-1} \equiv 1 \pmod p$ для любого целого $a$, взаимно простого с $p$. Возводя обе части этого сравнения в степень $z$, получаем $a^M \equiv 1 \pmod p$.

Обозначим $d = \text{НОД}(a^M - 1, n)$. Если $a^M \quad 1 \pmod n$, то число $d$ должно делиться на $p$, поскольку разность $a^M - 1$ делится на $p$ и число $n$ делится на $p$.

Алгоритм 6.2. $(p-1)$-Метод Полларда.

*Вход*. Составное число $n$.

*Выход*. Нетривиальный делитель $p$ числа $n$.

1. Выбрать базу разложения $B = \{p_1, p_2, \ldots, p_s\}$.
2. Выбрать случайное целое $a$, $2 \le a \le n-2$, и вычислить $d \leftarrow \text{НОД}(a, n)$. При $d \ge 2$ положить $p \leftarrow d$ и результат: $p$.
3. Для $i = 1, 2, \ldots, s$ выполнить следующие действия.

   3.1. Вычислить $l \leftarrow \left[\dfrac{\ln n}{\ln p_i}\right]$.

   3.2. Положить $a \leftarrow a^{p_i^l} \pmod n$.
4. Вычислить $d \leftarrow \text{НОД}(a-1, n)$.
5. При $d = 1$ или $d = n$ результат: «Делитель не найден». В противном случае положить $p \leftarrow d$ и результат: $p$. □

Равенство $d = n$ на шаге 5 означает, что каноническое разложение числа $q-1$ включает в себя те же простые числа, что и разложение числа $p-1$. В силу малой теоремы Ферма $a^{p-1} \equiv 1 \pmod p$ и $a^{q-1} \equiv 1 \pmod q$, а поскольку в этом случае число $M$ делится не только на $p-1$, но и на $q-1$, получаем $a^M \equiv 1 \pmod p$ и $a^M \equiv 1 \pmod q$, тогда $a^M \equiv 1 \pmod{pq}$.

Если $p_i \le P$ для $i = 1, 2, \ldots, s$ и модульное умножение выполняется «в столбик», то сложность алгоритма 6.2 равна $O(P \log P (\log n)^2)$. Размер базы выбирается исходя из предполагаемого времени работы алгоритма.

Пример 6.4. Разложим $(p-1)$-методом число $n = 1728239$. Выбираем базу разложения из первых трех простых чисел: $B = \{2, 3, 5\}$. Полагаем $a = 2$ — число, очевидно, взаимно простое с нечетным $n$.

Вычисляем последовательно:

$$l = \left[\frac{\ln n}{\ln 2}\right] = 20, \quad a \equiv a^{2^{20}} \equiv 1357228 \pmod{n};$$

$$l = \left[\frac{\ln n}{\ln 3}\right] = 13, \quad a \equiv a^{3^{13}} \equiv 987665 \pmod{n};$$

$$l = \left[\frac{\ln n}{\ln 5}\right] = 8, \quad a \equiv a^{5^{8}} \equiv 74463 \pmod{n}.$$

Находим $d = \text{НОД}(a-1, n) = \text{НОД}(74462, 1728239) = 1201$.

Таким образом, $p = 1201$ — нетривиальный делитель числа 1728239. Действительно, $1728239 = 1201 \cdot 1439$. При этом $p - 1 = 1200 = 2^4 \cdot 3 \cdot 5^2$. Заметим, что число $1438 = 1439 - 1$ не является $B$-гладким: $1438 = 2 \cdot 719$. □

Пример 6.5. Пусть $n = 1557697$. Выбираем ту же базу разложения, что и в предыдущем случае и снова полагаем $a = 2$.

Вычисляем последовательно:

$$l = \left[\frac{\ln n}{\ln 2}\right] = 20, \quad a \equiv a^{2^{20}} \equiv 301549 \pmod{n};$$

$$l = \left[\frac{\ln n}{\ln 3}\right] = 12, \quad a \equiv a^{3^{12}} \equiv 953296 \pmod{n};$$

$$l = \left[\frac{\ln n}{\ln 5}\right] = 8, \quad a \equiv a^{5^{8}} \equiv 1 \pmod{n}.$$

Находим $d = \text{НОД}(a-1, n) = \text{НОД}(0, 1557697) = 1557697$. Таким образом, $d = n$, и нетривиальный делитель числа $n$ не найден.

Заметим, что здесь $1557697 = 1201 \cdot 1297$, при этом $1297 - 1 = 2^4 \cdot 3^4$, то есть число 1296 тоже является $B$-гладким. □

Пример 6.6. Пусть $n = 3865489$. Если строить базу разложения, начиная с малых простых чисел 2, 3, 5, ..., то для нахождения нетриви-

ального делителя при случайных значениях $a$, взаимно простых с $n$, потребуется база, содержащая не менее 162 первых простых чисел. Это объясняется тем, что $n = pq = 1907 \cdot 2027$, где $1907 - 1 = 2 \cdot 953$ (953 — это 162-е простое число) и $2027 - 1 = 2 \cdot 1013$. Если же $a \equiv 1 \pmod{p}$ (или $a \equiv 1 \pmod{q}$), то на шаге 4 получаем $d = \text{НОД}(a - 1, n) = p$ (или $d = \text{НОД}(a - 1, n) = q$). □

## 6.4. Метод квадратов

Теорема 6.1 (Ферма, о разложении). Для любого положительного нечетного числа $n$ существует взаимно однозначное соответствие между множеством делителей числа $n$, не меньших, чем $\sqrt{n}$, и множеством пар $\{s, t\}$ таких неотрицательных целых чисел, что $n = s^2 - t^2$.

*Доказательство*. Пусть $n = pq$, где $q \geq p$. Полагая

$$s = \frac{p+q}{2}, \quad t = \frac{q-p}{2},$$

получаем нужную пару $\{s, t\}$.

Обратно, пусть $n = s^2 - t^2 = (s + t)(s - t)$. Полагая $p = s - t$, $q = s + t$, получаем требуемое разложение. □

Пример 6.7. У числа 15 два делителя, не меньших, чем $\sqrt{15}$, — это числа 5 и 15. Тогда получаем два представления:

1) $15 = pq = 3 \cdot 5$, откуда $s = 4$, $t = 1$ и $15 = 4^2 - 1^2$;

2) $15 = pq = 1 \cdot 15$, откуда $s = 8$, $t = 7$ и $15 = 8^2 - 7^2$. □

Пример 6.8. У числа 9 два делителя, не меньших, чем $\sqrt{9}$, — числа 3 и 9. Тогда получаем два представления:

1) $9 = pq = 3 \cdot 3$, откуда $s = 3$, $t = 0$ и $9 = 3^2 - 0^2$;

2) $9 = pq = 1 \cdot 9$, откуда $s = 5$, $t = 4$ и $9 = 5^2 - 4^2$. □

Пример 6.9. У числа 11 один делитель, не меньший, чем $\sqrt{11}$, — само число 11. Тогда получаем представление $11 = pq = 1 \cdot 11$, откуда $s = 6$, $t = 5$ и $11 = 6^2 - 5^2$. □

Если $n = pq$, где числа $p$ и $q$ близки друг к другу, то число $t$ мало, а значит, $s$ немного больше, чем $\sqrt{n}$. В этом случае можно найти $p$ и $q$, последовательно перебирая числа $s = \left[\sqrt{n}\right] + 1, \left[\sqrt{n}\right] + 2, \ldots$ до тех пор, пока не найдется такое $s$, что разность $s^2 - n$ является полным квадратом, то есть равна $t^2$ [3].

Далее будем считать, что число $n$ не является полным квадратом.

Пример 6.10. Разложим на множители число $n = 1406303$ методом Ферма.

Вычисляем:

$$s = \left[\sqrt{n}\right] + 1 = 1185 + 1 = 1186,\ s^2 - n = 1186^2 - 1406303 = 293;$$

$$s = \left[\sqrt{n}\right] + 2 = 1185 + 2 = 1187,\ s^2 - n = 1187^2 - 1406303 = 2666;$$

$$s = \left[\sqrt{n}\right] + 3 = 1185 + 3 = 1188,\ s^2 - n = 1188^2 - 1406303 = 5041 = 71^2.$$

Таким образом, $s = 1188$, $t = 71$, $p = s - t = 1117$, $q = s + t = 1259$. Действительно, $1406303 = 1117 \cdot 1259$. □

Понятно, что чем больше разность между числами $p$ и $q$, тем более трудоемким становится метод Ферма. В этом случае можно воспользоваться обобщенным метода Ферма [3]: для небольшого целого числа $k$ последовательно вычислять $s = \left[\sqrt{kn}\right] + 1$, $\left[\sqrt{kn}\right] + 2, \ldots$, пока не получится такое число $s$, что разность $s^2 - kn$ является полным квадратом, то есть равна $t^2$. Отсюда $(s + t)(s - t) = kn$, и значит, числа $s - t$ и $n$ имеют нетривиальный общий делитель.

Пример 6.11. Разложим на множители число $n = 5338771$. При разложении методом Ферма лишь на 160-м шаге получим $s = \left[\sqrt{n}\right] + 160 = 2310 + 160 = 2470$, откуда

$$t^2 = 2470^2 - 5338771 = 762129,\ t = 873,\ s + t = 3343,\ s - t = 1597.$$

Выбрав $k = 8$, уже со второй попытки получим

$$([\sqrt{kn}] + 2)^2 - kn = ([\sqrt{8 \cdot 5338771}] + 2)^2 - 8 \cdot 5338771 =$$
$$= 6537^2 - 8 \cdot 5338771 = 22201 = 149^2.$$

Таким образом, $s = 6537$, $t = 149$, $s - t = 6537 - 149 = 6388$ и НОД(6388, $n$) = 1597. Действительно, $n = 1597 \cdot 3343$. □

Поскольку подобрать такое число $k$ не всегда легко, на практике для разложения числа $n$ достаточно найти такие целые числа $s$, $t$, что $s^2 \equiv t^2 \pmod n$, то есть $(s + t)(s - t) \equiv 0 \pmod n$. Если $s \quad \pm t \pmod n$, то число $n$ делит произведение двух чисел $s + t$ и $s - t$, но не делит ни один из сомножителей. Значит, один делитель числа $n$ ($p$ = НОД($s - t$, $n$)) делит разность $s - t$, а другой делитель $q = \dfrac{n}{p}$ делит сумму $s + t$.

Алгоритм 6.3. Метод Диксона [9, 10].

*Вход*. Составное число $n$.

*Выход*. Нетривиальный делитель $p$ числа $n$.

1. Построить базу разложения $B = \{p_0, p_1, \ldots, p_h\}$, где $p_0 = -1$ и $p_1, \ldots, p_h$ — попарно различные простые числа.
2. Найти $h + 2$ целых чисел $s_i$, для каждого из которых абсолютно наименьший вычет $s_i^2 \pmod n$ является $B$-гладким:

$$s_i^2 \pmod n = \prod_{j=0}^{h} p_j^{\alpha_j(s_i)},$$

где $\alpha_j(s_i) \geq 0$, и каждому числу $s_i$ сопоставить вектор показателей $(\alpha_0(s_i), \alpha_1(s_i), \ldots, \alpha_h(s_i))$.

3. Найти (например методом гауссова исключения) такое непустое множество $K \subseteq \{1, 2, \ldots, h+1\}$, что $\bigoplus_{k \in K} \mathbf{e}_k = \mathbf{0}$, где $\mathbf{e}_k = (e_1^{(k)}, e_2^{(k)}, \ldots, e_h^{(k)})$, $e_j^{(k)} \equiv \alpha_j(s_k) \pmod 2$, $0 \leq j \leq h$.

4. Положить $s \leftarrow \prod_{k \in K} s_k \pmod n$, $t \leftarrow \prod_{i=1}^{h} p_i^{\frac{1}{2}\sum_{k \in K} \alpha_i(s_k)} \pmod n$. Тогда $s^2 \equiv t^2 \pmod n$.

5. Если $s \quad \pm t \pmod n$, то положить $p \leftarrow$ НОД$(s - t, n)$ и результат: $p$.

В противном случае вернуться на шаг 3 и поменять множество $K$ (на практике обычно есть несколько вариантов выбора множества $K$ при одной и той же базе разложения $B$. Если все возможности исчерпаны, то следует увеличить базу разложения). □

По этой схеме построены метод непрерывных дробей и метод квадратичного решета.

### 6.4.1. Метод непрерывных дробей

В этом методе, опубликованном Дж. Брилхартом (J. Brillhart) и М. Моррисоном (M. Morrison) в 1975 году [7], в качестве чисел $s_i$ выбираются числители подходящих дробей к обыкновенной непрерывной дроби, выражающей число $\sqrt{n}$. Малый размер чисел $s_i^2 \pmod n$ обеспечивается следующими утверждениями.

Теорема 6.2. Если $\frac{P_k}{Q_k}$, где $k = 1, 2, \ldots,$ — подходящие дроби к числу $\alpha > 1$, которое задано обыкновенной непрерывной дробью, то для всех $k$ справедлива оценка $\left|P_k^2 - \alpha^2 Q_k^2\right| < 2\alpha$.

*Доказательство*. Из следствия к теореме 2.1 и соотношений между знаменателями соседних подходящих дробей получаем:

$$\left|P_k^2-\alpha^2Q_k^2\right|=Q_k^2\cdot\left|\alpha-\frac{P_k}{Q_k}\right|\cdot\left|\alpha+\frac{P_k}{Q_k}\right|<$$

$$<Q_k^2\cdot\frac{1}{Q_kQ_{k+1}}\cdot\left(\alpha+\left(\alpha+\frac{1}{Q_kQ_{k+1}}\right)\right)=2\alpha\left(\frac{Q_k}{Q_{k+1}}+\frac{1}{2\alpha Q_{k+1}^2}\right)<$$

$$<2\alpha\left(\frac{Q_k}{Q_{k+1}}+\frac{1}{Q_{k+1}}\right)=\frac{2\alpha(Q_k+1)}{Q_{k+1}}<\frac{2\alpha Q_{k+1}}{Q_{k+1}}=2\alpha. \qquad \square$$

Следствие. Пусть положительное целое число $n$ не является полным квадратом и $\frac{P_k}{Q_k}$, где $k=1, 2, \ldots$, — подходящие дроби к числу $\sqrt{n}$. Тогда для абсолютно наименьшего вычета $P_k^2 \pmod n$ справедлива оценка $\left|P_k^2 \pmod n\right|<2\sqrt{n}$, причем $P_k^2 \pmod n=P_k^2-nQ_k^2$.

*Доказательство*. Учитывая, что $P_k^2-nQ_k^2\equiv P_k^2 \pmod n$, и применяя теорему 6.2 к числу $\alpha=\sqrt{n}$, получаем требуемые соотношения. $\square$

Таким образом, в алгоритме Диксона в качестве $s_i$ можно брать числители подходящих дробей к $\sqrt{n}$. Кроме того, из базы $B$ можно исключить те простые числа $p_i$, по модулю которых $n$ является квадратичным невычетом. Действительно, пусть $p$ — простой делитель числа $P_k^2 \pmod n=P_k^2-nQ_k^2$, то есть $P_k^2\equiv nQ_k^2 \pmod p$. По следствию из леммы 2.1 НОД($P_k$, $Q_k$) = 1, тогда НОД($p$, $Q_k$) = 1. Следовательно, существует мультипликативно обратное к числу $Q_k$ по модулю $p$:

$$(P_kQ_k^{-1})^2\equiv n \pmod p,$$

что равносильно условию $\left(\frac{n}{p}\right)=1$.

Пример 6.12. Разложим на множители методом непрерывных дробей число $n = 21299881$.

Строим базу разложения из маленьких простых чисел, выбирая только те числа, по модулю которых $n$ является квадратичным вычетом:

$$\left(\frac{n}{3}\right)=\left(\frac{n}{5}\right)=\left(\frac{n}{7}\right)=\left(\frac{n}{11}\right)=\left(\frac{n}{19}\right)=1,\quad \left(\frac{n}{13}\right)=\left(\frac{n}{17}\right)=-1.$$

Таким образом, в обозначениях алгоритма Диксона, $B = \{-1, 2, 3, 5, 7, 11, 19\}$, $h = 6$.

Ищем числители $P_i$ подходящих дробей к числу

$$\sqrt{n} = [4615; \{5, 1, 1, 2, 1, 7, 1, 27, 1, 6, 1, 2, 12, 23, 1, 8, 2, 3, 6, 1, 1, 1, \ldots\}]$$

и выбираем те из них, для которых значения $P_i^2 \pmod n$ являются $B$-гладкими. Результаты вычислений записываем в таблицу:

| $i$ | $k$ | $P_k$ | $P_k^2 \pmod n$ | $\mathbf{e}_i$ |
|---|---|---|---|---|
| 1 | 2 | 27691 | $-4235 = -1 \cdot 5 \cdot 7 \cdot 11^2$ | (1, 0, 0, 1, 1, 0, 0) |
| 2 | 3 | 50767 | $2688 = 2^7 \cdot 3 \cdot 7$ | (0, 1, 1, 0, 1, 0, 0) |
| 3 | 6 | 1389169 | $-7920 = -1 \cdot 2^4 \cdot 3^2 \cdot 5 \cdot 11$ | (1, 0, 0, 1, 0, 1, 0) |
| 4 | 13 | 12814433311 | $385 = 5 \cdot 7 \cdot 11$ | (0, 0, 0, 1, 1, 1, 0) |
| 5 | 16 | 2764443209657 | $-3800 = -1 \cdot 2^3 \cdot 5^2 \cdot 19$ | (1, 1, 0, 0, 0, 0, 1) |
| 6 | 18 | 20276855015255 | $-1331 = -1 \cdot 11^3$ | (1, 0, 0, 0, 0, 1, 0) |
| 7 | 19 | 127498600693396 | $5415 = 3 \cdot 5 \cdot 19^2$ | (0, 0, 1, 1, 0, 0, 0) |
| 8 | 24 | 2390521616955537 | $-112 = -1 \cdot 2^4 \cdot 7$ | (1, 0, 0, 0, 1, 0, 0) |

Поскольку $\mathbf{e}_1 \oplus \mathbf{e}_3 \oplus \mathbf{e}_6 \oplus \mathbf{e}_8 = \mathbf{0}$, находим

$$s = P_2 \cdot P_6 \cdot P_{18} \cdot P_{24} \equiv 12487442 \pmod n,$$

$$t = 2^4 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^3 \cdot 19^0 = 2236080,$$

$$s^2 \equiv t^2 \equiv 13201055 \pmod n.$$

Условие $s \not\equiv \pm t \pmod n$ выполнено, поэтому вычисляем $q =$ $= \text{НОД}(s - t, n) = \text{НОД}(10251362, 21299881) = 3851$.

Действительно, $21299881 = 3851 \cdot 5531$. □

Временная сложность алгоритма Диксона, использующего непрерывные дроби, равна $O\left(\exp\left(2\sqrt{\ln n \ln\ln n}\right)\right)$. Объем базы разложения равен $h \approx O\left(\exp\left(\frac{2}{3}\sqrt{\ln n \ln\ln n}\right)\right)$.

Метод непрерывных дробей был лучшим алгоритмом разложения с середины 1970-х до начала 1980-х годов, когда появился метод квадратичного решета.

### 6.4.2. Метод квадратичного решета

Еще один способ выбора чисел $s_i$ в алгоритме Диксона был разработан К. Померанцем (K. Pomerance) в 1981 году [12].

Рассмотрим функцию

$$f(x) = \left(x + \left[\sqrt{n}\right]\right)^2 - n = x^2 + 2\left[\sqrt{n}\right]x + \left[\sqrt{n}\right]^2 - n.$$

Поскольку $f(x) \approx x^2 + 2\left[\sqrt{n}\right]x$, при малых значениях $x$, $-c \le x \le c$, где $c$ — некоторая константа, значение $f(x)$ тоже мало, и с большой вероятностью легко раскладывается на множители, то есть в качестве $s_i$ можно брать значения $f(x)$, где $-c \le x \le c$.

Если $f(x)$ делится на простое число $p_i \ne 2$ для некоторого целого $x$, то сравнение

$$f(x) = \left(x + \left[\sqrt{n}\right]\right)^2 \equiv n \pmod{p_i} \tag{6.1}$$

выполняется только в том случае, если $n$ — квадратичный вычет по модулю $p_i$, то есть в базу разложения следует включать только те нечетные простые числа $p_i$, для которых $\left(\frac{n}{p_i}\right)=1$.

Чтобы числа $f(x)$ были с большей вероятностью $B$-гладкими, в методе квадратичного решета осуществим *просеивание*: решая сравнение (6.1) относительно $x$ для каждого простого числа $p_i \neq 2$ из базы разложения, получим два решения $x_1(p_i) \pmod{p_i}$, $x_2(p_i) \pmod{p_i}$ (для $p_1 = 2$ получим одно решение $x_1(p_1) \pmod{p_1}$). Тогда все целые числа вида $x_j(p_i) + kp_i$ будут удовлетворять сравнению (6.1). Таким образом, в интервале $[-c, c]$ можно оставить только те числа $x$, которые удовлетворяют сравнению $x \equiv x_1(p_i) \pmod{p_i}$ или $x \equiv x_2(p_i) \pmod{p_i}$ для достаточно большого числа элементов $p_i \in B$.

Оптимальное значение для $h$ здесь $O\left(\exp\left(\frac{1}{2}\sqrt{\ln n \ln\ln n}\right)\right)$. Временная сложность алгоритма равна $O\left(\exp\left(\sqrt{\ln n \ln\ln n}\right)\right)$.

Пример 6.13. Разложим на множители число $n = 8931721$ методом квадратичного решета.

Строим базу разложения из маленьких простых чисел, выбирая только те числа, по модулю которых $n$ является квадратичным вычетом:

$$\left(\frac{n}{3}\right)=\left(\frac{n}{5}\right)=\left(\frac{n}{7}\right)=\left(\frac{n}{19}\right)=\left(\frac{n}{23}\right)=1, \quad \left(\frac{n}{11}\right)=\left(\frac{n}{13}\right)=\left(\frac{n}{17}\right)=-1.$$

Таким образом, в обозначениях алгоритма Диксона: $B = \{-1, 2, 3, 5, 7, 19, 23\}$, $h = 6$.

Решая сравнения (6.1) для $p_i \in B$, $i = 1, 2, \ldots, 6$, получаем:

$$
\begin{aligned}
&x_1^{(2)} \equiv 1 \pmod 2,\\
&x_1^{(3)} \equiv 1 \pmod 3, \quad x_2^{(3)} \equiv 2 \pmod 3,\\
&x_1^{(5)} \equiv 1 \pmod 5, \quad x_2^{(5)} \equiv 3 \pmod 5,\\
&x_1^{(7)} \equiv 0 \pmod 7, \quad x_2^{(7)} \equiv 2 \pmod 7,\\
&x_1^{(19)} \equiv 2 \pmod{19}, \quad x_2^{(19)} \equiv 7 \pmod{19},\\
&x_1^{(23)} \equiv 6 \pmod{23}, \quad x_2^{(23)} \equiv 21 \pmod{23}.
\end{aligned}
\tag{6.2}
$$

Пусть $c = 25$. Выполним просеивание: из целых чисел $|x| \le 25$ выберем те, которые удовлетворяют трем и более сравнениям (6.2):

| | (mod 2) | (mod 3) | | (mod 5) | | (mod 7) | | (mod 19) | | (mod 23) | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 1 | 2 | 1 | 3 | 0 | 2 | 2 | 7 | 6 | 21 |
| –25 | + | | + | | | | | | | | + |
| –19 | + | | + | + | | | + | | | | |
| –17 | + | + | | | + | | | + | | + | |
| –14 | | + | | + | | + | | | | | |
| –12 | | | | | + | | + | | + | | |
| –7 | + | | + | | + | + | | | | | |
| –5 | + | + | | | | | + | | | | |
| –2 | | + | | | + | | | | | | + |
| 1 | + | + | | + | | | | | | | |
| 2 | | | + | | | | + | + | | | |
| 7 | + | + | | | | + | | | + | | |
| 11 | + | | + | + | | | | | | | |
| 13 | + | + | | | + | | | | | | |
| 16 | | + | | + | | | + | | | | |
| 21 | + | | | + | | + | | + | | | + |
| 23 | + | | + | | + | | + | | | | |

Для каждого из этих чисел $x$ проверяем значение $f(x)$ на $B$-гладкость, получаем:

| $i$ | $x$ | $s_i = x + \left[\sqrt{n}\right]$ | $f(x)$ | $\mathbf{e}_i$ |
|---|---|---|---|---|
| 1 | –25 | 2963 | $-152352 = -1 \cdot 2^5 \cdot 3^2 \cdot 23^2$ | (1, 1, 0, 0, 0, 0, 0) |
| 2 | –17 | 2971 | $-104880 = -1 \cdot 2^4 \cdot 3 \cdot 5 \cdot 19 \cdot 23$ | (1, 0, 1, 1, 0, 1, 1) |
| 3 | –7 | 2981 | $-45360 = -1 \cdot 2^4 \cdot 3^4 \cdot 5 \cdot 7$ | (1, 0, 0, 1, 1, 0, 0) |
| 4 | –2 | 2986 | $-15525 = -1 \cdot 3^3 \cdot 5^2 \cdot 23$ | (1, 0, 1, 0, 0, 0, 1) |
| 5 | 1 | 2989 | $2400 = 2^5 \cdot 3 \cdot 5^2$ | (0, 1, 1, 0, 0, 0, 0) |
| 6 | 2 | 2990 | $8379 = 3^2 \cdot 7^2 \cdot 19$ | (0, 0, 0, 0, 0, 1, 0) |
| 7 | 7 | 2995 | $38304 = 2^5 \cdot 3^2 \cdot 7 \cdot 19$ | (0, 1, 0, 0, 1, 1, 0) |
| 8 | 21 | 3009 | $122360 = 2^3 \cdot 5 \cdot 7 \cdot 19 \cdot 23$ | (0, 1, 0, 1, 1, 1, 1) |

Поскольку $\mathbf{e}_3 \oplus \mathbf{e}_4 \oplus \mathbf{e}_5 \oplus \mathbf{e}_6 \oplus \mathbf{e}_8 = \mathbf{0}$, находим

$$s = s_3 \cdot s_4 \cdot s_5 \cdot s_6 \cdot s_8 \equiv 702856 \pmod{n},$$

$$t = 2^6 \cdot 3^5 \cdot 5^3 \cdot 7^2 \cdot 19 \cdot 23 \equiv 5052140 \pmod{n},$$

$$s^2 \equiv t^2 \equiv 1999947 \pmod{n}.$$

Условие $s \not\equiv \pm t \pmod{n}$ выполнено, поэтому вычисляем $q =$ $= \text{НОД}(s - t, n) = \text{НОД}(4349284, 8931721) = 2179$.

Действительно, $8931721 = 2179 \cdot 4099$. □

## 6.5. Криптографическая система RSA

Криптосистема RSA [13], предложенная в 1977 году Р. Ривестом (R. Rivest), Э. Шамиром (A. Shamir) и Л. Адлеманом (L. Adleman) и названная по первым буквам фамилий авторов, широко используется для шифрования с открытым ключом и цифровой подписи.

Безопасность криптосистемы RSA основана на том, что по заданным целым числам найти их произведение легко, а разложить данное целое число на простые множители трудно.

### 6.5.1. Принцип действия

Каждому пользователю системы RSA соответствует пара открытый ключ/секретный ключ. Для выработки ключей нужно сгенерировать большие простые числа $p$ и $q$ (на практике, длины не менее 512 бит, $p \neq q$), вычислить их произведение $n = pq$ и функцию Эйлера $\varphi(n) = (p-1)(q-1)$. Далее нужно выбрать целое число $e$, $1 < e < \varphi(n) - 1$, взаимно простое с $\varphi(n)$, и вычислить $d$ — мультипликативно обратное к $e$ по модулю $\varphi(n)$: $d \equiv e^{-1} \pmod{\varphi(n)}$, то есть $ed \equiv 1 \pmod{\varphi(n)}$. Числа $e$ и $d$ называются *открытым* и *секретным показателями* соответственно. Пара $(n, e)$ является открытым ключом (она заносится в некоторую открытую базу данных, наподобие телефонного справочника), число $d$ является секретным ключом. Множители $p$ и $q$ должны храниться в секрете или могут быть уничтожены после выработки ключей.

Пусть $(n, e)$ — открытый ключ пользователя $A$. Чтобы передать пользователю $A$ зашифрованное сообщение $m$, $1 < m < n$, пользователь $B$ вычисляет шифртекст $c \equiv m^e \pmod{n}$. Для расшифрования шифртекста $c$ пользователь $A$ возводит его в степень $d$: $m \equiv c^d \pmod{n}$.

Покажем, что зашифрование и расшифрование определены корректно. Пусть $n = pq$, где $p$ и $q$ — простые числа. Согласно теореме Эйлера, для любого числа $m$, взаимно простого с $n$, справедливо сравнение $m^{\varphi(n)} \equiv 1 \pmod{n}$. Умножая обе его части на $m$, получаем сравнение $m^{\varphi(n)+1} \equiv m \pmod{n}$, справедливое уже для любого целого $m$. Перепишем соотношение $ed \equiv 1 \pmod{\varphi(n)}$ для открытого и секретного показателей в виде $ed = 1 + k\varphi(n)$ для некоторого целого $k$. Тогда

$$c^d \equiv (m^e)^d = m^{1+k\varphi(n)} = m^{1+\varphi(n)} m^{(k-1)\varphi(n)} \equiv m \cdot m^{(k-1)\varphi(n)} =$$

$$= m^{1+(k-1)\varphi(n)} \equiv \ldots \equiv m^{1+\varphi(n)} \equiv m \pmod{n}.$$

Аналогично реализуется *цифровая подпись*: подписью для сообщения $m$, $1 < m < n$, является число $s \equiv m^d \pmod{n}$, где $d$ — секретный

ключ подписи. Проверка подписи осуществляется возведением числа $s$ в степень $e$ — открытый ключ проверки: $s^e \equiv (m^d)^e \equiv m \pmod n$. При совпадении вычисленного и переданного значений $m$ подпись считается подлинной.

### 6.5.2. Безопасность криптосистемы RSA и задача разложения на множители

Лемма 6.3. Задача разложения на множители числа $n = pq$ и задача вычисления функции Эйлера $\varphi(n)$ полиномиально эквивалентны.

*Доказательство.* Если известно разложение числа $n = pq$, то со сложностью $O((\log n)^2)$ можно вычислить функцию Эйлера как $\varphi(n) = (p-1)(q-1)$. Если известны значения $n$ и $\varphi(n)$, то, зная, что $n$ есть произведение двух различных простых чисел, из соотношения $\varphi(n) = (p-1)(q-1) = pq - (p+q) + 1 = n - (p+q) + 1$ получаем, что сумма $p + q = n - \varphi(n) + 1$, а произведение $pq = n$. Следовательно, по теореме Виета числа $p$ и $q$ являются целочисленными корнями квадратного уравнения $x^2 - (n - \varphi(n) + 1)x + n = 0$, сложность решения которого равна $O((\log n)^3)$. □

Теорема 6.4. Задача вычисления секретного показателя $d$ сводится с полиномиальной сложностью к задаче вычисления функции $\varphi(n)$.

*Доказательство.* Пусть значение $\varphi(n)$ известно. Применив расширенный алгоритм Евклида к числам $e$ и $\varphi(n)$, получим два целых числа $a$, $b$, удовлетворяющих равенству $ae + b\varphi(n) = 1$, причем $0 < a < \varphi(n)$, $0 < b < e$. Тогда $a = d$. Сложность нахождения числа $d$ равна $O((\log n)^2)$. □

В общем случае задача дешифрования системы RSA эквивалентна задаче извлечения корня степени $e$ по модулю $n$.

Зная открытый и секретный показатели, можно разложить число $n$ на множители. Для этого достаточно найти значение квадратного корня из единицы, отличное от $\pm 1$. Если $t^2 \equiv 1 \pmod{n}$, $t \quad \pm 1 \pmod{n}$, то $t^2 - 1 = (t+1)(t-1) \equiv 0 \pmod{n}$. Тогда число $t-1$ делится на простой делитель $p$, а число $t+1$ — на простой делитель $q$ числа $n$. Разложение можно выполнить по аналогии с тестом Миллера–Рабина следующим алгоритмом.

Алгоритм 6.4. Разложение на множители по известным показателям RSA.

*Вход*. Число $n$, показатели $e$, $d$, где $ed \equiv 1 \pmod{\varphi(n)}$.

*Выход*. Такие числа $p$ и $q$, что $n = pq$.

1. Представить число $N = ed - 1$ в виде $N = 2^t s$, где число $s$ нечетное.
2. Выбрать случайное число $a$, $2 \le a \le n-2$, и вычислить $u \leftarrow a^s \pmod{n}$, $v \leftarrow u^2 \pmod{n}$.
3. Пока $v \ne 1$, полагать $u \leftarrow v$, $v \leftarrow u^2 \pmod{n}$.
4. При $u = -1$ вернуться на шаг 2. В противном случае вычислить $p \leftarrow \text{НОД}(u-1, n)$, $q \leftarrow \text{НОД}(u+1, n)$.
5. Результат: $p$, $q$. □

Пример 6.14. Пусть $n = 849915955f7a878971_{16}$; $e = 2246d67ad_{16}$; $d = baa5af7da82d99ddd_{16}$. Вычисляем $N = 18fda6fcb80155f5e546ac9958_{16}$ и находим представление $N = 2^3 s$, где $s = 31fb4df97002abebca8d5932b_{16}$. Выбираем $a = 5$, тогда $u \equiv a^s \equiv 1cffbf643a790a7c4b_{16} \pmod{n}$. Поскольку $v \equiv u^2 \equiv 1 \pmod{n}$, вычисляем $p = \text{НОД}(u-1, n) = c1a4c7337_{16}$, $q = \text{НОД}(u+1, n) = af4bf0c97_{16}$, или в десятичном виде: $n = 51980825399 \cdot 47055834263$. □

Значит, у каждого пользователя криптосистемы RSA должно быть свое составное число $n$. Оценим количество возможных чисел $n$ длины

1024 бита. Числа $p$ и $q$ в этом случае имеют длину примерно 512 бит. Как следует из асимптотического закона распределения, простых чисел такой длины примерно $T = 3{,}8 \cdot 10^{151}$, то есть возможных значений $n$ всего $\frac{T(T-1)}{2} \approx 7{,}1 \cdot 10^{302}$. Если каждому жителю Земли выдавать каждый день по десять значений $n$, то этих чисел хватит на $10^{287}$ лет, при этом ни разу не будет повторений [1].

### 6.5.3. Атаки на криптосистему RSA, не требующие разложения

В целях ускорения процедур зашифрования и расшифрования, а также формирования и проверки подписи, в системе RSA открытый или секретный показатели часто делают малыми. Поскольку размер числа $n$ составляет сотни бит, сокращение длины показателей первоначально могло выглядеть обоснованным. Однако такой способ повышения скорости шифрования часто приводит к снижению стойкости.

Теорема 6.5 (Винер). Пусть в системе RSA выполняются неравенства $p < q < 2p$ и $d < \frac{1}{3}\sqrt[4]{n}$. Тогда по открытому ключу $(n, e)$ можно вычислить секретный показатель $d$.

*Доказательство* [15]. Для показателей $e$ и $d$ выполняется равенство $ed - k\varphi(n) = 1$ при некотором целом $k$. Разделим обе части этого равенства на $d\varphi(n)$, получим

$$\left|\frac{e}{\varphi(n)} - \frac{k}{d}\right| = \frac{1}{d\varphi(n)},$$

то есть рациональное число $\frac{e}{\varphi(n)}$ является приближением к $\frac{k}{d}$.

Из неравенства $p < q < 2p$ и того, что $p \approx \sqrt{n}$, следует $p + q - 1 < 3\sqrt{n}$ и $|n - \varphi(n)| = |n - (n - (p + q - 1))| = |p + q - 1| < 3\sqrt{n}$.

Аппроксимируя значение $\varphi(n)$ числом $n$, получаем

$$\left|\frac{e}{n}-\frac{k}{d}\right|=\frac{|ed-kn|}{dn}=\frac{|(ed-k\varphi(n))+k\varphi(n)-kn|}{dn}=$$

$$=\frac{|1+k\varphi(n)-kn|}{dn}\le\frac{3k\sqrt{n}}{dn}=\frac{3k}{d\sqrt{n}}.$$

Далее, $k\varphi(n)=ed-1<ed$ и $e<\varphi(n)$, то есть $k<d<\frac{1}{3}\sqrt[4]{n}$. Тогда

$$\left|\frac{e}{n}-\frac{k}{d}\right|\le\frac{1}{d\sqrt[4]{n}}<\frac{1}{2d^2}.$$

Число дробей $\frac{k}{d}$, для которых $d<n$, удовлетворяющих полученному соотношению, не превосходит $\log n$, и все они являются подходящими дробями $\frac{P_i}{Q_i}$ к рациональному числу $\frac{e}{n}$. Для некоторого $i$ будет выполняться равенство $\frac{P_i}{Q_i}=\frac{k}{d}$. Из равенства $ed-k\varphi(n)=1$ следует, что числа $k$ и $d$ взаимно просты, значит, $k=P_i$, $d=Q_i$. □

Пример 6.15. Пусть $n=4617790059809965777$ и открытый показатель $e=2693216516134636609$. Раскладываем число $\frac{e}{n}$ в непрерывную дробь и находим последовательно подходящие дроби:

$$\frac{2693216516134636609}{4617790059809965777}=[0;\,1,1,2,1,1,64,3,1,1,61,2,9,\ldots],$$

$$\frac{P_1}{Q_1}=\frac{1}{1};\quad\frac{P_2}{Q_2}=\frac{1}{2};\quad\frac{P_3}{Q_3}=\frac{3}{5};\quad\frac{P_4}{Q_4}=\frac{4}{7};\quad\frac{P_5}{Q_5}=\frac{7}{12};$$

$$\frac{P_6}{Q_6}=\frac{452}{775};\quad\frac{P_7}{Q_7}=\frac{1363}{2337};\quad\frac{P_8}{Q_8}=\frac{1815}{3112};\quad\frac{P_9}{Q_9}=\frac{3178}{5449}.$$

Для девятой подходящей дроби получаем, что разность $eQ_9-1$ делится нацело на $P_9$:

$$2693216516134636609 \cdot 5449 - 1 = 3178 \cdot 4617790055512156980.$$

Полагаем $d = Q_9 = 5449$ — секретный показатель найден.

Теперь можем применить алгоритм 6.4 к числам $e$ и $d$ или решить квадратное уравнение $x^2 - (n - \varphi(n) + 1)x + n = 0$ относительно $x$, полагая $\varphi(n) = 4617790055512156980$, чтобы разложить число $n$ на множители. Получаем $n = 2148667267 \cdot 2149141531$. □

Для противодействия рассмотренной атаке нужно использовать показатель $d$ не меньший, чем $n^{0,292}$ [6, 14].

Для повышения скорости зашифрования иногда используются малые открытые показатели $e_i$, причем они могут быть одинаковыми (например, равными 3 или 5) для нескольких пользователей. В этом случае, даже если числа $n_i$ различны, можно выполнить дешифрование, не зная секретного ключа. Предположим, что отправитель посылает одно и то же сообщение $m < n_i$ трем пользователям, открытые ключи которых равны $(n_i, 3)$, $i = 1, 2, 3$. Обозначим $x = m^3$. Тогда выполняются сравнения $c_i \equiv m^3 \pmod{n_i}$, $x \equiv c_i \pmod{n_i}$ и значение $x$ может быть восстановлено по китайской теореме об остатках по известным $c_i$ и взаимно простым модулям $n_i$. Для определения сообщения $m$ нужно извлечь кубический корень из $x$ как целого числа, эта операция имеет полиномиальную сложность.

Для того чтобы данная атака была успешной, число пользователей в системе должно быть не меньше, чем значение общего показателя $e$.

Пример 6.16. Пусть в системе три пользователя, открытые ключи которых равны $(n_1, 3) = (3031125583, 3)$ $(n_2, 3) = (2382502391, 3)$, $(n_3, 3) = (2168736499, 3)$. Для того чтобы послать каждому из них зашифрованное по схеме RSA сообщение $m = 1234567890$, отправитель вычисляет шифртексты:

$$c_1 \equiv 1234567890^3 \equiv 1918160952 \pmod{n_1},$$

$$c_2 \equiv 1234567890^3 \equiv 439908825 \pmod{n_2},$$

$$c_3 \equiv 1234567890^3 \equiv 275991853 \pmod{n_3}.$$

Нарушитель, зная, что открытые показатели пользователей одинаковы, восстанавливает по китайской теореме об остатках значение

$$x \equiv 1881676371789154860897069000 \pmod{n_1 n_2 n_3}$$

и находит сообщение $m$, извлекая кубический корень в целых числах:

$$m = \sqrt[3]{1881676371789154860897069000} = 1234567890. \qquad \square$$

Рассмотрим другой простой вариант атаки на систему RSA на основе «частично известных» открытых текстов. Если два сообщения $m_1$, $m_2$ связаны соотношением $m_2 \equiv \alpha m_1 + \beta \pmod{n}$, где числа $\alpha$ и $\beta$ известны, то по известным шифртекстам $c_1$, $c_2$ можно восстановить оба сообщения [8]. Рассмотрим, как это сделать, например, для $e = 3$. По построению шифртекстов: $c_1 \equiv m_1^3 \pmod{n}$, $c_2 \equiv m_2^3 \pmod{n}$. Подставляя во второе сравнение выражение для $m_2$, получаем:

$$c_2 \equiv (\alpha m_1 + \beta)^3 \equiv \alpha^3 m_1^3 + 3\alpha^2\beta m_1^2 + 3\alpha\beta^2 m_1 + \beta^3 \pmod{n}. \qquad (6.3)$$

Прибавим к обеим частям сравнения (6.3) число $2\alpha^3 c_1 - \beta^3$ и умножим обе части сравнения на $\beta$, получим с учетом выражения для $c_1$:

$$\beta(c_2 + 2\alpha^3 c_1 - \beta^3) \equiv (3\alpha^3\beta m_1^2 + 3\alpha^2\beta^2 m_1 + 3\alpha\beta^3) m_1 \pmod{n}. \qquad (6.4)$$

Теперь прибавим к обеим частям сравнения (6.3) число $-\alpha^3 c_1 + 2\beta^3$ и умножим обе части сравнения на $\alpha$:

$$\alpha(c_2 - \alpha^3 c_1 + 2\beta^3) \equiv 3\alpha^3\beta m_1^2 + 3\alpha^2\beta^2 m_1 + 3\alpha\beta^3 \pmod{n}.$$

С учетом сравнения (6.4), получаем выражение для $m_1$:

$$m_1 \equiv \alpha^{-1}\beta(c_2 + 2\alpha^3 c_1 - \beta^3)(c_2 - \alpha^3 c_1 + 2\beta^3)^{-1} \pmod{n}. \qquad (6.5)$$

Пример 6.17. Пусть $n = 849915955f7a878971_{16}$, $e = 3$ и известны два шифртекста: $c_1 = 399a7ec1a60a391d42_{16}$, $c_2 = 1a7dc67779820a24ac_{16}$.

Пусть известно также, что соответствующие открытые тексты связаны соотношением $m_2 \equiv 1a85_{16} \cdot m_1 + 23c895_{16} \pmod{n}$. Подставляя эти значения в формулу (6.5), получаем:

$$m_1 \equiv ced735b52982f33ca_{16} \pmod{n},$$

$$m_2 \equiv 1a85_{16} \cdot m_1 + 23c895_{16} \equiv 75cf7a25d67bf653c2_{16} \pmod{n}. \qquad \square$$

В случае произвольного показателя $e$ имеют место соотношения:

$$m_1^e - c_1 \equiv 0 \pmod{n}, (\alpha m_1 + \beta)^e - c_2 \equiv 0 \pmod{n}.$$

Обозначим неизвестное сообщение $m_1$ через переменную $z$. Тогда, можно записать НОД$(z^e - c_1, (\alpha z + \beta)^e - c_2) = z - m_1$, где коэффициенты полиномов берутся по модулю $n$. Вычислив этот наибольший общий делитель, можно определить $m_1$.

Алгоритм 6.5. Нахождение линейно зависимых открытых текстов по шифртекстам.

*Вход*. Составное число $n$, открытый показатель $e$; шифртексты $c_1$, $c_2$; параметры $\alpha$, $\beta$.

*Выход*. Открытые тексты $m_1$, $m_2$.

1. Вычислить $m_1$ как свободный член линейного полинома $z - m_1 =$ НОД$(z^e - c_1, (\alpha z + \beta)^e - c_2)$, где все операции с коэффициентами выполняются по модулю $n$.
2. Положить $m_2 \leftarrow \alpha m_1 + \beta \pmod{n}$.
3. Результат: $(m_1, m_2)$. $\square$

При использовании умножения «в столбик» и арифметики Монтгомери сложность алгоритма 6.5 равна $O(e^2(\log n)^2)$. При использовании умножения с помощью быстрого преобразования Фурье сложность алгоритма равна $O(e^2(\log n)(\log\log n))$.

Пример 6.18. Пусть $n = 81089$, $c_1 = 32205$, $c_2 = 38069$, $e = 17$; $\alpha = 1$, $\beta = 1$. Найдем НОД$((z+1)^{17} - 38069, z^{17} - 32205)$, вычисляя коэффициенты по модулю $n$. Получаем последовательность вычетов для алгоритма Евклида (с учетом нормирования полиномов по старшему коэффициенту):

$$z^{16} + 8z^{15} + 40z^{14} + 140z^{13} + 364z^{12} + 728z^{11} + 1144z^{10} + 1430z^{9} + 1430z^{8} +$$

$$+ 1144z^{7} + 728z^{6} + 364z^{5} + 140z^{4} + 40z^{3} + 8z^{2} + z + 9195;$$

$$z^{15} + 40552z^{14} + 40576z^{13} + 91z^{12} + 195z^{11} + 20594z^{10} + 47719z^{9} + 429z^{8} +$$

$$+ 351z^{7} + 40772z^{6} + 40660z^{5} + 45z^{4} + 13z^{3} + 30411z^{2} + 36783z + 72676;$$

.....

$$z^{2} + 79994z + 24207;$$

$$z + 68744 = z - 12345,$$

то есть $m_1 = 12345$.

Второе сообщение: $m_2 = m_1 + 1 = 12346$. □

Для того чтобы стойкость к рассмотренному методу дешифрования была не хуже, чем сложность разложения, открытый показатель $e$ должен быть достаточно велик. Приведем минимально возможные значения показателя $e$ для различных размеров задачи разложения, для которых сложность указанной атаки равна сложности разложения [5]:

| $\log_2 n$ | 512 | 768 | 1024 | 2048 | 4096 | 8192 |
|---|---|---|---|---|---|---|
| $e_{\min}$ | $10^8$ | $10^{10}$ | $2\cdot10^{11}$ | $3\cdot10^{15}$ | $10^{21}$ | $10^{29}$ |

Дешифрование возможно и в том случае, если мал порядок открытого показателя $e$ по модулю $\varphi(n)$. Для нахождения открытого текста $m$ по шифртексту $c \equiv m^e \pmod n$ нужно выполнять последовательное зашифрование: $c_1 \equiv c^e \pmod n$, $c_2 \equiv c_1^e \pmod n$ и т. д. — до получения открытого текста (предполагается, что открытый текст обладает избыточ-

ностью, позволяющей его распознать). Отметим, что порядок элемента $e$ по модулю $\varphi(n)$ мал лишь в том случае, если он мал по модулям $p-1$ и $q-1$.

Пример 6.19. Пусть $n = 65710453$ ($p = 7993$, $q = 8221$), $e = 47986991$ и шифртекст $c = \mathrm{f1ecbf}_{16}$ представляет собой зашифрованный открытый текст $m = \mathrm{3ada4a1}_{16}$. Возводим $c$ в степень $e$:

$$c_1 \equiv c^e \equiv 37566_{16} \pmod{n},$$

$$c_2 \equiv c_1^e \equiv 2e85270_{16} \pmod{n},$$

$$c_3 \equiv c_2^e \equiv b5c89_{16} \pmod{n},$$

$$c_4 \equiv c_3^e \equiv 3569603_{16} \pmod{n},$$

$$c_5 \equiv c_4^e \equiv 3ada4a1_{16} \pmod{n}$$

— это и есть открытый текст $m$.

Здесь порядок элемента $e$ равен 6 по модулю $p-1$: $47986991^6 \equiv 1 \pmod{p-1}$, и равен 2 по модулю $q-1$: $47986991^2 \equiv 1 \pmod{q-1}$. □

Если же порядок показателя $e$ мал хотя бы для одного из значений $p-1$ или $q-1$, то можно разложить число $n$ следующим образом. Выбрать случайное число $a_0$, $1 < a_0 < n$. Затем для $i \geq 1$ находить последовательно $a_i \equiv a_{i-1}^e \pmod{n}$ и вычислять с помощью алгоритма Евклида $q = \text{НОД}(a_i - a_0, n)$. При $q > 1$ получим нетривиальный делитель числа $n$.

Пример 6.20. Пусть $n = 67680341$, $e = 57349075$. Выбираем $a_0 = 64201924$ и вычисляем:

$$a_1 = a_0^e = 64201924^{57349075} \equiv 64231195 \pmod{n},$$

$$\text{НОД}(a_1 - a_0, n) = \text{НОД}(29271, n) = 1,$$

$$a_2 = a_1^e = 64231195^{57349075} \equiv 36670270 \pmod{n},$$

$$\text{НОД}(a_2 - a_0, n) = \text{НОД}(-27531654, n) = 1,$$

$$a_3 = a_2^e = 36670270^{57349075} \equiv 36486576 \pmod{n},$$

$$\text{НОД}(a_3 - a_0, n) = \text{НОД}(-27715348, n) = 8419.$$

Действительно, $n = 67680341 = 8419 \cdot 8039$ (порядок элемента $e$ равен 3 по модулю 8418). □

Следовательно, числа $p - 1$ и $q - 1$ должны иметь большие простые делители.

Отметим, что в системе RSA всегда можно получить частичную информацию об открытом тексте $m$ по известному шифртексту $c$ и открытому ключу $(n, e)$. Поскольку открытый показатель $e$ взаимно прост с четным числом $\varphi(n)$, сам он должен быть нечетным. Следовательно, выполняется равенство для символов Якоби

$$\left(\frac{c}{n}\right) = \left(\frac{m^e}{n}\right) = \left(\frac{m}{n}\right)^e = \left(\frac{m}{n}\right),$$

то есть при известном шифртексте и открытом показателе всегда известен один бит информации о сообщении $m$.

## Упражнения к главе 6

1. Разложить следующие числа на множители, используя ρ-метод Полларда: а) 66124207; б) 35677933; в) 21478022263.

2. Разложить следующие числа на множители, используя $(p - 1)$-метод Полларда: а) 8644409; б) 17095777; в) 4839315539.

3. Разложить следующие числа на множители, используя обобщенный метод Ферма: а) 25549949; б) 21431227; в) 19534673.

4. Разложить следующие числа на множители, используя метод непрерывных дробей: а) 2355343; б) 6105409; в) 27658343.

5. Разложить на множители число $n = 46648a118ea35141f5_{16}$, если открытый показатель $e = 5$ и сообщения $m_1$, $m_2$ связаны соотношением $m_2 \equiv \alpha m_1 + \beta \pmod{n}$, где $\alpha = 3039_{16}$, $\beta = 12aff_{16}$ и соответствующие шифртексты $c_1 = 11ffe80b617c5cefc1_{16}$, $c_2 = 2d1bd236c7d4b841f3_{16}$.

## Литература к главе 6


1. *Вельшенбах М.* Криптография на Си и C++ в действии. — М.: ТРИУМФ, 2004.
2. *Кнут Д.* Искусство программирования. Т. 2. Получисленные алгоритмы. — М.–СПб.–Киев: Вильямс, 2000.
3. *Коблиц Н.* Курс теории чисел и криптографии / Пер. с англ. М. А. Михайловой и В. Е. Тараканова под ред. *А. М. Зубкова.* — М.: Научное изд-во ТВП, 2001.
4. *Коутинхо С.* Введение в теорию чисел. Алгоритм RSA. — М.: Постмаркет, 2001.
5. *Ростовцев А. Г., Маховенко Е. Б.* Введение в криптографию с открытым ключом. — СПб.: Мир и Семья, Интерлайн, 2001.
6. *Boneh D., Durfee G.* Cryptanalysis of RSA with private key *d* less than $N^{0.292}$ // IEEE Transactions on Information Theory. 2000. Vol. 46. N. 4. P. 1339–1349.
7. *Brillhart J., Morrison M. A.* A method of factoring and the factorization of F // Mathematics of Computation. 1975. Vol. 29. P. 183–205.
8. *Coppersmith D., Franklin M., Patarin J., Reiter M.* Low-exponent RSA with related messages // EUROCRYPT '96. Springer-Verlag, 1996. Lecture Notes in Computer Science. Vol. 1070. P. 1–9.
9. *Dixon J. D.* Asymptotically fast factorization of integers // Mathematics of Computation. 1981. Vol. 36. P. 255–260.
10. *Menezes A., Oorschot P. van, Vanstone S.* Handbook of Applied Cryptography. CRC Press, 1997.

(http://www.cacr.math.uwaterloo.ca/hac/).

11. *Pollard J. M.* Theorems on factorization and primality testing // Proceedings of the Cambridge Philosophical Society. 1974. Vol. 76. P. 521–528.

12. *Pomerance C.* The quadratic sieve factoring algorithm // Advances in Cryptology — Proceedings of EUROCRYPT 84. Lecture Notes in Computer Science. Springer–Verlag, 1985. Vol. 209. P. 169–182.

13. *Rivest R. L.*, *Shamir A.*, *Adleman L.* A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. 1978. Vol. 21. No 2. P. 120–126.

14. *Verheul E. L.*, van *Tilborg H. C. A.* Cryptanalysis of «less-short» RSA secret exponents // AAECC. 1997. Vol. 8. P. 425–435.

15. *Wiener M.* Cryptanalysis of short RSA secret exponents // IEEE Transactions on Information Theory. 1990. Vol. 36. P. 553–558.

# Глава 7

# ДИСКРЕТНОЕ ЛОГАРИФМИРОВАНИЕ В КОНЕЧНОМ ПОЛЕ

Задача дискретного логарифмирования, как и задача разложения на множители, применяется во многих алгоритмах криптографии с открытым ключом. Предложенная в 1976 году У. Диффи (W. Diffie) и М. Хеллманом (M. Hellman) для установления сеансового ключа, эта задача послужила основой для создания протоколов шифрования и цифровой подписи, доказательств с нулевым разглашением и других криптографических протоколов.

Следует отметить, что в криптографии эта задача возникла еще в 1950-х годах, когда вместо роторных машин стали использоваться регистры сдвига, и нужно было определить место конкретного элемента в данной последовательности сдвигов.

## 7.1. Задача дискретного логарифмирования в конечном поле

Как отмечалось в п. 1.6.1, кольцо классов вычетов $\mathbb{Z}/p\mathbb{Z}$, где $p$ — простое число, является полем, обозначается $\mathbb{F}_p$ и называется конечным полем из $p$ элементов.

Определение 7.1. *Задача дискретного логарифмирования* в конечном поле $\mathbb{F}_p$ формулируется так: для данных целых чисел $a$ и $b$, $1 < a, b < p$, найти *логарифм* — такое целое число $x$, что $a^x \equiv b \pmod p$ (если такое число существует). По аналогии с вещественными числами используется обозначение $x = \log_a b$.

Безопасность соответствующих криптосистем основана на том, что, зная числа $a, x, p$ вычислить $a^x \pmod p$ легко (например, алгоритмом $B$-арного возведения в степень), а решить задачу дискретного логарифмирования трудно. Рассмотрим некоторые методы решения этой задачи.

### 7.1.1. ρ-Метод Полларда

Рассмотренный в предыдущей главе ρ-метод Полларда может использоваться и для решения задачи дискретного логарифмирования. При этом случайное отображение $f$ должно обладать не только сжимающими свойствами, но и вычислимостью логарифма (логарифм числа $f(c)$ можно выразить через неизвестный логарифм $x$ и $\log_a f(c)$). Для дискретного логарифмирования в качестве случайного отображения $f$ чаще всего используются «ветвящиеся» отображения, например

$$f(c)=\begin{cases} ac & \text{ïðè } c<p/2, \\ bc & \text{ïðè } c>p/2. \end{cases}$$

При $c<p/2$ имеем $\log_a f(c)=\log_a c+1$, при $c>p/2$ — $\log_a f(c)=\log_a c+x$.

Алгоритм 7.1. Дискретное логарифмирование ρ-методом Полларда.

*Вход*. Простое число $p$, число $a$ порядка $r$ по модулю $p$, целое число $b$, $1<b<p$; отображение $f$, обладающее сжимающими свойствами и сохраняющее вычислимость логарифма.

*Выход*. Показатель $x$, для которого $a^x \equiv b \pmod p$, если такой показатель существует.

1. Выбрать произвольные целые числа $u$, $v$ и положить $c \leftarrow a^u b^v \pmod p$, $d \leftarrow c$.
2. Выполнять $c \leftarrow f(c) \pmod p$, $d \leftarrow f(f(d)) \pmod p$, вычисляя при этом логарифмы для $c$ и $d$ как линейные функции от $x$ по модулю $r$, до получения равенства $c \equiv d \pmod p$.
3. Приравняв логарифмы для $c$ и $d$, вычислить логарифм $x$ решением сравнения по модулю $r$. Результат: $x$ или «Решений нет». □

Пример 7.1. Решим задачу дискретного логарифмирования $10^x \equiv 64 \pmod{107}$, используя ρ-метод Полларда. Порядок числа 10 по модулю 107 равен 53.

Выберем отображение $f(c) \equiv 10c \pmod{107}$ при $c < 53$, $f(c) \equiv 64c \pmod{107}$ при $c \geq 53$. Пусть $u = 2$, $v = 2$. Результаты вычислений запишем в таблицу:

| Номер шага | $c$ | $\log_a c$ | $d$ | $\log_a d$ |
|---|---|---|---|---|
| 0 | 4 | $2+2x$ | 4 | $2+2x$ |
| 1 | 40 | $3+2x$ | 79 | $4+2x$ |
| 2 | 79 | $4+2x$ | 56 | $5+3x$ |
| 3 | 27 | $4+3x$ | 75 | $5+5x$ |
| 4 | 56 | $5+3x$ | 3 | $5+7x$ |
| 5 | 53 | $5+4x$ | 86 | $7+7x$ |
| 6 | 75 | $5+5x$ | 42 | $8+8x$ |
| 7 | 92 | $5+6x$ | 23 | $9+9x$ |
| 8 | 3 | $5+7x$ | 53 | $11+9x$ |
| 9 | 30 | $6+7x$ | 92 | $11+11x$ |
| 10 | 86 | $7+7x$ | 30 | $12+12x$ |
| 11 | 47 | $7+8x$ | 47 | $13+13x$ |

Приравниваем логарифмы, полученные на 11-м шаге: $7 + 8x \equiv 13 + 13x \pmod{53}$. Решая сравнение первой степени, получаем: $x \equiv 20 \pmod{53}$.

Проверка: $10^{20} \equiv 64 \pmod{107}$. □

Сложность алгоритма 7.1 в среднем составляет $4{,}5\sqrt{(\pi r)/8} \approx 2{,}82\sqrt{r}$ операций вычисления отображения $f$.

### 7.1.2. Методы Гельфонда и Сильвера–Полига–Хеллмана

Эти методы основаны на представлении показателя $x$ как элемента двумерной решетки (см. главу 8). Справедливо следующее утверждение [2].

Теорема 7.1 (А.О. Гельфонд, 1962). Пусть целые числа $a$ и $b$ таковы, что $1 < a, b < p$, где число $p$ простое, порядок числа $a$ по модулю $p$ равен $r$ и $a^x \equiv b \pmod p$. Тогда число $x$ можно найти, выполнив не более чем $2(\sqrt{r} + \log_2 r) - 1$ операций умножения по модулю $p$.

*Доказательство*. Обозначим $s = \left[\sqrt{r}\right] + 1$. Рассмотрим последовательности

$$1, a, a^2 \pmod p, \ldots, a^{s-1} \pmod p \tag{7.1}$$

и

$$b, ba^{-1\cdot s} \pmod p, ba^{-2\cdot s} \pmod p, \ldots, ba^{-(s-1)\cdot s} \pmod p. \tag{7.2}$$

По аналогии с теоремой о делении с остатком представим $x$ в виде $x \equiv \alpha + \beta s \pmod r$, где $0 \le \alpha, \beta < s$. Так как $r$ — порядок элемента $a$, то сравнение $b \equiv a^x \equiv a^{\alpha+\beta s} \pmod p$ выполняется тогда и только тогда, когда $a^\alpha \equiv ba^{-\beta s} \pmod p$, то есть когда в последовательностях (7.1) и (7.2) найдутся равные элементы.

Подсчитаем число операций, необходимых для получения равенства $a^x \equiv b \pmod p$. При вычислении последовательности (7.1) выполняется не более $s - 2$ модульных умножений. Для вычисления $a^{-s} \equiv a^{r-s} \pmod p$ требуется выполнить не более $2\log_2 r$ модульных умножений. Еще не более $s - 1$ модульных умножений требуется для вычисления всех элементов последовательности (7.2). Поэтому общее число умножений, необходимое для решения сравнения $a^x \equiv b \pmod p$, не превосходит величины

$$2s - 3 + 2\log_2 r \le 2(\sqrt{r} + \log_2 r) - 1. \qquad \square$$

Пример 7.3. Решим задачу дискретного логарифмирования $7^x \equiv 167 \pmod{587}$ методом Гельфонда. Порядок числа 7 по модулю 587 равен $r = 293$.

Положим $s = \left[\sqrt{r}\right] + 1 = 18$. Расширенным алгоритмом Евклида находим $7^{-s} \equiv 457 \pmod{587}$. Составляем базу данных вида $(167 \cdot 457^i \pmod{587}, i)$ из элементов последовательности (7.2) и соответствующих степеней при $7^{-s}$ и сортируем ее по первой «координате»:

$$\{(4, 2), (9, 1), (10, 11), (55, 6), (67, 3), (95, 4),$$

$$(124, 9), (167, 0), (236, 14), (279, 8), (316, 10), (322, 16), (404, 17),$$

$$(431, 15), (461, 12), (481, 7), (531, 13), (564, 5)\}.$$

Теперь начинаем строить последовательность (7.1) и сравниваем ее элементы с базой данных: $a^0 = 1$, $a^1 = 7$, $a^2 = 49$, $a^3 = 343$, $a^4 \equiv 53 \pmod{587}$, $a^5 \equiv 371 \pmod{587}$, $a^6 \equiv 249 \pmod{587}$, $a^7 \equiv 569 \pmod{587}$, $a^8 \equiv 461 \pmod{587}$. Нашли элемент базы данных: $b \cdot a^{-s \cdot 12} \equiv a^8 \equiv 461 \pmod{587}$. Останавливаемся и приравниваем значения логарифмов:

$$x \equiv 12 \cdot 18 + 8 \equiv 224 \pmod{293}.$$

Проверка: $7^{224} \equiv 167 \pmod{587}$. $\square$

В зарубежной литературе этот метод называется *методом «giant step–baby step»* или *методом Шэнкса* (D. Shanks).

Следующая теорема является обобщением теоремы 7.1 и была доказана в 1965 году В.И. Нечаевым [2].

Теорема 7.2. Пусть целые числа $a$ и $b$ таковы, что $1 < a, b < p$, где число $p$ простое, порядок числа $a$ по модулю $p$ равен $r$ и $a^x \equiv b \pmod{p}$. Пусть, кроме того, число $r = r_1 r_2$. Тогда число $x$ можно найти,

выполнив не более чем $2(\sqrt{r_1}+\sqrt{r_2})+6\log_2 r_1 r_2+2\log_2 r_1-1$ операций умножения по модулю $p$.

*Доказательство*. Разделим $x$ с остатком на $r_2$:

$$x=\alpha+\beta r_2,$$

тогда $b\equiv a^x\equiv a^{\alpha+\beta r_2}(\bmod p)$. Теперь возведем крайние части этого сравнения в степень $r_1$:

$$b^{r_1}\equiv a^{(\alpha+\beta r_2)r_1}=a^{\alpha r_1}a^{\beta r_2 r_1}\equiv a^{\alpha r_1}\ (\bmod p),$$

то есть $a_1^{\alpha}\equiv b_1\ (\bmod p)$, где $a_1\equiv a^{r_1}(\bmod p)$, $b_1\equiv b^{r_1}(\bmod p)$, при этом число $a_1$ имеет порядок $r_2$ по модулю $p$. А по теореме 7.1 для вычисления дискретного логарифма $\alpha$ числа $b_1$ по основанию $a_1$ требуется не более $2(\sqrt{r_2}+2\log_2 r_2)-1$ операций умножения по модулю $p$.

Еще раз обозначим: $a_2^{\beta}\equiv b_2\ (\bmod p)$, где $a_2\equiv a^{r_2}(\bmod p)$, $b_2\equiv ba^{-\alpha}$ $(\bmod p)$. Дискретный логарифм $\beta$ можно вычислить не более чем за $2(\sqrt{r_1}+2\log_2 r_1)-1$ операций умножения по модулю $p$.

Каждое из значений $a_1$, $b_1$, $a_2$, $b_2$ вычисляется соответственно не более чем за $2\log_2 r_1$, $2\log_2 r_1$, $2\log_2 r_2$ и $2\log_2 r+1$ операций модульного умножения. Отсюда получаем утверждение теоремы. □

Теперь приведем сам алгоритм (в зарубежной литературе он называется *алгоритмом Сильвера–Полига–Хеллмана* [7]).

Алгоритм 7.2. Дискретное логарифмирование методом Сильвера–Полига–Хеллмана.

*Вход*. Простое число $p$, число $a$ порядка $r$ по модулю $p$, где $r=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_n^{\alpha_n}$, целое число $b$, $1<b<p$.

*Выход*. Показатель $x$, для которого $a^x\equiv b\ (\bmod p)$, если такой показатель существует.

1. Для $i = 1, 2, \ldots, n$ выполнить следующие действия.

   1.1. Положить $q \leftarrow p_i$, $\beta \leftarrow \alpha_i$.

   1.2. Положить $c \leftarrow 1, y_{-1} \leftarrow 0$.

   1.3. Вычислить $a' \leftarrow a^{\frac{r}{q}} \pmod p$.

   1.4. Для $k = 0, 1, \ldots, \beta - 1$ выполнить следующие действия.

   1.4.1. Положить

$$c \leftarrow c \cdot a^{y_{k-1}q^{k-1}} \pmod p,\ b' \leftarrow (bc^{-1})^{r/(q^{k+1})} \pmod p.$$

   1.4.2. Вычислить логарифм $y_j \leftarrow \log_{a'} b'$ любым алгоритмом (например, ρ-методом Полларда).

   1.5. Положить $x_i \leftarrow y_0 + y_1 q + \ldots + y_{\beta-1} q^{\beta-1} \pmod{q^\beta}$.

2. Восстановить логарифм $x$ из $x_1, x_2, \ldots, x_n$ по китайской теореме об остатках.

3. Результат: $x$. □

Для обеспечения стойкости криптосистемы к методу Сильвера–Полига–Хеллмана число $p - 1$ должно иметь большой простой делитель.

Пример 7.4. Решим задачу дискретного логарифмирования $10^x \equiv 394 \pmod{541}$ методом Сильвера–Полига–Хеллмана. Число 10 по модулю 541 имеет порядок $r = 540 = 2^2 \cdot 3^3 \cdot 5$.

Результаты вычислений запишем в таблицу:

| $i$ | $q$ | $\beta$ | $a'$ | $k$ | $c$ | $b'$ | $y_j = \log_{a'} b'$ |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 2 | 540 | 0 | 1 | 1 | 0 |
| | | | | 1 | 1 | 540 | 1 |
| 2 | 3 | 3 | 411 | 0 | 1 | 411 | 1 |
| | | | | 1 | 10 | 411 | 1 |
| | | | | 2 | 262 | 129 | 2 |
| 3 | 5 | 1 | 140 | 0 | 1 | 1 | 0 |

Отсюда $x_1 = 0 + 1 \cdot 2 \equiv 2 \pmod{2^2}$, $x_2 = 1 + 1 \cdot 3 + 2 \cdot 3^2 \equiv 22 \pmod{27}$, $x_3 \equiv 0 \pmod 5$. Восстанавливаем логарифм $x$ по китайской теореме об остатках: $x \equiv 130 \pmod{2^2 \cdot 3^3 \cdot 5}$.

Проверка: $10^{130} \equiv 394 \pmod{541}$. □

### 7.1.3. Метод встречи посередине

*Метод встречи посередине* представляет собой вероятностный вариант алгоритма Гельфонда и предполагает создание базы данных объема $O(\sqrt{r})$ из пар вида $(a^{x_j} \pmod p, x_j)$ для случайных чисел $x_j$ и ее сортировку по первой «координате». Для случайных чисел $y_i$ вычисляются значения $b^{y_i}$ и сравниваются с базой данных. Сравнение $b^{y_i} \equiv a^{x_j} \pmod p$ означает, что $xy_i \equiv x_j \pmod r$, откуда $x \equiv x_j y_i^{-1} \pmod r$.

В основу метода встречи посередине положены следующие рассуждения. Пусть осуществляется выборка объема $m$ с возвращением из генеральной совокупности объема $r$, где $m \ll r$. Вероятность того, что в этой выборке не будет двух одинаковых элементов, равна

$$\Pr = \left(1 - \frac{m-1}{r}\right)\left(1 - \frac{m-2}{r}\right)\ldots\left(1 - \frac{1}{r}\right).$$

Прологарифмируем это равенство с учетом того, что $\ln(1 - x) \approx -x$ при $x \ll 1$:

$$-\ln \Pr \approx \sum_{i=1}^{m-1} \frac{m-i}{r} = \sum_{i=1}^{m-1} \frac{i}{r} = \frac{m(m-1)}{2r} \approx \frac{m^2}{2r},$$

откуда

$$\Pr = \exp\left(-\frac{m^2}{2r}\right).$$

Поэтому при $m = O(\sqrt{r})$ можно получить сколь угодно близкую к 1 вероятность совпадения двух элементов выборки. Это свойство вы-

борки с возвращением называют *парадоксом дней рождения*: если предположить, что дни рождения распределены равномерно, то вероятность того, что в группе из 23 человек двое родились в один день, превышает 0,5 (неравенство $e^{-m^2/(2\cdot 365)} > 0{,}5$ выполняется при $m \geq 23$).

Сложность метода встречи посередине определяется этапами создания базы данных и ее сортировки. Сложность создания базы данных равна $O(\sqrt{r})$, сложность сортировки равна $O(\sqrt{r}\log r)$. Поэтому итоговая сложность равна $O(\sqrt{r}\log r)$.

### 7.1.4. Метод базы разложения

Алгоритм Диксона, рассмотренный в главе 6, также можно использовать для решения задачи дискретного логарифмирования. В основе этого метода лежит следующее свойство поля $\mathbb{F}_p$ и кольца $\mathbb{Z}$ целых чисел. Если для некоторых целых чисел $a$, $b$ и $c$ выполняется равенство $ab = c$ в кольце $\mathbb{Z}$, то выполняется и сравнение $ab \equiv c \pmod p$ по модулю любого простого числа $p$. Кроме того, из равенства $a^x = b$ и сравнения $a^y \equiv b \pmod p$ следует $x \equiv y \pmod r$, где $r$ — порядок числа $a$ по модулю $p$.

Алгоритм 7.3. Логарифмирование методом базы разложения [1].

*Вход*. Простое число $p$, число $a$ порядка $r$ по модулю $p$, целое число $b$, $1 < b < p$.

*Выход*. Показатель $x$, для которого $a^x \equiv b \pmod p$, если такой показатель существует.

1. Построить базу разложения $B = \{-1, p_1, p_2, \ldots, p_h\}$ из первых простых чисел $p_j$, где $p_h \approx O(\exp(c\sqrt{\ln p \ln\ln p}))$, $c \approx 1$.

2. Случайным выбором показателей $u_i$ найти множество из $O(m)$ $B$-гладких чисел $b_i \leftarrow a^{u_i} \pmod p$ (при этом $B$-гладким может быть не $b_i$, а $p - b_i$, в этом случае в разложении участвует элемент $-1$ базы разложения):

$$b_i \equiv \prod_{j=0}^{h} p_j^{\alpha_{ij}} \pmod p. \tag{7.3}$$

3. Подбором найти такой показатель $v$, что число $b^v \pmod p$ является $B$-гладким:

$$b^v \equiv \prod_{j=0}^{h} p_j^{\beta_j} \pmod p. \tag{7.4}$$

4. Логарифмируя соотношения (7.3) и (7.4) по основанию $a$, записать систему линейных сравнений:

$$u_i \equiv \sum_{j=0}^{h} \alpha_{ij} \log_a p_j \pmod r, \quad xv \equiv \sum_{j=0}^{h} \beta_j \log_a p_j \pmod r.$$

5. Методом гауссова исключения выразить $xv$ в виде линейной комбинации чисел $u_i$:

$$xv \equiv \sum_i d_i u_i \pmod r. \tag{7.5}$$

6. Если сравнение (7.5) имеет решение $x$, то результат: $x$. Иначе: «Решений нет». □

В каждом сравнении (7.3) почти все показатели $\alpha_{ij}$ равны нулю, поэтому решение системы линейных сравнений по модулю $r$ можно ускорить, если воспользоваться технологиями разреженных матриц (см., например, работу [3]). Кроме того, на шаге 2 можно искать числа вида $b_i \equiv a^{u_i} b^{v_i} \pmod p$ для целых $u_i$, $v_i$ до получения системы линейно независимых сравнений, тогда шаг 3 не нужен.

Выбор на шагах 2 и 3 тех значений $u_i$ и $v$, для которых экспонента является $B$-гладкой, можно рассматривать как «просеивание» экспонент через «решето». Поэтому данный метод, так же как и методы разложения, использующие похожие приемы, относится к *методам решета*.

Сложность алгоритма 7.3 равна $O(\exp(2c\sqrt{\ln p \ln\ln p}))$.

Пример 7.6. Решим задачу дискретного логарифмирования $a^x \equiv b \pmod{547}$ для $a = 7$ (порядок числа 7 по модулю 547 равен 546), $b = 151$. Выберем $B = \{-1, 2, 3, 5\}$.

Находим: $u_1 = 5$, $a^5 \equiv -2 \cdot 3 \cdot 5^2 \pmod{547}$; $u_2 = 15$, $a^{15} \equiv -2 \cdot 5 \pmod{547}$; $u_3 = 23$, $a^{23} \equiv 2^6 \cdot 5 \pmod{547}$; $u_4 = 36$, $a^{36} \equiv 2^3 \cdot 3 \pmod{547}$; $v = 5$, $b^5 \equiv 2^9 \pmod{547}$.

Выражаем 5 из $a^{23}$: $5 \equiv a^{23} \cdot 2^{-6} \pmod{547}$, тогда

$$-1 \equiv a^{15} \cdot 2^{-1} \cdot 5^{-1} \equiv a^{15} \cdot 2^{-1} \cdot a^{-23} \cdot 2^6 = a^{-8} \cdot 2^5 \pmod{547}.$$

Выражаем 3 из $a^{36}$: $3 \equiv a^{36} \cdot 2^{-3} \pmod{547}$. Получаем

$$a^5 \equiv -2 \cdot 3 \cdot 5^2 \equiv (a^{-8} \cdot 2^5) \cdot 2 \cdot (a^{36} \cdot 2^{-3}) \cdot (a^{23} \cdot 2^{-6})^2 \equiv$$

$$\equiv a^{74} \cdot 2^{-9} \equiv a^{74} \cdot b^{-5} \pmod{547}.$$

Отсюда $5x \equiv 69 \pmod{546}$ и $x \equiv 123 \pmod{546}$.

Проверка: $7^{123} \equiv 151 \pmod{547}$. □

## 7.2. Протокол Диффи–Хеллмана

Первым криптографическим протоколом, основанным на задаче дискретного логарифмирования, был протокол Диффи–Хеллмана установления сеансового ключа с двумя участниками [5].

Алгоритм 7.4. Протокол Диффи–Хеллмана.

*Вход*. Простое число $p$, число $a$ простого порядка $r$ по модулю $p$; секретные показатели $x$ и $y$.

*Результат*. Установление общего для двух пользователей ключа $k \equiv a^{xy} \pmod p$.

1. Пользователь $A$ вычисляет значение $u \leftarrow a^x \pmod p$ и отправляет его пользователю $B$.
2. Пользователь $B$ вычисляет значение $v \leftarrow a^y \pmod p$ и отправляет его пользователю $A$.
3. Пользователь $A$ вычисляет значение $k \leftarrow v^x \pmod p$.
4. Пользователь $B$ вычисляет значение $k \leftarrow u^y \pmod p$. □

Число умножений (и, следовательно, длительность возведения в степень) зависит от числа единичных разрядов в двоичном представлении показателей $x$ и $y$. Измерение числа тактов, затраченных на вычисление значений $u$ и $v$, дает некоторую информацию о секретных показателях, поэтому при программной реализации протокола желательно, чтобы длительность вычислений не зависела от вида показателей $x$ и $y$.

Безопасность протокола 7.4 основана на *задаче Диффи–Хеллмана* в конечном поле $\mathbb{F}_p$: для числа $a$, имеющего простой порядок $r$ по модулю $p$, и значений $a^x \pmod p$, $a^y \pmod p$ с неизвестными показателями $x$, $y$ найти значение $a^{xy} \pmod p$. Эта задача полиномиально сводится к задаче дискретного логарифмирования: для заданных чисел $a$, $b$ найти показатель $x$, для которого выполняется сравнение $a^x \equiv b \pmod p$. Если по значению $a^x \pmod p$ можно найти $x$, то по значению $a^y \pmod p$ можно найти $a^{xy} \pmod p$. Обратная сводимость задачи дискретного логарифмирования к задаче Диффи–Хеллмана в общем случае пока не доказана.

Пусть число $p - 1$ имеет большой простой делитель $r$ и разложение числа $r - 1$ известно. Предположим, что задача Диффи–Хеллмана решена, то есть по заданным значениям $a$, $a^x \pmod p$, $a^y \pmod p$ можно найти $a^{xy} \pmod p$. Эта задача эквивалентна задаче вычисления любого из четырех перечисленных элементов по трем остальным. Например, поло-

жив $d \equiv a^x \pmod p$, получаем задачу вычисления значения $d^v \pmod p$ по известным значениям $d$, $d^u \pmod p$, $d^{uv} \pmod p$, где $u \equiv x^{-1} \pmod r$, $v \equiv x^{-1} \cdot y \pmod r$.

Предположим, что число $r-1$ имеет только малые простые делители (максимальный из них ограничен полиномом от $\log p$), порядок числа $g$ по модулю $r$ равен $r-1$ и $1 \le h < r$. Тогда задачу вычисления показателя $y$, для которого $g^y \equiv h \pmod r$, можно решить алгоритмом Сильвера–Полига–Хеллмана с полиномиальной от $\log p$ сложностью.

Покажем, что если в этом случае можно решить задачу Диффи–Хеллмана, то можно решить и задачу дискретного логарифмирования. Задачу нахождения числа $g$, обладающего требуемым свойством, по известному разложению числа $r-1$ можно решить с полиномиальной сложностью с использованием китайской теоремы об остатках. Вычисление логарифма на основании решенной задачи Диффи–Хеллмана выполняется аналогично алгоритму Сильвера–Полига–Хеллмана.

Пусть порядок числа $g_1$ по модулю $r$ равен $q$, где число $q$ — простой делитель числа $r-1$. Положим $a^x \equiv b \pmod p$, $a^y \equiv b^{g_1} \pmod p$, $a^z \equiv b^{g_1^{q-1}} \pmod p$. Решая задачу Диффи–Хеллмана, находим

$$c \equiv a^{yz} \equiv (b^{g_1})^z \equiv b^{g_1 x g_1^{q-1}} \equiv b^x \equiv (a^x)^x \equiv a^{x^2} \pmod p.$$

Затем полагаем $a^y \equiv c^{g_1} \pmod p$, $a^z \equiv c^{g_1^{q-1}} \pmod p$, находим $c_1 \equiv a^{yz} \equiv a^{x^4} \pmod p$ и т. д. Выполняя такие действия, можно вычислить $a^{x^n}$ для произвольного $n$. Придавая показателю $n$ значения делителей числа $r-1$ и сравнивая $a^{x^n}$ с $a$, находим наименьшее $n$, для которого $a^{x^n} \equiv a \pmod p$, при этом $x^n \equiv 1 \pmod r$. Определяем множество возможных значений $x$. Далее, полагая $b_1 \equiv a^s b^t \pmod p$ для случайных показателей $s$, $t$ и повторяя указанные операции, находим наименьшее нату-

ральное $n_1 \neq n$, для которого $(s+tx)^{n_1} \equiv 1 \pmod r$, и определяем множество возможных значений $x$ и т. д. Затем восстанавливаем $x$ по аналогии с китайской теоремой об остатках как пересечение указанных множеств.

Таким образом, при указанных выше ограничениях на максимальный простой делитель числа $r-1$ задача дискретного логарифмирования полиномиально эквивалентна задаче Диффи–Хеллмана [4].

По принципу протокола Диффи–Хеллмана можно строить и протокол шифрования с открытым ключом. Такой протокол *бесключевого шифрования* был предложен в 1986 году Дж. Месси (J. Massey) и Дж. Омурой (J. Omura) [6].

Алгоритм 7.5. Протокол Месси–Омуры.

*Вход*. Простое число $p$; сообщение, представленное числом $t$, где $1 < t < p-1$.

*Результат*. Зашифрование и расшифрование сообщения $t$.

1. Пользователь $A$ вырабатывает случайный показатель $u$, $1 \le u < p$, НОД$(u, p-1) = 1$, вычисляет значение $t^u \pmod p$ и отправляет его пользователю $B$.
2. Пользователь $B$ вырабатывает случайный показатель $v$, $1 \le v < p$, НОД$(v, p-1) = 1$, вычисляет значение $(t^u)^v \equiv t^{uv} \pmod p$ и посылает его пользователю $A$.
3. Пользователь $A$ возводит полученный шифртекст в степень $u^{-1}$: $(t^{uv})^{u^{-1}} \equiv t^v \pmod p$ и посылает значение $t^v \pmod p$ пользователю $B$.
4. Пользователь $B$ возводит полученный шифртекст в степень $v^{-1}$: $(t^v)^{v^{-1}} \equiv t \pmod p$. □

Безопасность этого протокола основана на задаче Месси–Омуры: для заданных $t^u \pmod p$, $t^v \pmod p$, $t^{uv} \pmod p$ найти $t$. Эта задача с полиномиальной сложностью сводится к задаче дискретного логарифми-

рования. Действительно, пусть известно значение $t^u \pmod p$ и логарифм $v$ для значения $t^{uv} \pmod p$. Тогда, вычислив расширенным алгоритмом Евклида значение $v^{-1} \pmod{p-1}$, можно найти $t \equiv (t^u)^{u^{-1}} \pmod p$.

Покажем, что эта задача с полиномиальной сложностью сводится к задаче Диффи–Хеллмана. Предположим, что задача Диффи–Хеллмана решена, то есть для заданных $s$, $s^x \pmod p$, $s^y \pmod p$ можно вычислить $s^{xy} \pmod p$. Полагая $s \equiv t^{uv} \pmod p$, $s^x \equiv t^u \pmod p$, $s^y \equiv t^v \pmod p$, получаем, что $x \equiv u^{-1} \pmod{p-1}$, $y \equiv v^{-1} \pmod{p-1}$, откуда $s^{xy} \equiv t \pmod p$. Таким образом, сложность решения задачи Месси–Омуры не превышает сложности решения задачи Диффи–Хеллмана.

В протоколе Месси–Омуры, как и в схеме RSA, всегда известен один бит информации о сообщении $t$. Действительно, числа $u$ и $v$ обратимы по модулю $p-1$, поэтому оба они должны быть нечетными. Следовательно, числа $t$, $t^u \pmod p$, $t^v \pmod p$, $t^{uv} \pmod p$ являются квадратичными вычетами или невычетами по модулю $p$ одновременно:

$$\left(\frac{t^u}{p}\right) = \left(\frac{t}{p}\right)^u = \left(\frac{t}{p}\right).$$

## Упражнения к главе 7

1. Решить задачу дискретного логарифмирования методом базы разложения и ρ-методом Полларда: а) $3^x \equiv 250 \pmod{1307}$, $r = 653$; б) $6^x \equiv 401 \pmod{2063}$, $r = 1031$; в) $22^x \equiv 651 \pmod{2819}$, $r = 1409$.

2. Решить задачу дискретного логарифмирования методом Гельфонда: а) $100^x \equiv 12 \pmod{11807}$, $r = 5903$; б) $11^x \equiv 11291 \pmod{21599}$, $r = 10799$; в) $12^x \equiv 9000 \pmod{32003}$, $r = 16001$.

3. Решить задачу дискретного логарифмирования методом Сильвера–Полига–Хеллмана: а) $10^x \equiv 100500 \pmod{406981}$; б) $47^x \equiv 123456 \pmod{537241}$; в) $22^x \equiv 456789 \pmod{671233}$.

4. Решить задачу дискретного логарифмирования методом базы разложения: а) $5^x \equiv 98765 \pmod{806087}$; б) $2^x \equiv 11111 \pmod{1221083}$; в) $8^x \equiv 536536 \pmod{1362443}$.

5. Реализовать протокол Месси–Омуры для:

а) $p = a41f825c2779df1d_{16}$, $t = 9ab3f0c1b9775a05_{16}$;

б) $p = 95a70710bd45b9b66bdaa7ebbf591313_{16}$,

$t = 62bc2d3f991f90b2df2957d321174ec4_{16}$;

в) p = 800000000003a5a6e6c075c106fdd0d181c2f8fcaf1bd5c8d3ed73c2b1efdcbb$_{16}$;

t = 39850c39e8dadaa4bc53d1b2d2e06f2bea258f687b00c8b6cf8e11f17c654f29$_{16}$.

## Литература к главе 7


1. *Коблиц Н.* Курс теории чисел и криптографии / Пер. с англ. М. А. Михайловой и В. Е. Тараканова под ред. *А. М. Зубкова.* — М.: Научное изд-во ТВП, 2001.
2. *Нечаев В. И.* Элементы криптографии (Основы теории защиты информации): Учебное пособие для университетов и пед. вузов / Под ред. *В. А. Садовничего.* — М.: Высшая школа, 1999.
3. *Писсанецки С.* Технология разреженных матриц. — М.: Мир, 1988.
4. *Ростовцев А. Г., Маховенко Е. Б.* Введение в криптографию с открытым ключом. — СПб.: Мир и Семья, Интерлайн, 2001.
5. *Diffie W., Hellman M.* New directions in cryptography // IEEE Transactions on Information Theory. 1976. Vol. IT–22. P. 644–654.
6. *Massey J., Omura J.* Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission. Pat. USA 4,567,600, 28 Jan 1986.

7. *Pohlig S. C.*, *Hellman M. E.* An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance // IEEE Transactions on Information Theory. 1978. Vol. 24. P. 106–110.

## Глава 8

# ЭЛЕМЕНТЫ ТЕОРИИ РЕШЕТОК

Решетки используются в криптографии для построения и анализа ранцевых криптосистем, а также при решении задач разложения чисел на множители и дискретного логарифмирования.

## 8.1. Процесс ортогонализации Грама–Шмидта

Определение 8.1. *Скалярным произведением* векторов $\mathbf{a} = (a_1, a_2, \ldots, a_n)$, $\mathbf{b} = (b_1, b_2, \ldots, b_n)$, где $a_i, b_i \in \mathbb{R}$, называется вещественное число

$$(\mathbf{a}, \mathbf{b}) = a_1b_1 + a_2b_2 + \ldots + a_nb_n.$$

Если $(\mathbf{a}, \mathbf{b}) = 0$, то говорят, что векторы $\mathbf{a}$ и $\mathbf{b}$ *ортогональны*.

Определение 8.2. Множество ненулевых векторов $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n \in \mathbb{R}^m$, $m \geq n$, называется *ортогональной системой*, если $(\mathbf{a}_i, \mathbf{a}_j) = 0$ при всех $i \neq j$.

Определение 8.3. Векторы $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$ называются *линейно независимыми* над полем $\mathbb{R}$, если равенство $c_1\mathbf{a}_1 + c_2\mathbf{a}_2 + \ldots + c_n\mathbf{a}_n = \mathbf{0}$ выполняется в том и только в том случае, когда все коэффициенты $c_1, c_2, \ldots, c_n \in \mathbb{R}$ равны нулю.

Определение 8.4. *Нормой* (*длиной*) вектора $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{R}^n$ называется вещественное число

$$\|\mathbf{a}\| = \sqrt{(\mathbf{a}, \mathbf{a})} = \sqrt{a_1^2 + a_2^2 + \ldots + a_n^2}.$$

Теорема 8.1. Пусть $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ — ортогональная система. Тогда векторы $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ линейно независимы.

*Доказательство*. Пусть числа $c_1, c_2, \ldots, c_n \in \mathbb{R}$ таковы, что

$$c_1\mathbf{b}_1 + c_2\mathbf{b}_2 + \ldots + c_n\mathbf{b}_n = \mathbf{0}.$$

Покажем, что все коэффициенты $c_i$ нулевые. Для этого умножим обе части равенства скалярно на произвольный вектор $\mathbf{b}_i$, $1 \le i \le n$, и воспользуемся свойствами скалярного произведения векторов:

$$(c_1\mathbf{b}_1 + c_2\mathbf{b}_2 + \ldots + c_i\mathbf{b}_i + \ldots + c_n\mathbf{b}_n, \mathbf{b}_i) =$$

$$= c_1(\mathbf{b}_1, \mathbf{b}_i) + c_2(\mathbf{b}_2, \mathbf{b}_i) + \ldots + c_i(\mathbf{b}_i, \mathbf{b}_i) + \ldots + c_n(\mathbf{b}_n, \mathbf{b}_i) = 0.$$

По определению ортогональной системы все произведения $(\mathbf{b}_i, \mathbf{b}_j)$ в последней сумме равны нулю при $i \ne j$. Тогда $c_i(\mathbf{b}_i, \mathbf{b}_i) = 0$. Произведение $(\mathbf{b}_i, \mathbf{b}_i)$ не равно нулю, поскольку все векторы $\mathbf{b}_i$ ненулевые, значит, $c_i = 0$. Вектор $\mathbf{b}_i$ был выбран произвольно, следовательно, доказательство справедливо для всех $i$, $1 \le i \le n$. □

Теорема 8.2 (процесс ортогонализации Грама–Шмидта). Пусть $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \in \mathbb{R}^m$, $m \ge n$, — система линейно независимых векторов. Тогда существует такая ортогональная система векторов $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_n^*$, что $\mathbf{b}_1^* = \mathbf{b}_1, \mathbf{b}_2^* = \mathbf{b}_2 + \mathbf{a}_2, \ldots, \mathbf{b}_n^* = \mathbf{b}_n + \mathbf{a}_n$, где каждый вектор $\mathbf{a}_k$, $2 \le k \le n$, представляет собой линейную комбинацию векторов $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}$.

*Доказательство* проведем методом математической индукции.

База индукции: $\mathbf{b}_1^* = \mathbf{b}_1$. Пусть уже построены векторы $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_i^*$, для которых справедливо утверждение теоремы. Будем искать вектор $\mathbf{b}_{i+1}^*$ в виде $\mathbf{b}_{i+1}^* = \mathbf{b}_{i+1} + \mu_{i+1,i}\mathbf{b}_i^* + \mu_{i+1,i-1}\mathbf{b}_{i-1}^* + \ldots + \mu_{i+1,1}\mathbf{b}_1^*$, где числа $\mu_{i+1,j} \in \mathbb{R}$ конкретизируем позже.

Умножим вектор $\mathbf{b}_{i+1}^*$ скалярно на произвольный вектор $\mathbf{b}_s^*$, $1 \le s \le i$:

$$(\mathbf{b}_{i+1}^*, \mathbf{b}_s^*) = (\mathbf{b}_{i+1} + \mu_{i+1,i}\mathbf{b}_i^* + \mu_{i+1,i-1}\mathbf{b}_{i-1}^* + \ldots + \mu_{i+1,1}\mathbf{b}_1^*, \mathbf{b}_s^*) =$$

$$= (\mathbf{b}_{i+1}, \mathbf{b}_s^*) + \mu_{i+1,i}(\mathbf{b}_i^*, \mathbf{b}_s^*) + \ldots + \mu_{i+1,s}(\mathbf{b}_s^*, \mathbf{b}_s^*) + \ldots + \mu_{i+1,1}(\mathbf{b}_1^*, \mathbf{b}_s^*).$$

Векторы $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_i^*$ ортогональны, значит, все слагаемые $\mu_{i+1,j}(\mathbf{b}_j^*, \mathbf{b}_s^*)$, где $1 \le j \le i$, равны нулю при $j \ne s$, откуда

$$(\mathbf{b}_{i+1}^*, \mathbf{b}_s^*) = (\mathbf{b}_{i+1}, \mathbf{b}_s^*) + \mu_{i+1,s}(\mathbf{b}_s^*, \mathbf{b}_s^*) = (\mathbf{b}_{i+1}, \mathbf{b}_s^*) + \mu_{i+1,s}\left\|\mathbf{b}_s^*\right\|^2.$$

Полагая $\mu_{i+1,s} = -\dfrac{(\mathbf{b}_{i+1}, \mathbf{b}_s^*)}{\left\|\mathbf{b}_s^*\right\|^2}$, получаем, что $(\mathbf{b}_{i+1}^*, \mathbf{b}_s^*) = 0$ при $1 \le s \le i$.

Покажем теперь, что вектор $\mathbf{b}_{i+1}^*$ ненулевой. Обозначим $\mathbf{a}_{i+1} = \mu_{i+1,i}\mathbf{b}_i^* + \mu_{i+1,i-1}\mathbf{b}_{i-1}^* + \ldots + \mu_{i+1,1}\mathbf{b}_1^*$ и предположим, что $\mathbf{b}_{i+1}^* = \mathbf{0}$. Тогда вектор $\mathbf{b}_{i+1} = -\mathbf{a}_{i+1}$ представляет собой линейную комбинацию векторов $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i$, а по условию теоремы векторы $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ линейно независимы. Противоречие. □

Алгоритм 8.1. Процесс ортогонализации Грама–Шмидта.

*Вход*. Линейно независимые векторы $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \in \mathbb{R}^m$, $m \ge n$.

*Выход*. Ортогональная система векторов $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_n^*$.

1. Положить $\mathbf{b}_1^* \leftarrow \mathbf{b}_1$, $B_1 \leftarrow \left\|\mathbf{b}_1^*\right\|^2$.
2. Для $i = 2, 3, \ldots, n$ выполнить следующие действия.
   2.1. Положить $\mathbf{b}_i^* \leftarrow \mathbf{b}_i$.
   2.2. Для $j = 1, 2, \ldots, i-1$ вычислить

$$\mu_{i,j} \leftarrow \frac{(\mathbf{b}_i, \mathbf{b}_j^*)}{B_j}, \quad \mathbf{b}_i^* \leftarrow \mathbf{b}_i^* - \mu_{i,j}\mathbf{b}_j^*.$$

   2.3. Положить $B_i \leftarrow \left\|\mathbf{b}_i^*\right\|^2$.
3. Результат: $\{\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_n^*\}$. □

Если точность вычислений составляет $l$ цифр, то сложность алгоритма равна $O(n^3 l^2)$.

Пример 8.1. Применим процесс ортогонализации Грамма–Шмидта к линейно независимым векторам $\mathbf{b}_1 = (1, 0, 0, 5)$, $\mathbf{b}_2 = (0, 1, 0, 5)$, $\mathbf{b}_3 = (0, 0, 1, 5)$.

Полагаем $\mathbf{b}_1^* = \mathbf{b}_1 = (1, 0, 0, 5)$, $B_1 = \|\mathbf{b}_1^*\|^2 = 26$.

Для $i = 2$ полагаем $\mathbf{b}_2^* = \mathbf{b}_2 = (0, 1, 0, 5)$ и вычисляем:

$$\mu_{2,1} = \frac{(\mathbf{b}_2, \mathbf{b}_1^*)}{B_2} = \frac{25}{26}, \quad \mathbf{b}_2^* = \mathbf{b}_2^* - \mu_{2,1}\mathbf{b}_1^* = \left(-\frac{25}{26}, 1, 0, \frac{5}{26}\right), \quad B_2 = \|\mathbf{b}_2^*\|^2 = \frac{51}{26}.$$

Для $i = 3$ полагаем $\mathbf{b}_3^* = \mathbf{b}_3 = (0, 0, 1, 5)$ и вычисляем:

$$\mu_{3,1} = \frac{(\mathbf{b}_3, \mathbf{b}_1^*)}{B_1} = \frac{25}{26}, \quad \mathbf{b}_3^* = \mathbf{b}_3^* - \mu_{3,1}\mathbf{b}_1^* = \left(-\frac{25}{26}, 0, 1, \frac{5}{26}\right),$$

$$\mu_{3,2} = \frac{(\mathbf{b}_3, \mathbf{b}_2^*)}{B_2} = \frac{25}{51}, \quad \mathbf{b}_3^* = \mathbf{b}_3^* - \mu_{3,2}\mathbf{b}_2^* = \left(-\frac{25}{51}, -\frac{25}{51}, 1, \frac{5}{51}\right),$$

$$B_3 = \|\mathbf{b}_3^*\|^2 = \frac{76}{51}.$$

Проверяем, что полученная система $\{\mathbf{b}_1^*, \mathbf{b}_2^*, \mathbf{b}_3^*\}$ ортогональна:

$$(\mathbf{b}_1^*, \mathbf{b}_2^*) = 1 \cdot \left(-\frac{25}{26}\right) + 0 \cdot 1 + 0 \cdot 0 + 5 \cdot \frac{5}{26} = -\frac{25}{26} + \frac{25}{26} = 0,$$

$$(\mathbf{b}_1^*, \mathbf{b}_3^*) = 1 \cdot \left(-\frac{25}{51}\right) + 0 \cdot \left(-\frac{25}{51}\right) + 0 \cdot 1 + 5 \cdot \frac{5}{51} = -\frac{25}{51} + \frac{25}{51} = 0,$$

$$(\mathbf{b}_2^*, \mathbf{b}_3^*) = \left(-\frac{25}{26}\right) \cdot \left(-\frac{25}{51}\right) + 1 \cdot \left(-\frac{25}{51}\right) + 0 \cdot 1 + \frac{5}{26} \cdot \frac{5}{51} = \frac{625 - 650 + 25}{26 \cdot 51} = 0.$$

□

## 8.2. Алгоритм Ленстры–Ленстры–Ловаша и его применение

Определение 8.5. Пусть векторы $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ линейно независимы, $n \le m$. Множество

$$L = L(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n) = \mathbb{Z}\mathbf{b}_1 + \mathbb{Z}\mathbf{b}_2 + \ldots + \mathbb{Z}\mathbf{b}_n$$

всех целочисленных линейных комбинаций векторов $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ называется *решеткой размерности n*. Множество $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ называется *базисом решетки L*.

Решетка является дискретным множеством: в любом ограниченном множестве пространства $\mathbb{R}^m$ содержится лишь конечное число точек решетки.

Решетка может иметь много различных базисов.

Теорема 8.3. Пусть $[\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n]$ — матрица, столбцами которой являются линейно независимые векторы $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \in \mathbb{R}^m$, $n \le m$. Векторы $\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_n \in \mathbb{R}^m$ образуют базис решетки $L(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ тогда и только тогда, когда существует такая матрица $M$ размера $n \times n$ с целыми элементами, $\det M = \pm 1$, что

$$[\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_n]^{\mathrm{T}} = M \cdot [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n]^{\mathrm{T}}. \tag{8.1}$$

*Доказательство.* Пусть $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ и $\{\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_n\}$ — базисы решетки $L(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$. Каждый вектор $\mathbf{d}_i$, $i = 1, 2, \ldots, n$, как вектор решетки можно представить в виде целочисленной линейной комбинации векторов базиса $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$, то есть существует такая матрица $M$ размера $n \times n$ с целыми элементами, что $[\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_n]^{\mathrm{T}} = M \cdot [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n]^{\mathrm{T}}$. Векторы $\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_n$ линейно независимы, поэтому матрица $M$ невырождена, и существует обратная к ней матрица $M^{-1}$: $M^{-1} \cdot [\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_n] = [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n]$.

Поскольку $\{\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_n\}$ — тоже базис, то элементы матрицы $M^{-1}$ — целые числа, значит, определители $\det M$, $\det M^{-1}$ — тоже целые числа, и в силу равенства $\det M \cdot \det M^{-1} = 1$ получаем, что $\det M = \pm 1$.

Обратно, пусть матрица $M$ удовлетворяет условиям теоремы. Из соотношения (8.1) следует, что каждый вектор $\mathbf{d}_i$ можно представить в виде целочисленной линейной комбинации векторов $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$, то есть $\mathbf{d}_i \in L(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$, $i = 1, 2, \ldots, n$. Умножая равенство (8.1) на $M^{-1}$,

получаем $M^{-1}\cdot[\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_n] = [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n]$, то есть $\mathbf{b}_i \in L(\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_n)$, $i = 1, 2, \ldots, n$. Значит, $L(\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_n) = L(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$. □

Определение 8.6. *Определителем* решетки $L(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n) \in \mathbb{R}^m$ называется число

$$d(L) = \sqrt{\det\begin{pmatrix} (\mathbf{b}_1,\mathbf{b}_1) & (\mathbf{b}_1,\mathbf{b}_2) & \ldots & (\mathbf{b}_1,\mathbf{b}_n) \\ (\mathbf{b}_2,\mathbf{b}_1) & (\mathbf{b}_2,\mathbf{b}_2) & \ldots & (\mathbf{b}_2,\mathbf{b}_n) \\ \ldots & \ldots & \ldots & \ldots \\ (\mathbf{b}_n,\mathbf{b}_1) & (\mathbf{b}_n,\mathbf{b}_2) & \ldots & (\mathbf{b}_n,\mathbf{b}_n) \end{pmatrix}}.$$

Из равенства для скалярного произведения векторов $(\mathbf{u}, \mathbf{v}) = \mathbf{u}^{\mathrm{T}}E\mathbf{v}$, где $E$ — единичная матрица, получаем $d(L) = \sqrt{\det(B^{\mathrm{T}}EB)} = \sqrt{\det(B^{\mathrm{T}}B)}$, где $B = [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n]$.

Теорема 8.4. Определитель решетки не зависит от выбора базиса, то есть является инвариантом решетки.

*Доказательство*. Пусть $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$, $\{\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_n\}$ — базисы решетки $L$, и пусть матрица $M$ удовлетворяет условию теоремы 8.3. Обозначим $B = [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n]$, $D = [\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_n]$, то есть $D = BM$. Тогда

$$d(L) = \sqrt{\det((\mathbf{b}_i,\mathbf{b}_j))_{1\le i,j\le n}} = \sqrt{\det(B^{\mathrm{T}}B)} = \sqrt{\det(M^{\mathrm{T}}B^{\mathrm{T}}BM)}$$
$$= \sqrt{\det((BM)^{\mathrm{T}}(BM))} = \sqrt{\det(D^{\mathrm{T}}D)} = \sqrt{\det((\mathbf{d}_i,\mathbf{d}_j))_{1\le i,j\le n}}.$$

□

Имеет место *неравенство Адамара*:

$$d(L) \le \prod_{i=1}^{n} \|\mathbf{b}_i\|.$$

Если $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$ — ортонормированный базис ($\|\mathbf{e}_i\| = 1$ для всех $1 \le i \le n$) и $\mathbf{b}_i = \sum_{j=1}^{n} b_{ij}\mathbf{e}_j$ для $i = 1, 2, \ldots, n$, то $d(L) = \det((b_{ij})_{1\le i,j\le n})$.

Определение 8.7. Пусть $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ — базис решетки $L$. *Фундаментальным параллелепипедом* решетки $L$ называется множество

$$\left\{\sum_{i=1}^{n} t_i \mathbf{b}_i \,\middle|\, 0 \le t_1, t_2, \ldots, t_n < 1\right\}.$$

Пример 8.2 [2]. Рассмотрим двумерную решетку, заданную точками с целочисленными координатами в декартовой системе координат на плоскости. Фундаментальный параллелепипед (параллелограмм) образуют любые четыре точки этой решетки, кроме своих вершин не содержащие ни внутри себя, ни на сторонах никаких других точек решетки (рис. 8.1).

Обозначим $f(r)$ точек решетки, расположенных внутри круга радиуса $r$ с центром в точке решетки, где $r$ — целое число. Каждой точке решетки сопоставим *фундаментальный квадрат*, для которого эта точка является левой нижней вершиной. Площадь каждого квадрата равна 1, поэтому $f(r)$ есть сумма площадей всех тех квадратов, у которых левая нижняя вершина лежит внутри или на границе круга (рис. 8.2).

Таким образом, $f(r)$ отличается от площади $\pi r^2$ круга радиуса $r$ не более чем на величину площади $A(r)$ квадратов, пересекаемых окружностью:

$$|f(r) - \pi r^2| \le A(r).$$

Перепишем это равенство:

$$\left|\frac{f(r)}{r^2} - \pi\right| \le \frac{A(r)}{r^2}$$

и оценим величину $A(r)$. Наибольшее расстояние между двумя точками фундаментального квадрата равно $\sqrt{2}$. Следовательно, все квадраты, пересекаемые окружностью, расположены в круговом кольце ширины $2\sqrt{2}$, внешний и внутренний радиусы которого равны, соответственно, $r+\sqrt{2}$ и $r-\sqrt{2}$ (рис. 8.3). Площадь этого кругового кольца равна:

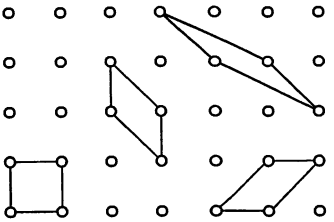


*Рис. 8.1. Двумерная квадратная решетка*

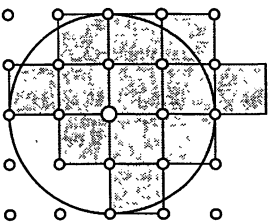


*Рис. 8.2. Вычисление f(r) через сумму площадей единичных квадратов*

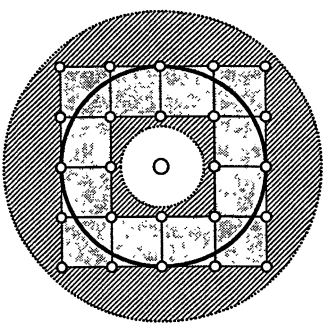


*Рис. 8.3. Квадраты, пересекаемые окружностью радиуса r*

$$B(r)=\left\{(r+\sqrt{2})^2-(r-\sqrt{2})^2\right\}\pi=4\sqrt{2}\pi r.$$

Тогда

$$\left|\frac{f(r)}{r^2}-\pi\right|\le\frac{A(r)}{r^2}<\frac{B(r)}{r^2}=\frac{4\sqrt{2}\pi}{r}.$$

Переходя в этом неравенстве к пределу при $r\to\infty$, получаем:

$$\lim_{r\to\infty}\frac{f(r)}{r^2}=\pi. \tag{8.2}$$

Отсюда следует, что площадь любого фундаментального параллелограмма равна 1. Действительно, каждой точке решетки, попавшей в круг, сопоставим одним и тем же способом параллелограмм, для которого она служит вершиной, и сравним суммарную площадь $S$ этих параллелограммов с площадью круга. Здесь опять разность между обеими площадями меньше площади $B_c(r)$ кругового кольца, внешний и внутренний радиусы которого равны $r+c$ и $r-c$, где $c$ — наибольшее расстояние (не зависящее от $r$) между двумя точками фундаментального параллелограмма. Если площадь фундаментального параллелограмма равна $a$, то площадь $S$ равна $af(r)$. Тогда

$$|af(r)-\pi r^2|<B_c(r)=4\pi rc,$$

$$\left|\frac{af(r)}{r^2}-\pi\right|<\frac{4\pi c}{r},$$

$$\lim_{r\to\infty}\frac{f(r)}{r^2}=\frac{\pi}{a}.$$

Отсюда, в силу формулы (8.2), $a=1$.

Для каждой двумерной решетки, образованной из фундаментального параллелограмма площади $a^2$, наименьшее расстояние $d$ между двумя точками решетки есть характеристическая величина, имеет место неравенство

$$D \le a\sqrt{\frac{2}{\sqrt{3}}},$$

причем равенство достигается тогда и только тогда, когда фундаментальный параллелограмм составлен из двух равносторонних треугольников. Это означает, что при данном наименьшем расстоянии эта решетка имеет фундаментальный параллелограмм наименьшей возможной площади. Таким образом, из всех решеток, расположенных внутри некоторой заданной плоской фигуры и имеющих заданное наименьшее расстояние, решетка, составленная из равносторонних треугольников, дает наибольшее число точек. □

Пусть $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ — базис решетки $L \subset \mathbb{R}^m$ и пусть числа $\mu_{i,j}$, $1 \le j < i \le n$, и векторы $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_n^*$ получены в результате процесса ортогонализации Грама–Шмидта.

Определение 8.8. Базис $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ называется *LLL-приведенным* (*приведенным по Ловашу*), если этот базис приведен по норме и

$$\|\mathbf{b}_i^*\|^2 \ge \left(\frac{3}{4} - \mu_{i,i-1}^2\right)\|\mathbf{b}_{i-1}^*\|^2,\ 1 < i \le m. \tag{8.3}$$

Рассмотрим основные свойства LLL-приведенного базиса.

Лемма 8.5. Если $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ — LLL-приведенный базис решетки $L \subset \mathbb{R}^m$, то для всех $1 \le j < i \le n$ выполняется неравенство

$$\|\mathbf{b}_j^*\|^2 \le 2^{i-j}\|\mathbf{b}_i^*\|^2.$$

*Доказательство*. Из определения LLL-приведенного базиса имеем:

$$\frac{3}{4}\|\mathbf{b}_j^*\|^2 \le \|\mathbf{b}_{j+1}^*\|^2 + \mu_{j+1,j}^2\|\mathbf{b}_j^*\|^2 \le \|\mathbf{b}_{j+1}^*\|^2 + \frac{1}{4}\|\mathbf{b}_j^*\|^2,$$

то есть $\|\mathbf{b}_j^*\|^2 \le 2\|\mathbf{b}_{j+1}^*\|^2$. Далее по индукции: из неравенства $\|\mathbf{b}_j^*\|^2 \le 2^{i-j}\|\mathbf{b}_i^*\|^2$ получаем $2^{i+1-j}\|\mathbf{b}_{i+1}^*\|^2 \ge 2^{i-j}\|\mathbf{b}_i^*\|^2 \ge \|\mathbf{b}_j^*\|^2$. □

Замечание. При $j = 1$ получаем

$$\|\mathbf{b}_1^*\|^2 \le 2^{i-1}\|\mathbf{b}_i^*\|^2, \quad 1 \le i \le n. \tag{8.4}$$

Теорема 8.6. Для LLL-приведенного базиса $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ решетки $L \subset \mathbb{R}^m$ справедливы следующие утверждения.

1. $\|\mathbf{b}_i\|^2 \le 2^{j-1}\|\mathbf{b}_j^*\|^2$ для всех $1 \le i < j \le n$.

2. $d(L) \le \prod_{i=1}^{n}\|\mathbf{b}_i\| \le 2^{\frac{n(n-1)}{4}} d(L)$.

3. $\|\mathbf{b}_1\|^2 \le 2^{\frac{n-1}{4}} \sqrt[n]{d(L)}$.

*Доказательство*. Для LLL-приведенного базиса по лемме 8.5 получаем для $i = 1, 2, \ldots, n$

$$\|\mathbf{b}_i\|^2 \le \|\mathbf{b}_i^*\|^2\left(1 + \frac{1}{4}\sum_{j=1}^{i-1} 2^{i-j}\right) = \|\mathbf{b}_i^*\|^2 \cdot \left(2^{i-2} + \frac{1}{2}\right) \le 2^{i-1}\|\mathbf{b}_i^*\|^2.$$

Снова воспользуемся леммой 8.5:

$$\|\mathbf{b}_i\|^2 \le 2^{i-1}\|\mathbf{b}_i^*\|^2 \le 2^{i-1} \cdot 2^{j-i}\|\mathbf{b}_j^*\|^2 = 2^{j-1}\|\mathbf{b}_j^*\|^2$$

для всех $1 \le i < j \le n$.

Докажем второе утверждение. Из доказательства теоремы 8.4 следует, что

$$d(L) = \sqrt{\det((\mathbf{b}_i^*, \mathbf{b}_j^*))_{1 \le i, j \le n}} = \prod_{i=1}^{n}\|\mathbf{b}_i^*\|^2.$$

Тогда

$$\|\mathbf{b}_1\|\cdot\|\mathbf{b}_2\|\cdot\ldots\cdot\|\mathbf{b}_n\| \le 2^{\frac{1-1}{2}}\|\mathbf{b}_1^*\|\cdot 2^{\frac{2-1}{2}}\|\mathbf{b}_2^*\|\cdot\ldots\cdot 2^{\frac{n-1}{2}}\|\mathbf{b}_n^*\| = 2^{\frac{n(n-1)}{4}}\prod_{i=1}^{n}\|\mathbf{b}_i^*\| = 2^{\frac{n(n-1)}{4}}d(L).$$

Из замечания к лемме 8.5 следует, что

$$\|\mathbf{b}_1\|^{2n} \le 2^0\|\mathbf{b}_1^*\|^2\cdot 2^1\|\mathbf{b}_2^*\|^2\cdot\ldots\cdot 2^{n-1}\|\mathbf{b}_n^*\|^2 = 2^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}\|\mathbf{b}_i^*\|^2 = 2^{\frac{n(n-1)}{2}}d(L)^2,$$

откуда получаем третье утверждение теоремы. □

Покажем, что в LLL-приведенном базисе вектор $\mathbf{b}_1$ — один из самых коротких.

Теорема 8.7. Для LLL-приведенного базиса $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ решетки $L$ и любого ненулевого вектора $\mathbf{x} \in L$ справедливо неравенство $\|\mathbf{b}_1\| \le 2^{\frac{n-1}{2}}\|\mathbf{x}\|$.

*Доказательство.* Разложим ненулевой вектор $\mathbf{x}$ решетки $L$ по базису $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$: $\mathbf{x} = \sum_{i=1}^{n} r_i\mathbf{b}_i$, где $r_i \in \mathbb{Z}$. Можно записать $\mathbf{x} = \sum_{i=1}^{n} r_i^*\mathbf{b}_i^*$, где $r_i^* \in \mathbb{R}$. Если $i_0$ — максимальный номер, для которого $r_i \ne 0$, то $r_{i_0}^* = r_{i_0}$. Поэтому

$$\|\mathbf{x}\|^2 = \sum_{i=1}^{n}(r_i^*)^2\|\mathbf{b}_i^*\|^2 \ge (r_{i_0}^*)^2\|\mathbf{b}_{i_0}^*\|^2 \ge \|\mathbf{b}_{i_0}^*\|^2.$$

Из неравенства (8.4) имеем $\|\mathbf{b}_1\|^2 \le 2^{i_0-1}\|\mathbf{b}_{i_0}^*\|^2$. Следовательно,

$$\|\mathbf{x}\|^2 \ge \frac{1}{2^{i_0-1}}\|\mathbf{b}_1\|^2 \ge \frac{1}{2^{n-1}}\|\mathbf{b}_1\|^2.$$ □

Теорема 8.8. LLL-приведенный базис $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ решетки $L$ является минимальным в том смысле, что для любых линейно независимых векторов $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_t$ решетки $L$ для всех $1 \le i \le t$ выполняется неравенство

$$\|\mathbf{b}_i\| \le 2^{\frac{n-1}{2}} \max_{1\le j\le t} \|\mathbf{x}_j\|.$$

*Доказательство* [1]. Каждый из векторов $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_t$ представим в виде линейной комбинации векторов базиса:

$$\mathbf{x}_i = \sum_{j=1}^{n} r_{ij}\mathbf{b}_j,$$

где $r_{ij} \in \mathbb{Z}$, $1 \le i \le t$.

Обозначая $j_0(i)$ наибольший номер $j$, для которого $r_{ij} \ne 0$, и проводя рассуждения аналогично доказательству предыдущей теоремы, получаем $\|\mathbf{x}_i\|^2 \ge \|\mathbf{b}^*_{j_0(i)}\|^2$, $1 \le i \le t$.

Упорядочим векторы $\mathbf{b}^*_j$ так, чтобы $j_0(1) \le j_0(2) \le \ldots \le j_0(t)$. Тогда $j_0(i) \ge i$ для всех $1 \le i \le t$. Действительно, если найдется номер $i$, для которого $j_0(i) < i$, то каждый из векторов $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_t$ можно представить в виде линейной комбинации векторов $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{j_0(i)}$, что противоречит линейной независимости векторов $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_t$.

Воспользовавшись утверждением 1 теоремы 8.6, получаем

$$\|\mathbf{b}_i\|^2 \le 2^{j_0(i)-1}\|\mathbf{b}^*_{j_0(i)}\|^2 \le 2^{n-1}\|\mathbf{x}_i\|^2. \qquad \square$$

Алгоритм Ленстры–Ленстры–Ловаша, называемый также LLL-алгоритмом или $L^3$-алгоритмом, по данному базису находит LLL-приведенный базис решетки.

Алгоритм 8.2. Алгоритм Ленстры–Ленстры–Ловаша [6].

*Вход*. Базис $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ решетки в $\mathbb{R}^m$, $m \ge n$.

*Выход*. LLL-Приведенный базис решетки.

1. Алгоритмом 8.1 выполнить процесс ортогонализации Грама–Шмидта для векторов $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$.
2. Положить $k \leftarrow 2$.

3. При $|\mu_{k,k-1}| > \frac{1}{2}$ выполнить следующие действия.

3.1. При $\mu_{k,k-1} > 0$ вычислить $r \leftarrow \left[\frac{1}{2} + \mu_{k,k-1}\right]$. В противном случае вычислить $r \leftarrow -\left[\frac{1}{2} - \mu_{k,k-1}\right]$.

3.2. Положить $\mathbf{b}_k \leftarrow \mathbf{b}_k - r\mathbf{b}_{k-1}$.

3.3. Для $j = 1, 2, \ldots, k-2$ вычислить $\mu_{k,j} \leftarrow \mu_{k,j} - r\mu_{k-1,j}$.

3.4. Положить $\mu_{k,k-1} \leftarrow \mu_{k,k-1} - r$.

4. При $B_k < \left(\frac{3}{4} - \mu_{k,k-1}^2\right) B_{k-1}$ выполнить:

4.1. Положить $\mu \leftarrow \mu_{k,k-1}$, $B \leftarrow B_k + \mu^2 B_{k-1}$, $\mu_{k,k-1} \leftarrow \frac{\mu B_{k-1}}{B}$, $B_k \leftarrow \frac{B_{k-1} B_k}{B}$, $B_{k-1} \leftarrow B$.

4.2. Поменять местами векторы $\mathbf{b}_k$ и $\mathbf{b}_{k-1}$.

4.3. При $k > 2$ поменять местами коэффициенты $\mu_{k,j}$ и $\mu_{k-1,j}$ для $j = 1, 2, \ldots, k-2$.

4.4. Для $s = k+1, k+2, \ldots, n$ положить $t \leftarrow \mu_{s,k}$, $\mu_{s,k} \leftarrow \mu_{s,k-1} - \mu t$, $\mu_{s,k-1} \leftarrow t + \mu_{k,k-1}\mu_{s,k}$.

4.5. Положить $k \leftarrow \max(2, k-1)$ и вернуться на шаг 3.

5. При $B_k \geq \left(\frac{3}{4} - \mu_{k,k-1}^2\right) B_{k-1}$ выполнить:

5.1. Для $l = k-2, k-3, \ldots, 1$ при $|\mu_{k,l}| > \frac{1}{2}$ выполнить:

5.1.1. При $\mu_{k,l} > 0$ вычислить $r \leftarrow \left[\frac{1}{2} + \mu_{k,l}\right]$. В противном случае вычислить $r \leftarrow -\left[\frac{1}{2} - \mu_{k,l}\right]$.

5.1.2. Положить $\mathbf{b}_k \leftarrow \mathbf{b}_k - r\mathbf{b}_l$.

5.1.3. Для $j = 1, 2, \ldots, l-1$ положить $\mu_{k,j} \leftarrow \mu_{k,j} - r\mu_{l,j}$.

5.1.4. Положить $\mu_{k,l} \leftarrow \mu_{k,l} - r$.

5.2. Положить $k \leftarrow k + 1$.

6. Если $k \le n$, то вернуться на шаг 3.

7. Результат: $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$. □

Покажем, что алгоритм заканчивает работу. Обозначим $\Delta_i = \det((\mathbf{b}_j, \mathbf{b}_l))_{1 \le j,l \le i}$, $i = 1, 2, \ldots, n$. Справедливо соотношение

$$\Delta_i = \det([\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i] \cdot [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i]^{\mathrm{T}}) = \det([\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i])^2 =$$

$$= \det([\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_i^*])^2 = \det([\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_i^*] \cdot [\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_i^*]^{\mathrm{T}}) = \prod_{j=1}^{i} \left\|\mathbf{b}_j^*\right\|^2 .$$

На шаге 4 при данном значении $k$ значение $\Delta_k$ уменьшается более чем в $\frac{3}{4}$ раз — так же, как значение $B_k = \left\|\mathbf{b}_k^*\right\|^2$. Величины $\Delta_k$ ограничены снизу положительным числом $\delta(L)$ — квадратом нормы кратчайшего ненулевого вектора решетки:

$$\Delta_k \ge \delta(L) \cdot (4/3)^{\frac{i(i-1)}{2}} .$$

Поэтому шаг 4 выполняется конечное число раз, и алгоритм заканчивает работу.

Если $L \subset \mathbb{Z}^n$ — решетка с базисом $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ и $\|\mathbf{b}_i\|^2 \le d^i$, $1 \le i \le n$, для системы счисления с основанием $d$, то сложность алгоритма LLL равна $O(n^4 l^2)$ арифметических операций.

Пример 8.3. Приведем базис $\{\mathbf{b}_1, \mathbf{b}_2\} = \{(2, 1), (3, 2)\}$ решетки $L \subset \mathbb{R}^2$. Результатом процесса ортогонализации будут значения

$$\mathbf{b}_1^* = (2, 1); \ \mu_{2,1} = \frac{8}{5}; \ \mathbf{b}_2^* = \left(-\frac{1}{5}, \frac{2}{5}\right)^{\mathrm{T}} .$$

На шаге 3 преобразуем коэффициент $\mu_{2,1}$ так, чтобы выполнялось условие (8.3), и изменяем вектор $\mathbf{b}_2$: $\mu_{2,1} = -\frac{2}{5}$; $\mathbf{b}_2 = (-1, 0)^{\mathrm{T}}$.

Для $B_1$ и $B_2$ выполняется условие шага 4, поэтому вычисляем:

$$\mu = \mu_{2,1} = -\frac{2}{5};\ B = B_2 + \mu^2 B_1 = 1;\ \mu_{2,1} = \frac{\mu B_1}{B} = -2;\ B_2 = \frac{B_1 B_2}{B} = 1;\ B_1 = 1.$$

Меняем местами векторы $\mathbf{b}_2$ и $\mathbf{b}_1$: $\mathbf{b}_2 = (2, 1)$; $\mathbf{b}_1 = (-1, 0)$ и, выполняя шаг 3 для $k = 2$, получаем $\mu_{2,1} = 0$. Теперь выполняется условие шага 5 для $k = 2$. Полагаем $k = k + 1 = 3$, и алгоритм заканчивает работу с результатом $\mathbf{b}_1 = (-1, 0)$; $\mathbf{b}_2 = (0, 1)$ (рис. 8.4 на стр. 272). □

Пример 8.4. Пусть $n = 3$ и базис решетки задан векторами $\mathbf{b}_1 = (1, 0, 1, 2)$, $\mathbf{b}_2 = (1, -1, 2, 0)$, $\mathbf{b}_3 = (-1, 2, 0, 1)$.

Результатом процесса ортогонализации будут значения

$$\begin{aligned}
&\mathbf{b}_1^* = (1, 0, 1, 2), && B_1 = 6; \\
&\mathbf{b}_2^* = (1, -1, 2, 0), && \mu_{2,1} = \frac{1}{2}, \quad \mathbf{b}_2^* = \left(\frac{1}{2}, -1, \frac{3}{2}, -1\right), \quad B_2 = \frac{9}{2}; \\
&\mathbf{b}_3^* = (-1, 2, 0, 1), && \mu_{3,1} = \frac{1}{6}, \quad \mathbf{b}_3^* = \left(-\frac{7}{6}, 2, -\frac{1}{6}, \frac{2}{3}\right), \\
& && \mu_{3,2} = -\frac{7}{9}, \quad \mathbf{b}_3^* = \left(-\frac{7}{9}, \frac{11}{9}, 1, -\frac{1}{9}\right), \quad B_3 = \frac{28}{9}.
\end{aligned}$$

Для $k = 2$ выполняется условие шага 5, поэтому полагаем $k = k + 1 = 3$ и переходим на шаг 3.

Минимизируем коэффициент $\mu_{3,2}$:

$$r = -1,\ \mathbf{b}_3 = (0, 1, 2, 1),\ \mu_{3,1} = \frac{2}{3},\ \mu_{3,2} = \frac{2}{9}.$$

Для $k = 3$ выполняется условие шага 4. Вычисляем

$$\mu = \mu_{3,2} = \frac{2}{9},\ B = \frac{10}{3},\ \mu_{3,2} = \frac{3}{10},\ B_3 = \frac{21}{5},\ B_2 = \frac{10}{3}.$$

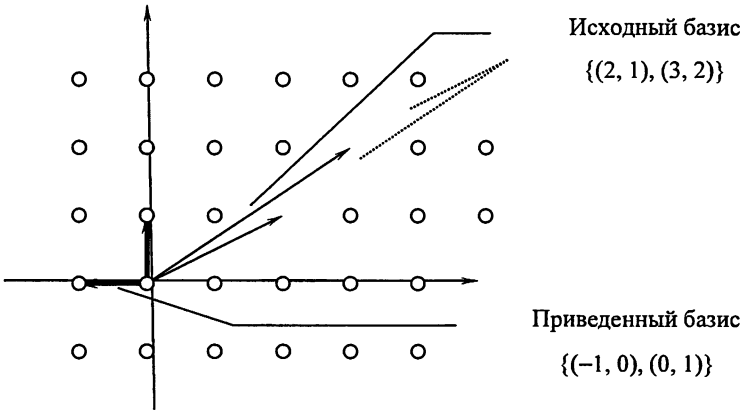



***Рис. 8.4.*** *Приведенный базис двумерной решетки*

Полагаем $\mathbf{b}_2 = (0, 1, 2, 1)$, $\mathbf{b}_3 = (1, -1, 2, 0)$, $\mu_{3,1} = \frac{1}{2}$, $\mu_{2,1} = \frac{2}{3}$, $k = 2$ и переходим на шаг 3.

Минимизируем коэффициент $\mu_{2,1}$: $r = 1$, $\mathbf{b}_2 = (-1, 1, 1, -1)$, $\mu_{2,1} = -\frac{1}{3}$.

Выполняется условие шага 4, поэтому полагаем

$$\mu = \mu_{2,1} = -\frac{1}{3},\ B = 4,\ \mu_{2,1} = -\frac{1}{2},\ B_2 = 5,\ B_1 = 4.$$

Меняем местами $\mathbf{b}_1$ и $\mathbf{b}_2$: $\mathbf{b}_1 = (-1, 1, 1, -1)$, $\mathbf{b}_2 = (1, 0, 1, 2)$.

На шаге 4.4 для $s = 3$ вычисляем $t = \mu_{3,2} = \frac{3}{10}$, $\mu_{3,2} = \frac{3}{5}$, $\mu_{3,1} = 0$, затем полагаем $k = 2$.

Выполняется условие шага 5, поэтому полагаем $k = 3$ и переходим на шаг 3.

Минимизируем коэффициент $\mu_{3,2}$:

$$r = 1,\ \mathbf{b}_3 = (0, -1, 1, -2),\ \mu_{3,1} = \frac{1}{2},\ \mu_{3,2} = -\frac{2}{5}.$$

Снова выполняется условие шага 5, поэтому полагаем $k = 4$ и получаем результат: $\mathbf{b}_1 = (-1, 1, 1, -1)$, $\mathbf{b}_2 = (1, 0, 1, 2)$, $\mathbf{b}_3 = (0, -1, 1, -2)$. □

## 8.3. Задача об укладке ранца

Определение 8.9. *Задача об укладке ранца* (задача о рюкзаке) формулируется следующим образом: имеется $n$ предметов, каждый из которых обладает массой $m_i$, объемом $v_i$, ценой $c_i$ и численной оценкой полезности в походе $p_i$, где $i = 1, 2, \ldots, n$. Турист составляет набор предметов с номерами $i_1, i_2, \ldots, i_k$ (число $k$ не фиксировано) так, чтобы их суммарная масса и объем не превосходили заданных границ (веса $M$, который может нести турист, и объема его рюкзака $V$):

$$m_{i_1} + m_{i_2} + \ldots + m_{i_k} \le M;\quad v_{i_1} + v_{i_2} + \ldots + v_{i_k} \le V,$$

суммарная цена $c_{i_1}+c_{i_2}+\ldots+c_{i_k}$ была бы наименьшей, а суммарная полезность $p_{i_1}+p_{i_2}+\ldots+p_{i_k}$ по возможности наибольшей.

В 1978 году Р. Меркль (R. Merkle) предложил для построения криптосистем с открытым ключом использовать следующую частную задачу об укладке ранца: для данного множества $\{a_1, a_2, \ldots, a_n\}$, $a_i \in \mathbb{N}$, и данного натурального числа $S$ найти такой вектор $\mathbf{x}=(x_1, x_2, \ldots, x_n)$, где $x_i \in \{0, 1\}$, что $\sum_{i=1}^{n} x_i a_i = S$ (если такой вектор существует). Число $\dfrac{n}{\max\limits_{1\le i\le n}(\log_2 a_i)}$ называется *плотностью ранца*.

Эту задачу иногда называют *аддитивной*, в отличие от *мультипликативной задачи об укладке ранца*: для данного множества $\{a_1, a_2, \ldots, a_n\}$, $a_i \in \mathbb{N}$, и данного натурального числа $P$ найти такой вектор $\mathbf{x}=(x_1, x_2, \ldots, x_n)$, где $x_i \in \{0, 1\}$, что $\prod_{i=1}^{n} a_i^{x_i} = P$ (если такой вектор существует).

### 8.3.1. Способы решения

Задачу об укладке ранца можно решать, например, методом встречи посередине (см. п. 7.1.3).

Алгоритм 8.3. Решение задачи об укладке ранца методом встречи посередине [6].

*Вход*. Множество $\{a_1, a_2, \ldots, a_n\}$, $a_i \in \mathbb{N}$; натуральное число $S$.

*Выход*. Вектор $\mathbf{x}=(x_1, x_2, \ldots, x_n)$, $x_i \in \{0, 1\}$, для которого $\sum_{i=1}^{n} x_i a_i = S$ (если такой вектор существует).

1. Положить $t \leftarrow \left[\dfrac{n}{2}\right]$.

2. Построить базу данных с элементами вида $((x_1, x_2, \ldots, x_t), \sum_{i=1}^{t} a_i x_i)$, где $(x_1, x_2, \ldots, x_t)$ — случайные двоичные векторы, и отсортировать ее по второй «координате».

3. Выбрать случайный двоичный вектор $(x_{t+1}, x_{t+2}, \ldots, x_n)$.

   3.1. Положить $l \leftarrow S - \sum_{i=t+1}^{n} a_i x_i$.

   3.2. Если $l$ является второй «координатой» какого-нибудь элемента базы данных, то результат: $(x_1, x_2, \ldots, x_n)$.

4. Результат: решений нет. □

Сложность алгоритма равна $O(n \cdot 2^{n/2})$, поэтому данный алгоритм на практике не используется.

В настоящее время наиболее эффективным является алгоритм, сводящий решение задачи об укладке ранца к поиску вектора малой длины в решетке размерности $n + 1$.

Алгоритм 8.4. Решение задачи об укладке ранца с использованием LLL-алгоритма [6].

*Вход*. Множество $\{a_1, a_2, \ldots, a_n\}$, $a_i \in \mathbb{N}$, натуральное число $S$.

*Выход*. Вектор $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $x_i \in \{0, 1\}$, для которого $\sum_{i=1}^{n} x_i a_i = S$ (если такой вектор существует).

1. Положить $m \leftarrow \left\lceil \frac{1}{2}\sqrt{n} \right\rceil$, где через $\lceil x \rceil$ обозначено наименьшее целое число, не меньшее $x$.

2. LLL-Алгоритмом найти приведенный базис по базису решетки из $\mathbb{Z}^{n+1}$, задаваемому строками матрицы

$$C = \begin{pmatrix} 1 & 0 & \dots & 0 & ma_1 \\ 0 & 1 & \dots & 0 & ma_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & ma_n \\ \frac{1}{2} & \frac{1}{2} & \dots & \frac{1}{2} & mS \end{pmatrix}.$$

3. Для каждого вектора $\mathbf{b} = (b_1, b_2, \dots, b_{n+1})$ приведенного базиса, для которого $b_{n+1} = 0$ и $b_i \in \left\{-\frac{1}{2}, \frac{1}{2}\right\}$ при $i = 1, 2, \dots, n$, выполнить:

   3.1. Положить $x_i \leftarrow b_i + \frac{1}{2}$ для $i = 1, 2, \dots, n$.

   Если $\sum_{i=1}^{n} x_i a_i = S$, то результат: $(x_1, x_2, \dots, x_n)$.

   3.2. Положить $x_i \leftarrow -b_i + \frac{1}{2}$ для $i = 1, 2, \dots, n$.

   Если $\sum_{i=1}^{n} x_i a_i = S$, то результат: $(x_1, x_2, \dots, x_n)$.

4. Результат: решений нет. □

Пусть вектор $\mathbf{c}_i \in C$ является элементом базиса решетки $L$ и вектор $(x_1, x_2, \dots, x_n)$ удовлетворяет условию $\sum_{i=1}^{n} x_i a_i = S$. Рассмотрим вектор $\mathbf{b} = (b_1, b_2, \dots, b_{n+1}) = \left(\sum_{i=1}^{n} x_i \mathbf{c}_i\right) - \mathbf{c}_{n+1}$. Этот вектор принадлежит решетке $L$, его координаты удовлетворяют условиям $b_{n+1} = 0$ и $b_i \in \left\{-\frac{1}{2}, \frac{1}{2}\right\}$ для $i = 1, 2, \dots, n$, и $\|\mathbf{b}\| = \sqrt{b_1^2 + b_2^2 + \dots + b_{n+1}^2} = \sqrt{\frac{n}{4} + 0} = \frac{\sqrt{n}}{2}$. Если плотность ранца мала (числа $a_i$ велики), то большинство векторов решетки $L$ будут иметь относительно большие длины. Таким образом, вектор $\mathbf{b}$ будет с большой вероятностью самым коротким ненулевым вектором решетки.

Если плотность ранца не превосходит 0,9408, то алгоритм 8.4 решает задачу об укладке ранца с вероятностью, близкой к 1.

Пример 8.5. Пусть ранец задан набором чисел {12, 11, 10, 9, 33, 44, 55, 66} и $S = 100$.

Полагаем $m = \left\lceil \frac{1}{2}\sqrt{8} \right\rceil = 2$ и строим базис:

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 24 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 22 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 20 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 18 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 66 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 88 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 110 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 132 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 200 \end{pmatrix}.$$

LLL-приведенный базис имеет вид

$$B = \begin{pmatrix} -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{3}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & -1 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ -\frac{1}{2} & -\frac{1}{2} & \frac{3}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{3}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -2 \end{pmatrix}.$$

В качестве решения задачи об укладке ранца можно взять один из двух векторов:

$\mathbf{x} = (1, 0, 0, 0, 1, 0, 1, 0)$, получаемый при выполнении шага 3 для вектора $\mathbf{b}_1$ (проверка: $12 + 33 + 55 = 100$);

$\mathbf{x} = (1, 1, 0, 0, 1, 1, 0, 0)$, получаемый при выполнении шага 3 для вектора $\mathbf{b}_4$ (проверка: $12 + 11 + 33 + 44\} = 100$). □

### 8.3.2. Ранцевые алгоритмы шифрования с открытым ключом

Определение 8.10. Назовем последовательность $\{b_1, \ldots, b_n\}$, где $b_i \in \mathbb{Z}$, *сверхвозрастающей*, если $b_k > \sum_{i=1}^{k-1} b_i$ для всех $k \le n$. Для сверхвозрастающей последовательности задача об укладке ранца решается однозначно с линейной сложностью. Для этого число $s$ сравниваем с $b_n$. Если $s \ge b_n$, то полагаем $x_n = 1$, в противном случае полагаем $x_n = 0$. Далее находим $s - b_n x_n$, переходим к слагаемому с номером $n - 1$ и т. д.

Пример 8.6. Пусть $\{b_1, b_2, b_3, b_4, b_5\} = \{171, 196, 459, 1191, 2410\}$ и $s = 4060$. Найдем двоичные коэффициенты $y_1, \ldots, y_5$, для которых $s = \sum_{i=1}^{n} y_i b_i$. Тогда $y_5 = 1$, так как при $y_5 = 0$, даже если $y_1 = y_2 = y_3 = y_4 = 1$, сумма первых четырех элементов будет равна $2017 < s$. Теперь нужно представить разность $s - y_5 b_5 = 1650$ в виде линейной комбинации первых четырех элементов. Так как $1650 > b_4 = 1191$, то элемент $y_4$ также должен быть равен 1. Далее, $1650 - y_4 b_4 = 459 = b_3$, откуда $y_3 = 1, y_2 = y_1 = 0$. □

В случае если компоненты $b_i$ представляют собой числа 1, 2, 4, 8, …, то решение задачи сводится к переводу десятичного числа $s$ в двоичную систему счисления.

Для построения шифра на основе сверхвозрастающей последовательности Р. Меркль и М. Хеллман предложили «замаскировать» эту последовательность с помощью линейного преобразования [7].

Алгоритм 8.5. Генерация ключа для протокола Меркля–Хеллмана.

*Вход*. Длина блока $n$.

*Выход*. Открытый и секретный ключи.

1. Выбрать сверхвозрастающую последовательность из $n$ натуральных чисел: $\{b_1, \ldots, b_n\}$.
2. Выбрать целое число $u > b_1 + \ldots + b_n$.
3. Выбрать случайное число $v$, взаимно простое с $u$.
4. Выбрать случайную перестановку $\psi$ чисел $1, 2, \ldots, n$.
5. Замаскировать сверхвозрастающую последовательность, для этого вычислить последовательность $\{a_1, \ldots, a_n\}$ вида $a_i \leftarrow vb_{\psi(i)} \pmod u$.
6. Результат: $\{a_1, \ldots, a_n\}$ — открытый ключ; $(\psi, v, u, \{b_1, \ldots, b_n\})$ — секретный ключ. □

Пример 8.7. Пусть последовательность $\{b_i\}$ — как выше. Сумма элементов этой последовательности равна 4427. В качестве $u$ выберем наименьшее простое число, большее 4427, — $u = 4441$. Число $v$ может быть любым, не делящимся на $u$: полагаем $v = 5522$. Пусть $\psi$: $(1, 2, 3, 4, 5) \to (3, 5, 2, 1, 4)$. Тогда открытым ключом будет:

$$a_1 = v \cdot b_{\psi(1)} = v \cdot b_3 = 5522 \cdot 459 \equiv 3228 \pmod{4441},$$

$$a_2 = v \cdot b_{\psi(2)} = v \cdot b_5 = 5522 \cdot 2410 \equiv 2784 \pmod{4441},$$

$$a_3 = v \cdot b_{\psi(3)} = v \cdot b_2 = 5522 \cdot 196 \equiv 3149 \pmod{4441},$$

$$a_4 = v \cdot b_{\psi(4)} = v \cdot b_1 = 5522 \cdot 171 \equiv 2770 \pmod{4441},$$

$$a_5 = v \cdot b_{\psi(5)} = v \cdot b_4 = 5522 \cdot 1191 \equiv 4022 \pmod{4441}$$

— эта последовательность маскирует сверхвозрастающую структуру последовательности $\{b_i\}$. □

Алгоритм 8.6. Протокол Меркля–Хеллмана.

*Вход отправителя.* Открытый ключ $\{a_1, \ldots, a_n\}$ из алгоритма 8.5.

*Вход получателя.* Секретный ключ $(\psi, v, u, \{b_1, \ldots, b_n\})$ из алгоритма 8.5.

*Результат.* Зашифрование и расшифрование сообщения.

Для зашифрования сообщения длины $n$ бит, представленного в виде двоичного вектора $(m_1, \ldots, m_n)$, отправитель вычисляет шифртекст $c \leftarrow \sum_{i=1}^{n} m_i a_i$.

Для расшифрования шифртекста получатель выполняет следующие действия.

1. Вычисляет $s \leftarrow cv^{-1} \pmod u$.
2. Решает задачу об укладке ранца для сверхвозрастающей последовательности: представляет число $s$ в виде линейной комбинации элементов $b_i$: $s = y_1 b_1 + \ldots + y_n b_n$.
3. Вычисляет вектор $(m_1, \ldots, m_n)$, где $m_i \leftarrow y_{\psi(i)}$. □

Расшифрование корректно, поскольку выполняется соотношение

$$s \equiv cv^{-1} \equiv \sum_{i=1}^{n} m_i a_i v^{-1} \equiv \sum_{i=1}^{n} m_i b_{\psi(i)} \pmod u.$$

Пример 8.8. Пусть пользователь $A$ хочет передать сообщение (1, 1, 0, 0, 1) пользователю $B$, открытый и секретный ключи которого выработаны в примере 8.7. Шифртекстом, соответствующим этому сообщению, будет

$$c = 1 \cdot 3228 + 1 \cdot 2784 + 0 \cdot 3149 + 0 \cdot 2770 + 1 \cdot 4022 = 10034.$$

Пользователь $B$ умножает шифртекст 10034 на $v^{-1} = 5522^{-1} \equiv 1746 \pmod{4441}$, получает $s \equiv 10034 \cdot 1746 \equiv 4060 \pmod{4441}$. Далее решает задачу об укладке ранца для сверхвозрастающей последовательности (это мы делали в примере 8.6), получая $y_1 = y_2 = 0$, $y_3 = y_4 = y_5 = 1$.

Осталось восстановить правильный порядок битов в сообщении, используя перестановку $\psi$ из примера 8.7:

$$m_1 = y_{\psi(1)} = y_3 = 1,\ m_2 = y_{\psi(2)} = y_5 = 1,\ m_3 = y_{\psi(3)} = y_2 = 0,$$

$$m_4 = y_{\psi(4)} = y_1 = 0,\ m_5 = y_{\psi(5)} = y_4 = 1$$

— исходное сообщение получено. □

В протоколах шифрования на основе мультипликативной задачи об укладке ранца вместо сверхвозрастающей последовательности используется последовательность взаимно простых чисел [4].

Алгоритм 8.7. Генерация ключа для мультипликативного протокола Меркля–Хеллмана.

*Вход*. Длина блока $n$.

*Выход*. Открытый и секретный ключи.

1. Выбрать последовательность из $n$ натуральных попарно взаимно простых чисел: $\{b_1, \ldots, b_n\}$.
2. Выбрать простое число $u > b_1 b_2 \ldots b_n$.
3. Выбрать случайное число $v$, взаимно простое с $u$.
4. Выбрать случайную перестановку $\psi$ чисел $1, 2, \ldots, n$.
5. Замаскировать последовательность $\{b_i\}$, для этого вычислить последовательность $\{a_1, \ldots, a_n\}$ вида $a_i \leftarrow \log_v b_{\psi(i)} \pmod{u}$.
6. Результат: $\{a_1, \ldots, a_n\}$ — открытый ключ; $(\psi, v, u, \{b_1, \ldots, b_n\})$ — секретный ключ. □

Пример 8.9. Пусть последовательность $\{b_i\} = \{2, 3, 5, 7, 11, 13\}$. Произведение элементов этой последовательности равно 30030. В

качестве $u$ выберем наименьшее простое число, большее 30030, — $u = 30047$. Число $v$ может быть любым, не делящимся на $u$: полагаем $v = 10$. Пусть $\psi$: (1, 2, 3, 4, 5, 6) $\to$ (2, 4, 1, 5, 6, 3). Тогда открытым ключом будет:

$$a_1 = \log_v b_{\psi(1)} = \log_v b_2 = \log_{10} 3 \equiv 138 \pmod{30047},$$

$$a_2 = \log_v b_{\psi(2)} = \log_v b_4 = \log_{10} 7 \equiv 14366 \pmod{30047},$$

$$a_3 = \log_v b_{\psi(3)} = \log_v b_1 = \log_{10} 2 \equiv 8420 \pmod{30047},$$

$$a_4 = \log_v b_{\psi(4)} = \log_v b_5 = \log_{10} 11 \equiv 5456 \pmod{30047},$$

$$a_5 = \log_v b_{\psi(5)} = \log_v b_6 = \log_{10} 13 \equiv 18426 \pmod{30047},$$

$$a_6 = \log_v b_{\psi(6)} = \log_v b_3 = \log_{10} 5 \equiv 21627 \pmod{30047}. \qquad \square$$

Алгоритм 8.8. Мультипликативный протокол Меркля–Хеллмана.

*Вход отправителя.* Открытый ключ $\{a_1, \ldots, a_n\}$ из алгоритма 8.7.

*Вход получателя.* Секретный ключ ($\psi$, $v$, $u$, $\{b_1, \ldots, b_n\}$) из алгоритма 8.7.

*Результат.* Зашифрование и расшифрование сообщения.

Для зашифрования сообщения длины $n$ бит, представленного в виде двоичного вектора $(m_1, \ldots, m_n)$, отправитель вычисляет шифртекст $c \leftarrow \sum_{i=1}^{n} m_i a_i$.

Для расшифрования шифртекста получатель выполняет следующие действия.

1. Вычисляет $s \leftarrow v^c \pmod{u}$.
2. Решает задачу об укладке ранца для последовательности взаимно простых чисел: представляет число $s$ в виде произведения: $s = b_1^{y_1} b_2^{y_2} \ldots b_n^{y_n}$.
3. Вычисляет вектор $(m_1, \ldots, m_n)$, где $m_i \leftarrow y_{\psi(i)}$. $\square$

Расшифрование корректно, поскольку выполняется соотношение

$$s \equiv v^c = v^{\sum_{i=1}^{n} m_i a_i} = \prod_{i=1}^{n} v^{m_i a_i} = \prod_{i=1}^{n} (v^{a_i})^{m_i} \equiv \prod_{i=1}^{n} b_{\psi(i)}^{m_i} \pmod{u}.$$

Пример 8.10. Пусть пользователь $A$ хочет передать сообщение (1, 0, 1, 1, 0, 1) пользователю $B$, открытый и секретный ключи которого выработаны в примере 8.9. Шифртекстом, соответствующим этому сообщению, будет

$$c = 1 \cdot 138 + 0 \cdot 14366 + 1 \cdot 8420 + 1 \cdot 5456 + 0 \cdot 18426 + 1 \cdot 21627 = 35641.$$

Для расшифрования получатель вычисляет $s \equiv 10^{35641} \equiv 330 \pmod{30047}$, раскладывает число $s$ на множители:

$$330 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^1 \cdot 13^0,$$

то есть $y_1 = y_2 = y_3 = y_5 = 1$, $y_4 = y_6 = 0$, и восстанавливает правильный порядок битов в сообщении:

$$m_1 = y_{\psi(1)} = y_2 = 1,\ m_2 = y_{\psi(2)} = y_4 = 0,\ m_3 = y_{\psi(3)} = y_1 = 1,$$

$$m_4 = y_{\psi(4)} = y_5 = 1,\ m_5 = y_{\psi(5)} = y_6 = 0,\ m_6 = y_{\psi(6)} = y_3 = 1$$

— это и есть исходное сообщение. □

Скорость шифрования в ранцевых криптоалгоритмах сравнима со скоростью симметричного шифрования. Однако шифрование в таких алгоритмах может быть представлено как нахождение кратчайшего вектора $n$-мерной решетки, то есть вскрытие ключа можно осуществить LLL-алгоритмом.

## Упражнения к главе 8

1. На плоскости расположен квадрат площади 4. Какое наименьшее число точек с целочисленными координатами он содержит?

2. На плоскости расположен квадрат площади 4, содержащий не менее семи точек с целочисленными координатами. Доказать, что он содержит ровно девять точек с целочисленными координатами.

3. Пусть решетка построена на векторах (0, 1), $(0,\sqrt{-2})$. Для каких простых $p$ на окружности радиуса $\sqrt{p}$ с центром в начале координат лежит не менее четырех точек решетки?

4. Пусть решетка построена на векторах (0, 1), $(0,\sqrt{-3})$. Для каких простых $p$ на окружности радиуса $\sqrt{p}$ с центром в начале координат лежит не менее четырех точек решетки?

5. Минимизировать базис $\{1+2\sqrt{2}+3\sqrt{3},\ -\sqrt{2}+4\sqrt{3},\ 2+\sqrt{3}\}$.

6. Решить задачу об укладке ранца:

а) ранец $\{17, 24, 11, 12, 3, 21, 15, 18, 1, 5\}$, $S = 100$;

б) ранец $\{21, 12, 13, 14, 15, 18, 23, 1, 2, 3\}$, $S = 70$;

в) ранец $\{1, 2, 3, 4, 25, 35, 45, 50, 60, 70\}$, $S = 200$.

## Литература к главе 8

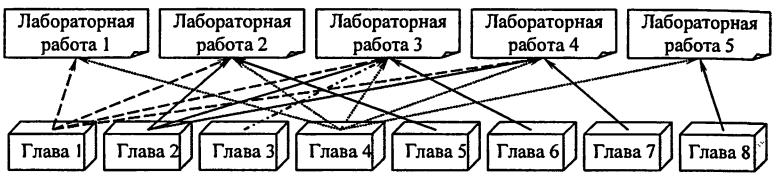

1. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. — М.: МЦНМО, 2003.
2. *Гильберт Д., Кон-Фоссен С.* Наглядная геометрия. — М.: Наука, 1981.
3. *Dwork C.* Lattices and their application to cryptography: Lecture notes. Stanford University, 1998.
4. *Lai M. K.* Knapsack cryptosystems: the past and the future. 2001. Доступно с http://www.ics.uci.edu/~mingl/knapsack.html.
5. *Lenstra A. K., Lenstra H. W., Lovász L.* Factoring polynomials with rational coefficients // Mathematische Annalen. 1982. Vol. 261. No. 4. P. 515–534.

6. *Menezes A., Oorschot P. van, Vanstone S.* Handbook of Applied Cryptography. CRC Press, 1997 (http://www.cacr.math.uwaterloo.ca/hac/).
7. *Merkle R., Hellman M.* Hiding information and signatures in trapdoor knapsacks // IEEE Transactions on Information Theory. 1978. Vol. IT–24. P. 525–530.

# ПРИЛОЖЕНИЕ

Цикл, состоящий из пяти лабораторных работ, позволяет закрепить знание теоретического курса и получить практические навыки реализации и анализа вычислительных алгоритмов.

Теоретический материал, обеспечивающий выполнение каждой лабораторной работы, распределен по главам следующим образом:




При выполнении лабораторной работы 1 «Вычисление наибольшего общего делителя» следует реализовать алгоритмы Евклида (обычный, бинарный, расширенный). Программы, реализующие указанные алгоритмы, используются в двух следующих лабораторных работах и, кроме того, могут быть использованы при выработке параметров криптосистемы RSA.

При выполнении работы «Вероятностные алгоритмы проверки чисел на простоту» необходимо написать программы, реализующие тесты Ферма, Соловэя–Штрассена и Миллера–Рабина. Следует убедиться в работоспособности алгоритмов (учитывая вероятностный характер тестирования), исследовать алгоритмы с точки зрения количества ошибок, допускаемых ими в зависимости от вида тестируемого числа (распознавание чисел Кармайкла) и от количества прогонов теста, обработать полученные статистические данные, а также измерить и сравнить время работы программ. Для выработки чисел Кармайкла можно предложить студентам дополнительно реализовать алгоритм Эрдеша. Полученные

навыки используются в курсовых работах по дисциплине «Криптографические методы защиты информации» при выработке параметров криптосистем с открытым ключом (для шифрования, цифровой подписи, алгоритмов на эллиптических кривых).

Алгоритмы разложения чисел на множители, составляющие содержание работы 3, сравниваются по двум направлениям: специальные (методы Полларда), эффективность которых существенно зависит от вида составного числа, и универсальные (метод непрерывных дробей и метод квадратичного решета).

В лабораторной работе 4 изучаются основные методы дискретного логарифмирования: ρ-метод Полларда и метод базы разложения. При достаточной теоретической подготовке можно реализовать эти методы для произвольной конечной группы, например для группы точек эллиптической кривой.

Лабораторная работа 5 служит для закрепления материала и развития практических навыков по теме «Элементы теории решеток». Студентам предлагается реализовать алгоритм Ленстры–Ленстры–Ловаша и применить его для решения задачи об укладке ранца.

При выполнении каждой лабораторной работы студент должен написать программу, реализующую приведенные алгоритмы (языки программирования: C, C++, Java — на усмотрение студента), проанализировать результаты работы программы, ответить на контрольные вопросы и сделать соответствующие выводы.

## Лабораторная работа 1

## Вычисление наибольшего общего делителя

Цель работы — изучение алгоритмов вычисления наибольшего общего делителя целых чисел и анализ их быстродействия.

## Порядок выполнения работы

1. Написать программу, реализующую алгоритмы нахождения наибольшего общего делителя и его линейного представления, убедиться в ее работоспособности.
2. Сравнить время работы алгоритмов для различных входных данных:
   - для пар чисел из одного диапазона (отличающихся на один-два десятичных разряда);
   - для пар чисел из различных диапазонов (отличающихся на три и более десятичных разрядов);
   - в обоих случаях провести измерения для чисел как небольших, так и высоких порядков.
3. Обосновать полученные результаты.

## Содержание отчета

1. Постановка задачи.
2. Теоретические сведения.
3. Результаты работы, в том числе:
   - текст программы, реализующей алгоритмы вычисления наибольшего общего делителя;
   - примеры работы программ: наибольший общий делитель (для каждого алгоритма) и его линейное представление (для расширенных алгоритмов);
   - результаты исследования скорости работы алгоритмов для различных входных данных (на определенной аппаратной платформе).
4. Теоретическое обоснование полученных результатов.
5. Ответы на контрольные вопросы.
6. Выводы по работе.

## Контрольные вопросы

1. Предложить варианты оптимизации алгоритмов.
2. В каком случае обычный алгоритм Евклида может опережать бинарный?
3. Как влияет способ выбора чисел на результаты тестирования того или иного алгоритма? Рассмотреть диапазоны, из которых выбираются числа, вид этих чисел и фактор их случайности.
4. Предложить способы проверки быстродействия алгоритмов.
5. Является ли линейное представление наибольшего общего делителя двух чисел единственным и почему?

## Пример отчета о выполненной работе

В ходе работы был рассмотрен алгоритм Евклида вычисления наибольшего общего делителя, а также его модификации: бинарный алгоритм, расширенный алгоритм, бинарный расширенный алгоритм.

Для проверки работоспособности и эффективности этих алгоритмов была написана программа на языке С (текст программы приводится студентом самостоятельно). Алгоритмы реализованы в виде подпрограмм, что позволяет тестировать как корректность их работы, так и быстродействие.

Примеры работы алгоритмов (анализ корректности)

| | Числа | |
|---|---|---|
| Алгоритм Евклида | 35, 14 | 232564, 7679 |
| Обычный | 7 | 1097 |
| Бинарный | 7 | 1097 |
| Расширенный | $7 = 35 \cdot 1 + 14 \cdot (-2)$ | $1097 = 232564 \cdot (-3) + 7679 \cdot 91$ |
| Расширенный бинарный | $7 = 35 \cdot 7 + 14 \cdot (-17)$ | $1097 = 232564 \cdot (-45) + 7679 \cdot 1363$ |

Оценка скорости алгоритмов производилась с использованием библиотечной функции языка С для измерения времени совместно с различными искусственными способами замедления работы программы. Первый из них (тест 1) — многократное повторение (1000000 проходов) вызова функции вычисления наибольшего общего делителя для одних и тех же входных данных. Тесты такого рода позволяют экспериментально установить зависимость скорости работы алгоритмов от вида входных данных (см. контрольный вопрос 3). Второй (тест 2) — вычисление наибольшего общего делителя всех комбинаций чисел из достаточно большого диапазона. Такой тест позволит получить общие характеристики алгоритмов. (Возможно совмещение этих и подобных тестов быстродействия алгоритмов.)

Результаты тестирования алгоритмов на быстродействие (Pentium 166, 80 Мб ОЗУ)

| | *Тест 1* | | *Тест 2* | |
|---|---|---|---|---|
| | Числа | | Диапазон | |
| Алгоритм Евклида | 321, 123 | 16777217, 1023 | 1÷1000 | 20000÷21000 |
| Обычный | 4,34 с | 3,19 с | 3,74 с | 4,34 с |
| Бинарный | 2,25 с | 6,48 с | 3,08 с | 4,56 с |
| Расширенный | 7,69 с | 5,49 с | 6,43 с | 7,75 с |
| Расширенный бинарный | 2,97 с | 7,75 с | 3,96 с | 5,99 с |

## Лабораторная работа 2

### ВЕРОЯТНОСТНЫЕ АЛГОРИТМЫ ПРОВЕРКИ ЧИСЕЛ НА ПРОСТОТУ

Цель работы — изучение вероятностных алгоритмов проверки чисел на простоту и их сравнительный анализ.

## Порядок выполнения работы

1. Написать программу, реализующую вероятностные алгоритмы проверки чисел на простоту (тест Ферма, тест Соловэя–Штрассена, тест Миллера–Рабина).
2. Убедиться в работоспособности алгоритмов (учитывая вероятностный характер тестирования).
3. Исследовать алгоритмы с точки зрения числа ошибок, допускаемых ими в зависимости:
   - от вида числа;
   - от числа прогонов теста,

   и обработать полученные статистические данные.
4. Измерить и сравнить время работы алгоритмов.
5. Обосновать полученные результаты.

## Содержание отчета

1. Постановка задачи.
2. Теоретические сведения.
3. Результаты работы, в том числе:
   - текст программы, реализующей алгоритмы тестирования;
   - примеры работы программ: демонстрация корректной и ошибочной работы алгоритмов в зависимости от входных данных;
   - результаты статистического исследования корректности работы алгоритмов;
   - результаты исследования скорости работы алгоритмов для различных входных данных (на определенной аппаратной платформе).
4. Теоретическое обоснование полученных результатов.
5. Ответы на контрольные вопросы.
6. Выводы по работе.

## Контрольные вопросы

1. Предложить варианты оптимизации алгоритмов.
2. Является ли оптимизацией алгоритмов проверки чисел на простоту предварительное применение к этим числам признаков делимости на другие числа?
3. Как зависят результаты тестирования от свойств используемого генератора псевдослучайных чисел?
4. Указать основания для заданного целого числа, по которым оно всегда будет псевдопростым; эйлеровым псевдопростым; сильным псевдопростым.
5. В каких ситуациях предпочтительнее тот или иной алгоритм проверки чисел на простоту?

## Пример отчета о выполненной работе

В ходе работы были рассмотрены следующие вероятностные алгоритмы проверки целых чисел на простоту: тест Ферма, тест Соловэя–Штрассена, тест Миллера–Рабина. Была написана программа на языке С (текст программы приводится студентом самостоятельно). Тесты реализованы в виде подпрограмм. Кроме того, потребовались дополнительные подпрограммы для анализа эффективности и быстродействия тестов.

Примеры работы алгоритмов (анализ корректности)

| Тестируемое число | Число повторов теста | Результат | | |
|---|---|---|---|---|
| | | Тест Ферма | Тест Соловэя–Штрассена | Тест Миллера–Рабина |
| 113 | 30 | Простое | Простое | Простое |
| 12673 | 1 | Простое | Составное | Составное |

Результаты статистического исследования алгоритмов

При использовании алгоритмов в силу вероятностного характера проводимого тестирования возможно ошибочное определение составных чисел как простых по двум причинам:

1) число повторов теста слишком мало;
2) тест Ферма применен к числам Кармайкла.

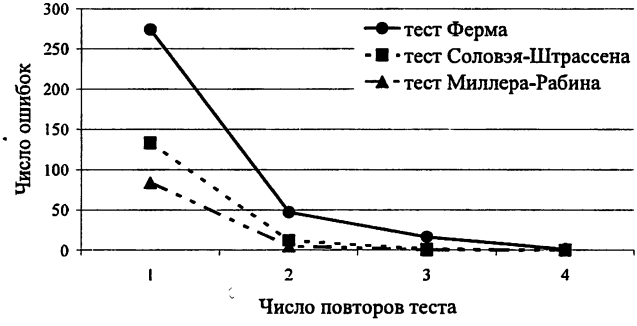
Для исследования зависимости числа ошибок, сделанных каждым тестом (для числа, не являющегося числом Кармайкла), от числа повторов использовалось число 3277.

*Число ошибок, допущенных тестами для числа 3277*

*(на 1000 запусков программы)*

| Число повторов | Тест Ферма | Тест Соловэя–Штрассена | Тест Миллера–Рабина |
|---|---|---|---|
| 1 | 274 | 133 | 84 |
| 2 | 47 | 12 | 5 |
| 3 | 16 | 1 | 0 |
| 4 | 1 | 0 | 0 |

*Зависимость числа ошибок, допущенных тестами, от числа шагов*



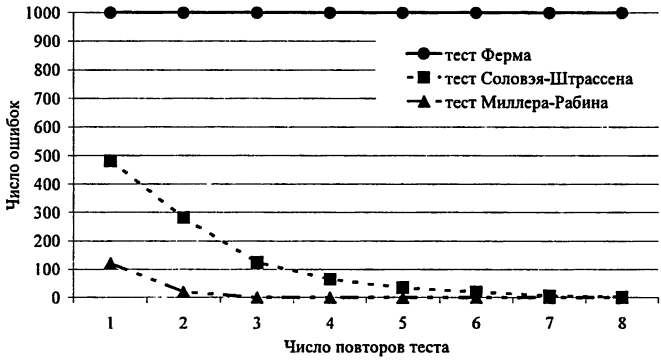
Для исследования зависимости числа ошибок, сделанных при тестировании числа Кармайкла, от числа проходов использовалось число 1729.

*Число ошибок, допущенных тестами для числа 1729*

*(на 1000 запусков программы)*

| Число повторов | Тест Ферма | Тест Соловэя–Штрассена | Тест Миллера–Рабина |
|---|---|---|---|
| 1 | 1000 | 481 | 121 |
| 2 | 1000 | 282 | 20 |
| 3 | 1000 | 124 | 0 |
| 4 | 1000 | 65 | 0 |
| 5 | 1000 | 35 | 0 |
| 6 | 1000 | 20 | 0 |
| 7 | 1000 | 6 | 0 |
| 8 | 1000 | 2 | 0 |

*Зависимость числа ошибок, допущенных тестами для числа Кармайкла, от числа шагов*

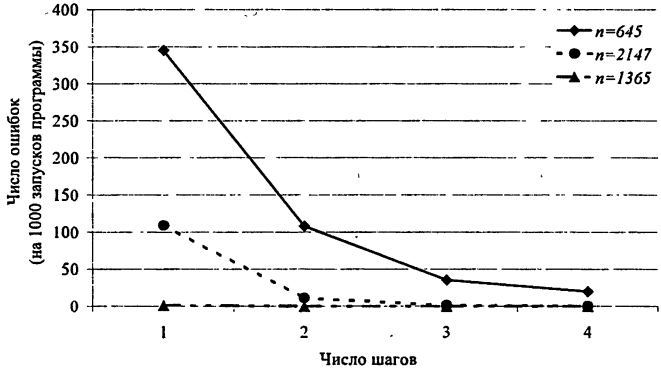


Рассмотрим теперь, как влияет выбор числа на каждый из алгоритмов.

*Число ошибок, допущенных тестом Ферма (на 1000 запусков программы)*

| Число повторов | Число ошибок | | |
|---|---|---|---|
| | $n = 645$ | $n = 2147$ | $n = 1365$ |
| 1 | 345 | 109 | 1 |
| 2 | 108 | 11 | 0 |
| 3 | 35 | 1 | 0 |
| 4 | 20 | 0 | 0 |

*Зависимость числа ошибок, допущенных тестом Ферма, от вида числа*




Лучший результат получился для сильно составного числа $1365 = 3 \cdot 5 \cdot 7 \cdot 13$. Для чисел, в каноническое разложение которых входят большие простые множители ($645 = 3 \cdot 5 \cdot 43$ и $2147 = 19 \cdot 113$), тест Ферма работает хуже. (Аналогичные исследования других тестов студент проводит самостоятельно.)

Результаты тестирования алгоритмов на быстродействие

Для получения объективной оценки быстродействия алгоритмов нужно применить их к простым числам. Для числа 1093 и 10000 повторов теста получились следующие результаты (Pentium 166, 80 Мб ОЗУ, оценка производилась программой-профилировщиком, входящей в поставку компилятора Borland C++ v.3.1): время выполнения теста Ферма — 6,3 с, Соловэя–Штрассена — 6,7 с, Миллера–Рабина — 1,5 с.

Худший результат показал тест Соловэя–Штрассена. Тест Миллера–Рабина не только самый достоверный, но и самый быстрый. Тест Ферма неэффективен по сравнению с тестом Миллера–Рабина, так как основной цикл его программы (модульное возведение в степень) по крайней мере в два раза длиннее аналогичного цикла программы, реализующей тест Миллера–Рабина, а второй цикл последней работает не всегда.

## Лабораторная работа 3

## Разложение чисел на множители

Цель работы — изучение алгоритмов разложения целых чисел на множители и их анализ.

### Порядок выполнения работы

1. Написать программу, реализующую алгоритмы разложения чисел на множители.
2. Убедиться в работоспособности алгоритмов.
3. Исследовать алгоритмы с точки зрения их результативности и эффективности в зависимости от вида числа.
4. Обосновать полученные результаты.

## Содержание отчета

1. Постановка задачи.
2. Теоретические сведения.
3. Результаты работы, в том числе:
   - текст программы, реализующей алгоритмы разложения чисел на множители;
   - примеры работы программ: демонстрация корректной (и некорректной — для алгоритмов Полларда) работы алгоритмов в зависимости от входных данных;
   - сравнительный анализ эффективности алгоритмов Полларда.
4. Теоретическое обоснование полученных результатов.
5. Ответы на контрольные вопросы.
6. Выводы по работе.

## Контрольные вопросы

1. Предложить варианты оптимизации алгоритмов.
2. Как можно упростить интенсивную работу с памятью (избежать ее перераспределения) в методах непрерывных дробей и квадратичного решета?
3. Предложить способы восстановления после неудачного завершения работы ρ-метода Полларда. Как следует выбирать случайное отображение?
4. Предложить способы восстановления после неудачного завершения работы $(p-1)$-метода Полларда. Как следует составлять базу разложения?
5. В каких ситуациях предпочтительнее тот или иной метод разложения чисел на множители?

## Пример отчета о выполненной работе

В ходе работы были рассмотрены следующие методы разложения целых чисел на множители: метод непрерывных дробей, метод квадратичного решета, ρ-метод Полларда, $(p-1)$-метод Полларда. Так как в общем случае проверка числа на простоту является менее трудоемкой, чем любой из алгоритмов разложения числа на множители, то имеет смысл каждое число перед разложением на множители проверить на простоту.

Была написана программа на языке С (текст программы приводится студентом самостоятельно). Каждый метод оформлен в виде подпрограммы. Кроме того, потребовались следующие функции:

- возведение в степень по модулю $n$;
- вычисление наибольшего общего делителя чисел (алгоритм Евклида);
- вероятностный алгоритм проверки числа на простоту (тест Миллера–Рабина).

Примеры работы алгоритмов (анализ корректности)

| | Делитель | | | |
|---|---|---|---|---|
| Число | Метод непрерывных дробей | Метод квадратичного решета | ρ-Метод Полларда | $(p-1)$-Метод Полларда |
| 493 | 17 | 29 | 17 | 17 |
| 1987 | Число прошло тест на простоту! | | | |
| 29563 | 17 | 47 | 37 | 629 |

Примеры работы алгоритмов (анализ эффективности)

Для сравнительного анализа алгоритмов Полларда целесообразно воспользоваться тестом, аналогичным одному из тестов модификаций алгоритма Евклида.

Для фиксированного числа оцениваем время работы алгоритмов (на 1000 запусков). При такой оценке многое зависит как от вида числа, так и от свойств выбранного отображения. В данном случае оно представляло собой функцию $x^2 + 1 \pmod n$. Эту функцию достаточно легко вычислить. Очевидно, такая реализация ρ-метода Полларда будет выигрывать по сравнению с реализацией $(p-1)$-метода хотя бы потому, что последняя требует (помимо операций умножения и деления) вычисления экспоненты и трехкратного вычисления логарифма на каждой итерации. Действительно, ρ-метод Полларда превосходит $(p-1)$-метод более чем в 10 раз для числа любого вида.

Сравнение алгоритмов Полларда по скорости

| | ρ-Метод Полларда | | $(p-1)$-Метод Полларда | |
|---|---|---|---|---|
| Число | Делитель | Время | Делитель | Время |
| 11021 | 107 | 0,22 | 103 | 25,33 |
| 10000 | 16 | 0,05 | 16 | 2,03 |

Несмотря на эффективность, ρ-метод Полларда имеет существенный недостаток: если случайное отображение фиксировано, то для некоторых чисел он не работает. В этом случае требуется поменять отображение (соответственно изменятся временные показатели) или воспользоваться иным методом разложения на множители.

## Лабораторная работа 4

## ДИСКРЕТНОЕ ЛОГАРИФМИРОВАНИЕ В КОНЕЧНОМ ПОЛЕ

Цель работы — изучение методов дискретного логарифмирования.

## Порядок выполнения работы

1. Получить у преподавателя задание, содержащее числа $p$, $a$, $b$ и метод дискретного логарифмирования.
2. Написать программу, реализующую алгоритм дискретного логарифмирования, убедиться в ее работоспособности.
3. Вычислить логарифм заданным методом.
4. Обосновать полученные результаты.

## Содержание отчета

1. Постановка задачи.
2. Теоретические сведения.
3. Результаты работы, в том числе:
   - текст программы, вычисляющей логарифм;
   - полученное значение логарифма.
4. Ответы на контрольные вопросы.
5. Выводы по работе.

## Контрольные вопросы

1. Почему число $p-1$ должно иметь большой простой делитель?
2. На чем основан ρ-метод логарифмирования Полларда?
3. Как работает алгоритм базы разложения?

## Пример отчета о выполненной работе

Исходные данные. $p = 993121$, $a = 4096$, $b = 230611$. В работе требовалось найти логарифм $x$, $a^x \equiv b \pmod p$, ρ-методом Полларда и методом базы разложения.

### ρ-Метод Полларда

Находим представление $p-1=2^5\cdot 3\cdot 5\cdot 2069$. Порядок числа $a$ равен 2068 по модулю 2069. Выберем отображение вида $u_{i+1}\equiv u_i a \pmod p$ при $u_i<500000$; $u_{i+1}\equiv u_i b \pmod p$ при $u_i\geq 500000$. Если число умножается на $a$, то его логарифм увеличивается на 1, если умножается на $b$, то логарифм увеличивается на $x$.

Результаты вычислений $u_i$ ρ-методом Полларда для начальных значений $u_{-1}=a$, $u_0=a^2$

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 887280 | 829087 | 927237 | 183055 | 980046 | 869652 | 462632 | 65804 | 397393 | 989530 |
| | $2x+0$ | $2x+0$ | $2x+2$ | $2x+3$ | $3x+3$ | $3x+4$ | $3x+5$ | $4x+5$ | $5x+5$ | $6x+5$ |
| 10 | 138813 | 512836 | 801632 | 648607 | 961946 | 898115 | 806836 | **64962** | 921045 | 347741 |
| | $6x+6$ | $7x+6$ | $7x+7$ | $7x+8$ | $7x+9$ | $7x+10$ | $7x+11$ | $\mathbf{7x+12}$ | $8x+12$ | $8x+13$ |
| 20 | 211622 | 802200 | 543683 | 733426 | 645139 | 665403 | 139281 | 443522 | 247803 | 31426 |
| | $9x+13$ | $10x+13$ | $10x+14$ | $10x+15$ | $10x+16$ | $10x+17$ | $10x+18$ | $11x+18$ | $12x+18$ | $13x+18$ |
| 30 | 608287 | 325228 | 358627 | 110233 | 637434 | 501117 | 553564 | 188022 | 469337 | 715217 |
| | $14x+18$ | $14x+19$ | $15x+19$ | $16x+19$ | $17x+19$ | $17x+20$ | $17x+21$ | $17x+22$ | $18x+22$ | $19x+22$ |
| 40 | 365028 | 507583 | 16548 | 248380 | 408576 | 118411 | 368408 | 448369 | 238695 | 463656 |
| | $19x+23$ | $20x+23$ | $20x+24$ | $21x+24$ | $22x+24$ | $23x+24$ | $24x+24$ | $25x+24$ | $26x+24$ | $27x+24$ |
| 50 | 287624 | 266398 | 719350 | 84131 | 980710 | 61601 | **64962** | 921045 | 347741 | 211622 |
| | $28x+24$ | $29x+24$ | $30x+24$ | $30x+25$ | $31x+25$ | $31x+26$ | $\mathbf{32x+26}$ | | | |

Приравниваем логарифмы для $u_{17}\equiv u_{56}\equiv 64962 \pmod{993121}$: $7+12x\equiv 32+26x \pmod{2069}$. Отсюда $14x+25\equiv 0 \pmod{2069}$, $x\equiv 14^{-1}\cdot(-25)\equiv 146 \pmod{2069}$.

Проверка: $4096^{146}\equiv 230611 \pmod{993021}$.

## Метод базы разложения

Выбираем базу разложения: $B=\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43\}$.

Находим $B$-гладкие степени числа $a$ (само оно также является $B$-гладким: $a = 2^{12}$).

| | $p_i$ | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a^{u_i}$ | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 |
| $a^{16}$ | 2 | 5 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| $a^{-8}$ | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| $a^{114}$ | 5 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| $a^{42}$ | 3 | 2 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| $a^{1234}$ | 7 | 3 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| $a^{66}$ | 4 | 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $a^{75}$ | 3 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| $a^{999}$ | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| $a^{220}$ | 3 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| $a^{206}$ | 3 | 0 | 2 | 2 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $a^{272}$ | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 |
| $a^{265}$ | 6 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| $a^{943}$ | 0 | 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $a^{315}$ | 8 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $a^{1771}$ | 6 | 3 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| $b^{101}$ | 0 | 2 | 3 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Числа 29, 31, 41 из базы разложения не встречаются ни разу, их можно не учитывать.

Выражаем числа, не встречающиеся в $b^{101}$, через степени основания $a$ и числа 3, 5, 13, 17:

$$2^4 \equiv a^{66}3^{-7} \pmod{993021},\ 7^2 \equiv a^{206}2^{-3}5^{-2}17^{-1} \pmod{993021},$$

$$19^2 \equiv a^{272}2^{-1}5^{-1}13^{-1} \pmod{993021},$$

и подставляем их в выражение для $a^{1771}$:

$$a^{1771\cdot 2} \equiv 2^{12}3^6 7^2 19^2 = 2^{12}3^6 7^2 a^{272} 2^{-1} 5^{-1} 13^{-1} \equiv$$

$$\equiv 2^{11}3^6 a^{272} 5^{-1} 13^{-1} a^{206} 2^{-3} 5^{-2} 17^{-1} \equiv a^{478} 2^8 3^6 5^{-3} 13^{-1} 17^{-1} \equiv$$

$$\equiv a^{478} a^{132} 3^{-14} 3^6 5^{-3} 13^{-1} 17^{-1} \equiv a^{610} 3^{-8} 5^{-3} 13^{-1} 17^{-1} \pmod{993021}$$

или

$$a^{-863} \equiv 3^8 \cdot 5^3 \cdot 13 \cdot 17 \pmod{993021},$$

поскольку $a^{2069} \equiv 1 \pmod{993021}$.

Сравнивая этот результат с разложением числа $b^{101}$, получаем $3^6 b^{101} \equiv a^{-863} \pmod{993021}$. Из разложения $a^{943} \equiv 3^6 \pmod{993021}$ получаем $b^{101} \equiv a^{-943-863} \pmod{993021}$, $b^{101} \equiv a^{263} \pmod{993021}$. Для показателей уравнение имеет вид $101x \equiv 263 \pmod{2069}$. Отсюда $x \equiv 263 \cdot 101^{-1} \equiv 146 \pmod{2069}$.

## Лабораторная работа № 5

## Алгоритм Ленстры–Ленстры–Ловаша и его применение

Цель работы — изучение алгоритма минимизации базиса решетки и его применение для решения задачи об укладке ранца.

### Порядок выполнения работы

1. Написать программу, реализующую LLL-алгоритм.
2. На простых примерах убедиться в результативности алгоритма.
3. Реализовать алгоритм решения задачи об укладке ранца на базе LLL-алгоритма. Проанализировать, при каких входных данных алгоритм с наибольшей вероятностью успешно завершается (при условии существования ответа).
4. Обосновать полученные результаты.

## Содержание отчета

1. Постановка задачи.
2. Теоретические сведения.
3. Результаты работы, в том числе:
   - текст программы, реализующей LLL-алгоритм;
   - примеры работы программы: демонстрация работоспособности LLL-алгоритма и алгоритма решения задачи об укладке ранца (с выводом промежуточных результатов);
   - анализ зависимости результативности алгоритмов решения задачи об укладке ранца от входных данных.
4. Теоретическое обоснование полученных результатов.
5. Ответы на контрольные вопросы.
6. Выводы по работе.

## Контрольные вопросы

1. Является ли LLL-приведенный базис решетки единственным?
2. Как можно обобщить алгоритм решения рассмотренной задачи об укладке ранца для решения задачи общего вида (возможно, с неравенствами в условии)?
3. Проанализировать результативность алгоритмов решения задачи об укладке ранца в зависимости от входных данных.

## Пример отчета о выполненной работе

В ходе работы был изучен и реализован LLL-алгоритм и метод решения задач об укладке ранца на базе этого алгоритма. Для проверки работоспособности алгоритмов была написана программа на языке С. Алгоритмы реализованы в виде подпрограмм. (Текст программы приводится студентом самостоятельно.)

## Примеры работы программ (анализ корректности)

### *Реализация LLL-алгоритма*

1. Исходный базис: $\mathbf{b}_0 = (2, 1)$, $\mathbf{b}_1 = (3, 2)$; LLL-приведенный базис: $\mathbf{b}_0 = (-1, 0)$; $\mathbf{b}_1 = (0, 1)$.

2. Исходный базис: $\mathbf{b}_0 = (1, 0, 1, 2)$, $\mathbf{b}_1 = (1, -1, 2, 0)$, $\mathbf{b}_2 = (-1, 2, 0, 1)$; LLL-приведенный базис: $\mathbf{b}_0 = (-1, 1, 1, -1)$; $\mathbf{b}_1 = (1, 0, 1, 2)$; $\mathbf{b}_2 = (0, -1, 1, -2)$.

### *Решение задачи об укладке ранца*

Исходные данные: «ранец»: {20, 30, 30, 23, 4, 16, 30, 15, 5, 14}; $S = 50$.

Исходный базис:

$$\mathbf{b}_0 = (1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 40)$$

$$\mathbf{b}_1 = (0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 60)$$

$$\mathbf{b}_2 = (0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 60)$$

$$\mathbf{b}_3 = (0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 46)$$

$$\mathbf{b}_4 = (0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 8)$$

$$\mathbf{b}_5 = (0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 32)$$

$$\mathbf{b}_6 = (0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 60)$$

$$\mathbf{b}_7 = (0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 30)$$

$$\mathbf{b}_8 = (0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 10)$$

$$\mathbf{b}_9 = (0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 28)$$

$$\mathbf{b}_{10} = \left(\frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ 100\right)$$

LLL-приведенный базис:

$$\mathbf{b}_0 = (0,\ -1,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0)$$

$$\mathbf{b}_1 = (0,\ 0,\ -1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0)$$

$$\mathbf{b}_2 = \left(-\frac{1}{2},\ \frac{1}{2},\ -\frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ 0\right)$$

$$\mathbf{b}_3 = (-\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, 0)$$

$$\mathbf{b}_4 = (0, -1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$$

$$\mathbf{b}_5 = (-\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, 0)$$

$$\mathbf{b}_6 = (-1, 1, 0, 0, 0, 0, 0, -1, 1, 0, 0)$$

$$\mathbf{b}_7 = (\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, -\frac{3}{2}, \frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 0)$$

$$\mathbf{b}_8 = (\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{3}{2}, -\frac{1}{2}, 0)$$

$$\mathbf{b}_9 = (0, -1, 0, 0, 1, -1, -1, -1, 0, 0, 0)$$

$$\mathbf{b}_{10} = (\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 2)$$

Результат:

$$\mathbf{x} = (1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$$

или

$$\mathbf{x} = (1, 1, 0, 0, 0, 0, 0, 0, 0, 0).$$

## Оценка зависимости результативности алгоритма от входных данных

Предлагается следующий метод анализа алгоритма решения задачи об укладке ранца: для ранца фиксированной мощности $n$ (30÷50 элементов) последовательно изменяем верхнюю границу $a = \max\{a_i \mid 1 \le i \le n\}$ и случайным образом заполняем ранец числами от 1 до $a$. Таким образом, имеется возможность оценить плотность ранца. После этого пытаемся на полученном множестве решить задачу для чисел $s$ из некоторого фиксированного отрезка, выбранного таким образом, что (почти) всегда имеется решение. Количество неудач, таким образом, является характеристикой алгоритма.

Пример выбора параметров: $n = 40$, $a$ изменяется от 3 до 10 с шагом 1, $s$ изменяется от 40 до 60 с шагом 1.

Чистота оценки сильно зависит от свойств используемого генератора случайных чисел. Для получения более точных характеристик алгоритма повторяем тест несколько раз с различными параметрами, результаты (число неудачных завершений алгоритма) выражаем в процентном отношении:

Таким образом, показан убывающий характер зависимости. (От студента, выполняющего работу, требуется разработать и провести по крайней мере еще один тест данной зависимости.)

## ОТВЕТЫ И УКАЗАНИЯ К УПРАЖНЕНИЯМ

### Глава 1

1. Рассмотреть произведение $n(n^3 - 1)(n^3 + 1)$.

3. Пусть $n = 2^k + r$, где $r < 2^k$. Сумма $s = [n/2] + [n/2^2] + \ldots + [n/2^k]$ представляет собой степень числа 2, делящую $n!$. Число $s$ принимает максимальное значение, если все слагаемые без квадратных скобок. Оценивая $s$ суммой геометрической прогрессии: $s \le 1 + 2 + 4 + \ldots + 2^k/2 = (2^k - 1)/(2 - 1) = 2^k - 1$, получаем, что $s < n$ и $n!$ делится на $2^s$, но не на $2^n$.

4. Пусть $d_1 = \text{НОД}(a, b)$, $d_2 = \text{НОД}(d_1, c)$, $d_3 = \text{НОД}(a, b, c)$. Числа $a$ и $b$ делятся на $d_3$, значит, и их наибольший общий делитель $d_1$ делится на $d_3$. Число $c$ также делится на $d_3$, значит, наибольший общий делитель $d_2$ чисел $d_1$ и $c$ делится на $d_3$.

Обратно, $d_2 = \text{НОД}(d_1, c)$, значит, $d_1$ делится на $d_2$. Но $d_1$ — это наибольший общий делитель чисел $a$ и $b$, то есть оба этих числа делятся на $d_2$. А так как $c$ тоже делится на $d_2$, число $d_3$ как наибольший общий делитель чисел $a$, $b$ и $c$ должно делиться на $d_2$. Таким образом, $d_2$ делится на $d_3$, и $d_3$ делится на $d_2$, то есть $d_2 = \pm d_3$.

6. а) 1 или 2; б) 1.

7. При $m = n = 1$.

8. Заметим сначала, что любое простое число, отличное от 2, имеет вид $4m + 1$ или $4m + 3$. Произведение чисел вида $4m + 1$ имеет вид $4m + 1$.

Пусть $p_1, p_2, \ldots, p_k$ — все простые числа вида $4m + 3$. Рассмотрим число $4p_1p_2\ldots p_k - 1$. Это число имеет вид $4m + 3$, но простым не является. Все его простые делители не могут иметь вид $4m + 1$, поскольку тогда само это число имело бы вид $4m + 1$. Значит, найдется простое число $p_i$, $1 \le i \le k$, которое делит $4p_1p_2\ldots p_k - 1$. Но тогда 1 должна делиться на $p_i$. Противоречие.

## Глава 2

1. Нет, поскольку ни одно из чисел вида $2^k$ не делится на 13.

2. Любое число $A$ в системе счисления с основанием 100 представляется в виде $A = a_0 + 100a_1 + 100^2a_2 + \ldots$ . Делимость числа $A$ на 101 означает, что $A \equiv 0 \pmod{101}$. Поскольку $100 \equiv -1 \pmod{101}$, получаем требуемое условие делимости: $A \equiv a_0 + (-1)a_1 + (-1)^2a_2 + \ldots \equiv (a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots) \equiv 0 \pmod{101}$.

3. а) 294; б) 9216; в) 46080.

4. а) $x \equiv 10 \pmod{15}$; б) решений нет; в) $x \equiv 7 \pmod{22}$, $x \equiv 18 \pmod{22}$; г) решений нет.

5. Сравнение $y^2 \equiv 2 \pmod 3$ неразрешимо.

6. а) $x \equiv 148 \pmod{315}$; б) $x \equiv 157 \pmod{935}$; в) $x \equiv 59 \pmod{210}$; г) $x \equiv 335 \pmod{924}$.

7. Квадратичные вычеты по модулю 7: 1, 2, 4; квадратичные вычеты по модулю 11: 1, 3, 4, 5, 9; квадратичные вычеты по модулю 13: 1, 3, 4, 9, 10, 12; квадратичные вычеты по модулю 17: 1, 2, 4, 8, 9, 13, 15, 16.

8. 1, –1, –1, 1.

9. Согласно квадратичному закону взаимности Гаусса,

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

По свойству 3 символа Лежандра $\left(\frac{2^p-1}{3}\right) \equiv (2^p-1)^{(3-1)/2} \pmod 3$.

Таким образом, $\left(\frac{3}{2^p-1}\right) \equiv -(2^p-1) \equiv -2^p + 1 \equiv -(-1)^p + 1 \equiv (-1)^{p+1} + 1 \pmod 3$. По условию число $p$ простое, нечетное, значит, $(-1)^{p+1} = 1$ и $\left(\frac{3}{2^p-1}\right) \equiv 2 \equiv -1 \pmod 3$, то есть 3 является квадратичным невычетом по модулю $2^p - 1$.

10. а) $1 = \left(\frac{7}{p}\right) = (-1)^{(p+1)/2}\left(\frac{p}{7}\right) \equiv (-1)^{(p+1)/2}p^3 \pmod 7$. Значит, $p^3 \equiv 1 \pmod 7$, если число $(p+1)/2$ четное, то есть $p \equiv 3 \pmod 4$, и $p^3 \equiv -1 \pmod 7$, если число $(p+1)/2$ нечетное, то есть $p \equiv 1 \pmod 4$. Из условия $p^3 \equiv 1 \pmod 7$ получаем $p \equiv 1, 2$ или $4 \pmod 7$. Из условия $p^3 \equiv -1 \pmod 7$ получаем $p \equiv 3, 5$ или $6 \pmod 7$. Применяя китайскую теорему об остатках, получаем, что 7 является квадратичным вычетом, если $p \equiv \pm 1, \pm 3$ или $\pm 9 \pmod{28}$; б) $p \equiv \pm 1, \pm 7, \pm 11$ или $\pm 17 \pmod{60}$.

11. б) Привести сравнение к виду $x^2 \equiv d \pmod p$.

13. а) $x \equiv \pm 8 \pmod{19}$; б) $x \equiv \pm 11 \pmod{23}$; в) $x \equiv \pm 13 \pmod{31}$.

14. а) $x \equiv \pm 9 \pmod{37}$; б) $x \equiv \pm 15 \pmod{53}$; в) $x \equiv \pm 18 \pmod{61}$.

15. а) $x \equiv \pm 107 \pmod{3^5}$; б) $x \equiv \pm 284 \pmod{5^4}$; в) $x \equiv \pm 145 \pmod{7^3}$.

16. а) $x \equiv \pm 9, \pm 23 \pmod{2^6}$; б) $x \equiv \pm 43, \pm 85 \pmod{2^8}$; в) $x \equiv \pm 65, \pm 191 \pmod{2^9}$.

17. а) $x \equiv \pm 17, \pm 27 \pmod{5 \cdot 11}$; б) $x \equiv \pm 31, \pm 61, \pm 169, \pm 199, \pm 261, \pm 291, \pm 399, \pm 429 \pmod{2^3 \cdot 5 \cdot 23}$; в) $x^2 \equiv \pm 1637, \pm 3949, \pm 7033, \pm 9345 \pmod{2^2 \cdot 17^2 \cdot 19}$.

## Глава 3

2. $\sqrt{5} = [2; \{4\}]$; $P_1/Q_1 = 9/4$, $P_2/Q_2 = 38/17$, $P_3/Q_3 = 161/72$, $P_4/Q_4 = 682/305$, $P_5/Q_5 = 2889/1292$.

$1/\sqrt{5} = [0; 2, \{4\}]$; $P_1/Q_1 = 1/2$, $P_2/Q_2 = 4/9$, $P_3/Q_3 = 17/38$, $P_4/Q_4 = 72/161$, $P_5/Q_5 = 305/682$.

$2 - 1/\sqrt{5} = [1; 1, 1, \{4\}]$; $P_1/Q_1 = 2/1$, $P_2/Q_2 = 3/2$, $P_3/Q_3 = 14/9$, $P_4/Q_4 = 59/38$, $P_5/Q_5 = 250/161$.

5. $\sqrt{n^2+1} = [n; \{2n\}]$; $\sqrt{n^2+2} = [n; \{n, 2n\}]$.

7. а) $x = 25 + 53t$, $y = 40 + 85t$; б) $x = -28 + 11t$, $y = -105 + 41t$, где число $t$ целое.

8. Наименьшие положительные решения: $x=9$, $y=4$ при $N=5$; $x=5, y=2$ при $N=6$; $x=3, y=1$ при $N=8$; $x=10, y=3$ при $N=11$; $x=7$, $y=2$ при $N=12$; $x=649, y=180$ при $N=13$; $x=1520, y=273$ при $N=31$; $x=82, y=9$ при $N=83$.

9. а) Обозначим $x=\cfrac{1}{1+\cfrac{1}{1+\ddots}}$, тогда $x=\cfrac{1}{1+x}$, значит, $x$ является положительным корнем квадратного уравнения $x^2+x-1=0$. Находим $x=\dfrac{-1+\sqrt{5}}{2}$, тогда $x^3=\sqrt{5}-2$.

Аналогично, $y=\cfrac{1}{4+\cfrac{1}{4+\ddots}}$, то есть $y=\cfrac{1}{4+y}$, значит, $y$ является положительным корнем квадратного уравнения $y^2+4y-1=0$, откуда $y=\sqrt{5}-2$ и $x^3=y=\sqrt{5}-2$.

10. а) $\dfrac{2+x}{1-3x+5x^2}=\left[0;\dfrac{2}{1},\dfrac{-7x}{2},\dfrac{-27x}{-7},\dfrac{-270x}{-27}\right]$;

б) $\dfrac{1-2x+3x^2}{1+2x-x^2+x^3}=\left[0;\dfrac{1}{1},\dfrac{4x}{1},\dfrac{-4x}{4},\dfrac{-28x}{-4},\dfrac{-324x}{-28},\dfrac{1296x}{-324}\right]$;

в) $\dfrac{3+x+4x^2+x^3}{1-2x+x^2-x^3+2x^4}=\left[0;\dfrac{3}{1},\dfrac{-7x}{3},\dfrac{-4x}{-7},\dfrac{-108x}{-4},\dfrac{1092x}{-108},\dfrac{107604x}{1092},\right.$
$\left.\dfrac{308819952x}{107604},\dfrac{-8093553302016x}{308819952}\right]$.

## Глава 4

2. У матрицы $A^2$ все элементы $a_{i,-i\,(\mathrm{mod}\,p)}$, где $i=0, 1, \ldots, p-1$, равны $p$, остальные элементы нулевые. Матрица $A^4$ диагональная, все элементы главной диагонали равны $p^2$.

3. $F(\Delta\mathbf{a})=(0, a'_1(1-\omega), a'_2(1-\omega^2), \ldots, a'_{n-1}(1-\omega^{n-1}))$, где $\omega$ — корень $n$-й степени из единицы для преобразования Фурье.

4. Тройка (4, 6, 7) не является допустимой, так как $\sum_{k=0}^{5} 4^{3k} \equiv 6 \not\equiv 0 \pmod 7$ — не выполняется условие 3 для примитивного корня. Тройки (3, 11, 23) и (2, 10, 11) допустимые.

5. $6x^{11} + 8x^9 + x^8 + 11x^7 + 9x^6 + 12x^5 + 11x^4 + 6x^3 + 10x^2 + 1$.

6. $(33a9e62ded3e64777cb08539dd42447cd7f0932d2e0e289c194439eef)_{16}$.

7. $R = 2^{64}$, $aR \equiv 14741726490803884080 \pmod N$,

$bR \equiv 11719000365764191833 \pmod N$,

$(ab)R \equiv 15800334514918459205 \pmod N$,

$ab \equiv 9896734725571940431 \pmod N$.

8. $a(3) = 144613$; $a(12) = 73957102273$; $a(20) = 11356163208001$.

9. а) $(4d8be6a4)_{16}$; б) $(cb4abd6d)_{16}$; в) $(7d2bd32c29268f48)_{16}$.

10. а) $1347234713 = 574513 \cdot 2345 + 1728$;

б) $90824757298347 = 38 \cdot 2345234953459 + 1705829066905$;

в) $42945828529348140931 = 24679619 \cdot 1740133342343 + 631126333614$.

## Глава 5

3. а) 341; б) 91; в) 217.

5. $a = 10$, $n = 33$.

9. Если $a^r \equiv 1 \pmod n$, то, очевидно, $(a^r)^k = (a^k)^r \equiv 1 \pmod n$.

Рассмотрим случай $a^{2^j r} \equiv -1 \pmod n$. Представим показатель $k$ в виде $k = 2^q t$, где число $t$ нечетное. При $q > j$ получаем $(a^k)^r \equiv 1 \pmod n$; при $q \le j$ получаем $(a^k)^{2^{j-q} r} = (a^{2^q t})^{2^{j-q} r} = (a^{2^j r})^t \equiv (-1)^t \equiv -1 \pmod n$.

10. Пусть $a^{n-1} \equiv 1 \pmod n$, $n - 1 = 2^s r$, где $r$ — нечетное, $a^{2^{s-1} r} \equiv b \pmod n$. Возводя второе сравнение в квадрат, получаем $1 \equiv a^{n-1} \equiv$ $\equiv (a^{2^{s-1} r})^2 \equiv b^2 \pmod n$, то есть $(b-1)(b+1) \equiv 0 \pmod n$. Вычисляя НОД$(b \pm 1, n)$, находим нетривиальный делитель числа $n$.

## Глава 6

1. а) $66124207 = 3571 \cdot 18517$;

б) $35677933 = 1823 \cdot 19571$; в) $21478022263 = 33457 \cdot 641959$.

2. а) $8644409 = 3251 \cdot 2659$ ($3251 - 1 = 2 \cdot 5^3 \cdot 13$);

б) $17095777 = 4931 \cdot 3467$ ($4931 - 1 = 2 \cdot 5 \cdot 17 \cdot 29$);

в) $4839315539 = 65521 \cdot 73859$ ($65521 - 1 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$).

3. а) $25549949 = 2963 \cdot 8623$ ($s = [\sqrt{3n}] + 2 = 8756$);

б) $21431227 = 2011 \cdot 10657$ ($s = [\sqrt{5n}] + 5 = 10356$);

в) $19534673 = 1973 \cdot 9901$ ($s = [\sqrt{5n}] + 1 = 9883$).

4. а) $2355343 = 1321 \cdot 1783$ (база разложения $B = \{2, 3, 7, 11\}$, $B$-гладкими являются числа $P_1^2$ и $P_3^2$);

б) $6105409 = 2137 \cdot 2857$ (база разложения $B = \{2, 3, 5\}$, $B$-гладкими являются числа $P_1^2$ и $P_3^2$);

в) $27658343 = 4703 \cdot 5881$ (база разложения $B = \{2, 19, 31\}$, $B$-гладкими являются числа $P_5^2$ и $P_7^2$).

5. $n = 34840062373 \cdot 37270791697$.

## Глава 7

1. а) $x \equiv 545 \pmod{653}$; б) $x \equiv 541 \pmod{1031}$; в) $x \equiv 1105 \pmod{1409}$.

2. а) $x \equiv 1207 \pmod{5903}$; б) $x \equiv 10751 \pmod{10799}$; в) $x \equiv 8421 \pmod{16001}$.

3. а) $x \equiv 29048 \pmod{406980}$; б) $x \equiv 1633 \pmod{537240}$; в) $x \equiv 459919 \pmod{671232}$.

4. а) $x \equiv 112940 \pmod{806086}$; б) $x \equiv 77501 \pmod{1221082}$; в) $x \equiv 43637 \pmod{1362442}$.

## Глава 8

7. а) (1, 1, 0, 1, 1, 1, 0, 1, 0, 1) (вектор $\mathbf{b}_6$), (1, 0, 1, 1, 0, 1, 1, 1, 1, 1) (вектор $\mathbf{b}_7$) или (1, 1, 1, 1, 1, 0, 1, 1, 0, 0) (вектор $\mathbf{b}_9$); б) (0, 0, 1, 1, 0, 1, 1, 0, 1, 0) (вектор $\mathbf{b}_2$), (0, 1, 0, 0, 1, 1, 1, 0, 1, 0) (вектор $\mathbf{b}_3$), (0, 1, 0, 1, 0, 1, 1, 1, 1, 0) (вектор $\mathbf{b}_4$) или (0, 0, 0, 1, 1, 1, 1, 0, 0, 0) (вектор $\mathbf{b}_6$); в) (0, 0, 0, 0, 0, 1, 1, 1, 0, 1) (вектор $\mathbf{b}_6$), (1, 1, 1, 1, 1, 0, 1, 1, 0, 1) (вектор $\mathbf{b}_8$) или (1, 1, 1, 1, 0, 1, 1, 1, 1, 0) (вектор $\mathbf{b}_{10}$).

8. а) (1/21, 2/21, 2/21, 6/21, 2/21), (1/18, 2/18, 2/18, 5/18, 2/18) или (2/46, 4/46, 5/46, 13/46, 5/46); б) (1/8, 1/8, 1/8, 2/8, 1/8), (1/16, 2/16, 2/16, 4/16, 2/16), (2/28, 3/28, 3/28, 7/28, 4/28), (3/48, 5/48, 6/48, 12/48, 7/48) или (3/51, 5/51, 6/51, 13/51, 7/51); в) (8/45, 5/45, 4/45, 10/45, 10/45).

## ОГЛАВЛЕНИЕ


**Введение** ..... 3

**Глава 1. ДЕЛИМОСТЬ В КОЛЬЦЕ ЦЕЛЫХ ЧИСЕЛ** ..... 5

1.1. Делимость в кольце целых чисел ..... 7

1.2. Наибольший общий делитель и наименьшее общее кратное 11

1.3. Вычисление наибольшего общего делителя ..... 16

1.3.1. Алгоритм Евклида ..... 16

1.3.2. Бинарный алгоритм Евклида ..... 20

1.3.3. Расширенный алгоритм Евклида ..... 22

1.4. Простые числа ..... 27

1.4.1. Свойства простых чисел ..... 27

1.4.2. Распределение простых чисел ..... 30

Упражнения к главе 1 ..... 32

Литература к главе 1 ..... 33

**Глава 2. СРАВНЕНИЯ С ОДНИМ НЕИЗВЕСТНЫМ** ..... 34

2.1. Отношение сравнимости ..... 34

2.2. Решение сравнений ..... 40

2.2.1. Сравнения первой степени ..... 41

2.2.2. Китайская теорема об остатках ..... 45

2.2.3. Сравнения произвольной степени по простому модулю ..... 48

2.3. Сравнения второй степени ..... 50

2.3.1. Символы Лежандра и Якоби ..... 50

2.3.2. Случаи простого модуля ..... 62

2.3.3. Случаи составного модуля ..... 67

Упражнения к главе 2 ..... 79

Литература к главе 2 ..... 81

**Глава 3. ОСНОВЫ ТЕОРИИ НЕПРЕРЫВНЫХ ДРОБЕЙ** ..... 82

3.1. Определение непрерывной дроби ..... 82

3.2. Подходящие дроби ..... 86

3.3. Квадратичные иррациональности ..... 99

3.4. Использование непрерывных дробей для решения задач ..... 103

3.4.1. Простейшие диофантовы уравнения и сравнения первой степени ..... 104

3.4.2. Уравнение Пелля ..... 105

3.4.3. Представление числа в виде суммы квадратов ..... 111

3.5. Разложение функций в непрерывные дроби ..... 113

Упражнения к главе 3 ..... 116

Литература к главе 3 ..... 117

**Глава 4. АРИФМЕТИЧЕСКИЕ ОПЕРАЦИИ НАД ЦЕЛЫМИ ЧИСЛАМИ И ПОЛИНОМАМИ** ..... 118

4.1. Сложение и вычитание ..... 118

4.2. Умножение ..... 121

4.2.1. Умножение «в столбик». Возведение в квадрат ..... 121

4.2.2. Умножение методом Карацубы–Офмана ..... 124

4.2.3. Умножение в классах вычетов ..... 125

4.3. Умножение с помощью быстрого преобразования Фурье ..... 130

4.3.1. Дискретное преобразование Фурье ..... 130

4.3.2. Алгоритм быстрого преобразования Фурье ..... 140

4.3.3. Алгоритм Шенхаге–Штрассена для умножения целых чисел ..... 146

4.4. Модульное умножение ..... 150

4.4.1. Метод Монтгомери ..... 150

4.4.2. Модульное возведение в степень ..... 154

4.5. Целочисленное деление с остатком ..... 157
4.5.1. Схема Горнера ..... 158
4.5.2. Деление на $2^m - c$ ..... 160
4.5.3. Общий случай ..... 161
Упражнения к главе 4 ..... 166
Литература к главе 4 ..... 167

**Глава 5. ПРОВЕРКА ЧИСЕЛ НА ПРОСТОТУ** ..... 169

5.1. Вероятностные алгоритмы проверки чисел на простоту ..... 169
5.1.1. Тест Ферма ..... 171
5.1.2. Тест Соловэя–Штрассена ..... 179
5.1.3. Тест Миллера–Рабина ..... 183
5.1.4. Генерация простого числа ..... 192
5.2. Детерминированные алгоритмы проверки чисел на простоту ..... 193
5.2.1. Проверка чисел Мерсенна ..... 194
5.2.2. Проверка с использованием разложения числа $n - 1$ ..... 200
Упражнения к главе 5 ..... 203
Литература к главе 5 ..... 205

**Глава 6. РАЗЛОЖЕНИЕ ЧИСЕЛ НА МНОЖИТЕЛИ И КРИПТОСИСТЕМА RSA** ..... 207

6.1. Метод пробного деления ..... 207
6.2. ρ-Метод Полларда ..... 209
6.3. $(p - 1)$-Метод Полларда ..... 213
6.4. Метод квадратов ..... 216
6.4.1. Метод непрерывных дробей ..... 219
6.4.2. Метод квадратичного решета ..... 222
6.5. Криптографическая система RSA ..... 225

6.5.1. Принцип действия ..... 226
6.5.2. Безопасность криптосистемы RSA и задача разложения на множители ..... 227
6.5.3. Атаки на криптосистему RSA, не требующие разложения 229
Упражнения к главе 6 ..... 236
Литература к главе 6 ..... 237

**Глава 7. ДИСКРЕТНОЕ ЛОГАРИФМИРОВАНИЕ В КОНЕЧНОМ ПОЛЕ** ..... 239

7.1. Задача дискретного логарифмирования в конечном поле .. 239
7.1.1. ρ-Метод Полларда ..... 240
7.1.2. Методы Гельфонда и Сильвера–Полига–Хеллмана ..... 242
7.1.3. Метод встречи посередине ..... 246
7.1.4. Метод базы разложения ..... 247
7.2. Протокол Диффи–Хеллмана ..... 249
Упражнения к главе 7 ..... 253
Литература к главе 7 ..... 254

**Глава 8. ЭЛЕМЕНТЫ ТЕОРИИ РЕШЕТОК** ..... 256

8.1. Процесс ортогонализации Грама–Шмидта ..... 256
8.2. Алгоритм Ленстры–Ленстры–Ловаша и его применение ..... 259
8.3. Задача об укладке ранца ..... 273
8.3.1. Способы решения ..... 274
8.3.2. Ранцевые алгоритмы шифрования с открытым ключом ..... 278
Упражнения к главе 8 ..... 283
Литература к главе 8 ..... 284

**ПРИЛОЖЕНИЕ** ..... 286

Лабораторная работа 1. Вычисление наибольшего общего делителя ..... 287
Лабораторная работа 2. Вероятностные алгоритмы проверки чисел на простоту ..... 290
Лабораторная работа 3. Разложение чисел на множители ..... 296
Лабораторная работа 4. Дискретное логарифмирование в конечном поле ..... 299
Лабораторная работа 5. Алгоритм Ленстры–Ленстры–Ловаша и его применение ..... 303
**ОТВЕТЫ И УКАЗАНИЯ К УПРАЖНЕНИЯМ** ..... 308

Учебное издание

**Елена Борисовна Маховенко**

# ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Заведующая редакцией *Т. А. Денисова*
Корректор *Е. Н. Клитина*
Компьютерная верстка *О. Ю. Самариной*

Издательство «Гелиос АРВ»
Издательская лицензия ЛР № 066255
107140, г. Москва, Верхняя Красносельская ул., 16.
Тел./факс (495) 264-44-39, e-mail info@gelios-arv.ru
Адрес в Internet: http://www.gelios-arv.ru
Гигиенический сертификат №77.99.02.953.Д.000390.01.06
от 25.01.2006 г.
Формат 84x108/32. Бумага офсетная. 10 п. л. Тираж 1000 экз.
Заказ № 59
Отпечатано с готовых диапозитивов в типографии ГП «Облиздат».
248640, г. Калуга, пл. Старый торг, 5.

# Учебное пособие

В учебном пособии излагаются методы решения алгебраических и теоретико-числовых задач, возникающих при разработке и исследовании криптографических методов и средств защиты информации. Изучаются алгоритмы арифметики больших целых чисел и полиномов, проверки чисел на простоту и разложения на множители. Исследуется безопасность криптосистем RSA, Диффи–Хеллмана, ранцевых криптосистем.

Приведены примеры практических заданий по реализации ряда алгоритмов.

Гелиос АРВ