Теория чисел

Sokolnikov Alex

2025-2026

Содержание

1. Вступление

Сложность некоторых основных алгоритмов:

- Логарифм

  $q \geq 2$

  $Lq(n) = \lfloor \log_q n \rfloor + 1$

  $Lq(0) = 1$

  $Lq(n) = O(Lq'(n))$

- Сложение

  $a + b$ за $O(\max(L(a), L(b)))$

- Умножение

  $M(n) = O(n^2)$ — столбик

  $M(n) = O(n^{\log_2 3})$ — алгоритм Карацубы

  $M(n) = O_\varepsilon(n^{1+\varepsilon})$ — алгоритм Тома-Кука

  $M(n) = O(n \log n \log\log n)$ — алгоритм Шенхаге-Штрассена

  $M(n) = O(n \log n)$ (2019) — чтобы обогнать предыдущий алгоритм, нужно число порядка $\log n = 2^{7 \cdot 10^{38}}$

2. Алгоритм Евклида

Определение 2.1

$a_1, \ldots, a_n \in \mathbb{Z}$ не равные одновременно 0
Тогда их НОД-ом называется наибольшее число d, которое делит их всех, и обозначается $(a_1, \ldots, a_n)$

$(a, b) = ?$
$a = bq + r,\ 0 \le r < b$
$(a, b) = (b, r)$
Остается сделать так несколько раз:

$$\begin{cases} m_0 = a_0 m_1 + m_2 \\ m_1 = a_1 m_2 + m_3 \\ \ldots \\ m_{k-1} = a_{k-2} m_{k-1} + m_k \\ m_{k-1} = a_{k-1} m_k \\ m_k = d \end{cases} \qquad m_1 > m_2 > \ldots > m_k > 0$$

Лемма 2.2

Пусть $m_0 \ge m_1$, тогда $k = O(\log m_1)$

Действительно: $m_{i-1} = a_{i-1} m_i + m_{i+1} \ge m_i + m_{i+1} \ge 2m_{i+1}$

Нетрудно убедиться, что взятие модуля через деление в столбик занимает $O(L(b) \cdot (L(q) + 1)) = O(L(b)(L(a) - L(b) + 1))$

Теорема 2.3

Сложность алгоритма Евклида, примененного к числам a, b с длинами $L(a), L(b) \le n$ есть $O(n^2)$

$$\begin{gathered} L(m_1)(L(m_0) - L(m_1) + 1) + L(m_2)(L(m_1) - L(m_2) + 1) + \ldots \le \\ \le L(m_1)(L(m_0) - L(m_1) + 1 + L(m_1) - L(m_2) + 1 + \ldots) \le \\ \le L(m_1)(L(m_0) + k) = O(L(m_1)L(m_0)) \end{gathered}$$

Замечание 2.4

Существуют более быстрые варианты алгоритма Евклида
На сегодняшний день известна оценка сложности $O(M(n) \log n)$
С алгоритмом Шенхаге-Штрассена, получим $O(n \log^2 n \log\log n)$

3. Группы, кольца и поля

Определение 3.1: Группа

Множество $(G, *)$ называется группой, если выполняется 3 свойства:

1. $(a * b) * c = a * (b * c)$ — ассоциативность
2. $\exists e : a * e = e * a = a$ — нейтральный элемент
3. $\forall a \in G \ \exists b : a * b = b * a = e$ — обратный элемент

Пример 3.2

- $G = \{e\}$
- $G = \{\mathbb{Z}, +\}$
- $G = \{R^*, \cdot\}$ — действительные числа без нуля
- $Isom(E^2)$ — движения плоскости ($E^2 = \mathbb{R}^2$ — Евклидова плоскость)
- S_n — множество перестановок

Определение 3.3: Абелева группа

Если $\forall a, b \in G$ верно $a * b = b * a$, группа называется коммутативной или абелевой.

Определение 3.4: Кольцо

Множество R с бинарными операциям $+$ и $\cdot$ называется кольцом, если:

1. $(R, +)$ — абелева группа
2. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ — ассоциативность умножения
3. $a \cdot (b + c) = a \cdot b + a \cdot c$ и $(b + c)a = b \cdot a + c \cdot a$ — дистрибутивность

Пример 3.5

- R — кольцо, тогда $R[x]$ — тоже кольцо
- $R = \{0\}$
- $(\mathbb{Z}, +, \cdot), (\mathbb{R}, +, \cdot), (M_n(\mathbb{R}), +, \cdot)$
- $\mathbb{Z}_m$ — кольцо вычетов по $\mod m$

- $\mathbb{R}[[x]]$ — кольцо формальных степенных рядов над $\mathbb{R}$

Определение 3.6

1. Если $\exists 1 \in R : 1 \cdot a = a \cdot 1 = a$, то R называют кольцом с единицей
2. Если $\forall a, b \in R\ a \cdot b = b \cdot a$, то R называют коммутативным кольцом

Пример 3.7

$2\mathbb{Z} = \{2a : a \in \mathbb{Z}\}$ — кольцо без 1

Определение 3.8

Если R — кольцо с 1, то $a \in R$ называют обратимым элементом, если $\exists b$: $a \cdot b = 1 = b \cdot a$

Определение 3.9: Поле

Если в кольце R с 1 любой ненулевой элемент обратим, то R называют полем

Пример 3.10: Поля

$\mathbb{C}, \mathbb{R}, \mathbb{Q}$

Пример 3.11: Кольца, не являющиеся полями

$M_n(\mathbb{R}), 2\mathbb{Z}, \mathbb{R}[x], \mathbb{R}[[x]]$

Теорема 3.12: Основная теорема арифметики

Произвольное натуральное число $n > 1$ единственным образом (с точностью до порядка сомножителей) раскладывается в произведение простых:

$$n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$$

Существование несложно показать по индукции: если n не простое, то $n = ab$, где $a, b < n$, после чего применяем предположение индукции.

Единственность покажем от противного. Пусть n — наименьшее число, обладающее двумя разложениями:

$$n = p_1^{\alpha_1} \dots p_s^{\alpha_s} = q_1^{\beta_1} \dots q_t^{\beta_t}, \text{причем } p_i \neq q_j$$

Лемма 3.13: Лемма Евклида

$a \mid bc, (a, b) = 1 \Rightarrow a \mid c$

С помощью расширенного алгоритма Евклида (лемма о линейном представление НОД) получим $au + bv = 1$

$$au + bv = 1$$
$$acu + bcv = c$$
$$a \mid acu, a \mid bcv \Rightarrow a \mid c$$

Используя лемму выше можно "отщепляя" q_j можно доказать, что $p_1|1$ — противоречие.

Пример 3.14

Не во всех кольцах число раскладывается на простыми единственным способом: например, в $2\mathbb{Z}$ верно $30 \cdot 2 = 60 = 6 \cdot 10$

Определение 3.15

$m \geq 1$
Числа a и b называется сравнимыми по модулю m, если $a - b$ делится на m
Будем обозначать $a \equiv b \,(\mod m)$ или $a \equiv b \,(m)$

Определение 3.16

Классом вычетов $\overline{a}$ называется множество (по модулю m)

$$\overline{a} = \{a + mt \,|\, t \in \mathbb{Z}\}$$

4. Кольцо $\mathbb{Z}_m$ и группа $\mathbb{Z}_m^*$

4.1. Всякие определения

Определение 4.1

$\mathbb{Z}_m$ — множество классов вычетов

Лемма 4.2: Свойство сравнений

- $a \equiv b\,(m),\ c \equiv d\,(m) \Rightarrow a + c \equiv b + d\,(m)$
- $a \equiv b\,(m),\ c \equiv d\,(m) \Rightarrow ac \equiv bd\,(m)$
- $ak \equiv bk\,(m),\ (k, m) = 1 \Rightarrow a \equiv b\,(m)$
- $ak \equiv bk\,(m),\ k \mid m \Rightarrow a \equiv b\,(m/k)$

Свойства непосредственно следуют из определения.

Следствие 4.3

На $\mathbb{Z}_m$ можно ввести структуру кольца:

1. $\overline{a} + \overline{b} = \overline{a + b}$
2. $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$

Получим коммутативное кольцо с 1

Нужно еще проверить корректность (проверяется ручками):

1. $\overline{a_1} = \overline{a_2},\ \overline{b_1} = \overline{b_2}$

   Хотим $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ и $\overline{a_1 \cdot b_1} = \overline{a_2 \cdot b_2}$.

   Но это сразу следует из свойств сравнений.
2. $\overline{0} + \overline{a} = \overline{a} + \overline{0} = \overline{a}$
3. $\overline{a} + \overline{-a} = \overline{0}$
4. $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$
5. $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$
6. $\overline{a}(\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$
7. $\overline{1} \cdot \overline{a} = \overline{a} \cdot \overline{1} = \overline{a}$

8. $\overline{a} \cdot (\overline{b} + \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$

Определение 4.4

Пусть R — кольцо с 1, то множество

$$R^* = \{a \in R \ : \ a\text{— обратим}\}$$

называется множеством обратимых элементов кольца.

Лемма 4.5

R^* — группа по умножению

Тоже несложно доказывается:
$a, b \in R^*$, хотим $a \cdot b \in R^*$
$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$
А ассоциативность следует из ассоциативности в кольце.
$\mathbb{Z}_m^*$ — группа обратимых элементов кольца $\mathbb{Z}_m$

Теорема 4.6

$\mathbb{Z}_m^* = \{\overline{a} \in \mathbb{Z}_m \ : \ (a, m) = 1\}$

Пусть $\overline{a} \in Z_m^*$.
Значит $\exists b : ab = 1 + mt \Rightarrow (a, m) = 1$.
Докажем в обратную сторону, пусть $(a, m) = 1$. В таком случае:

$$\exists u, v \in \mathbb{Z} : au + mv = 1$$

Перейдя к сравнению получим, что $au = 1$, то есть $\overline{a}$ — обратим.

Определение 4.7

Полной системой вычетов по модулю m называется набор чисел $a_1, \ldots, a_m$, где из каждого класса вычетов взято ровно одно число.
Понятно, что на таком наборе можно ввести вышеописанную структуру кольца.

Пример 4.8

Зачастую берутся $\{0, 1, \ldots, m\}$

Или можно взять наименьшие по модулю: $\{-\frac{m-1}{2}, \ldots, 0, 1, \ldots, \frac{m-1}{2}\}$

Определение 4.9

Приведенной системой вычетом по модулю m называется набор чисел, взятых по одному из каждого класса $\overline{a}$ такого, что $(a, m) = 1$.
Аналогично, на этом можно ввести структуру группы.

Определение 4.10

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$
$\mathbb{Z}_6^* = \{1, 5\}$

Определение 4.11

Функцией Эйлера $\varphi(m)$ называется $|\mathbb{Z}_m^*|$
(количество натуральных чисел $\leq m$, взаимно простых с ним)

Определение 4.12

Функция $f : \mathbb{N} \to \mathbb{C}$ называется мультипликативной, если:

1. $f(1) = 1$
2. $\forall m, n \in \mathbb{N} : (m, n) = 1$ верно $f(m) \cdot f(n) = f(m \cdot n)$

Замечание 4.13

Пусть $f(mn) = f(m)f(n)$ для всех $m, n \in \mathbb{N}$.
Тогда f называется вполне мультипликативной.

Лемма 4.14

φ — мультипликативная функция

Следствие 4.15

$$\varphi(m) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right)$$

Докажем лемму:
Пусть $m = m_1 m_2$ и $(m_1, m_2) = 1$
$|Z_m^*| = \varphi(m) = \varphi(m_1 m_2)$

С другой стороны:

$$\forall x \in \mathbb{Z}_m \quad x = ym_1 + z \quad 0 \le y \le m_2 - 1, 0 \le z \le m_1 - 1$$
$$(x, m) = 1 \Leftrightarrow \begin{cases} (x, m_1) = 1 \\ (x, m_2) = 1 \end{cases}$$

Но $(x, m_1) = 1 \Leftrightarrow (z, m_1) = 1$, поэтому есть $\varphi(m_1)$ способов выбрать z.

Если же y пробегает полную систему вычетов по модулю m_2, то и $x = ym_1 + z$ тоже пробегает полную систему вычетов по модулю m_2.

Пусть система не полная, тогда:

$$y_1 m_1 + z \equiv y_2 m_1 + z \ (m_2)$$
$$(y_1 - y_2) m_1 \equiv 0 \ (m_2)$$
$$y_1 - y_2 \equiv 0 \ (m_2)$$

Но все y различны, значит такого не могло быть.

Значит $(x, m_2) = 1$ возможно для $\varphi(m_2)$ значений y.

Но тогда мы выбираем x $\varphi(m_1) \cdot \varphi(m_2)$ способами, что и требовалось доказать.

Теорема 4.16: Теорема Эйлера

$$m \in \mathbb{N}, (a, m) = 1 \Rightarrow a^{\varphi}(m) \equiv 1 \ (m)$$

Теорема 4.17: Малая теорема Ферма

Это частный случай предыдущей теоремы

$$p \text{ — простое}, (a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \ (p)$$

Пусть $\{r_1, r_2, \ldots, r_{\varphi m}\}$ — приведенная система вычетов по модулю m. Умножим каждое на a, тогда $\{ar_1, ar_2, \ldots, ar_{\varphi m}\}$ тоже является приведенной системой вычетов по модулю m:

$$ar_1 \equiv ar_2 \ (m)$$
$$\Updownarrow$$
$$r_1 \equiv r_2 \ (m)$$

В таком случае:

$$r_1 \cdot r_2 \ldots r_{\varphi(m)} \equiv (ar_1) \cdot (ar_2) \ldots (ar_{\varphi(m)}) \ (m)$$
$$\Updownarrow$$
$$1 \equiv a^{\varphi(m)} \ (m)$$

Замечание 4.18

Обратное к МТФ утверждение неверно.
Например, $2^{340} \equiv 1\ (341)$, но $341 = 31 \cdot 11$

Определение 4.19

Пусть $b > 1$ — натуральное. Тогда составное число m называется псевдопростым по основанию b, если $b^{m-1} \equiv 1\ (m)$.
(псевдопростым Ферма по основаниб b)

Пример 4.20

91 является псевдопростым по основанию 3

4.2. Тест Ферма

Вход: n
Выход: "n — составное" или "n вероятно простое"

1. $b \in_R \{2, 3, \ldots, n-2\}$ и проверяем $b^{n-1} \equiv 1\ (n)$
2. Если сравнение нарушается, то n — составное, иначе "n вероятно простое"

Определение 4.21

Если n — составное и $\forall a \in \mathbb{Z}_n^*$ выполнено $a^{n-1} \equiv 1\ (n)$, то такое число называется числом Кармайкла или абсолютно псевдопростым.

Пример 4.22

Первое число Кармайкла — 561

4.3. Улучшение теста на простоту (Миллер-Рабин)

Пусть n — нечетное простое. Разложим в виде $n - 1 = 2^s \cdot d,\ (d, 2) = 1,\ s \geq 1$

$$a^{n-1} - 1 \equiv 0\ (n)$$
$$a^{2^s d} - 1 = (a^{2^{s-1} d} + 1) \cdot (a^{2^{s-2} d} + 1) \ldots (a^d + 1)(a^d - 1) \equiv 0\ (n)$$

Получили лемму:

Лемма 4.23

Пусть $p > 2$ — простое, $p - 1 = 2^s d$, d — нечетно.
Тогда:

1. Либо $a^d \equiv 1\ (p)$
2. Либо $\exists r : 0 \leq r \leq s - 1$, что $a^{2^r d} \equiv -1\ (p)$.

,

Такая идея доводится до теста Миллера-Рабина:
Вход: n
Выход: "n — составное" или "n вероятно простое"

1. $b \in_R \{2, 3, \ldots, n - 2\}$ и проверяем $b^{n-1} \equiv 1\ (n)$

   Проверим два вышеописанных условия на p.

2. Если оба условия неверны, то n — составное, иначе "не удалось определить"
3. Повторить 1-й шаг несколько раз. Если везде "не удалось определить", то возвращаем "n вероятно простое"

Замечание 4.24

Среди первых $25 \cdot 10^9$ есть 13 чисел, которые являются сильно псевдопростыми по основаниям $2, 3, 5$.
Если добавить $7, 11$, то все числа определяются корректно.