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

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

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

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

Лемма 2.2

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

Действительно: $m_{i-1} = a_{i-1} m_i + m_{i+1} \geq m_i + m_{i+1} \geq 2 m_{i+1}$
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 $L(a), L(b) \leq n$ есть $O(n^2)$

$$\begin{aligned} L(m_1)(L(m_0) - L(m_1) + 1) + L(m_2)(L(m_1) - L(m_2) + 1) + \dots \leq \\ \leq L(m_1)(L(m_0) - L(m_1) + 1 + L(m_1) - L(m_2) + 1 + \dots) \leq \\ \leq L(m_1)(L(m_0) + k) = O(L(m_1) L(m_0)) \end{aligned}$$

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 $a \equiv b \pmod m$ или $a \equiv b\,(m)$

Определение 3.16

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

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