

# Алгебра. Глава 2. Целые числа.

Д. В. Карпов

2024

# Делимость

## Определение

Пусть  $a, b \in \mathbb{Z}$ ,  $b \neq 0$ . Тогда  $a$  *делится* на  $b$  (обозначение:  $a \div b$ ) или, что то же самое,  $b$  *делит*  $a$  (обозначение:  $b \mid a$ ), если  $a = bc$ , где  $c \in \mathbb{Z}$ .

Если  $a \div b$ , то  $b$  — *делитель*  $a$ .

## Свойство 1

Если  $a \div b$  и  $b \div c$ , то  $a \div c$ .

**Доказательство.** Тогда  $a = kb$  и  $b = nc$ , где  $k, n \in \mathbb{Z}$ , откуда следует  $a = knc$ . □

## Свойство 2

Пусть  $a, b \div d$ ,  $a, x, y \in \mathbb{Z}$ . Тогда  $ax + by \div d$ .

**Доказательство.** Тогда  $a = kd$  и  $b = nd$ , где  $k, n \in \mathbb{Z}$ , откуда следует  $ax + by = (kx + ny)d$ . □

## Свойство 3

Пусть  $a, d \in \mathbb{N}$ ,  $a \div d$ . Тогда  $a \geq d$ .

**Доказательство.** Тогда  $a = kd$ , где  $k \in \mathbb{N}$ , откуда следует  $a = kd \geq d$ .

## Теорема 1

Пусть  $a \in \mathbb{Z}$ ,  $b \in \mathbb{N}$ . Тогда существуют единственные такие  $q, r \in \mathbb{Z}$ , что  $0 \leq r < b$  и  $a = bq + r$ .

- Число  $r$  называется *остатком* от деления  $a$  на  $b$ .

**Доказательство.**  $\exists$ . Пусть  $q$  — такое целое число, что  $bq \leq a < b(q+1)$ , а  $r = a - bq$ . Тогда  $0 \leq r < b$  (вычтем из всех трех частей первого неравенства  $bq$ ).

! • Пусть  $a = bq_1 + r_1 = bq_2 + r_2$ , причем  $0 \leq r_1 < b$  и  $0 \leq r_2 < b$ .

• НУО  $r_1 > r_2$ . Тогда  $0 < r_1 - r_2 < b$ .

• С другой стороны,  $r_1 - r_2 = b(q_2 - q_1) \geq b$ .

Противоречие. □

# НОД

## Определение

Пусть  $a_1, \dots, a_n \in \mathbb{Z}$ . Обозначим через  $\text{OD}(a_1, \dots, a_n)$  множество всех общих делителей этих чисел, а через  $(a_1, \dots, a_n)$  — их НОД (наибольший из общих делителей).

## Свойство 1

Если  $b \in \mathbb{N}$ .  $a \div b$ , то  $\text{OD}(a, b)$  — это все делители  $b$  и  $(a, b) = b$ .

**Доказательство.** • Если  $d$  — общий делитель  $a$  и  $b$ , то  $d$  — делитель  $b$ .

• Если  $d$  — делитель  $b$ , то  $a \div d$  по свойству 1 делимости. Значит,  $d$  — общий делитель  $a$  и  $b$ . □

## Свойство 2

Пусть  $a, b, c, k \in \mathbb{Z}$ ,  $c = a + kb$ . Тогда  $\text{OD}(a, b) = \text{OD}(c, b)$ , а следовательно, и  $(a, b) = (c, b)$ .

**Доказательство.** • Пусть  $d \in \text{OD}(a, b)$ . Тогда  $c \div d$ , а значит,  $d \in \text{OD}(c, b)$ .

• Наоборот, если  $d \in \text{OD}(c, b)$ , то  $a = c - kb \div d$ , а значит,  $d \in \text{OD}(a, b)$ .

## Алгоритм Евклида

• Пусть  $a, b \in \mathbb{N}$ ,  $a > b$ . Каждая строка алгоритма — деление с остатком.

$$1) \quad a = bq_1 + r_1, \quad 0 \leq r_1 < b;$$

$$2) \quad b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1;$$

$$3) \quad r_1 = r_2q_3 + r_3, \quad 0 \leq r_3 < r_2;$$

...

$$n) \quad r_{n-2} = r_{n-1}q_n + r_n, \quad 0 \leq r_n < r_{n-1};$$

$$n+1) \quad r_{n-1} = r_nq_{n+1}.$$

• Так как  $b > r_1 > r_2 > \dots$  и все эти числа неотрицательны, алгоритм обязательно закончит работу.

### Теорема 2

$(a, b) = r_n$ ,  $a$   $\text{OD}(a, b)$  — это все делители  $(a, b)$ .

**Доказательство.** • По свойству 2 НОД  $\text{OD}(a, b) = \text{OD}(b, r_1) = \text{OD}(r_1, r_2) = \dots = \text{OD}(r_{n-1}, r_n)$ , а это по свойству 1 НОДа — все делители  $r_n$ .

• Тогда  $(a, b)$  — наибольший из делителей  $r_n$ , а это  $r_n$ . □

## Теорема 3

Пусть  $a, b, m, d \in \mathbb{N}$ . Тогда:

1)  $(am, bm) = m(a, b)$ .

2) Если  $d \in \text{OD}(a, b)$ , то  $(\frac{a}{d}, \frac{b}{d}) = \frac{(a, b)}{d}$ .

**Доказательство.** • НУО  $a > b$ .

1) • Рассмотрим первую строку алгоритма Евклида для  $am$  и  $bm$ :  
 $am = bm \cdot q_1 + r_1 m, \quad 0 \leq r_1 m < bm$ .

- Неполное частное не меняется, а остаток умножается на  $m$ .
- Так будет и со следующими строчками, в результате получится столько же строк, сколько в алгоритме Евклида для  $a$  и  $b$ , а НОД — последний ненулевой остаток — умножится на  $m$ .

2) • Рассмотрим первую строку алгоритма Евклида для  $\frac{a}{d}$  и  $\frac{b}{d}$ :  
 $\frac{a}{d} = \frac{b}{d} \cdot q_1 + \frac{r_1}{d}, \quad 0 \leq \frac{r_1}{d} < \frac{b}{d}$ .

- Неполное частное не меняется, а остаток мы делим на  $d$  (в результате он остается целым).
- Так будет и со следующими строчками, в результате получится столько же строк, сколько в алгоритме Евклида для  $a$  и  $b$ , а НОД — последний ненулевой остаток — разделится на  $d$ .

## Линейное представление НОД

### Теорема 4

Пусть  $a, b \in \mathbb{Z}$ . Тогда существуют такие  $x, y \in \mathbb{Z}$ , что  $(a, b) = ax + by$ .

• Это называется *линейным представлением* НОДа.

**Доказательство.** • Так как делители  $u$  чисел  $a$  и  $-a$  одни и те же,  $(a, b) = (a, -b)$ . Поэтому, можно считать, что  $a, b \in \mathbb{N}$ .

• НУО  $a \geq b$ . Воспользуемся алгоритмом Евклида и соответствующими обозначениями, дополним их: пусть  $r_0 = b$  и  $r_{-1} = a$ .

• Докажем, что существует представление  $(a, b) = x_k r_k + y_k r_{k-1}$  для всех  $k = \{n, \dots, 0\}$  (где  $(a, b) = r_n$ ) индукцией с обратным ходом. При  $k = 0$  получим утверждение теоремы.

• **База  $k = n$**  очевидна:  $(a, b) = 1 \cdot r_n + 0 \cdot r_{n-1}$ .

• **Переход  $k \rightarrow k - 1$ .** Из алгоритма Евклида мы знаем, что  $r_k = r_{k-2} - r_{k-1}q_k$ . Подставим:

$$(a, b) = x_k r_k + y_k r_{k-1} = x_k(r_{k-2} - r_{k-1}q_k) + y_k r_{k-1} =$$

$$(-x_k q_k + y_k) r_{k-1} + x_k r_{k-2}.$$



## Теорема 5

Пусть  $n \geq 2$ ,  $a_1, \dots, a_n \in \mathbb{Z}$ . Положим  $m_2 = (a_1, a_2)$ ,  
 $m_3 = (m_2, a_3)$ ,  $\dots$ ,  $m_n = (m_{n-1}, a_n)$ . Тогда  
 $m_n = (a_1, \dots, a_n)$ , а  $\text{OD}(a_1, \dots, a_n)$  — это все делители  
 $m_n$ .

**Доказательство.** • Индукцией по  $k$  докажем, что  
 $\text{OD}(a_1, \dots, a_k)$  — все делители  $m_k$ .

- База  $k = 2$  доказана в Теореме 2.
- Переход  $k \rightarrow k + 1$ .  $\text{OD}(a_1, \dots, a_k, a_{k+1})$  — это все числа из  $\text{OD}(a_1, \dots, a_k)$ , являющиеся делителями  $a_{k+1}$ .
- Так как  $\text{OD}(a_1, \dots, a_k)$  — это все делители  $m_k$ , получаем, что  $\text{OD}(a_1, \dots, a_k, a_{k+1}) = \text{OD}(m_k, a_{k+1})$ , а это все делители  $m_{k+1} = (m_k, a_{k+1})$  по Теореме 2.
- Итак, утверждение доказано и  $\text{OD}(a_1, \dots, a_n)$  — это все делители  $m_n$ . Теперь понятно, что  $m_n = (a_1, \dots, a_n)$ .  $\square$



## Следствие 1

Для  $a_1, \dots, a_n \in \mathbb{Z}$  существует линейное представление НОД, то есть, такие  $x_1, \dots, x_n \in \mathbb{Z}$ , что

$$(a_1, \dots, a_n) = x_1 a_1 + \dots + x_n a_n.$$

**Доказательство.** • Докажем индукцией по  $k$ , что существует линейное представление  $m_k = (a_1, \dots, a_k)$ .

База  $k = 2$  доказана в Теореме 4.

• **Переход  $k \rightarrow k + 1$ .** По Теореме 5 и индукционному предположению,

$$\begin{aligned} m_{k+1} &= (a_1, \dots, a_k, a_{k+1}) = (m_k, a_{k+1}) = y m_k + x_{k+1} a_{k+1} = \\ &= y(x'_1 a_1 + \dots + x'_k a_k) + x_{k+1} a_{k+1} = \\ &= (y x'_1) a_1 + \dots + (y x'_k) a_k + x_{k+1} a_{k+1}. \end{aligned}$$

Все коэффициенты  $y x'_1, \dots, y x'_k$ , очевидно, целые.  $\square$

## Определение

- Числа  $a_1, \dots, a_n \in \mathbb{Z}$  называются **взаимно простыми**, если  $(a_1, \dots, a_n) = 1$ .
- Если любые два из  $a_1, \dots, a_n$  взаимно просты, эти числа называются **попарно взаимно простыми**.

## Свойство 1

*Если  $a_1, \dots, a_n \in \mathbb{Z}$  попарно взаимно просты, то они взаимно просты.*

**Доказательство.** Если  $(a_1, \dots, a_n) = d > 1$ , то  $(a_1, a_2) \vdots d$ , а значит,  $(a_1, a_2) > 1$ . □

## Свойство 2

Если  $a, b, c \in \mathbb{Z}$  и  $(a, b) = 1$ , то  $(ac, b) = (c, b)$ .

**Доказательство.** • Пусть  $d = (c, b)$  и  $f = (ac, b)$ .

- Из  $c \div d$  следует, что  $ac \div d$ . Значит,  $d \in \text{OD}(ac, b)$  и по Теореме 2  $f \div d$ .
- Из  $b \div f$  следует, что  $bc \div f$ . Значит,  $f \in \text{OD}(ac, bc)$ .
- По Теоремам 3 и 2,  $c = c(a, b) = (ac, bc) \div f$ .
- Следовательно,  $f \in \text{OD}(c, b)$  и по Теореме 2  $d \div f$ .
- Из  $d, f \in \mathbb{N}$ ,  $d \div f$  и  $f \div d$  следует, что  $d = f$ . □

## Свойство 3

Если  $a, b, c \in \mathbb{Z}$ ,  $(a, b) = 1$  и  $ac \div b$ , то  $c \div b$ .

**Доказательство.** По Свойству 2  $(c, b) = (ac, b) = b$  (последнее верно так как  $ac \div b$ ). Следовательно,  $c \div b$ . □

## Свойство 4

Пусть  $a_1, \dots, a_n, b_1, \dots, b_m \in \mathbb{Z}$ , причем  $(a_i, b_j) = 1$  для всех  $i \in \{1, \dots, n\}$  и  $j \in \{1, \dots, m\}$ . Тогда  $(a_1 \dots a_n, b_1 \dots b_m) = 1$ .

**Доказательство.** • Докажем, что  $(a_1 \dots a_k, b_j) = 1$  для всех  $j \in \{1, \dots, m\}$  и  $k \in \{1, \dots, n\}$  индукцией по  $k$ .

**База  $k = 1$ :** дано в условии.

**Переход  $k \rightarrow k + 1$ :**  $(a_1 \dots a_k a_{k+1}, b_j) = (a_1 \dots a_k, b_j) = 1$  по свойству 2 (так как  $(a_{k+1}, b_j) = 1$ ).

• Пусть  $A = a_1 \dots a_n$ . Докажем, что  $(A, b_1 \dots b_k) = 1$  для всех  $k \in \{1, \dots, m\}$  индукцией по  $k$ .

**База  $k = 1$ :** доказано выше.

**Переход  $k \rightarrow k + 1$ :**  $(A, b_1 \dots b_k b_{k+1}) = (A, b_1 \dots b_k) = 1$  по свойству 2 (так как  $(A, b_{k+1}) = 1$ ). □

## Простые числа

### Определение

- Натуральное число, имеющее ровно два натуральных делителя, называется **простым**.
- Натуральное число, имеющее более двух натуральных делителей, называется **составным**.
- Множество всех простых чисел обозначается  $\mathbb{P}$ .
- Если  $p \in \mathbb{P}$ , то натуральные делители числа  $p$  — это 1 и  $p$ .
- $1 \notin \mathbb{P}$ . Любое натуральное число, большее 1 — простое или составное.

### Определение

Пусть  $a \in \mathbb{N}$ . **Собственный делитель** числа  $a$  — это любой его делитель, отличный от 1.

### Свойство 1

Если  $a \in \mathbb{N}$  — составное, то существует разложение  $a = bc$ , где  $b, c \in \mathbb{N}$ ,  $a > b, c > 1$ .

**Доказательство.** • Составное число  $a$  имеет собственный делитель  $b < a$ . Тогда  $a = bc$ , где  $c \in \mathbb{N}$ . Очевидно,  $1 < c < a$ .



## Свойство 2

Пусть  $a \in \mathbb{N}$ ,  $a \neq 1$ , а  $d$  — минимальный собственный делитель  $a$ . Тогда  $d \in \mathbb{P}$ .

**Доказательство.** • По определению,  $d > 1$ .

• Предположим, что  $d$  — составное. По свойству 1 тогда  $d = bc$ , где  $d > b > 1$ .

• Из  $a \div d$  и  $d \div b$  следует, что  $a \div b$ . Значит,  $b < d$  — собственный делитель  $a$ , противоречие с выбором  $d$ . □

## Теорема 6

*Простых чисел бесконечно много.*

**Доказательство.** • Предположим противное, пусть  $\mathbb{P} = \{p_1, \dots, p_n\}$ .

• Пусть  $m = p_1 \dots p_n + 1$ , а  $q$  — наименьший собственный делитель  $m$ .

• По свойству 2 тогда  $q \in \mathbb{P}$ . Значит,  $q = p_i$  для некоторого  $i \in \{1, \dots, n\}$

• Так как  $m - 1 \div p_i$ ,  $(m, p_i) = (1, p_i) = 1$  (по свойству 2 НОДа). Значит,  $m \not\div p_i$ , противоречие. □

### Свойство 3

Пусть  $a \in \mathbb{Z}$ ,  $p \in \mathbb{P}$ . Тогда либо  $a \div p$ , либо  $(a, p) = 1$ .

**Доказательство.** • Так как  $d = (a, p) \in \mathbb{N}$  и  $p \div d$ , то  $d = 1$  или  $d = p$ .

• Во втором случае  $(a, p) = p$ , следовательно,  $a \div p$ . □

### Свойство 4

Пусть  $a_1, \dots, a_n \in \mathbb{Z}$  и  $p \in \mathbb{P}$  таковы, что  $a_1 \dots a_n \div p$ .  
Тогда существует такое  $i \in \{1, \dots, n\}$ , что  $a_i \div p$ .

**Доказательство.** • Предположим противное, пусть  $a_i \not\div p$  для всех  $i \in \{1, \dots, n\}$ . По Свойству 3 тогда  $(a_i, p) = 1$ .

• По Свойству 4 взаимно простых чисел, тогда и  $(a_1 \dots a_n, p) = 1$ . Значит,  $a_1 \dots a_n \not\div p$ . Противоречие. □

## Теорема 7

*Любое натуральное число  $a > 1$  раскладывается в произведение простых чисел. Такое разложение единственно с точностью до порядка сомножителей.*

**Доказательство.**  $\exists$ . Индукция. База  $a \in \mathbb{P}$  очевидна: подходит разложение  $a = a$ .

**Переход.** • Пусть  $a$  — составное, а для всех меньших чисел теорема доказана.

- Тогда  $a = bc$ , где  $1 < b, c < a$ . Следовательно,  $b = p_1 \dots p_n$  и  $c = q_1 \dots q_m$ .
- Тогда  $a = p_1 \dots p_n q_1 \dots q_m$  — искомое разложение.



! Предположим противное, пусть  $a = p_1 \dots p_n = q_1 \dots q_m$  — два разложения  $a$  в произведение простых, причем  $a$  — наименьшее натуральное число, для которого разложение в произведение простых неединственно.

- Из  $a = p_1 \dots p_n \dot{\vdots} q_1$  следует, что  $p_i \dot{\vdots} q_1$  для некоторого  $i \in \{1, \dots, n\}$ . НУО  $i = 1$ .
- Из  $p_1, q_1 \in \mathbb{P}$  и  $p_1 \dot{\vdots} q_1$  следует, что  $p_1 = q_1$  (единственным делителем простого  $p_1$ , большим 1, является само  $p_1$ ).
- Тогда  $a' = \frac{a}{p_1} = p_2 \dots p_n = q_2 \dots q_m$ . Но разложение  $a'$  в произведение простых единственно с точностью до порядка сомножителей, откуда следует, что разложение  $a$  — тоже единственно с точностью до порядка сомножителей. □

## Определение

**Каноническое разложение** — это представление натурального числа в виде  $n = p_1^{k_1} \dots p_s^{k_s}$ , где  $p_1, \dots, p_s \in \mathbb{P}$  различны.

## Определение

Для  $n \in \mathbb{N}$  обозначим через  $d(n)$  количество натуральных делителей  $n$ .

## Теорема 8

Пусть  $n = p_1^{k_1} \dots p_s^{k_s}$  — каноническое разложение. Тогда выполнены следующие утверждения.

- 1)  $n \vdots d$ , если и только если  $d = p_1^{\ell_1} \dots p_s^{\ell_s}$ , где  $0 \leq \ell_i \leq k_i$  для всех  $i \in \{1, \dots, s\}$ .
- 2)  $d(n) = (k_1 + 1) \dots (k_s + 1)$ .

**Доказательство.** 1)  $\Leftarrow$ . Очевидно.

$\Rightarrow$ . • Если  $n \vdots d$ , то  $d$  не может иметь простых делителей, кроме  $p_1, \dots, p_s$ . Следовательно,  $d = p_1^{\ell_1} \dots p_s^{\ell_s}$ .

• Если  $\ell_i > k_i$  для какого-то  $i \in \{1, \dots, s\}$ , то очевидно, что  $n \not\vdots d$ .

2) • Показатель степени простого числа  $p_i$  в каноническом разложении делителя  $d \mid n$  можно выбрать  $k_i + 1$  способами  $(0, 1, \dots, k_i)$ .

• Перемножаем количества вариантов для  $p_1, \dots, p_s$  и получаем доказываемую формулу. □

## Теорема 9

Пусть  $a_1, \dots, a_m \in \mathbb{N}$ ,  $p_1, \dots, p_s \in \mathbb{P}$  причем  $a_i = p_1^{k_{i,1}} \dots p_s^{k_{i,s}}$  для всех  $i \in \{1, \dots, m\}$  (некоторые из показателей могут быть равны 0). Тогда

$$(a_1, \dots, a_m) = p_1^{\min(k_{1,1}, \dots, k_{m,1})} \dots p_s^{\min(k_{1,s}, \dots, k_{m,s})}.$$

**Доказательство.** • По теореме 8,  $d \mid a_t$ , если и только если  $d = p_1^{\ell_1} \dots p_s^{\ell_s}$ , где  $\ell_j \leq k_{t,j}$  для всех  $j \in \{1, \dots, s\}$ .

• Следовательно,  $d \in \text{OD}(a_1, \dots, a_m)$ , если и только если  $d = p_1^{\ell_1} \dots p_s^{\ell_s}$ , где  $\ell_j \leq \min(k_{1,j}, \dots, k_{m,j})$  для всех  $i \in \{1, \dots, s\}$ .

• Теперь понятно, что наибольший элемент в  $\text{OD}(a_1, \dots, a_m)$  вычисляется в точности по формуле из условия. □

## Линейные диофантовы уравнения с двумя неизвестными

$$\bullet \quad ax + by = c, \quad (*)$$

где  $a, b, c \in \mathbb{Z}$  — константы,  $x, y \in \mathbb{Z}$  — неизвестные.

• Пусть  $d = (a, b)$ . Если  $c \not\vdots d$ , то  $(*)$  не имеет решений.

• Далее  $c \vdots d$ . Пусть  $a = da'$ ,  $b = db'$ ,  $c = dc'$ . Тогда уравнение  $(*)$  эквивалентно

$$a'x + b'y = c', \quad \text{где } (a', b') = 1. \quad (**)$$

• Существует линейное представление НОД:  $a'x_0 + b'y_0 = 1$ . Умножив на  $c'$ , получим  $a'(x_0c') + b'(y_0c') = c'$ .

### Теорема 10

*Решения уравнения  $(*)$  представляются в виде  $x = x_0c' + tb'$ ,  $y = y_0c' - ta'$ , где  $t \in \mathbb{Z}$ .*

**Доказательство.** • Будем работать с эквивалентным уравнением  $(**)$ . Проверим, что это действительно его решения:

$$a'(x_0c' + tb') + b'(y_0c' - ta') = a'(x_0c') + b'(y_0c') + a'tb' - b'ta' = c'.$$

- Пусть  $(x, y)$  — решение  $(*)$ . Тогда

$$a'x + b'y = c' = a'(x_0c') + b'(y_0c') \Rightarrow a'(x - x_0c') = b'(y_0c' - y).$$

- Тогда  $a'(x - x_0c') \div b'$ . Так как  $(a', b') = 1$ , откуда  $x - x_0c' \div b'$ . Пусть  $x - x_0c' = tb'$ .
- Аналогично,  $y_0c' - y \div a'$ . Пусть  $y_0c' - y = sa'$ .
- Тогда  $a'tb' = b'sa'$ , откуда  $s = t$ . □

## Идеалы в $\mathbb{Z}$

- Пусть  $m \in \mathbb{N}$ , тогда нетрудно проверить, что  $m\mathbb{Z} = \{mx : x \in \mathbb{Z}\}$  — идеал в  $\mathbb{Z}$ .

### Теорема 11

Пусть  $I$  — идеал в  $\mathbb{Z}$ . Тогда  $I = m\mathbb{Z}$ , где  $m \in \mathbb{N}_0$ .

**Доказательство.** • Если  $I = \{0\}$ , то подходит  $m = 0$ .  
Далее  $I \neq \{0\}$ .

- Пусть  $a \in I$ ,  $a \neq 0$ . Тогда и  $-a \in I$ . Одно из чисел  $a$  и  $-a$  — натуральное. Таким образом,  $I' = I \cap \mathbb{N} \neq \emptyset$ .
- Тогда существует минимальный элемент в  $I'$ , обозначим его  $m$ . Докажем, что  $I = m\mathbb{Z}$ .
- Предположим противное, пусть  $b \in I$ ,  $b \not\equiv m$ . Тогда  $b = mq + r$ , где  $0 < r < m$  (теорема о делении с остатком).
- Так как  $b, m \in I$ , имеем  $r = b - mq \in I$ . Тогда  $r \in I'$ . Противоречие с минимальностью  $m$ . □

## Теорема 12

Пусть  $a_1, \dots, a_n \in \mathbb{Z} \setminus \{0\}$ . Тогда существует линейное представление  $(a_1, \dots, a_n)$ , а  $\text{OD}(a_1, \dots, a_n)$  состоит из всех делителей  $(a_1, \dots, a_n)$ .

**Доказательство.** • Пусть  $I = \langle \{a_1, \dots, a_n\} \rangle$ . Этот идеал состоит из линейных комбинаций чисел  $a_1, \dots, a_n$ .

• Очевидно,  $I \neq \{0\}$ . Тогда по Теореме 11 существует такое  $d \in \mathbb{N}$ , что  $I = d\mathbb{Z}$  — состоит из кратных  $d$ .

• Так как  $a_1, \dots, a_n \in I$ , все они делятся на  $d$ , значит,  $d \in \text{OD}(a_1, \dots, a_n)$ .

• С другой стороны,  $d \in I$ , а значит,  $d = x_1 a_1 + \dots + x_n a_n$ , где  $x_1, \dots, x_n \in \mathbb{Z}$ .

• Значит, для любого  $f \in \text{OD}(a_1, \dots, a_n)$  мы имеем  $d \mid f$ .

• Так как  $d > 0$ ,  $d$  — наибольший элемент в  $\text{OD}(a_1, \dots, a_n)$ , то есть,  $d = (a_1, \dots, a_n)$ .





## Определение

Пусть  $m \in \mathbb{N}$ ;  $a, b \in \mathbb{Z}$ . Будем говорить, что  $a$  **сравнимо** с  $b$  по модулю  $m$ , если  $a - b \div m$ . Обозначения:  $a \equiv_m b$  или  $a \equiv b \pmod{m}$ .

## Лемма 1

Пусть  $m \in \mathbb{N}$ ;  $a, b \in \mathbb{Z}$ . Следующие утверждения равносильны.

1°  $a \equiv b \pmod{m}$ .

2°  $a - b \div m$ .

3°  $a$  и  $b$  имеют одинаковые остатки от деления на  $m$ .

4°  $a \equiv b \pmod{m\mathbb{Z}}$ .

**Доказательство.** 1°  $\iff$  2° по определению сравнения.

2°  $\iff$  3° очевидно.

2°  $\iff$  4° по определению главного идеала  $m\mathbb{Z}$ . □

## Свойство 1

Если  $a \equiv_m a'$  и  $b \equiv_m b'$ ,  $a, x, y \in \mathbb{Z}$ , то  $ax + by \equiv_m a'x + b'y$ .

**Доказательство.**

$$ax + by - (a'x + b'y) = x(a - a') + y(b - b') \div m.$$



## Свойство 2

Если  $a \equiv_m a'$  и  $b \equiv_m b'$ , то  $ab \equiv_m a'b'$ .

**Доказательство.**  $ab - a'b' = (ab - a'b) + (a'b - a'b') = (a - a')b + a'(b - b') \div m.$



## Свойство 3

Если  $a \equiv_m b$  и  $n \in \mathbb{N}$ , то  $a^n \equiv_m b^n$ .

**Доказательство.** • Индукция по  $n$ . База  $n = 1$  очевидна.

• Переход  $n \rightarrow n + 1$ . Так как  $a^n \equiv_m b^n$  (по индукционному предположению) и  $a \equiv_m b$ , по свойству 2 имеем  $a^{n+1} = a^n \cdot a \equiv_m b^n \cdot b = b^{n+1}.$



## Свойство 4

Если  $(a, m) = 1$  и  $ab \equiv_m ac$ , то  $b \equiv_m c$ .

**Доказательство.**  $ab \equiv_m ac \Rightarrow a(b - c) \div m \Rightarrow b - c \div m \Rightarrow b \equiv_m c$  (по Свойству 3 взаимно простых чисел можно сократить на  $a$ ).



## Вычеты

- $\equiv_m$  — отношение эквивалентности, так как это частный случай сравнения по модулю идеала (впрочем, можно несложно проверить напрямую).

### Определение

**Вычет** по модулю  $m$  — это класс эквивалентности по  $\equiv_m$ .

- Перечислим тривиальные следствия Леммы 1.
- Каждый вычет по модулю  $m$  имеет вид  $a + m\mathbb{Z}$  для некоторого  $a \in \mathbb{Z}$ .
- В каждом вычете все числа имеют одинаковый остаток от деления на  $m$ , а числа из разных вычетов имеют разные остатки.
- Существует ровно  $m$  вычетов по модулю  $m$ .

### Определение

Числа  $a_1, \dots, a_m \in \mathbb{Z}$  — образуют **полную систему вычетов** по модулю  $m$  (сокращенно: **ПСВ (mod  $m$ )**), если каждый вычет по модулю  $m$  содержит ровно одно из них.

## Лемма 2

$a_1, \dots, a_m \in \mathbb{Z}$  — ПСВ  $(\text{mod } m)$ , если и только если никакие два из них не сравнимы по модулю  $m$ .

**Доказательство.**  $\Rightarrow$  очевидно следует из определения.

$\Leftarrow$ . Если есть  $m$  чисел, и никакие два из них не сравнимы по модулю  $m$ , то в каждом вычете по модулю  $m$  ровно одно из них.  $\square$

## Теорема 13

Пусть  $a_1, \dots, a_m$  — ПСВ  $(\text{mod } m)$ ,  $k, b \in \mathbb{Z}$ , причем  $(k, m) = 1$ . Тогда  $ka_1 + b, \dots, ka_m + b$  — ПСВ  $(\text{mod } m)$ .

**Доказательство.** • Достаточно проверить критерий из Леммы 2.

• Пусть  $ka_i + b \equiv_m ka_j + b \iff k(a_i - a_j) \dot{\div} m$ .

• Так как  $(k, m) = 1$ , это означает, что  $a_i - a_j \dot{\div} m \iff a_i \equiv_m a_j$ , что не так.  $\square$

## НОД вычета и модуля. Приведенная система вычетов

- Если  $a \equiv_m b$ , то  $a - b \vdots m$  и по свойству 2 НОД мы имеем  $(a, m) = (b, m)$ .
- Таким образом, для каждого вычета  $\bar{a} = a + m\mathbb{Z}$  корректно определен НОД  $(\bar{a}, m) := (a, m)$ .

### Определение

- 1) Вычет  $\bar{a}$  по модулю  $m$  называется **взаимно простым** с модулем  $m$ , если  $(\bar{a}, m) = 1$ .
  - 2) Для  $m \in \mathbb{N}$  **функция Эйлера**  $\varphi(m)$  — количество чисел от 1 до  $m$ , взаимно простых с  $m$ .
- !!!  $\varphi(1) = 1$ .
  - Существует ровно  $\varphi(m)$  вычетов по модулю  $m$ , взаимно простых с  $m$ .

### Определение

Числа  $a_1, \dots, a_{\varphi(m)}$  образуют **приведенную систему вычетов** по модулю  $m$ , (сокращенно: **ПрСВ**  $(\text{mod } m)$ ), если каждый вычет по модулю  $m$ , взаимно простой с  $m$ , содержит ровно одно из них.

### Лемма 3

$a_1, \dots, a_{\varphi(m)} \in \mathbb{Z}$  — ПрСВ  $(\text{mod } m)$ , если и только если все эти числа взаимно просты с  $m$  и никакие два из них не сравнимы по модулю  $m$ .

**Доказательство.**  $\Rightarrow$  очевидно следует из определения.

$\Leftarrow$ . Есть  $\varphi(m)$  чисел, и никакие два из них не сравнимы по модулю  $m$ , а также есть ровно  $\varphi(m)$  вычетов в ПрСВ (взаимно простых с  $m$ ). Значит, в каждом вычете из ПрСВ ровно одно из этих чисел.  $\square$

### Теорема 14

Пусть  $a_1, \dots, a_{\varphi(m)}$  — ПрСВ  $(\text{mod } m)$ ,  $k \in \mathbb{Z}$ , причем  $(k, m) = 1$ . Тогда  $ka_1, \dots, ka_{\varphi(m)}$  — ПрСВ  $(\text{mod } m)$ .

**Доказательство.** • Достаточно проверить критерий из Леммы 3.

- Так как  $(k, m) = 1$  и  $(a_i, m) = 1$ , то  $(ka_i, m) = 1$  (для всех  $i \in \{1, \dots, \varphi(m)\}$ ).
- Если  $ka_i \equiv_m ka_j$ , то  $a_i \equiv_m a_j$  по Свойству 4 сравнений, что не так.  $\square$

## Теорема 15

Пусть  $m \in \mathbb{N}$ ,  $a \in \mathbb{Z}$ ,  $(a, m) = 1$ . Тогда  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

**Доказательство.** • Пусть  $r_1, \dots, r_{\varphi(m)}$  — ПрСВ  $\pmod{m}$ .

• По Теореме 14 тогда и  $ar_1, \dots, ar_{\varphi(m)}$  — ПрСВ  $\pmod{m}$ .

• Введем обозначения  $i_1, \dots, i_{\varphi(m)}$  так, что  $r_1 \equiv_m ar_{i_1}$ ,  $\dots$ ,  $r_{\varphi(m)} \equiv_m ar_{i_{\varphi(m)}}$  и  $\{1, \dots, \varphi(m)\} = \{i_1, \dots, i_{\varphi(m)}\}$ .

• Пусть  $R = r_1 \cdots r_{\varphi(m)}$ . Тогда  $(R, m) = 1$ .

• Перемножая записанные выше сравнения, получаем

$$R \equiv r_1 \cdots r_{\varphi(m)} \equiv ar_1 \cdots ar_{\varphi(m)} \equiv a^{\varphi(m)} \cdot R \pmod{m}.$$

Сокращая на  $R$ , получаем  $1 \equiv a^{\varphi(m)} \pmod{m}$ . □

## Функция Эйлера

### Лемма 4

Функция Эйлера *мультипликативна*, то есть, если  $a, b \in \mathbb{N}$  взаимно просты, то  $\varphi(ab) = \varphi(a)\varphi(b)$ .

**Доказательство.** • Запишем числа от 1 до  $ab$  в таблицу  $a \times b$  так, что в первой строке — числа от 1 до  $a$ , во второй — от  $a + 1$  до  $2a$ , и т.д., в  $b$  строке — числа от  $(b - 1)a + 1$  до  $ba$ .

• Все числа в  $i$  столбце принадлежат одному вычету  $\bar{i} = i + a\mathbb{Z}$  по модулю  $a$ . Эти числа взаимно просты с  $a$ , если и только если  $(i, a) = 1$ .

• Вычеркнем все столбцы с номерами  $i$ , не взаимно простыми с  $a$ . Останутся ровно  $\varphi(a)$  столбцов.

• Все числа, взаимно простые с  $ab$ , должны быть взаимно простыми и с  $a$ , они лежат в оставшихся  $\varphi(a)$  столбцах.

• Рассмотрим любой оставшийся столбец, пусть числа в нем имеют вид  $j, a + j, \dots, (b - 1)a + j$ . Эти числа образуют ПСВ  $(\text{mod } b)$  в силу теоремы 13 (так как получены из ПСВ  $0, 1, \dots, b - 1$  умножением на  $a$ , взаимно простое с  $b$  и прибавлением  $j$ :  $0 \rightarrow j, 1 \rightarrow a + j, \dots, b - 1 \rightarrow (b - 1)a + j$ ).



- Значит, среди чисел  $j, a + j, \dots, (b - 1)a + j$  ровно  $\varphi(b)$  взаимно простых с  $b$ . Остальные числа точно не взаимно просты с  $ab$ , вычеркнем их.
- Оставшиеся  $\varphi(a)\varphi(b)$  чисел взаимно просты и с  $a$ , и с  $b$ , а значит, взаимно просты с  $ab$ . Значит, осталось ровно  $\varphi(ab)$  чисел (все числа от 1 до  $ab$ , взаимно простые с  $ab$ ).  $\square$

## Лемма 5

Если  $p \in \mathbb{P}$ ,  $n \in \mathbb{N}$ , то  $\varphi(p^n) = p^n - p^{n-1}$ .

**Доказательство.** • Посчитаем количество чисел от 1 до  $p^n$ , не взаимно простых с  $p^n$ .

- Пусть  $(a, p^n) = d > 1$ . Так как  $p^n \div d$ , должно быть  $d \div p$ .
- Следовательно, числа от 1 до  $p^n$ , не взаимно простые с  $p^n$  — это в точности числа от 1 до  $p^n$ , кратные  $p$ . Их количество равно  $\frac{p^n}{p} = p^{n-1}$ .  $\square$

## Теорема 16

Если  $n \in \mathbb{N}$  имеет каноническое разложение  $n = p_1^{k_1} \dots p_m^{k_m}$ , то

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_m}\right).$$

**Доказательство.** • Докажем индукцией по количеству простых делителей  $s$ , что  $\varphi(p_1^{k_1} \dots p_s^{k_s}) = \prod_{i=1}^s \varphi(p_i^{k_i})$ .

- База для  $s = 1$  очевидна.
- **Переход  $s \rightarrow s + 1$ .** Так как  $(p_1^{k_1} \dots p_s^{k_s}, p_{s+1}^{k_{s+1}}) = 1$ , по Лемме 4 и индукционному предположению имеем

$$\begin{aligned} \varphi(p_1^{k_1} \dots p_s^{k_s} \cdot p_{s+1}^{k_{s+1}}) &= \varphi(p_1^{k_1} \dots p_s^{k_s}) \cdot \varphi(p_{s+1}^{k_{s+1}}) = \\ &= \left( \prod_{i=1}^s \varphi(p_i^{k_i}) \right) \cdot \varphi(p_{s+1}^{k_{s+1}}) = \prod_{i=1}^{s+1} \varphi(p_i^{k_i}). \end{aligned}$$

- Следовательно,

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

## Теорема 17

Для любого  $n \in \mathbb{N}$

$$\sum_{d \in \mathbb{N}, d | n} \varphi(d) = n.$$

**Доказательство.** • Рассмотрим все  $\mathbb{N}$  числа от 1 до  $n$  — их как раз  $n$  штук. Каждое из них имеет НОД с  $n$  — и этот НОД — делитель  $n$ .

• Для любого  $d | n$  подсчитаем количество всех чисел из  $\{1, \dots, n\}$ , чей НОД с  $n$  равен  $d$ .

• Такие числа делятся на  $d$ , значит, их нужно искать среди  $d, 2d, \dots, n = \frac{n}{d}d$ . Так как

$$d = (kd, n) = (kd, \frac{n}{d}d) = d \cdot (k, \frac{n}{d}) \iff (k, \frac{n}{d}) = 1,$$

количество чисел из  $\{1, \dots, n\}$ , чей НОД с  $n$  равен  $d$  — это в точности количество таких  $k \in \{1, \dots, \frac{n}{d}\}$ , что  $(k, \frac{n}{d}) = 1$ , а это количество равно  $\varphi(\frac{n}{d})$ .

• Если  $d$  пробегает все натуральные делители  $n$ , то  $d' = \frac{n}{d}$  также пробегает все натуральные делители  $n$ . Поэтому,

$$n = \sum_{d \in \mathbb{N}, d | n} \varphi(\frac{n}{d}) = \sum_{d' \in \mathbb{N}, d' | n} \varphi(d').$$



## Кольцо вычетов

- Вычеты по модулю  $m \in \mathbb{Z}$  — они же вычеты по модулю идеала  $m\mathbb{Z}$  — образуют **кольцо вычетов**  $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ .

### Лемма 6

Обратимые элементы  $\mathbb{Z}_m$  — это в точности вычеты из ПрСВ  $(\text{mod } m)$ .

**Доказательство.** • Если  $\bar{a} \in \mathbb{Z}_m$  обратим, то существует такой  $\bar{b} \in \mathbb{Z}_m$ , что  $\bar{a}\bar{b} = \bar{1} \iff ab \equiv_m 1$ . Тогда  $(ab, m) = 1$ , а значит и  $(a, m) = 1$ .

• Наоборот, пусть  $(a, m) = 1$ . По Теореме 13 тогда  $0, a, 2a, \dots, (m-1)a$  — ПСВ  $(\text{mod } m)$ . Значит,  $\exists b : ab \equiv_m 1 \Rightarrow \bar{a}\bar{b} = \bar{1}$ . □

• Если вычет  $\bar{a}$  обратим, то **обратный вычет**  $(\bar{a})^{-1}$  единственен (это доказано в общем случае для кольца ранее, а в данном случае следует из доказательства Леммы 6).

### Теорема 18

Если  $p \in \mathbb{P}$ , то  $\mathbb{Z}_p$  — поле.

**Доказательство.** Так как все некрратные  $p$  числа взаимно просты с  $p$ , ПрСВ  $(\text{mod } p)$  — это все ненулевые вычеты. Тогда по Лемме 6, все ненулевые элементы  $\mathbb{Z}_p$  обратимы. □

- Пусть  $a \in \mathbb{Z}$ ,  $m \in \mathbb{N}$ , причем  $(a, m) = 1$ . Как найти обратный вычет  $a^{-1}$  ?
- Пусть  $r$  — остаток от деления  $a$  на  $m$ . Тогда  $0 \leq r < m$ .
- Если  $r = 0$ , то  $(a, m) > 1$  и обратного вычета не существует.
- Если  $r > 0$ , то с помощью алгоритма Евклида ищем  $d = (r, m) = (a, m)$ .
- Если  $d > 1$ , то обратного вычета не существует.
- Если  $d = 1$ , то при помощи (выполненного ранее) алгоритма Евклида ищем линейное представление НОД:  $1 = ax + my$ .
- Тогда  $ax \equiv 1 \pmod{m}$ , а значит,  $(\bar{a})^{-1} = \bar{x}$  в  $\mathbb{Z}_m$ .

- Пусть  $a, b \in \mathbb{Z}$ ,  $m \in \mathbb{N}$ . Нужно решить (относительно  $x$ ) сравнение

$$ax \equiv b \pmod{m}. \quad (*)$$

- Пусть  $d = (a, m)$ . Если  $b \not\vdots d$ , то очевидно,  $(*)$  решений не имеет.

- Если  $b \vdots d$ , то пусть  $a = a'd$ ,  $b = b'd$ ,  $m = m'd$ . Тогда

$$(*) \iff ax - b \vdots m \iff a'x - b' \vdots m' \iff a'x \equiv b' \pmod{m'}. \quad (**)$$

- Так как  $(a', m') = 1$ , существует обратный вычит  $(\overline{a'})^{-1}$  в  $\mathbb{Z}_{m'}$ .

- Пусть  $s \in (\overline{a'})^{-1}$ . Тогда  $x \equiv b's \pmod{m'}$  — решение сравнения  $(**)$ , а значит, и исходного сравнения  $(*)$ .

### Лемма 7

Пусть  $m_1, \dots, m_k$  — попарно взаимно простые натуральные числа,  $m = m_1 \dots m_k$ . Пусть  $b \in \mathbb{Z}$  таково, что  $b \div m_1, \dots, b \div m_k$ . Тогда  $b \div m$ .

**Доказательство.** Пусть  $n_\ell = m_1 \dots m_\ell$ . Докажем индукцией по  $\ell$ , что  $b \div n_\ell$ .

• База  $\ell = 1$  очевидна.

**Переход  $\ell \rightarrow \ell + 1$ .** • По индукционному предположению  $b = cn_\ell$ , где  $c \in \mathbb{Z}$ .

• Так как  $cn_\ell = b \div m_{\ell+1}$  и  $(n_\ell, m_{\ell+1}) = 1$ , по Свойству 3 взаимно простых чисел имеем  $c \div m_{\ell+1}$ .

• Тогда  $c = dm_{\ell+1}$  и  $b = dm_{\ell+1}n_\ell = dn_{\ell+1}$ . □

## Китайская теорема об остатках

## Теорема 19

Пусть  $m_1, \dots, m_k$  — попарно взаимно простые натуральные числа,  $m = m_1 \dots m_k$ ,  $a_1, \dots, a_k \in \mathbb{Z}$ . Тогда существует единственное такое  $a \in \{0, 1, \dots, m-1\}$ , что  $a \equiv_{m_1} a_1, \dots, a \equiv_{m_k} a_k$ .

**Доказательство.**  $\exists$ . • Пусть  $n_\ell = m_1 \dots m_\ell$ . Докажем индукцией по  $\ell$  существование такого  $b_\ell \in \mathbb{Z}$ , что  $b_\ell \equiv_{m_1} a_1, \dots, b_\ell \equiv_{m_\ell} a_\ell$ .

**База**  $\ell = 1$  очевидна.

**Переход**  $\ell \rightarrow \ell + 1$ . • Так как  $(m_{\ell+1}, n_\ell) = 1$  по Теореме 13 числа  $b_\ell, b_\ell + n_\ell, b_\ell + 2n_\ell, \dots, b_\ell + (m_{\ell+1} - 1)n_\ell$  — ПСВ  $(\text{mod } m_{\ell+1})$  (они получены из ПСВ  $0, 1, \dots, m_{\ell+1} - 1$  умножением на  $n_\ell$  и прибавлением  $b_\ell$ ).

• Значит, среди этих чисел есть число  $kn_\ell + b_\ell \equiv_{m_{\ell+1}} a_{\ell+1}$ .

Положим  $b_{\ell+1} := kn_\ell + b_\ell$ .

• Тогда  $b_{\ell+1} - a_{\ell+1} \vdots m_{\ell+1}$ .

• По построению  $b_{\ell+1} - b_\ell \vdots n_\ell$ . Так как по индукционному предположению  $b_\ell - a_i \vdots m_i$  для всех  $i \in \{1, \dots, \ell\}$ , мы имеем

$b_{\ell+1} - a_i = (b_{\ell+1} - b_\ell) + (b_\ell - a_i) \vdots m_i$



- Итак, мы получили число  $b_k$ , удовлетворяющее всем требованиям теоремы, кроме одного: число должно быть от 0 до  $m - 1$ .
- Для получения такого числа  $a$  поделим  $b_k$  с остатком на  $m$ : пусть  $b_k = mq + a$ ,  $0 \leq a \leq m - 1$ .
- Так как  $a - b_k \div m \div m_i$  и  $b_k - a_i \div m_i$ , то и  $a - a_i \div m_i$  для всех  $i \in \{1, \dots, k\}$ .

! • Предположим, что  $a$  и  $a'$  — два различных числа, удовлетворяющих условию. Тогда  $a - a' \div m_i$  для всех  $i \in \{1, \dots, k\}$ .

• Так как  $m_1, \dots, m_k$  попарно взаимно просты, по Лемме 7  $a - a' \div m = m_1 \dots m_k$ . Но  $|a - a'| < m$ , противоречие. □

• Из доказательства единственности в Теореме 19 видно, что все целые числа  $a$ , для которых  $a - a_i \div m_i$  при всех  $i \in \{1, \dots, k\}$  образуют в точности один вычет по модулю  $m = m_1 \dots m_k$ .

## Алгоритмы поиска решения для КТО

- Пусть  $m_1, \dots, m_k$  — попарно взаимно простые натуральные числа,  $m = m_1 \dots m_k$ ,  $a_1, \dots, a_k \in \mathbb{Z}$ .
- Мы ищем такое  $a$ , что  $a \equiv_{m_1} a_1, \dots, a \equiv_{m_k} a_k$  (\*)
- Будет использоваться алгоритм поиска обратного вычета, описанный выше.

## Алгоритм 1.

- Пусть  $m'_i = \frac{m_1 \dots m_k}{m_i}$ . Тогда  $(m'_i, m_i) = 1$ .  
 $b_i \in \{0, 1, \dots, m_i - 1\}$  — такое число, что  $b_i \cdot m'_i \equiv 1 \pmod{m_i}$   
 (мы найдем  $b_i$  с помощью алгоритма поиска обратного вычета).

## Утверждение

$a = a_1 b_1 m'_1 + a_2 b_2 m'_2 + \dots + a_k b_k m'_k$  — решение (\*).

**Доказательство.** Так как  $m'_j \vdots m_i$  при всех  $j \neq i$ , для любого  $i \in \{1, \dots, k\}$

$$a \equiv a_i b_i m'_i \equiv a_i \pmod{m_i}. \quad \square$$

- Как сказано выше, все решения системы (\*) — это в точности числа, сравнимые с  $a$  по модулю  $m$ .
- Поделив  $a$  на  $m$  с остатком, мы найдем решение системы среди чисел  $0, 1, \dots, m - 1$ .

## Алгоритм 2

- Индукцией по  $s$  найдем  $x_s$ , удовлетворяющее первым  $s$  сравнениям:

$$x_s \equiv_{m_1} a_1, \dots, x_s \equiv_{m_s} a_s.$$

- База  $s = 1$  очевидна: подойдет  $x_1 = a_1$ .

**Переход  $s \rightarrow s + 1$ .** • Пусть  $n_s = m_1 \dots m_s$ .

Будем искать решение в виде  $x_{s+1} = x_s + c_s n_s$ .

- Тогда  $x_{s+1} - x_s \equiv m_j$  для всех  $j \in \{1, \dots, s\}$ , поэтому,  $x_{s+1}$  удовлетворяет первым  $s$  сравнениям.

- Подберем  $c_s$  так, чтобы  $x_{s+1} \equiv a_{s+1} \pmod{m_{s+1}}$ :

$$\begin{aligned} x_s + c_s n_s &\equiv a_{s+1} \pmod{m_{s+1}} \iff c_s n_s \equiv a_{s+1} - x_s \\ &\pmod{m_{s+1}} \iff c_s \equiv (a_{s+1} - x_s) \cdot (n_s)^{-1} \pmod{m_{s+1}}. \end{aligned}$$

- Так как  $(n_s, m_{s+1}) = 1$ , обратный вычет  $(n_s)^{-1}$  существует и может быть найден с помощью описанного выше алгоритма.

- Второй алгоритм решения КТО на первый взгляд сложнее, чем первый, но требует применения  $k - 1$  алгоритмов поиска обратного вычета (а не  $k$ ): мы не ищем обратный вычет по модулю  $m_1$ .

- Поэтому, целесообразно нумеровать модули так, чтобы  $m_1$  оказался самым большим.

# Функция Мёбиуса

## Определение

Функция Мёбиуса  $\mu(n) :=$

$$\begin{cases} 1, & \text{если } n = 1, \\ (-1)^k, & \text{если } n = p_1 \dots p_k \text{ — произведение различных простых чисел,} \\ 0, & \text{если } n \text{ делится на квадрат простого числа.} \end{cases}$$

## Лемма 8

Пусть  $m, d \in \mathbb{N}$ ,  $m \vdots d$ . Тогда  $\sum_{d|n|m} \mu\left(\frac{m}{n}\right) = \begin{cases} 1, & m = d, \\ 0, & m > d. \end{cases}$

(суммирование ведется по всем  $n$ , кратным  $d$  и делящим  $m$ ).

**Доказательство.** • Пусть  $k := \frac{m}{d} = p_1^{t_1} \dots p_r^{t_r}$  — каноническое разложение. Тогда  $\sum_{d|n|m} \mu\left(\frac{m}{n}\right) = \sum_{s | \frac{m}{d} = p_1^{t_1} \dots p_r^{t_r}} \mu(s) =$

$$\sum_{s | p_1 \dots p_r} \mu(s) = \sum_{\ell=0}^r C_r^\ell (-1)^\ell = (1-1)^r$$

(так как ненулевое значение  $\mu$  достигается только на произведениях различных простых).

• Наша сумма равна 0 во всех случаях, кроме  $r = 0$  (а это в точности  $k = 1 \iff m = d$ ). В последнем случае сумма равна 1.

## Теорема 20

Пусть  $f, g : \mathbb{N} \rightarrow \mathbb{C}$ , причем  $f(m) = \sum_{d|m} g(d)$ . Тогда

$$g(m) = \sum_{n|m} \mu\left(\frac{m}{n}\right) f(n).$$

Доказательство.

$$\begin{aligned} \sum_{n|m} \mu\left(\frac{m}{n}\right) f(n) &= \sum_{n|m} \mu\left(\frac{m}{n}\right) \cdot \sum_{d|n} g(d) = \\ &= \sum_{d|m} \left( g(d) \cdot \sum_{d|n|m} \mu\left(\frac{m}{n}\right) \right) = g(m) \end{aligned}$$

по Лемме 8. □

## Функция Эйлера через формулу обращения Мёбиуса

## Теорема 21

Пусть  $n = p_1^{k_1} \dots p_s^{k_s}$  — каноническое разложение числа  $n$ .

Тогда  $\varphi(n) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_s})$ .

**Доказательство.** • По Теореме 17,  $\sum_{d \in \mathbb{N}, d | n} \varphi(d) = n$ .

• По Формуле обращения Мёбиуса,

$$\varphi(n) = \sum_{d \in \mathbb{N}, d | n} \mu(d) \cdot \frac{n}{d}.$$

• Напомним, что при  $d = p_{i_1} \dots p_{i_t}$  мы имеем  $\mu(d) = (-1)^t$  (здесь  $i_1, \dots, i_t$  — различные индексы),  $\mu(1) = 1$ , а в остальных случаях  $\mu(d) = 0$ . Поэтому,

$$\begin{aligned} \varphi(n) &= n - \sum_{1 \leq i \leq s} \frac{n}{p_i} + \sum_{1 \leq i_1 < i_2 \leq s} \frac{n}{p_{i_1} p_{i_2}} - \sum_{1 \leq i_1 < i_2 < i_3 \leq s} \frac{n}{p_{i_1} p_{i_2} p_{i_3}} + \dots = \\ &= n \left( 1 - \sum_{1 \leq i \leq s} \frac{1}{p_i} + \sum_{1 \leq i_1 < i_2 \leq s} \frac{1}{p_{i_1} p_{i_2}} - \sum_{1 \leq i_1 < i_2 < i_3 \leq s} \frac{1}{p_{i_1} p_{i_2} p_{i_3}} + \dots \right) = \\ &= n \left( 1 - \frac{1}{p_1} \right) \left( 1 - \frac{1}{p_2} \right) \dots \left( 1 - \frac{1}{p_s} \right). \quad \square \end{aligned}$$

# Формула обращения Мёбиуса. Мультипликативный вариант

## Теорема 22

Пусть  $K$  — поле,  $f, g : \mathbb{N} \rightarrow K \setminus \{0\}$ , причем  $f(m) = \prod_{d|m} g(d)$ .

Тогда  $g(m) = \prod_{n|m} f(n) \mu\left(\frac{m}{n}\right)$ .

Доказательство.

$$\begin{aligned} \prod_{n|m} f(n) \mu\left(\frac{m}{n}\right) &= \prod_{n|m} \left( \prod_{d|n} g(d) \right)^{\mu\left(\frac{m}{n}\right)} = \\ &= \prod_{d|m} g(d)^{\sum_{n|m} \mu\left(\frac{m}{n}\right)} = g(m) \end{aligned}$$

по Лемме 8. □

## Сумма мультипликативной функции по делителям числа

## Теорема 23

Пусть  $f : \mathbb{N} \rightarrow \mathbb{C}$  — мультипликативная функция,  
 $g(n) = \sum_{d|n} f(d)$ . Тогда  $g$  — мультипликативная функция.

**Доказательство.** • Пусть  $a, b \in \mathbb{N}$ ,  $(a, b) = 1$ .

•  $a = p_1^{k_1} \dots p_s^{k_s}$  и  $b = q_1^{\ell_1} \dots q_t^{\ell_t}$  — канонические разложения.

• Так как  $(a, b) = 1$ , все эти простые различны и  
 $ab = p_1^{k_1} \dots p_s^{k_s} q_1^{\ell_1} \dots q_t^{\ell_t}$  — каноническое разложение.

• По Теореме 8,  $d | ab \iff d = p_1^{k'_1} \dots p_s^{k'_s} q_1^{\ell'_1} \dots q_t^{\ell'_t}$ , где  $0 \leq k'_i \leq k_i$  для всех  $i \in \{1, \dots, s\}$  и  $0 \leq \ell'_j \leq \ell_j$  для всех  $j \in \{1, \dots, t\}$ .

• Следовательно,  $d = d_a d_b$ , где  $d_a | a$  и  $d_b | b$ , причем  $(d_a, d_b) = 1$  и такое представление единственно:

$d_a = p_1^{k'_1} \dots p_s^{k'_s}$  и  $d_b = q_1^{\ell'_1} \dots q_t^{\ell'_t}$ .



- Таким образом,

$$g(ab) = \sum_{d|ab} f(d) = \sum_{d_a|a} \sum_{d_b|b} f(d_a d_b) = \sum_{d_a|a} \sum_{d_b|b} f(d_a) f(d_b) =$$

$$\left( \sum_{d_a|a} f(d_a) \right) \left( \sum_{d_b|b} f(d_b) \right) = g(a)g(b). \quad \square$$

## Определение

Для  $n \in \mathbb{N}$   $\sigma(n)$  — сумма натуральных делителей  $n$ .

## Теорема 24

Если  $n = p_1^{k_1} \dots p_s^{k_s}$ , то  $\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \dots \frac{p_s^{k_s+1}-1}{p_s-1}$ .

**Доказательство.** • Пусть  $n_r = p_1^{k_1} \dots p_r^{k_r}$ .

• Докажем индукцией по  $r$ , что  $\sigma(n_r) = \frac{p_1^{k_1+1}-1}{p_1-1} \dots \frac{p_r^{k_r+1}-1}{p_r-1}$ .

**База** для  $r = 1$ : делители  $p_1^{k_1}$  — это  $1, p_1, \dots, p_1^{k_1}$  и по формуле суммы геометрической прогрессии их сумма равна  $\frac{p_1^{k_1+1}-1}{p_1-1}$ .

**Переход  $r \rightarrow r+1$ .** Так как  $(n_r, p_{r+1}^{k_{r+1}}) = 1$ , а по Теореме 23 функция  $\sigma(n) = \sum_{d|n} d$  мультипликативна,

$$\begin{aligned} \sigma(n_{r+1}) &= \sigma(n_r p_{r+1}^{k_{r+1}}) = \sigma(n_r) \sigma(p_{r+1}^{k_{r+1}}) = \\ &= \left( \frac{p_1^{k_1+1}-1}{p_1-1} \dots \frac{p_r^{k_r+1}-1}{p_r-1} \right) \frac{p_{r+1}^{k_{r+1}+1}-1}{p_{r+1}-1}. \quad \square \end{aligned}$$

## Первообразные корни из 1 в $\mathbb{C}$

### Определение

Пусть  $n \in \mathbb{N}$ . Число  $\varepsilon \in \mathbb{C}$  такое, что  $\varepsilon^n = 1$ , но  $\varepsilon^k \neq 1$  при натуральных  $k < n$  называется *первообразным корнем из 1* степени  $n$ .

- Пусть  $\varepsilon_0, \dots, \varepsilon_{n-1}$  — все корни степени  $n$  из 1,  
 $\varepsilon_k = (\cos(\frac{2\pi k}{n}), \sin(\frac{2\pi k}{n}))$ .

### Теорема 25

- Существует в точности  $\varphi(n)$  первообразных корней степени  $n$  из 1, это в точности такие корни  $\varepsilon_j$ , что  $(j, n) = 1$ .
- Если  $\varepsilon_j$  — первообразный корень степени  $n$  из 1, то  $\varepsilon_j, \varepsilon_j^2, \dots, \varepsilon_j^n$  — все корни степени  $n$  из 1.

**Доказательство.** • По формуле Муавра,  $\arg(\varepsilon_j^k) = \frac{2\pi kj}{n}$ .  
Разберем два случая.

**Случай 1:**  $(j, n) = d > 1$ .

- Тогда  $m = \frac{n}{d} \in \mathbb{N}$ ,  $m < n$  и  $y = \frac{j}{d} \in \mathbb{Z}$ .
- Следовательно,  $\arg(\varepsilon_j^m) = \frac{2\pi mdy}{md} = 2\pi y$  и  $\varepsilon_j^m = 1$ . Это означает, что  $\varepsilon_j$  не является первообразным корнем из 1 степени  $n$ .

Случай 2:  $(j, n) = 1$ .

- Тогда аргументы  $\varepsilon_j, \varepsilon_j^2, \dots, \varepsilon_j^{n-1}, \varepsilon_j^n$  — это  $\frac{2\pi j}{n}, \dots, \frac{2\pi nj}{n}$ .
- По Теореме 13, числа  $j, 2j, \dots, nj$  — ПСВ  $(\text{mod } n)$ .  
Значит, среди их остатков от деления на  $n$  каждый встречается ровно один раз.
- Тогда  $\frac{2\pi \cdot j}{n}, \frac{2\pi \cdot 2j}{n}, \dots, \frac{2\pi \cdot nj}{n}$  — это в точности такие аргументы, как  $\frac{2\pi}{n}, \frac{4\pi}{n}, \dots, \frac{2n\pi}{n}$  (напомним, что аргумент не меняется при прибавлении  $2\pi$ ).
- Это означает, что  $\varepsilon_j, \varepsilon_j^2, \dots, \varepsilon_j^{n-1}, \varepsilon_j^n$  — это в точности  $\varepsilon_0, \dots, \varepsilon_{n-1}$  — все корни степени  $n$  из 1.
- Понятно, что  $\varepsilon_j^n = 1$ , значит, в меньших степенях  $\varepsilon_j$  не равен 1, то есть, это первообразный корень степени  $n$  из 1. □