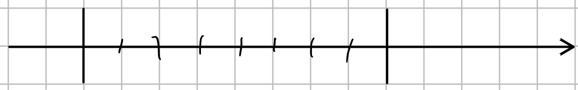
11.11.25 — Теория чисел

$\frac{a}{b}$ - ? $\quad a \in \mathbb{Z}, \; b \in \mathbb{N}$

$a = b a + r, \quad 0 \le r < b$



$1+1+1+\ldots+1 > a$

$НОД(a,b) = c$	$НОД(a,b,c) = d$
1. $c \mid a, \; c \mid b$ 2. $d \mid a, \; d \mid b \Rightarrow d \mid c$	1. $d \mid a, \; d \mid b, \; d \mid c$ 2. $h \mid a, \; h \mid b, \; h \mid c \Rightarrow h \mid d$
$НОД(a,b) = (a,b)$	$НОД(a,b,c) = (a,b,c)$

$НОК(a,b) = c$
1. $a \mid c, \; b \mid c$ 2. $a \mid d, \; b \mid d \Rightarrow c \mid d$
$НОК(a,b) = [a,b]$

$a = b s_1 + r_1 \qquad 0 \le r_1 < b \qquad (a, b) = (b, r_1) = (r_1, r_2) = \ldots$

$b = r_1 s_2 + r_2 \qquad 0 \le r_2 < r_1$

$r_1 = r_2 s_3 + r_3 \qquad \ldots$

Обобщённый алгоритм Евклида

$(a_1, a_2, \ldots, a_k)$

1. На 1-е место $\min a_i$
2. $a_i, \; i > 1$ на остаток от деления на a_1
3. „0" убрать

Пример. $(12, 15, 24, 6) \Rightarrow (6, 12, 15, 24) \Rightarrow (6, 0, 3, 0) \Rightarrow$
$\Rightarrow (3, 6) \Rightarrow (3, 0) \Rightarrow (3)$

Опр. $(a, b) = 1$ | $(a, b, c) = 1$

a, b – взаимно простые (ВП) | a, b, c – взаимно простые

Пример. $(6, 9, 4)$

$(6, 9) = 3$, $(6, 4) = 2$, но $(6, 9, 4) = 1$

не ВП, не ВП, ВП

Опр. $(a, b, c) = 1$

a, b, c – попарно ВП $\Leftrightarrow (a_i, a_j) = 1$, $i \neq j$

Диофантовы уравнения

$ax + by = c$ $\quad a, b, c \in \mathbb{Z}$ $\quad x, y \in \mathbb{Z}$

Пример.

$x + y = 1$

Реш $= \{(1, 0), (0, 1) \dots\}$

$\underset{\text{even}}{2x} + \underset{\text{odd}}{4y = 3} \Rightarrow$ Реш $= \varnothing$

Теорема

$ax + by = c$ $\quad (x_0, y_0)$ – решение

$(a, b) \mid c \Rightarrow X = X_0 + \frac{b}{(a,b)} t, \quad Y = Y_0 - \frac{a}{(a,b)} t, \quad t \in \mathbb{Z}$

$(a, b) \nmid c \Rightarrow$ нет реш.

$ax_0 + by_0 = c \quad a\left(X_0 + \frac{b}{(a,b)} t\right) + b\left(Y_0 - \frac{a}{(a,b)} t\right) = c$

$ax_0 + \cancel{\frac{ab}{(a,b)} t} + bY_0 - \cancel{\frac{ab}{(a,b)} t} = aX_0 + bY_0 = c$

Пример.

$-23x + 79y = 2$

$23; 79$

$(23, 79) = 1$

$79 = 23 \cdot 3 + 10$

$23 = 10 \cdot 2 + 3$

$10 = 3 \cdot 3 + 1$

$3 = 1 \cdot 3 + 0$

$a = 79; \quad b = 23$

$10 = a - 3b$

$b = 2(a - 3b) + 3$

$3 = -2a + 7b$

$1 = 7 \cdot 79 - 24 \cdot 23 \quad | \cdot 2$

$2 = 14 \cdot 79 - 48 \cdot 23$

$X_0 = 48, \quad Y_0 = 14$

Ответ: $\begin{cases} X = 48 + 79t \\ Y = 14 + 23t \end{cases} \quad t \in \mathbb{Z}$

$a - 3b = 3(-2a + 7b) + 1$

$(a, b) = 1 = 7a - 24b$

Простое, составное число

Опр

p – простое $\Rightarrow 1 | p, \; p | p$

Решето Эратосфена

2 3 $\cancel{4}$ 5 $\cancel{6}$ 7 $\cancel{8}$ $\cancel{9}$ $\cancel{10}$

Теорема

n – простое ?

$n / 2, \; n / 3, \; n / 5, \; \ldots, \; n / \sqrt{n}$

2 – един. чёт

3, 5   5, 7   17, 19

$p, \; p+2$ – простые – беск. кол-во

$p, \; 2p+1$ – простые   3, 7 ?

Теорема. Простых ∞ много

$\blacktriangle \; p_1, p_2, p_3, \ldots, p_k$ ← По индукции

$p_1, p_2, \ldots, p_{k+1} \; \blacktriangle$

$\pi(x)$ – кол-во простых чисел $\alpha \le x$

$\pi(10) = 4; \quad \pi(13) = 6; \quad \pi(100) = 25$

$\pi(x) \underset{x \to +\infty}{\sim} \dfrac{x}{\ln x}$

$n! + 2, \; n! + 3, \; \ldots, \; n! + n \; \leftarrow n - 1$ сост. число подряд

Мультипликативные функции

$\Theta(x)$

$\forall (m,n)=1 \quad \Theta(mn)=\Theta(m)\,\Theta(n)$

$\varphi(n)$ – функция Эйлера

$\varphi(n) = Len([m_i]) : \; m_i \le n, \; (m_i, n)=1$

$\boxed{\varphi(5) = 4 \qquad \varphi(6) = 2}$

1) $\varphi(1) = 1$

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

3) $\varphi(p^k) = p^k - p^{k-1}$

4) $\varphi(n) = n\prod\left(1-\frac{1}{p}\right) \quad p|n$

$$\boxed{\varphi(1000) = \varphi(2^3\cdot 5^3) = 1000\cdot\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 1000\cdot\frac{1\cdot 4}{10} = 400}$$

$$\varphi(p^\alpha, p_2^\beta) = \varphi(p_1^\alpha)\cdot\varphi(p_2^\beta) = (p_1^\alpha - p_1^{\alpha-1})(p_2^\beta - p_2^{\beta-1}) =$$

$$= p_1^\alpha\left(1-\frac{1}{p_1}\right)p_2^\beta\left(1-\frac{1}{p_2}\right) = p_1^\alpha p_2^\beta\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)$$