

Линейные диофантовы уравнения и КТО

1. Критерий разрешимости

Фиксированные $a, b, c \in \mathbb{Z}$, неизвестные $x, y \in \mathbb{Z}$, уравнение $ax + by = c$.

Это уравнение имеет решение $\Leftrightarrow c : (a, b)$.

Решение имеет вид $x = x_0 + \frac{b}{(a, b)} \cdot w$, $y = y_0 - \frac{a}{(a, b)} \cdot w$, параметр $w \in \mathbb{Z}$.

Аналогично, уравнение $ax + by + \dots = c$ имеет решение $\Leftrightarrow c : (a, b, \dots)$.

2. Теорема Сильвестра

Пусть $a, b \in \mathbb{N}$, $a \perp b$. Наибольшее c , для которого уравнение $ax + by = c$ не имеет решений $x, y \in \mathbb{N} \cup \{0\}$, имеет вид $c = ab - a - b$.

□ «не имеет» $ax + by = ab - a - b \Rightarrow x + 1 : b, y + 1 : a \Rightarrow$

$\Rightarrow x \geq b - 1, y \geq a - 1 \Rightarrow ax + by \geq 2ab - a - b$ ⚡

«наибольшее» Пусть $c \geq ab - a - b + 1$.

$\exists x \in \{0, 1, \dots, b - 1\} : c - ax : b$. Пусть $c - ax = by, y \in \mathbb{Z}$.

$x \leq b - 1 \Rightarrow c - ax \geq (ab - a - b + 1) - a(b - 1) = -b + 1 > -b \Rightarrow y \geq 0$. ■

3. Китайская теорема об остатках

Пусть m_1, m_2, \dots, m_n — попарно взаимно простые натуральные числа, b_1, b_2, \dots, b_n — произвольные целые числа. Система сравнений

$$x \equiv_{m_1} b_1, \quad x \equiv_{m_2} b_2, \quad \dots, \quad x \equiv_{m_n} b_n$$

имеет единственное по модулю $m_1 m_2 \dots m_n$ решение.

□ **Существование.** Пусть $M = m_1 m_2 \dots m_n$, $m'_k = M/m_k$ и $f_k m'_k \equiv_{m_k} 1$.

Тогда $x_0 = b_1 f_1 m'_1 + b_2 f_2 m'_2 + \dots + b_n f_n m'_n$ является решением.

Единственность. x_1 и x_2 — решения $\Rightarrow x_1 - x_2 : m_1, m_2, \dots, m_n \Rightarrow x_1 \equiv_{m_1 m_2 \dots m_n} x_2$. ■

□ Рассмотрим $\begin{cases} x \equiv_k a, \\ x \equiv_\ell b \end{cases}$ ($k \perp \ell$). Тогда $ks + a = x = \ell t + b$, т.е. $ks - \ell t = b - a$.

Это уравнение имеет решение $s = c + \ell u$ (фиксированное $c \in \mathbb{Z}$, любое $u \in \mathbb{Z}$).

Тогда $x = d + k\ell u$ (фиксированное $d \in \mathbb{Z}$), т.е. $x \equiv_{k\ell} d$. ■