Практика 9
(теория чисел)

Владимир Латыпов
donrumata03@gmail.com

Vladimir Latypov
donrumata03@gmail.com

Содержание

5 Число решений 3
13 Выражение через линейные комбинации 4

5 Число решений

Напоминалочка 5.1 *(memorizer 1: Класс решений)*

$$(x_0 + k \cdot \mathrm{d}x, y_0 + k \cdot \mathrm{d}y)$$

, где $\mathrm{d}x = \frac{b}{\gcd(a,b)}$, $\mathrm{d}y = -\frac{a}{\gcd(a,b)}$

Условие 5.2 Найдите число решений диофантового уравнения $ax + by = c$, в которых $|x|, |y| \leq M$.

Найдём отрезок $[l_x, r_x]$ значений k, при которых $-M \leq x_0 + k \cdot \mathrm{d}x \leq M$:

$$l_x = \frac{\lceil -M - x_0 \rceil}{\mathrm{d}x}$$

$$r_x = \frac{\lfloor M - x_0 \rfloor}{\mathrm{d}x}$$

PS: если $\mathrm{d}x$ отрицательный, $\longrightarrow$ поставим минусы

Аналогично для y получаем $\left[l_y, r_y\right]$.

Тогда ответом будет $\max\left(0, \min\left(r_x, r_y\right) - \max\left(l_x, l_y\right) + 1\right)$.

13 Выражение через линейные комбинации

Условие 13.3 Есть массив a_i. Найти максимальное y, для которого существуют x и b_i такие, что $a_i = x + y \cdot b_i$.

Теорема 13.4 *(theorem 4: Эквивалентная переформулировка)* Нужно найти максимальный модуль, по которому a_i сравнимы

Доказательство Если зафиксирован y, то существование $x, \{b_i\} \Longleftrightarrow a_i \underset{y}{\equiv} a_j \underset{y}{\equiv} a_0$, так как

- Если нашли, $x, \{b_i\}$, то $\forall i : x \bmod y \underset{y}{\equiv} a_i = x + y \cdot b_i$
- Если $\forall i : c \underset{y}{\equiv} a_i$, то для $a_i = x + y \cdot b_i$ возьмём

$$\begin{cases} x := c \\ b_i = \frac{a_i - c}{y} \end{cases}$$

□

Введём $a_i' = a_i - a_0$

Очереная переформулировка: нужно найти максимальный модуль, по которому a_i' сравнимы с 0, aka делятся на этот модуль.

Тогда ответом будет $\gcd(\{a_i'\})$.