Билет 5. НОД, НОК, Алгоритм Евклида

Определение

Общий делитель — всякое целое, делящее одновременно целые $a, b, \ldots, l$.
Наибольший общий делитель (НОД) — наибольший из всех общих делителей. Обозначается $(a, b, \ldots, l)$.

Определение

Взаимно простые — если $(a, b, \ldots, l) = 1$
Попарно простые — если $\forall i, j, i \neq j : (x_i, x_j) = 1$

Замечание: Попарно простые всегда являются взаимно простыми. Для случая двух чисел понятия совпадают.

Теорема

Если $a = bq + r$, то $(a, b) = (b, r)$

Доказательство

Доказательство:
Пусть $(a, b) = k$. Тогда a и b делятся на k, значит bq делится на k, следовательно $r = a - bq$ также делится на k.
С другой стороны, пусть $(b, r) = t$. Тогда b и r делятся на t, значит bq делится на t, следовательно $a = bq + r$ также делится на t.
Предположим, что $t > k$ (или $t < k$), но так как k (t) — НОД, получаем противоречие. Следовательно, $t = k$.

Алгоритм

Алгоритм Евклида
Пусть a и b — положительные целые, $a > b$. Тогда:

$$
\begin{aligned}
a &= b \cdot q_1 + r_2, & 0 < r_2 < b \\
b &= r_2 \cdot q_2 + r_3, & 0 < r_3 < r_2 \\
r_2 &= r_3 \cdot q_3 + r_4, & 0 < r_4 < r_3 \\
&\vdots \\
r_{n-2} &= r_{n-1} \cdot q_{n-1} + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n \cdot q_n + 0
\end{aligned}
$$

Тогда $(a, b) = r_n$

$$(a, b) = (b, r_2) = (r_2, r_3) = \dots = (r_{n-1}, r_n) = r_n$$

Пример: Найдём $(1071, 462)$

$$
\begin{array}{llll}
\boxed{1071,\ 462} & 1071 = 462 \cdot 2 + 147 & & \\
& \boxed{462,\ 147} & 462 = 147 \cdot 3 + 21 & \\
& & \boxed{147,\ 21} & 147 = 21 \cdot 7 + 0 \\
& & & \boxed{21}
\end{array}
$$

$$(1071, 462) = 21$$

Определение

Наименьшее общее кратное (НОК) — всякое целое, кратное всем данным числам. Рассматриваем только положительные общие кратные.
Связь НОД и НОК:

$$\text{НОК}(a, b) = \frac{a \cdot b}{\text{НОД}(a, b)}$$

Теорема

Свойства НОД:

1. $(a, b) = (b, a)$ (коммутативность)
2. $(a, (b, c)) = ((a, b), c)$ (ассоциативность)
3. $(ac, bc) = c \cdot (a, b)$
4. Если $(a, b) = 1$, то $(ac, b) = (c, b)$

Сложность алгоритма Евклида: $O(\log(\min(a, b)))$

Обоснование: На каждой итерации один из аргументов уменьшается хотя бы в 2 раза.