

# НОД, НОК, Алгоритм Евклида

ceagest

## 1 Наибольший общий делитель

**Определение 1.1.** Всякое целое, делящее одновременно целые  $x_1, x_2, \dots, x_n$ , называется их общим делителем. Наибольший из всех общих делителей — наибольший общий делитель. Обозначение:  $(x_1, x_2, \dots, x_n)$ .

**Определение 1.2.** Если  $(x_1, x_2, \dots, x_n) = 1$ , то  $x_1, x_2, \dots, x_n$  называются взаимно простыми.

**Определение 1.3.** Если для  $x_1, x_2, \dots, x_n \quad \forall i, j : i \neq j \quad \hookrightarrow \quad (x_i, x_j) = 1$ , то  $x_1, x_2, \dots, x_n$  называются попарно взаимно простыми.

## 2 Алгоритм Евклида

**Теорема 2.1.** Если  $a = bq + r$ , то  $(a, b) = (b, r)$ .

*Доказательство.* Пусть  $(a, b) = k$ . Тогда и  $a$  и  $bq$  делятся на  $k$ , но тогда и  $r$  делится на  $k$ .

С другой стороны, пусть  $(b, r) = k_1$ . Тогда из аналогичных рассуждений  $a$  делится на  $k_1$ .

Предположим, что  $k \neq k_1$ . Без ограничения общности  $k_1 > k$ . Но тогда  $(a, b) \geq k_1 > k \implies$  получаем противоречие с тем, что  $k$  — наибольший из всех общих делителей  $a$  и  $b$ .  $\square$

**Алгоритм Евклида.** Пусть  $a$  и  $b$  — положительные целые,  $a > b$ . Тогда получим систему равенств:

$$\begin{cases} a = bq_1 + r_1, & 0 \leq r_1 < b \\ b = r_1q_2 + r_2, & 0 \leq r_2 < r_1 \\ r_1 = r_2q_3 + r_3, & 0 \leq r_3 < r_2 \\ \vdots \end{cases}$$

Этот ряд можно продолжать, пока не получим 0. Из теоремы 2.1 имеем:

$$(a, b) = (b, r_1) = (r_1, r_2) = \dots = (r_{n-1}, r_n) = \dots = (r, 0) = r$$

Из равенств выше легко видеть, что  $r$  есть искомый НОД  $a$  и  $b$ .

---

### Algorithm 1 Алгоритм Евклида

---

```
1: function GCD( $n, m$ )
2:   while  $n > 0$  and  $m > 0$  do
3:     if  $n > m$  then
4:        $t \leftarrow m$ 
5:        $m \leftarrow n \% m$ 
6:        $n \leftarrow t$ 
7:     else
8:        $t \leftarrow n$ 
9:        $n \leftarrow m \% n$ 
10:       $m \leftarrow t$ 
11:   return  $\max(n, m)$ 
```

---

### 3 Наименьшее общее кратное

**Определение 3.1.** *Наименьшее из всех целых, делящихся одновременно на целые  $x_1, x_2, \dots, x_n$ , называется наименьшим общим кратным  $x_1, x_2, \dots, x_n$ . Обозначение:  $[x_1, x_2, \dots, x_n]$ .*