

## Лекция №2 (10.09.20)

### 1. Теория делимости.

#### 1.3. Алгоритм Евклида.

Пусть  $a$  и  $b$  – два целых числа, наибольший общий делитель которых нужно найти. Поскольку  $\text{НОД}(|a|, |b|) = \text{НОД}(a, b)$ , то предположим, что  $a \geq b > 0$ .

1. Применим алгоритм деления к  $a$  и  $b$ , чтобы получить

$$a = q_1b + r_1, 0 \leq r_1 < b.$$

Если  $r_1 = 0$ , значит  $b|a$  и  $\text{НОД}(a, b) = b$ . Если  $r_1 \neq 0$ , то делим  $b$  на  $r_1$  для получения целых чисел  $q_2$  и  $r_2$ , удовлетворяющих условию

$$b = q_2r_1 + r_2, 0 \leq r_2 < r_1.$$

Если  $r_2 = 0$ , то алгоритм завершён; в противном случае, действуем так же, как и раньше, чтобы получить

$$r_1 = q_3r_2 + r_3, 0 \leq r_3 < r_2.$$

2. Процесс деления продолжается до тех пор, пока не появится некоторый нулевой остаток, например, на  $(n + 1)$ -шаге, где  $(r_n - 1)|r_n$  (нулевой остаток возникает в любом случае, поскольку убывающая последовательность  $b > r_1 > r_2 > \dots \geq 0$  не может содержать более  $b$  целых чисел).

3. В результате получается следующая система уравнений:

$$\begin{aligned} a &= q_1b + r_1, 0 \leq r_1 < b, \\ b &= q_2r_1 + r_2, 0 \leq r_2 < r_1, \\ r_1 &= q_3r_2 + r_3, 0 \leq r_3 < r_2, \\ &\vdots \\ r_{n-2} &= q_n r_n + r_n, 0 \leq r_n < r_{n-1}, \\ r_{n-1} &= q_n + 1r_n + 0. \end{aligned}$$

Мы утверждаем, что  $r_n$  – последний ненулевой остаток, равный  $\text{НОД}(a, b)$ .

**Лемма 1.** Если  $a = qb + r$ , значит  $\text{НОД}(a, b) = \text{НОД}(b, r)$ .

Используя результаты этой леммы, работу алгоритма можно упростить:

$$\text{НОД}(a, b) = \text{НОД}(b, r_1) = \dots = \text{НОД}(r_{n-1}, r_n) = \text{НОД}(r_n, 0) = r_n.$$

Важным следствием алгоритма Евклида является следующая теорема.

**Теорема 1.** Если  $k > 0$ , то  $\text{НОД}(ka, kb) = k\text{НОД}(a, b)$ .

**Следствие 1.** Для любых целых  $k \neq 0$ ,  $\text{НОД}(ka, kb) = |k|\text{НОД}(a, b)$ .

**Определение 1.** Наименьшее общее кратное двух ненулевых целых чисел  $a$  и  $b$ , обозначаемое  $\text{lcm}(a, b)$ , является положительным целым числом  $m$ , удовлетворяющим

1.  $a|m$  и  $b|m$ ,
2. если  $a|c$  и  $b|c$ , при  $c > 0$ , то  $m \leq c$ .

**Теорема 2.** Для положительных целых  $a$  и  $b$ ,

$$\text{НОД}(a, b)\text{НОК}(a, b) = ab.$$

**Следствие 2.** Для целых  $a$  и  $b$ :  $\text{НОК}(a, b) = ab$  тогда и только тогда, когда  $\text{НОД}(a, b) = 1$ .

#### 1.4. Простейшие диофантовы уравнения $ax + by = c$ .

**Теорема 3.** Линейное диофантово уравнение  $ax + by = c$  имеет решение тогда и только тогда, когда  $d|c$ , где  $d = \text{НОД}(a, b)$ . Если  $x_0, y_0$  — частное решение исходного уравнения, то общее решение имеет вид:

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t$$

для  $t \in \mathbb{Z}$ .