1 | # НОД (наибольший общий делитель) и НОК. Алгоритм Евклида нахождения НОД.

Опр. Наибольшим общим делителем целых чисел $a, b \in \mathbb{Z}$ ~~$\setminus\{0\}$~~ над наибольшее целое число $c \in \mathbb{Z}$ т.ч. $c \mid a$ и $c \mid b$ (обозн. $НОД(a,b)$)

Замечание $НОД(0,0)$ не определен!

Аналогично, можно определить $НОД(a,b,c)$ и т.д.: $НОД(a_1, a_2, \dots, a_k)$ для произвольного $k \geq 2$ и $a_1, a_2, \dots, a_k \in \mathbb{Z}$ т.ч. $\exists i \in \overline{1,k}$ $(a_i \neq 0)$.

Опр. Целые числа $a, b \in \mathbb{Z}$ наз. **взаимно простыми** (обозн. $\boxed{(a,b) = 1}$), если $НОД(a,b) = 1$

Опр. ① Целые числа $a_1, a_2, \dots, a_k \in \mathbb{Z}$ наз. **взаимно простыми**, если $НОД(a_1, a_2, \dots, a_k) = 1$.

② Целые числа $a_1, a_2, \dots, a_k \in \mathbb{Z}$ наз. **попарно взаимно простыми**, если $НОД(a_i, a_j) = 1$ $\forall i, j \in \overline{1,k}$ т.ч. $i \neq j$.

Лемма $\forall a, b \in \mathbb{Z}$ т.ч. $a \neq 0 \vee b \neq 0$

$$\boxed{НОД(a,b) = НОД(a-b, b)}$$

◀ Пусть $m \in \mathbb{Z}$ т.ч. $m \mid a$ и $m \mid b$, тогда $m \mid (a-b)$.
Наоборот, пусть $m \in \mathbb{Z}$ т.ч. $m \mid (a-b)$ и $m \mid b$, тогда $m \mid (a-b)+b$, т.е. $m \mid a$.

Т.о., множество общих делителей a и b совпадает с мн-вом общих делителей $a-b$ и b, поэтому $НОД(a,b) = НОД(a-b, b)$ ▶

2) Теорема. Пусть $a = qb + r$, где $a, b, q, r \in \mathbb{Z}$, причем хотя бы одно из чисел a, b неравно 0. Тогда $\boxed{НОД(a,b) = НОД(b,r)}$

Док-во: используем предыдущую лемму: имеем
$НОД(a,b) = НОД(a-b,b) = НОД((a-b)-b,b) = НОД(a-2b,b) = \ldots = НОД(a-qb,b) = НОД(r,b) = НОД(b,r)$.

Док-но

На этой теореме основан алгоритм поиска наиб. общего делителя двух натур. чисел, который носит название алгоритма Евклида: пусть $a, b \in \mathbb{N}$ и требуется найти $НОД(a,b)$. Можно считать, для определенности, что $a \geq b$. Разделим с остатком a на b: получим $a = bq_1 + r_1$. По теореме, $НОД(a,b) = НОД(b,r_1)$. Если $r_1 = 0$, то $НОД(b,r_1) = b$, т.е. $НОД(a,b) = b$. Если же $r_1 \neq 0$, то разделим теперь с остатком b на r_1: пусть $b = r_1 q_2 + r_2$. По теореме, $НОД(b,r_1) = НОД(r_1,r_2)$. Если $r_2 = 0$ то искомый наиб. общий делитель найден ($= r_1$), если $r_2 \neq 0$, то разделим с остатком r_1 на r_2: $r_1 = r_2 q_3 + r_3$ и т.д.:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \end{aligned}$$

Т.к. $b > r_1 > r_2 \ldots$, то по опред. деления с остатком процесс конечен ($r_i \geq 0 \ \forall i$), т.е дает в качестве результата $НОД(a,b)$ за конечное число шагов.

3| Замечание: если $a, b \in \mathbb{Z} \setminus \{0\}$, то их наиб. общий делитель также можно определить, применив алгоритм Евклида к числам $|a|, |b| \in \mathbb{N}$, т.к. очевидно, что $\boxed{НОД(a,b) = НОД(|a|,|b|)}$

Важными следствиями из алгоритма Евклида явл следующие теоремы:

Теорема. Если $НОД(a,b) = d$, то существуют $u, v \in \mathbb{Z}$ т.ч. $\boxed{au + bv = d}$.

Док-во. Используем для нахождения d алгоритм Евклида:

$$\begin{aligned}
a &= bq_1 + r_1 \\
b &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
r_2 &= r_3 q_4 + r_4 \\
&\vdots \\
r_{n-4} &= r_{n-3} q_{n-2} + r_{n-2} \\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} \\
r_{n-2} &= r_{n-1} q_n + r_n \\
r_{n-1} &= r_n q_{n+1}.
\end{aligned} \qquad (*)$$

Последний ненулевой остаток r_n и равен $НОД(a,b)$. Перепишем равенства $(*)$ так, чтобы каждый остаток выражался через два предыдущих:

$$\begin{aligned}
r_1 &= a - bq_1 \\
r_2 &= b - r_1 q_2 \\
r_3 &= r_1 - r_2 q_3 \\
r_4 &= r_2 - r_3 q_4 \\
&\vdots
\end{aligned}$$

$$r_{n-2} = r_{n-4} - r_{n-3} q_{n-2}$$
$$r_{n-1} = r_{n-3} - r_{n-2} q_{n-1}$$
$$r_n = r_{n-2} - r_{n-1} q_n$$

Из двух последних равенств получим выражение r_n через r_{n-2} и r_{n-3}:

$$r_n = r_{n-2} - r_{n-1} q_n = r_{n-2} - (r_{n-3} - r_{n-2} q_{n-1}) q_n =$$
$$= r_{n-2}(1 + q_{n-1} q_n) - r_{n-3} q_n .$$

Аналогично, используя выражение r_{n-2} через r_{n-3} и r_{n-4}, получим выражение r_n через r_{n-3} и r_{n-4} и т.д. В итоге получим выражение r_n вида $au + bv$ для некоторых $u, v \in \mathbb{Z}$. Док-во.

Непосредственным следствием этой теоремы явл.

Теорема. Если a и b - взаимно простые числа, то существуют $u, v \in \mathbb{Z}$ т.ч.

$$\boxed{au + bv = 1}$$

Из этих теорем несложно получить в качестве следствия такие утверждения

Утв. Если $a \vdots c$, $b \vdots c$ и $d = НОД(a, b)$, то $d \vdots c$

◀ упр. ▶

Теорема. Если $(ab) \vdots c$ и $НОД(a, c) = 1$, то $b \vdots c$

◀ упр. ▶