№25 р.1 | Основы теории делимости: наибольший общий делитель, наименьшее общее кр-е, алгоритм Евклида

Def: d - НОД $a_1 \dots a_n$, если

1) d - общий делитель
2) d делится на любой общий делитель $a_1 \dots a_n$

Th (алгоритм Евклида)

Если
$$\begin{cases} a = b \cdot q_0 + r_1 & 0 \le r_1 < b, \\ b = r_1 \cdot q_1 + r_2 & 0 \le r_2 < r_1 \\ r_1 = r_2 \cdot q_2 + r_3 & \vdots \\ \vdots & \\ r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n & \\ r_{n-1} = r_n \cdot q_n & \end{cases}$$

То НОД$(a,b) = r_n$.

Сл-е Пусть $d =$ НОД$(a,b) \Rightarrow \exists\, u, v : d = a \cdot u + v \cdot b$.

Def m - НОК $a_1 \dots a_n$, если

1) m - общее кр-е
2) $\forall$ общее кр-е делится на m

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

Д-во.

Пусть M - общее кр-е a, b.

Тогда $M \vdots a \Rightarrow \exists k: M = a \cdot k$

$M \vdots b \Rightarrow ak \vdots b$. (1)

Пусть НОД$(a,b) = d$

Тогда $a = a_1 d \quad b = b_1 d$.

(1) $\Rightarrow a_1 d \cdot k \vdots b_1 d \Leftrightarrow k \vdots b_1$ (т.к. НОД$(a_1, b_1) = 1$)

Тогда $\exists\, t: k = t \cdot b_1$, $b_1 = \dfrac{b}{d}$

$M = ak = \dfrac{a \cdot b}{d} \cdot t$. НОК при $t = 1 \Rightarrow$ НОК $= \dfrac{a \cdot b}{d}$