

Еуклидов алгоритам

$\text{НЗД}(a, b)$ - највећи заједнички делилац укупних бројева $a, b \neq 0$

$$a = bq_1 + r_1, \quad 0 \leq r_1 < |b|$$

$$b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1$$

$$r_1 = r_2q_3 + r_3, \quad 0 \leq r_3 < r_2$$

$\vdots$

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, \quad 0 \leq r_{n-1} < r_{n-2}$$

$$r_{n-2} = r_{n-1}q_n + \boxed{r_n}, \quad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_nq_{n+1} + r_{n+1}, \quad 0 \leq r_{n+1} < r_n$$

} (*)

Остаци $r_1, r_2, \dots$ нису самог обликајући низ и сви су већи или једнаки од нуле:

$$0 \leq \dots r_{n+1} < r_n < \dots < r_2 < r_1.$$

Према томе, овај низ не може бесконачно да облика, иј. постоји $n \in \mathbb{N}$ тако да је $r_{n+1} = 0$.

Лема: Ако је $a = bq + r$, онда је $\text{НЗД}(a, b) = \text{НЗД}(b, r)$.

доказ:

S_1 - скуп заједничких делилаца елемената a и b

S_2 - скуп заједничких делилаца елемената b и r

Желимо да докажемо да је $S_1 = S_2$.

$S_1 \subseteq S_2$:

$$d \in S_1 \Rightarrow d \mid a \text{ и } d \mid b \Rightarrow d \mid \underbrace{a - bq}_{=r} \Rightarrow d \mid r$$

$d \in S_2$

$$S_2 \subseteq S_1:$$

$$d \in S_2 \Rightarrow d|b \text{ и } d|r \Rightarrow d|\underbrace{b_2+r}_{=a} \Rightarrow d|a$$

$$d \in S_1$$

Закне, $S_1 = S_2$, та је $\text{НЗД}(a, b) = \max S_1 = \max S_2 = \text{НЗД}(b, r)$.

Теорема: Последњи нетула остатак у процесу (*) је највећи заједнички делилац бројева a и b . □

доказ:

Нека је r_n последњи нетула остатак.

На основу прелиходне леме важи:

$$\begin{aligned} \text{НЗД}(a, b) &= \text{НЗД}(b, r_1) \\ &= \text{НЗД}(r_1, r_2) \\ &= \text{НЗД}(r_2, r_3) \\ &\vdots \\ &= \text{НЗД}(r_{n-1}, r_n). \end{aligned}$$

Како је $r_{n+1} = 0$, следи да је $r_{n-1} = r_n q_{n+1}$ та је $\text{НЗД}(r_{n-1}, r_n) = r_n$.

Закне, $\text{НЗД}(a, b) = r_n$. □

Обрнути Еуклидов алгоритам:

Твђење: Ако је $\text{НЗД}(a, b) = d$, онда постоје бројеви x и y такви да је $ax + by = d$.

доказ:

На основу Еуклидовог алгоритма:

$$d = r_n = r_{n-2} - r_{n-1} q_n,$$

односно $d = x_1 r_{n-2} + y_1 r_{n-1}$, за неке $x_1, y_1 \in \mathbb{Z}$.

Како је $r_{n-1} = r_{n-3} - r_{n-2}z_{n-1}$, из претходне једнакости
добивамо да је

$$d = x_2 r_{n-3} + y_2 r_{n-2}, \text{ за неке } x_2, y_2 \in \mathbb{Z}.$$

Настављајући на овај начин, показуемо да једнакости:

$$d = x_{n-1}b + y_{n-1}r_1 = \underbrace{x_n}_x a + \underbrace{y_n}_y b.$$

Закне, $d = xa + yb$.



Најмањи заједнички садржанац (НЗС)

Теорема: Нека су a и b природни бројеви. Тада важи да је $ab = \text{НЗД}(a, b) \cdot \text{НЗС}(a, b)$.

Доказ:

$$d = \text{НЗД}(a, b)$$

Тада је $a = da_0$ и $b = db_0$ за неке a_0, b_0 који су узajално прости природни бројеви.

Ако је $m = da_0b_0$, указујемо да је $\text{НЗС}(a, b) = m$.

Јасно је да $a|m$ и $b|m$ па је још употребом доказани да је m најмањи такав да је део a и b .

(јесће садржанац, указујемо да је најмањи).

Нека је n такође садржанац од a и b , пада је $n = ka = kda_0$ за неко $k \in \mathbb{N}$.

$$Како \quad b|n \Rightarrow b|kda_0 \Rightarrow db_0|kda_0 \Rightarrow b_0|ka_0 \Rightarrow b_0|k$$

$\uparrow$
 a_0 и b_0
узajално
прости

Закне, $m|n$ па је $\text{НЗС}(a, b) = m$.

$$\text{Тада је} \quad a \cdot b = da_0 \cdot db_0 = d \cdot \underbrace{da_0b_0}_m = \text{НЗД}(a, b) \cdot \text{НЗС}(a, b)$$

