Najväčší spoločný deliteľ

Najväčší spoločný deliteľ. Symbolom $\gcd(x, y)$ označime najväčšieho spoločného deliteľa celých čísel x a y. Operácia je definovaná nad oborom Z týmto vzťahom:

$$\gcd(x, y) = z \leftrightarrow (x \neq 0 \vee y \neq 0) \wedge z \mid x \wedge z \mid y \wedge \forall d(d \mid x \wedge d \mid y \rightarrow d \leq z) \vee \\ x = 0 \wedge y = 0 \wedge z = 0.$$

Euklidov algoritmus. Teraz uvedieme jednoduchý algoritmus pre výpočet najväčšieho spoločného deliteľa. Pretože $\gcd(x, y) = \gcd(|x|, |y|)$, stačí ho popísať len pre prirodzené čísla. Metóda vychádza z tejto jednoduchej vlastnosti najväčšieho spoločného deliteľa:

$$\gcd(x, qx + r) = \gcd(x, r).$$

Platí totiž

$$x \neq 0 \wedge z \mid x \rightarrow z \mid qx + r \leftrightarrow z \mid r.$$

Odtiaľ dostaneme

$$\gcd(x, y) = \begin{cases} y & \text{ak } x = 0, \\ \gcd(y \bmod x, x) & \text{ak } x \neq 0. \end{cases}$$

Posledné dve rovnosti môžme použíť pre výpočet funkcie gcd, Výpočet sa realizuje ako vyhodnocovanie výrazov. Nasledujúca vlastnosť zaručuje, že program skončí pre všetky vstupy:

$$x \neq 0 \rightarrow y \bmod x < x.$$

Príklad. Výpočet $\gcd(42, 30)$ podľa Euklidovho algoritmu:

$$\begin{aligned} \gcd(42, 30) &= \gcd(30 \bmod 42, 42) = \{30 = 0 \times 42 + 30 \wedge 0 \leq 30 < 42\} \\ \gcd(30, 42) &= \gcd(42 \bmod 30, 30) = \{42 = 1 \times 30 + 12 \wedge 0 \leq 12 < 30\} \quad (1) \\ \gcd(12, 30) &= \gcd(30 \bmod 12, 12) = \{30 = 2 \times 12 + 6 \wedge 0 \leq 6 < 12\} \quad (2) \\ \gcd(6, 12) &= \gcd(12 \bmod 6, 6) = \{12 = 2 \times 6 + 0 \wedge 0 \leq 0 < 6\} \\ \gcd(0, 6) &= 6. \end{aligned}$$

Tento výpočet môžeme využiť na nájdenie celých čísel x a y takých, že

$$42x + 30y = 6.$$

Platí totiž

$$6 \overset{(2)}{=} 30 - 2 \times 12 \overset{(1)}{=} 30 - 2 \times (42 - 30) = 42 \times (-2) + 30 \times 3.$$