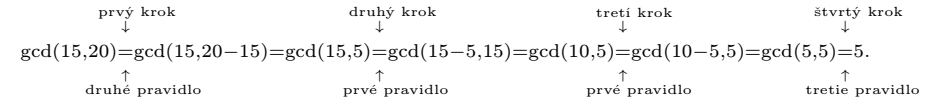
Euklidov algoritmus slúži na výpočet najväčšieho spoločného deliteľa (greatest common divisor, v skratke gcd) dvoch kladných celých čísel. Vysvetlíme si jeho pôvodnú verziu, ktorá je založená na odčítaní. Konkrétne, na opakovanom použití nasledujúcich pravidiel:

Nech k, n sú kladné celé čísla.
1) Ak $k > n$, potom $\gcd(k, n) = \gcd(k-n, n)$.
2) Ak $k < n$, potom $\gcd(k, n) = \gcd(k, n-k)$.
3) Ak $k = n$, potom $\gcd(k, n) = n$.

Najskôr si ukážeme ako funguje tento algoritmus pri výpočte najväčšieho spoločného deliteľa čísel 15 a 20. Ideme teda počítať hodnotu $\gcd(15, 20)$.

Najskôr stručne:



Teraz podrobnejšie:

V prvom kroku máme $k = 15$, $n = 20$. Pretože $k < n$, podľa druhého pravidla dostávame

$$\gcd(15, 20) = \gcd(15, 20 - 15).$$

Výpočet hodnoty $\gcd(15, 20)$ sme teda previedli na výpočet hodnoty $\gcd(15, 5)$.

V druhom kroku máme $k = 15$, $n = 5$. Pretože $k > n$, podľa prvého pravidla dostávame

$$\gcd(15, 5) = \gcd(15 - 5, 5).$$

Výpočet hodnoty $\gcd(15, 5)$ sme teda previedli na výpočet hodnoty $\gcd(10, 5)$.

V treťom kroku máme $k = 10$, $n = 5$. Pretože $k > n$, podľa prvého pravidla dostávame

$$\gcd(10, 5) = \gcd(10 - 5, 5).$$

Výpočet hodnoty $\gcd(10, 5)$ sme teda previedli na výpočet hodnoty $\gcd(5, 5)$.

Vo štvrtom kroku máme $k = 5$, $n = 5$. Pretože $k = n$, podľa tretieho pravidla dostávame

$$\gcd(5, 5) = 5.$$

Tu výpočty končia. Rovnosti získané v jednotlivých krokoch môžeme teraz spojiť do reťazca, ktorý sme uviedli vyššie. Odtiaľ priamo vidíme, že $\gcd(15, 20) = 5$.

Všimnime si, že výpočty v jednotlivých krokoch sme robili použitím prvých dvoch pravidiel až dovtedy, kým sme nedostali dvojicu rovnakých čísel (a teda v ďalšom kroku sme už nemohli použiť ani jedno z týchto dvoch pravidiel). Vtedy prišiel čas na použitie tretieho pravidla, čo je pre tento algoritmus kľúčové. Totiž prvé dve pravidlá nedávajú finálny výsledok, len prevádzajú výpočet najväčšieho spoločného deliteľa dvojice kladných celých čísel na výpočet najväčšieho spoločného deliteľa inej dvojice kladných celých čísel. Až tretie pravidlo dáva ako svoj výsledok konkrétne číslo, čím použitie algoritmu končí. Ukážeme, že takto to funguje pri každom použití Euklidovho algoritmu.

Ako sme uviedli vyššie, prvé dve pravidlá prevádzajú výpočet najväčšieho spoločného deliteľa dvojice kladných celých čísel na výpočet najväčšieho spoločného deliteľa inej dvojice kladných celých čísel. Ukážeme, že tieto pravidlá sú vymyslené tak, že sa pritom pôvodná úloha redukuje na jednoduchšiu úlohu v tom zmysle, že dvojica kladných celých čísel na výstupe má menší súčet ako dvojica kladných celých čísel na vstupe.

Nech $p \neq q$ sú kladné celé čísla. Použitím ktoréhokoľvek z prvých dvoch pravidiel dostávame

$$\gcd(p, q) = \gcd(p', q'), \text{ pričom } p + q > p' + q'.$$

Naozaj,

$$\begin{aligned} &\text{ak } p > q, \text{ potom } p' + q' = (p - q) + q = p < p + q; \\ &\text{ak } p < q, \text{ potom } p' + q' = p + (q - p) = q < p + q. \end{aligned}$$

Pozrime sa teraz na situáciu po prvých j krokoch za predpokladu, že v každom z nich sme použili práve jedno z prvých dvoch pravidiel:

$$\gcd(k, n) \underset{\substack{\uparrow \\ \text{prvý krok}}}{=} \gcd(k_1, n_1) \underset{\substack{\uparrow \\ \text{druhý krok}}}{=} \gcd(k_2, n_2) \underset{\substack{\uparrow \\ \text{tretí krok}}}{=} \gcd(k_3, n_3) = \cdots \underset{\substack{\uparrow \\ j\text{-ty krok}}}{=} \gcd(k_j, n_j).$$

Ako sme ukázali vyššie, platí

$$s > s_1 > s_2 > s_3 > \cdots > s_j,$$

kde $s = k + n$, $s_1 = k_1 + n_1$, $s_2 = k_2 + n_2$, $s_3 = k_3 + n_3$, $\ldots$, $s_j = k_j + n_j$ sú kladné celé čísla.

Pretože kladných celých čísel menších ako číslo s existuje len konečne veľa, číslo j nemôže byť ľubovoľne veľké. Inými slovami, existuje také $j_{\max}$, že v prvých $j_{\max}$ krokoch sa použije práve jedno z prvých dvoch pravidiel, ale v nasledujúcom kroku už nie je možné použiť ani jedno z prvých dvoch pravidiel. To však znamená, že sa použije tretie pravidlo, čím výpočet najväčšieho spoločného deliteľa končí.

Na záver overíme korektnosť použitých pravidiel.

Definícia.
Nech k a n sú celé čísla. Hovoríme, že číslo k je deliteľom čísla n, ak číslo n možno vyjadriť v tvare $n = k \cdot \ell$, kde ℓ je vhodné celé číslo. Inými slovami: ak rovnica

$$n = k \cdot \ell$$

(s neznámou ℓ) má celočíselný koreň. Zapisujeme to $k|n$.

Tvrdenie 1.
Nech r, s, t sú celé čísla. Ak $r|s$ a $r|t$, potom platí $r|(s+t)$ a $r|(s-t)$.

Dôkaz. Nech $r|s$ a $r|t$.
Pretože $r|s$, existuje celé číslo ℓ_1 také, že platí $s = r \cdot \ell_1$.
Pretože $r|t$, existuje celé číslo ℓ_2 také, že platí $t = r \cdot \ell_2$.

Najskôr ukážeme, že $r|(s+t)$:

$$s + t = r \cdot \ell_1 + r \cdot \ell_2 = r \cdot (\ell_1 + \ell_2).$$

Položme $\ell = \ell_1 + \ell_2$. Zrejme ℓ je celé číslo, pre ktoré platí

$$s + t = r \cdot \ell.$$

Preto $r|(s+t)$.

Teraz ukážeme, že $r|(s-t)$:

$$s - t = r \cdot \ell_1 - r \cdot \ell_2 = r \cdot (\ell_1 - \ell_2).$$

Položme $\ell = \ell_1 - \ell_2$. Zrejme ℓ je celé číslo, pre ktoré platí

$$s - t = r \cdot \ell.$$

Preto $r|(s-t)$.

Tvrdenie 2.
Nech a, b sú nenulové celé čísla. Potom $\gcd(a,b) = \gcd(a-b,b)$.

Dôkaz.
Položme $d_1 = \gcd(a,b)$, $d_2 = \gcd(a-b,b)$. Pretože $d_1|a$, $d_1|b$, podľa tvrdenia 1 máme $d_1|(a-b)$. Teda číslo d_1 je spoločným deliteľom čísel $a-b$, b. Pretože d_2 je najväčší spoločný deliteľ čísel $a-b$, b, platí $d_1 \leq d_2$.
Pretože $d_2|(a-b)$, $d_2|b$, podľa tvrdenia 1 máme $d_2|((a-b)+b)$, t.j. $d_2|a$. Teda číslo d_2 je spoločným deliteľom čísel a, b. Pretože d_1 je najväčší spoločný deliteľ čísel a, b, platí $d_2 \leq d_1$.
Ukázali sme, že $d_1 \leq d_2 \leq d_1$, odkiaľ $d_1 = d_2$.