Euklidův algoritmus a Bezoutova rovnost

Euklidův algoritmus

Nechť $a_1, a_2 \in \mathbb{N}$ (rozšíření na celá čísla rozmyslíme snadno - stačí například uvažovat zvlášť nulu a záporná čísla lze vyřešit pomocí absolutní hodnoty).
Pak $(a_1, a_2) = d$ dostaneme jako **poslední nenulový zbytek**, který dostaneme pomocí postupného dělení se zbytkem.
Nechť $a_1 \geq a_2$, pak:

$$\begin{aligned} a_1 &= q_1 a_2 + a_3 \\ a_2 &= q_2 a_3 + a_4 \\ a_3 &= q_3 a_4 + a_5 \\ &\vdots \\ a_{k-2} &= q_{k-2} a_{k-1} + \underbrace{a_k}_{\neq 0} \\ a_{k-1} &= q_{k-1} a_k + 0 \end{aligned}$$

A platí: $(a_1, a_2) = a_k$

Bezoutova identita

Nechť $a, b \in \mathbb{Z}$, $(a, b) = d$. Pak platí:
$\exists k, l \in \mathbb{Z} : ak + bl = d$.

Příklad

Spočtěte $(2013, 612)$ a nalezněte koeficienty z Bezoutovy identity.

$$\begin{aligned} 2013 &= 3 \cdot 612 + 177 \\ 612 &= 3 \cdot 177 + 81 \\ 177 &= 2 \cdot 81 + 15 \\ 81 &= 5 \cdot 15 + 6 \\ 15 &= 2 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

Největší společný dělitel je posledním nenulovým zbytkem. Tj. $(2013, 612) = 3$
Nyní opačným postupem vyjádříme 3 jako nějakou lineární kombinaci 2013 a 612.

$$\begin{aligned} 3 &= 15 - 2 \cdot 6 \\ 3 &= 15 - 2 \cdot (81 - 5 \cdot 15) = 11 \cdot 15 - 2 \cdot 81 \\ 3 &= 11 \cdot (177 - 2 \cdot 81) - 2 \cdot 81 = 11 \cdot 177 - 24 \cdot 81 \\ 3 &= 11 \cdot 177 - 24 \cdot (612 - 3 \cdot 177) = 83 \cdot 177 - 24 \cdot 612 \\ 3 &= 83 \cdot (2013 - 3 \cdot 612) - 24 \cdot 612 = 83 \cdot 2013 - 273 \cdot 612 \end{aligned}$$

Příklad

Dokažte: $a \mid b \cdot c,\ (a, b) = 1 \quad \Rightarrow \quad a \mid c$.
Užitím Bezoutovy rovnosti dostáváme: $ak + bl = 1$ pro nějaká $k, l \in \mathbb{Z}$.
Pak $c = ack + bcl$.
Z předpokladu: $a \mid bc \Rightarrow a \mid bcl$
a dále: $a \mid a \Rightarrow a \mid ack$
Dohromady pak dostáváme $a \mid ack + bcl = c$.

Příklad

Spočtěte $\left(3^{35}-1, 3^{14}-1\right)$

$$3^{35}-1 = \left(3^{14}-1\right)\left(3^2 1+3^7\right)+\left(3^7-1\right)$$
$$3^{14}-1 = \left(3^7-1\right)\left(3^7+1\right)+0$$

$\Rightarrow \left(3^{35}-1\,,\, 3^{14}-1\right) = 3^7-1$

Příklad

Spočtěte $(2013, 1452)$ a spočtěte Bezoutovu rovnost.

$$\begin{aligned}
2013 &= 1452+561 & 33 &= 231-2\cdot 99\\
1452 &= 2\cdot 561+330 & 33 &= 231-2\cdot(330-231) = 3\cdot 231-2\cdot 330\\
561 &= 330+231 & 33 &= 3\cdot(561-330)-2\cdot 330 = 3\cdot 561-5\cdot 330\\
330 &= 231+99 & 33 &= 3\cdot 561-5\cdot(1452-2\cdot 561) = 13\cdot(561)-5\cdot 1452\\
231 &= 2\cdot 99+33 & 33 &= 13\cdot(2013-1452)-5\cdot 1452 = 13\cdot 2013-18\cdot 1452\\
99 &= 3\cdot 33+0
\end{aligned}$$

$\Rightarrow (2013, 1452) = 33, \qquad 33 = 13\cdot 2013-18\cdot 1452$