Euklidův algoritmus – co se nestihlo

2. listopadu 2010

Celý tento text je nepovinný, na Euklidův algoritmus dojde až příští semestr.

Na cvičení jsme si popsali Euklidův algoritmus, který pro vstupní čísla a, b, kde $b \geq a$, hledá nová čísla $a_0, a_1, a_2, \ldots$ a $k_0, k_1, k_2, \ldots$ tak, aby platilo:

$$\begin{aligned} b &= a \cdot k_0 + a_1 \\ a = a_0 &= a_1 \cdot k_1 + a_2 \\ a_1 &= a_2 \cdot k_2 + a_3 \\ &\vdots \\ a_{l-1} &= a_l \cdot k_l + a_{l+1} \\ a_l &= a_{l+1} \cdot k_{l+1} + 0 \end{aligned}$$

Tvrdíme nyní, že jsme schopni číslo a_{l+1} napsat jako lineární kombinaci a, b s celočíselnými koeficienty. Budeme postupovat indukcí a dokážeme, že takto umíme zapsat každé číslo a_i, kde $i = 0, 1, \ldots, l+1$: Pro $a_0 = a$ a číslo a_1 tvrzení zjevně platí (máme $a_1 = b - k_0 \cdot a$). Pokud nyní umíme vyjádřit čísla $a_0, \ldots, a_i$, tak platí $a_{i+1} = a_{i-1} - a_i \cdot k_i$, takže když nyní za a_i, a_{i-1} dosadíme odpovídající kombinaci a, b, tak dostáváme zápis a_{i+1} jako celočíselnou lineární kombinaci a, b.

Důsledek: Pokud a, b jsou celá čísla, tak existují celá čísla c, d taková, že $ac + bd = nsd(a, b)$.

Důsledek důsledku: Pokud a, b jsou nesoudělná celá čísla, tak existují celá čísla c, d taková, že $ac + bd = 1$.

Příklad: Buďte $a = 3, b = 11$. Potom máme:

$$\begin{aligned} 11 &= 3 \cdot 3 + 2 \\ 3 &= 2 \cdot 1 + 1, \end{aligned}$$

takže můžeme dosazovat: Spočteme nejprve $2 = 11 - 3 \cdot 3$ a potom

$$1 = 3 - (11 - 3 \cdot 3) \cdot 1 = 3 \cdot 4 + 11 \cdot (-1),$$

což jsme přesně chtěli.