1. cvičení

Připomeňme rozšířený Eukleidův algoritmus hledání největšího společného dělitele čísel a a b:

`VSTUP:` $a, b \in \mathbb{N}$, $a \geq b$
`VÝSTUP:` $\mathrm{NSD}(a,b), x, y \in \mathbb{Z}$, `pro které` $\mathrm{NSD}(a,b) = x \cdot a + y \cdot b$

`0.` $i := 1$, $(a_0, a_1) := (a, b)$; $(x_0, x_1) := (1, 0)$; $(y_0, y_1) := (0, 1)$;

`1.` `while`$(a_i > 0)$ `do`
$\{a_{i+1} := (a_{i-1}) \mathrm{mod}\ a_i$; $q_i := (a_{i-1}) \mathrm{div}\ a_i$; %`tj.` $a_{i-1} = q_i a_i + a_{i+1}$
$x_{i+1} := x_{i-1} - x_i \cdot q_i$; $y_{i+1} := y_{i-1} - y_i \cdot q_i$; $i := i + 1;\}$

`2.` `return` $a_{i-1}, x_{i-1}, y_{i-1}$.

1. Spočítejte největší společný dělitel a příslušné Bézoutovy koeficienty v celých číslech

(a) čísel 539 a 84,

(b) čísel 256 a 27,

(c) čísel $2^{92} - 1$ a $2^{31} - 1$.

2. Spočtěte 23^{-1} v tělese $\mathbb{Z}_{37}$.

3. Dokažte pro hodnoty běhu Eukleidova algoritmu, že

(a) $\mathrm{NSD}(a_{i-1}, a_i) = \mathrm{NSD}(a_i, a_{i+1})$,

(b) $a_i = x_i \cdot a + y_i \cdot b$,

(c) $\mathrm{NSD}(a, b) = x \cdot a + y \cdot b$.

Řešení:

1. (a) $\text{NSD}(539, 84) = 7 = 5 \cdot 539 - 32 \cdot 84$,

   (b) $\text{NSD}(256, 27) = 1 = -2 \cdot 256 + 19 \cdot 27$,

   (c) $\text{NSD}(2^{92} - 1, 2^{31} - 1) = 1 = (-2)(2^{92} - 1) + (1 + 2^{31} + 2^{62})(2^{31} - 1)$.

2. Spočítáme Bezoutův koeficient $y = -8$ ve vztahu

$$37x + 23y = \text{NSD}(37, 23) = 1$$

   , potom $23^{-1} = (-8) \text{mod } 37 = 29$.

3. (a) Při využití vztahů $a_{i-1} = a_{i+1} + q_i \cdot a_i$ a $a_{i+1} = a_{i-1} - q_i \cdot a_i$ uvážíme, že

$$c/a_{i-1}, a_i \Rightarrow c/a_{i+1} = a_{i-1} - q_i \cdot a_i,$$

$$d/a_i, a_{i+1} \Rightarrow d/a_{i-1} = a_{i-1} + q_i \cdot a_i.$$

   (b) Dokážeme indukcí: Tvrzení platí pro $i = 0$ a $i = 1$ a předpokládejme, že tvrzení platí pro i a $i - 1$, tedy $a_i = x_i \cdot a_0 + y_i \cdot a_1$ a $a_{i-1} = x_{i-1} \cdot a_0 + y_{i-1} \cdot a_1$. Dokážeme rovnost pro $i + 1$ dosazením za a_i a a_{i-1} do vztahu:

$$a_{i+1} = a_{i-1} - a_i \cdot q_i = (x_{i-1} \cdot a_0 + y_{i-1} \cdot a_1) - (x_i \cdot a_0 + y_i \cdot a_1) \cdot q_i =$$

$$= (x_{i-1} - x_i \cdot q_i) \cdot a_0 + (y_{i-1} - y_i \cdot q_i) \cdot a_1 = x_{i+1} \cdot a_0 + y_{i+1} \cdot a_1.$$

   (c) Plyne z (a) a (b).