Cvičení 15. 3. 2012

Víme že pro $a, b \in \mathbb{Z}$ lze pomocí rozšířeného Euklidova algoritmu nalézt $c, d \in \mathbb{Z}$, že $ac + bd = NSD(a, b)$.

Čínská zbytková věta tvrdí, že pokud $n_1, \ldots, n_k$ jsou po dvou nesoudělná čísla, tak má pro každá $m_1, \ldots, m_k$ soustava

$$\begin{aligned} x &\equiv m_1 \pmod{n_1} \\ x &\equiv m_2 \pmod{n_2} \\ &\vdots \\ x &\equiv m_k \pmod{n_k} \end{aligned}$$

právě jedno řešení v množině $\{1, \ldots, n_1 \cdots n_k\}$.

Jak řešení nalézt: Pomocí rozšířeného Euklidova algoritmu spočteme pro n_i, n_j čísla a_{ij}, b_{ij}, že $n_i a_{ij} + n_j b_{ij} = 1$ a čísla a_{ij}, b_{ij} šikovně pronásobíme a sečteme (viz vzorový příklad).

Příklad 1. Najděte číslo $x \in \{1, \ldots, 273\}$ takové, aby dávalo po dělení 3 zbytek 1, po dělení 7 zbytek 2 a po dělení 13 zbytek 4.

Příklad 2. Skupině třinácti pirátů se podařilo uloupit bednu zlatých mincí. Zkusili je rozdělit rovným dílem na třináct hromádek, ale deset mincí jim zbylo. O zbylé mince se strhla rvačka, při níž jednoho piráta propíchli. Přestali tedy bojovat a zkusili mezi sebe znovu rozdělit mince rovným dílem. Tentokrát zbyly tři mince, o které opět začali bojovat. V boji zahynul další pirát a tak si ostatní opět zkusili mince spravedlivě rozdělit, tentokrát úspěšně. Kolik bylo nejméně mincí, které piráti ukradli?

Příklad 3. Najděte všechna celočíselná řešení soustavy:

1. $x \equiv 4 \pmod{13}, x \equiv 1 \pmod{49}$
2. $5x \equiv 1 \pmod{15}$
3. $2x \equiv -5 \pmod{23}, 3x \equiv 2 \pmod{5}$
4. $3x \equiv 3 \pmod{15}, 2x \equiv 4 \pmod{7}$

Příklad 4. Najděte všechny involuce v grupě $\mathbb{Z}_n$. Involuce jsou prvky řádu přesně 2.

Příklad 5. Popište všechny endomorfismy a všechny automorfismy grupy $(\mathbb{Z}_n, +)$.

Příklad 6. Dokažte, že následující podmínky jsou ekvivalentní pro každou dvojici $n \in \mathbb{N}, a \in \mathbb{Z}$:

1. a, n jsou nesoudělná
2. $(a \mod n) \in \mathbb{Z}_n^\star$
3. $i \mapsto ai \pmod n$ je automorfismus grupy $\mathbb{Z}_n$
4. $a\mathbb{Z}_n = \mathbb{Z}_n$

Příklad 7 (návrat těžké úlohy)**.** Buď $p > 2$ prvočíslo. Dokažte, že p dělí čitatele zlomku

$$1 + 1/2 + \cdots + 1/(p-1).$$