8. cvičení

Ve škole:

1. Najděte všechna $x \in \mathbb{Z}$, pro která platí
(a) $x \equiv 5 \pmod 7$, $x \equiv 4 \pmod 8$, $x \equiv 2 \pmod 9$,
(b) $2x + 1 \equiv 2 \pmod 3$, $3x + 2 \equiv 3 \pmod 4$, $4x + 3 \equiv 2 \pmod 5$,
(c) $10x \equiv 6 \pmod{32}$ a $3x \equiv 1 \pmod 5$,
(d) $x^{11} \equiv 2 \pmod 5$ a $x^8 \equiv 1 \pmod 7$.

2. Spočítejte všechna $x \in \mathbb{Z}$ splňující
(a) $x^2 \equiv 1 \pmod 3$ a $x^2 \equiv 1 \pmod 7$,
(b) $x^2 \equiv -1 \pmod{65}$,
(c) $x^2 \equiv 36 \pmod{45}$.

3. Najděte všechny kořeny polynomů
(a) $x^2 - 1$ nad $\mathbb{Z}_{21}$, (b) $x^2 + 1$ nad $\mathbb{Z}_{65}$, (c) $x^2 + 3x + 2$ nad $\mathbb{Z}_{14}$.

Úloha pro samostatné počítání:

4. Nechť jsou p a q dvě různá lichá prvočísla.
(a) Dokažte, že má polynom $x^3 + 3x^2 + 2x$ v okruhu $\mathbb{Z}_{pq}$ právě 9 kořenů.
(b) Rozhodněte, zda existují $a, b \in \mathbb{Z}_{pq}$, aby měl polynom $x^2 + ax + b$ v okruhu $\mathbb{Z}_{pq}$ právě 3 kořeny.

Řešení:

1. Počítáme pomocí dosazovacího (Garnerova) algoritmu na výpočet vzorů Čínské věty o zbytcích:

   (a) $x \equiv 236 \pmod{504}$, (b) $x \equiv 11 \pmod{60}$, (c) $x \equiv 7 \pmod{80}$.

   (d) Všimneme si, že pro $5/x$ nebo $7/x$ kongruence splněny nejsou. Za předpokladu, že 5 ani 7 nedělí x ekvivalentně upravíme kongruence pomocí Eulerovy věty na

   $$1 \equiv 2x \pmod{5}, \quad x^2 \equiv 1 \pmod{7},$$

   druhá z kongruencí je díky kořenovým vlastnostem polynomu $x^2 - 1$ ekvivalentní podmínce $x \equiv \pm 1 \pmod{7}$, odtud už stejným postupem jako v (a)-(c) dostaneme, že $x \equiv 8 \pmod{35}$ nebo $x \equiv 13 \pmod{35}$.

2. (a) $x \in \{\pm 1 + 21k |\ k \in \mathbb{Z}\} \cup \{8 + 21k |\ k \in \mathbb{Z}\} \cup \{13 + 21k |\ k \in \mathbb{Z}\}$

   (b) $x \equiv \pm 8 \pmod{65}$ nebo $x \equiv \pm 18 \pmod{65}$,

   (c) $x \equiv \pm 6 \pmod{15}$, tj. $x \in \{\pm 6 + 15k |\ k \in \mathbb{Z}\}$.

3. Využijeme opět Čínskou větu o zbytcích. Polynomiální rovnice pro (a) a (b) jsme vyřešili už v předchozí úloze.

   (a) $x^2 - 1$ má kořeny $1, 8, 13, 20$,

   (b) $x^2 + 1$ má kořeny $8, 18, 47, 57$,

   (c) $x^2 + 3x + 2 = (x + 1)(x + 2)$ má kořeny $5, 6, 12, 13$.

4. (a) Označme $F_p : \mathbb{Z}_{pq} \to \mathbb{Z}_p$ $F_q : \mathbb{Z}_{pq} \to \mathbb{Z}_q$ zobrazení daná předpisem

   $$F_p(a) = (a) \text{mod } p, \quad F_q(a) = (a) \text{mod } q$$

   a nechť $f = x^3 + 3x^2 + 2x = x(x + 1)(x + 2)$. Pak je podle Čínské věty o zbytcích zobrazení $a \to (F_p(a), F_q(a))$ bijekce množin $\mathbb{Z}_{pq}$ a $\mathbb{Z}_p \times \mathbb{Z}_q$, navíc $a \in \mathbb{Z}_{pq}$ je kořenem polynomu f nad okruhem $\mathbb{Z}_{pq}$, právě když je $F_p(a)$ kořenem polynomu f nad tělesem $\mathbb{Z}_p$ a zároveň je $F_q(a)$ kořenem polynomu f nad tělesem $\mathbb{Z}_q$. Protože má f nad tělesem $\mathbb{Z}_p$ i nad tělesem nad tělesem $\mathbb{Z}_q$ právě 3 kořeny a každá dvojice těchto kořenů odpovídá právě jednomu kořenu nad $\mathbb{Z}_{pq}$, má f nad okruhem $\mathbb{Z}_{pq}$ právě $3 \cdot 3 = 9$ kořenů.

   (b) Ne. Podle předchozí úvahy by musel mít polynom $x^2 + ax + b$ nad tělesem $\mathbb{Z}_p$ nebo $\mathbb{Z}_q$ právě 3 kořeny (a nad druhým tělesem nutně právě jeden), což pro polynom stupně dva nad žádným tělesem není možné.