9. cvičení

Ve škole:

1. Najděte všechny polynomy $f \in \mathbb{R}[x]$, pro které platí:
(a) $f(0) = 2$, $f(1) = 1$, $f(-1) = 3$,
(b) $f(0) = 2$, $f(1) = 1$, $f(-1) = 3$, $f(2) = 6$,
(c) $f(0) = 1$, $f(1) = 2$, $f(-1) = 3$,
(d) $f(0) = 1$, $f(1) = 2$, $f(-1) = 3$, $f(2) = 6$,

2. Najděte všechny polynomy $f \in \mathbb{Z}_3[x]$, pro které platí:
(a) $f \equiv x + 2 \pmod{x^2 + 1}$ a $f \equiv 1 \pmod{x^2 + x + 1}$,
(b) $f \equiv 2 \pmod{x^2 + 1}$ a $f \equiv 2x \pmod{x^2 + x + 1}$.

3. Ověřte, že je $\mathbb{Z}_3[\alpha]/(\alpha^2 + 1)$ těleso a spočítejte
(a) α^{-1}, (b) $(\alpha + 1)^{-1}$, (c) $2\alpha \cdot (2\alpha + 1)$, (d) $\alpha^{-1} \cdot (\alpha + 2)$.

4. Zkonstruujte šestnáctiprvkové těleso.

Úlohy pro samostatné počítání:

5. Dokažte, že existuje izomorfismus mezi okruhy $\mathbb{Z}_5[x]/(x^4 - 1)$ a $\mathbb{Z}_5^4$.

6. Ověřte, že je $\mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$ těleso a najděte v něm všechny kořeny polynomu $x^7 + 1$.

Řešení:

1. (a) Například pomocí Lagrangeova interpolačního polynomu dostaneme $-x+2 = 2 \cdot \frac{(x+1)(x-1)}{-1} + 1 \cdot \frac{x(x+1)}{2} + 3 \cdot \frac{x(x-1)}{2}$, proto $f \in \{-x+2+g(x^3-x) \mid g \in \mathbb{R}[x]\}$.

   (b) Řešíme kongruence $f \equiv -x+2 \pmod{x^3-x}$, $f \equiv 6 \pmod{x-2}$, proto

   $f \in \{x^3-2x+2+g(x^3-x)(x-2) \mid g \in \mathbb{R}[x]\}$.

   (c) $\frac{3}{2}x^2 - \frac{1}{2}x + 1 = 1 \cdot \frac{(x+1)(x-1)}{-1} + 2 \cdot \frac{x(x+1)}{2} + 3 \cdot \frac{x(x-1)}{2}$, proto

   $f \equiv \frac{3}{2}x^2 - \frac{1}{2}x + 1 \pmod{x^3-x}$.

   (d) $f \equiv \frac{3}{2}x^2 - \frac{1}{2}x + 1 \pmod{(x^3-x)(x-2)}$.

2. Postupujeme obdobně jako při řešení kongruencí v $\mathbb{Z}$:

   (a) $f \equiv 2x^3+2 \pmod{(x^2+x+1)(x^2+1)}$, tj.

   $f \in \{2x^3+2+g(x^2+x+1)(x^2+1) \mid g \in \mathbb{Z}_3[x]\}$.

   (b) $f \equiv x^3+2x^2+x+1 \pmod{(x^2+x+1)(x^2+1)}$, tj.

   $f \in \{x^3+2x^2+x+1+g(x^2+x+1)(x^2+1) \mid g \in \mathbb{Z}_3[x]\}$.

3. Protože polynom x^2+1 nemá v $\mathbb{Z}_3$ kořen, není součinem kořenových činitelů (tedy polynomů stupně 1), a proto je ireducibilní. Tudíž je podle pozorování z přednášky okruh $\mathbb{Z}_3[\alpha]/(\alpha^2+1)$ těleso.

   (a) Řešíme kongruenci $\alpha f \equiv 1 \pmod{\alpha^2+1}$ (všimněme si, že $\alpha^2 \equiv -1 \pmod{\alpha^2+1}$) a dostáváme $\alpha^{-1} = 2\alpha$,

   (b) $(\alpha+1)^{-1} = \alpha+2$, (c) $2\alpha \cdot (2\alpha+1) = 2\alpha+2$, (d) $\alpha^{-1} \cdot (\alpha+2) = \alpha+1$.

4. Stačí najít ireducubilní polynom stupně 4 nad tělesem $\mathbb{Z}_2$, takový polynom nesmí mít kořen 0 ani 1, což znamená, že má absolutní člen 1 a lichý počet členů a dále nemůže být součinem dvou ireducibilních polynomů stupně 2. Protože jediný ireducibilní polynom stupně 2 nad tělesem $\mathbb{Z}_2$ je polynom x^2+x+1 a $(x^2+x+1)^2 = x^4+x^2+1$ je ireducibilní například polynom x^4+x+1. Tudíž $\mathbb{Z}_2[x]/(x^4+x+1)$ je šestnáctiprvkové těleso.

5. Definujeme-li $\varphi(g) = (g(1), g(2), g(3), g(4))$ pro každé $g \in \mathbb{Z}_5[x]/(x^4-1)$ a všimneme-li si, že $x^4-1 = (x-1)(x-2)(x-3)(x-4)$, je zobrazení $\varphi : \mathbb{Z}_5[x]/(x^4-1) \to \mathbb{Z}_5^4$ podle Čínské věty o zbytcích izomorfismus.

6. Protože polynom x^3+x+1 nemá v $\mathbb{Z}_2$ kořen, není násobkem kořenového činitele, tedy součinem tedy polynomu stupně 1 a 2. Proto je ireducibilní a okruh $T = \mathbb{Z}_2[\alpha]/(\alpha^3+\alpha+1)$ je tělesem. Kořenem x^7+1 jsou všechny nenulové prvky tělesa T (ověření je bez dalších znalostí teorie poněkud pracné), tedy $x^7+1 = \prod_{t \in T \setminus \{0\}} (x-t)$.