12. cvičení

1. Najděte všechny polynomy $f \in \mathbb{Q}[x]$ stupně < 4 splňující
(a) $f(0) = 1$, $f(1) = 0$, $f(2) = 2$,
(b) $f \equiv x + 1 \pmod{x^2 + 1}$ a $f(0) = 3$,
(c) $f \equiv 1 \pmod{x^2 - 1}$ a $f \equiv x + 1 \pmod{x^2 + 1}$.

2. V tělese $\mathbb{F}_{125} = \{a_0 + a_1\alpha + a_2\alpha^2 |\ a_i \in \mathbb{Z}_5\}$ s počítáním modulo $\alpha^3 + \alpha + 1$ v $\mathbb{Z}_5[\alpha]$ spočtěte
(a) $(3\alpha^2 + 4\alpha + 1) + (2\alpha^2 + 4)$,
(b) $(3\alpha^2 + 4\alpha + 1) \cdot (2\alpha^2 + 4)$,
(c) α^{-1}, $(\alpha^2)^{-1}$, $(\alpha^2 + 1)^{-1}$,
(d) řešení lineární rovnice $\alpha \cdot x + (\alpha + 1) = \alpha^2$.

3. V tělese $\mathbb{F}_4 = \{a_0 + a_1\alpha |\ a_i \in \mathbb{Z}_2\}$ s počítáním modulo $\alpha^2 + \alpha + 1$ v $\mathbb{Z}_2[\alpha]$ spočtěte řešení soustavy lineárních rovnic zadané maticí

$$\left(\begin{array}{cc|c} \alpha & 1 & \alpha + 1 \\ \alpha + 1 & \alpha + 1 & \alpha \end{array}\right)$$

4. Najděte v tělese $\mathbb{F}_9 = \{a_0 + a_1\alpha |\ a_i \in \mathbb{Z}_3\}$ s počítáním modulo $\alpha^2 + 1$ v $\mathbb{Z}_3[\alpha]$ prvek u s vlastností, že každý prvek $v \in \mathbb{F}_9 \setminus \{0\}$ lze napsat jako mocnina u a Najděte ireducibilní rozklad polynomů $x^8 - 1$ v $\mathbb{F}_9[x]$.

Řešení:

1. (a) $\frac{3}{2}x^2 - \frac{5}{2}x + 1 + cx(x-1)(x-2)$ pro libovolné $c \in \mathbb{Q}$,
   (b) $2x^2 + x + 3 + bx(x^2+1)$ pro libovolné $b \in \mathbb{Q}$,
   (c) $-\frac{1}{2}x^3 + \frac{1}{2}x + 1$
2. (a) $(3\alpha^2 + 4\alpha + 1) + (2\alpha^2 + 4) = 4\alpha$,
   (b) $(3\alpha^2 + 4\alpha + 1) \cdot (2\alpha^2 + 4) = 3\alpha^2 + 2\alpha + 1$,
   (c) $\alpha^{-1} = 4\alpha^2 + 4$, $(\alpha^2)^{-1} = \alpha^2 + 4\alpha + 1$, $(\alpha^2+1)^{-1} = 4\alpha$,
   (d) $x = \alpha^2 + \alpha$
3. $(0, \alpha + 1)^T$
4. Například $\alpha + 1$, $x^8 - 1 = \prod_{\gamma \in \mathbb{F}_9 \setminus \{0\}} (x - \gamma)$.