4. cvičení

1. Spočítejte největší společný dělitel a příslušné Bézoutovy koeficienty

(a) čísel 539 a 84 v $\mathbb{Z}$,

(b) čísel 256 a 27 v $\mathbb{Z}$,

(c) čísel $2^{92} - 1$ a $2^{31} - 1$ v $\mathbb{Z}$,

(d) polynomů $x^3 + x^2 + x + 1$ a $x^2 + 2x + 2$ v okruhu $\mathbb{Z}_3[x]$ a v okruhu $\mathbb{Z}_5[x]$.

2. Spočtěte 23^{-1} v tělese $\mathbb{Z}_{37}$ a v okruhu $\mathbb{Z}_{39}$.

3. Najděte všechna $x \in \mathbb{Z}$ splňující

(a) $5x + 3 \equiv 9x + 13 \pmod{17}$,

(b) $10x + 5 \equiv 7 \pmod{14}$,

(c) $x^2 + 5x \equiv 0 \pmod{19}$,

(d) $x^2 + 10x \equiv 11 \pmod{17}$.

4. Najděte všechna $x, y, z \in \mathbb{Z}$ splňující $x^2 + y^2 + z^2 = 15w^2$ (návod: řešte nejprve kongruenci modulo 8).

Řešení:

1. (a) $\mathrm{NSD}(539, 84) = 7 = 5 \cdot 539 - 32 \cdot 84$,
   (b) $\mathrm{NSD}(256, 27) = 1 = -2 \cdot 256 + 19 \cdot 27$,
   (c) $\mathrm{NSD}(2^{92} - 1, 2^{31} - 1) = 1 = (-2)(2^{92} - 1) + (1 + 2^{31} + 2^{62})(2^{31} - 1)$,
   (d) $\mathrm{NSD}(x^3 + x^2 + x + 1, x^2 + 2x + 2) =$
   $= 2 = (2x + 1)(x^3 + x^2 + x + 1) + (x^2 + x + 2)(x^2 + 2x + 2)$ v $\mathbb{Z}_3[x]$,
   $= x + 3 = 1(x^3 + x^2 + x + 1) + (4x + 1)(x^2 + 2x + 2)$ v $\mathbb{Z}_5[x]$.

2. $23^{-1} = 29$ v $\mathbb{Z}_{37}$ a $23^{-1} = 17$ v $\mathbb{Z}_{39}$.

3. (a) $x \equiv 6 \pmod{17}$, tj. $x \in \{6 + 17z |\ z \in \mathbb{Z}\}$,
   (b) $x \equiv 3 \pmod{7}$, tj. $x \in \{3 + 7z |\ z \in \mathbb{Z}\}$,
   (c) $x \in \{19z |\ z \in \mathbb{Z}\} \cup \{14 + 19z |\ z \in \mathbb{Z}\}$,
   (d) $x \in \{1 + 17z |\ z \in \mathbb{Z}\} \cup \{6 + 17z |\ z \in \mathbb{Z}\}$,

4. nutná podmínka: $x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{8}$ a $a^2 \equiv 1 \pmod{8}$ pro a liché $a^2 \equiv 0$ nebo $4 \pmod{8}$ pro a sudé $\Rightarrow x, y, z, w$ sudé. Nyní vytkneme ze všech neznámých číslo 2 a vykrátíme číslem 4 a řešíme stejnou rovnici $\Rightarrow x = y = z = w = 0$.