## 1. Třetí písemná zkouška MB204 18.6.2013

**1.1.** Mějme kongruenci $922 \cdot x \equiv 1284 \pmod{644}$. Pomocí kritéria udávajícího řešitelnost (a počet řešení) lineární kongruence určete počet řešení této kongruence a pak kongruenci vyřešte.

**Řešení**. $922 = 2.461$, $1284 = 2^2.3.107$ a $644 = 2^2.7.23$. Platí $(922, 644) = 2|1284$, soustava má tedy právě dvě řešení modulo 644. Podle čínské zbytkové věty je kongruence ekvivalentní soustavě

$$\begin{aligned} x &\equiv 0 \mod 2 \\ 6x &\equiv 5 \mod 7 \\ x &\equiv 21 \mod 23 \end{aligned}$$

Řešením je $x \equiv 44$ nebo $x \equiv 366 \mod 644$. □

**1.2.** Určete $\sigma^{-1}$ a $\sigma^{2013}$, kde

- (a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 2 & 7 & 8 & 9 & 6 & 1 \end{pmatrix}$ v grupě permutací $(S^9, \circ)$.
- (b) $\sigma = [4]_{13}$ v grupě $(\mathbb{Z}_{13}^{\times}, \cdot)$.

**Řešení**. (a) $\sigma = (1,3,5,7,9) \circ (2,4) \circ (6,8)$, $\sigma^{-1} = (1,9,7,5,3) \circ (2,4) \circ (6,8)$, $\sigma^{10} = 1 \Rightarrow \sigma^{2013} = \sigma^3 = (1,7,3,9,5) \circ (2,4) \circ (6,8)$. (b) $4^6 \equiv 1 \mod 13 \Rightarrow \sigma^{-1} = 4^5 \equiv -3 \equiv 10 \mod 13$ a $\sigma^{2013} = 4^{2013} \equiv 4^3 \equiv -1 \equiv 12 \mod 13$. □

**1.3.** Je dána soustava polynomiálních rovnic

$$\begin{aligned} x^2yz^2 + x^2y^2 + yz - xyz^2 - z^2 &= 0 \\ x^2y + z &= 0 \\ xyz + z + 1 &= 0 \end{aligned}$$

Seřaďte monomy polynomů podle lexikografického uspořádání s $x > y > z$, pak vydělte první polynom druhým a třetím a výsledek využijte k vyřešení soustavy v oboru reálných čísel.

**Řešení**. $x^2y^2 + x^2yz^2 - xyz^2 + yz - z^2 = (y + z^2)(x^2y + z) - y(xyz + z + 1) - z^3 + z$. Odtud $z = 0, \pm 1$. Potom např. $0 = z(x^2y + z) - x(xyz + z + 1) = z^2 - zx - x$. Odtud $x = \frac{z^2}{z+1}$ a z třetí rovnice $y = -\frac{(1+z)^2}{z^3}$. Vyhovuje jediný reálný bod $(\frac{1}{2}, -4, 1)$. □

**1.4.** Sedmibitovou zprávu $a_0a_1 \dots a_6$, chápanou jako $a_0 + a_1x + \cdots + a_6x^6$, kódujeme polynomiálním kódem generovaným polynomem $x^4 + x^3 + 1$.

- (a) Zakódujte zprávu 1100110.
- (b) Obdrželi jste kód 00111010111. Jaká byla posílaná zpráva, když budete předpokládat, že došlo k chybě na maximálně jednom bitu?
- (c) Jaká byla zpráva v (b), pokud předpokládáme, že došlo k chybě právě na dvou bitech?

**Řešení**. (a) $x^4 \equiv x^3 + 1$, $x^5 \equiv x^3 + x + 1$, $x^6 \equiv x^3 + x^2 + x + 1$, $x^7 \equiv x^2 + x + 1$, $x^8 \equiv x^3 + x^2 + x$ $x^9 \equiv x^2 + 1$, $x^{10} \equiv x^3 + x \Rightarrow 1 + x + x^4 + x^5 \mapsto x^4 + x^5 + x^8 + x^9 + x^3 + 1 + x^3 + x + 1 + x^3 + x^2 + x + x^2 + 1 = 1 + x^3 + x^4 + x^5 + x^8 + x^9$. Kód je tedy 10011100110. (b) $x^2 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{10}$ dává po dělení $x^4 + x^3 + 1$ zbytek $x^5$. Došlo tedy k chybě na šestém bitu a původní zpráva byla 1110111. (c) $x^5 \equiv x^3 + x + 1 \equiv 1 + x^{10} \equiv x + x^4 \equiv x^2 + x^6 \equiv x^8 + x^9$. Buď tedy nastala chyba na prvním a posledním bitu nebo na druhém a pátém nebo třetím a sedmém nebo na devátém a desátém. V prvním případě byla zpráva 1010110, ve druhém 0010111, ve třetím 1000111 a ve čtvrtém 1010001. □