**Druhá písemná zkouška MB204 5.6.2013**

**1.** Mějme kongruenci $963 \cdot x \equiv 2766 \pmod{1716}$. Pomocí kritéria, udávajícího řešitelnost (a počet řešení) lineární kongruence, určete počet řešení této kongruence a pak kongruenci vyřešte.

**Řešení**. $963 = 3^2.107$, $2766 = 2.3.461$, $1716 = 2^2.3.11.13$ $(963, 1716) = 3|2766$. Soustava má právě tři řešení modulo 1716. Najdeme $x = 4t + 2$ a $t \equiv 2 \mod 11$ a $t \equiv 2 \mod 13$, což dává $x \equiv 10 \mod 4.11.13 = 572$, neboli $x_{1,2,3} \equiv 10, 582, 1154$ mod 1716. □

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

- (a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 7 & 6 & 1 & 2 & 3 \end{pmatrix}$ v grupě permutací $(S^7, \circ)$.
- (b) $\sigma = [4]_{11}$ v grupě $(\mathbb{Z}_{11}^{\times}, \cdot)$.

**Řešení**. (a) $\sigma = (1, 4, 6, 2, 5) \circ (3, 7)$, $\sigma^{-1} = (1, 5, 2, 6, 4) \circ (3, 7)$, $\sigma^5 = 1 \Rightarrow \sigma^{2013} = \sigma^3 = (1, 2, 4, 5, 6) \circ (3, 7)$. (b) $4^5 \equiv 1 \mod 11 \Rightarrow \sigma^{-1} = 4^4 \equiv 3 \mod 11$ a $\sigma^{2013} = 4^{2013} \equiv 4^3 \equiv 9 \mod 11$. □

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

- (a) Zakódujte zprávu 1101011.
- (b) Obdrželi jste kód 01001011101. 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) $x^4 \equiv x^3 + 1$, $x^5 \equiv x^3 + x + 1$, $x^7 \equiv x^2 + x + 1$ $x^9 \equiv x^2 + 1$, $x^{10} \equiv x^3 + x$ $\Rightarrow 1 + x + x^3 + x^5 + x^6 \mapsto x^4 + x^5 + x^7 + x^9 + x^{10} + x^3 + 1 + x^3 + x + 1 + x^2 + x + 1 + x^2 + 1 + x^3 + x = x^3 + x^4 + x^5 + x^7 + x^9 + x^{10} + x^3 + x$. Kód je tedy 01011101011. (b) $x + x^4 + x^6 + x^7 + x^8 + x^{10}$ dává po dělení $x^4 + x^3 + 1$ zbytek $x^2 + x + 1 \equiv x^7$. Došlo tedy k chybě na osmém bitu a původní zpráva byla 1010101. (c) Buď nastala chyba na druhém a desátém bitu ($x + x^9 \equiv x^2 + x + 1$), nebo na čtvrtém a sedmém ($x^3 + x^6 \equiv x^2 + x + 1$) nebo pátém a devátém ($x^4 + x^8 \equiv x^2 + x + 1$). V prvním případě byla zpráva 00001011111, ve druhém 01011010101, ve třetím 01000011001. □

**4.** Bankomat vydává bankovky v hodnotě 200, 500 a 1 000 korun. Kolika způsoby mohu vybrat 7 000 korun? Ukažte řešení pomocí vytvořující funkce.

**Řešení**. Úlohu můžeme přeformulovat jako hledání počtu celočíselných řešení

$$2a + 5b + 10c = 70; \quad a, b, c \geq 0.$$

To je také rovno koeficientu u $x^{70}$ v funkce

$$G(x) = (1 + x^2 + x^4 + \cdots)(1 + x^5 + x^{10} + \cdots)(1 + x^{10} + x^{20} + \cdots)$$

Tato funkce je rovna

$$G(x) = \frac{1}{1 - x^2} \frac{1}{1 - x^5} \frac{1}{1 - x^{10}}$$

a protože

$$\frac{1 - x^{10}}{1 - x^5} = 1 + x^5 \text{ a } \frac{1 - x^{10}}{1 - x^2} = 1 + x^2 + x^4 + x^6 + x^8,$$

můžeme ji upravit do tvaru

$$G(x) = \frac{(1 + x^2 + x^4 + x^6 + x^8)(1 + x^5)}{(1 - x^{10})^3}.$$

Podle binomické věty máme

$$(1-x^{10})^3 = \sum_{k=0}^{\infty} (-1)^k \binom{-3}{k} x^{10k}$$

a tedy

$$G(x) = (1+x^2+x^4+x^5+x^6+x^7+x^8+x^9+x^{11}+x^{13}) \sum_{k=0}^{\infty} (-1)^k \binom{-3}{k} x^{10k}$$

Mocninu $x^{70}$ dostaneme jediným způsobem a to jako $7.10+0$, tj. koeficient u $x^{70}$ je

$$[x^{70}]G(x) = -\binom{-3}{7} = \binom{3+7-1}{7} = \frac{9.8}{2} = 36.$$

□