**První písemná zkouška MB204 22.5.2013**

**1.** Ukažte, že nejmenší primitivní kořen modulo 41, tj. generátor grupy $(\mathbb{Z}_{41}^{\times}, \cdot)$, je $g = 6$. Tohoto kořene využijte k vyřešení binomické kongruence $x^2 \equiv 4 \pmod{41}$. Můžeme říct, kolik řešení má tato kongruence modulo 41, aniž bychom je museli explicitně spočítat?

**Řešení**. $2^{\frac{41-1}{2}} \equiv 1$, $3^{\frac{41-1}{5}} \equiv 1$, $5^{\frac{41-1}{2}} \equiv 1$ mod 41 a zároveň $6^{\frac{41-1}{2}} \equiv 10 \neq 1$ a $6^{\frac{41-1}{5}} \equiv -1$ mod 41. Dále $6^6 \equiv -2 \Rightarrow 4 \equiv 6^{12}$ a tedy pro $x = 6^t$ platí $6^{2t} \equiv 6^{12}$ mod 41, což je ekvivalentní $2t \equiv 12$ mod $\varphi(41) = 40$, tj. $t \equiv 6$ mod 20. Řešením je tedy $6^6 \equiv -2$ a $6^{26} \equiv 2$. Kopngruence má právě dvě řešení protože $\varphi(41) = 40$ a $(40, 2) = 2$ a $4^{\frac{40}{2}} = 4^{20} = 2^{2.20} \equiv 1$. Tím pádem hned víme, že kongruence má právě řešení $x \equiv \pm 2$. □

**2.** O polynomu $p = x^6 + x^5 + 4x^4 + 2x^3 + 5x^2 + x + 2$ víte, že má vícenásobný kořen $x = i$. Rozložte jej na ireducibilní polynomy v $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Z}_2[x], \mathbb{Z}_5[x]$ a $\mathbb{Z}_7[x]$. Polynom $q = x^2y^2 + y^2 + xy + x^2y + 2y + 1$ vydělte se zbytkem ireducibilními faktory polynomu $p$ v $\mathbb{R}[x]$ a výsledek využijte k vyřešení soustavy polynomiálních rovnic $p = q = 0$ nad $\mathbb{C}$.

**Řešení**. $p = (x^2+1)^2(x^2+x+2)$, v $\mathbb{Z}_2$: $p = x(x+1)^5$, v $\mathbb{Z}_5$: $p = (x-2)^2(x+2)^2(x^2+x+2)$, v $\mathbb{Z}_7$: $p = (x^2+1)^2(x+4)^2$. Pro druhý polynom dostáváme $q = (y^2+y)(x^2+x+2) - y^2(x+1) + 1$ a $q = (y^2+y)(x^2+1) + y(x+1) + 1$. Je-li tedy $x = \alpha$ kořenem $x^2+x+2$, tj. $\alpha = -\frac{1}{2} \pm \frac{1}{2}i\sqrt{7}$, pak je $y = \frac{1}{\sqrt{1+\alpha}}$. Pokud $x = \beta$ je kořenem faktoru $x^2+1$, tj. $\beta = \pm i$, pak je $y = -\frac{1}{1+\beta}$ □

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

- (a) Zakódujte zprávu 1100011.
- (b) Obdrželi jste kód 10111010001. 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) $x^4 \equiv x+1$, $x^5 \equiv x^2+x$, $x^9 \equiv x^3+x$, $x^{10} \equiv x^2+x+1 \Rightarrow 1+x+x^5+x^6 \mapsto x^4+x^5+x^9+x^{10}+x+1+x^2+x+x^3+x+x^2+x+1 = x^3+x^4+x^5+x^9+x^{10}$. Kód je tedy 00011100011. (b) $1+x^2+x^3+x^4+x^6+x^{10}$ dává po dělení $x^4+x+1$ zbytek $x^2+1 \equiv x^8$. Došlo tedy k chybě na devátém bitu a původní zpráva byla 1010101. (c) Buď nastala chyba na prvním a třetím bitu $(x^2+1)$, nebo na pátém a šestém $(x^4+x^5 \equiv x^2+1)$. V prvním případě byla zpráva 1010001, ve druhém 0110001. □

**4.** Najděte vytvořující funkci a explicitní vyjádření pro $n$-tý člen posloupnosti $\{a_n\}$ definované rekurentním vztahem

$$a_0 = 1, a_1 = 2$$
$$a_n = 4a_{n-1} - 3a_{n-2} + 1 \text{ pro } n \geq 2.$$

**Řešení**. Univerzální formule platná pro všechna $n \in \mathbb{Z}$ je $a_n = 4a_{n-1} - 3a_{n-2} + 1 - 3[n=1]$. Vynásobením $x^n$ a sečtením přes všechna $n$ dostaneme rovnici pro vytvořující funkci $A(x) = \sum_{n=0}^{\infty} a_nx^n$, ze které vyjádříme $A(x) = \frac{3x^2-3x+1}{(1-x)^2(1-3x)} = \frac{3}{4}\frac{1}{1-x} - \frac{1}{2}\frac{1}{(1-x)^2} + \frac{3}{4}\frac{1}{1-3x}$. Takže člen u $x^n$ je $a_n = \frac{3}{4}(-1)^k\binom{-1}{n} - \frac{1}{2}(-1)^n\binom{-2}{n} + \frac{3}{4}(-3)^n\binom{-1}{n} = \frac{3}{4} - \frac{1}{2}(n+1) + \frac{3}{4}3^n = \frac{1-2n+3^{n+1}}{4}$ □