# Vnitrosemestrální písemka – MIN401 – jaro 2021 – 30. 4. 2021

Veškeré odpovědi musí být zdůvodněny a výpočty musí být doprovozeny komentářem. (Řešení sestávající pouze z odpovědí budou považována za opsaná a hodnocena 0 body.)

**1.** (3 body)

(i) Ukažte, že $5|(67^{41}+2)^9+1$.

(ii) Rozhodněte, zda $25|(67^{41}+2)^9+1$.

**2.** (5 bodů)

(i) Rozhodněte, zda existuje primitivní kořen modulo 32.

(ii) Určete inverzní prvek k 5 modulo 32.

(iii) Určete řád 5 modulo 32.

(iv) Najděte nějaké $a \in \mathbb{Z}$ řádu 2 modulo 32.

(v) Určete počet prvků v množinách

$$M_1 = \{1, 5, 5^2, 5^3, \dots\} \qquad \text{a} \qquad M_2 = \{-1, -5, -5^2, -5^3, \dots\}$$

modulo 32 a rozhodněte, které z těchto prvků jsou invertibilní.

(vi) Ukažte, $M_1 \cap M_2 = \emptyset$ modulo 32.

(vii) Ukažte, že každé $x$ splňující kongruenci

$$x^3 \equiv 25 \mod 32$$

je invertibilní modulo 32 a pak tuto kongruenci vyřešte.

**3.** (2 body) Nalezněte všechna řešení kongruence

$$3x^2 - 4x + 17 \equiv 0 \mod 13.$$

.

# Řešení a bodování:

**1. [3 body]**

(i) Modulo 5 platí

$$(67^{41}+2)^9+1 \equiv (2^{41}+2)^9+1 \equiv (2^{10\cdot 4+1}+2)^9+1 \equiv (2+2)^9+1 \equiv (-1)^9+1 \equiv 0,$$

neboť $2^{\varphi(5)} = 2^4 \equiv 1 \mod 5$.

(ii) Modulo 25 platí

$$(67^{41}+2)^9+1 \equiv (17^{41}+2)^9+1 \equiv (17^{2\cdot 20+1}+2)^9+1 \equiv (17+2)^9+1 \equiv 19^9+1 \equiv (-6)^9+1,$$

neboť $17^{\varphi(25)} = 17^{20} \equiv 1 \mod 25$. Dalším výpočtem modulo 25 dostaneme

$$(-6)^9+1 \equiv -2^9\cdot(3^3)^3+1 \equiv -2^9\cdot 2^3+1 \equiv -64^2+1 \equiv -14^2+1 \equiv -196+1 \equiv -(-4)+1 \equiv 5,$$

tj. 25 nedělí $(67^{41}+2)^9+1$.

**2. [5 bodů]**

(i) Neexistuje, neboť 32 není mocnina lichého prvočíslo ani dvojnásobek mocniny lichého prvočísla.

(ii) Inverzní prvek k 5 modulo 32 jistě existuje, protože $(5, 32) = 1$. Z Bezoutovi rovnosti $5\cdot 13 - 2\cdot 32 = 1$ plyne $5\cdot 13 \equiv 1 \mod 32$, tedy hledaná inverze je 13.

(iii) Máme $\varphi(32) = 16$, což má dělitele tvaru $2^k$, $0 \le k \le 4$. Tedy možné řády jsou 2, 4 a 8 (16 by byl řád primitivního kořene, který 32 nemá). Postupným zkoušením se zjistí, že řád 5 je 8.

(iv) $5^4$.

(v) Platí $|M_1| = |M_2| = 8$, protože řád 5 modulo 32 je 8. Prvky v těchto množinách jsou liché a tedy invertibilní.

(vi) Je-li $a \in M_1 \cap M_2$, $0 \le i, j \le 7$ pak $a \equiv 5^i \equiv -5^j \mod 32$. Předpokládejme $i \le j$ (opačná nerovnost se ukáže podobně); pak $5^i + 5^j \equiv 5^i(5^{j-i}+1) \equiv 0 \mod 32$, tj. $5^{j-i} \equiv -1 \mod 32$. Vzhledem k řádu 5 pak nutně $j - i = 4$, ale přímým výpočtem se lehce ověří, že $5^4 \not\equiv -1 \mod 32$.

(vii) Invertibilní jsou čísla nesoudělná s 32, což jsou právě lichá čísla. Tedy každé řešení $x$ kongruence je invertibilní, tj. $x = 5^\ell$ nebo $x = -5^\ell$ pro nějaké $0 \le \ell \le 7$. v Prvním případě dosazením dostaneme $5^{3\ell} \equiv 5^2 \mod 32$, tj. $3\ell \equiv 2 \mod \varphi(32)$, tj. $5^{3\ell} \equiv 5^2 \mod 16$. Tato kongruence má jediné řešení $\ell \equiv 6 \mod 16$, tj. řešením kongruence je $5^6 \mod 32$. Případ $x = -5^\ell$ nemůže být řešením, neboť $M_1 \cap M_2 = \emptyset$.

**3. [2 body]** Levou stranu kongruence vynásobíme 4 (abychom u $x^2$ dostali koeficient $-1$) a upravíme modulo 13:

$$4(3x^2-4x+17) \equiv -x^2-3x+3 \equiv x^2+3x-3 \equiv x^2-10x-3 \equiv (x-5)^2-28 \equiv (x-5)^2-2.$$

Substitucí $y = x-2$ dostaneme kongruenci $y^2 \equiv 2 \mod 13$, která nemá řešení. Vskutku, použitím kritéria z přednáška pro $d := (3, \varphi(13)) = 3$ dostaneme $2^{\frac{\varphi(13)}{d}} = 2^{\frac{12}{3}} = 2^4 \not\equiv 1 \mod 13$. Zadaná kongruence $3x^2 - 4x + 17 \equiv 0 \mod 13$ tedy nemá řešení.