# Teorie čísel: Cvičení 13

Simona Hlavinková, email: simonkahlavinkova@gmail.com

**Definice.** Buď $G(\cdot)$ grupa, $a, b \in G$. Prvek $a$ *míjí* prvek $b$, pokud $a^i \neq b$ a $b^i \neq a$ pro všechna $i \in \mathbb{Z}$.

V aditivním zápise tedy požadujeme $ka \neq b$ a $kb \neq a$ pro každé $k \in \mathbb{Z}$. Jednu i druhou podmínku lze přepsat jako $a \notin \langle b \rangle$ a $b \notin \langle a \rangle$. Zjevně se jedná o symetrickou relaci.

**Definice.** Číslo $N \in \mathbb{N}$ se nazývá *Carmichaelovo číslo*, pokud není prvočíslo a pro všechna $a \in \mathbb{Z}$, $\mathrm{NSD}(a, N) = 1$, platí $a^{N-1} \equiv 1 \pmod{N}$.

**Definice.** Buď $N \in \mathbb{N}$ složené liché, $N - 1 = 2^e m, m$ liché. Pokud pro $0 < a < N$ platí, že

$$(\heartsuit) \quad \begin{cases} a^{m2^j} \equiv -1 & \pmod{N} \text{ pro nějaké } 0 \leq j < e, \text{ nebo} \\ a^m \equiv 1 & \pmod{N}, \end{cases}$$

nazývá se $N$ *silné pseudoprvočíslo v bázi* $a$, neboli $a$ je (Rabin–Millerův) *lhář* pro $N$. Naopak, pokud $a$ nesplňuje podmínku $(\heartsuit)$, nazývá se $a$ *svědek* složenosti $N$.

-2. Vyřešte kongruenci $x^3 \equiv 1 \pmod{13}$.

-1. V grupě $\mathbb{Z}_{45}$ najděte všechny prvky, které míjejí prvek (a) 5, (b) 2, (c) 3.

0. Najděte nějakého lháře různého od 1 a nesoudělného svědka pro (a) $N = 51$, (b) $N = 221$, (c) $N = 365$, (d) $N = 93$.

! 1. Vyřešte kongruence
   (a) $x^5 \equiv 1 \pmod{13}$,
   (b) $x^{10} \equiv 1 \pmod{13}$,
   (c) $x^4 \equiv 3 \pmod{13}$,
   (d) $x^5 \equiv 8 \pmod{11}$,
   (e) $x^4 \equiv 9 \pmod{11}$.

! 2. V grupě $\mathbb{Z}_{60}$ najděte všechny prvky, které míjejí prvek (a) 7, (b) 2, (c) 4, (d) 6.

! 3. Ukažte, že $561 = 3 \cdot 11 \cdot 17$ a $1105 = 5 \cdot 13 \cdot 17$ jsou Carmichaelova čísla.

! 4. Najděte všechna $0 < a < 9$ taková, že $a$ je lhář pro 9.

! 5. Najděte nějakého lháře různého od 1 a nesoudělného svědka pro
   (a) $N = 39$,
   (b) $N = 121$.

! 6. Najděte všechna $0 < a < 77$ taková, že $a$ je lhář pro 77.

! 7. Pomocí Rabin–Millerova testu ukažte, že 7 je prvočíslo.

8. Nechť $A$, $B$ jsou grupy, $(e, f) \in A \times B$, $a \in A$. Pokud $a$ míjí $e$ v $A$, pak pro každé $b \in B$ prvek $(a, b)$ míjí prvek $(e, f)$ v $A \times B$.

9. Nechť $p > 2$ je prvočíslo. Dokažte, že $-1$ je jediná involuce v $\mathbb{Z}_p^*$.

10. V grupě $\mathbb{Z}_{100}$ najděte všechny prvky, které míjejí prvek (a) 7, (b) 5, (c) 20, (d) 85.

∗ 11. Najděte všechna $n \in \mathbb{N}$, pro něž platí, že všechny prvky $\mathbb{Z}_n^* \setminus \{1\}$ jsou involuce.

∗ 12. Najděte obecné kritérium, kdy se v $\mathbb{Z}_n$ míjejí prvky $a$ a $b$.

∗ 13. Buď $p$ prvočíslo. Dokažte, že pak číslo $p^k$ není Carmichaelovo číslo pro žádné $k \in \mathbb{N}$.

∗ 14. Nechť $p$ a $q$ jsou dvě různá prvočísla. Ukažte, že $pq$ není Carmichaelovo číslo.

*Úlohy s nekladným číslem budou předvedeny na cvičení jako vzorové.*
*Úlohy s ! je doporučeno řešit přednostně.*
*Úlohy s ∗ jsou náročnější. (Tentokrát jsou ale rozhodně všechny zvládnutelné, zvlášť s nápovědami.)*