

Teorie čísel: Cvičení 12

9. května 2022

Web: <https://www2.karlin.mff.cuni.cz/~raskam/vyuka/tc.html>

Email: raska.martin@gmail.com

Definice: Buď $G(\cdot)$ grupa. Prvek $a \in G$ je *involuce*, pokud má řád 2, čili $a \neq 1$ a $a^2 = 1$.

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 $i \in \mathbb{Z}$.

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

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

-1. Najděte všechny involuce v \mathbb{Z}_{15}^* a dokažte, že tato grupa není cyklická.

0. V grupě \mathbb{Z}_{45} najděte všechny prvky, které míjí prvek

- (a) 5,
- (b) 2,
- (c) 3.

! 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) $x^5 \equiv 2 \pmod{13}$,
- (e) $x^5 \equiv 8 \pmod{11}$,
- (f) $x^4 \equiv 9 \pmod{11}$.

! 2. Najděte všechny involuce v grupě

- (a) \mathbb{Z}_{30}^* ,
- (b) \mathbb{Z}_{51}^* .

! 3. V grupě \mathbb{Z}_{60} najděte všechny prvky, které míjí prvek

- (a) 7,
- (b) 2,
- (c) 4,
- (d) 6.

! 4. Ukažte, že 561 a 1105 jsou Carmichaelova čísla.

5. Necht' 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 $A \times B$.

6. Necht' $p > 2$ je prvočíslo. Pak -1 je jediná involuce v \mathbb{Z}_p^* .

* 7. Najděte všechna $n \in \mathbb{N}$ takové, že všechny prvky $\mathbb{Z}_n^* \setminus \{1\}$ jsou involuce.

* 8. Najděte obecné kritérium, kdy se v \mathbb{Z}_n míjí prvky a a b .

* 9. Buď p prvočíslo. Dokažte, že pak číslo p^k není Carmichaelovo číslo pro libovolné $k \in \mathbb{N}$.

* 10. Necht' p a q jsou dvě různá prvočísla. Ukažte, že číslo $p \cdot q$ není Carmichaelovo číslo.

Úlohy s nekladným číslem budou předvedeny na cvičení jako vzorové.

Úlohy s ! je doporučeno řešit přednostně.

Úlohy s * jsou náročnější.