Teorie čísel: Cvičení 12

Simona Hlavinková, email: simonkahlavinkova@gmail.com

Definice. Je-li grupa $\mathbb{Z}_n^*$ cyklická, nazýváme libovolný její generátor *primitivní prvek* modulo n.

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

Věta. *Je-li p liché prvočíslo a $e \geq 1$, pak $\mathbb{Z}_{p^e}^* \simeq \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{e-1}} \simeq \mathbb{Z}_{(p-1)p^{e-1}}$, což je cyklická grupa. Je-li $e \geq 2$, pak $\mathbb{Z}_{2^e}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{e-2}}$, což pro $e \geq 3$ není cyklická grupa.*

-2. Rozložte grupu $\mathbb{Z}_{360}^*$ na součin cyklických grup.

-1. Najděte všechny primitivní prvky modulo 11.

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

! 1. Najděte primitivní prvek modulo 125 a modulo 250.

! 2. Které z následujících grup jsou cyklické?
   (a) $\mathbb{Z}_4^*$,
   (b) $\mathbb{Z}_{14}^*$,
   (c) $\mathbb{Z}_{16}^*$,
   (d) $\mathbb{Z}_{35}^*$.

! 3. Najděte všechny primitivní prvky modulo 13.

! 4. Rozložte následující grupy na součin cyklických grup:
   (a) $\mathbb{Z}_{45}^*$,
   (b) $\mathbb{Z}_{200}^*$,
   (c) $\mathbb{Z}_{64}^*$,
   (d) $\mathbb{Z}_{81}^*$.

! 5. Najděte všechny involuce v grupě
   (a) $\mathbb{Z}_{30}^*$,
   (b) $\mathbb{Z}_{51}^*$.

6. Nechť $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ je konečná komutativní grupa, $H \subseteq G$ a $g, h \in G$. Dokažte, že
   (a) H je podgrupa $\mathcal{G} \Leftrightarrow a \cdot b \in H \ \forall a, b \in H$,
   (b) $\mathrm{ord}(g \cdot h) = \mathrm{ord}(g) \cdot \mathrm{ord}(h)$, jestliže $\mathrm{NSD}(\mathrm{ord}(g), \mathrm{ord}(h)) = 1$
   (c) $\mathrm{ord}(g^a) = b$, jestliže $\mathrm{ord}(g) = ab$.

7. Najděte alespoň dva primitivní prvky modulo a) 49, b) 81, c) 26, d) 98, e) 45.

8. Nechť R a S jsou komutativní okruhy s jednotkou. Dokažte:
   (a) $(R \times S)^* = R^* \times S^*$,
   (b) $R \cong S \Rightarrow R^* \cong S^*$.
   (c) Pomocí ČZV dokažte: Pokud $n = p_1^{e_1} \cdots p_k^{e_k}$ je rozklad na prvočísla, pak $\mathbb{Z}_n^* \cong \mathbb{Z}_{{p_1}^{e_1}}^* \cdots \mathbb{Z}_{{p_k}^{e_k}}^*$.

9. Ukažte, že $\mathbb{Z}_{24}^* \ncong \mathbb{Z}_4^* \times \mathbb{Z}_6^*$. Rozložte $\mathbb{Z}_{24}^*$ na součin cyklických grup.

10. Dokažte, že pro sudé n obsahuje grupa $\mathbb{Z}_n$ právě jeden prvek řádu 2 a pro liché n neobsahuje $\mathbb{Z}_n$ žádný prvek řádu 2. Rozmyslete si, co z toho lze vyvodit pro cyklické grupy.

11. Určete počet primitivních prvků modulo p, kde p je prvočíslo.

12. Najděte izomorfismus mezi množinou $\{1, -1, \mathrm{i}, -\mathrm{i}\}$ s násobením a $\mathbb{Z}_4$.

13. Najděte všechna $n \in \mathbb{N}$, pro něž je grupa $\mathbb{Z}_n^*$ je cyklická.

Úlohy s nekladným číslem budou předvedeny na cvičení jako vzorové.
Úlohy s ! je doporučeno řešit přednostně.
Úlohy s $*$ jsou náročnější.