Teorie čísel: Cvičení 11

2. květen 2022

Web: https://www2.karlin.mff.cuni.cz/~raskam/vyuka/tc.html
Email: raska.martin@gmail.com

Definice: Nechť $n \geq 2$. Pokud je $\mathbb{Z}_n^*$ cyklická, tak se její libovolný generátor nazývá *primitivní prvek modulo n*.
Věta: Je-li p liché prvočíslo a $e \geq 1$, pak

$$\mathbb{Z}_{p^e}^*(\cdot) \simeq \mathbb{Z}_{p-1}(+) \times \mathbb{Z}_{p^{e-1}}(+) \simeq \mathbb{Z}_{(p-1)p^{e-1}}(+)$$

je cyklická grupa.
Je-li $e \geq 2$, pak

$$\mathbb{Z}_{2^e}^*(\cdot) \simeq \mathbb{Z}_2(+) \times \mathbb{Z}_{2^{e-2}}(+),$$

což není cyklická grupa, pokud $e \geq 3$.

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

-1. Najděte všechny primitivní prvky modulo 11.

0. Najděte primitivní prvek modulo 125 a modulo 250.

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

! 2. Najděte všechny primitivní prvky modulo 13.

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

! 4. Najděte alespoň 2 primitivní prvky modulo n, pro
   (a) $n = 49$,
   (b) $n = 81$,
   (c) $n = 26$,
   (d) $n = 98$,
   (e) $n = 45$.

5. Nechť R a S jsou komutativní okruhy s jednotkou. Dokažte:
   (a) $(R \times S)^* = R^* \times S^*$,
   (b) $R \cong S \implies R^* \cong S^*$.
   (c) Pomocí Čínské věty o zbytcích dokažte: Pokud $n = p_1^{e_1} \cdot ... \cdot p_k^{e_k}$ je rozklad na prvočísla, pak $\mathbb{Z}_n^* \cong \mathbb{Z}_{{p_1}^{e_1}}^* \times ... \times \mathbb{Z}_{{p_k}^{e_k}}^*$.

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

7. 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.

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

9. Najděte izomorfizmus mezi množinou $\{1, -1, i, -i\}$ s násobením a $\mathbb{Z}_4$.

10. Najděte všechny $n \in \mathbb{N}$ takové, že 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.