Teorie čísel: Cvičení 7

Simona Hlavinková; email: simonkahlavinkova@gmail.com

-1. Napište číslo (a) 13, (b) 29 jako součet dvou čtverců. Kolika způsoby je to možné provést?

0. Najděte ireducibilní rozklady čísel 260 a $18 + 6i$ v oboru Gaussový celých čísel $\mathbb{Z}[i]$.

! 1. Najděte až na asociovanost všechny ireducibilní prvky oboru $\mathbb{Z}[i]$ s normou menší než 20.

2. Rozhodněte, zda existují Gaussova celá čísla s normou 7, 10, 11, 15, 31, 37, 178.

Definice. Grupa $(G, \cdot, ^{-1}, 1)$ se nazývá *cyklická*, pokud existuje prvek $g \in G$ takový, že $\langle g \rangle = G$, čili g generuje celou grupu G – pro každé $h \in G$ tedy existuje $n \in \mathbb{Z}$ splňující $g^n = h$. (Upozornění: Ve sčítacích grupách píšeme přirozeně $ng = h$ místo $g^n = h$.) Každá cyklická grupa je abelovská, tj. komutativní.

Poznámka. Množina $\mathbb{Z}_n = \{0, \ldots, n-1\}$ zbytků po dělení n přirozeně tvoří grupu $(\mathbb{Z}_n, +, -, 0)$. Když píšeme $\mathbb{Z}_n$, myslí se tím vždy tato sčítací grupa. Pokud nás zajímá grupa zbytků modulo n s násobením (značíme ji $\mathbb{Z}_n^*$), pak její nosná množina obsahuje právě ty prvky, které mají inverzní prvek (z Algebry byste měli vědět, že jsou to právě prvky $a \in \mathbb{Z}_n$, pro které $\mathrm{NSD}(a, n) = 1$).

Definice. Nechť $n \geq 2$. Pokud je $\mathbb{Z}_n^*$ cyklická, tak se její libovolný generátor nazývá *primitivní prvek* modulo n. (Na přednášce se brzo dokáže, že primitivní prvek existuje, právě když $n = p^k$ nebo $n = 2p^k$ pro liché prvočíslo p, nebo $n = 2, 4$.)

Definice. Pro prvek $a \in G$ ještě zavedeme pojem *řád* prvku a. Jde o nejmenší přirozené k splňující $a^k = 1$, a značíme ho $\mathrm{ord}(a)$. Je-li G konečná, pak podle Lagrangeovy věty řád každého prvku dělí $|G|$.

! 3. Najděte všechny generátory grupy $\mathbb{Z}_{12}$.

! 4. Rozhodněte, zda jsou grupy $\mathbb{Z}_{11}^*$ a $\mathbb{Z}_8^*$ cyklické; pokud ano, najděte v nich nějaký primitivní prvek.

5. Rozmyslete si následující fakta o generátorech grup $\mathbb{Z}_n$:
   ! (a) Najděte všechny generátory grupy $\mathbb{Z}_{18}$.
   (b) Které prvky $\mathbb{Z}_n$ určitě nemohou generovat celou grupu $\mathbb{Z}_n$?
   (c) Popište všechny generátory grupy $\mathbb{Z}_n$. (Nápověda: Bézoutovy koeficienty)

! 6. Určete řády všech prvků v grupách $\mathbb{Z}_7$ a $\mathbb{Z}_7^*$.

! 7. Rozhodněte, které z grup $\mathbb{Z}_5^*$, $\mathbb{Z}_6^*$, $\mathbb{Z}_9^*$, $\mathbb{Z}_{12}^*$ jsou cyklické.

8. Platí, že pro každé prvočíslo p existuje primitivní prvek modulo p.
   (a) Najděte nějaký primitivní prvek modulo 3, 5 a 7.
   (b) Pomocí části (a) sestrojte izomorfizmus grup $\mathbb{Z}_7^*$ a $\mathbb{Z}_6$.

9. Uvažujme grupu $\mathbb{Z}_p^*$, kde p je prvočíslo.
   (a) Najděte všechny prvky této grupy. Kolik jich je?
   (b) Víme, že tato grupa je cyklická. Označme některý její generátor a. Jaký řád má a v grupě $\mathbb{Z}_p^*$?

10. Najděte všechny primitivní prvky modulo 7.

11. Které prvky obsahuje grupa invertibilních prvků oboru $\mathbb{Z}[i]$? Je tato grupa cyklická?

∗ 12. Jestliže p je prvočíslo a $a \in \mathbb{Z}_p$ splňující $p \equiv 1 \pmod 4$ a $a \equiv (\frac{p-1}{2})! \pmod p$, dokažte, že $\mathrm{NSD}_{\mathbb{Z}[i]}(a + i, p)$ je v oboru $\mathbb{Z}[i]$ ireducibilní prvek s normou p.

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