Teorie čísel: Cvičení 7 – výsledky, nápovědy, vzorová řešení

Simona Hlavinková; email: simonkahlavinkova@gmail.com

Nápovědy:

-1. Jde to kvůli gaussovskosti oboru $\mathbb{Z}[i]$ až na pořadí jediným způsobem, který zkusmo snadno najdeme.

0. Nejprve rozložíme normu a podle toho, zda jsou prvočísla modulo čtyři kongruentní 1 nebo -1 rozkládáme dál.

1. Připadají v úvahu jen čísla s prvočíselnou normou kongruentní 1 modulo čtyři a se čtvecem prvočíselné normy kongruentním -1 modulo čtyři.

1. Nepřipadají v úvahu čísla s lichou valuací prvočísla s normou kongruentní -1 modulo čtyři.

3. Buď vycházejte přímo z definice, nebo uvažujte např. o největších společných dělitelích.

4. Vycházejte přímo z definice. To, kdy primitivní prvek existuje, je ostatně bez důkazu napsáno nahoře na papíru se zadáním.

5. Postupujte jako v příkladu 3.

6. Je poměrně snadné to spočítat přímo. Znáte-li Lagrangeovu větu, hodí se využít k tomu, abyste předem vyloučili některé hodnoty řádů.

7. Hledáte primitivní prvek. Na to neexistuje žádný příliš chytrý způsob: Zkoušejte prvky postupně, dokud nebudete mít štěstí. Můžete si trochu pomoci Lagrangeovou větou.

8. Hledání primitivních prvků funguje podobně jako v úloze 5.; při sestavování izomorfismu je klíčové určit obraz generátoru cyklické grupy, tj. primitivního prvku.

9. První dvě části by měly být až směšně snadné. Ve třetí části si uvědomte, že máme dvě cyklické grupy a generátor jedné by se měl zobrazit na generátor druhé.

10. Výsledek už znáte z úlohy 6.

11. Jsou to čtyři prvky s normou 1, grupu generuje prvek $\pm i$.

12. Stačí uvážit, že $\mathrm{NSD}(a+i,p) = \mathrm{NSD}((\frac{p-1}{2})! + i, p)$ a použít argument důkazu Věty 3.2.

Výsledky:

-1. $13 = 3^2 + 2^2$, $29 = 5^2 + 2^2$.

0. $260 = (1+i)(1-i)(1+i)(1-i)(2+i)(2-i)(3+2i)(3-2i)$,
$18 + 6i = 3(1+i)(1-i)(1+i)(2-i)$.

1. $1+i$, 3, $2+i$, $3+2i$, $4+i$.

2. Existují jen ta s normou 10, 37, 178.

3. $1, 5, 7, 11$. Jde právě o čísla nesoudělná s 12.

4. Grupa $\mathbb{Z}_{11}^*$ je cyklická a primitivním prvkem je například 2. Grupa $\mathbb{Z}_8^*$ cyklická není.

5. a) Jde o čísla $1, 5, 7, 11, 13, 17$, tj. čísla nesoudělná s 18. b) Žádné číslo soudělné s n může nagenerovat zase jen prvky soudělné s n. c) Vždy jde právě o prvky nesoudělné s n.

6. V $\mathbb{Z}_7$ máme $\mathrm{ord}(0) = 1$, všechny ostatní prvky mají řád 7. (Každý nenulový prvek je tedy generátorem $\mathbb{Z}_7$.) V $\mathbb{Z}_7^*$ máme $\mathrm{ord}(1) = 1$, $\mathrm{ord}(6) = 2$ $\mathrm{ord}(2) = \mathrm{ord}(4) = 3$, a konečně $\mathrm{ord}(3) = \mathrm{ord}(5) = 6$.

7. Cyklické jsou právě $\mathbb{Z}_5^*$ (primitivní prvky $2, 3$), $\mathbb{Z}_6^*$ (primitivní prvek 5) a $\mathbb{Z}_9^*$ (primitivní prvky $2, 5$). Grupa $\mathbb{Z}_{12}^*$ naopak cyklická není, neboť v ní všechny prvky mají řád nanejvýš 2. (Výsledek jsme samozřejmě věděli předem: Grupa $\mathbb{Z}_n^*$ je cyklická právě tehdy, když n je $2, 4$ nebo p^k či $2p^k$ pro liché prvočíslo p. Čísla 5, 6 a 9 požadovaného tvaru jsou, zatímco 12 nikoli.)

8. (a) Primitivní prvek modulo 3 je 2; modulo 5 jde o čísla $2, 3$; modulo 7 o $3, 5$.
   (b) Existují dva izomorfismy; první zobrazuje čísla $1, 3, 2, 6, 4, 5$ postupně na $0, 1, 2, 3, 4, 5$; druhý takto zobrazuje čísla $1, 5, 4, 6, 2, 3$.

9. (a) Jde o nenulové zbytky modulo p: $\{1, \ldots, p-1\}$. Je jich $p-1$.
   (b) Má řád $|\mathbb{Z}_p^*| = p-1$.
   (c) Zvolíme-li primitivní prvek a v $\mathbb{Z}_p^*$, je jeden izomorfismus popsán vztahem $\varphi(a^k) = k$.

10. Jde o prvky 3 a 5.

Řešení vybraných příkladů:

3. $\mathbb{Z}_{12} = \{0, 1, \ldots, 11\}$. Zřejmě $a \in \mathbb{Z}_{12}$ generuje $\mathbb{Z}_{12}$ právě tehdy, když $\mathbb{Z}_{12} = \{na \mid n \in \mathbb{Z}\}$. Vzhledem k tomu, že navíc $12a = 0$, tak se ekvivalentně ptáme, kdy $\mathbb{Z}_{12} = \{na \mid n = 0, 1, \ldots, 11\}$.

   Dále si všimněme, že pokud $d = \mathrm{NSD}(a, 12) > 1$, tak $d \mid na$ pro všechna n, tedy se nikdy nemůže stát $na = 1$ a a negeneruje celou $\mathbb{Z}_{12}$. Zbývá dokázat, že všechny zbylé $a \in \mathbb{Z}_{12}$, $\mathrm{NSD}(a, 12) = 1$ jsou generátory $\mathbb{Z}_{12}$.

   Zřejmě $\langle 1 \rangle = \mathbb{Z}_{12}$. Pro $a \in \{5, 7, 11\}$ si jde buď vypsat celou množinu $\{na \mid n = 0, 1, \ldots, 11\}$ (např. pro $a = 5$ vyjde $0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7$, tedy $\langle 5 \rangle = \mathbb{Z}_{12}$), nebo můžeme najít odpověď na otázku, zda má kongruence $na \equiv b \pmod{12}$ řešení $n \in \mathbb{Z}$ pro libovolné $b \in \mathbb{Z}$.

   Pro $a = 5$ z Bézoutovy rovnosti díky $\mathrm{NSD}(5, 12) = 1$ najdeme $n, m \in \mathbb{Z}$, že $5n + 12m = 1$, tedy $5n \equiv 1 \pmod{12}$. Neboli 5 má inverz modulo 12 a kongruence $5n \equiv 1 \pmod{12}$ má řešení. Pak má samozřejmě řešení i každá kongruence $b \equiv 5(nb) \pmod{12}$, a tedy $\langle 5 \rangle = \mathbb{Z}_{12}$.

   Rozmyslete si, že podobný argument lze použít i pro $a = 7, 11$. V úloze 1 si rozmyslíte, že tento argument jde zobecnit pro libovolné $\mathbb{Z}_n$.

   Generátory $\mathbb{Z}_{12}$ jsou $1, 5, 7, 11$.

4. a) Protože 11 je prvočíslo, tak z přednášky / teorie v horní části papíru víme, že grupa je cyklická. Ale tuto znalost ani nepotřebujeme, příklad vyřešíme prostě nalezením konkrétního primitivního prvku. $|\mathbb{Z}_{11}^*| = 10$, řád libovolného prvku $a \in \mathbb{Z}_{11}^*$ tak z Lagrangeovy věty dělí 10, tedy $\mathrm{ord}(a) \in \{1, 2, 5, 10\}$. Řád jedna má pouze neutrální prvek (tj. 1), řád deset mají právě primitivní prvky. Tudíž pro ověření, že a je primitivní prvek, stačí ukázat, že $a, a^2, a^5 \neq 1$.

   Zkusme například $a = 2$. Pak $a = 2 \neq 1$, $a^2 = 2^2 = 4 \neq 1$ a $a^5 = 10 \neq 1$. Řád 2 je tak nutně 10 a 2 je primitivní prvek.

   b) $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$, hledáme prvek řádu 4. Nicméně 1 má řád 1 a pro zbylé prvky platí $3^2 = 5^2 = 7^2 = 1$, a tedy mají řád 2. Vidíme tedy, že žádný prvek negeneruje celou $\mathbb{Z}_8^*$ a grupa není cyklická.

5. a) $\mathbb{Z}_{18} = \{0, 1, \ldots, 17\}$. Analogicky k úloze -2. pro $a \in \mathbb{Z}_{18}$ platí, že pokud $\mathrm{NSD}(a, 18) > 1$, tak $\mathrm{NSD}(a, 18) \mid na$ pro všechna n a $\langle a \rangle \subsetneq \mathbb{Z}_{18}$.

   Pro $\mathrm{NSD}(a, 18) = 1$, tedy $a \in \{1, 5, 7, 11, 13, 17\}$, lze stejně jako v -2. ukázat, že skutečně generují celou $\mathbb{Z}_{18}$.

   b) Pokud pro $a \in \mathbb{Z}_n$ platí $d = \mathrm{NSD}(a, n) > 1$, tak $d \mid na$ pro všechna n, $1 \notin \langle a \rangle \subsetneq \mathbb{Z}_{18}$ a a tak negeneruje celou $\mathbb{Z}_n$.

   c) V návaznosti na část b) si rozmyslíme, že všechny prvky splňující $\mathrm{NSD}(a, n) = 1$ už jsou generátory. Jde o přímé zobecnění důkazu provedeného v příkladu -2.

   Z Bézoutovy rovnosti díky $\mathrm{NSD}(a, n) = 1$ najdeme $x, y \in \mathbb{Z}$, že $xa + yn = 1$, tedy $xa \equiv 1 \pmod{n}$. Neboli a má inverz modulo n a kongruence $ax \equiv 1 \pmod{n}$ má řešení. Rovněž pak má řešení i kongruence $b \equiv a(xb) \pmod{n}$, a tedy $\langle a \rangle = \mathbb{Z}_n$.

6. a) Z Lagrangeovy věty platí, že řády prvků jsou buď 1 nebo 7. Očividně jediný prvek řádu 1 je 0 (jednotka v této grupě) a ostatní prvky budou mít řád 7.

   b) $\mathbb{Z}_7^*$ je cyklická, jak víme. Buď můžeme řády spočítat pro každý prvek zvlášť, nebo si pro zjednodušení práce můžeme najít nějaký primitivní prvek modulo 7. S trochou snahy zjistíme, že je jím například 3 (nebo si vzpomeneme na minulé cvičení). Každý prvek jde potom tedy zapsat ve tvaru 3^k, a hledáme nejmenší n takové, že $(3^k)^n = 1$, neboli $nk \equiv 0 \pmod 6$, neboť $3^6 = 1$. Z toho už snadno odvodíme, že $n = \frac{6}{\mathrm{NSD}(6,k)}$.

   Speciálně tak vidíme, že řád 1 má přesně $3^0 = 1$, řád 2 má přesně $3^3 = 6$, řád 3 mají přesně $3^2 = 2$, $3^4 = 4$ a řád 6 mají $3^1 = 3$, $3^5 = 5$.

8. b) Hledáme homomorfismus, který bude zároveň bijekce. Protože jsou velikosti grup shodné, tak stačí ukázat, že bude homomorfismus na celou grupu $\mathbb{Z}_6$. Toho lze docílit tím, že zobrazíme generátor $\mathbb{Z}_7^*$ (primitivní prvek modulo 7, např. 3) na generátor $\mathbb{Z}_6$ (např. 1). Chceme tak $\varphi(3) = 1$ a definujme tedy po prvcích bijekci $\varphi(3^k) = k$ pro $k \in \{0, \ldots, 5\}$. Zbývá ověřit, že je to homomorfismus (to jste viděli například ve skriptech nebo na minulém cviku při počítání charakterů).

9. a) Chceme právě prvky $a \in \mathbb{Z}_p$ nesoudělné s p, to jsou jistě všechny kromě 0, a tak $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$ a $|\mathbb{Z}_p^*| = p - 1$.

   b) Označme řád a jako k, tedy $a^k = 1$. Jistě $k \leq p - 1$, neboť řád prvku dělí řád grupy. Nicméně prvky generované a jsou v množině $1, a, a^2, \ldots a^{k-1}$ (libovolné jiné (i záporné) mocniny umíme přenásobením dostat na jednu z těchto). Prvek a má ale generovat celou $\mathbb{Z}_p^*$, tedy alespoň $p - 1$ prvků. Z toho už dostaneme i $k \geq p - 1$ a nutně $k = p - 1$.

   c) Podobně jako v předchozím případě definujeme zobrazení po prvcích jako $\varphi(a^k) = k$ a ověříme, že jde skutečně o dobře definovaný izomorfismus.

10. Stačí si uvědomit, že to jsou přesně prvky $\mathbb{Z}_7^*$ s řádem 6, což jsme už v úloze 4. určili, že jsou 3 a 5.

    Obecně, pokud už zvládneme najít jeden primitivní prvek (v tomto případě například 3), tak z postupu z příkladu 4 vyplývá, že ostatní získáme přesně tak, že tento prvek umocníme na čísla nesoudělná s řádem grupy. Speciálně v našem případě chceme umocnit 3 na čísla nesoudělná s $|\mathbb{Z}_7^*| = 6$, což dá přesně $3^1 = 3$ a $3^5 = 5$.