Teorie čísel: Cvičení 12 – výsledky, nápovědy, vzorová řešení

Simona Hlavinková, email: simonkahlavinkova@gmail.com

Nápovědy:

-2. Použijte standardní postup, tj. nejprve rozložte grupu na součin několika grup $\mathbb{Z}_{p^e}^*$ pomocí ČZV a následně využijte větu uvedenou v záhlaví cvičení.

-1. Jeden primitivní prvek g najděte jako na předešlých cvičeních (tj. uhodnutím a následným ověřením, že několik vhodných mocnin je různých od 1). Ostatní naleznete jako vhodné mocniny g.

0. Pracujte nezávisle modulo 3 a modulo 5 (ČZV). Kolik involucí může obsahovat cyklická grupa?

1. Primitivní prvek modulo 250 najdete díky ČZV snadno, znáte-li primitivní prvek modulo 125. K nalezení prvku modulo 5^3 lze šikovně využít všechny části nedokázané věty uvedené na cvičení.

2. Taky na to víceméně máme větu.

3. Jako příklad -1.

4. Jako příklad -2.

5. Hledejte všechna řešení $x^2 \equiv 1$ a na úplný závěr zahoďte jedničku. Použijte ČZV, nalezněte řešení modulo jednotlivá prvočísla a následně je pomocí ČZV zase slepte dohromady.

7. Jeden najdete podobně jako v příkladu 0. pomocí uvedené nedokázané věty; druhý se dá snadno určit třeba jako vhodná mocnina toho prvního.

8. Jde o vcelku elementární vlastnosti okruhů. Část c) vyplývá z b) a ČZV okamžitě.

9. Mají ty grupy vůbec stejný počet prvků? Rozklad na součin cyklických grup je standardní úloha, viz příklad -2.

10. První část plyne snadno z definice. Pokud jde o cyklické grupy, existují vlastně vůbec nějaké jiné než $\mathbb{Z}_n$?

11. Určujete počet generátorů jisté cyklické grupy; to už jste dokonce asi na některém cvičení dělali.

12. Generátor se musí zobrazit na generátor. (Existují dva takové izomorfismy.)

13. Využijte větu uvedenou na zadání. (Viz také důsledek 5.6 z přednášky.)

Výsledky:

1. a) ANO; b) ANO; c) NE; d) NE

2. $2, 6, 7, 11$

3. Uvedené grupy jsou izomorfní následujícím grupám:

   (a) $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3$;
   (b) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$;
   (c) $\mathbb{Z}_2 \times \mathbb{Z}_{16}$;
   (d) $\mathbb{Z}_2 \times \mathbb{Z}_{27}$;

   Není to jediná správná odpověď, protože například $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ a na obou stranách je součin cyklických grup.

4. V částech (a) až (d) je možností hodně. Správnost svého výsledku můžete ověřit například pomocí WolframAlpha zadáním dotazu typu ord_2(125) (nebo pomocí jiného matematického softwaru).

   V části (e) žádné primitivní prvky neexistují, protože grupa $\mathbb{Z}_{45}^*$ není cyklická.

5. (a) $11, 19, 29$,
   (b) $16, 35, 50$.

9. Grupy nejsou izomorfní, protože ani nemají stejný počet prvků. (Vidíme tedy, že předpoklad nesoudělnosti m, n je v ČZV důležitý.) Platí $\mathbb{Z}_{24}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

11. $\varphi(\varphi(p)) = \varphi(p-1)$

12. Izomorfismus je kompletně popsaný tím, že se i musí zobrazit na 1 nebo na 3. Explicitně jde tedy o zobrazení $\mathrm{i}^k \mapsto k$ a $\mathrm{i}^k \mapsto 3k$.

Vybraná vzorová řešení:

-2. Díky Čínské zbytkové větě platí $\mathbb{Z}_{360}^* \cong \mathbb{Z}_{2^3}^* \times \mathbb{Z}_{3^2}^* \times \mathbb{Z}_5^*$. Zdůvodněme si, proč. (Vám ale při řešení úloh stačí jen napsat, že toto platí díky ČZV, a dál to nerozpatlávat.) Formálně máte tvrzení „Pro nesoudělná m, n platí $\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$.“ dokázat v úloze 5., ale snad by pro vás mělo být alespoň na intuitivní úrovni vcelku uvěřitelné: Z ČZV víte, že platí izomorfismus okruhů $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. Jsou-li izomorfní okruhy, pak z toho snadno plyne, že jsou izomorfní jednak jejich sčítací grupy, jednak jejich násobicí grupy (to ověříte přímo z definice), takže $\mathbb{Z}_{mn}^* \cong (\mathbb{Z}_m \times \mathbb{Z}_n)^*$. Zbývá dokázat, že $(\mathbb{Z}_m \times \mathbb{Z}_n)^* = \mathbb{Z}_m^* \times \mathbb{Z}_n^*$, tj. že k prvku $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ existuje multiplikativní inverz právě tehdy, když existuje multiplikativní inverz pro $a \in \mathbb{Z}_m$ i pro $b \in \mathbb{Z}_n$. To není těžké tvrzení a platí obecně pro jakoukoliv dvojici okruhů, nejen pro $\mathbb{Z}_m$ a $\mathbb{Z}_n$.

Máme tedy $\mathbb{Z}_{360}^*$ rozložené na součin tří grup typu $\mathbb{Z}_n^*$, kde n je mocnina prvočísla. Pro takovéto grupy máme větu (napsanou přímo na zadání). Podle ní platí:

$$\mathbb{Z}_{2^3}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2; \qquad \mathbb{Z}_{3^2}^* \cong \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3; \qquad \mathbb{Z}_5^* \cong \mathbb{Z}_4.$$

Dohromady dostáváme

$$\mathbb{Z}_{360}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4.$$

Každá grupa $\mathbb{Z}_n$ je cyklická (až na izomorfismus dokonce ani jiné konečné cyklické grupy neexistují), takže jsme splnili úkol.

Ještě dva dodatky: Jednak, zadaná úloh nemá jediné řešení. Například nás nic nenutí rozkládat $\mathbb{Z}_6$ jako $\mathbb{Z}_2 \times \mathbb{Z}_3$, takže správnou odpovědí je zjevně i $\mathbb{Z}_{360}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_4$; navíc není těžké si (na základě ČZV) rozmyslet, že platí také $\mathbb{Z}_{360}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{12}$. Navíc samozřejmě můžeme jednotlivé grupy v součinu libovolně permutovat.

Zadruhé si můžeme položit otázku, není-li sama grupa $\mathbb{Z}_{360}^*$ cyklická. Obecnou odpověď poskytuje úloha 10., jejíž řešení je obsaženo i ve skriptech jako důsledek 5.6. Když ale využijeme zápis pomocí rozkladu $\mathbb{Z}_{360}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4$, snadno si rozmyslíme tento konkrétní příklad: Můžeme si všimnout, že v této grupě existuje více než jeden prvek řádu 2 (takzvaná *involuce*, např. $(1,0,0,0,0)$, $(0,1,0,0,0)$, …). Naopak v cyklických grupách (tj. $\mathbb{Z}_n$ pro nějaké přirozené číslo n) je vždy nanejvýš jeden prvek řádu 2, protože kongruence $2x \equiv 0 \pmod{n}$ má pro každé n nanejvýš jedno netriviální řešení. Z toho vidíme, že tato grupa není cyklická.

-1. Nejprve chceme nalézt jeden primitivní prvek. To se dělá tipováním: Zkusíme ověřit, že je 2 primitivní prvek. Máme $|\mathbb{Z}_{11}^*| = 10$, z Lagrangeovy věty proto v této grupě řád každého prvku dělí 10; jde tedy buď o $1, 2, 5$ (pokud prvek není primitivní), nebo o 10 (takový prvek generuje celou grupu, neboli je primitivní). Vidíme, že $2^1 \neq 1$, $2^2 = 4 \neq 1$ a $2^5 = -1 \neq 1$. Jediná zbývající možnost je $\mathrm{ord}(2) = 10$, takže 2 je skutečně primitivní prvek. Podobně bychom mohli i pro všechna ostatní čísla určit řády a tím zjistit, zda jde o primitivní prvky. To by ale znamenalo poměrně dost výpočtů. Ukážeme si chytřejší způsob využívající toho, že jeden generátor jsme již našli.

Z toho, že 2 je primitivní prvek, dostáváme explicitní izomorfismus $\mathbb{Z}_{10} \cong \mathbb{Z}_{11}^*$: Prvku $a \in \mathbb{Z}_{10}$ odpovídá $2^a \in \mathbb{Z}_{11}^*$.[1] Víme, že generátory $\mathbb{Z}_{10}$ jsou právě čísla nesoudělná s 10, tedy $1, 3, 7, 9$.

[1] Mimochodem, takovéto zobrazení je homomorfismem i v případě, že 2 nahradíme kterýmkoliv jiným prvkem $\mathbb{Z}_{10}$; izomorfismus je to ale právě tehdy, když použijeme primitivní prvek. A kdybychom zobrazovali do jiné grupy než $\mathbb{Z}_{11}^*$, může se to úplně pokazit – potřebujeme totiž $1 \in \mathbb{Z}_{10}$ zobrazit na prvek, jehož řád je dělitelem 10.

(Pokud si toto tvrzení nepamatujete, můžete si to snadno dokázat.) Zároveň musí izomorfismus zobrazovat generátory na generátory. Z toho dostáváme, že primitivní prvky modulo 11 jsou právě $2^1 = 2, 2^3 = 8, 2^7 = 7$ a $2^9 = 6$.

Aternativní postup, který klidně ignorujte: V tomto konkrétním případě lze určit primitivní prvky také tak, že ze $\mathbb{Z}_{11}^*$ zahodíme všechny kvadratické zbytky a ještě prvek -1. Kvadratické zbytky jsou $\{1, 4, 9, 16, 25\} = \{1, 4, 9, 5, 3\}$, takže vidíme, že skutečně platí $\mathbb{Z}_{11}^* \setminus \{kv.\ zbytky\} \setminus \{-1\}$ dá právě čísla $2, 6, 7, 8$, která nám vyšla z předešlého, pracnějšího postupu.

Proč takový postup (v tomto případě!) funguje? Potřebujeme totiž ze $\mathbb{Z}_{11}^*$ odebrat všechny prvky splňující $x^5 = 1$ nebo $x^2 = 1$. Kvadratické zbytky první rovnici splňují (neboť $x^5 = (y^2)^5 = y^{10} = 1$), a lze si rozmyslet, že kvadratické nezbytky ji naopak splňovat nemohou. Rovnice $x^2 = 1$ může mít modulo prvočíslo (a obecně v cyklické grupě) nejvýše dvě řešení, takže vidíme, že jejími řešeními jsou právě ± 1. Je ovšem dlužno dodat, že tento výpočet se hodí jen ve chvíli, kdy hledáme primitivní prvky modulo $n = 2q + 1$, kde q je prvočíslo; navíc je potřeba vědět, že nějaký primitivní prvek existuje, jinak se naše argumenty rozpadnou.

0. Hledáme prvky $x \in \mathbb{Z}_{15}^*$ takové, že $x^2 = 1$ a $x \neq 1$. Máme tak $x^2 \equiv 1 \pmod{15}$, což lze přepsat jako

$$(x - 1)(x + 1) \equiv 0 \pmod{15}.$$

To je splněno právě tehdy, když $x \equiv \pm 1 \pmod 3$ a $x \equiv \pm 1 \pmod 5$ (3 a 5 jsou prvočísla, a tedy už musí některou z uvedených závorek dělit). To můžeme rozdělit na čtyři případy, které vyřešíme pomocí Čínské zbytkové věty:

(a) $x \equiv 1 \pmod 3$ a $x \equiv 1 \pmod 5$. To odpovídá prvku $1 \in \mathbb{Z}_{15}^*$; ten má ale řád 1 a není involucí.
(b) $x \equiv 1 \pmod 3$ a $x \equiv -1 \pmod 5$. To odpovídá prvku $4 \in \mathbb{Z}_{15}^*$.
(c) $x \equiv -1 \pmod 3$ a $x \equiv 1 \pmod 5$. To odpovídá prvku $11 \in \mathbb{Z}_{15}^*$.
(d) $x \equiv -1 \pmod 3$ a $x \equiv -1 \pmod 5$. To odpovídá prvku $14 = -1 \in \mathbb{Z}_{15}^*$.

Všechny involuce v $\mathbb{Z}_{15}^*$ jsou tedy $4, 11, 14$.

Jak víme z předchozích cvičení, v každé cyklické grupě existuje nejvýše jedna involuce (to plyne z úvah o rovnici $2x \equiv 0 \pmod n$ v $\mathbb{Z}_n$); grupa $\mathbb{Z}_{15}^*$ proto nemůže být cyklická. (Což už také víme, ale díky ne zcela dokázané větě; teď jsme si to ověřili.)

1. Výpočet bude přímo kopírovat důkaz věty 5.5.a) a explicitně popíšeme izomorfismus $\mathbb{Z}_4 \times \mathbb{Z}_{5^2} \cong \mathbb{Z}_{125}^*$. Proto tento postup v principu funguje **pouze** pro mocniny lichých prvočísel. Z důkazu věty plyne, že uvedený izomorfismus číslu (a, b) přiřadí $x^a \cdot 6^b$, kde x je libovolný pevný prvek řádu 4 a 6 je zvoleno jako $5 + 1$ ($125 = 5^3$). Zbývá nám tedy určit nějaký prvek řádu 4.

Z důkazu plyne, že se stačí podívat na nějaký primitivní prvek modulo 5, ten bude mít v $\mathbb{Z}_{125}^*$ řád dělitelný 4, a tudíž po jeho vhodném umocnění už nějaký prvek řádu 4 najdeme. Primitivní prvek modulo 5 je například 2. $|\mathbb{Z}_{125}^*| = 100 = 2^2 \cdot 5^2$, tedy řád 2 musí dělit 100. Po vyzkoušení všech dělitelů zjistíme, že řád je 100 (pro potvrzení stačí ověřit $2^{50} \neq 1$, $2^{20} \neq 1$, ostatní menší dělitelé některého z těchto dělí). Mohli bychom tady skončit a prohlásit, že 2 je primitivní prvek modulo 125. Dokončeme ale konstrukci uvedeného izomorfismu. Protože má 2 řád 100, tak $2^2 5 = 57$ má řád 4.

Výše uvedený izomorfismus tak může být tvaru $(a, b) \to 57^a 6^b$. V $\mathbb{Z}_4 \times \mathbb{Z}_{5^2}$ umíme generátory zase jednoduše popsat (v obou souřadnicích musí být číslo nesoudělné se základem), jedním z nich je například $(1, 1)$, jako další primitivní prvek modulo 125 tak dostaneme $57 \cdot 6 = 92$.

b) $\mathbb{Z}_{250}^* \cong \mathbb{Z}_{125}^* \times \mathbb{Z}_2^*$, kde tento izomorfismus je dán z Čínské věty o zbytcích tak, že číslu modulo 250 přiřadí jeho zbytky po dělení 125 a 2. Prvky $\mathbb{Z}_{125}^* \times \mathbb{Z}_2^*$ jsou všechny tvaru $(a, 1)$ a protože 2 je primitivní prvek modulo 125, tak $(2, 1)$ bude generátor. Zbývá tedy určit, jaký prvek $\mathbb{Z}_{250}^*$ přísluší této dvojici, neboli jaké číslo dává zbytek 2 po dělení 125 a 1 po dělení 2. Snadno nahlédneme, že jde o 127; to je kýžený primitivní prvek modulo 250.