Teorie čísel: Cvičení 11 – výsledky a vybraná řešení

2. května 2022

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

Výsledky a řešení:

-2. Jako důsledek Čínské věty o zbytcích platí $\mathbb{Z}_{360}^* \cong \mathbb{Z}_{2^3}^* \times \mathbb{Z}_{3^2}^* \times \mathbb{Z}_5^*$ (viz úloha 5, mělo by být známé z Algebry). Podle vět zmíněných na začátku cvičení následně rozložíme $\mathbb{Z}_{2^3}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_{3^2}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ a $\mathbb{Z}_5^* \cong \mathbb{Z}_4$. Dohromady dostáváme

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

Je tato grupa cyklická? Můžeme si všimnout, že 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. Zkusíme ověřit zda je 2 primitivní prvek. $|\mathbb{Z}_{11}^*| = 10$, z Lagrangeovy věty mají prvky řád této grupě řád, jež dělí 10, tedy $1, 2, 5$ nebo 10. Vidíme, že $2^1 \neq 1$, $2^2 = 4 \neq 1$ a $2^5 = -1 \neq 1$. Z toho už plyne, že řád 2 je 10 neboli že 2 primitivní prvek. Podobně bychom mohli vyzkoušet pro všechna ostatní čísla, zda jsou to primitivní prvky. Ukažme si ale chytřejší způsob využívající toho, že jeden generátor jsme již našli.

Z toho, že 2 je primitivní prvek, tak můžeme explicitně popsat izomorfismus $\mathbb{Z}_{10} \cong \mathbb{Z}_{11}^*$ tak, že prvku $a \in \mathbb{Z}_{10}$ přiřazuje $2^a \in \mathbb{Z}_{11}^*$. Víme, že generátory $\mathbb{Z}_{10}$ jsou právě čísla nesoudělná s 10, tedy $1, 3, 7, 9$, a zároveň izomorfismus musí zobrazovat generátory na generátory. Z toho dostáváme, že primitivní prvky modulo 11 jsou právě $2^1 = 2, 2^3 = 8, 2^7 = 7$ a $2^9 = 6$.

0. a) 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 $2^25 = 57$ 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 číslo 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 je 127 a dostali jsme tak primitivní prvek modulo 250.

1. a) ANO

b) ANO

c) NE

d) NE

2. $2, 6, 7, 11$

3. 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) $\mathbb{Z}_2 \times \mathbb{Z}_{27}$

4. V částech (a) až (d) je možností vždy hodně (konkrétně $\varphi(\varphi(n))$), 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.

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

10. Viz důsledek 5.6 z přednášky.