Teorie čísel: Cvičení 9 – výsledky a vybraná řešení

11. dubna 2022

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

Výsledky:

-1. a) Existují právě 2 charaktery modulo 3. Triviální $\varepsilon(1) = \varepsilon(2) = 1$ a netriviální definovaný po prvcích jako $\chi(1) = 1$, $\chi(2) = -1$.

b) Existuje právě 6 charakterů modulo 7. Pokud si je označíme $\chi_1, \ldots, \chi_6$, tak je můžeme definovat po prvcích například jako $\chi_m(3^k) = \zeta_6^{km}$ pro $0 \leq m \leq 5$ (je to plná definice, protože 3 je primitivní prvek modulo 7 a tak 3^k postupně prochází všemi prvky v $\mathbb{Z}_7^*$). Postup viz v řešení níže.

c) Existují právě 4 charaktery modulo 12. Můžeme je zadat například po prvcích tabulkou (pro postup viz řešení níže):

	1	5	7	11
χ_1	1	1	1	1
χ_2	1	1	−1	−1
χ_3	1	−1	1	−1
χ_4	1	−1	−1	1

0. Pro triviální charakter vyjde $g(\varepsilon) = \zeta_3 + \zeta_3^2 = -1$. Pro jediný netriviální charakter modulo 3 dostaneme $g(\chi) = \zeta_3 - \zeta_3^2 = i\sqrt{3}$. (Triviální charakter jde vypočítat stejně jako ve skriptech za použití $\sum_{a \in \mathbb{Z}_p} \zeta_p^a = 0$ nebo si jde uvědomit, že $\zeta_3 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ a $\zeta_3^2 = \overline{\zeta_3}$.)

1. a) Existují právě 2 charaktery modulo 4. Triviální $\varepsilon(1) = \varepsilon(3) = 1$ a netriviální definovaný po prvcích jako $\chi(1) = 1$, $\chi(3) = -1$.

b) Analogicky k $-2b$) existují právě 4 charaktery modulo 5. Pokud si je označíme $\chi_1, \ldots, \chi_4$, tak je můžeme definovat po prvcích například jako $\chi_m(2^k) = \zeta_4^{km}$ pro $0 \leq k \leq 3$.

c) Existují právě 4 charaktery modulo 8. Můžeme je zadat například po prvcích tabulkou:

	1	3	5	7
χ_1	1	1	1	1
χ_2	1	1	−1	−1
χ_3	1	−1	1	−1
χ_4	1	−1	−1	1

d) Analogicky k $-2b$) existuje právě 16 charakterů modulo 17. Pokud si je označíme $\chi_1, \ldots, \chi_{16}$, tak je můžeme definovat po prvcích například jako $\chi_m(3^k) = \zeta_6^{km}$ pro $0 \leq k \leq 15$.

Poznámka: Jde si všimnout, že charaktery modulo 4 *a modulo* 3 *vypadají až na přeznačení čísel stejně. Podobně pro charaktery modulo* 8 *a* 12. *Je to dáno izomorfismy grup* $\mathbb{Z}_4^* \cong \mathbb{Z}_3^*$ *a* $\mathbb{Z}_8^* \cong \mathbb{Z}_{12}^*$ *(důkazy těchto izomorfismů uvidíme na cviku v následujících týdnech).*

2. Vyjde, že řád charakteru χ_m (viz značení z úlohy -1) je roven přesně $\frac{6}{NSD(6,m)}$. Myšlenka řešení je taková, že z definice řádu v grupě hledáme nejmenší přirození číslo r takové, že $\chi_m^r = \varepsilon$ v grupě charakterů. To v překladu znamená, že chceme $1 = (\chi_m(3^k))^r = \zeta_6^{kmr}$ pro všechna $0 \leq k \leq 5$. To se zřejmě stane právě tehdy, když $6 \mid kmr$, z čehož už plyne požadovaný výsledek.

3. Jednak je nutné ověřit, že takto po prvcích zadefinovaný součin a inverz charakterů je skutečně opět charakter modulo n (tj. homomorfismus ze $\mathbb{Z}_n^*$ do $\mathbb{C}^*$). Grupová asociativita pak bude plynout z asociativity násobení komplexních čísel. To, že je ε jednotka je snadné a funkčnost inverzů plyne z toho, že pro prvky $\mathbb{C}$ na jednotkové kružnici platí $\overline{z} = z^{-1}$.

4. a) Definujme operaci násobení, inverzu a jednotku jako v $\mathbb{C}$. Budou tedy splňovat požadované vlastnosti grupových operací a jediné co potřebujeme ověřit je, že součin dvou prvků z C_n opět leží v C_n, inverz prvku C_n je opět v C_n a jednotka je v C_n.

   Obojí je poměrně snadné. Všimněte si, že tato grupa je izomorfní $\mathbb{Z}_n$ ($k \to e^{\frac{2\pi i k}{n}}$).

   b) Tvrzení plyne přesně z toho, jak vypadají primitivní n-té odmocniny z 1 (přesně ty jsou generátory grupy všech odmocnin). V podstatě člověk chce dokázat, kdy jsou prvky $1, \zeta_n^k, \zeta_n^{2k}, \dots \zeta_n^{(n-1)k}$ po dvou různé, což přesně odpovídá různosti prvků $0k, 1k, 2k, \dots$ modulo n.

   c) Z toho, že $\chi(a)^{\varphi(n)} = 1$ máme, že $Im(\chi)$ je skutečně podmnožina $C_{\varphi(n)}$. Zbývá ukázat, že tam leží jednotka a že je to uzavřené na násobení a inverzy, a tedy je to podrgupa. Vše poměrně přímočaře plyne z toho, že je χ homomorfismus ($\chi(a)\chi(b) = \chi(ab)$, $\chi(a)^{-1} = \chi(a^{-1})$).

   d) Všimněme si, že primitivní prvek modulo 11 je například 2, charaktery modulo jedenáct jsou tedy dány hodnotou $\chi(2)$. Obrazem χ pak bude celá C_{10} právě tehdy, když se $\chi(2)$ bude generátor C_n. Jejich popis máme v bodu b) – budou to přesně ty charaktery dané $\chi(2) = \zeta_{10}^a$, $NSD(a, 10) = 1$.

5. Legendreův symbol zřejmě dobře definuje zobrazení ze $\mathbb{Z}_p^*$ do $\mathbb{C}^*$. To, že je to homomorfismus (a tedy charakter modulo p), plyne z multiplikativity Legendreova symbolu.

   Pro druhou část si nejdříve rozmysleme, že ε a $\left(\frac{a}{p}\right)$ jistě zadanou rovnost splňují. Navíc platí, že jsou to jediné takovéto charaktery. To plyne z toho, že charakter je jednoznačně určen obrazem nějakého primitivního prvku g modulo p. Nicméně $\chi(g)^2 = 1$, takže máme pouze dvě možnosti $\chi(g) = \pm 1$ a existují tak právě dva charaktery splňující $\chi^2 = \varepsilon$. Nutně to tedy jsou právě ε a $\left(\frac{a}{p}\right)$. Můžete si rozmyslet, proč platí $\left(\frac{g}{p}\right) = -1$ pro libovolný primitivní prvek g.

6. Důkaz je ve skriptech na konci sekce 4.2. Zásadní myšlenka je taková, že když přenásobíme sumu nějakou n-tou odmocninou z 1, tak se množina sčítanců nezmění (a tedy ani výsledná suma.)

7. a) $g(\chi_1) = 1 \cdot e^{\frac{2\pi i}{5}} + ie^{\frac{4\pi i}{5}} + (-i)e^{\frac{6\pi i}{5}} - 1 \cdot e^{\frac{8\pi i}{5}} = i\sqrt[4]{-15 + 20i}$. Dojít k tomuto výsledku je poměrně pracné, jedna možná cesta (možná ne nejsnazší) je například napřímo spočítat $\sin(x)$ a $\cos(x)$ pro $x = \frac{2\pi}{5}$ za použití $(\cos(x) + i\sin(x))^5 = \cos(5x) + i\sin(5x)$. Pointou nicméně je, že spočítat Gaussovy součty přímo je obecně poměrně pracné, i když umíme říct, že jsou v absolutní hodnotě rovny $\sqrt{p}$.

   b) Můžeme se podívat například na charakter příslušící Legendreovu symbolu $\chi(a) = \left(\frac{a}{p}\right)$. Dostaneme $g(\chi) = \zeta_7 + \zeta_7^2 - \zeta_7^3 + \zeta_7^4 - \zeta_7^5 - \zeta_7^6$. Můžete si zkusit spočítat tuto hodnotu napřímo. Z přednášky nicméně víme, že vyjde přesně $i\sqrt{7}$ (konec sekce 4.3).

8. Důkaz není nejlehčí. Na přednášce jste tuto větu viděli pro prvočísla. Zobecnění pro mocniny lichých prvočísel je pořád poměrně přímočaré, neboť v multiplikativní grupě existuje primitivní prvek. Pro mocniny dvojky tuto vlastnost obecně nemáme a je třeba strukturu multiplikativní grupy popsat jinak (jak, to brzo uvidíme na cvičení). Jakmile zvládneme situaci vyřešit pro mocniny prvočísel, tak již s trochou snahy složíme získané znalosti za pomocí čínské zbytkové věty a grupových součinů.

9. Nejdřív si uvědomte, že $\chi(n)\overline{\chi}(a) = \chi(na^{-1})$. Nedělalo se na přednášce nějaké tvrzení, které by na tuto sumu šlo napasovat?

Vybraná vzorová řešení:

-2.) Na začátek si obecně uvědomíme klíčové pozorování o řádech prvků. Pokud pro nějaký prvek $a \in \mathbb{Z}_n^*$ platí $a^k = 1$, tak

$$1 = \chi(1) = \chi(a^k) = (\chi(a))^k,$$

neboť χ je homomorfismus. Speciálně tak dostáváme, že $\chi(a)$ je nějaká k-tá odmocnina z 1. Protože z Eulerovy věty máme v $\mathbb{Z}_n^*$ pro libovolný prvek rovnost $a^{\varphi(n)} = 1$, tak je speciálně $\chi(a)$ nějaká $\varphi(n)$-tá odmocnina z 1 pro každý charakter modulo n a každé $a \in \mathbb{Z}_n^*$.

b) $n = 7$. Všimneme si, že 3 je primitivní prvek modulo 7, neboť všechny mocniny $3, 3^2, \dots, 3^5$ jsou různé od 1. Z toho dostáváme, že každý prvek $a \in \mathbb{Z}_7^*$ lze zapsat ve tvaru 3^k a platí $\chi(a) = \chi(3^k) = \chi(3)^k$. Volba $\chi(3)$ nám tedy již jednoznačně definuje celý charakter. Pro $\chi(3)$ máme podle výše uvedeného

pozorování nanejvýš 6 možných voleb a jsou jimi právě 6-té odmocniny z 1 (ζ_6^m , $0 \leq m \leq 5$). Pro tyto volby pak můžeme dodefinovat zobrazení jediným přípustným způsobem jako $\chi_m(3^k) = \zeta_6^{km}$. Jak dokazuje Lemma 4.5. ze skript, tak toto již skutečně jsou dobře definované charaktery modulo 7.

Je tedy přesně 6 výše popsaných charakterů modulo 7.

c) Pro $n = 12$ máme $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$. Neexistuje zde primitivní prvek, nicméně si můžeme všimnout, že $5^2 = 7^2 = 11^2 = 1$. Všechny $\chi(5), \chi(7), \chi(11)$ jsou tedy buď 1 nebo -1. Jistě taktéž $\chi(1) = 1$ (to platí pro každý charakter). Navíc si můžeme všimnout, že $5 \cdot 7 = 11$, tedy $\chi(5)\chi(7) = \chi(11)$. Z toho vidíme, že stačí určit pouze hodnoty $\chi(5)$ a $\chi(7)$ a ty nám už jednoznačně určí zbytek. Máme tak pouze čtyři níže uvedené možnosti, jak je zvolit a snadno se již přesvědčíme, že každá z nich skutečně definuje homomorfismus.

	1	5	7	11
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1