Teorie čísel: Cvičení 9 – výsledky, nápovědy, vzorová řešení

Simona Hlavinková, email: simonkahlavinkova@gmail.com

Nápovědy:

-1. Pokud tento příklad vidíte poprvé, není úplně snadný. Zaprvé si musíte uvědomit, že ačkoliv v definici zobrazujeme $\mathbb{Z}_n^*$ do celého $\mathbb{C}^*$, ve skutečnosti je oborem hodnot každého charakteru modulo n nanejvýš množina všech $\varphi(n)$-tých odmocnin z jedné. Zadruhé, pokud modulo n existuje primitivní prvek, odvoďte, že charakter je jednoznačně určen svou hodnotou v tomto primitivním prvku. Zatřetí, ověřte, že všechna zobrazení, která vám vyjdou jako „kandidáti na charaktery“ jsou skutečně charaktery, tj. homomorfismy.

0. Vyjděte z definice. Využijte toho, že $\zeta_3 = -\frac{1}{2} + \mathrm{i}\frac{\sqrt{3}}{2}$ a $\zeta_3^2 = \overline{\zeta_3}$. Pro triviální charakter lze také podobně jako ve skriptech zužitkovat rovnost $\sum_{a\in\mathbb{Z}_p} \zeta_p^a = 0$.

1. Postupujte stejně jako u úlohy -1.

2. Z definice řádu v grupě hledáme nejmenší přirozené číslo r takové, že $\chi_m^r = \varepsilon$ v grupě charakterů. Uvědomte si, že se dva charaktery rovnají právě tehdy, když se shodují jejich hodnoty v jednom primitivním prvku. Zbytek už by měl být snadný. (Využijte popis charakterů z úlohy -1b).)

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) Dokazujete, že jde o podgrupu $\mathbb{C}^*$, takže stačí dokázat uzavřenost na všechny potřebné operace. b) Vyjděte přímo z definice. c) Stačí dokázat, že jde o podmnožinu (což už jste viděli v předešlých příkladech). Že jde o podgrupu, to by vám mělo být jasné z Algebry (*chi* je homomorfismus). d) Využijte primitivní prvek.

5. Důkaz, že jde o charakter, je snadný a přímočarý. (Odvoláte se na už známé tvrzení.) Při hledání charakterů, které mají v grupě $X(\mathbb{Z}_p^*)$ řád nejvýše 2, využijte primitivní prvek.

6. Odpověď včetně vysvětlení je ve skriptech na úplném konci sekce 4.2. Co se stane, když celou sumu přenásobíme ζ_n?

7. Když použijete „nejjednodušší netriviální charakter“, tj. Legendreův symbol, můžete využít tvrzení ze skript. (To ale není záměrem – bude mnohem lepší, když si ty součty právě pro Legendreův symbol zkusíte spočítat ručně.) Ať už si vyberete kterýkoliv charakter, měli byste být schopni výsledek vyjádřit ve tvaru konečného součtu, v němž se vyskytují mocniny ζ_p a ζ_{p-1} (to vlastně dostanete přímo z definice). To by se, pokud budete mít chuť, dalo přepsat čistě pomocí mocnin $\zeta_{p(p-1)}$. Pro $p = 7$ nedoporučuju zkoumat jiný charakter než Legendreův symbol; při práci modulo 5 můžete výsledek pro Legendreův symbol přepsat pomocí $\cos\frac{2\pi}{2}$, a to se dokonce dá upravit: $\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{2}$.

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 $\chi(n)\overline{\chi}(a) = \chi(na^{-1})$. Pak už by vám měly stačit znalosti z přednášky.

Výsledky:

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

b) Existuje šest charakterů modulo 7. Označíme je $\chi_0, \ldots, \chi_5$, a můžeme je definovat po prvcích například jako $\chi_m(3^k) = \zeta_6^{mk}$ pro $0 \leq m \leq 5$ (je to kompletní definice, protože 3 je primitivní prvek modulo 7, takže 3^k postupně prochází všemi prvky v $\mathbb{Z}_7^*$). Jiný možný formát řešení je následující tabulka; v ní využijeme toho, že $\zeta_6^5 = \overline{\zeta_6}$, $\zeta_6^2 = \zeta_3$, $\zeta_6^4 = \overline{\zeta_3}$ a $\zeta_6^3 = -1$. (Šlo by ta čísla vypsat ještě explicitněji, protože $\zeta_6 = \frac{1+\sqrt{3}\mathrm{i}}{2}$ apod.)

	1	3	2	6	4	5
χ_0	1	1	1	1	1	1
χ_1	1	ζ_6	ζ_3	-1	$\overline{\zeta_3}$	$\overline{\zeta_6}$
χ_2	1	ζ_3	$\overline{\zeta_3}$	1	ζ_3	$\overline{\zeta_3}$
χ_3	1	-1	1	-1	1	-1
χ_4	1	$\overline{\zeta_3}$	ζ_3	1	$\overline{\zeta_3}$	ζ_3
χ_5	1	$\overline{\zeta_6}$	$\overline{\zeta_3}$	-1	ζ_3	ζ_6

c) Existují čtyři charaktery modulo 12. Můžeme je zadat například po prvcích tabulkou:

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

0. Pro triviální charakter vyjde $g(\varepsilon) = \zeta_3 + \zeta_3^2 = -1$. Pro jediný netriviální charakter modulo 3 dostaneme $g(\chi) = \zeta_3 - \zeta_3^2 = \mathrm{i}\sqrt{3}$.

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

b) Analogicky k příkladu -1 b) existují právě čtyři charaktery modulo 5. Označíme je $\chi_0, \ldots, \chi_3$ a definujeme $\chi_m(2^k) = \mathrm{i}^{mk}$ pro $0 \leq k \leq 3$. (Platí $\zeta_4 = \mathrm{i}$.) Jiným možným formátem odpovědi je explicitní tabulka:

	1	2	4	3
χ_0	1	1	1	1
χ_1	1	i	-1	$-\mathrm{i}$
χ_2	1	-1	1	-1
χ_3	1	$-\mathrm{i}$	-1	i

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

	1	3	5	7
ε	1	1	1	1
χ_1	1	1	-1	-1
χ_2	1	-1	1	-1
χ_3	1	-1	-1	1

d) Analogicky k $-1b$) existuje právě 16 charakterů modulo 17. Lze je označit $\chi_0, \ldots, \chi_{15}$ a definovat je po prvcích jako $\chi_m(3^k) = \zeta_6^{km}$ pro $0 \leq k \leq 15$.

Poznámka: Můžete 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. Při značení z úlohy -1 platí $\mathrm{ord}(\chi_m) = \frac{6}{\mathrm{NSD}(6,m)}$.

3. Skutečně to je grupa. :-)

4. a,b,c) Platí to. d) Jde o charaktery $\chi_m(2) = \zeta_{10}^m$, kde $\mathrm{NSD}(m, 10) = 1$.

5. Skutečně jde o charakter. Modulo liché prvočíslo jsou jedinými takovými charaktery ε a právě Legendreův symbol.

6. Je to nula.

7. a) Pro Legendreův symbol vyjde $g(\chi_{\text{Leg}}) = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 = 1 + 2\zeta_5 + 2\zeta_5^4 = 1 + 2(\zeta_5 + \overline{\zeta_5}) = 1 + 4\cos\frac{2\pi}{5} = 1 + 4\frac{\sqrt{5}-1}{4} = \sqrt{5}$. Každý tvar výsledku je svým způsobem odpovědí (a u složitějších příkladů vůbec nemusí lepší tvar existovat), ale sami asi poznáte, které tvary jsou hezčí. Pro charakter χ_1 definovaný jako $\chi_1(2^k) = \zeta_4^k = \mathrm{i}^k$ vyjde z definice $\mathrm{i}\zeta_5 - \zeta_5^2 - i\zeta_5^3 + \zeta_5^4 = \mathrm{i}\zeta_5 + \overline{\zeta_5} + \zeta_5^2 + \mathrm{i}\overline{\zeta_5^2}$. Vůbec to není vidět, ale toto se dá upravit jako $\mathrm{i}\sqrt[4]{-15+20\mathrm{i}}$.

   b) Pro Legendreův symbol přímo z definice máme $g(\chi_{\text{Leg}}) = \zeta_7 + \zeta_7^2 - \zeta_7^3 + \zeta_7^4 - \zeta_7^5 - \zeta_7^6$. Jak víme z přednášky, toto je rovno $\mathrm{i}\sqrt{7}$ (viz konec sekce 4.3). Můžete si zkusit tento výsledek odvodit. Pro jiné charaktery než Legendreův symbol to počítejte, jen pokud se obrníte velkou dávkou trpělivosti.

8.,9. Skutečně to platí.

Vybraná vzorová řešení:

-1.) 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 každé $\chi(a)$ nějaká $\varphi(n)$-tá odmocnina z 1 pro každý charakter modulo n a každé $a \in \mathbb{Z}_n^*$.

a) $n = 3$. Lze postupovat stejně jako u b), ale tady se obejdeme i víceméně bez přemýšlení: Máme $\mathbb{Z}_3^* = \{1, 2\}$ a každý homomorfismus splňuje $\chi(1) = 1$; zbývá tedy určit hodnotu $\chi(2)$. Víme už ale, že to musí být druhá odmocnina z jedné, takže existují dvě možnosti: $\chi(2) = \pm 1$. U obou snadno ověříme, že se skutečně jedná o homomorfismus: V prvním případě jde o triviální charakter, ve druhém musíme ověřit (díky komutativitě) jen rovnosti $\chi(1^2) = \chi(1)^2$, $\chi(2^2) = \chi(2)^2$ a $\chi(1 \cdot 2) = \chi(1) \cdot \chi(2)$. Po dosazení vyjde po řadě $1 = 1^2$, $1 = (-1)^2$ a $-1 = 1 \cdot (-1)$, takže všechny jsou splněny.

b) $n = 7$. Všimneme si, že 3 je primitivní prvek modulo 7, neboť všechny mocniny $3, 3^2, \ldots, 3^5$ jsou různé od 1. (Díky vlastnostem řádů prvků stačilo ověřit jen dělitele šestky, tj. první, druhou a třetí mocninu.) 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 šesté odmocniny z 1 (ζ_6^m , $0 \le m \le 5$). Pro každou z těchto voleb pak jich můžeme dodefinovat zobrazení jediným přípustným způsobem, a to $\chi_m(3^k) = \zeta_6^{mk}$. Jak dokazuje Lemma 4.5 ze skript (nebo jak si snadno ověříme), jsou všechna tato zobrazení skutečně dobře definované charaktery modulo 7.

Existuje tedy přesně šest charakterů modulo 7; jde o zobrazení $\chi_0, \ldots, \chi_5$ popsaná výše.

c) Pro $n = 12$ máme $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$. Neexistuje zde primitivní prvek, protože $5^2 = 7^2 = 11^2 = 1$. Díky těmto rovnostem jsou všechny hodnoty $\chi(5), \chi(7), \chi(11)$ v množině $\{\pm 1\}$. Pro každý charakter samozřejmě platí $\chi(1) = 1$. Navíc si můžeme všimnout, že $5 \cdot 7 = 11$, tedy $\chi(5)\chi(7) = \chi(11)$. Z toho vidíme, že když už známe hodnoty $\chi(5)$ a $\chi(7)$, tak $\chi(11)$ musí být jejich součin. V následující tabulce proto projdeme všechny možné volby hodnot $\chi(5)$ a $\chi(7)$, ty nám už jednoznačně určí zbytek, a následně se musíme pro každé zobrazení z definice přesvědčit, že jde o 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

4.) (Nástin.) **a)** Díky tomu, že násobení, inverz a jednotku jsou stejné jako v $\mathbb{C}$, jsou axiomy grupy splněny automaticky, protože $\mathbb{C}^*$ je grupa. Musíme jen ověřit, 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 $\mathbb{Z}_n$ ($k \mapsto \mathrm{e}^{\frac{2\pi\mathrm{i}k}{n}}$).

b) Tvrzení plyne přesně z toho, jak vypadají primitivní n-té odmocniny z 1 (protože právě ony jsou generátory grupy všech odmocnin, tj. C_n). Je třeba určit, kdy jsou prvky $1, \zeta_n^k, \zeta_n^{2k}, \dots \zeta_n^{(n-1)k}$ po dvou různé, což přesně odpovídá vzájemné různosti prvků $0k, 1k, 2k, \dots, (n-1)k$ modulo n.

c) Z toho, že $\chi(a)^{\varphi(n)} = 1$ máme, že $\mathrm{Im}(\chi)$ je skutečně podmnožina $C_{\varphi(n)}$. Zbývá ukázat, že v ní leží jednotka a že je uzavřená na násobení i inverzy – tedy že je to podgrupa. To se jednak dá ověřit snadno na koleni, jednak je to obecná vlastnost homomorfismů: Obor hodnot každého homomorfismu je podgrupa cílové grupy.

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 právě charaktery dané $\chi(2) = \zeta_{10}^a$, kde $\mathrm{NSD}(a, 10) = 1$.

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 $\left(\frac{\cdot}{p}\right)$ jistě zadanou rovnost splňují. Zbývá ukázat, že jsou to jediné takové charaktery. Zvolme si libovolný primitivní prvek g modulo p. Pak je charakter jednoznačně určen obrazem g. Přitom $\chi(g)^2 = 1$, takže máme pouze dvě možnosti: $\chi(g) = \pm 1$. Existují tedy skutečně nejvýše dva charaktery splňující $\chi^2 = \varepsilon$ (a už je známe – jde o triviální charakter a o Legendreův symbol). Mimochodem jsme také ukázali $\left(\frac{g}{p}\right) = -1$ pro každý primitivní prvek g. Také si všimněte, že například modulo 8 a 12 (viz předchozí příklady) splňují rovnost $\chi^2 = \varepsilon$ všechny charaktery a je jich více než dva.

7.) (Nástin) Velkou část postupu už máte zahrnutou pod hlavičkou Výsledky. Tady jen předvedu, jak dojít k překvapivému výsledku $\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$.

Nejprve si uvědomme, že stačí dokázat $\zeta_5 + \overline{\zeta}_5 = \frac{\sqrt{5}-1}{2}$. Pro každé komplexní číslo totiž máme $z + \overline{z} = 2\Re z$, a $\zeta_5 = \cos\frac{2\pi}{5} + \mathrm{i}\sin\frac{2\pi}{5}$. Dále, k důkazu $\zeta_5 + \overline{\zeta_5} = \frac{\sqrt{5}-1}{2}$ nám stačí ověřit, že $\zeta_5 + \overline{\zeta_5}$ je kořenem kvadratické rovnice $x^2 + x - 1 = 0$. (Druhý kořen můžeme zahodit, protože ζ_5 leží v prvním kvadrantu a má tedy zjevně kladnou reálnou část; jiná forma tohoto argumentu je, že kosinus 72° je samozřejmě kladný.)

Víme, že $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0$. To lze přepsat do podoby $0 = 1 + \zeta_5 + \zeta_5^2 + \overline{\zeta}_5^2 + \overline{\zeta}_5 = 1 + (\zeta_5 + \overline{\zeta_5}) + (\zeta_5^2 + \overline{\zeta}_5^2 + 2) - 2$. Přitom

$$(\zeta_5 + \overline{\zeta_5})^2 = \zeta_5^2 + \overline{\zeta}_5^2 + 2\zeta_5\overline{\zeta_5} = \zeta_5^2 + \overline{\zeta}_5^2 + 2.$$

Dostáváme tedy $0 = -1 + (\zeta_5 + \overline{\zeta_5}) + (\zeta_5 + \overline{\zeta_5})^2$, což jsme právě chtěli.

Alternativně by šlo využít identitu $(\cos\frac{2\pi}{5} + \mathrm{i}\sin\frac{2\pi}{5})^2 = 1$.