Teorie čísel: Cvičení 9

Simona Hlavinková, email: simonkahlavinkova@gmail.com

Definice. *Multiplikativní charakter modulo n* je grupový homomorfismus $\chi : \mathbb{Z}_n^* \to \mathbb{C}^*$, tedy zobrazení splňující

$$\chi(a)\chi(b) = \chi(a \cdot b \mod n).$$

Gaussův součet charakteru χ je $g(\chi) = \sum_{a \in \mathbb{Z}_n^*} \chi(a)\zeta_n^a$, kde $\zeta_n = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$.

Definice. Charaktery modulo n tvoří grupu, kterou značíme $X(\mathbb{Z}_n^*)$. Grupové operace jsou definované (pro všechna $a \in \mathbb{Z}_n^*$) takto:

- Součin: $(\chi_1\chi_2)(a) := \chi_1(a)\chi_2(a)$.
- Jednotka: *triviální charakter* $\varepsilon(a) := 1$. Ostatní charaktery jsou *netriviální.*
- Inverzní prvek: $\overline{\chi}(a) := \overline{\chi(a)}$.

-1. Určete všechny charaktery modulo n pro a) $n = 3$, b) $n = 7$, c) $n = 12$.

0. Pro každý charakter modulo 3 spočtěte jeho Gaussův součet.

! 1. Určete všechny charaktery modulo n pro
   (a) $n = 4$,
   (b) $n = 5$,
   (c) $n = 8$,
   (d) $n = 17$.

   Nemusíte vyčíslit hodnoty na jednotlivých prvcích – jen je nějak jednoznačně popište.

! 2. Pro všechny charaktery modulo 7 určete jejich řád v grupě $X(\mathbb{Z}_7^*)$.

3. Ověřte, že $X(\mathbb{Z}_n^*)$ s operacemi definovanými výše tvoří grupu.

! 4. Označme $C_n := \left\{\mathrm{e}^{\frac{2\pi \mathrm{i}k}{n}} : k = 0, \dots, n-1\right\} = \langle \zeta_n \rangle$ množinu všech komplexních n-tých odmocnin z 1.
   (a) Ukažte, že C_n s klasickou operací násobení je grupa.
   (b) Ukažte, že generátory grupy C_n (čili primitivní n-té odmocniny z 1) jsou právě ζ_n^k, pro které $\mathrm{NSD}(k, n) = 1$.
   (c) Nechť χ je charakter modulo n. Ukažte, že jeho obraz $\mathrm{Im}(\chi) := \{\chi(a) : a \in \mathbb{Z}_n^*\}$ je podgrupa $C_{\varphi(n)}$.
   (d) Popište všechny charaktery modulo 11, jejichž obraz je celá C_{10}.

5. Ukažte, že Legendreův symbol $\left(\frac{\cdot}{p}\right)$ je charakter modulo p pro každé liché prvočíslo p. Najděte všechny charaktery χ modulo p splňující $\chi^2 = \varepsilon$.

6. Určete hodnotu $\sum_{a \in \mathbb{Z}_n} \zeta_n^a$.

7. Spočtěte Gaussův součet nějakého netriviálního charakteru modulo
   (a) 5,
   (b) 7.

∗ 8. Ukažte, že $X(\mathbb{Z}_n^*) \simeq \mathbb{Z}_n^*$.

∗ 9. Ukažte, že pokud $k \in \mathbb{N}, a, n \in \mathbb{Z}_k^*$, pak platí:

$$\frac{1}{\varphi(k)} \sum_{\chi \in X(\mathbb{Z}_k^*)} \chi(n) \cdot \overline{\chi}(a) = \begin{cases} 0 & \text{pokud } n \not\equiv a \pmod{k}, \\ 1 & \text{pokud } n \equiv a \pmod{k}. \end{cases}$$

Úlohy s nekladným číslem budou předvedeny na cvičení jako vzorové.
Úlohy s ! je doporučeno řešit přednostně.
Úlohy s ∗ jsou náročnější.