

Teorie čísel: Cvičení 9

11. dubna 2022

Web: <https://www2.karlin.mff.cuni.cz/~raskam/vyuka/tc.html>

Email: raska.martin@gmail.com

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

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

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

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 se nazývají *netriviální*.
- Inverzní prvek: $\bar{\chi}(a) := \overline{\chi(a)}$.

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

0. Pro každý charakter modulo 3 spočítejte 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, ale nějak je 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 $C_n := \left\{ e^{\frac{2\pi ik}{n}} : k = 0, \dots, n-1 \right\}$ množinu všech n -tých komplexních odmocnin z 1.

- (a) Ukažte, že C_n s operací násobení (jako v \mathbb{C}) je grupa.
- (b) Ukažte, že generátory grupy C_n (čili primitivní n -té odmocniny z 1) jsou právě ζ_n^k , pro které $\text{NSD}(k, n) = 1$.
- (c) Nechť χ je charakter modulo n . Ukažte, že jeho obraz $\text{Im}(\chi) := \{\chi(a); a \in \mathbb{Z}_n^*\}$ je podgrupa $C_{\varphi(n)}$.
- (d) Popište všechny charaktery modulo 11, jejichž obraz je celá C_{10} .

5. Ukažte, že Legendreův symbol $\left(\frac{a}{p}\right)$ je charakter modulo p (p prvočíslo). Najděte všechny charaktery χ modulo p takové, že $\chi^2 = \varepsilon$, kde ε značí triviální charakter.

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

7. Spočítejte 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:

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

Úlohy s nekladným číslem budou předvedeny na cvičení jako vzorové.

Úlohy s ! je doporučeno řešit přednostně.

Úlohy s * jsou náročnější.