Domácí úkol z 3. prosince 2015

Nechť p je prvočíslo a f číslo přirozené. Označme $\mathbb{F}_q$ konečné těleso mající $q = p^f$ prvků. Nechť $\zeta = e^{2\pi i/p} \in \mathbb{C}$ je komplexní primitivní p-tá odmocnina z jedné a $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ komplexní aditivní charakter tělesa $\mathbb{F}_q$ určený podmínkou $\psi(t) = \zeta^{\mathrm{Tr}(t)}$, kde $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ je stopa, tj. $\mathrm{Tr}(t) = t + t^p + \cdots + t^{p^{f-1}}$; přitom $\zeta^{\mathrm{Tr}(t)}$ je korektně definováno, neboť každý prvek tělesa $\mathbb{F}_p$ lze považovat za zbytkovou třídu modulo p.

Pro každé $a \in \mathbb{F}_q$ je $\psi_a : \mathbb{F}_q \to \mathbb{C}^\times$, kde $\psi_a(t) = \psi(at)$ pro libovolné $t \in \mathbb{F}_q$, komplexní aditivní charakter tělesa $\mathbb{F}_q$.

V semináři jsme ukázali, že ψ je netriviální aditivní charakter a že $\{\psi_a;\, a \in \mathbb{F}_q\}$ je množina všech q komplexních aditivních charakterů tělesa $\mathbb{F}_q$, speciálně tedy pro libovolná $a, b \in \mathbb{F}_q$ z $a \neq b$ plyne $\psi_a \neq \psi_b$.

Pro libovolný komplexní multiplikativní charakter χ tělesa $\mathbb{F}_q$, tj. homomorfismus grup $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$, definujeme Gaussovu sumu předpisem

$$\mathcal{G}_a(\chi) = -\sum_{t \in \mathbb{F}_q^\times} \psi_a(t)\chi(t).$$

1. Dokažte, že platí
$$\sum_{t \in \mathbb{F}_q} \psi(t) = 0.$$

2. Dokažte, že pro libovolné $t \in \mathbb{F}_q$ je
$$\sum_{a \in \mathbb{F}_q} \psi_a(t) = \begin{cases} q & \text{je-li } t = 0, \\ 0 & \text{je-li } t \neq 0. \end{cases}$$

3. Dokažte, že je-li χ netriviální multiplikativní charakter, pak $\mathcal{G}_0(\chi) = 0$.

4. Dokažte, že pro libovolné $a \in \mathbb{F}_q$, $a \neq 0$, je $\mathcal{G}_a(\chi) = \chi(a)^{-1} \cdot \mathcal{G}_1(\chi)$, a tedy obě Gaussovy sumy $\mathcal{G}_a(\chi)$ a $\mathcal{G}_1(\chi)$ mají stejné absolutní hodnoty.

5. Dokažte, že je-li χ netriviální multiplikativní charakter, pak absolutní hodnota $|\mathcal{G}_1(\chi)| = \sqrt{q}$.

[Návody:

1. Využijte toho, že ψ je netriviální, a tedy existuje $s \in \mathbb{F}_q$ takové, že $\psi(s) \neq 1$. Přitom zobrazení $t \mapsto t + s$ je bijekcí na $\mathbb{F}_q$, a tedy uvažovaná suma se po vynásobení číslem $\psi(s)$ nezmění.

2. Pro libovolné $t \in \mathbb{F}_q$, $t \neq 0$, je zobrazení $a \mapsto ta$ bijekcí na $\mathbb{F}_q$. Pak lze použít 1.

3. Je možné postupovat analogicky jako v 1, jen pracovat s multiplikativní grupou místo s aditivní.

4. Využitím bijekce z 2 lze ukázat, že $\chi(a) \cdot \mathcal{G}_a(\chi) = \mathcal{G}_1(\chi)$. Zřejmě $\chi(a)^{q-1} = 1$, tedy $|\chi(a)| = 1$.

5. Podle úloh 3 a 4 je $\sum_{a \in \mathbb{F}_q} \mathcal{G}_a(\chi)\overline{\mathcal{G}_a(\chi)} = (q-1)|\mathcal{G}_1(\chi)|^2$. Spočítejte tuto sumu jinak: dosaďte z definice za $\mathcal{G}_a(\chi)$ a upravte tak, abyste mohli užít úlohu 2.

Budete-li potřebovat, můžete v knize Ireland, Rosen: A classical introduction to modern number theory v kapitole 8.2 najít podobné výpočty (až na drobné odlišnosti v definici jde o speciální případ $f = 1$ tohoto zadání).]