Суммы Гаусса и квадратичный закон взаимности

Везде в этом листке p и q — различные нечетные простые числа.

Определение. *Символ Лежандра* $\left(\frac{a}{p}\right)$ определяется как

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \text{ делится на } p; \\ 1, & \text{если } a \text{ квадратичный вычет по модулю } p; \\ -1, & \text{если } a \text{ квадратичный невычет по модулю } p. \end{cases}$$

A5.1. Докажите следующие утверждения:

а) В $\mathbb{F}_p^\times$ поровну квадратичных вычетов и невычетов.

б) Символ Лежандра мультипликативен: $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Определение. Пусть ζ — корень степени q из единицы. Выражение

$$S(\zeta; q) := \sum_{a \in \mathbb{F}_q^\times} \left(\frac{a}{q}\right) \zeta^a$$

называется *суммой Гаусса* по модулю q.

A5.2. а) $S(\zeta, q)^2 = \left(\frac{-1}{q}\right) q$.

б*) Пусть $\zeta = \cos\frac{2\pi}{q} + i\sin\frac{2\pi}{q}$. Из предыдущего пункта следует, что

$$S(\zeta, q) = \begin{cases} \pm\sqrt{q}, & q = 4k+3; \\ \pm i\sqrt{q}, & q = 4k+1. \end{cases}$$

Найдите знаки.

A5.3. Докажите, что любое расширение поля $\mathbb{Q}$ с группой Галуа $\mathbb{Z}/2\mathbb{Z}$ содержится в циклотомическом.

Замечание. *Теорема Кронекера-Вебера* утверждает, что вообще любое абелево расширение поля $\mathbb{Q}$ содержится в циклотомическом.

A5.4. Пусть Fr — автоморфизм Фробениуса ($x \mapsto x^p$) поля $\mathbb{F}_p[\zeta]/\Phi_q(\zeta)$. Положим $q^* := \left(\frac{-1}{q}\right) q$. Докажите, что

а) $\operatorname{Fr} S(\zeta, q) = \left(\frac{q^*}{p}\right) S(\zeta; q)$;

б) $\operatorname{Fr} S(\zeta; q) = \left(\frac{p}{q}\right) S(\zeta; q)$.

A5.5. Докажите, что равенство

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$$

эквивалетно обычному квадратичному закону взаимности

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$