FAILURE OF CONVERSE THEOREMS OF GAUSS SUMS MODULO ℓ

ELAD ZELINGHER

Gauss sums are prominant objects in number theory. Given two characters $\alpha \colon \mathbb{F}_{q^n}^\times \to \mathbb{C}^\times$ and $\beta \colon \mathbb{F}_{q^m}^\times \to \mathbb{C}^\times$ and a non-trivial character $\psi \colon \mathbb{F}_q \to \mathbb{C}^\times$, one can attach a Gauss sum

$$G\left(\alpha \times \beta, \psi\right).$$

A celebrated theorem by Nien is the converse theorem of Gauss sums: suppose that $\alpha_1, \alpha_2 \colon \mathbb{F}_{q^n}^\times \to \mathbb{C}^\times$ are multiplicative characters such $\alpha_1 \restriction_{\mathbb{F}_q^\times} = \alpha_2 \restriction_{\mathbb{F}_q^\times}$ and such that for any $1 \le m \le \frac{n}{2}$ and any character $\beta \colon \mathbb{F}_{q^m}^\times \to \mathbb{C}^\times$ we have

$$G\left(\alpha_1 \times \beta, \psi\right) = G\left(\alpha_2 \times \beta, \psi\right).$$

Then there exists $0 \le k \le n-1$ such that $\alpha_1 = \alpha_2^{q^k}$.

Recently, Bakeberg–Gerbelli-Gauthier–Goodson–Iyengar–Moss–Zhang investigated the question what happens if we replace $\mathbb{C}$ with $\overline{\mathbb{F}_\ell}$ for some ℓ prime, such that ℓ is coprime to q. They found counterexamples for this theorem for $n = 2$ and made a conjecture of the pairs (q, ℓ) for which the converse theorem fails when $n = 2$. In this project, we will investigate this question for more general n and will try to come up with a more general conjecture.

Prerequisites.

- Familiarity with finite fields and group theory.
- Coding experience. We will mostly be using SageMath.