Failure of Converse Theorems of Gauss Sums Modulo ℓ

James Evans, Xinning Ma, Yanshun Zhang
Mentors: Dr. Elad Zelingher, Calvin Yost-Wolff
University of Michigan Laboratory of Geometry

LOG(M)

Abstract

We investigate the failure of the Converse Theorem for Gauss sums when these sums are reduced modulo a prime power ℓ. Traditionally, if two characters produce identical Gauss sums across all additive and multiplicative variations, then the characters must coincide or be related by a known twist. Over the complex field, no counterexamples to the Converse Theorem have been observed—the theorem holds as expected. However, when these sums are computed over the algebraic closure of a finite field, $\overline{\mathbb{F}}_\ell$, our computations reveal genuine counterexamples where distinct characters yield identical sums.

Objective: Use our custom SageMath program to find counterexamples for $n = 2$, examine whether they follow the specific form proposed by an existing conjecture, and explore any underlying patterns they may reveal. If consistent structure is identified, we may propose our own refined conjecture on character uniqueness modulo ℓ.

Finite Fields

Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements, where p is a prime and m is a positive integer. The multiplicative group of nonzero elements $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ forms a cyclic group of order $q-1$. This means there exists a *generator* $g \in \mathbb{F}_q^*$ such that every nonzero element of the field can be written as a power of g:

$$\mathbb{F}_q^* = \{g^0, g^1, g^2, \ldots, g^{q-2}\}.$$

The additive group $(\mathbb{F}_q, +)$ is a finite abelian group of order q under addition. Every element $a \in \mathbb{F}_q$ satisfies

$$\underbrace{a + a + \cdots + a}_{p \text{ times}} = 0,$$

It is not cyclic when $m > 1$.

Gauss Sums

Let $\mathbb{K}$ be a field. A multiplicative character θ is a group homomorphism from $\mathbb{F}_q^*$ to $\mathbb{K}^*$ that respects multiplication, that is, $\theta(a \cdot b) = \theta(a)\theta(b) \quad \forall a, b \in \mathbb{F}_q^*$.
An additive character ψ is a homomorphism from $(\mathbb{F}_q, +)$ to $\mathbb{K}^*$ that respects addition, that is, $\psi(a+b) = \psi(a)\psi(b) \quad \forall a, b \in \mathbb{F}_q$.
To define the *Twisted Gauss Sum*:
Given multiplicative characters $\theta : \mathbb{F}_{q^2}^* \to \mathbb{K}^*$, $\alpha : \mathbb{F}_q^* \to \mathbb{K}^*$, and an additive character $\psi : \mathbb{F}_q \to \mathbb{K}^*$, define:

$$G(\theta \times \alpha, \psi) = \sum_{x \in \mathbb{F}_{q^2}^*} \theta(x)\, \alpha(N(x))\, \psi(\mathrm{tr}(x)),$$

where $N(x)$ and $\mathrm{tr}(x)$ are the norm and trace from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$.

Converse Theorem (Classical)

Take $\mathbb{K} = \mathbb{C}$.

Consider two multiplicative characters θ_1 and θ_2 from $\mathbb{F}_{q^2}^*$ to $\mathbb{K}^*$, and let $\psi \colon \mathbb{F}_q \to \mathbb{K}^*$ be a fixed non-trivial additive character. Suppose

$$\theta_1|_{\mathbb{F}_q^*} = \theta_2|_{\mathbb{F}_q^*}$$

and for all multiplicative characters $\alpha \colon \mathbb{F}_q^* \to \mathbb{K}^*$, we have

$$G(\theta_1 \times \alpha, \psi) = G(\theta_2 \times \alpha, \psi).$$

Then

$$\theta_1 = \theta_2 \quad \text{or} \quad \theta_1 = \theta_2^q.$$

The Conjecture

Take $\mathbb{K} = \overline{\mathbb{F}_\ell}$.
It is known that if $\ell \nmid q-1$, then the converse theorem holds. It is thus interesting to investigate what happens when $\ell \mid q-1$. Hence, we have the following conjectcure:

Conjecture (Bakeberg et al.): *The converse theorem for Gauss sums fails exactly when $q = 2\ell^i + 1$ for some integer $i > 0$.*

However, in our project we found counterexamples for the converse theorem which are not of teh form $q = 2\ell^i + 1$.

Parameterizing Characters via Generators

Let q be a prime power and ℓ a prime. There exists an integer N, depending only on q and ℓ, such that every multiplicative character

$$\theta : \mathbb{F}_{q^2}^* \to \overline{\mathbb{F}_\ell}^*, \qquad \alpha : \mathbb{F}_q^* \to \overline{\mathbb{F}_\ell}^*$$

has image in $\mathbb{F}_{\ell^N}^*$.
Let h be a generator of the cyclic group $\mathbb{F}_{\ell^N}^*$. By raising h to an appropriate power we obtain a generator ζ of the group of roots of unity of order q^2-1 in $\mathbb{F}_{\ell^N}^*$.
Fix a generator g of $\mathbb{F}_{q^2}^*$, and define the multiplicative characters θ_i by:

$$\theta_i(g^k) = \zeta^{ki}, \qquad i \in \mathbb{Z}/(q^2-1)\mathbb{Z}.$$

Similarly, define characters α_j on $\mathbb{F}_q^*$ by:

$$\alpha_j(g^{(q+1)k}) = \zeta^{(q+1)kj}, \qquad j \in \mathbb{Z}/(q-1)\mathbb{Z}.$$

Note that these index sets may yield some characters multiple times, and we handle them appropriately in our implementation.

Our Program

We implemented a SageMath program to automatically identify potential counterexamples to the Converse Theorem. The parameters used here are $\ell = 2$ and $q = 49$.

Theta Groupings	Size	$\theta_1\|_{\mathbb{F}_q^*} = \theta_2\|_{\mathbb{F}_q^*}$	Size
{1,7,43,49}	4	{1,7,43,49}	4
{2,11,14,23}	4	{2,11,14,23}	4
{3,21,54,72}	4	{3,21,54,72}	4
{4,22,28,46}	4	{4,22,28,46}	4
{5,20,35,65}	4	{5,20,35,65}	4
{6,33,42,69}	4	{6,33,42,69}	4

Table 1: *Partial program output of counterexample groupings (with and without restriction)*

Each row shows a set of θ that yield identical Gauss sums for all α. The left two columns display these groupings without imposing any restrictions. The right two columns show groupings under the additional constraint that $\theta_1|_{\mathbb{F}_q^*} = \theta_2|_{\mathbb{F}_q^*}$, as required by the classical Converse Theorem.
The presence of a grouping of size $m > 2$ under this restriction indicates a failure of the theorem in the $(\ell, q) = (2, 49)$ setting.

Conjecture Investigation

ℓ	q	Size
2	3	1
2	7	1
2	11	2
2	13	2
2	19	2
2	23	2

Table 2: *CSV used to find counterexamples not following proposed form*

ℓ	q	Size
2	5	3
2	9	5
2	17	9
2	257	1
3	7	4
3	19	10

Table 2: *CSV used to find a pair in the proposed form that is not a counterexample*

To produce a counterexample to the Converse Theorem, it suffices to find a θ-grouping of size $m > 2$. The theorem states that if two characters θ_1 and θ_2 yield the same Gauss sum, then they must either be equal or satisfy $\theta_1 = \theta_2^q$. Consequently, each equivalence class under this relation contains at most two distinct characters.

References

[1] A.R. Duncan, *Character Theory*, 2023. Available at: `https://duncan.math.sc.edu/s23/math742/notes/characters.pdf`

[2] C. Nien and L. Zhang, *Converse Theorem Meets Gauss Sums* (with an appendix by Zhiwei Yun), arXiv preprint arXiv:1806.04850 (2018). `https://arxiv.org/abs/1806.04850`

[3] C. Pinner, *Twisted Gauss Sums and Prime Power Moduli*, Preprint, available from Kansas State University. Accessed: February 4, 2025. `https://www.math.ksu.edu/~pinner/Pubs/tgauss4aRevised2.pdf`

[4] D. Forney, Lecture Notes, Massachusetts Institute of Technology, 2005. [Online]. Available: `https://ocw.mit.edu/courses/6-451-principles-of-digital-communication-ii-spring-2005/`

[5] J. Bakeberg, M. Gerbelli-Gauthier, H. Goodson, A. Iyengar, G. Moss, and R. Zhang, *Mod ℓ Gamma Factors and a Converse Theorem for Finite General Linear Groups*, arXiv:2307.07593 (2023). `https://arxiv.org/abs/2307.07593`

Acknowledgment: We thank Dr. Elad Zelingher and Calvin Yost-Wolff for their guidance and support.