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. These findings not only challenge long-standing number-theoretic assumptions, but also have significant implications for cryptography, which relies on the uniqueness of characters modulo ℓ.

Objective: Find counterexamples for $n = 2$ using our custom SageMath program, explore the potential patterns behind these counterexamples, and investigate existing conjectures related to these patterns. Based on our computational findings, we may propose our own conjecture on character uniqueness modulo ℓ.

INTRODUCTION

Gauss sums are sums over finite fields that link multiplicative and additive characters together, encoding deep algebraic information. The *Converse Theorem* asserts a strong uniqueness property: two characters yielding identical sums must be the same or related by a well understood transformation. However, recent evidence shows that for modulo ℓ, this uniqueness can, quite unexpectedly in practice, fail. Our research reproduces known failures when $n = 2$, searches for new examples, and investigates how these failures might affect number theory and cryptographic security, where modular arithmetic is pervasive.

RESEARCH GOALS

- **Confirm Known Failures:** Validate previously identified counterexamples for $n = 2$.
- **Pattern Detection:** Use our SageMath code to find additional counterexamples and use those counter examples to find potential patterns and for conjecture investigation.
- **Conjecture Investigation:** Investigate existing conjectures regarding the forms that counterexamples must take; if a consistent pattern emerges, propose our own.

THEORETICAL BACKGROUND

Finite Fields A finite field $\mathbb{F}_q$ is a field with exactly $q = p^m$ elements, where p is a prime and m is a positive interger. For each such q, there is a unique field (up to isomorphism) $\mathbb{F}_q$, and its nonzero elements form a cyclic group under multiplication.

Characters A *multiplicative character* is a function

$$\theta\colon \mathbb{F}_q^* \to \mathbb{C}^*,$$

which is a group homomorphism from the multiplicative group $\mathbb{F}_q^*$ (all nonzero elements of the finite field $\mathbb{F}_q$) to the nonzero complex numbers. This means that for all $a, b \in \mathbb{F}_q^*$,

$$\theta(a \cdot b) = \theta(a)\theta(b).$$

Similarly, an *additive character* is a function

$$\psi\colon \mathbb{F}_q \to \mathbb{C}^*,$$

which is a group homomorphism from the additive group $\mathbb{F}_q$ to $\mathbb{C}^*$; that is, for all $a, b \in \mathbb{F}_q$,

$$\psi(a + b) = \psi(a)\psi(b).$$

Definition (Gauss Sum)**.** *For $\mathbb{F}_q$, a multiplicative character θ, and an additive character ψ, the classical Gauss sum is*

$$G(\theta, \psi) = \sum_{a \in \mathbb{F}_q^*} \theta(a)\,\psi(a).$$

Twisted Gauss Sum in $\mathbb{F}_{q^2}$: Consider $m = 2$. If given two multiplicative characters $\theta\colon \mathbb{F}_{q^2}^* \to \mathbb{C}^*$ and $\alpha\colon \mathbb{F}_q^* \to \mathbb{C}^*$, and ψ is an additive character on $\mathbb{F}_q$, then

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

where N is the norm and tr is the trace from $\mathbb{F}_{q^2}$ down to $\mathbb{F}_q$.

Converse Theorem (Classical): Consider two multiplicative characters θ_1 and θ_2 of $\mathbb{F}_{q^2}^*$ to $\mathbb{C}^*$. Let $\psi\colon \mathbb{F}_q \to \mathbb{C}^*$ be a fixed non-trivial additive character. Suppose $\theta_1 \mid_{\mathbb{F}_q^*} = \theta_2 \mid_{\mathbb{F}_q^*}$, and suppose $\forall$ multiplicative characters $\alpha\colon \mathbb{F}_q^* \to \mathbb{C}^*$, the following equality holds:

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

then

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

Why do collisions occur? Originally, one might suspect that distinct characters could collapse into the same residue classes, creating apparent collisions in Gauss sums. However, our code has been updated to avoid merging distinct characters this way. Any collisions we now observe must therefore arise from deeper structural reasons that are intrinsic to the sums themselves. Investigating these collisions remains central to our research, as they indicate genuine failures of the expected uniqueness in Gauss sums modulo ℓ.

OUR CONJECTURE & PROGRAM

Proposed Form: Some prior work by Bakeberg, Gerbelli-Gauthier, Goodson, Iyengar, Moss, and Zhang suggests that failures may occur when $q = 1 + 2\,\ell^j$. However, our code detected an example not fitting this form (3,25), suggesting there might exist a broader and more complex structure of counterexamples than previously believed or documented.

SageMath Approach:

- We systematically loop over all possible combinations of primes ℓ and prime powers q.
- For each (ℓ, q), we build all relevant characters and compute $G(\theta \times \alpha, \psi)$ in $\overline{\mathbb{F}}_\ell$.
- We check if $\theta_1 \neq \theta_2$ yet yield identical sums across all columns. If such collisions exist in groups of size ≥ 3, we record all of the theta value in the group along with its size.
- For each recorded counterexample, we verify whether q satisfies the form proposed in the conjecture. Our terminal output, for instance, highlights a prime $\ell = 29$ along with certain q values that deviate from the expected form $q = 1 + 2\,\ell^j$, yet still produce large identical groups challenging the usual expectation of uniqueness.

Goal: Identify patterns among the counterexamples and refine (or replace) the conjecture.

CRYPTOGRAPHIC IMPLICATIONS

Many cryptographic protocols rely on the distinctness of certain character sums modulo ℓ. If the same Gauss sum signature can arise from multiple characters, key generation or signature verification methods that assume uniqueness might be at risk. Although no immediate break has been demonstrated, our findings highlight a potential vulnerability: cryptosystems using Gauss sums must confirm that collisions do not undermine security.

FIGURES & EXAMPLES

(l,q)	Size	$q = 1 + 2\,\ell^j$	Remarks
$(3, 9)$	3	True	Matches form
$(5, 26)$	4	False	Outside form, still fails
$(29, \dots)$	$\dots$	False	Terminal output shows collisions

Table 1: *Sample program output. Some counterexamples fit $q = 1 + 2\,\ell^j$, while others do not. Our goal is to detect patterns and refine the conjecture from our counter examples.*

RESULTS

- **Multiple Collisions:** We found many distinct θ that produce identical Gauss sums.
- **Group Size ≥ 3:** We focus on collisions of at least three rows, indicating deeper failures.
- **Form $q = 1 + 2\,\ell^j$** is not universal. Some examples match this form, but others do not, motivating a broader conjecture.
- **Cryptography Impact:** Collisions in Gauss sums may degrade assumptions about uniqueness, potentially affecting cryptosystems based on character sums.

FUTURE DIRECTIONS

In our future work, we plan to extend our computational tests to larger values of q and ℓ in order to determine whether a more general pattern emerges. This extended search will allow us to explore a broader range of parameters, capturing subtle variations in the behavior of Gauss sums that may not be evident at smaller scales. At the same time, we aim to propose a new structural description that encompasses both cases where $q = 1 + 2\,\ell^j$ holds and cases where the observed pattern deviates. By integrating these findings, we intend to develop a refined conjecture that provides a comprehensive framework for understanding when and why the Converse Theorem fails in the modular setting.

References

[1] A.R. Duncan, *Character Theory*, 2023.

[2] C. Nien and L. Zhang, *Converse Theorem Meets Gauss Sums*, arXiv:1806.04850 (2018).

[3] C. Pinner, *Twisted Gauss Sums and Prime Power Moduli*, Preprint.

[4] Stanford University, *Introduction to Finite Fields*, 2025.

[5] E. Zelingher, *Failure of Converse Theorems of Gauss Sums Modulo ℓ*, Preprint (2025).

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