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

February 27, 2025

Failure of the Converse Theorem in Modular Fields

- **Observation:** Recent work by Bakeberg–Gerbelli-Gauthier–Goodson–Iyengar–Moss–Zhang shows that when we reduce Gauss sums modulo a prime ℓ, *distinct* characters can yield *identical* Gauss sums. This contradicts the usual Converse Theorem [2].
- **Motivation:** Such failures challenge the uniqueness of characters under modular reduction, with potential repercussions in cryptography and coding theory (where mod ℓ operations are common).
- **Our Plan:**
    - Investigate these counterexamples for $n = 2$ in more depth.
    - Extend to larger n, aiming to identify precisely when and why the theorem breaks down mod ℓ.
    - Refine conjectures regarding character uniqueness in modular settings.
    - Utilize SageMath to generate and analyze new examples.

Introduction

- Gauss sums are essential in number theory and finite field analysis.
- We break down key concepts before defining Gauss sums rigorously.
- This will provide a structured understanding before analyzing the code.

Definition of a Group

James Evans, Xinning Ma, Yanshun Zhang
Mentors: Dr. Elad Zelingher, Calvin Yost-Wolff

- A group G is a non-empty set equipped with a binary operation $\cdot : (a, b) \mapsto a \cdot b$, satisfying:
  1. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in G$.
  2. Identity: There exists an element e such that $e \cdot a = a \cdot e = a \quad \forall a \in G$.
  3. Inverse: Each $a \in G$ has an inverse a^{-1} such that $a \cdot a^{-1} = e$.
- A group is called **abelian** if $a \cdot b = b \cdot a \quad \forall a, b \in G$.
- A group is called **cyclic** if it can be generated by a single element. That is, G is cyclic if there exists an element $a \in G$ such that $G = \langle a \rangle$.

University of Michigan LoG(M)

James Evans, Xinning Ma, Yanshun Zhang
Mentors: Dr. Elad Zelingher, Calvin Yost-Wolff

Definition of a Field

- A **field** $\mathbb{F}$ is a set with two operations: addition $(+)$ and multiplication $(\cdot)$, satisfying:
  1. $(\mathbb{F}, +)$ is an abelian group under addition.
  2. $(\mathbb{F}^{\times} = \mathbb{F} \setminus \{0\}, \cdot)$ is an abelian group under multiplication.
  3. There exist identity elements $0 \in \mathbb{F}$ (the additive identity) and $1 \in \mathbb{F}$ (the multiplicative identity), such that:

     $$a + 0 = a, \quad a \cdot 1 = a \quad \forall a \in \mathbb{F}.$$

  4. Distributive law: $a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall a, b, c \in \mathbb{F}.$
- A **finite field** (or Galois field) $\mathbb{F}_q$ has q elements, where q is a prime power.
- For every finite field $\mathbb{F}_q$, the multiplicative group $\mathbb{F}_q^*$ is cyclic.

Example: The Field $\mathbb{F}_3$

University of Michigan LoG(M)

James Evans, Xinning Ma, Yanshun Zhang
Mentors: Dr. Elad Zelingher, Calvin Yost-Wolff

- Elements: $\mathbb{F}_3 = \{0, 1, 2\}$.
- **Identity Elements:**
  - Additive identity: 0, since $a + 0 = a \quad \forall a$.
  - Multiplicative identity: 1, since $a \cdot 1 = a \quad \forall a \neq 0$.
- **Inverses:**
  - Additive inverse: $1 + (2) = 3 \equiv 0 \pmod 3$, $2 + (1) \equiv 0 \pmod 3$, $0 = 0 \pmod 3$.
  - Multiplicative inverse: $1 \cdot (1) = 1 \pmod 3$, $2 \cdot (2) = 4 \equiv 1 \pmod 3$.
- **Example of Closure and Associativity:**
  - Closure: $1 + 2 = 0 \mod 3$, stays in $\mathbb{F}_3$.
  - Associativity: $(1 + 2) + 1 = 0 + 1 = 1$ is the same as $1 + (2 + 1) = 1 + 0 = 1$.
- This satisfies all field axioms.

Definition of a character

- Let G be a finite group of order n. A *character* of G is a group homomorphism

$$\chi : G \to \mathbb{C}^*.$$

That is, $\chi(g_1 g_2) = \chi(g_1)\chi(g_2) \quad \forall g_1, g_2 \in G$

- Since $\chi(1_G \cdot g) = \chi(1_G)\chi(g) \quad \forall g \in G$, we must have $\chi(1_G) = 1$.
- $(\chi(g))^n = \chi(g^n) = \chi(1_G) = 1 \quad \forall g \in G$, so the value of $\chi(g)$ is an nth roots of unity.
- **Example:**
  - Let $G = \langle g \rangle$ be a finite cyclic group of order n. Then $\chi(g) = e^{\frac{2\pi i}{n}}$. For a fixed integer j , $0 \leq j \leq n-1$, the function

$$\chi_j(g^k) = e^{\frac{2\pi ijk}{n}}, k = 0, 1, ..., n-1$$

defines a character of G.

Gauss Sums: Definition

University of Michigan LoG(M)

James Evans, Xinning Ma, Yanshun Zhang
Mentors: Dr. Elad Zelingher, Calvin Yost-Wolff

- The Gauss sum is an element of $\mathbb{C}$ (and is zero when ψ is trivial) and is associated with the field $\mathbb{F}_{q^m}$.
- Given a finite field $\mathbb{F}_{q^m}$ and two characters:
  - Multiplicative character $\theta : \mathbb{F}_{q^m}^* \to \mathbb{C}^*$.
  - Additive character $\psi : \mathbb{F}_{q^m} \to \mathbb{C}^*$.
  - The norm $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \to \mathbb{F}_q$
  - The trace $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \to \mathbb{F}_q$
- The Gauss sum is defined as:

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

- The function $\alpha : \mathbb{F}_q^* \to \mathbb{C}^*$ is an additional multiplicative character used for twisting.

Twisted Gauss Sum

Definition: We consider the case when $m = 2$. The twisted Gauss sum is an element of $\mathbb{C}$ (and is zero when ψ is trivial) and is associated with the field $\mathbb{F}_{q^2}$. If $G(\alpha, \psi)$ is a standard Gauss sum for a multiplicative character α and an additive character ψ, a twisted Gauss sum is of the form:

$$G(\Theta \times \alpha, \Psi) = \sum_{x \in \mathbb{F}_{q^2}^*} \Theta(x) \cdot \alpha(N(x)) \cdot \Psi(\mathrm{tr}(x)), \qquad (1)$$

where:

- Θ and α are multiplicative characters of $\mathbb{F}_{q^2}^*$, mapping $\mathbb{F}_{q^2}^*$ to $\mathbb{C}^*$.
- Ψ is an additive character of $\mathbb{F}_{q^2}$, mapping $\mathbb{F}_{q^2}$ to $\mathbb{C}^*$.
- $N(x)$ represents the norm function $N : \mathbb{F}_{q^2} \to \mathbb{F}_q$.
- $\mathrm{tr}(x)$ represents the trace function $\mathrm{tr} : \mathbb{F}_{q^2} \to \mathbb{F}_q$.

The Converse Theorem of Gauss Sums [1]

University of Michigan LoG(M)

James Evans, Xinning Ma, Yanshun Zhang
Mentors: Dr. Elad Zelingher, Calvin Yost-Wolff

Theorem

We consider the case when $m = 2$*. Consider two multiplicative characters* θ_1 *and* θ_2 *of* $\mathbb{F}_{q^2}^*$*. Let* $\psi : \mathbb{F}_q \to \mathbb{C}^*$ *be a fixed non-trivial additive character. Suppose* $\theta_1 |_{\mathbb{F}_q^*} = \theta_2 |_{\mathbb{F}_q^*}$*, and suppose* $\forall$ *multiplicative characters* $\alpha : \mathbb{F}_q^* \to \mathbb{C}^*$*, the following equality holds:*

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

then

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

Macro Purpose of the Code

University of Michigan LoG(M)

James Evans, Xinning Ma, Yanshun Zhang
Mentors: Dr. Elad Zelingher, Calvin Yost-Wolff

- The purpose of this code is to generate a **table of Gauss sums** over the finite field $\mathbb{F}_{q^2}$.
- In this table:
  - Each **row** corresponds to a multiplicative character α.
  - Each **column** corresponds to a multiplicative character θ.
  - The additive character ψ is **fixed** throughout.
- For a given pair (θ, α), the table stores the value of the twisted Gauss sum: $G(\theta \times \alpha, \psi)$.

Constructing the Table

University of Michigan LoG(M)

James Evans, Xinning Ma, Yanshun Zhang
Mentors: Dr. Elad Zelingher, Calvin Yost-Wolff

- The multiplicative generator of $\mathbb{F}_{q^2}^*$ is used to systematically construct different possible characters.
- Raising the generator to different powers gives distinct character mappings for α and θ.
- Each row and each column corresponds to a different possible character created from the generator.
- An entry in the table represents the twisted Gauss sum for the combination of those two particular characters.

Relation to the Converse Theorem

- This structure allows us to compare different character mappings.
- The table provides a framework for analyzing the behavior of twisted Gauss sums in relation to the Converse Theorem.
- Understanding how character mappings interact helps in proving or refuting generalizations of Gauss sum identities.

Gauss Sum Table Example Output

University of Michigan LoG(M)

James Evans, Xinning Ma, Yanshun Zhang
Mentors: Dr. Elad Zelingher, Calvin Yost-Wolff

$\theta \backslash \alpha$	0	1	$\dots$	$q-1$
0	$G(0,0)$	$G(0,1)$	$\dots$	$G(0,q-1)$
1	$G(1,0)$	$G(1,1)$	$\dots$	$G(1,q-1)$
2	$G(2,0)$	$G(2,1)$	$\dots$	$G(2,q-1)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
q^2-1	$G(q^2-1,0)$	$G(q^2-1,1)$	$\dots$	$G(q^2-1,q-1)$

Applying the Converse Theorem

University of Michigan LoG(M)

James Evans, Xinning Ma, Yanshun Zhang
Mentors: Dr. Elad Zelingher, Calvin Yost-Wolff

- The Converse Theorem of Gauss Sums states that if two multiplicative characters produce identical Gauss sums across all additive characters ψ and all multiplicative characters α, then θ_1 and θ_2 must be identical or related by a well-understood transformation.
- In the Gauss sum table, each row corresponds to a different multiplicative character θ, and each column corresponds to a different multiplicative character α.
- To apply the theorem:
  - Identify two rows in the table where all entries match across all ψ and α values.
  - Highlight these rows and investigate the corresponding θ_1 and θ_2.
  - Check whether θ_1 and θ_2 are identical or related by a known transformation.
- This process helps verify whether the Converse Theorem holds in our computed Gauss sum table.

References

[1] Chufeng Nien and Lei Zhang. *Converse Theorem Meets Gauss Sums (with an appendix by Zhiwei Yun).* arXiv preprint, arXiv:1806.04850 (2018). Available at: https://arxiv.org/abs/1806.04850.

[2] Elad Zelingher. *Failure of Converse Theorems of Gauss Sums Modulo ℓ.* Preprint, 2025. Available at: https://lsa.umich.edu/content/dam/math-assets/logm/wn2025/ELAD-ZELINGHER.pdf.

Acknowledgments

Thank You!

We extend our gratitude to:

Dr. Elad Zelingher and **Calvin Yost-Wolff**

for their guidance, insights, and contributions to this research.