Failure of Converse Theorems of Gauss Sums Modulo ℓ

James Evans

05/08/2025

Motivating Move

The truth isn't as it first appears: although Gauss sums are known to determine characters uniquely over the complex numbers, this property can break down over finite fields, raising the question of when and why this failure occurs.

Introduction

Gauss sums are fundamental objects in number theory. They encode deep arithmetic information through the interaction of additive and multiplicative characters over finite fields. A key result in this area is the **converse theorem of Gauss sums**, which holds even under character modifications. For more details about the **converse theorem of Gauss sums**, see [3]. The term "character modifications" refers to transformations applied to multiplicative or additive characters of a finite field, which can change how these characters interact in Gauss sums. These modifications often involve shifting or scaling characters in a way that theoretically preserves key properties of the sums. One important example of a character modification is the concept of a **twisted Gauss sum** [4].

Definition 0.1 (Twisted Gauss Sum)**.** 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:

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

such that:

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

Twisting modifies the behavior of the Gauss sum and is often used in proving results related to the converse theorem of Gauss sums. In some cases, these modifications lead to counterexamples where the expected properties of Gauss sums break down, contributing to the failure of the theorem. This project investigates the failure of the converse theorem of Gauss sums when the complex field $\mathbb{C}$ is replaced by the finite field $\mathbb{F}_\ell$, where $\ell = p^k$ is a prime power and $k \geq 1$. In particular, we will examine prior counterexamples found for the case when the dimension n of the finite field extension is equal to 2. These counterexamples raise questions about the general validity of the converse theorem of Gauss sums. In this project, we investigate known and newly generated counterexamples to assess whether they conform to the form proposed by Bakeberg, Gerbelli-Gauthier, Goodson, Iyengar, Moss, and Zhang [1]. We then examine whether these counterexamples exhibit any consistent patterns and, based on this analysis, hope to propose a new conjecture characterizing when and how the theorem fails in modular settings.

Background and Motivation

A Gauss sum is a fundamental mathematical construct that arises in the study of finite fields and their applications in number theory. To define it, we first need to understand the basic components involved:

Definition 0.2 (Finite Field)**.** A *finite field*, denoted as $\mathbb{F}_q$, is a set with a finite number of q elements, where q is a prime power ($q = p^n$ for some prime p and integer $n \geq 1$).

Finite fields satisfy all the standard properties of fields: they allow addition, subtraction, multiplication, and division (except by zero) in a manner that satisfies the familiar algebraic rules [5, Definition 7.2]. For example:

- $\mathbb{F}_2 = \{0, 1\}$ is a field with two elements, commonly used in boolean algebra.
- For $q > 2$, $\mathbb{F}_q$ is constructed using polynomials over $\mathbb{F}_p$ modulo an irreducible polynomial of degree n.

To better understand how field extensions work in finite fields, it's helpful to begin with a familiar example: the complex numbers. The real numbers $\mathbb{R}$ form a field — you can add, subtract, multiply, and divide (except by zero). However, the equation $x^2 + 1 = 0$ has no solution in $\mathbb{R}$, since no real number squared gives -1. To resolve this, we define a new number i such that $i^2 = -1$, and construct the field of complex numbers $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$. This process is called a *field extension*: we start with a base field and extend it by adding a new element that satisfies an otherwise unsolvable polynomial equation.

The same idea applies to finite fields. To construct the field $\mathbb{F}_4$, we begin with the base field $\mathbb{F}_2 = \{0, 1\}$, where arithmetic is done modulo 2. Our goal is to create a field with four elements, which requires introducing a new element that isn't already in $\mathbb{F}_2$. We do this by adjoining a root α of the polynomial $x^2 + x + 1$. This polynomial has no solutions in $\mathbb{F}_2$ — neither 0 nor 1 satisfies it, so it is irreducible over $\mathbb{F}_2$. Now that we've defined this new element α, we construct all the possible expressions of the form:

$$a + b\alpha \quad \text{where } a, b \in \mathbb{F}_2.$$

Since each of a and b can be either 0 or 1, we get four combinations:

$$0, \quad 1, \quad \alpha, \quad \alpha + 1.$$

These are the elements of $\mathbb{F}_4$. This process is similar to how you work with basis vectors in a vector space: the field $\mathbb{F}_4$ can be viewed as a 2-dimensional vector space over $\mathbb{F}_2$ with basis $\{1, \alpha\}$. Every element in the field is a linear combination of these two terms, and none of the elements can be written as a combination of the others — they are linearly independent.

Definition 0.3 (Character)**.** A *character* is a type of function that encodes algebraic properties into complex numbers.

Specifically, two types of characters are essential in defining Gauss sums:

- A **multiplicative character** $\alpha : \mathbb{F}_q^\times \to \mathbb{C}^\times$ maps elements of the multiplicative group of $\mathbb{F}_q$ (excluding 0) to the nonzero complex numbers. These characters respect multiplication, meaning $\alpha(ab) = \alpha(a)\alpha(b)$ for all $a, b \in \mathbb{F}_q^\times$.
- An **additive character** $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ maps elements of the entire field $\mathbb{F}_q$ to the nonzero complex numbers. These characters respect addition, meaning $\psi(a + b) = \psi(a)\psi(b)$ for all $a, b \in \mathbb{F}_q$.

In classical settings, characters are often defined with values in $\mathbb{C}^\times$, but when studying reductions modulo ℓ or working over finite fields, it is more appropriate to define them with values in $\overline{\mathbb{F}_\ell}^\times$. For more details about **characters** see [2].

Gauss Sums

A Gauss sum is a fundamental object in number theory that encapsulates important algebraic and analytic information about **finite fields** [5].

Definition 0.4 (Gauss Sum)**.** Given a finite field $\mathbb{F}_q$ and two characters:

- A multiplicative character $\alpha : \mathbb{F}_q^\times \to \mathbb{C}^\times$,
- An additive character $\psi : \mathbb{F}q \to \mathbb{C}^\times$,

we define the Gauss sum as:

$$G(\alpha, \psi) = \sum_{a \in \mathbb{F}_q^\times} \alpha(a)\, \psi(a). \tag{2}$$

Gauss sums play a key role in understanding how characters interact over finite fields and serve as a bridge between algebra and analysis in number theory.

The Converse Theorem of Gauss Sums

The **converse theorem of Gauss sums** states that under certain conditions, two multiplicative characters on a finite field must be identical if their associated Gauss sums behave in the same way across all additive characters [3, Theorem 1.2].

Theorem 0.1 (Converse Theorem of Gauss Sums)**.** *Let θ_1 and θ_2 be multiplicative characters defined on the multiplicative group $\mathbb{F}_{q^m}^\times$. Let ψ be a fixed nontrivial additive character on $\mathbb{F}_{q^m}$. Let $\theta_1|_{\mathbb{F}_q^\times} = \theta_2|_{\mathbb{F}_q^\times}$. If for all multiplicative characters α on $\mathbb{F}_{q^m}^\times$, the following identity holds:*

$$G(\theta_1 \times \alpha, \psi) = G(\theta_2 \times \alpha, \psi), \tag{3}$$

$$\sum_{a \in \mathbb{F}_{q^m}^\times} \theta_1(a)\alpha(a)\psi(a) = \sum_{a \in \mathbb{F}_{q^m}^\times} \theta_2(a)\alpha(a)\psi(a), \tag{4}$$

then it must be the case that

$$\theta_1 = \theta_2 \quad or \quad \theta_1 = \theta_2^q.$$

Intuitively, this theorem tells us that Gauss sums over the complex numbers contain enough information to "uniquely" determine a character. However, recent work by **Bakeberg, Gerbelli-Gauthier, Goodson, Iyengar, Moss, and Zhang** has shown that this conclusion no longer holds when the Gauss sums are reduced modulo a prime ℓ — that is, when they are considered over the finite field $\mathbb{F}_\ell$ [1]. In this modular setting, the authors discovered explicit counterexamples for the case $n = 2$ where two distinct characters $\theta_1 \neq \theta_2$ and $\theta_1 \neq \theta_2^q$ nonetheless satisfy

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

for all additive characters ψ on $\mathbb{F}_{q^2}$ and all multiplicative characters α on $\mathbb{F}_q^\times$. These examples demonstrate a breakdown of the converse theorem in modular arithmetic, revealing that the behavior of Gauss sums over $\mathbb{F}_\ell$ can diverge significantly from their behavior over $\mathbb{C}$. This failure of the theorem suggests that new phenomena arise in modular arithmetic that are not present over $\mathbb{C}$. Our project investigates these counterexamples in depth. By analyzing patterns in these modular failures, we hope to better understand the limitations of the converse theorem and propose a refined conjecture that captures when it does and does not hold in the modular setting.

Computational Framework

To investigate the failure of the converse theorem of Gauss sums in modular settings, we developed a computational framework in SageMath to construct and analyze Gauss sum tables under both complex and modular arithmetic.

Constructing Gauss Sums over $\mathbb{C}$

The first version of our implementation focused on computing Gauss sums over the complex numbers. This choice offered significant simplicity: defining characters and finding explicit generators was much more straightforward over $\mathbb{C}$. This allowed us to rapidly prototype and validate our logic before extending the implementation to work over finite fields. We defined a class `GaussSumTable` that takes as input:

- a finite field size q,
- a generator for an additive character over $\mathbb{F}_q$, and
- a generator for a multiplicative character over $\mathbb{F}_{q^2}^\times$.

We initialize the field $\mathbb{F}_{q^2}$ using `GF(q^2)` and collect all nonzero field elements to form the multiplicative group. The Gauss sum table is then built using a nested loop: the outer loop runs over all multiplicative characters θ on $\mathbb{F}_{q^2}^\times$ (indexed by discrete logarithms), and the inner loop iterates over multiplicative characters α on $\mathbb{F}_q^\times$ via the norm map. For each pair (θ, α), we compute the twisted Gauss sum:

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

where $\mathrm{tr}(x)$ and $N(x)$ denote the trace and norm of x from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$, respectively. For complex Gauss sums, we used:

$$\psi(x) = e^{2\pi i \cdot \mathrm{tr}(x)/p}, \quad \theta(x) = e^{2\pi i \cdot \log(x)/(q^2-1)},$$

where p is the characteristic of the field and $\log(x)$ denotes the discrete log of x relative to a fixed generator. To visualize the results of our computation, we constructed a two-dimensional Gauss sum table indexed by multiplicative characters θ and twisting characters α. Each cell $G(\theta, \alpha)$ contains the value of the Gauss sum associated with those two characters. This table structure allows us to systematically investigate patterns and identify counterexamples that defy the predictions of the converse theorem. The format of the table is as follows:

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

Computing Gauss Sums over $\overline{\mathbb{F}_\ell}$

To study Gauss sums modulo ℓ, we extended our implementation to work over $\overline{\mathbb{F}_\ell}$. This required constructing additive and multiplicative characters whose values lie in a finite field $\mathbb{F}_{\ell^c}$, which contains all necessary roots of unity. Let q be a prime power and ℓ a prime. Define $N = p(q^2-1)$, where p is the underlying prime of q. To ensure $\mathbb{F}_{\ell^c}$ contains the needed N-th roots of unity, we set

$$c = \lambda\left(\frac{p(q^2-1)}{\ell^m}\right),$$

where ℓ^m is the largest power of ℓ dividing N, and λ denotes the multiplicative order of ℓ modulo N/ℓ^m. We then work in $\mathbb{F}_{\ell^c}$, whose multiplicative group contains the desired N-th roots of unity. We select a generator $h \in \mathbb{F}_{\ell^c}^\times$, and define

$$\zeta = h^{p(\ell^c-1)/N'}, \quad \text{where } N' = \frac{p(q^2-1)}{\ell^m}.$$

This gives a generator ζ of the group of (q^2-1)-th roots of unity. To define the relevant characters, we first fix a generator $g \in \mathbb{F}_{q^2}^\times$, which has order q^2-1. For each $i \in \mathbb{Z}/(q^2-1)\mathbb{Z}$, we define the multiplicative character θ_i by

$$\theta_i(g^k) = \zeta^{ik}.$$

Similarly, we define characters α on $\mathbb{F}_q^\times$, using the same generator g, by setting

$$\alpha(g^k) = \zeta^{\alpha(q+1)k},$$

where $\alpha \in \mathbb{Z}/\left(\frac{q-1}{\ell^{m'}}\right)\mathbb{Z}$, and m' is the largest power of ℓ dividing $q-1$. Finally, we define the additive character as:

$$\psi_{\text{add}} = h^{(\ell^c-1)/p}.$$

This construction mirrors the complex case but is fully adapted to the modular setting, giving us complete control over the character values used in evaluating Gauss sums modulo ℓ. The breakthrough we experienced after implementing the character generators needed to express these Gauss sums over $\mathbb{F}_{\ell^c}$ inadvertently led to another hurdle. Initially, our code computed Gauss sums by iterating over all possible character indices θ and α in the ranges $0, 1, \ldots, q^2-2$ and $0, 1, \ldots, q-2$, respectively. However, due to the cyclic nature of the character generators in finite fields, many of these index combinations resulted in redundant or equivalent characters. This led to repeated evaluations of essentially the same Gauss sum values. To fix this and ensure our computations were both correct and meaningful for detecting true counterexamples to the converse theorem, we adjusted the iteration ranges. Specifically, we now loop over $\theta \in \{0, 1, \ldots, N-1\}$ and $\alpha \in \{0, 1, \ldots, M-1\}$, where $N = (q^2-1)//\ell$ and $M = (q-1)//\ell$. This change eliminated duplicate cases caused by ℓ-torsion and enables us to properly probe the modular structure for counterexamples.

$\theta\backslash\alpha$	0	1	$\cdots$	j	$\cdots$	$M-1$
0	$G(0,0)$	$G(0,1)$	$\cdots$	$G(0,j)$	$\cdots$	$G(0,M-1)$
1	$G(1,0)$	$G(1,1)$	$\cdots$	$G(1,j)$	$\cdots$	$G(1,M-1)$
2	$G(2,0)$	$G(2,1)$	$\cdots$	$G(2,j)$	$\cdots$	$G(2,M-1)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
i	$G(i,0)$	$G(i,1)$	$\cdots$	$G(i,j)$	$\cdots$	$G(i,M-1)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
$N-1$	$G(N-1,0)$	$G(N-1,1)$	$\cdots$	$G(N-1,j)$	$\cdots$	$G(N-1,M-1)$

Table 1: Revised Gauss sum table with optimized loop bounds $\theta \in \{0, \ldots, N-1\}$ and $\alpha \in \{0, \ldots, M-1\}$.

Verifying Counterexamples

Using our revised Gauss sum table implementation, we revisited the counterexamples identified by **Bakeberg, Gerbelli-Gauthier, Goodson, Iyengar, Moss, and Zhang** [1]. The results are summarized in the tables below. Each table displays theta groupings whose associated Gauss sums are identical for all multiplicative characters α and a fixed additive character ψ, i.e.,

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

According to the classical converse theorem for Gauss sums, this identity should imply

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

which would mean that each equivalence class of theta values under Gauss sums contains at most two distinct characters. However, our results demonstrate the existence of multiple equivalence classes whose sizes exceed two — even after imposing the standard restriction

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

which is equivalent to requiring that

$$\theta_1 \equiv \theta_2 \pmod{(q-1) \,//\, \ell}.$$

This restriction is fully respected in our updated implementation. The groupings in the third and fourth columns of the tables are formed using this congruence condition, and still we observe group sizes of 3, 4, and in some cases far larger — up to 30. This proves that these are not false positives or implementation artifacts. Rather, they are genuine counterexamples to the converse theorem of Gauss sums in the modular setting. Our findings confirm that the classical converse fails to hold when characters are defined over finite fields modulo ℓ, even with all the standard hypotheses enforced. These counterexamples establish clear boundaries for the applicability of the classical theory and underscore the need for refined formulations in the modular case.

Theta Groupings	**Size**	$\boldsymbol{\theta_1}\vert_{\mathbb{F}_q^*} = \boldsymbol{\theta_2}\vert_{\mathbb{F}_q^*}$	**Size**
{0, 1, 2}	3	{0, 1, 2}	3

Table 2: Identical theta groups for $l = 2$, $q = 5$

Theta Groupings	**Size**	$\boldsymbol{\theta_1}\vert_{\mathbb{F}_q^*} = \boldsymbol{\theta_2}\vert_{\mathbb{F}_q^*}$	**Size**
{0, 1, 2, 3, 4, 5, 6, 7, 8}	9	{0, 1, 2, 3, 4, 5, 6, 7, 8}	9

Table 3: Identical theta groups for $l = 2$, $q = 17$

Theta Groupings	**Size**	$\boldsymbol{\theta_1}\vert_{\mathbb{F}_q^*} = \boldsymbol{\theta_2}\vert_{\mathbb{F}_q^*}$	**Size**
{2,6,10,14}	4	{2,6,10,14}	4
{1,7}	2	{1,7}	2
{3,5}	2	{3,5}	2
{4,12}	2	{4,12}	2
{9,15}	2	{9,15}	2
{11,13}	2	{11,13}	2

Table 4: Identical theta groups for $l = 3$, $q = 7$

Theta Groupings	**Size**	$\boldsymbol{\theta_1}\vert_{\mathbb{F}_q^*} = \boldsymbol{\theta_2}\vert_{\mathbb{F}_q^*}$	**Size**
{2,6,10,14,18,22,26,30,34,38}	10	{2,6,10,14,18,22,26,30,34,38}	10
{4,8,12,16,24,28,32,36}	8	{4,8,12,16,24,28,32,36}	8
{5,15,25,35}	4	{5,15,25,35}	4
{1,19}	2	{1,19}	2
{3,17}	2	{3,17}	2
{7,13}	2	{7,13}	2
{9,11}	2	{9,11}	2
{21,39}	2	{21,39}	2
{23,37}	2	{23,37}	2
{27,33}	2	{27,33}	2
{29,31}	2	{29,31}	2

Table 5: Identical theta groups for $l = 3$, $q = 19$

Theta Groupings	**Size**	$\boldsymbol{\theta_1}\vert_{\mathbb{F}_q^*} = \boldsymbol{\theta_2}\vert_{\mathbb{F}_q^*}$	**Size**
{2,6,10,14,18,22}	6	{2,6,10,14,18,22}	6
{4,8,16,20}	4	{4,8,16,20}	4
{1,11}	2	{1,11}	2
{3,9}	2	{3,9}	2
{5,7}	2	{5,7}	2
{13,23}	2	{13,23}	2
{15,21}	2	{15,21}	2
{17,19}	2	{17,19}	2

Table 6: Identical theta groups for $l = 5$, $q = 11$

Theta Groupings	**Size**	$\boldsymbol{\theta_1}\vert_{\mathbb{F}_q^*} = \boldsymbol{\theta_2}\vert_{\mathbb{F}_q^*}$	**Size**
{2,6,10,14,18,22,26,30,34,38,42,46}	12	{2,6,10,14,18,22,26,30,34,38,42,46}	12
{4,8,12,16,20,28,32,36,40,44}	10	{4,8,12,16,20,28,32,36,40,44}	10
{1,23}	2	{1,23}	2
{3,21}	2	{3,21}	2
{5,19}	2	{5,19}	2
{7,17}	2	{7,17}	2
{9,15}	2	{9,15}	2
{11,13}	2	{11,13}	2
{25,47}	2	{25,47}	2
{27,45}	2	{27,45}	2
{29,43}	2	{29,43}	2
{31,41}	2	{31,41}	2
{33,39}	2	{33,39}	2
{35,37}	2	{35,37}	2

Table 7: Identical theta groups for $l = 11$, $q = 23$

Theta Groupings	**Size**	$\boldsymbol{\theta_1}\vert_{\mathbb{F}_q^*} = \boldsymbol{\theta_2}\vert_{\mathbb{F}_q^*}$	**Size**
{2,6,10,...,90,94}	24	{2,6,10,...,90,94}	24
{4,8,12,...,84,88,92}	22	{4,8,12,...,84,88,92}	22
{1,47}	2	{1,47}	2
{3,45}	2	{3,45}	2
{5,43}	2	{5,43}	2
{7,41}	2	{7,41}	2
{9,39}	2	{9,39}	2
{11,37}	2	{11,37}	2
{13,35}	2	{13,35}	2
{15,33}	2	{15,33}	2
{17,31}	2	{17,31}	2
{19,29}	2	{19,29}	2
{21,27}	2	{21,27}	2
{23,25}	2	{23,25}	2
{49,95}	2	{49,95}	2
{51,93}	2	{51,93}	2
{53,91}	2	{53,91}	2
{55,89}	2	{55,89}	2
{57,87}	2	{57,87}	2
{59,85}	2	{59,85}	2
{61,83}	2	{61,83}	2
{63,81}	2	{63,81}	2
{65,79}	2	{65,79}	2
{67,77}	2	{67,77}	2
{69,75}	2	{69,75}	2
{71,73}	2	{71,73}	2

Table 8: Identical theta groups for $l = 23$, $q = 47$

Theta Groupings	**Size**	$\boldsymbol{\theta_1\vert_{\mathbb{F}_q^*} = \theta_2\vert_{\mathbb{F}_q^*}}$	**Size**
{2,6,10,...,114,118}	30	{2,6,10,...,114,118}	30
{4,8,12,...,112,116}	28	{4,8,12,...,112,116}	28
{1,59}	2	{1,59}	2
{3,57}	2	{3,57}	2
{5,55}	2	{5,55}	2
{7,53}	2	{7,53}	2
{9,51}	2	{9,51}	2
{11,49}	2	{11,49}	2
{13,47}	2	{13,47}	2
{15,45}	2	{15,45}	2
{17,43}	2	{17,43}	2
{19,41}	2	{19,41}	2
{21,39}	2	{21,39}	2
{23,37}	2	{23,37}	2
{25,35}	2	{25,35}	2
{27,33}	2	{27,33}	2
{29,31}	2	{29,31}	2
{61,119}	2	{61,119}	2
{63,117}	2	{63,117}	2
{65,115}	2	{65,115}	2
{67,113}	2	{67,113}	2
{69,111}	2	{69,111}	2
{71,109}	2	{71,109}	2
{73,107}	2	{73,107}	2
{75,105}	2	{75,105}	2
{77,103}	2	{77,103}	2
{79,101}	2	{79,101}	2
{81,99}	2	{81,99}	2
{83,97}	2	{83,97}	2
{85,95}	2	{85,95}	2
{87,93}	2	{87,93}	2
{89,91}	2	{89,91}	2

Table 9: Identical theta groups for $l = 29$, $q = 59$

Disproving the Conjecture

In light of the empirical patterns observed across many counterexamples, Bakeberg, Gerbelli-Gauthier, Goodson, Iyengar, Moss, and Zhang proposed the following conjecture:

Conjecture 1. *The naive converse theorem for mod ℓ representations of* $\mathrm{GL}_2(\mathbb{F}_q)$ *fails exactly when $q = 2\ell^i + 1$ for some value of $i > 0$*[1].

This conjecture reflects a pattern that does indeed hold for many values of ℓ and q. However, our updated implementation of our program reveals a counterexample that contradicts this claim.

Counterexample: Let $\ell = 2$ and $q = 49$. The following identical theta group, computed by our Sage script, satisfies the Gauss sum equivalence condition:

$$G(\theta_1 \times \alpha, \psi) = G(\theta_2 \times \alpha, \psi) \quad \text{for all } \alpha.$$

This leads to a multiple theta groupings of size 4, which violates the converse theorem.

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
{8,17,44,56}	4	{8,17,44,56}	4
{9,12,63,66}	4	{9,12,63,66}	4
{10,40,55,70}	4	{10,40,55,70}	4
{13,16,34,37}	4	{13,16,34,37}	4
{15,30,45,60}	4	{15,30,45,60}	4
{18,24,51,57}	4	{18,24,51,57}	4
{19,31,58,67}	4	{19,31,58,67}	4
{26,32,68,74}	4	{26,32,68,74}	4
{27,36,39,48}	4	{27,36,39,48}	4
{29,47,53,71}	4	{29,47,53,71}	4
{38,41,59,62}	4	{38,41,59,62}	4
{52,61,64,73}	4	{52,61,64,73}	4

Table 10: Counterexample data for $\ell = 2$, $q = 49$

This counterexample is particularly striking because $q = 49$ does not satisfy the form $q = 2\ell^i + 1$ for any integer $i > 0$. Therefore, this example shows that the conjecture is too restrictive: while it captures many instances where the converse theorem fails, it does not account for all cases.

Additional Counterexamples

While our group has not yet been able to identify a unifying pattern among all known counterexamples to the converse theorem, we did find additional examples where the conjecture fails. These instances further suggest that the failure is not isolated to a specific class of primes or field sizes. Below we present two such counterexamples. Note that for the case $(\ell, q) = (2, 97)$, the table contains *partial output* due to formatting constraints.

Theta Groupings	Size	$\theta_1\|_{\mathbb{F}_q^*} = \theta_2\|_{\mathbb{F}_q^*}$	Size
{1, 2, 3, 4}	4	{1, 2, 3, 4}	4

Table 11: Counterexample for $\ell = 3$, $q = 4$

Theta Groupings	Size	$\theta_1\|_{\mathbb{F}_q^*} = \theta_2\|_{\mathbb{F}_q^*}$	Size
{7,28,70,91,112,133}	6	{7,28,70,91,112,133}	6
{14,35,56,77,119,140}	6	{14,35,56,77,119,140}	6
{21,42,63,84,105,126}	6	{21,42,63,84,105,126}	6
{1,97}	2	{1,97}	2
{2,47}	2	{2,47}	2
{3,144}	2	{3,144}	2
{4,94}	2	{4,94}	2
{5,44}	2	{5,44}	2
{6,141}	2	{6,141}	2
{8,41}	2	{8,41}	2
{9,138}	2	{9,138}	2
{10,88}	2	{10,88}	2
{11,38}	2	{11,38}	2
{12,135}	2	{12,135}	2

Table 12: Partial counterexample output for $\ell = 2$, $q = 97$

Obstacles

The conjecture above has already been disproven by explicit counterexamples. However, we sought to go further by investigating whether *every* failure of the converse theorem arises when $q = 2\ell^i + 1$. Specifically, we examined (ℓ, q) pairs of the form $q = 2\ell^i + 1$ to find a case that *does not* result in a counterexample. Discovering such a pair would show that the conjecture fails not only to describe when the theorem holds, but also to correctly identify when it fails—capturing neither the true nor the false cases accurately. Unfortunately, our search was hindered by computational bottlenecks. For large values of q, Sage's built-in algebraic tools struggled to factor group orders or compute character restrictions over $\mathbb{F}_{q^2}$. In many cases, the process resulted in stack overflows due to the size of the multiplicative groups involved. The table below summarizes our findings. Each row corresponds to a candidate (ℓ, q) pair of the form $q = 2\ell^i + 1$, and the third column records the size of the largest θ-grouping detected under character restriction. A value of `-1` indicates that the computation failed due to the aforementioned bottlenecks. We include the first 17 entries for illustration.

ℓ	q	**Size of Largest θ Grouping**
2	5	3
2	9	5
2	17	9
2	257	-1
3	7	4
3	19	10
3	163	-1
3	487	-1
3	1459	-1
5	11	6
5	251	-1
11	23	12
11	243	-1
11	2663	-1
13	27	14
23	47	24
29	59	30

Table 13: Partial results for (ℓ, q) pairs of the form $q = 2\ell^i + 1$. A value of `-1` indicates a failed computation.

References

[1] Jacksyn Bakeberg et al. *Mod ℓ gamma factors and a converse theorem for finite general linear groups.* 2023. arXiv: `2307.07593 [math.NT]`. URL: `https://arxiv.org/abs/2307.07593`.

[2] Alexander Rhys Duncan. *Character Theory.* Available at `https://duncan.math.sc.edu/s23/math742/notes/characters.pdf`. 2023.

[3] Chufeng Nien and Lei Zhang. "Converse Theorem Meets Gauss Sums (with an appendix by Zhiwei Yun)". In: *arXiv preprint arXiv:1806.04850* (2018). URL: `https://arxiv.org/abs/1806.04850`.

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

[5] Stanford University. *Introduction to Finite Fields.* Online PDF. Accessed: February 4, 2025. URL: `https://web.stanford.edu/~marykw/classes/CS250_W19/readings/Forney_Introduction_to_Finite_Fields.pdf`.