Failure of Converse Theorems of Gauss Sums Modulo ℓ

James Evans

01/24/2025

Introduction

Gauss sums are fundamental objects in number theory, with applications in areas such as modular forms and cryptography. These sums encode deep algebraic structures and are used in studying finite fields, characters, and exponential sums. A key result in this area is the converse theorem of Gauss sums, which provides conditions under which Gauss sums remain invariant under character modifications. For more details about the **converse theorem of Gauss sums** see [2]. Character modifications refer 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 should theoretically preserve key properties of the sums. One important example of a character modification is the concept of a **twisted Gauss sum** [3].

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 with p a prime 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 challenge the theorem's validity, and we will analyze their properties and explore possible generalizations for larger values of n. Our goal is to determine under what conditions the theorem holds or fails and propose a refined conjecture on the behavior of Gauss sums in modular arithmetic.

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 elements q, 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 [4, Definition 7.2]. For example:

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

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 $a, b \in \mathbb{F}_q$. A standard example is $\psi(a) = e^{2\pi i \mathrm{Tr}(a)/p}$, where $\mathrm{Tr}(a)$ is the trace of a over the base field $\mathbb{F}_p$.

For more details about **characters** see [1].

Gauss Sums

A Gauss sum is a fundamental object in number theory that encapsulates important algebraic and analytic information about **finite fields** [4].

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 properties of these sums are well studied, particularly their connection to quadratic residues, exponential sums, and character sums.

Intuition Behind Gauss Sums: The Gauss sum $G(\alpha, \psi)$ can be thought of as a weighted sum that combines the structure of the multiplicative group of the field (via α) with the additive group (via ψ). The interplay between these two characters encapsulates deep algebraic and analytic information about the field. For example:

- Gauss sums generalize the classical exponential sums studied in modular arithmetic.
- They are closely tied to quadratic residues and have applications in solving polynomial equations over finite fields.
- The absolute value of a Gauss sum is directly related to the size of the field: $|G(\alpha, \psi)| = \sqrt{q}$, a result that is crucial in understanding their properties.

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 [2, Theorem 1.2].

Theorem 0.1 (Converse Theorem of Gauss Sums)**.** *Consider two multiplicative characters α_1 and α_2 defined on the multiplicative group of a finite field $\mathbb{F}_{q^m}^\times$. If for all additive characters ψ on $\mathbb{F}_{q^m}$ and all multiplicative characters θ on $\mathbb{F}_{q^m}^\times$, the following equality holds:*

$$G(\alpha_1 \times \theta, \psi) = G(\alpha_2 \times \theta, \psi), \tag{3}$$

$$\sum_{a \in \mathbb{F}_{q^m}^\times} \alpha_1(a)\theta(a)\psi(a) = \sum_{a \in \mathbb{F}_{q^m}^\times} \alpha_2(a)\theta(a)\psi(a), \tag{4}$$

then it must be the case that α_1 and α_2 are identical, or at least related by a well-understood transformation.

Intuitively, this theorem tells us that Gauss sums contain enough information to uniquely determine a character. However, recent work by **Bakeberg, Gerbelli-Gauthier, Goodson, Iyengar, Moss, and Zhang** has discovered counterexamples when $n = 2$, meaning there exist distinct characters $\alpha_1 \neq \alpha_2$ that still satisfy the above equation [5]. This suggests that the theorem may not hold in general, raising new questions about when and why such failures occur. Our project aims to analyze these counterexamples and determine whether they extend to higher dimensions. Understanding these failures could lead to improvements in our knowledge of Gauss sums and their applications in number theory.

Research Objectives (Paragraph form)

- Reproducing prior counterexamples for $n = 2$ and verifying their correctness.
- Investigating whether these failures generalize to larger values of n.
- Formulating a refined conjecture regarding the conditions under which the theorem holds or fails.
- Exploring computational methods using SageMath to generate and analyze new examples.

Motivation for Studying This Problem

Understanding the failure of the converse theorem of Gauss sums provides insight into deeper algebraic structures underlying finite fields. Our motivation for studying this problem stems from its connections to modular forms, coding theory, and cryptography. Identifying where the theorem breaks down allows for refinements in theoretical frameworks and potential applications in constructing error-correcting codes and cryptographic schemes.

References

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

[2] 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`.

[3] 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`.

[4] 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`.

[5] Elad Zelingher. "Failure of Converse Theorems of Gauss Sums Modulo ℓ". preprint, available from a webpage, https://lsa.umich.edu/content/dam/math-assets/logm/wn2025/ELAD-ZELINGHER.pdf. 2025.