QUADRATIC RECIPROCITY AND GAUSS SUMS

TRISTAN SHIN

Abstract. In this expository paper, we discuss the background and proof of quadratic reciprocity using Gauss sums. Reciprocity laws are important results in algebraic number theory, and understanding the application of Gauss sums is an important step in the process. We introduce these sums and related objects through the discrete Fourier transform and demonstrate how the computation of Gauss sums can be used to access quadratic reciprocity.

1. Introduction

An important question in elementary number theory is to determine when an integer is congruent to a perfect square modulo a prime. The quadratic reciprocity law, along with its supplements, essentially resolves this question by providing an easily computable method to make this determination. In this expository paper, we will discuss the theory of quadratic reciprocity as well as some related ideas.

Definition 1.1. Let m and n be integers with n positive. We say that m is a **quadratic residue** modulo n if there exists an integer x for which $x^2 \equiv m \pmod{n}$. We say that m is a **quadratic nonresidue** modulo n if there is no such x (i.e. m is not a quadratic residue).

To keep track of quadratic residues modulo an odd prime p, we have the Legendre symbol.

Definition 1.2. The **Legendre symbol** $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p \to \mathbb{C}$ is defined to be

$$\left(\frac{a}{p}\right) \coloneqq \begin{cases} 1 & \text{if } a \text{ is a nonzero quadratic residue mod } p; \\ -1 & \text{if } a \text{ is a quadratic nonresidue mod } p; \\ 0 & \text{if } a = 0. \end{cases}$$

It is straightforward to check the following fact (e.g. using factorization over $\mathbb{F}_p[X]$).

Proposition 1.3 (Euler's criterion)**.** *We have that* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

This immediately implies that the Legendre symbol is multiplicative. Additionally when $a = -1$, both sides of the congruence are in $\{\pm 1\}$ and equality actually holds.

Corollary 1.4. *We have that* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

We can now state the main theorem.

Theorem 1.5 (Quadratic reciprocity)**.** *If p and q are distinct odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Equivalently, we have that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ *if and only if* p *and* q *are not both* $3 \bmod 4$.

There are many known proofs of quadratic reciprocity in the literature, including eight given by Gauss. The most common proof involves a counting argument on a grid that is mostly symmetrical in the variables p and q (see Chapter 5 of [AZ10]). In this paper, we focus instead on a more algebraic proof that requires breaking the symmetry in the theorem. This will be done through the quadratic Gauss sum which encodes important information about the Legendre symbol into an exponential sum. The Gauss sum appears as an important object in many parts of number theory beyond the discussion of quadratic residues, but we primarily concern ourselves with the relevant properties involved in quadratic reciprocity.

This paper is split into several sections. In Section 2, we introduce preliminaries of the discrete Fourier transform. In Section 3, we define the Gauss and Jacobi sums, then evaluate important properties of the Gauss sum. In Section 4, we prove the quadratic reciprocity law using Gauss sums. Then we discuss supplements to the theorem and how to apply it. In Section 5, we discuss the general implications of the framework that we have used to prove quadratic reciprocity, particularly in the context of higher order reciprocity laws. The presentation of quadratic reciprocity roughly follows and generalizes that of Terras in Chapter 8 of [Ter99].

1.1. **Acknowledgements.** The author would like to thank Minh-Tâm Trinh for providing resources and guidance throughout the process of writing this paper, as well as suggesting the topic. The author would also like to thank Alan Peng for providing useful feedback in peer review. This paper was written as part of MIT's Undergraduate Seminar in Algebra (18.704).

2. Discrete Fourier transform

A key tool in the study of Gauss sums is the discrete Fourier transform over a cyclic group $\mathbb{Z}/n\mathbb{Z}$ for $n > 1$. We present a brief introduction which will allow us to use it to analyze functions. Let $\zeta_n = e^{\frac{2\pi i}{n}}$.

Definition 2.1. The **discrete Fourier transform** of a function $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ is $\hat{f}\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ given by

$$\hat{f}(r) \coloneqq \sum_{a \in \mathbb{Z}/n\mathbb{Z}} f(r)\zeta_n^{-ar}.$$

The definition lends its way to a few basic properties.

Proposition 2.2. *The discrete Fourier transform satisfies the following properties:*

- *(linearity) The map* $f \mapsto \hat{f}$ *is a linear operator on the space of functions from* $\mathbb{Z}/n\mathbb{Z}$ *to* $\mathbb{C}$.
- *(negation of parameter) If* $g(x) = f(-x)$, *then* $\hat{g}(r) = \hat{f}(-r)$.
- *(conjugation) We have that* $\overline{\hat{f}}(r) = \hat{\overline{f}}(-r)$.

2.1. **Theory of the discrete Fourier transform.** One main motivating force behind Fourier analysis is that it provides the theory of exponential functions as a basis for the space of functions. Indeed, the following theorem formalizes this for discrete Fourier analysis.

Theorem 2.3 (Fourier inversion)**.** *For any $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$, we have that*

$$f(a) = \frac{1}{n} \sum_{r \in \mathbb{Z}/n\mathbb{Z}} \hat{f}(r)\zeta_n^{ar} = \frac{1}{n}\hat{\hat{f}}(-a).$$

The Fourier transform also provides a useful way to analyze an alternate form of multiplication.

Definition 2.4. The **convolution** of two functions $f, g\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ is $f*g\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ given by

$$(f * g)(a) \coloneqq \sum_{\substack{b+c=a \\ b,c \in \mathbb{Z}/n\mathbb{Z}}} f(b)g(c) = \sum_{b \in \mathbb{Z}/n\mathbb{Z}} f(b)g(a-b).$$

Proposition 2.5. *For any $f, g\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$, we have that $\widehat{f * g} = \hat{f} \cdot \hat{g}$.*

Remark 2.6. Of course, we can iterate convolution and Proposition 2.5 to more functions. It is straightforward to check that convolution is associative and that the Fourier transform of $f * g * h$ is the product of the Fourier transforms $\hat{f}$, $\hat{g}$, and $\hat{h}$. This can be extended for the case of even more functions. Because convolution is associative, we can write f^{*k} to denote the k-fold convolution $f * f * \cdots * f$ (also known as the convolution power).

The discrete Fourier transform also satisfies many more properties besides these with additional theory behind it. For a more complete picture of the Fourier transform as well as proofs of the above properties, we defer the reader to Chapter 2 of [Ter99].

3. Gauss sums

In this section, we discuss the Gauss sums of Dirichlet characters modulo an integer $n > 1$. This is a more general overview of Gauss sums than we will need, but allows for study of other related objects.

3.1. Dirichlet characters.

The study of Gauss sums concerns a specific class of characters, the Dirichlet characters.

Definition 3.1. We say that $\chi\colon \mathbb{Z} \to \mathbb{C}$ is a **Dirichlet character modulo** n if for all integers a and b,

- (multiplicative) $\chi(ab) = \chi(a)\chi(b)$;
- (periodic) $\chi(a+n) = \chi(a)$; and
- $\chi(a) = 0$ if and only if $\gcd(a, n) \neq 1$.

Euler's theorem (equivalently Lagrange's theorem for multiplicative groups of integers) implies that the values of χ are actually quite constrained.

Proposition 3.2. *If $\gcd(a, n) = 1$, then $\chi(a)$ is a $\varphi(n)$-th root of unity.*

Example 3.3. The most basic example of a Dirichlet character modulo n is the trivial character:

$$\chi_0(a) \coloneqq \begin{cases} 1 & \text{if } \gcd(a, n) = 1; \\ 0 & \text{if otherwise.} \end{cases}$$

Example 3.4. The Legendre symbol, extended to the domain $\mathbb{Z}$ by applying the "mod p" map, is a Dirichlet character modulo p. This follows from Euler's criterion.

We can also go in the other direction — that is, we can treat a Dirichlet character as a function $\chi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$. When we consider the entire set of Dirichlet characters modulo a fixed n, we have additional structure which can be proven by applying the definitions.

Proposition 3.5. *Fix an integer $n > 1$. The set of Dirichlet characters modulo n forms a group under multiplication with identity χ_0 and inverse map $\chi \mapsto \overline{\chi}$. This group is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.*

In the case that the modulus is prime, we have useful results involving the Fourier transform.

Proposition 3.6. *Let χ be a nontrivial Dirichlet character modulo some prime p. Then $\hat{\chi}(r) = \overline{\chi}(-r)\hat{\chi}(-1)$.*

Proof. We first deal with the case that $r \in (\mathbb{Z}/p\mathbb{Z})^\times$. We can directly compute the Fourier transform $\hat{\chi}(r)$ as

$$\sum_{a\in\mathbb{Z}/p\mathbb{Z}} \chi(a)\zeta_p^{-ar} \overset{b=-ar}{=} \sum_{b\in\mathbb{Z}/p\mathbb{Z}} \chi(-br^{-1})\zeta_p^b = \chi(-r)^{-1} \sum_{b\in\mathbb{Z}/p\mathbb{Z}} \chi(b)\zeta_p^b$$

which simplifies to the desired expression.

Now, we settle the $r = 0$ case. Let $c \in \mathbb{Z}/p\mathbb{Z}$ such that $\gcd(c, p) = 1$ and $\chi(c) \neq 1$ (possible because χ is nontrivial). Then

$$\chi(c)\hat{\chi}(0) = \chi(c) \sum_{a\in\mathbb{Z}/p\mathbb{Z}} \chi(a) = \sum_{a\in\mathbb{Z}/p\mathbb{Z}} \chi(ca) \overset{b=ca}{=} \sum_{b\in\mathbb{Z}/p\mathbb{Z}} \chi(b) = \hat{\chi}(0)$$

from which it follows that $\hat{\chi}(0) = 0$. □

Remark 3.7. The statement still holds when the modulus is not prime and the input is relatively prime to the modulus, with identical proof. When the input is not relatively prime, things get more complicated and the same proof does not work.

3.2. **Gauss sum.** The formula for the Fourier transform of a Dirichlet character motivates the following definition.

Definition 3.8. The **Gauss sum** of a Dirichlet character χ is $g(\chi) \coloneqq \hat{\chi}(-1)$.

While computing the Gauss sum is hard in general, we can evaluate some properties with ease.

Proposition 3.9. *Let χ be a nontrivial Dirichlet character modulo some prime p. Then $g(\chi)g(\overline{\chi}) = \chi(-1)p$ and $|g(\chi)| = \sqrt{p}$.*

Proof. The Fourier transform of Proposition 3.6 gives that $\hat{\hat{\chi}}(a) = \widehat{\overline{\chi}}(-a)\hat{\chi}(-1)$. Applying inversion gives that $\chi(-a) = \frac{1}{p}\hat{\hat{\chi}}(a)$. Combining these at $a = 1$ results in the first equality. But $\widehat{\overline{\chi}}(-a) = \overline{\hat{\chi}(a)}$, so combining the two equations at $a = -1$ results in the second equality. □

3.3. **Quadratic Gauss sum.** We can simplify Proposition 3.6 in the case of the Legendre symbol for an odd prime p because all values of the symbol are real. Let $h_p(a) \coloneqq \left(\frac{a}{p}\right)$ be the character and $g_p \coloneqq g(h_p)$ be the quadratic Gauss sum.

Corollary 3.10. *We have that* $\widehat{h_p}(r) = \left(\frac{-r}{p}\right) g_p$.

Remark 3.11. Because $\left(\frac{-r}{p}\right) = h_p(r)\left(\frac{-1}{p}\right)$, this implies that the Legendre symbol and its Fourier transform are proportional to each other. Additionally, with $r = 0$ this recovers the fact that there are equally many nonzero quadratic residues as quadratic nonresidues (which also follows from Euler's criterion).

Similarly, Proposition 3.9 can be simplified for h_p. For notational purposes, let $p^* = (-1)^{\frac{p-1}{2}} p \in \mathbb{Z}$.

Corollary 3.12. *We have that* $g_p^2 = p^*$.

A natural follow-up question is to determine the sign of the quadratic Gauss sum, i.e. compute the value of g_p. For arbitrary Dirichlet characters, this problem is not easily resolvable. But here, Gauss evaluated this sum.

Proposition 3.13. *We have that*

$$g_p = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4; \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

This can be proven by looking at the matrices of the Fourier transform with respect to multiple bases of the space of functions from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{C}$. For a full proof, see Chapter 8 of [Ter99].

3.4. **Jacobi sum.** The Jacobi sum is a closely related object to the Gauss sum.

Definition 3.14. Let χ_1, χ_2 be Dirichlet characters modulo some prime p. The **Jacobi sum** of the characters is $J(\chi_1, \chi_2) \coloneqq (\chi_1 * \chi_2)(1)$.

Proposition 3.15. *Let* χ_1, χ_2 *be Dirichlet characters modulo some prime* p *such that* $\chi_1\chi_2$ *is nontrivial. Then* $J(\chi_1, \chi_2) = \frac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)}$.

We prove the following more general proposition about an iterated Jacobi sum.

Proposition 3.16. *Let* $\chi_1, \ldots, \chi_k$ *be Dirichlet characters modulo some prime* p *such that* $\chi_1 \cdots \chi_k$ *is nontrivial. Then*

$$(\chi_1 * \cdots * \chi_k)(1) = \frac{g(\chi_1) \cdots g(\chi_k)}{g(\chi_1 \cdots \chi_k)}.$$

Proof. For notational purposes, let $C = \chi_1 * \cdots * \chi_k$. Observe that

$$g(\chi_1) \cdots g(\chi_k) = \widehat{\chi_1}(-1) \cdots \widehat{\chi_k}(-1) = \widehat{C}(-1).$$

But $C(a) = \chi_1(a) \cdots \chi_k(a) C(1)$ because

$$\sum_{a_1 + \cdots + a_k = a} \chi_1(a_1) \cdots \chi_k(a_k) \overset{a_i' = a_i/a}{=} \chi_1(a) \cdots \chi_k(a) \sum_{a_1' + \cdots + a_k' = 1} \chi_1(a_1') \cdots \chi_k(a_k'),$$

so

$$g(\chi_1)\cdots g(\chi_k) = \sum_{a\in\mathbb{Z}/p\mathbb{Z}} C(a)\zeta_p^a = \sum_{a\in\mathbb{Z}/p\mathbb{Z}} \chi_1(a)\cdots\chi_k(a)C(1)\zeta_p^a.$$

We can pull out a factor of $C(1)$ and divide by $g(\chi_1\cdots\chi_k)$ to finish because Proposition 3.9 implies that the Gauss sum of a nontrivial Dirichlet character is nonzero. □

By applying Proposition 3.16 to a fixed Dirichlet character χ and requiring $\chi^k = \chi$, we have the following result.

Corollary 3.17. *Let χ be a nontrivial Dirichlet character modulo some prime p, and k be a positive integer such that the order of χ (as an element of the group of Dirichlet characters) divides $k-1$. Then $\chi^{*k}(1) = g(\chi)^{k-1}$.*

3.5. **Similarities to gamma function.** The Gauss and Jacobi sums bear similarities to the gamma and beta functions in analysis and integration. The **gamma function** is defined on the right half-plane to be

$$\Gamma(z) \coloneqq \int_0^\infty t^{z-1}e^{-t}\,\mathrm{d}t$$

while the **beta function** for x, y on the right half-plane is defined to be

$$B(x,y) \coloneqq \int_0^1 t^{x-1}(1-t)^{y-1}\,\mathrm{d}t.$$

Already in the definitions we can see similarities — with appropriate choice of differential and basis, the gamma function can be interpreted as a coefficient of t^z and the beta function as a unit convolution of t^x and t^y. We also have the well-known formula that $B(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}$, which can be proven in precisely the same way as our proof of Proposition 3.15. Furthermore, Proposition 3.9 can be interpreted as a reflection formula, similar to Euler's reflection formula which states that $\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}$. Refer to Table 1 for a concise comparison between Gauss sums and Gamma functions.

Object	Gauss sum	Gamma function
Exp. sum/integral	$g(\chi)$	$\Gamma(z)$
Unit convolution	$J(\chi_1,\chi_2)$	$B(x,y)$
Evaluation	$J = \frac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)}$	$B = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}$
Reflection	$g(\chi)g(\overline{\chi}) = \chi(-1)p$	$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}$

Table 1. Counterparts between Gauss sums and Gamma functions.

4. Quadratic reciprocity

In this section, we prove the quadratic reciprocity law using the discrete Fourier transform and Gauss sums. We provide two similar proofs, the first of which relies more on the Fourier transform while the second is more algebraic in nature. We also provide supplements which allow for easy computation of quadratic residues.

4.1. **Proof of quadratic reciprocity.** This proof takes advantage of the iterated Jacobi sum to evaluate $g_p^{q-1} \bmod q$ in two ways — first by expanding the iterated Jacobi sum, then by using the previously computed value of g_p^2. This proof is modified from a proof given by Rademacher in [Rad64].

Proof of Theorem 1.5. The order of h_p as a Dirichlet character is 2, so we can combine Corollary 3.17 at $k = q$ with Corollary 3.12 to get that $h_p^{*q}(1) = (p^*)^{\frac{q-1}{2}}$. The left hand side is

$$h_p^{*q}(1) = \sum_{a_1+a_2+\cdots+a_q=1} \left(\frac{a_1 a_2 \cdots a_q}{p}\right) = \left(\frac{q^{-q}}{p}\right) + \sum_{\substack{a_1+a_2+\cdots+a_q=1 \\ a_i \text{ not constant}}} \left(\frac{a_1 a_2 \cdots a_q}{p}\right).$$

The indices of this last sum can be grouped into collections of $(a_1, a_2, \ldots, a_q)$ and its cyclic shifts[1]. Each collection corresponds to q identical summands, so the total sum is 0 mod q. Consequently, $h_p^{*q}(1) \equiv \left(\frac{q^{-q}}{p}\right) \equiv \left(\frac{q}{p}\right) \pmod q$.

We also have that the right hand side is $(p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \pmod q$ by Euler's criterion. It follows that $\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \pmod q$. But both sides of this congruence are in $\{\pm 1\}$, so they must be equal. Rearranging terms gives us the statement of quadratic reciprocity. □

Let us review the ingredients of this proof. We do not use much more than the facts developed in Section 3. The steps required are:

(1) Compute the Fourier transform of a Dirichlet character (Proposition 3.6).
(2) Compute the reflection formula for Gauss sums (Proposition 3.9).
(3) Compute the iterated Jacobi sum (Proposition 3.16).
(4) Interpret the above results for the Legendre symbol.
(5) Combine an elementary counting argument (cyclic shifts) with an elementary number theoretical argument (Euler's criterion) to finish.

It is stunning how simply the result falls out once we have applied our Fourier toolbox to the problem.

4.2. **Another proof of quadratic reciprocity.** Once again, we compute a power of $g_p \bmod q$ in two ways — first by evaluating the q-th power of the Fourier definition of g_p, then by using the previously computed value of g_p^2. Many parts of this proof correspond to parts of the previous proof, but computed algebraically. This proof is closer in nature to Gauss's original application of his namesake sums.

Proof of Theorem 1.5. Work in $\mathbb{Z}[\zeta_p]$. Observe that

$$g_p^q = (\widehat{h_p}(-1))^q = \left(\sum_{a=0}^{p-1} h_p(a)\zeta_p^a\right)^q \equiv \sum_{a=0}^{p-1} \left(h_p(a)\zeta_p^a\right)^q \pmod q$$

by properties of the Frobenius endomorphism. But $h_p(a)^q = h_p(a)$ because q is odd, so the right hand side just turns into $\widehat{h_p}(-q)$. But Corollary 3.10 implies that $\widehat{h_p}(-q) = \left(\frac{q}{p}\right) g_p$, so $g_p^q \equiv \left(\frac{q}{p}\right) g_p \pmod q$.

[1] This idea is perhaps more commonly used in the classic "necklace" proof of Fermat's little theorem, given by Golomb (see [Gol56]).

At this point, it might be tempting to divide by g_p. However, the ring $\mathbb{Z}[\zeta_p]/(q)$ is not necessarily an integral domain, so we cannot divide[2]. Instead, we multiply by g_p to get that $g_p^{q+1} \equiv \left(\frac{q}{p}\right) g_p^2 \pmod{q}$.

Now, combine Corollary 3.12 for p with Euler's criterion for q to deduce that $g_p^{q-1} \equiv \left(\frac{p^*}{q}\right) \pmod{q}$. Combining this with the previous paragraph and Corollary 3.12 gives that $p^* \left(\frac{p^*}{q}\right) \equiv p^* \left(\frac{q}{p}\right) \pmod{q}$ over $\mathbb{Z}[\zeta_p]$. Both sides of this equation are in $\mathbb{Z}$, so we can treat this as a congruence modulo q over $\mathbb{Z}$ and divide out by p^* (which is not divisible by q) to get that $\left(\frac{p^*}{q}\right) \equiv \left(\frac{q}{p}\right) \pmod{q}$. We can finish as in the previous proof. □

4.3. **Supplements.** To complete the picture of quadratic residues, we must deal with negative numbers and even numbers. For negative numbers, Corollary 1.4 gives us a handle already. All that remains is the even prime 2.

Proposition 4.1. *We have that* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Proof. Work in $\mathbb{Z}[\zeta_8]$, and let $y = \zeta_8 + \zeta_8^{-1}$ so that $y^2 = 2$.

If $p \equiv \pm 1 \pmod 8$, then $y^p \equiv \zeta_8^p + \zeta_8^{-p} \pmod p$. But $\{\zeta_8^p, \zeta_8^{-p}\} = \{\zeta_8, \zeta_8^{-1}\}$ so $\zeta_8^p + \zeta_8^{-p} = \zeta_8 + \zeta_8^{-1} = y$ and hence $y^p \equiv y \pmod p$. As before, we cannot divide by y, but multiplying by y again does the trick because Euler's criterion implies that $y^{p-1} \equiv \left(\frac{2}{p}\right) \pmod p$ so $\left(\frac{2}{p}\right) = 1$.

In the case that $p \equiv \pm 3 \pmod 8$, then everything is the same except $\{\zeta_8^p, \zeta_8^{-p}\} = \{-\zeta_8, -\zeta_8^{-1}\}$. As a result, all signs thereafter get flipped so $\left(\frac{2}{p}\right) = -1$. □

This gives us enough information to compute any Legendre symbol.

Example 4.2. To determine if 167 is a quadratic residue modulo 101, we can do the following sequence of computations:

$$\begin{aligned}\left(\frac{167}{101}\right) = \left(\frac{66}{101}\right) &= \left(\frac{2}{101}\right)\left(\frac{3}{101}\right)\left(\frac{11}{101}\right) = (-1)\left(\frac{101}{3}\right)\left(\frac{101}{11}\right) \\ &= (-1)\left(\frac{2}{3}\right)\left(\frac{2}{11}\right) = (-1)(-1)(-1) \\ &= -1.\end{aligned}$$

So no, 167 is not a quadratic residue modulo 101.

4.4. **Jacobi symbol.** To make computations easier, we can consolidate information into a single symbol.

Definition 4.3. Let n be an odd positive integer, and write $n = p_1 p_2 \cdots p_k$ for (not necessarily distinct) odd primes $p_1, p_2, \ldots, p_k$. The **Jacobi symbol** $\left(\frac{\cdot}{n}\right) : \mathbb{Z} \to \mathbb{C}$ is defined to be

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right).$$

We can directly check that the Jacobi symbol inherits many properties from the Legendre symbol. The proofs of these properties follow from building up an integer prime-by-prime.

[2]One can work around this issue by setting up a different proof over $\mathbb{F}_q[\zeta_p]$, but this has other subtleties to deal with.

Proposition 4.4. *The following hold:*

(1) $\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right)$
(2) $\left(\frac{a}{bc}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{c}\right)$
(3) *If* $a \equiv b \pmod{c}$, *then* $\left(\frac{a}{c}\right) = \left(\frac{b}{c}\right)$.
(4) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$
(5) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$
(6) *If* m, n *are odd and relatively prime, then* $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$.

If we try the computation in Example 4.2 now, we will find ourselves doing much less work.

Example 4.5. To determine if 167 is a quadratic residue modulo 101, we can do the following (simpler) sequence of computations:

$$\begin{aligned}\left(\frac{167}{101}\right) = \left(\frac{66}{101}\right) &= \left(\frac{2}{101}\right)\left(\frac{33}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{101}{33}\right) \\ &= \left(\frac{2}{101}\right)\left(\frac{2}{33}\right) = \left(\frac{2}{3333}\right) \\ &= -1.\end{aligned}$$

Note that we took a shortcut in going from 101 and 33 to 3333; it will not always be the case that we can combine "denominators."

Remark 4.6. Unlike the Legendre symbol, the Jacobi symbol does not strictly correspond to quadratic residues. On one hand, it is easy to check that if $\gcd(a, n) = 1$ and a is a quadratic residue modulo n, then $\left(\frac{a}{n}\right) = 1$. But on the other hand, there are examples such as $\left(\frac{2}{15}\right) = 1$ where 2 is a quadratic nonresidue modulo 15.

5. Concluding remarks

The proof of quadratic reciprocity begs the question of how to generalize to higher orders. For the simplest example, we can look at cubic reciprocity. The proper setting in which we can apply the Gauss sum for cubic residues is no longer the integers, but rather the Eisenstein integers $\mathbb{Z}[\zeta_3]$. This ring is a unique factorization domain, which allows us to discuss primes and factorization. A number-theoretical argument similar to that in the integers allows us to state that for any α relatively prime to a prime π in $\mathbb{Z}[\zeta_3]$, there exists a third root of unity ω_α such that $\alpha^{\frac{N(\pi)-1}{3}} \equiv \omega_\alpha \pmod{\pi}$, where $N(a + b\zeta_3) = a^2 - ab + b^2$ is the Eisenstein norm.

Definition 5.1. The **cubic residue character** $\left(\frac{\cdot}{\pi}\right)_3 : \mathbb{Z}[\zeta_3]/(\pi) \to \mathbb{C}$ is defined to be

$$\left(\frac{\alpha}{\pi}\right)_3 := \begin{cases} \omega_\alpha & \text{if } \alpha \neq 0; \\ 0 & \text{if } \alpha = 0. \end{cases}$$

The statement of cubic reciprocity requires some additional distinction among primes.

Definition 5.2. We say that a prime $\pi \in \mathbb{Z}[\zeta_3]$ is **primary** if $\pi \equiv 2 \pmod{3}$.

Theorem 5.3 (Cubic reciprocity)**.** *If π_1 and π_2 are distinct primary primes relatively prime to 3, then*

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3.$$

Much of the work done to apply Gauss sums and Jacobi sums to quadratic reciprocity is useful in the proof of cubic reciprocity. Only a little more computation is needed outside of what we have already presented. Recall that our proofs of quadratic reciprocity relied heavily on the computation of the square of the quadratic Gauss sum. Cubic reciprocity relies on computing the cube of the cubic Gauss sum, which is defined analogously to the quadratic Gauss sum but for the cubic residue character. For a complete discussion, see Chapter 7 of [Lem00].

We can go further and generalize to even higher orders. The celebrated Eisenstein reciprocity theorem is a direct generalization of cubic reciprocity and once again relies on the computation of the m-th power of the m-th power Gauss sum. This computation is known as the Stickelberger relation. More about these higher order reciprocity laws can be found in Chapter 14 of [IR90].

The importance of reciprocity laws, beginning with quadratic reciprocity and going even beyond Eisenstein reciprocity, cannot be overstated. They provide important information about the structure of the ring of integers in cyclotomic fields and contribute heavily to the field of algebraic number theory. Central to these theorems is the Gauss sum defined and interpreted through the lens of the discrete Fourier transform, as we have demonstrated. Though the scope of reciprocity laws extend far beyond elementary number theory, we can gain a glimpse into this vast world with the study of quadratic reciprocity.

References

[AZ10] M. Aigner and G. Ziegler. *Proofs from THE BOOK*, fourth edition. Springer-Verlag (2010).

[Gol56] S. W. Golomb. Classroom Notes: Combinatorial Proof of Fermat's "Little" Theorem. *Amer. Math. Monthly*, **63** (Dec., 1956), 718.

[IR90] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, second edition. Springer-Verlag (1990).

[Lem00] F. Lemmermeyer. *Reciprocity laws*. Springer-Verlag (2000).

[Rad64] H. Rademacher. *Lectures on elementary number theory*. Blaisdell Publishing Co. (1964).

[Ter99] A. Terras. *Fourier Analysis on Finite Groups and Applications*. Cambridge University Press (1999).

Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139