PROOFS AND APPLICATIONS OF QUADRATIC RECIPROCITY

MATIAS RELYEA

Abstract. As one of the most important theorems in Elementary Number Theory, the Law of Quadratic Reciprocity is both incredibly beautiful and rewarding to explore. In this paper, we will explore characteristics of quadratic residues and quadratic nonresidues, and apply them to varying conditions on primes. After that, we will illustrate and prove a statement of equivalence of the Law of Quadratic Reciprocity using an assertion by Euler. Following this, we offer three unique proofs of the Law of Quadratic Reciprocity using Eisenstein's Lemma and lattice-point counting, primitive nth roots of unity, and Quadratic Gauss Sums. Finally, we give a brief introduction to a generalization of the Legendre Symbol known as the Jacobi Symbol, and then prove Fermat's Theorem on the Sum of two Squares using the Law of Quadratic Reciprocity and the Method of Infinite Descent.

Contents

Introduction 2
0. Preliminaries 3
1. An Equivalence and Application of Quadratic Reciprocity 9
1.1. Application 9
1.2. Proof of Equivalence 11
2. Quadratic Reciprocity and a Lattice Point Construction by Eisenstein 14
2.1. Gauss' Lemma 14
2.2. Quadratic Character of 2 modulo p by Gauss' Lemma 17
2.3. Eisenstein's Lemma 18
2.4. Proof 20
3. Quadratic Reciprocity and Primitive nth Roots of Unity 22
3.1. Preliminaries 23
3.2. Proof 26
4. Quadratic Reciprocity and Quadratic Gauss Sums 27
4.1. Some algebra 27
4.2. Quadratic Character of 2 modulo p using primitive 8th roots of unity 29
4.3. Quadratic Gauss Sums 31
4.4. Proof 36
5. Applications 38
5.1. Jacobi Symbol 38

Date: Summer 2022.

5.2. Fermat's Theorem on the Sum of Two Squares 41
Acknowledgements 44
References 44

Introduction

Number Theory, in its innate beauty, lies in its imaginative absurdness, yet also in its spontaneous ingenuity. The Law of Quadratic Reciprocity, when stated and proven by Carl Friedric Gauss, was a revolutionary theorem; in Gauss' words, it was the "Aureum Theorema", or the "Golden Theorem" of Number Theory. What may have made this theorem so significant to Gauss?

Until Gauss' death on the 23rd of February, 1855, he had proven the Law of Quadratic Reciprocity 8 times. Of his numerous proofs, the first and second - the first being one by induction, and the second by composition of forms - were published together in 1801 in his now renowned *Disquisitiones Arithmeticae*, an ingenious textbook containing a large amount of material, ranging from the very foundations of Number Theory to what we now call Genus Theory. In the final sections, Gauss developed Class Field Theory and Genus Theory, both of which he applied to higher reciprocity (namely, the use of higher powers in the nth degree congruence $x^n \equiv A \pmod{p}$, where $n \in \mathbb{Z}^+$), and thereby provided rigorous proofs for Cubic and Biquadratic (quartic) reciprocity.

Throughout his lifetime and after his death in 1855, countless mathematicians until the present have contributed significantly to the area of reciprocity laws. These include the Swiss polymath Leonhard Euler, who contributed significantly to the discovery and foundation of Quadratic Reciprocity, the French mathematician Adrien-Marie Legendre, who devised effective notation for the Legendre Symbol, a notation that is useful for expressing whether an integer a is a quadratic residue or nonresidue modulo p, and the Austrian mathematician Emil Artin, who, in a series of papers in 1924, 1927, and 1930, derived the general premise of Artin Reciprocity, which is a generalized reciprocity law. Above I have only named three, but countless more mathematicians have considered reciprocity laws, and have made contributions ranging in significance of contribution from small to field-revolutionizing.

However, in this paper, we will only consider the Law of Quadratic Reciprocity and will not explore higher reciprocity, as it lies beyond the scope of the purpose of this essay. As of now, 334 proofs of Quadratic Reciprocity have been devised, ranging from the usage of Finite Field extensions to the use of Quadratic Gauss Sums. Each proof is unique, yet many share subtle similarities. In this paper, as the dear reader can gather from the abstract, we will be presenting a beautiful proof of equivalence of Quadratic Reciprocity to another statement due to Euler, as well as three other proofs: namely a subtle yet elegant proof due to Eisenstein, which utilizes the ideas of lattice point counting; another proof also due to Eisenstein, using primitive nth roots of unity; and finally a proof using Quadratic Gauss Sums.

The first proof of equivalence is rather elementary, yet uses several rather logically complex arguments to prove the equivalence of the statement of Quadratic Reciprocity

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

(where p and q are distinct odd primes) to the statement that

$$\text{if } p \text{ and } q \text{ are distinct odd primes, } a \geq 1 \text{ is any integer}$$
$$\text{such that } p \nmid a, \text{ and } p \equiv \pm q \pmod{4a}, \text{ then } \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

The second proof that we consider is by using lattice point counting, and uses the creation of two relatively reoriented triangles to form the sum of lattice points strictly bounded within them, and utilizes Gauss' Lemma to finalize the result and thereby prove Quadratic Reciprocity.

The third proof we will explore is one using primitive nth roots of unity, and as we will see later, many facts about complex numbers and complex functions will be used.

Finally, we prove Quadratic Reciprocity by using Quadratic Gauss Sums. This, in its entirety, is one of the most crucial proofs, at least in the context of higher reciprocity; this proof can be generalized, using the theory of Finite Fields, to cubic and biquadratic reciprocity, in the form of Gauss Sums (as I indicated before, we will not consider these in this paper, but if the dear reader is interested, [IRR90] is a wonderful place to begin).

More about Genus Theory and its numerous applications, as well as a rigorous yet non-unambitious treatment of the Artin Reciprocity law alongside its applications and formulations can be found in [Cox11]. Finally, as a rigorous yet beautiful introduction to working number theory and its numerous details, [Sil14] is an informative place to begin.

For a group-theoretic proof of Quadratic Reciprocity and more details on Fermat's Theorem on the Sum of Two Squares, [Alm19] is a good place to begin.

0. Preliminaries

Before we may begin to explore proofs of the Law of Quadratic Reciprocity, we must become somewhat familiar with several preliminaries. Here we will introduce the notion of a quadratic residue and quadratic nonresidue, two objects that will be the central focus of study in this first section, as well as throughout the rest of the paper. After a brief introduction to quadratic residues and nonresidues, we will continue by defining and proving several properties of the Legendre Symbol, which is a useful object when studying quadratic characters modulo p a prime. Finally, we will conclude the section with an introduction to the Law of Quadratic

Reciprocity, as well as a demonstration of its uses for computing various quadratic characters modulo p.

The quadratic congruences that we will study in the majority of this paper will be of the form $x^2 \equiv a \pmod{p}$, where p is a prime.

Definition 0.1. Let $\gcd(a, p) = 1$. An integer a is called a *quadratic residue modulo* p if there exists a solution to the quadratic congruence $x^2 \equiv a \pmod{p}$, and is called a *quadratic nonresidue modulo* p otherwise.

Let $p = 3$. Then the congruence $x^2 \equiv a \pmod{3}$ has three possible values for a. The residues modulo 3 of this congruence are contained within the set {0,1,2}, so we will consider these values for a. Squaring each residue, we have $0^2 = 0$, $1^2 = 1$, and $2^2 = 4 \equiv 1 \pmod{3}$. Thus the quadratic residue modulo 3 is 1 and the quadratic nonresidue is 2.

Now consider $p = 11$. Then we consider the residues $\{0, 1, 2, 3, \ldots, 10\}$ of the congruence $x^2 \equiv a \pmod{11}$. Squaring each residue, we have

$$\begin{array}{lll} 0^2 = 0 & 4^2 = 16 \equiv 5 \pmod{11} & 8^2 = 64 \equiv 9 \pmod{11} \\ 1^2 = 1 & 5^2 = 25 \equiv 3 \pmod{11} & 9^2 = 81 \equiv 4 \pmod{11} \\ 2^2 = 4 & 6^2 = 36 \equiv 3 \pmod{11} & 10^2 = 100 \equiv 1 \pmod{11} \\ 3^2 = 9 & 7^2 = 49 \equiv 5 \pmod{11}. & \end{array}$$

Thus the quadratic residues are $1, 3, 4, 5, 9$, and the quadratic nonresidues are $2, 6, 7, 8, 10$.

Now we will introduce the Legendre Symbol. The Legendre Symbol allows us to denote whether an integer a is a quadratic residue or nonresidue modulo p.

Definition 0.2 (Legendre Symbol)**.** Let $\gcd(a, p) = 1$. Then the Legendre Symbol is defined as

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

For example, we can write $(\frac{3}{11}) = 1$ because 3 is a quadratic residue modulo 11, and $(\frac{6}{11}) = -1$ because 6 is a quadratic nonresidue modulo 11, as seen from above.

Notice that if $a \equiv 0 \pmod{p}$, then the Legendre Symbol is defined to be 0. This explains why 0 is neither a quadratic residue nor quadratic nonresidue modulo any prime number p. We will not provide a proof, but there is also a statement that states that it is true that there are an equal number of quadratic residues and quadratic nonresidues modulo a prime p. This can be observed when computing quadratic residues and quadratic nonresidues, and the statement will be of use later.

The numerator of the Legendre Symbol is sometimes referred to as the quadratic character modulo p prime.

Now we will prove several properties of the Legendre Symbol, many of which will be used to generalize the Legendre Symbols to the Jacobi Symbols in Section 5, and assist in the computation of the Legendre Symbol.

Proposition 0.3 (Properties of the Legendre Symbol I)**.** *Let* $\gcd(a,p) = 1$ *and* $a, b \in \mathbb{Z}$*. Then*

(a)

$$a \equiv b \pmod{p} \iff \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

(b)

$$\left(\frac{0}{p}\right) = 0$$

(c)

$$\left(\frac{a^2}{p}\right) = 1.$$

Proof. The assertion of (a) is trivial, because it follows from the definition. The numerator of the Legendre Symbol is periodic, which means that changing it does not affect the value of the symbol. Since a and b both belong to the same residue class modulo p, they are periodic, and always differ by some multiple of p. This means that when simplifying a Legendre Symbol, one can reduce the numerator modulo p.

The expression for (b) also follows from the definition, in the case of $a = 0$.

To prove (c), notice that the numerator a^2 is a square, so by definition, it must be a quadratic residue modulo p. ■

Before we may prove two more crucial properties of the Legendre Symbol, we must introduce a certain theorem, followed by a corollary to the theorem known as Wilson's Theorem.

Theorem 0.4. *For p prime,*

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-p+1) \pmod{p}.$$

Corollary 0.5 (Wilson's Theorem)**.** *For p prime,*

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. Substituting $x = 0$ in Theorem **0.4**, we have

$$\begin{aligned} 0^{p-1} - 1 &\equiv (0-1)(0-2)\cdots(0-p+1) \pmod{p} \\ -1 &\equiv (-1)(-2)\cdots(0-(p-1)) \pmod{p} \\ -1 &\equiv (p-1)! \pmod{p}. \end{aligned}$$

■

Now we proceed to prove the second theorem about properties of the Legendre Symbol.

Theorem 0.6 (Properties of the Legendre Symbol II)**.** *Let p prime,* $\gcd(a,p) = 1$*, and* $a, b \in \mathbb{Z}$*. Then*

(a)

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

(b)

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Proof. To prove (a), we consider two cases for the quadratic congruence $x^2 \equiv a \pmod{p}$: the first in which a is a quadratic residue modulo p, and the second in which a is a quadratic nonresidue modulo p. We begin with the case in which a is a quadratic nonresidue.

Case 1: Let a be a quadratic nonresidue modulo p. Also, allow some b to be in the set $\{0, 1, 2, \ldots, p-1\}$. The linear congruence $bx \equiv a \pmod{p}$ has a unique solution $x = b'$. This value b' cannot be equivalent to b because it would result in the congruence $b^2 \equiv a \pmod{p}$, which provides the condition for a to be a quadratic residue, and we are assuming that it is a quadratic nonresidue. The aforementioned set can be divided into two, such that we form exactly $\frac{p-1}{2}$ pairs (b, b') such that $bb' \equiv a \pmod{p}$. Then we can form a congruence by taking the product

$$\begin{aligned} 1 \times 2 \times \cdots \times (p-1) &\equiv a^{\frac{p-1}{2}} \pmod{p} \\ (p-1)! &\equiv a^{\frac{p-1}{2}} \pmod{p}. \end{aligned}$$

By Wilson's Theorem, this is equivalent to

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

which is the condition for a to be a quadratic nonresidue.

Case 2: Now let a be a quadratic residue. By the definition of a quadratic residue, the congruence $x^2 \equiv a \pmod{p}$ has solutions for x. Consider another solution given by y. By the Additive Property of Congruences, this is equivalent to $x^2 - y^2 \equiv a - a \pmod{p}$ and so $x^2 - y^2 \equiv 0 \pmod{p}$. We can factor so that $(x-y)(x+y) \equiv 0 \pmod{p}$ and so $x - y \equiv 0 \pmod{p}$ and $x + y \equiv 0 \pmod{p}$. Since we have these two cases, for some solution c modulo p, $-c$ is also a solution modulo p. We can remove the two solutions c and $-c + p = p - c$ from the set $\{0, 1, 2, \ldots, p-1\}$, so that this set now has cardinality $p - 3$ (It can be seen that these two solutions are distinct and are the only solutions). Split this set in two so that there are $\frac{p-3}{2}$ pairs (b, b') such that $bb' \equiv a \pmod{p}$. Then we can form a congruence by taking the product

$$\begin{aligned} 1 \times \cdots \times c \times \cdots \times (p-c) \times \cdots \times (p-1) &\equiv a \times \cdots \times a \times c \times (-c) \pmod{p} \\ (p-1)! &\equiv a^{\frac{p-3}{2}}(-c^2). \end{aligned}$$

Notice now that $-c^2 = -a$, since it is a quadratic residue modulo p, so

$$\begin{aligned} (p-1)! &\equiv a^{\frac{p-3}{2}}(-a) \pmod{p} \\ &\equiv -a^{\frac{p-1}{2}}. \end{aligned}$$

Again by Wilson's Theorem, this implies that

$$\begin{aligned} -a^{\frac{p-1}{2}} &\equiv -1 \\ a^{\frac{p-1}{2}} &\equiv 1, \end{aligned}$$

which is the condition for a quadratic residue.

Combining these two cases, we have the conditions for quadratic residues and quadratic nonresidues, so we are done.

To prove (b), substitute ab for a in (a), so that we have

$$\begin{aligned} \left(\frac{ab}{p}\right) &\equiv (ab)^{\frac{p-1}{2}} \pmod{p} \\ &= a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p} \\ &= \left(\frac{a}{p}\right)\left(\frac{b}{p}\right). \end{aligned}$$

The Legendre Symbol takes on the value ±1, so being congruent to another Legendre Symbol is for it to be equivalent to it modulo p, so we have proven (b). ■

The expression of (a) is commonly referred to as Euler's Criterion, and appears consistently throughout many proofs of the Law of Quadratic Reciprocity. Euler's Criterion answers one significant question: is a a quadratic residue or quadratic nonresidue modulo p, where p is a fixed prime? Although this is fundamental, what if we desired to know for what p would some fixed a be a quadratic residue or quadratic nonresidue? This question can be answered with the Law of Quadratic Reciprocity.

In this Section, we will state the Complete Law of Quadratic Reciprocity alongside its numerous representations, and provide several examples of how it can be used to compute the Legendre Symbol.

Theorem 0.7 (Complete Law of Quadratic Reciprocity)**.** *The Law of Quadratic Reciprocity is comprised of three statements. Let p and q be distinct odd primes.*

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

(b)
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

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

The expression for (a) is not difficult to prove. Recall Euler's Criterion and substitute $a = -1$. Then
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$
and we are done. The second equivalence for (b) is a bit more difficult to prove, so we will explore that in more depth in Section 2.

The expressions (a) and (b) are commonly omitted when presenting the Law of Quadratic Reciprocity; this is for good reason as well, as (c) is usually the most interesting and applicable one. However, as we will see, Quadratic Reciprocity is far more intuitive when stated as a series of conditions and equivalences, rather than as a formulaic equivalence such as the above.

Looking at the equivalence in (c), one can easily see that by multiplying both sides by $(\frac{p}{q})$ or $(\frac{q}{p})$ and using Proposition **0.3**, one can obtain

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

Notice that in this expression, certain restrictions on p and q can yield equivalent relationships between the two reciprocal Legendre Symbols. The sign of the right-hand-side of $(*)$ is entirely determined by the exponent to which -1 is raised. We can study this exponent to obtain some information about the term $(-1)^{(p-1)/2\cdot(q-1)/2}$: if this exponent is even, then the sign is 1, but if the exponent is odd, then the sign is -1. Through some experimentation with p and q distinct odd primes, one will find that $(\frac{p-1}{2})(\frac{q-1}{2})$ is even when either $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, and is odd when $p \equiv q \equiv 3 \pmod 4$.

With this information, and after evaluating the right-hand-side of $(*)$, a relationship between the two reciprocal Legendre Symbols emerges. Thus
$$\left(\frac{p}{q}\right) = \begin{cases} (\frac{q}{p}) & \text{if } p \equiv 1 \pmod 4 \text{ or } p \equiv 1 \pmod 4 \\ -(\frac{q}{p}) & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4. \end{cases}$$

For example, let us evaluate the Legendre Symbol $(\frac{11}{29})$. After performing several mental calculations, one can see that 29 is congruent to 1 modulo 4. However, since there is at least one condition satisfied, we can write $(\frac{29}{11})$. By Proposition **0.3**, we can reduce $29 \equiv 7 \pmod{11}$, so that we have $(\frac{11}{29}) = (\frac{7}{11})$. Both $7 \equiv 11 \equiv 3$

(mod 4), so we have $(\frac{7}{11}) = -(\frac{11}{7})$. Simplifying again, we obtain $-(\frac{11}{7}) = -(\frac{4}{7})$. Since the numerator 4 is clearly a square, $(\frac{4}{7}) = 1$, so $(\frac{11}{29}) = -1$, and 11 is a quadratic nonresidue modulo 29.

The above is a rather simple example, but the equivalences are applicable for large p and q, and can be used to calculate a Legendre Symbol with large distinct primes such as $(\frac{1247}{1481})$.

The technique for converting statements about Legendre Symbols into conditions on primes is nothing unique; it can be used to construct similar congruences for (a) and (b). The statement for (a) can be represented as

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Similarly, (b) can be represented as

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 5 \pmod 8. \end{cases}$$

Notice how the modulus in both Legendre Symbols is a multiple of 4; this is no coincidence.

Now we are interested in another application of Quadratic Reciprocity. The previous representation for it was found to be rather useful for evaluating Legendre Symbols, so what if we instead desired a general representation for primes p for which some a, which we will take to be an odd prime q, is a quadratic residue? We will gradually answer this question in Section 1 as more elements of Quadratic Reciprocity and the work of Euler, Gauss, and others reveal themselves.

1. An Equivalence and Application of Quadratic Reciprocity

1.1. **Application.** As an interesting application of the Law of Quadratic Reciprocity, and addressing the question posed at the end of Section 0, we will assume that Quadratic Reciprocity is true and state and prove the following theorem.

Theorem 1.1. *If we allow q to be an odd prime, then*

(a) *if $q \equiv 1 \pmod 4$, then $p \equiv r \pmod q$, where r is a quadratic residue modulo q, if and only if $\left(\frac{q}{p}\right) = 1$.*

(b) *if $q \equiv 3 \pmod 4$, then $p \equiv \pm b^2 \pmod{4q}$, where b is an odd integer and $\gcd(b, p) = 1$, if and only if $\left(\frac{q}{p}\right) = 1$.*

Proof. We will first prove the forward direction of (a), while using the condition that $q \equiv 1 \pmod 4$. First notice that by Theorem **0.7**, (a) reduces to a simple statement. Since we provided the condition for $q \equiv 1 \pmod 4$, we have the necessary criteria for $(\frac{q}{p})$ to be equivalent to $(\frac{p}{q})$. Thus the statement follows, and we are done.

Now we will prove the forward direction of (b), while using the condition that $q \equiv 3 \pmod 4$. To do so, we have to reconsider equation $(*)$. Notice that since $q \equiv 3 \pmod 4$, we have two possible conditions on p; namely $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$. By performing quick calculations, one can see that the former condition produces $(\frac{q}{p}) = (\frac{p}{q})$, while the latter condition produces $(\frac{q}{p}) = -(\frac{p}{q})$. Of course, these are expected; they are the conditions that should occur due to Quadratic Reciprocity, so we can write that when $q \equiv 3 \pmod 4$ is a set condition, and $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$,

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

As in the theorem, we will assume that $p \equiv \pm b^2 \pmod{4q}$, where b is an odd integer. We will consider both $+$ and $-$ cases. Taking the $+$ in the congruence first, we have that $p \equiv b^2 \equiv 1 \pmod 4$. Since b is presumed to be odd, and the square of an odd number is still odd, it is always congruent to 1 modulo 4. Returning to (1), we thus see that since $p \equiv 1 \pmod 4$ and $p \equiv b^2 \pmod q$,

$$(-1)^{\frac{p-1}{2}} = 1 \text{ and } \left(\frac{p}{q}\right) = 1,$$

so that $(\frac{q}{p}) = (1)(1) = 1$, and we have proven the $+$ case.

Now taking the $-$ in the congruence, we have $p \equiv -b^2 \equiv -1 \equiv 3 \pmod 4$. The congruence modulo 4 arises similarly. Returning again to (1), we see that since $\equiv 3 \pmod 4$ and $p \equiv -b^2 \pmod q$, and using Theorem **0.7**,

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

Using the presumed fact that $q \equiv 3 \pmod 4$, we know that this is just

$$\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}} = (-1)^{\frac{(4k+3)-1}{2}} = -1,$$

so that $(\frac{q}{p}) = (-1)(-1) = 1$, and we have proven the $-$ case.

We will now prove the converse of (a) and (b). To prove the converse of both statements, we will first assume that $(\frac{q}{p}) = 1$. In order to continue similarly to above, we will consider the two previously calculated cases:

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

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

From (1) we can easily see that it must be true that both $p \equiv 1 \pmod 4$ and $p \equiv b^2 \pmod q$. We can assume that b is odd because in the case that it is even, we could create another number of the form $b' = b + q$, thus creating another odd number. Since b is odd, $b^2 \equiv 1 \pmod 4$ as follows from a previous argument, so that $p \equiv b^2$

(mod 4). Given these conditions, it must be true that $p \equiv b^2 \pmod{4q}$, completing the positive case.

To prove (2), we first have to show that every quadratic nonresidue is the negative of a quadratic residue.

Consider some congruence $a \equiv b^2 \pmod{p}$. Then $(\frac{a}{p}) = 1$ because a is a quadratic residue modulo p by definition. Now consider $c \not\equiv d^2 \pmod{p}$. Since c is not, by definition, a quadratic residue modulo p, it must be that it is a quadratic nonresidue, and if so, its Legendre Symbol is -1, so $(\frac{c}{p}) = -1$. It is not hard to see that this implies that $(\frac{c}{p}) = -(\frac{a}{p})$, and we are done.

From (2) we thus have $p \equiv 3 \pmod{4}$ and $p \equiv -b^2 \pmod{q}$ via the statement proven above. Assuming that b is again odd, we have that $-b^2 \equiv 3 \pmod{4}$ and $p \equiv -b^2 \pmod{4}$, thus implying that $p \equiv -b^2 \pmod{4q}$, and we are done, since combining (1) and (2) yields the desired result. ■

1.2. **Proof of Equivalence.** With this theorem now equipped, we are prepared to confront the second of the two main theorems in this section. What follows is a proof of equivalence. While investigating Fermat's Theorem on the Sum of Two Squares, Euler discovered an equivalence between a particular statement and the expression in Theorem **0.7**. To prove the equivalence of these two statements, we will first assume that Quadratic Reciprocity in Theorem **0.7** is true, and use it to prove that the second statement is true. Then we will show that the second statement must imply the first in two different cases.

Theorem 1.2. *The Law of Quadratic Reciprocity in Theorem **0.7** is equivalent to the following statement: (a) if p and q are distinct odd primes, $a \geq 1$ is any integer such that $p \nmid a$, and $p \equiv \pm q \pmod{4a}$, then* $\left(\dfrac{a}{p}\right) = \left(\dfrac{a}{q}\right)$.

Proof. To prove this statement, we must divide it into manageable parts. In this proof, we will first assume that Quadratic Reciprocity is true. In order to show that Theorem **0.7** implies (a), we will first reduce the problem from the matter of any integer $a \geq 1$ to a problem concerning a a prime integer. It is in fact enough to show that the assertion described in (a) about $a \geq 1$ an integer is equivalent to an assertion that we will call (b) about a a prime integer. This would effectively reduce the statement to an easier one. We may do this with several properties of the Legendre Symbol.

We assume that (a) is true. Noticing the statement in (b), we have that some p_i for some $1 \leq i \leq n$ that $(\frac{p_i}{p}) = (\frac{p_i}{q})$ for distinct odd primes p and q. If $a \geq 1$ is an integer, then it can be written in the form $a = p_1p_2p_3 \cdots p_n$ where $p_1, p_2, p_3, \ldots, p_n$ are not necessarily distinct. Since i ranges from 1 to n, we can take the product of both sides to obtain

$$\begin{aligned}\prod_{i=1}^{n}\left(\frac{p_i}{p}\right) &= \prod_{i=1}^{n}\left(\frac{p_i}{q}\right)\\ \left(\frac{p_1p_2p_3\cdots p_n}{p}\right) &= \left(\frac{p_1p_2p_3\cdots p_n}{q}\right)\\ \left(\frac{a}{p}\right) &= \left(\frac{a}{q}\right),\end{aligned}$$

so we have proven that (b) implies (a) and reduced the problem to a a prime integer.

Now that we have done this, we can consider two cases for a; the first is when a is an even prime, and the second when a is an odd prime.

In the first case, if a is an even prime, then $a = 2$. Using the statement about $(\frac{2}{p})$ from earlier, it can be shown that the relation indeed holds, since there is already an explicit expression for $(\frac{2}{p})$ for p an odd prime. We will prove the statement about $(\frac{2}{p})$ first seen in Section 0 later in Section 2.

We now move on to the second case. If a is an odd prime, then using $(*)$,

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

In the case that $p \equiv q \pmod{4a}$ in (b), we have that $(\frac{p}{a}) = (\frac{q}{a})$, so that

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

Using the equation above, we can rewrite $(\frac{q}{a})$ as $(-1)^{\frac{a-1}{2}\frac{q-1}{2}}(\frac{a}{q})$, so that

$$\begin{aligned}\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}\left(\frac{q}{a}\right) &= (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}(-1)^{\frac{a-1}{2}\cdot\frac{q-1}{2}}\left(\frac{a}{q}\right)\\ &= (-1)^{\frac{(p-1)(a-1)}{4}+\frac{(q-1)(a-1)}{4}}\left(\frac{a}{q}\right)\\ &= (-1)^{\frac{a-1}{2}\cdot\frac{p+q-2}{2}}\left(\frac{a}{q}\right).\end{aligned}$$

Since $p \equiv q \pmod{4a}$, we have that $p + q - 2 \equiv 0 \pmod 4$, because, checking separate cases for conditions on p and q; namely when (a) $p \equiv q \equiv 1 \pmod 4$ and (b) $p \equiv q \equiv 3$, we can add congruences so that for (a) we have

$$\begin{aligned}p + q &\equiv 1 + 1 \pmod 4\\ p + q - 2 &\equiv 0 \pmod 4,\end{aligned}$$

and for (b) we have

$$\begin{aligned} p+q &\equiv 3+3 \pmod 4 \\ p+q-6 &\equiv 0 \pmod 4 \\ p+q-2 &\equiv 0 \pmod 4. \end{aligned}$$

This demonstrates the equivalence.

Now we consider the case in which $p \equiv -q \pmod{4a}$. Since $p \equiv -q \pmod{4a}$ we have that $(\frac{p}{a}) = (\frac{-q}{a}) = (-1)^{\frac{a-1}{2}}(\frac{q}{a})$. Thus we have

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

Notice again that we can rewrite $(\frac{q}{a})$ as $(-1)^{\frac{a-1}{2}\cdot\frac{q-1}{2}}(\frac{a}{q})$, so that

$$\begin{aligned} \left(\frac{a}{p}\right) &= (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}(-1)^{\frac{a-1}{2}}(-1)^{\frac{a-1}{2}\cdot\frac{q-1}{2}}\left(\frac{a}{q}\right) \\ &= (-1)^{\frac{(p-1)(a-1)}{4}+\frac{2(a-1)}{4}+\frac{(a-1)(q-1)}{4}}\left(\frac{a}{q}\right) \\ &= (-1)^{\frac{(a-1)[(p-1)+2+(q-1)]}{4}}\left(\frac{a}{q}\right) \\ &= (-1)^{\frac{a-1}{2}}(-1)^{\frac{p+q}{2}}\left(\frac{a}{q}\right). \end{aligned}$$

Since $p \equiv -q \pmod{4a}$, we have that $p+q \equiv 0 \pmod 4$, because, checking separate conditions on p and q again; namely when (a) $p \equiv 1 \pmod 4$ and $q \equiv -1 \pmod 4$ and (b) $p \equiv 3 \pmod 4$ and $q \equiv -3 \pmod 4$, we can add congruences for (a) to obtain

$$\begin{aligned} p+q &\equiv 1+3 \pmod 4 \\ p+q &\equiv 0 \pmod 4, \end{aligned}$$

and for (b) we have

$$\begin{aligned} p+q &\equiv 3+1 \pmod 4 \\ p+q &\equiv 0 \pmod 4. \end{aligned}$$

This also demonstrates the equivalence, and we have proven (a) $\Longrightarrow$ (b).

Now we must prove the converse. For the sake of simplicity, allow $p > q$, and also allow $p \equiv q \pmod 4$, which is the first case that we will consider. By the Definition of Congruence, this means that $p = 4a + q$ for some integer $a \geq 1$. This means that the Legendre Symbol $(\frac{p}{q}) = (\frac{4a+q}{q})$. Simplifying this expression, we have

$$\left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{4}{q}\right)\left(\frac{a}{q}\right) = (1)\left(\frac{a}{q}\right) = \left(\frac{a}{q}\right).$$

Then $(\frac{p}{q}) = (\frac{a}{q}) = (\frac{a}{p})$. Computing $(\frac{p}{q})$ again, we have that

$$\left(\frac{p}{q}\right) = \left(\frac{4a}{p}\right) = \left(\frac{p-q}{p}\right) = \left(\frac{-q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{q}{p}\right).$$

In the case that $p \equiv 1 \pmod 4$, we can substitute $p = 4k + 1$ to obtain the expression $(\frac{p}{q}) = (\frac{q}{p})$, which is the corresponding case in Quadratic Reciprocity. Similarly, if $p \equiv 3 \pmod 4$ then $q \equiv 3 \pmod 4$, and $(\frac{p}{q}) = -(\frac{q}{p})$ in that particular case of Quadratic Reciprocity.

We now consider the second case, in which $p \equiv -q \pmod 4$. Again from the Definition of Congruence, this means that $p = 4a - q$ for some $a \geq 1$. This means that we have the Legendre Symbol $(\frac{p}{q}) = (\frac{4a-q}{q})$. Simplifying this expression, we have

$$\left(\frac{4a-q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{4}{q}\right)\left(\frac{a}{q}\right) = (1)\left(\frac{a}{q}\right) = \left(\frac{a}{q}\right).$$

Then

$$\left(\frac{p}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{p+q}{p}\right) = \left(\frac{q}{p}\right),$$

which is the statement of Quadratic Reciprocity in the case where either p or q is congruent to 1 modulo 4. Then we are finished, and have proven both directions. ■

2. Quadratic Reciprocity and a Lattice Point Construction by Eisenstein

Now that we are equipped with one rather elegant proof of an equivalence of Quadratic Reciprocity to another statement by Euler, we are prepared to introduce a complete proof. The proof that we will introduce next is one by Eisenstein, and uses two very important lemmas; namely Gauss' Lemma and Eisenstein's Lemma.

2.1. Gauss' Lemma.

Gauss' Lemma is what we will introduce first, as it introduces a certain number that we will explicitly calculate in the proof of Eisenstein's Lemma. Let us first begin by introducing Gauss' Lemma. Let p be an odd prime.

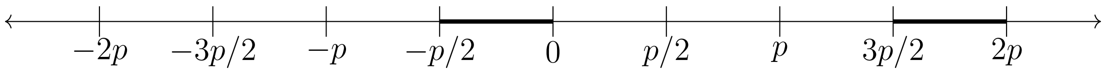
Theorem 2.1 (Gauss' Lemma). *Let* $\gcd(a, p) = 1$. *Then*

$$\left(\frac{a}{p}\right) = (-1)^{\mu(a,p)},$$

where $\mu(a, p)$ is the number of least negative residues modulo p, and is dependent on a and p.

Before we prove Theorem **2.1**, we will first introduce the meaning of "least negative residues modulo p".

Consider a set $S = \{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$. Let $p \nmid a$. We are going to reduce the elements of this set modulo p so that they lie within the open interval $(\frac{-p}{2}, \frac{p}{2})$. To show why this interval is correct, consider the number line below.



Consider some number lying in any of the open intervals displayed in the above number line (note that the intervals are open because the value $p/2$ is not an integer). To show why the open interval of the integers that are multiples of a is $(-\frac{p}{2}, \frac{p}{2})$, consider some number $j \in (\frac{3p}{2}, 2p)$. If we want to determine what interval j will lie in, we reduce its bounds modulo p, so that we have $(\frac{3p}{2} - 3p, 2p - 2p) = (-\frac{p}{2}, 0)$. This is one half of the open interval that we described above. To determine the other half of the open interval, we can reduce the bounds of other open intervals modulo p to obtain $(0, \frac{p}{2})$. Taking the union, we have

$$\Big(-\frac{p}{2}, 0\Big) \cup \Big(0, \frac{p}{2}\Big) = \Big(-\frac{p}{2}, \frac{p}{2}\Big).$$

In general, this fact about reduction of bounds modulo p is true for all open intervals $(\frac{(k)p}{2}, \frac{(k+1)p}{2})$, where $k \in \mathbb{Z}$. In other words, any positive integer is congruent to some integer within the open interval $(\frac{-p}{2}, \frac{p}{2})$, as they lie within the same equivalence class modulo p.

After reducing modulo p, as shown above, any points will reside within the open interval $(\frac{-p}{2}, \frac{p}{2})$, which means that a certain number of points will be negative and positive, depending on their original position. The reduced variant of the aforementioned points is known as the set of *least residues* of S. The reduced variants that are less than zero are known as the *least negative residues*, and the number of these points is $\mu(a, p)$.

As can be seen in Gauss' Lemma, the construction of this set and the reduction of its elements modulo p is useful for determining the Legendre Symbol $(\frac{a}{p})$. Before we prove it in general, we will evaluate a Legendre Symbol so we can understand how the reduction functions on integers. Consider $(\frac{3}{11})$. Notice that $\frac{11-1}{2} = 5$. Construct the set $S = \{1 \cdot 3, 2 \cdot 3, 3 \cdot 3, 4 \cdot 3, 5 \cdot 3\}$. Reducing it modulo 11, and noticing that the reduced elements must lie in the open interval $(\frac{-11}{2}, \frac{11}{2})$ we have the new set $T = \{3, -5, -2, 1, 4\}$. There are 2 least negative residues modulo, so $\mu = 2$, and $(\frac{3}{11}) = (-1)^2 = 1$, so 3 is a quadratic residue modulo 11. We can check that this is indeed true, since $(\frac{3}{11}) = (\frac{25}{11}) = 1$.

Now we are prepared to prove Gauss' Lemma.

Proof of Gauss' Lemma. Construct the set $S = \{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$, where we allow $\gcd(a, p) = 1$. Our objective is to reduce elements of S modulo p to form another set T of least residues of S. We will then determine several characteristics of T and use them to reach the finale of our proof.

We will state and prove 3 properties of T. The first is that no elements in T are going to be congruent modulo p; this is clear due to the fact that all elements of S are distinct, so their reduced variants cannot possibly be congruent modulo p. To show why this is true, consider some αa and βa both contained within the set S. Then it is true that $1 \leq \alpha, \beta \leq \frac{p-1}{2}$. If they are congruent modulo p, or in other words reduce to the same integer within the open interval $(-\frac{p}{2},\frac{p}{2})$, then $\alpha a \equiv \beta a \pmod{p}$. This implies that $\alpha a - \beta a \equiv 0 \pmod{p}$, and so $p|a(\alpha-\beta)$. But $p \nmid a$, so this is just $p|\alpha-\beta$. However, this is impossible given the restrictions on α and β; the only scenario in which this is true is when $\alpha=\beta$, but that is the exact statement that we are attempting to disprove.

The second statement is that every element of T will be nonzero because no element of S is a multiple of p.

The third property is the assertion that for all $t_1, t_2 \in T$, $t_1 \neq -t_2$. First assume that $t_1 = -t_2$, so that $t_1+t_2=0$. Since every $t_i \in T$ was reduced modulo p, both t_1 and t_2 can be written in the form $s_1 = t_1 + mp$ and $s_2 = t_2 + np$ respectively, where $s_1, s_2 \in S$. Allowing $m+n=k$, we have that $s_1+s_2 = t_1+t_2+mp+np$, but $t_1+t_2=0$, so this is simply $s_1+s_2=kp$. Since s_1 and s_2 belong to S, they must be integers of the form $j_1 a$ and $j_2 a$ respectively, where $1 \leq j_1, j_2 \leq \frac{p-1}{2}$. Then $(j_1+j_2)a = kp$. However, noticing the restrictions on j_1 and j_2, we can see that it is impossible for this equivalence to be true. Regardless of the values of j_1 and j_2, their sum cannot surpass $p-1$. This means that the assertion that $t_1=-t_2$ is false, and it is impossible for elements in T to be negatives of other elements in T.

Before we may finish, we must understand one particular case. Suppose that after reduction, the elements of T are all positive and lie within the open interval $(0,\frac{p}{2})$; in other words, the set is exactly $T=\{1,2,3,\ldots,\frac{p-1}{2}\}$. This means that it contains exactly $\frac{p-1}{2}$ elements. Extending this same logic to T where its elements can either be positive or negative, noticing that it must also contain $\frac{p-1}{2}$ elements, and finally using the fact that no element is a negative of another in T, the set must be exactly $T=\{\pm 1, \pm 2, \pm 3, \ldots, \pm\frac{p-1}{2}\}$.

Now we can finish. Take the product of elements of S and T and equate them modulo p, so that

$$\begin{aligned}
\prod_{i=1}^{\frac{p-1}{2}} t_i &\equiv \prod_{i=1}^{\frac{p-1}{2}} s_i \pmod{p}\\
(\pm 1)(\pm 2)(\pm 3)\cdots\left(\pm\frac{p-1}{2}\right) &\equiv (a)(2a)(3a)\cdots\left(\frac{p-1}{2}a\right) \pmod{p}\\
\left(\frac{p-1}{2}\right)!(\pm 1)(\pm 1)(\pm 1)\cdots(\pm 1) &\equiv a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \pmod{p}\\
(\pm 1)(\pm 1)(\pm 1)\cdots(\pm 1) &\equiv a^{\frac{p-1}{2}} \pmod{p}.
\end{aligned}$$

Notice that the left-hand-side of this congruence is simply a product of the sign of the least negative residues modulo p, so there are exactly $\mu(a,p)$ of these numbers. Thus

$$(-1)^{\mu(a,p)} \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

By Euler's Criterion in Theorem **0.6**,

$$(-1)^{\mu(a,p)} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Since both left and right-hand-side are either 1 or -1, they are equivalent and the modulus is irrelevant. Thus

$$(-1)^{\mu(a,p)} = \left(\frac{a}{p}\right),$$

and we are done. ■

2.2. **Quadratic Character of 2 modulo p by Gauss' Lemma.** The proof of Gauss' Lemma presents another form of calculation of the Legendre Symbol. Instead of counting the number of least negative residues, we can take the product from $i = 1$ to $\frac{p-1}{2}$ of each the original elements of the set S and the set of least residues modulo p, and then equate them modulo p. As an example, we will consider the Legendre Symbol $(\frac{3}{11})$ again. We construct the set $S = \{3 \cdot 1, 3 \cdot 2, 3 \cdot 3, 3 \cdot 4, 3 \cdot 5\}$, and its set of least residues modulo 11 given by $T = \{3, -5, -2, 1, 4\}$. We then equate the products:

$$\begin{aligned} 3 \cdot 1 \cdot 3 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 4 \cdot 3 \cdot 5 &\equiv 3 \cdot (-5) \cdot (-2) \cdot 1 \cdot 4 \pmod{11} \\ 3^5 5! &\equiv (-1)^2 5! \pmod{11} \\ 3^5 &\equiv 1 \pmod{11}, \end{aligned}$$

so 3 is a quadratic residue modulo 11.

Although this technique for calculating is rather complex, it introduces an interesting combinatorial proof technique, and can be used to prove Quadratic Reciprocity. First, however, recalling the statement about $(\frac{2}{p})$ from Section 0, we will now show that its conditions on primes are indeed true.

Proof of the derivation of the quadratic character of 2 *modulo p.* To show that the conditions on p are true, we must evaluate the Legendre Symbol $(\frac{2}{p})$ using Gauss' Lemma.

We begin by constructing the set $S = \{1\cdot2, 2\cdot2, 3\cdot2, \ldots, \frac{p-1}{2}\cdot2\} = \{2, 4, 6, \ldots, p-1\}$. Our goal is to reduce S modulo p so as to obtain the set T, which will be composed of the least residues of elements of S. Notice first that $\mu(a,p)$ is the exact number of elements in S that exceed $\frac{p-1}{2}$. This is because elements that exceed $\frac{p-1}{2}$ are able to be reduced modulo p such that they lie within the open interval $(-\frac{p}{2}, \frac{p}{2})$.

Our goal is to determine the value of $\mu(a,p)$. Since $\mu(a,p)$ is the number of least negative residues, it is equivalent to the difference:

$$\mu(a,p) = \left\{\text{elements in } S\right\} - \left\{\begin{matrix}\text{elements in } S \text{ that are} \\ \text{positive least residues modulo } p\end{matrix}\right\}$$

Clearly there are $\frac{p-1}{2}$ elements in S, by construction. The number of elements in S that are positive least residues modulo p is confined by several inequalities. Since S is constructed with multiples of 2, each element can be represented as $2m \in S$, where $1 \leq m \leq \frac{p-1}{2}$. It is clear that $2m < \frac{p}{2}$ describes elements of S after reduction modulo p that are positive, and that it is equivalent to $m < \frac{p}{4}$. Since p is an odd integer, it cannot be divided by a non-prime, so we must take its floor. Thus we have $\lfloor \frac{p}{4} \rfloor$. Then we can write

$$\mu(a,p) = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor.$$

Now that we have an explicit formula for individual evaluations of the Legendre Symbol $(\frac{2}{p})$, we can consider cases for different conditions on p.

(1) When $p \equiv 1 \pmod 8$, we have $\frac{(8k+1)-1}{2} = 4k$, and $m = \lfloor \frac{8k+1}{4} \rfloor = 2k$. Then $\mu(a,p) = 4k - 2k = 2k$, and $(-1)^{2k} = 1$.
(2) When $p \equiv 3 \pmod 8$, we have $\frac{(8k+3)-1}{2} = 4k+1$, and $m = \lfloor \frac{8k+3}{4} \rfloor = 2k$. Then $\mu(a,p) = (4k+1) - 2k = 2k+1$, and $(-1)^{2k+1} = -1$.
(3) When $p \equiv 5 \pmod 8$, we have $\frac{(8k+5)-1}{2} = 4k+2$, and $m = \lfloor \frac{8k+5}{4} \rfloor = 2k+1$. Then $\mu(a,p) = (4k+2) - (2k+1) = 2k+1$, and $(-1)^{2k+1} = -1$.
(4) When $p \equiv 7 \pmod 8$, we have $\frac{(8k+7)-1}{2} = 4k+3$, and $m = \lfloor \frac{8k+7}{4} \rfloor = 2k+1$. Then $\mu(a,p) = (4k+3) - (2k+1) = 2k+2$, and $(-1)^{2k+2} = 1$.

Then we are done. ■

The techniques shown above are not unique to $(\frac{2}{p})$; they can be replicated for other Legendre Symbols modulo p. We will not explore the derivation or evaluation of any of those Legendre Symbols, and that can be left as an exercise for the reader.

2.3. **Eisenstein's Lemma.**

Now we will introduce Eisenstein's Lemma. Although it is rather technical and specific, it will allow us to prove Quadratic Reciprocity in an entirely different way. The goal of Eisenstein's Lemma is to explicitly calculate the value of $\mu(a,p)$ modulo 2, and use that fact about $\mu(a,p)$ modulo 2 to state a fact about the Legendre Symbol $(\frac{a}{p})$. For the sake of simplicity, we will let $\frac{p-1}{2} = P$. We will now state Eisenstein's Lemma.

Lemma 2.2 (Eisenstein's Lemma)**.** *Let a be an odd integer and $p \nmid a$. Let $\mu(a,p)$ be the number of least negative residues of the set $S = \{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$. Then*

$$\sum_{k=1}^{P} \left\lfloor \frac{ka}{p} \right\rfloor \equiv \mu(a,p) \pmod 2.$$

(Note that the expression is (mod 2) *because the left-hand-side is either even or odd, both of which determine the eventual sign of the Legendre Symbol.)*

Proof. We may write every multiple ka as

$$ka = q_k p + r_k, \text{ where } -p < r_k < p \tag{1}$$

by The Division Algorithm. The two variables q_k and r_k represent the quotient and remainder respectively. Dividing each side by p, we have

$$\frac{ka}{p} = q_k + \frac{r_k}{p}, \text{ where } -\frac{1}{2} < \frac{r_k}{p} < \frac{1}{2}.$$

Taking the floor, we can notice that $\frac{ka}{p}$ can take on two values, so

$$\left\lfloor \frac{ka}{p} \right\rfloor = \begin{cases} q_k & \text{if } r_k > 0 \\ q_k - 1 & \text{if } r_k < 0. \end{cases}$$

Notice that if some $r_k < 0$, then $\lfloor \frac{ka}{p} \rfloor$ must be a least negative residue. Now if we take the sum, we have

$$\begin{aligned} \sum_{k=1}^{P} \left\lfloor \frac{ka}{p} \right\rfloor &= \sum_{k=1}^{P} q_k - \begin{Bmatrix} \text{number of } k \\ \text{such that } r_k < 0 \end{Bmatrix} \\ &= \sum_{k=1}^{P} q_k - \mu(a,p). \qquad (2) \end{aligned}$$

This is because exactly if there are k numbers such that $r_k < 0$, then exactly $(k)(1) = \mu(a,p)$ must be subtracted from the left-hand-side. To proceed, we must determine $\sum_{k=1}^{P} q_k$. Reducing (1) modulo 2, we have, since a and p are both presumed to be odd integers (p is obviously odd),

$$\begin{aligned} ka &\equiv q_k p + r_k \pmod 2 \\ k &\equiv q_k + r_k \pmod 2. \end{aligned}$$

Taking the sum, we have

$$\sum_{k=1}^{P} k \equiv \sum_{k=1}^{P} q_k + \sum_{k=1}^{P} r_k \pmod 2.$$

Notice that Gauss' Lemma asserts the existence of positive and negative least residues modulo p; thus, the individual r_i's in $\sum_{k=1}^{P} r_k \pmod 2$ correspond to the values $\pm 1, \pm 2, \pm 3, \dots,$
$\pm P$ in some unknown order. Since we are working in modulo 2, whether an integer is positive or negative is irrelevant, so we will take the positive sequence of correspondence for the sake of simplicity. Then

$$\begin{aligned} 1 + 2 + 3 + \cdots + P &\equiv \sum_{k=1}^{P} q_k + (1 + 2 + 3 + \cdots + P) \pmod 2 \\ \sum_{k=1}^{P} q_k &\equiv 0 \pmod 2. \end{aligned}$$

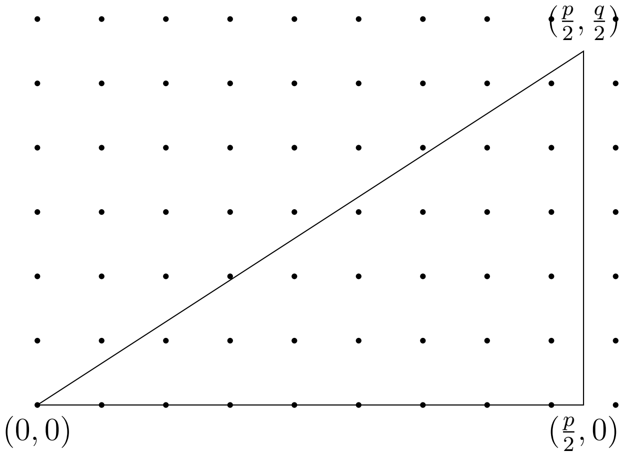
Substituting the above result and reducing (2) modulo 2, we are left with

$$\sum_{k=1}^{P} \left\lfloor \frac{ka}{p} \right\rfloor = \sum_{k=1}^{P} q_k - \mu(a,p) \equiv \mu(a,p) \pmod 2,$$

and we are done. ■

2.4. **Proof.** Now that we have proven Eisenstein's Lemma, we are prepared to prove Quadratic Reciprocity.

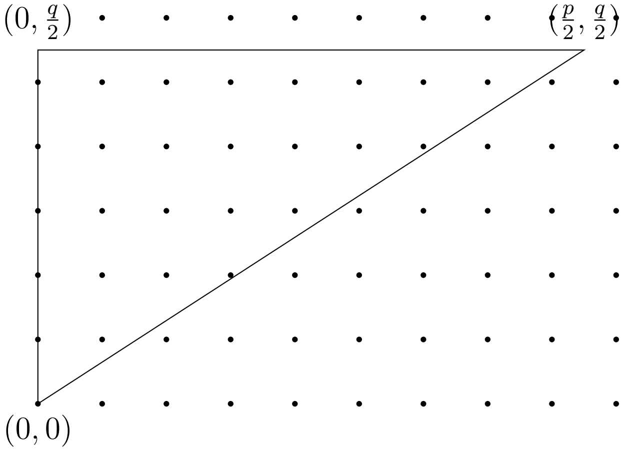
Proof of Quadratic Reciprocity. We begin by letting p and q be odd primes, and $P = \frac{p-1}{2}$ and $Q = \frac{q-1}{2}$. We will construct a triangle $T(q,p)$ with vertices at $(0,0), (\frac{p}{2}, 0)$, and $(\frac{p}{2}, \frac{q}{2})$.



Our goal is to count the exact number of points that are bounded by the sides of the triangle $T(q,p)$. Intersected points on the horizontal and vertical axes will not be included when counting; there are also no lattice points lying on the hypotenuse. Looking at the figure above, we can count the exact number of points by inspecting each column, beginning at $x = 1$. Thus we have $7 + 5 + 4 + 2 + 1 = 19$. The hypotenuse of $T(q,p)$ can be represented by the equation $y = \frac{q}{p}x$, so we can evaluate the number of points on a column by going through values of x and taking the floor. Thus for $x = 1$, we have $\lfloor \frac{q}{p} \rfloor$ points; for $x = 2$, we have $\lfloor \frac{2q}{p} \rfloor$ points; for $x = 3$, we have $\lfloor \frac{3q}{p} \rfloor$ points. In general, the kth column has $\lfloor \frac{kq}{p} \rfloor$ points, and the total number of points strictly bounded in $T(q,p)$ is given by the sum of all these, or

$$\sum_{k=1}^{P} \left\lfloor \frac{kq}{p} \right\rfloor.$$

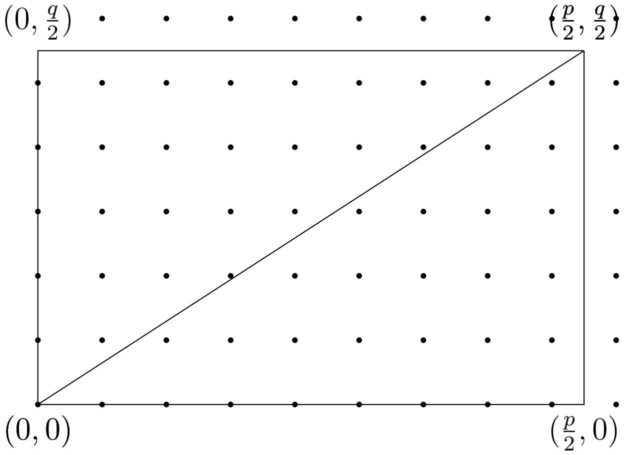
Now we consider another triangle $T'(p,q)$ with vertices at $(0,0), (0, \frac{q}{2})$, and $(\frac{p}{2}, \frac{q}{2})$.



Similar to $T(q,p)$, our goal is to count the number of points bounded by the sides of $T'(p,q)$. However, instead of counting the points in each column, we will count the number of points in each row; thus we begin with $y=1$, $y=2$, and so on. We will find the inverse of the previously determined representation of the hypotenuse, so that $x=\frac{p}{q}y$. We will evaluate this function for $y=1$, $y=2$, and so on, and then take the floor. Thus for $y=1$, we have $\lfloor\frac{p}{q}\rfloor$ points; for $y=2$, we have $\lfloor\frac{2p}{q}\rfloor$; for $y=3$, we have $\lfloor\frac{3p}{q}\rfloor$ points. In general, the kth row has $\lfloor\frac{kp}{q}\rfloor$ points, and the total number of points bounded in $T'(p,q)$ is given by the sum of all these, or

$$\sum_{k=1}^{Q}\left\lfloor\frac{kp}{q}\right\rfloor.$$

Now considering the combination of these two figures, we obtain a rectangle $R(p,q)$ with vertices at $(0,0),(0,\frac{q}{2}),(\frac{p}{2},\frac{q}{2}),(\frac{p}{2},0)$.



If we count the total number of points strictly bounded by the sides of both triangles, including the shared hypotenuse, we find that there are exactly

$$\sum_{k=1}^{P}\left\lfloor\frac{kq}{p}\right\rfloor+\sum_{k=1}^{Q}\left\lfloor\frac{kp}{q}\right\rfloor$$

points in $R(p,q)$. By Lemma **2.2**,

$$\sum_{k=1}^{P}\left\lfloor\frac{kq}{p}\right\rfloor+\sum_{k=1}^{Q}\left\lfloor\frac{kp}{q}\right\rfloor\equiv\mu(q,p)+\mu(p,q)\pmod 2. \tag{1}$$

Now we will calculate the number of lattice points in $R(p,q)$ in a different way. Notice that there are exactly $\lfloor\frac{p}{2}\rfloor$ columns and $\lfloor\frac{q}{2}\rfloor$ rows. Thus there are exactly

$$\begin{aligned}\sum_{k=1}^{P}\left\lfloor\frac{kq}{p}\right\rfloor+\sum_{k=1}^{Q}\left\lfloor\frac{kp}{q}\right\rfloor &= \left\lfloor\frac{p}{2}\right\rfloor\left\lfloor\frac{q}{2}\right\rfloor\\ &=\frac{p-1}{2}\cdot\frac{q-1}{2}\end{aligned}$$

points in $R(p,q)$. Then

$$\frac{p-1}{2}\cdot\frac{q-1}{2}\equiv\mu(q,p)+\mu(p,q)\pmod 2.$$

By Theorem **2.1**, this means that

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)&=(-1)^{\mu(p,q)}(-1)^{\mu(q,p)}\\ &=(-1)^{\mu(p,q)+\mu(q,p)}.\end{aligned}$$

However, by (1),

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

so we are done. ■

3. Quadratic Reciprocity and Primitive nth Roots of Unity

We will now introduce a proof of Quadratic Reciprocity using primitive nth roots of unity. The results in this section will be of utmost importance in the next section, as they form the basis for using complex-valued functions to compute integer equivalences. In the next section, we will explore Quadratic Gauss Sums, and how their compositions, alongside the use of algebraic integers and primitive pth roots of unity, correlates with Quadratic Reciprocity.

Before we may prove Quadratic Reciprocity in this way, we must introduce several small facts about primitive roots of unity.

3.1. **Preliminaries.** We call some complex number ζ an nth root of unity if it is a solution to the equation $\zeta^n = 1$ for some $n \in \mathbb{Z}^+$. If n is the least integer with this property, then ζ is a primitive nth root of unity. As can be seen by solving the equation $x^n - 1 = 0$, the roots are $1, e^{2\pi i/n}, e^{2(2\pi i/n)}, e^{3(2\pi i/n)}, \dots, e^{(n-1)(2\pi i/n)}$, and the primitive nth roots among these are written as $e^{k(2\pi i/n)}$, where $\gcd(k, n) = 1$. Since the power to which nth roots of unity are raised to is confined to the residues modulo n, it is clear that if $m \equiv l \pmod{n}$, then $\zeta^m = \zeta^l$, and the converse as well.

Consider the function $f(z) = e^{2\pi iz} - e^{-2\pi iz}$. Using the polar form of a complex number, this is just

$$\begin{aligned} f(z) &= e^{2\pi iz} - e^{-2\pi iz} \\ &= e^{i(2\pi z)} - e^{i(-2\pi z)} \\ &= \cos 2\pi z + i \sin 2\pi z - [\cos(-2\pi z) + i \sin 2\pi z] \\ &= 2i \sin 2\pi z. \end{aligned}$$

Notice that this satisfies $f(z + 1) = f(z)$ and $f(-z) = -f(z)$. The real zeroes of this function are only the half-integers (numbers of the form $n + 1/2$ for $n \in \mathbb{Z}$), because if there is some real number r and $2r \notin \mathbb{Z}$, then $f(r) \neq 0$. This is because, for some half integer α, the value $2\alpha \in \mathbb{Z}$, so if $2r \notin \mathbb{Z}$, then it is impossible for $f(r) = 0$. With these small results, we can begin.

Lemma 3.1. *If $n > 0$ is odd, then the following factorization is true:*

$$x^n - y^n = \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y),$$

where $\zeta = e^{2\pi i/n}$.

Proof. Notice that $1, \zeta, \zeta^2, \zeta^3, \dots, \zeta^{n-1}$ are roots of the complex equation $z^n - 1 = 0$. Since the Fundamental Theorem of Algebra asserts that there are exactly n roots to this nth degree equation, we can factorize it as

$$\begin{aligned} z^n - 1 &= (z - 1)(z - \zeta)(z - \zeta^2)(z - \zeta^3) \cdots (z - \zeta^{n-1}) \\ &= \prod_{k=0}^{n-1} (z - \zeta^k). \end{aligned}$$

Letting $z = x/y$, we see that

$$\begin{aligned} \frac{x^n}{y^n} - 1 &= \prod_{k=0}^{n-1} \left(\frac{x}{y} - \zeta^k \right) \\ x^n - y^n &= y^n \prod_{k=0}^{n-1} \left(\frac{x}{y} - \zeta^k \right). \end{aligned}$$

Noticing that y^n can be distributed across the product, we have

$$\begin{aligned} x^n - y^n &= (x-y)(x-\zeta y)(x-\zeta^2 y)(x-\zeta^3 y)\cdots(z-\zeta^{n-1}y) \\ &= \prod_{k=0}^{n-1}(x-\zeta^k y). \end{aligned}$$

Since n remains odd as k goes through the complete set of residues modulo n, $-2k$ does as well. Then we can equivalently write this as

$$\begin{aligned} \prod_{k=0}^{n-1}(x-\zeta^k y) &= \prod_{k=0}^{n-1}(x-\zeta^{-2k}y) \\ &= \prod_{k=0}^{n-1}\zeta^{-k}(\zeta^k x-\zeta^{-k}) \\ &= \zeta^{-[1+2+3+\cdots+(n-1)]}\prod_{k=0}^{n-1}(\zeta^k x-\zeta^{-k}y), \end{aligned}$$

and using the fact that $1+2+3+\cdots+(n-1) = \frac{(n-1)(n-1+1)}{2} = \frac{n(n-1)}{2}$, and that is must be divisible by n, we have

$$\zeta^{-(n(n-1)/2)}\prod_{k=0}^{n-1}(\zeta^k x-\zeta^{-k}y) = \prod_{k=0}^{n-1}(\zeta^k x-\zeta^{-k}y),$$

and we are done. ■

We will now show another result.

Lemma 3.2. *If $n \in \mathbb{Z}^+$ and is odd and $f(z) = e^{2\pi iz} - e^{-2\pi iz}$, then*

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{(n-1)/2} f\left(z+\frac{k}{n}\right)f\left(z-\frac{k}{n}\right).$$

Proof. We can let $x = e^{2\pi iz}$ and $y = e^{-2\pi iz}$ in Lemma **3.1**. Then

$$\begin{aligned} f(nz) &= e^{2\pi izn} - e^{-2\pi izn} \\ &= \prod_{k=1}^{n-1}(e^{2\pi ik/n}e^{2\pi iz} - e^{2\pi ik/n}e^{-2\pi iz}) \\ &= \prod_{k=1}^{n-1}(e^{2\pi i(k/n+z)} - e^{-2\pi i(k/n+z)}) \\ &= \prod_{k=0}^{n-1} f\left(\frac{k}{n}+z\right). \end{aligned}$$

Notice that

$$f\left(z+\frac{k}{n}\right)=f\left(z+\frac{k}{n}-1\right)=f\left(z-\frac{n-k}{n}\right).$$

In this expression, notice that as k ranges from $(n+1)/2$ to $n-1$, the value of $n-k$ ranges from $(n-1)/2$ to 1. Thus we have

$$\begin{aligned}\frac{f(nz)}{f(z)}&=\prod_{k=1}^{(n-1)/2} f\left(z+\frac{k}{n}\right)\prod_{k=(n+1)/2}^{n-1} f\left(z+\frac{k}{n}\right)\\&=\prod_{k=1}^{(n-1)/2} f\left(z+\frac{k}{n}\right)\prod_{k=(n+1)/2}^{n-1} f\left(z-\frac{n-k}{n}\right)\\&=\prod_{k=1}^{(n-1)/2} f\left(z+\frac{k}{n}\right)f\left(z-\frac{k}{n}\right),\end{aligned}$$

and we are done. ■

Now we show the final result.

Lemma 3.3. *If p is an odd prime, $a\in\mathbb{Z}$ such that $p\nmid a$, and f is the aforementioned function $f(z)=e^{2\pi iz}-e^{-2\pi iz}$, then*

$$\prod_{l=1}^{(p-1)/2} f\left(\frac{la}{p}\right)=\left(\frac{a}{p}\right)\prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right).$$

Proof. We begin by returning to the technique used in Gauss' Lemma. Notice that some multiple, say la, could be reduced modulo p so that $la\equiv\pm m_l \pmod p$, where the least residue $m_l>0$ so that it can be bounded within the interval $[1,\frac{p}{2})$, and can have a sign that varies between positive and negative in the congruence. Then it is true that la/p and $\pm m_l/p$ differ by an integer by the statement of their congruence modulo p, so that

$$f\left(\frac{la}{p}\right)=f\left(\frac{\pm m_l}{p}\right)=\pm f\left(\frac{m_l}{p}\right).$$

Now taking the product from $l=1$ to $\frac{p-1}{2}$ of the left-hand-side and right-hand-side, we have

$$\begin{aligned}\prod_{l=1}^{(p-1)/2} f\left(\frac{la}{p}\right)&=\prod_{l=1}^{(p-1)/2}\pm f\left(\frac{m_l}{p}\right)\\&=(-1)^{\mu(a,p)}\prod_{l=1}^{(p-1)/2} f\left(\frac{m_l}{p}\right).\end{aligned}$$

This is because there are exactly $\mu(a,p)$ least negative residues residues within, so taking the product, you obtain exactly $(-1)^{\mu(a,p)}$. By Theorem **2.1**,

$$(-1)^{\mu(a,p)} \prod_{l=1}^{(p-1)/2} f\left(\frac{m_l}{p}\right) = \left(\frac{a}{p}\right) \prod_{l=1}^{(p-1)/2} f\left(\frac{m_l}{p}\right),$$

and we are done. ■

3.2. **Proof.** Now that we are familiar with these three results, we are able to finish with a proof of Quadratic Reciprocity.

Proof of Quadratic Reciprocity. By Lemma **3.3**, we have

$$\prod_{l=1}^{(p-1)/2} f\left(\frac{lq}{p}\right) = \left(\frac{q}{p}\right) \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right).$$

Notice that by Lemma **3.2**,

$$\frac{f(\frac{lq}{p})}{f(\frac{l}{p})} = \prod_{m=1}^{(q-1)/2} f\left(\frac{l}{p} + \frac{m}{q}\right) f\left(\frac{l}{p} - \frac{m}{q}\right). \tag{1}$$

Now we want to isolate the Legendre Symbol $(\frac{q}{p})$, so we can isolate it by dividing both sides by the product on the right-hand-side, yielding

$$\left(\frac{q}{p}\right) = \frac{\prod_{l=1}^{(p-1)/2} f(\frac{lq}{p})}{\prod_{l=1}^{(p-1)/2} f(\frac{l}{p})} = \prod_{l=1}^{(p-1)/2} \frac{f(\frac{lq}{p})}{f(\frac{l}{p})}.$$

By (1), this is

$$\left(\frac{q}{p}\right) = \prod_{l=1}^{(p-1)/2} \prod_{m=1}^{(q-1)/2} f\left(\frac{l}{p} + \frac{m}{q}\right) f\left(\frac{l}{p} - \frac{m}{q}\right). \tag{2}$$

We can compute an identical expression for $(\frac{p}{q})$ using the same techniques above, so that

$$\left(\frac{p}{q}\right) = \prod_{l=1}^{(p-1)/2} \prod_{m=1}^{(q-1)/2} f\left(\frac{m}{q} + \frac{l}{p}\right) f\left(\frac{m}{q} - \frac{l}{p}\right). \tag{3}$$

Using the fact that $f(-z) = -f(z)$ for the particular function in study, we can see that

$$f\left(\frac{m}{q} - \frac{l}{p}\right) = f\left[-\left(\frac{l}{p} - \frac{m}{q}\right)\right] = -f\left(\frac{l}{p} - \frac{m}{q}\right).$$

Substituting this expression into (3) and noticing the correspondence with (2), we thus have

$$\begin{aligned}\left(\frac{p}{q}\right) &= \prod_{l=1}^{(p-1)/2}\prod_{m=1}^{(q-1)/2} f\left(\frac{m}{q}+\frac{l}{p}\right)\left[-f\left(\frac{l}{p}-\frac{m}{q}\right)\right]\\ &= \left[\prod_{l=1}^{(p-1)/2}\prod_{m=1}^{(q-1)/2}(-1)\right]\left(\frac{q}{p}\right)\\ &= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right).\end{aligned}$$

This is simply a restatement of Quadratic Reciprocity as in $(*)$, so we are done. ■

4. Quadratic Reciprocity and Quadratic Gauss Sums

The introduction of primitive nth roots of unity in the previous section was very important for the this section. In this section, we will demonstrate a proof of Quadratic Reciprocity using Quadratic Gauss Sums.

4.1. **Some algebra.**

Before we may define Quadratic Gauss Sums and begin the proof, we must first introduce the notion of an algebraic integer, and show how it corresponds with our goal.

Definition 4.1. An algebraic integer is a complex number, often denoted ω, that is a root of a polynomial

$$x^n + b_1x^{n-1} + b_2x^{n-2} + \cdots + b_{n-1}x + b_n,$$

where all coefficients $b_1, b_2, b_3, \ldots, b_n \in \mathbb{Z}$.

We will not introduce the notion of an algebraic number because it is irrelevant to our objective in this section, but it can be defined similarly, where the coefficients of the polynomial in study has coefficients $a_1, a_2, a_3, \ldots, a_n \in \mathbb{Q}$, where $\mathbb{Q}$ is the set of all rational numbers. There is a clear correspondence between algebraic numbers and algebraic integers: every algebraic integer is an algebraic number, due to nearly the same reasons that every integer is a rational number.

Theorem 4.2. *The set of algebraic integers forms a ring.*

We will not prove this here, but this theorem will be of utmost importance to us later; it allows us to notice a correspondence between complex numbers in the form of congruence.

From now onward, we let Ω denote the ring of algebraic integers. If three algebraic integers $\omega_1, \omega_2, \gamma \in \Omega$, then we can say that

$$\omega_1 \equiv \omega_2 \pmod{\gamma}$$

if and only if it is true that $\omega_1 - \omega_2 = \gamma\alpha$, where $\alpha \in \Omega$. Notice that this is nearly identical to the definition of congruence over $\mathbb{Z}$; it is merely modified to accommodate for algebraic integers. This can be informally referred to as a "complex" definition of congruence. We will now prove some facts about algebraic integers, and use them to introduce Quadratic Gauss Sums later.

We will now establish a fact about the binomial coefficient $\binom{p}{k}$ where p is prime.

Lemma 4.3. *If p is a prime and $1 \leq k < p$, then*

$$p \mid \binom{p}{k}.$$

Proof. Recall that

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$

We may rewrite this expression as

$$p! = k!(p-k)!\binom{p}{k}.$$

Notice that $p \mid p!$, because that is the definition of the factorial. However, $p \nmid k!(p-k)!$, because all integers in $(p-k)!$ are indeed less than p, and therefore relatively prime to p. Since this is true, it must follow that

$$p \mid \binom{p}{k},$$

so we are done. ■

Now we will introduce an important theorem about congruence over the algebraic integers.

Theorem 4.4. *If $\omega_1, \omega_2 \in \Omega$ and $p \in \mathbb{Z}$ is a prime, then*

$$(\omega_1 + \omega_2)^p \equiv \omega_1^p + \omega_2^p \pmod{p}.$$

Proof. By the Binomial Theorem,

$$\begin{aligned}
(\omega_1 + \omega_2)^2 &= \sum_{k=0}^{p} \binom{p}{k} \omega_1^{p-k} \omega_2^k \\
&= \binom{p}{0} \omega_1^p \omega_2^0 + \cdots + \binom{p}{p} \omega_2^p \\
&= \omega_1^p + \binom{p}{1} \omega_1^{p-1} \omega_2 + \cdots + \binom{p}{p-1} \omega_1 \omega_2^{p-1} + \omega_2^p.
\end{aligned}$$

Notice that the expression within the $\cdots$ contains binomial coefficients ranging from $\binom{p}{1}$ to $\binom{p}{p-1}$. They are all divisible by p by Lemma **4.3** and therefore are congruent to 0 modulo p, so

$$\omega_1^p + \cdots + \omega_2^p \equiv \omega_1^p + \omega_2^p \pmod{p},$$

and we are finished. ■

We will use this fact later. Returning to our discussion on nth roots of unity, notice that in the polynomial equation $x^n - 1 = 0$ of degree n, any singular root of this polynomial equation must be an algebraic integer, because the coefficients satisfy the conditions for its roots to be algebraic integers (recall that the roots of this polynomial equation are $1, e^{2\pi i/n}, e^{2(2\pi i/n)}, e^{3(2\pi i/n)}, \ldots,$ and $e^{(n-1)(2\pi i/n)}$). This forms a link between algebraic integers and nth roots of unity, and we will now expand that idea a bit more.

4.2. **Quadratic Character of 2 modulo p using primitive 8th roots of unity.**

To prepare as a prerequisite to later generalizations, we will use an example of the computation and technique of computation of the quadratic character of 2.

Let us define a primitive 8th root of unity $\zeta = e^{2\pi i/8}$. This means that $\zeta^8 = 1$ or $\zeta^8 - 1 = 0$. We can factorize this so that $(\zeta^4 - 1)(\zeta^4 + 1) = 0$; notice that $\zeta^4 \neq 1$ because $e^{i\pi} = -1$ by Euler's Identity, so it must be that $\zeta^4 = -1$. We can modify this expression so that

$$\begin{aligned} \zeta^4 &= -1 \\ \zeta^{-2}\zeta^4 &= (-1)(\zeta^{-2}) \\ \zeta^2 + \zeta^{-2} &= 0. \end{aligned}$$

This relation is extremely important as it allows the derivation of the following:

$$(\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = 2.$$

Let $\tau = \zeta + \zeta^{-1}$. Since $\zeta, \zeta^{-1} \in \Omega$, by the definition of Ω, both τ and ζ are both roots of monic polynomials with integer coefficients, and are algebraic integers. Thus we can work with them in "complex" congruences.

Let $p \in \mathbb{Z}$ be an odd prime. Note that from the relation derived above, $\tau^2 = 2$. Notice that

$$\tau^{p-1} = (\tau^2)^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p}$$

by Euler's Criterion in Theorem **0.6**. Then we can see that

$$\tau^p \equiv \left(\frac{2}{p}\right)\tau \pmod{p}.$$

By Theorem **4.4**, this means that

$$\tau^p = (\zeta + \zeta^{-1})^p \equiv \zeta^p + \zeta^{-p} \pmod{p}.$$

If we recall that $\zeta^8 = 1$, then we can notice that there is a correspondence between conditions on p and the value of τ^p modulo p. If we allow $p \equiv \pm 1 \pmod 8$ and $p \equiv \pm 3 \pmod 8$, then we can see that

$$\tau^p = \begin{cases} \zeta + \zeta^{-1} & \text{if } p \equiv \pm 1 \pmod 8 \\ \zeta^3 + \zeta^{-3} & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

(We can show that the first equivalence is true by substituting $p = 8k + 1$ and $8k - 1$ for p. The second equivalence can be shown by recalling that $\zeta^4 = -1$, so that $\zeta^3 = -\zeta^{-1}$. Then $\zeta^3 + \zeta^{-3} = -\zeta^{-1} + (-\zeta^{-1})^{-1} = -(\zeta + \zeta^{-1}) = -\tau$.) In other words,

$$\zeta^p + \zeta^{-p} = \begin{cases} \tau & \text{if } p \equiv \pm 1 \pmod 8 \\ -\tau & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

Recalling the exponential expression in the expression for the Legendre Symbol of $(\frac{2}{p})$, notice that this means

$$\begin{aligned} (-1)^{\frac{p^2-1}{8}}\tau &\equiv \left(\frac{2}{p}\right)\tau \pmod p \\ (-1)^{\frac{p^2-1}{8}}(2) &\equiv \left(\frac{2}{p}\right)(2) \pmod p \\ (-1)^{\frac{p^2-1}{8}} &\equiv \left(\frac{2}{p}\right) \pmod p. \end{aligned}$$

where γ is some algebraic integer. To show why this implies that

$$(-1)^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right)$$

is true, consider some $a \in \mathbb{Q}$ and $a \in \Omega$, where $\mathbb{Q}$ denotes the rationals. Then a is also a rational integer, hence an ordinary integer. Previously we had the assertion that if two numbers that are ± 1 are congruent to each other modulo p, then they must be equivalent. We can extend this argument to be true - hence proving our assertion here - for algebraic integers as well. Thus, by using the statement above, we can conclude that the statement below

$$(-1)^{\frac{p^2-1}{8}} - \left(\frac{2}{p}\right) = p\gamma, \tag{1}$$

where $\gamma \in \Omega$, is equivalently a statement about integers. Since we have reduced this problem from algebraic integers to the ordinary integers, we can proceed as follows. Assuming $\gamma \neq 0$, then it must be that $|\gamma| \geq 1$; this is because if $\gamma = 0$, then immediately we would have $(-1)^{\frac{p^2-1}{8}} = (\frac{2}{p})$, and our assertion is true. Also, p is an odd prime, so $|p| \geq 3$. Notice that the left-hand-side of (1) is going to be constrained to $-2, 0$, or 2 because either number will be -1 or 1. Therefore, by (1), we have that

$$\left|(-1)^{\frac{p^2-1}{8}} - \left(\frac{2}{p}\right)\right| = |p| \cdot |\gamma| \geq 3 \cdot 1 = 3.$$

However, we showed above that $(-1)^{\frac{p^2-1}{8}} - (\frac{2}{p})$ is either $-2, 0$, or 2, so we have a contradiction, and our original assumption that $\gamma \neq 0$ is false. Thus $\gamma = 0$, and we have

$$(-1)^{\frac{p^2-1}{8}} - \left(\frac{2}{p}\right) = 0$$
$$(-1)^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right),$$

and we have proven our assertion.

What we have done here is derive the value of the Legendre Symbol $(\frac{2}{p})$ (or the quadratic character of 2 modulo p prime) using primitive 8th roots of unity.

4.3. **Quadratic Gauss Sums.** What we will do next is utilize a generalization of this technique to derive Quadratic Reciprocity. We allow $\zeta = e^{2\pi i/p}$, a pth primitive root of unity, in the following. We define the following two lemmas which will be of use when defining a Quadratic Gauss Sum.

Lemma 4.5. *The expression*

$$\sum_{t=0}^{p-1} \zeta^{at} = \begin{cases} p & \text{if } a \equiv 0 \pmod{p} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If $a \equiv 0 \pmod{p}$, then a may be written as kp for some $k \in \mathbb{Z}$. If we substitute kp for a in ζ^a, then we can see that $\zeta^a = \zeta^{kp} = e^{kp(2\pi i/p)} = e^{2k\pi i}$. Since every multiple of 2π when rotating counterclockwise will always return to 1, it is true that $e^{2k\pi i} = \zeta^a = 1$. Substituting this back into the sum, it is thus clear that

$$\sum_{t=0}^{p-1} \zeta^{at} = \sum_{t=0}^{p-1} 1^t = p.$$

Now considering the case otherwise, we see by the sum of a geometric series that

$$\sum_{t=0}^{p-1} \zeta^{at} = \frac{1(1-\zeta^{ap})}{1-\zeta^a} = \frac{\zeta^{ap}-1}{\zeta^a - 1} = \frac{0}{\zeta^a - 1} = 0.$$

∎

Corollary 4.6. *It is true that*

$$p^{-1} \sum_{t=0}^{p-1} \zeta^{t(x-y)} = \delta(x, y),$$

where

$$\delta(x, y) = \begin{cases} 1 & \text{if } x \equiv y \pmod{p} \\ 0 & \text{if } x \not\equiv y \pmod{p}. \end{cases}$$

Proof. This result can be derived by substituting $t = x - y$ in Lemma **4.5**. We begin by considering two cases. If $x - y \equiv 0 \pmod{p}$, then it is clear that, if we allow some $t = x - y$ that, by Lemma **4.5**,

$$p^{-1}\sum_{t=0}^{p-1}\zeta^{\beta t} = p^{-1}(p) = 1,$$

which is indeed the implication of $x \equiv y \pmod{p}$.

Considering the next case, if $x - y \not\equiv 0 \pmod{p}$, then we can see by the sum of a geometric series that

$$p^{-1}\sum_{t=0}^{p-1}\zeta^{t(x-y)} = p^{-1}\left[\frac{1(1-(\zeta^{x-y})^{p}}{1-\zeta^{p}}\right] = p^{-1}\left(\frac{1-\zeta^{p(x-y)}}{1-\zeta^{p}}\right) = p^{-1}\left(\frac{0}{1-\zeta^{p}}\right) = 0,$$

so we have proven the second case. ■

The next lemma is a reconsideration of a previous statement regarding the equivalence of the number of quadratic residues and quadratic nonresidues in Section 0.

Lemma 4.7. *The sum*

$$\sum_{t=0}^{p-1}\left(\frac{t}{p}\right) = 0.$$

Proof. It is true that there are an equal number of quadratic residues and quadratic nonresidues modulo p. Since there are an equal number of quadratic residues and quadratic nonresidues, and their values fluctuate between 1 and -1, their sum must be 0. ■

We are now in a position to define a Quadratic Gauss Sum.

Definition 4.8. The Quadratic Gauss Sum is defined as

$$g_a = \sum_{t=0}^{p-1}\left(\frac{t}{p}\right)\zeta^{at},$$

where $p \in \mathbb{Z}$ is prime, $a, t \in \mathbb{Z}$, and ζ is a primitive pth root of unity.

Leading toward yet another proof of Quadratic Reciprocity, we will prove several important properties of the Quadratic Gauss Sum.

Proposition 4.9.

$$g_a = \left(\frac{a}{p}\right)g_1.$$

Proof. We consider two cases. If $a \equiv 0 \pmod{p}$, then a may be written as kp for some $k \in \mathbb{Z}$. Then $\zeta^{at} = e^{kp(2\pi i/p)t} = e^{(2k\pi i)t} = 1^t = 1$. Substituting this expression into the Quadratic Gauss Sum, we see that this means

$$g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right),$$

which is, by Lemma **4.7**, equivalent to 0. Now looking to the statement of the Proposition, if $a \equiv 0 \pmod{p}$, then the Legendre Symbol $(\frac{a}{p}) = 0$ by Proposition **0.3**. Thus the statement is true for $a \equiv 0 \pmod{p}$.

If $a \not\equiv 0 \pmod{p}$, then we can write

$$\begin{aligned} \left(\frac{a}{p}\right) g_a &= \left(\frac{a}{p}\right) \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{at} \\ &= \sum_{t=0}^{p-1} \left(\frac{a}{p}\right)\left(\frac{t}{p}\right) \zeta^{at} \\ &= \sum_{t=0}^{p-1} \left(\frac{at}{p}\right) \zeta^{at}. \end{aligned}$$

Notice that the numerator of the Legendre Symbol and the power of ζ are the same. We take $at = x$. Then

$$\sum_{t=0}^{p-1} \left(\frac{at}{p}\right) \zeta^{at} = \sum_{t=0}^{p-1} \left(\frac{x}{p}\right) \zeta^{x}.$$

Notice that at runs through a complete residue system modulo p, ranging from 0 to $p-1$. Since we replaced it with x, x must as well since the product within the sum depends only on the residue class of x, so, by the evaluation of g_1,

$$\sum_{t=0}^{p-1} \left(\frac{x}{p}\right) \zeta^{x} = g_1.$$

Comparing with the evaluation of the Quadratic Gauss Sum at $a = 1$, we see that

$$g_1 = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{t},$$

which is the exact form of what we just derived. Then the statement is true for $a \not\equiv 0 \pmod{p}$.

To finish, notice that we can rewrite, by Proposition **0.3**,

$$\left(\frac{a}{p}\right)g_a = g_1$$
$$g_a = \left(\frac{a}{p}\right)g_1,$$

and we are done. ■

The next proposition will interlink Quadratic Reciprocity and Quadratic Gauss Sums. In the following statement, we will allow g_1 to be g as a change in notation for ease of use.

From Proposition **4.9**, it can be seen that $g_a^2 = g^2$ by squaring the left-hand-side and right-hand-side.

In the next proposition, we will see the significance of a particular value, denoted $p^* = (-1)^{\frac{p-1}{2}}p$. In fact, this value is equivalent to g^2, as we will see in the following.

Proposition 4.10.

$$g^2 = (-1)^{\frac{p-1}{2}}p = p^*.$$

Proof. Much like the previous proofs, our goal in this proof is to derive two different instances of the same things, and then equate them to show their correspondence. What we will do here is analogous, but we will evaluate the sum

$$\sum_{a=0}^{p-1} g_a g_{-a}$$

in two different ways. In the case that $a \not\equiv 0 \pmod{p}$, by Proposition **4.9** we can evaluate the interior of the sum as

$$\begin{aligned} g_a g_{-a} &= \left(\frac{a}{p}\right)g\left(\frac{-a}{p}\right)g \\ &= \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right)g^2. \end{aligned}$$

By Proposition **0.3**, this is

$$\left(\frac{-1}{p}\right)g^2.$$

Returning to the sum, we have

$$\begin{aligned} \sum_{a=0}^{p-1} g_a g_{-a} &= \sum_{a=0}^{p-1}\left(\frac{-1}{p}\right)g^2 \\ &= \left(\frac{-1}{p}\right)(p-1)g^2. \end{aligned}$$

We now consider the other representation of $g_a g_{-a}$. Taking x and y as the index of both sums for convenience,

$$\begin{aligned} g_a g_{-a} &= \sum_{x=0}^{p-1}\left(\frac{x}{p}\right)\zeta^{ax}\sum_{y=0}^{p-1}\left(\frac{y}{p}\right)\zeta^{-ay} \\ &= \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{x}{p}\right)\zeta^{ax}\left(\frac{y}{p}\right)\zeta^{-ay} \\ &= \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\zeta^{a(x-y)}. \end{aligned}$$

Taking the sum of left-hand-side and right-hand-side, we have

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_{a=0}^{p-1}\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\zeta^{a(x-y)}.$$

By **4.6**, we can sum the right portion over a, so we have

$$\begin{aligned} \sum_{a=0}^{p-1}\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\zeta^{a(x-y)} &= \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\sum_{a=0}^{p-1}p^{-1}\zeta^{a(x-y)}\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)p \\ &= p\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\delta(x,y)\left(\frac{xy}{p}\right). \end{aligned}$$

Notice that by Proposition **0.3**, it is true that $x \equiv y \pmod{p}$. This means that, by definition, $\delta(x,y) = 1$. Then we can rewrite this expression as

$$p\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{xy}{p}\right).$$

Since x and y both run through the residues modulo p, their product must always be a square modulo p, so that the numerator of the Legendre Symbol $(\frac{xy}{p})$ is $0^2, 1^2, 2^2, \ldots, (p-1)^2$. However, since these are all squares, again by Proposition **0.3**, the Legendre Symbol is always 1, and so the sum to $p-1$ will simply be $p-1$. Thus

$$p\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{xy}{p}\right) = p(p-1).$$

Equating the two statements that we derived, we have that

$$\begin{aligned}\left(\frac{-1}{p}\right)(p-1)g^2 &= p(p-1)\\ \left(\frac{-1}{p}\right)g^2 &= p\\ g^2 &= \left(\frac{-1}{p}\right)p.\end{aligned}$$

By (a) of Theorem **0.7**,

$$g^2 = (-1)^{\frac{p-1}{2}}p,$$

so we are done. ■

Now that we are equipped with all relevant devices with which to prove Quadratic Reciprocity, we will do so. It is important to note that our previous realization of the allowed use of algebraic integers led to this result; it is obvious that integers are the only mathematical objects that should belong in modular congruences, yet the fact that primitive nth roots of unity are algebraic integers is the very realization that leads to the use of non-integer - even non-real - values in modular congruences.

Recall that $p^* = (-1)^{\frac{p-1}{2}}p$. Recall also that earlier, we wrote $\tau^2 = 2$, where $\tau = \zeta + \zeta^{-1}$, and also from Proposition **4.10**, $g^2 = p^*$. These two expressions are analogous, as they represent the same idea in different contexts. The first is a statement about primitive 8th roots of unity, while the second is a generalization to different expressions; namely, the forms of Quadratic Gauss Sums.

4.4. **Proof.** Now we will prove Quadratic Reciprocity by working with congruences modulo q over the ring of algebraic integers.

Proof of Quadratic Reciprocity. First, notice that

$$g^{q-1} = g^{2(\frac{q-1}{2})} = p^{*(\frac{q-1}{2})} \equiv \left(\frac{p^*}{q}\right) \pmod{q}, \tag{1}$$

by Euler's Criterion in Theorem **0.6**. By Theorem **4.4** and the Binomial Theorem, we have

$$\begin{aligned} g^q &= \left(\sum_{t=0}^{p-1}\left(\frac{t}{p}\right)\zeta^t\right)^q \\ &= \left[\left(\frac{0}{p}\right)\zeta^0 + \left(\frac{1}{p}\right)\zeta^1 + \cdots + \left(\frac{p-1}{p}\right)\zeta^{p-1}\right]^q \\ &\equiv \left[\left(\frac{0}{p}\right)\zeta^0\right]^q + \left[\left(\frac{1}{p}\right)\zeta^1\right]^q + \cdots + \left[\left(\frac{p-1}{p}\right)\zeta^{p-1}\right]^q \pmod q \\ &\equiv \sum_{t=0}^{p-1}\left(\frac{t}{p}\right)^q \zeta^{qt} \pmod q \\ &\equiv g_q \pmod q. \end{aligned}$$

By Proposition **4.9**, this is

$$g^q \equiv g_q \equiv \left(\frac{q}{p}\right) g \pmod q.$$

Using (1), we can write

$$\begin{aligned} g^{q-1}g &\equiv \left(\frac{q}{p}\right) g \pmod q \\ \left(\frac{q}{p}\right) g &\equiv \left(\frac{p^*}{q}\right) g \pmod q. \end{aligned}$$

Multiplying the left-hand-side and right-hand-side by g and substituting $g^2 = p^*$ from Proposition **4.10**, we obtain

$$\begin{aligned} \left(\frac{q}{p}\right) p^* &\equiv \left(\frac{p^*}{q}\right) p^* \pmod q \\ \left(\frac{q}{p}\right) &\equiv \left(\frac{p^*}{q}\right) \pmod q \\ \left(\frac{q}{p}\right) &= \left(\frac{p^*}{q}\right), \end{aligned}$$

since the left-hand-side are either 1 or -1, and are not changed modulo q. To see why this is Quadratic Reciprocity, notice that

$$\begin{aligned} \left(\frac{p^*}{q}\right) &= \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\frac{p}{q}\right) \\ \left(\frac{p^*}{q}\right) &= \left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\left(\frac{p}{q}\right). \end{aligned}$$

Since we established earlier that $(\frac{p^*}{q}) = (\frac{q}{p})$, we can write

$$\begin{aligned}\left(\frac{q}{p}\right) &= \left[(-1)^{\frac{p-1}{2}}\right]^{\frac{q-1}{2}}\left(\frac{p}{q}\right)\\ \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},\end{aligned}$$

which is the statement of Quadratic Reciprocity, and we are done. ■

5. Applications

In this section, we will utilize some previously determined results to explore several interesting applications of both Quadratic Reciprocity and the Legendre Symbol.

We will first introduce the Jacobi Symbol, which is a generalization of the the Legendre Symbol that possesses several interesting properties, such as multiplicativity, identity, and surprisingly, an analogous version of Quadratic Reciprocity. The Jacobi Symbol is useful for evaluating the quadratic character of a non-prime integer, and that will be the primary focus in the first part of this section.

We will then introduce and prove Fermat's Theorem on the Sum of Two Squares. Fermat's Theorem on the Sum of Two Squares uses the Method of Infinite Descent, which we will briefly introduce. The Method of Infinite Descent features two steps; namely, the Reciprocity Step, and then the Descent Step. As can be predicted, the Reciprocity Step utilizes several characteristics of Quadratic Reciprocity.

5.1. **Jacobi Symbol.** We begin by defining the Jacobi Symbol.

Definition 5.1 (Jacobi Symbol)**.** The Jacobi Symbol is defined as follows:

$$\begin{aligned}\left(\frac{a}{b}\right) &= \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\left(\frac{a}{p_3}\right)\cdots\left(\frac{a}{p_m}\right)\\ &= \prod_{i=1}^{m}\left(\frac{a}{p_i}\right),\end{aligned}$$

where the p_i are not necessarily distinct primes, and $b = p_1p_2p_3\cdots p_m$.

It is important to notice that the Jacobi Symbol is, by definition, no different from the Legendre Symbol. In its essence, it is a product of Legendre Symbols with modulus p, and can be evaluated as such; you first determine the prime factorization of the denominator of the Jacobi Symbol, and express it as a product of Legendre Symbols with modulus prime factors $p_1, p_2, p_3, \ldots, p_m$.

However, there is one important observation to make: the Jacobi Symbol does not always denote whether some a is a quadratic residue or quadratic nonresidue modulo some composite b. For example, we consider the Jacobi Symbol $(\frac{2}{15})$. Using the definition of the Jacobi Symbol, we have $(\frac{2}{15}) = (\frac{2}{3})(\frac{2}{5})$. We see that

$(\frac{2}{3}) = -1$ because $3 \equiv 3 \pmod 8$, and $(\frac{2}{5}) = -1$ because $5 \equiv 5 \pmod 8$, so $(\frac{2}{3})(\frac{2}{5}) = (-1)(-1) = 1$, but 2 is not a quadratic residue modulo 15.

Furthermore, unlike the Legendre Symbol, the Jacobi Symbol is not constrained by a prime denominator; especially with the following properties equipped, it will become increasingly clearer that the Jacobi Symbol drastically simplifies computation time. Rather than computing individual Legendre Symbols, we can instead use the properties of the Jacobi Symbol to produce analogous results in less time and with fewer computations.

We will now prove several properties of the Jacobi Symbol.

Proposition 5.2. *Let $b = p_1p_2p_3 \dots p_m$. The following statements are true:*

(1)
$$\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right) \iff a_1 \equiv a_2 \pmod b$$

(2)
$$\left(\frac{a_1a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$$

(3)
$$\left(\frac{a}{b_1b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right).$$

Proof. To prove (1), recall the properties of the Legendre Symbol in Proposition **0.3**; since $b = p_1p_2p_3 \dots p_m$, we can use the definition of the Jacobi Symbol to expand the expression so that we have a series of equivalences of Legendre Symbols, so

$$\left(\frac{a_1}{p_1}\right) = \left(\frac{a_2}{p_1}\right), \left(\frac{a_1}{p_2}\right) = \left(\frac{a_2}{p_2}\right), \dots, \left(\frac{a_1}{p_m}\right) = \left(\frac{a_2}{p_m}\right).$$

Then

$$\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right).$$

To prove (2), we begin with

$$\prod_{i=1}^{m} \left(\frac{a_1a_2}{p_i}\right)$$

by definition. By Proposition **0.6**, this is

$$\begin{aligned}\prod_{i=1}^{m} \left(\frac{a_1a_2}{p_i}\right) &= \prod_{i=1}^{m} \left(\frac{a_1}{p_i}\right)\left(\frac{a_2}{p_i}\right)\\ &= \prod_{i=1}^{m} \left(\frac{a_1}{p_i}\right) \prod_{i=1}^{m} \left(\frac{a_2}{p_i}\right),\end{aligned}$$

and we are done.

Notice that (3) is a simplification of the definition of the Legendre Symbol. ■

We will not prove the following two statements here, but they will be of use in our proof of the properties of the Jacobi Symbol that resemble that of Quadratic Reciprocity.

Lemma 5.3. *Let r and s be odd integers.*

(1)
$$\frac{rs-1}{2} \equiv \frac{r-1}{2} + \frac{s-1}{2} \pmod 2$$

(2)
$$\frac{r^2s^2-1}{8} \equiv \frac{r^2-1}{8} + \frac{s^2-1}{8} \pmod 2.$$

Corollary 5.4. *Let $r_1, r_2, r_3, \ldots, r_m$ be odd integers.*

(1)
$$\sum_{i=1}^{m} \frac{r_i-1}{2} \equiv \frac{r_1r_2r_3\cdots r_m-1}{2} \pmod 2$$

(2)
$$\sum_{i=1}^{m} \frac{r_i^2-1}{8} \equiv \frac{r_1^2r_2^2r_3^2\cdots r_m^2-1}{8} \pmod 2.$$

We now proceed to prove the analog of Theorem **0.7** for the Jacobi Symbol.

Theorem 5.5 (Analogue of Quadratic Reciprocity for Jacobi Symbols)**.** *Let $b = p_1p_2p_3\cdots p_m$. Then*

(a)
$$\left(\frac{-1}{b}\right) = (-1)^{\frac{p-1}{2}}$$

(b)
$$\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$$

(c) *If $a, b < 0$ are odd, then*
$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}.$$

Proof. To prove (a), first notice that

$$\begin{aligned}\left(\frac{-1}{b}\right) &= \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\left(\frac{-1}{p_3}\right)\cdots\left(\frac{-1}{p_m}\right)\\ &= (-1)^{\frac{p_1-1}{2}}(-1)^{\frac{p_2-1}{2}}(-1)^{\frac{p_3-1}{2}}\cdots(-1)^{\frac{p_m-1}{2}}\\ &= (-1)^{\sum_{i=1}^{m}\frac{p_i-1}{2}}\end{aligned}$$

by (a) in Theorem **0.7**. By Corollary **5.4**, this is

$$\begin{aligned}(-1)^{\sum_{i=1}^{m}\frac{p_i-1}{2}} &= (-1)^{\frac{p_1p_2p_3\cdots p_m-1}{2}}\\ &= (-1)^{\frac{b-1}{2}}.\end{aligned}$$

To prove (b), first notice that

$$\begin{aligned}\left(\frac{2}{b}\right) &= \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\left(\frac{2}{p_3}\right)\cdots\left(\frac{2}{p_m}\right)\\ &= (-1)^{\frac{p_1^2-1}{8}}(-1)^{\frac{p_2^2-1}{8}}(-1)^{\frac{p_3^2-1}{8}}\cdots(-1)^{\frac{p_m^2-1}{8}}\\ &= (-1)^{\sum_{i=1}^{m}\frac{p_i^2-1}{8}}\end{aligned}$$

By Corollary **5.4**, this is

$$\begin{aligned}(-1)^{\frac{p_1^2p_2^2p_3^2\cdots p_m^2-1}{8}} &= (-1)^{\frac{(p_1p_2p_3\cdots p_m)^2-1}{8}}\\ &= (-1)^{\frac{b^2-1}{8}}.\end{aligned}$$

To begin proving (c), let $a = q_1q_2q_3\cdots q_l$. Then

$$\begin{aligned}\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) &= \prod_{j=1}^{l}\prod_{i=1}^{m}\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right)\\ &= (-1)^{\sum_{j=1}^{l}\sum_{i=1}^{m}\frac{q_j-1}{2}\cdot\frac{p_i-1}{2}}\end{aligned}$$

by Quadratic Reciprocity in Theorem **0.7**. Then by Corollary **5.4**, notice that

$$\begin{aligned}\sum_{j=1}^{l}\sum_{i=1}^{m}\frac{q_j-1}{2}\cdot\frac{p_i-1}{2} &\equiv \frac{q_1q_2q_3\cdots q_l-1}{2}\cdot\frac{p_1p_2p_3\cdots p_m-1}{2} \pmod 2\\ &\equiv \frac{a-1}{2}\cdot\frac{b-1}{2} \pmod 2,\end{aligned}$$

which can be substituted to yield the Jacobi analogue of the Law of Quadratic Reciprocity, so we are done. ■

5.2. **Fermat's Theorem on the Sum of Two Squares.** As can be seen above, the Jacobi Symbol is a rather versatile tool that can be used to study other areas of reciprocity, including in higher reciprocity.

We will now introduce Fermat's Theorem on the Sum of Two Squares. The statement of the theorem is as follows.

Theorem 5.6. *Given $x, y \in \mathbb{Z}$ and p a prime, the Diophantine equation $x^2+y^2 = p$ has solutions for primes of the form $p \equiv 1 \pmod 4$ and does not have solutions for primes of the form $p \equiv 3 \pmod 4$.*

Alternatively, we can restate this theorem as two conditional statements:

(a) *If p is a sum of two squares, then $p \equiv 1 \pmod 4$.*

(b) *If* $p \equiv 1 \pmod 4$*, then it is a sum of two squares.*

Before we may begin to prove this statement, we must prove a particularly beautiful lemma that will be used throughout the proof.

Lemma 5.7.

$$(a^2+b^2)(c^2+d^2) = (ad+bc)^2 + (ac-bd)^2.$$

Proof. The proof can follow by simply expanding the above, but that is of no interest. In fact, this identity describes an important characteristic of complex numbers. We can restate the identity as

$$|z_1 z_2| = |z_1||z_2|,$$

where $z_1 = a + bi$ and $z_2 = c + di$ are complex numbers, and the absolute value denotes modulus. Recalling that $i^2 = -1$, we have

$$\begin{aligned} |(a+bi)(c+di)| &= |a+bi||c+di| \\ |ac+adi+bic+bdi^2| &= \sqrt{a^2+b^2}\sqrt{c^2+d^2} \\ |(ac-bd)+i(ad+bc)| &= \sqrt{(a^2+b^2)(c^2+d^2)} \\ \sqrt{(ac-bd)^2+(ad+bc)^2} &= \sqrt{(a^2+b^2)(c^2+d^2)} \\ (ac-bd)^2+(ad+bc)^2 &= (a^2+b^2)(c^2+d^2), \end{aligned}$$

which is what we sought to prove. ■

This will be of use later.

In order to prove Theorem **5.6**, we must prove each of its two conditional statements (a) and (b). We will begin by proving (a) in two different ways.

Proof I of (a) in Theorem 5.6. In order for the condition to be satisfied, notice that p must be of the form $4k+1$ for some $k \in \mathbb{Z}$, which is an odd number. This means that we must find certain conditions on x and y that guarantee that the sum of their squares is odd. Through some experimentation, it can be seen that

$$\text{odd}^2 + \text{even}^2 = \text{odd}$$

is the only compatible case. Since this is true, we can express each x and y as some $2k+1$ and $2m$ respectively, where $k, m \in \mathbb{Z}$. Then

$$\begin{aligned} p &= (2k+1)^2 + (2m)^2 \\ &= 4k^2 + 4k + 1 + 4m^2 \\ &= 4(k^2+m^2) + 4(k+m) + 1 \\ &\equiv 1 \pmod 4, \end{aligned}$$

and we are done. ■

Proof II of (a) in Theorem 5.6. This proof is by far easier. Take the expression and reduce the left-hand-side and right-hand-side modulo p. Then you obtain $x^2 \equiv -y^2 \pmod{p}$. Using Proposition **0.3**, we see that this means

$$\begin{aligned}\left(\frac{x^2}{p}\right) &= \left(\frac{-y^2}{p}\right)\\ 1 &= \left(\frac{-1}{p}\right)(1)\\ (-1)^{\frac{p-1}{2}} &= 1.\end{aligned}$$

By Theorem **0.7**, this is the condition for $p \equiv 1 \pmod{4}$, so we are done. ■

What is shown above may be referred to as the Reciprocity Step. Before proving the converse, we must first briefly introduce the notion of Infinite Descent. This will be used to prove the Descent Step, which is part (b) of Theorem **5.6**.

Let us begin with the expression $x_1^2 \equiv -y_1^2 \pmod{p}$, or $x_1^2 + y_1^2 \equiv 0 \pmod{p}$. Then we can write $x_1^2 + y_1^2 = m_1 p$ for some $m \in \mathbb{Z}$. The Descent Step involves finding two x_2 and y_2 such that $x_2^2 + y_2^2 = m_2 p$, where $m_2 < m_1 - 1$. In the event that $m_2 = p$, we are immediately done. Otherwise, we can repeat this process until the multiple of p reaches 1, and we have a sum of two squares.

To prove the Descent Step in Theorem **5.6**, we must illustrate the entire process of Infinite Descent in the Context of $p \equiv 1 \pmod{4}$. This will prove the theorem.

The Method of Infinite Descent for $p \equiv 1 \pmod{4}$ is as follows:

(1) Let $p \equiv 1 \pmod{4}$ for some prime p.

(2) Write the expression $x^2 + y^2 = Mp$ for some $M < p$, as described earlier. The number M is a factor of p, and can be used as an auxiliary value.

(3) Select two numbers α and β with the properties that

$$\begin{aligned}\alpha &\equiv x \pmod{M}\\ \beta &\equiv y \pmod{M}.\end{aligned}$$

These values satisfy the condition that

$$-\frac{1}{2}M \leq \alpha, \beta \leq \frac{1}{2}M.$$

(4) By Properties of Congruences, it is true that

$$\begin{aligned}\alpha^2 + \beta^2 &\equiv x^2 + y^2\\ &\equiv 0 \pmod{M}.\end{aligned}$$

Then we can write

$$\begin{aligned}\alpha^2 + \beta^2 &= Mr\\ x^2 + y^2 &= Mp,\end{aligned}$$

for some $1 \leq r < M$.

(5) We multiply these expression to obtain

$$(x^2+y^2)(\alpha^2+\beta^2) = M^2 rp$$

By Lemma **5.7**, this is simply

$$(\alpha x+\beta y)^2 + (\alpha y - \beta x)^2 = M^2 rp.$$

(6) Dividing by M^2, we obtain

$$\left(\frac{\alpha x+\beta y}{M}\right)^2 + \left(\frac{\alpha y-\beta x}{M}\right)^2 = rp.$$

To show why this is possible, we have to show that $\alpha x + \beta y \equiv 0 \pmod{M}$ and $\alpha y - \beta x \equiv 0 \pmod{M}$, or they are both multiples of M. Recalling that $\alpha \equiv x \pmod{M}$ and $\beta \equiv y \pmod{M}$, we have

$$\alpha\alpha + \beta\beta \equiv 0 \pmod{M}$$
$$\alpha x + \beta y \equiv 0 \pmod{M},$$

so $\alpha x + \beta y$ is a multiple of M. For $\alpha y - \beta x$, we have

$$\alpha y - \beta x \equiv xy - yx \equiv 0 \pmod{M},$$

so that $\alpha y - \beta x$ is a multiple of M, and we are done.

Given the original condition that $r < M$, we have thus found a multiple of p that is smaller than what it was prior to reduction.

If $r \neq 1$, then we can repeat this process until $r = 1$, yielding a sum of two squares.

What we have just shown above is the complete Method of Infinite Descent. Since we provided the condition for $p \equiv 1 \pmod{4}$, this proves the converse of (a) in Theorem **5.6**. Thus we are done.

Acknowledgements

The author would like to thank Simon Rubinstein-Salzedo for assisting in proofs and comprehension of material, and Neel Murthy for incredibly informative discussions.

References

[Alm19] Awatef Noweafa Almuteri. *Quadratic Reciprocity: Proofs and Applications.* The University Of Mississippi eGrove, 2019.

[Cox11] David A Cox. *Primes of the form x2+ ny2: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011.

[IRR90] Kenneth Ireland, Michael Ira Rosen, and Michael Rosen. *A classical introduction to modern number theory*, volume 84. Springer Science & Business Media, 1990.

[Sil14] Joseph H Silverman. *A friendly introduction to number theory.* Pearson, 2014.