ON FINITE FIELDS AND HIGHER RECIPROCITY

MATIAS CARL RELYEA

Abstract. Cubic and biquadratic reciprocity have long since been referred to as "the forgotten reciprocity laws", largely since they provide special conditions that are widely considered to be unnecessary in the study of number theory. However, this paper aims to approach reciprocity with ample detail to motivate its existence. In this exposition of finite fields and higher reciprocity, we will begin by introducing concepts in abstract algebra and elementary number theory. This will motivate our approach toward understanding the structure and then existence of finite fields, especially with a focus on understanding the multiplicative group $\mathbb{F}^*$. While surveying finite fields we will provide another proof of quadratic reciprocity. We will proceed to investigate properties of the general multiplicative character, covering the concept of a general Gauss sum as well as basic notions of the Jacobi sum. From there we will begin laying the foundations for the cubic reciprocity law, beginning with a classification of the primes and units of the Eisenstein integers, denoted $\mathbb{Z}[\omega]$, and further investigations into the residue class ring $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ for π prime, which is predominantly the world in which cubic reciprocity lies.

We will then use multiplicative characters to define the cubic residue character and state cubic reciprocity in its entirety. Following this, we provide a proof of the cubic reciprocity law as well as its supplementary theorems using cubic Gauss sums. We will finish the section on cubic reciprocity with a brief survey of the cubic residue character of the even prime 2 and state a significant result due to Gauss that summarizes the conditions for 2 to be a cubic residue.

We conclude with the statement of biquadratic reciprocity and provide a brief discussion on how it relates to cubic reciprocity in both its proof and usage of the analogy between the Eisenstein integers, $\mathbb{Z}[\omega]$, and the Gaussian integers, $\mathbb{Z}[i]$.

Contents

Date: Summer 2024.

Introduction

Reciprocity laws have been studied for over 200 years. As of now, there exist over 300 proofs of quadratic reciprocity, but there exist far fewer proofs of cubic and biquadratic reciprocity. Quadratic reciprocity, the first reciprocity law, was proven by Carl Friedrich Gauss in 1796, and he deemed it the "Theorema Aureum", or "Golden Theorem". Gauss went on to prove quadratic reciprocity in 6 different ways, with 2 more posthumously. Unlike other techniques, one particular technique used, which certainly wouldn't have been named what it is named now, was quadratic Gauss sums. The formulation of quadratic Gauss sums would become the first step toward investigating higher reciprocity laws. Gotthold Eisenstein first published his proof of cubic reciprocity in 1844, and it used the techniques of Gauss and Jacobi sums. In 1850, Eisenstein published his paper on generalized higher reciprocity, a result now known as Eisenstein reciprocity. Even though Eisenstein reciprocity eventually became a direct corollary to work completed by Emil Artin on higher reciprocity using class field theory in the earlier 20th century, it became the first formal law for reciprocity of odd primes. Though Eisenstein reciprocity is a generalisation of cubic and biquadratic reciprocity and is highly relevant to modern research regarding reciprocity laws and algebraic number theory, it lies beyond the scope of this paper.

Quadratic reciprocity asks the question: under what conditions does the congruence $x^2 \equiv a \pmod{p}$ have solutions? Cubic reciprocity asks a similar question: under what conditions does the congruence $x^3 \equiv a \pmod{p}$ have solutions? The difference is subtle, but cubic reciprocity demands significantly more mechanics, and this is primarily what we will address in this paper.

This paper seeks to explore 3 reciprocity laws: a proof of quadratic reciprocity, a more familiar result in the context of finite fields; a proof of cubic reciprocity; and finally the statement of the law of biquadratic reciprocity. The preliminary section introduces necessary technical and conceptual preliminaries. Section 1 defines, states, and proves facts concerning the structure and existence of finite fields. Section 2 focuses primarily on motivating the study of multiplicative characters alongside Gauss and Jacobi sums. Section 3 states and proves cubic reciprocity and provides a sketch for the cubic character of 2. Section 4 concludes the paper with an overview of the different components needed for the proof of biquadratic reciprocity.

As we see in section 1, finite fields play an important role in higher reciprocity. In this paper, we survey the finite field $\mathbb{F}$ of order p and its multiplicative subgroup $\mathbb{F}^*$ of order $p-1$. While the construction and existence of this finite field are important facts of theory covered in section 1, we use them primarily to show that a residue class ring involving the Eisenstein integers $\mathbb{Z}[\omega]$ and an element of $\mathbb{Z}[\omega]$, introduced in section 3, are a finite field. This forms an important connection between algebra and cubic reciprocity and uses objects such as associates, norms, etc. that we are already familiar with. Since cubic reciprocity is considered over the finite field $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ for π a prime in $\mathbb{Z}[\omega]$, it is only logical that biquadratic reciprocity will be considered over the

finite field $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ for π a prime in $\mathbb{Z}[i]$, where $\mathbb{Z}[i]$ is the Gaussian integers. We will omit many of the details relating to Gaussian integers as it lies beyond the general scope of this paper, but [IRR90] gives a strict yet enlightening overview of its intricacies.

Though this paper aims to introduce finite fields and higher reciprocity to a fairly new reader, it also assumes a certain degree of abstract mathematics knowledge. We assume fluency with elementary number theory and most of algebra with the exception of some facts from ring theory that are introduced when needed. [Gal02] is an excellent resource for understanding and gaining useful insight on the group-theoretic and ring-theoretic portions of this paper. We also assume familiarity with the definitions of the algebraic integers and algebraic numbers as well as their algebraic structures; for instance, that the algebraic integers form a ring and that the algebraic numbers form a field. Everything in relation to finite fields is constructed from elementary principles with the exception of some facts and definitions about fields. As stated in the abstract, immediately following finite fields - the backbone of much of what we will do here - we will survey multiplicative characters and their uses, especially in the context of cubic residue characters. This leads naturally into an elegant proof of cubic reciprocity after surveying the Eisenstein integers.

This expository work is a continuation of previous work done in [CR22] related to quadratic reciprocity. For more insightful information about the history of early higher reciprocity, [Col77] is an excellent introduction. As mentioned earlier, [IRR90] is an extensive text not only for higher reciprocity but for algebraic number theory as well, and contains a proof for Eisenstein reciprocity for interested and advanced readers. [Rou12] provides even more detailed proofs for cubic reciprocity and its supplements. Many algebraic results that we do not prove may be found in [Gal02], and even so it is a wonderful text to gain further insight into finite fields.

Preliminaries

0.1. **Algebra.** Much of the algebra used in this paper is self-contained, in that any algebraic definitions or theorems used are largely either stated or proven before they are needed. Readers who are unfamiliar with more basic algebra, for instance that of groups, may find the opening chapters of [Gal02] illuminating. Many later chapters of this textbook also cover the theory of finite fields in more detail and are interesting in their own right. Knowledge of ring theory is also assumed, but we will state and prove several of the larger results when they are needed.

Definition 1 (Homomorphism)**.** We define a *homomorphism* to be a structure preserving mapping from one set to another set of the same type. In other words, if A and B are two sets of the same type, then under the mapping $\phi : A \to B$, it is true for all $(x, y) \in A$ that

$$\phi(xy) = \phi(x)\phi(y).$$

In this paper we will be utilising multiple types of homomorphisms, namely *group homomorphisms* and *ring homomorphisms*, which in practice are functionally identical. Each homomorphism also possesses a *kernel*.

Definition 2 (Kernel of a Homomorphism)**.** Let ϕ be a homomorphism defined with $\phi : A \to B$, and let B have some identity element e. We define the *kernel* of ϕ to be

$$\mathrm{Ker}(\phi) = \{x \in A | \phi(x) = e\}.$$

In other words, the kernel of ϕ is the set of elements in A that map to the identity element of B.

Much of the results that we are concerned with utilize ring theory, so we will define some basic objects. Ideals are analogous to normal subgroups in group theory. In the following definitions we let R be a commutative ring.

Definition 3 (Associate)**.** We say two members of R are *associate* if for $r, s \in R$ there exists some unit $u \in R$ such that $r = us$. In this case we say that r is associate to s.

Definition 4 (Ideal)**.** We define an *ideal* to be a subring $\overline{R} \subset R$ such that for every $r \in R$ and every $a \in \overline{R}$, both $ar, ra \in \overline{R}$.

Definition 5 (Maximal Ideal)**.** Some ideal $\overline{R}$ is a *maximal ideal* if whenever there is some ideal B of R with $\overline{R} \subseteq B \subseteq R$, either $B = \overline{R}$ or $B = R$. In other words, it is the largest ideal of R that is not R. An ideal of R is *proper* if it is not the entirety of R.

Definition 6 (Prime Ideal)**.** Some ideal $\overline{R}$ is a *prime ideal* if for the product $ab \in R$, then either a or b is in $\overline{R}$.

A prime ideal is in fact a ring-theoretic analogue to Euclid's Lemma.

Definition 7 (Principal Ideal)**.** Some ideal $\overline{R}$ is a *principal ideal* if it can be generated by a singular element.

Definition 8 (Integral Domain)**.** We define an *integral domain* to be a nonzero commutative ring.

Integral domains are generalizations of the ring of integers, and the product of any two members yields a nonzero output.

Definition 9 (PID)**.** An integral domain is a *principal ideal domain*, conventionally a *PID*, if every proper ideal of the integral domain is principal.

Definition 10 (Euclidean Domain)**.** Some integral domain R is a Euclidean domain if there exists some function λ, known as the *norm*, that maps the nonzero elements of R to $\mathbb{Z}_{\geq 0}$ such that if there exist some $a, b \in R$ with $b \neq 0$, then there also exist some $c, d \in R$ with the property that $a = cb + d$ and either $d = 0$ or $\lambda(d) < \lambda(b)$.

Essentially, a Euclidean domain asserts the existence of a division algorithm (more specifically, the Euclidean algorithm) over a ring.

Remark 1. It can be seen that $k[x]$ for some field k is a Euclidean domain, as we can map polynomials from $k[x]$ to the degrees of polynomials from $\mathbb{Z}_{\geq 0}$ via the norm.

Definition 11 (UFD)**.** An integral domain R is a *unique factorization domain*, conventionally *UFD*, if every nonzero element of x in R may be written as a product of some unit $u \in R$ and some finite number of irreducible elements p_i as follows:

$$x = up_1p_2 \cdots p_n.$$

Furthermore, this representation is unique in that any other x that can represented in the same way must have a bijection between its irreducible elements and p_i with $1 \leq i \leq n$.

Remark 2. Integral domains, Euclidean domains, PIDs, and UFDs are ultimately what we will use to study finite fields later in section 1. A diagram of their class inclusions may be described as follows.

field $\subset$ Euclidean domain $\subset$ PID $\subset$ UFD $\subset$ integral domain

Figure 1. Diagram of class inclusions for algebraic structures

Class inclusions are useful because they allow us to make statements about complex algebraic structures when working with simpler algebraic structures.

We show in Theorem 0.1 that every Euclidean domain is a PID. It is also possible to show that every PID is a UFD and that every UFD is an integral domain. We will not do this, but

in the case of $\mathbb{Z}[\omega]$, the Eisenstein integers, we note that since it is a UFD it is also an integral domain.

We define a field more rigorously in Section 1.

Theorem 0.1 (Every Euclidean domain is a PID)**.** *If R is an integral domain and $I \subseteq R$ is an ideal, then there exists some element $a \in R$ such that $I = Ra = aR = \{ra = ar | r \in R\}$. This is necessarily the requirement to be a PID.*

Proof. We proceed by double inclusion. First consider the set of nonnegative integers given by $\{\lambda(b) | b \in I, b \neq 0\}$. By well-ordering, every nonnegative set of integers must have a lowest term; we call this term $a \in I, a \neq 0$ with the property that $\lambda(a) \leq \lambda(b)$ for all $b \in I, b \neq 0$. We claim that $I = Ra = aR$, namely that the ideal I is generated by a. By the definition of I, we know that $Ra = aR \subseteq I$. We want to show that $I \subseteq Ra = aR$. To begin, we know that since I is a subring of R, it retains the properties of R and is thus a Euclidean domain. Namely, for any $b \in I$, there exist $c, d \in R$ such that $b = ca + d$ with either $d = 0$ or $\lambda(d) < \lambda(a)$. Clearly $d = b - ca \in I$, so it is not possible for $\lambda(d) < \lambda(a)$. Therefore $d = 0$, and so $b = ca$. Then $b = ca \in I$. Since we showed this for any b, it follows that $I = Ra = aR$, and thus every Euclidean domain is a PID. ■

In developing finite fields in section 1 we will need the following results.

Theorem 0.2 (Lagrange's Theorem; Gallian)**.** *Let G be a finite group and let H be a subgroup of G. Then the order of H divides the order of G. Furthermore, there are exactly $|G|/|H|$ distinct left or right cosets of H in G.*

Proof. The proof may be found in Chapter 7 of [Gal02]. ■

An important result that is necessary to prove Proposition 1.12 is the First Isomorphism Theorem, alternatively referred to as the Fundamental Theorem of Group Homomorphisms. The theorem can easily be extended to rings for our purposes, but we will only prove the theorem for groups.

Theorem 0.3 (First Isomorphism Theorem; Gallian)**.** *Let ϕ be a group homomorphism from a group G to $\overline{G}$. Then the mapping from the quotient group $G/Ker(\phi)$ to the image of ϕ given as $\phi(G)$ is an isomorphism, i.e.*

$$G/Ker(\phi) \approx \phi(G).$$

Before we can prove this theorem, let us first examine what the different components are. We will first examine the quotient group $G/\text{Ker}(\phi)$. This set is defined as $\{gH | g \in \text{Ker}(\phi)\}$ for H a normal subgroup of G, so we can write it as $g\text{Ker}(\phi)$ for all $g \in G$. The set $\phi(G)$ is also known as the image of G or $\text{im}(\phi)$. If we consider these simplifications, then we can write that the mapping is now defined as $g\text{Ker}(\phi) \to \phi(g)$ for all $g \in G$. Now we proceed with the proof.

Proof of Theorem 0.3. For the sake of convenience, we will use the function ψ to denote the mapping $g\text{Ker}(\phi) \to \phi(g)$. An isomorphism requires that the mapping between two groups preserve group operations and is one-to-one (namely, an injective function, so we necessarily need to show that the homomorphism is a function). To begin, we must first show that ψ is well-defined, or that for any g, the *LHS* of the mapping remains unique: that is, g is the only such coset representative that generates the coset. Suppose that there exist x, y such that $x\text{Ker}(\phi) = y\text{Ker}(\phi)$. Then, multiplying both sides by y^{-1} we have that $y^{-1}x \in \text{Ker}(\phi)$. Then, by the definition of the kernel, we have $e = \phi(y^{-1}x) = \phi(y^{-1})\phi(x) = (\phi(y))^{-1}\phi(x)$. Multiplying both sides by $\phi(y)$, this means that $\phi(x) = \phi(y)$, so we have shown that ψ is well-defined and ψ is a function. Next we need to show that ψ preserves operations. Notice that

$$\psi(x\text{Ker}(\phi)y\text{Ker}(\phi)) = \psi(xy\text{Ker}(\phi)) = \phi(xy) = \phi(x)\phi(y) = \psi(x\text{Ker}(\phi))\psi(y\text{Ker}(\phi)),$$

which indeed shows that the group operation is preserved. Finally, we need to show that ψ is one-to-one. Note that $\psi(g_1\text{Ker}(\phi)) = \psi(g_2\text{Ker}(\phi)) \implies \phi(g_1) = \phi(g_2)$. Multiplying both sides by $\phi(g_2)^{-1}$ we have $e = (\phi(g_2)^{-1}\phi(g_1) = \phi(g_2^{-1})\phi(g_1) = \phi(g_2^{-1}g_1)$. Therefore, by the definition of the kernel, $g_2^{-1}g_1 \in \text{Ker}(\phi)$. Hence $g_1\text{Ker}(\phi) = g_2\text{Ker}(\phi)$, proving that ψ is one-to-one. Thus the mapping ψ is an isomorphism. ■

To conclude this subsection, we include some definitions in elementary field theory that will be useful to the language we use in our investigation of the existence of finite fields. We formally define a field in section 1.

Definition 12 (Field Extension)**.** Let K and L be fields such that $K \subseteq L$ is a subfield of L. We define a field extension K of L, which we denote as L/K, to be a field such that K is a subfield of L. In this way, L is referred to as a *K-vector space* as it forms a vector space over the scalar field K.

We might say that L is a field extension, or simply *extension*, of K. A useful concept is the idea of an *intermediate field extension*. If L is an extension of F, and F is an extension of K, then F is an intermediate field extension. We now have a definition for the degree of a field extension. Let K and L be the same fields.

Definition 13 (Degree of a Field Extension)**.** We define the degree of a field extension, denoted $[K : L]$, to be the dimension of the vector space L over its scalar field K.

0.2. **Elementary Number Theory.** In this paper we assume a general knowledge of elementary number theory, including results such as Bézout's Lemma, Fermat's Little Theorem, quadratic reciprocity, and including other results concerning quadratic residues and nonresidues. Some specific concepts such as primitive roots and units will be introduced as needed. Let (a/p) denote the Legendre symbol.

Lemma 0.4. *Let* $\gcd(a, p) = 1$ *and* $a, b \in \mathbb{Z}$ *for* p *prime. Then*

(1)
$$a \equiv b \pmod{p} \iff \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

(2)
$$\left(\frac{0}{p}\right) = 0$$

(3)
$$\left(\frac{a^2}{p}\right) = 1.$$

Proof. The proof of this may be found in the preliminary section of [CR22]. Everything follows through the definition of the Legendre symbol. ■

Lemma 0.5. *Let* p *prime,* $\gcd(a, p) = 1$*, and* $a, b \in \mathbb{Z}$*. Then*

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

(2)
$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Proof. The proof of this may be found in the preliminary section of [CR22]. ■

One result that will be of utmost use to us in this paper is the law of quadratic reciprocity. Though it ultimately resides in elementary number theory, it is a stepping stone for higher reciprocity.

Theorem 0.6 (The Law of Quadratic Reciprocity)**.** *Let $p, q \in \mathbb{Z}$ be odd primes. Then*

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

Alternatively, we can express this as

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

Proof. Several proofs of this may be found in [CR22] as well as Chapter 5 of [IRR90]. We will also provide a proof for this result using finite fields in section 1 due to Hausner. ■

There is also a supplement to quadratic reciprocity concerning whether -1 or 2 is a quadratic residue or nonresidue modulo p. In elementary number theory, the case of $(-1/p)$ is known as Euler's Criterion; when considering cubic residues, the case of -1 is trivial as $-1^3 = -1$, implying that it is always a cubic residue. The case of 2 will provide useful insights when considering whether 2 is a cubic residue or nonresidue in a similar sense.

Theorem 0.7 (Supplement to Theorem 0.6)**.** *Let p be an odd prime. Then*

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

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

Proof. The proof for (1) follows immediately by letting $a = -1$ in Lemma 0.5. The proof for (2) may be found in sections 2.2 and 4.2 of [CR22]. ■

As we will investigate later in section 2, Gauss sums generalize the notion of a quadratic Gauss sum to be expressed in terms of a multiplicative character of higher degree. In [CR22], we developed notions of quadratic Gauss sums in order to prove quadratic reciprocity. As we will see later in section 1.5, another proof of quadratic reciprocity can be given by combining the theory of finite fields and quadratic Gauss sums. As such, we state some elementary properties of the quadratic Gauss sum that will be useful later.

Definition 14 (Quadratic Gauss sum)**.**

$$g_a = \sum_t \left(\frac{t}{p}\right)\zeta_p^{at},$$

where ζ_p is a pth root of unity.

For the sake of notational convention, we denote the quadratic Gauss sum when $a = 1$, or g_1, as simply g. Proofs for the following identities may be found in section 4.3 of [CR22].

Proposition 0.8.

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

Proposition 0.9.

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

A useful tool we will use later is the Kronecker delta, $\delta(x, y)$, which is defined to be 1 if $x \equiv y \pmod p$ and 0 otherwise.

0.3. **Möbius Inversion.** A useful tool that will be used throughout this paper is the Möbius function and a powerful result known as Möbius inversion. Let $n \in \mathbb{Z}^+$.

Definition 15 (Möbius function)**.**

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ non-squarefree,} \\ 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \text{ for distinct } p_i. \end{cases}$$

An important property of the Möbius function is that it is multiplicative, or $\mu(mn) = \mu(m)\mu(n)$, the proof of which requires that we show it holds for $m = n = 1$ and then show that it also holds for m and n squarefree. There are many other interesting properties of the Möbius function, but we are most interested in Möbius inversion. We first need the following result.

Lemma 0.10. *Consider the summatory function $F(n) = \sum_{d|n} \mu(d)$. Then*

$$F(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

Proof. The result is obvious for $n = 1$. To prove it for $n > 1$, prove that it holds for p^k for some $k > 0$, and then use the multiplicativity of $\mu(n)$ to prove the result for any integer $n = p_1^{a_1} \cdots p_t^{a_t} > 1$ using the information gained from computing $F(p^k)$. ■

Recall that an arithmetic function, or number-theoretic function, is a function that maps $\mathbb{Z}$ to $\mathbb{Z}$. We now introduce Möbius inversion.

Theorem 0.11 (Möbius Inversion)**.** *Suppose that f is an arithmetic function and that F is its summatory function. Then*

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Proof.

$$\begin{aligned} \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{e|\frac{n}{d}} f(e) && \text{(By definition of } F.) \\ &= \sum_{d|n} \sum_{e|\frac{n}{d}} \mu(d) f(e) && \text{(By combining double sums.)} \\ &= \sum_{e|n} \sum_{d|\frac{n}{e}} \mu(d) f(e) && \text{(By divisibility in indices.)} \\ &= \sum_{e|n} f(e) \sum_{d|\frac{n}{e}} \mu(d) && \text{(By rearranging the double sums.)} \end{aligned}$$

Notice that $\sum_{d|\frac{n}{e}} \mu(d) = 0$ since $n/e > 1$. If we allow $n/e = 1$, then $n = e$, so $\sum_{d|\frac{n}{e}} \mu(d) = 1$. Then

$$\sum_{e|n} f(e) \sum_{d|\frac{n}{e}} \mu(d) = f(n)(1) = f(n).$$

■

The importance of Möbius inversion is that it allows us to form an algebraic relationship between arithmetic functions and their summatory functions. This will become evident in the next section and following sections.

1. Finite Fields

The language of cubic, biquadratic, and higher reciprocity is expressed in the language of finite fields, so naturally we will explore notions of a finite field in regard to both construction and existence as well as classification of its elements. The reason that finite fields are so fundamental to the study of reciprocity will be evident later.

Finite fields may also be referred to as "Galois fields" as they were created by Évariste Galois and are used widely in Galois theory and higher reciprocity. In this paper, we refer to such a field as a finite field.

A field is defined as follows.

Definition 16. We say that a set $\mathbb{F}$ is a field if it has two operations $+$, or addition (sometimes denoted as $\oplus$), and $*$, or multiplication, and it satisfies the following axioms:

(1) $\mathbb{F}$ is an abelian group under $\oplus$ with identity element 0,
(2) the multiplicative set $\mathbb{F}^* = \mathbb{F}/\{0\}$ is an abelian group under $*$ with identity element 1,
(3) and it satisfies the distributive law that $\forall a, b, c \in \mathbb{F}, (a \oplus b) * c = (a * c) \oplus (b * c)$.

Naturally, we can define a finite field to be one such field with a finite number of elements, say q. Then, since we exclude the additive identity, the multiplicative group $\mathbb{F}^*$ has $q-1$ elements. Therefore every element $\alpha \in \mathbb{F}^*$ satisfies the relation $\alpha^{q-1} = 1$. Similarly, every element $\beta \in \mathbb{F}^+$ the additive group satisfies the relation $\beta^q = \beta + \cdots + \beta = \beta$. In either case, α behaves like a generator of the multiplicative or additive group, but we only consider the multiplicative group of a finite field in this paper.

1.1. The Multiplicative Group of a Finite Field is Cyclic.

We denote the finite field of single-variable polynomials in x as $\mathbb{F}[x]$.

Proposition 1.1. *Suppose that $\mathbb{F}$ is a finite field of order q. Then*

$$x^q - x = \prod_{\alpha \in \mathbb{F}} (x - \alpha).$$

Proof. By the construction of $\mathbb{F}$, notice that every element $\alpha \in \mathbb{F}$ is a root of $x^q - x$ by the definition of α as a generator of $\mathbb{F}$. Since the polynomial on the *RHS* runs through all q elements of the additive group $\mathbb{F}$, its maximum degree must be q. Therefore the result follows from the factorization of the *LHS*. ∎

From this result we can prove the following about subfields.

Corollary 1.2. *Let $\mathbb{K}$ be a field with $\mathbb{F} \subset \mathbb{K}$ a subfield of $\mathbb{K}$. An element $\alpha \in \mathbb{K}$ is also contained within the subfield $\mathbb{F}$ if and only if $\alpha^q = \alpha$.*

Proof. By our original construction, any root $\alpha \in \mathbb{F}$ of $x^q - x$ must satisfy the relation $\alpha^q = \alpha$. By Proposition 1.1, the roots of some polynomial $x^q - x$ are exactly the elements of $\mathbb{F}$ (by its construction from $\alpha \in \mathbb{F}$), so we have proven the forward direction. We now prove the backward direction. If $\alpha^q = \alpha$, then α must be a root of $x^q - x$ by our original construction. Since the condition for an element to be a root of $x^q - x$ is for it to be contained within $\mathbb{F}$, we have $\alpha \in \mathbb{F}$, which proves the result. ∎

In order to develop another necessary corollary toward our result about $\mathbb{F}^*$, we must establish a result for polynomials in a field. Let k denote an arbitrary field.[1]

Proposition 1.3. *Let $f(x) \in k[x]$. Suppose that $\deg(f(x)) = n$. Then $f(x)$ has at most n distinct roots.*

[1]While the notation $R[x]$ to denote the ring of single-variable polynomials for some field R is often convention, we prefer the notation $k[x]$ to distinguish the fact k is a field for which polynomials in $k[x]$ take coefficients.

Proof. We prove this by induction on the degree of $f(x) \in k[x]$. If $n = 1$, then the assertion is clearly true, as a monic polynomial clearly has both a minimum and maximum equivalent number of roots, hence exactly 1 distinct root. Assume that the assertion is true for polynomials of degree $n-1$. This allows us to extend the assertion to degree n later.

To begin, if $f(x)$ has no roots in the field k, then clearly we are done as $f(x)$ therefore has 0 roots. However, if α is a root, then by the division algorithm for polynomials, we can write $f(x) = q(x)(x-\alpha) + r$, where r is some constant and $q(x) \in k[x]$. If we let $x = \alpha$ then $f(\alpha) = q(\alpha)(\alpha - \alpha) + r = r$. We assumed that α was a root of $f(x)$, so $r = 0$. Therefore $q(x)|f(x)$ and $f(x) = q(x)(x-\alpha)$ and $\deg(q(x)) = \deg(f(x)) - 1 = n-1$. Let $\beta \neq \alpha$ be another such root of $f(x)$. Then $f(\beta) = 0 = (\beta - \alpha)q(\beta)$, which is only possible when $q(\beta) = 0$. Therefore we have shown that $q(x)$ has at most $n-1$ distinct roots as we can repeat the process for distinct roots $\beta_1 \neq \beta_2 \neq \cdots \neq \beta_{n-1}$. Thus, since $q(x)$ has at most $n-1$ roots, $f(x)$ has at most n roots, and we are done. ∎

We now present one final corollary that relates polynomials to the polynomial $x^q - x$ and then prove that the multiplicative group of a finite field is cyclic.

Corollary 1.4. *If some polynomial $f(x)|x^q - x$, then $f(x)$ has exactly d distinct roots, where $\deg(f(x)) = d$.*

Proof. Let the product $f(x)g(x) = x^q - x$, where $g(x) = (x^q - x)/f(x)$ has the property $\deg(g(x)) = q - d$. Assume that $f(x)$ has fewer than d distinct roots. Then by Proposition 1.3, the product $f(x)g(x)$ would have fewer than $d + (q-d) = q$ roots, noninclusive. However, by the definition of the product, the product has at most q roots, contradicting our assumption. Therefore $f(x)$ has d distinct roots. ∎

The final proof of this section requires that we are familiar with some basic facts about cyclic groups. The following lemma can be proven using the Fundamental Theorem of Cyclic Groups and other results in elementary group theory.

Lemma 1.5 (Gallian)**.** *If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.*[2]

Proof. The proof may be found in Chapter 4 of [Gal02]. ∎

We now proceed with the final proof.

Theorem 1.6. *The multiplicative group of a finite field is cyclic.*

Proof. In order to prove that the multiplicative group of a finite field is cyclic, we must prove several important properties about its generator. Note first that some multiplicative group of a finite field $\mathbb{F}^*$ must have order $q-1$ in this proof. First, if there exists some subgroup with order $d|q-1$, then $x^d - 1|x^{q-1} - 1$ because we are using $\mathbb{F}[x]$ and degrees of polynomials in $\mathbb{F}[x]$ as an analogue for considering orders of the multiplicative group $\mathbb{F}^*$ and its subgroups. By Corollary 1.4, we know that since $x^{q-1} - 1$ and $x^q - x$ are equivalent forms (this is true because Corollary 1.4 also makes an assertion about divisibility in $\mathbb{F}^*$), we therefore can say that $x^d - 1$ has d distinct roots. Therefore the subgroup of $\mathbb{F}^*$ with elements satisfying the relation $x^d - 1 = 0$ or $x^d = 1$ has order d.

Let $\psi(d)$ be the number of elements in $\mathbb{F}^*$ of order d. Recall that the order of an element is the number of times an operation must be applied in order to return to itself; in this case, we are defining the arithmetic function $\psi(d)$ to be the order of the subgroup of $\mathbb{F}^*$ containing elements with order exactly d. Then we can make the assertion that for every c that divides this order

[2]Recall that the *Euler totient function* $\phi(n)$ returns the number of integers coprime to n, i.e. $\phi(n) = |\{a|\gcd(a,n) = 1\}|$.

d, there exists some summatory function that takes in all such c and outputs this exact order d. We can express this as

$$\sum_{c|d} \psi(c) = d. \tag{1.1}$$

For example, let there exist some set of divisors $c_1, c_2, \ldots, c_n$ such that $c_1, c_2, \ldots, c_n | d$. Then in 1.1 we have

$$\sum_{c|d} \psi(c) = \psi(c_1) + \psi(c_2) + \cdots + \psi(c_n) = d.$$

Therefore, by Möbius inversion, we can write

$$\psi(d) = \sum_{c|d} \mu(c) F\left(\frac{d}{c}\right).$$

Notice that the summatory function F no longer applies here. This is because for each divisor c_i of d, the arithmetic function $\psi(d)$ simply counts the number of c_i, adding 1 each time to its value. Therefore, we can write

$$\sum_{c|d} \mu(c) F\left(\frac{d}{c}\right) = \sum_{c|d} \mu(c) \frac{d}{c}.$$

Notice too, however, that this is simply the number of divisors coprime to d, or $\phi(d)$. We can remove $\mu(c)$ because it takes in divisors of d, which will always evaluate to 1 if there are $k \equiv 0 \pmod 2$ distinct prime factors, and 0 if there are $k \equiv 1 \pmod 2$ distinct prime factors. In either case, we have $\psi(d) = \phi(d)$, or the number of elements in $\mathbb{F}^*$ of order d is equivalent to the number of divisors coprime to d. By Lemma 1.5, $\mathbb{F}^*$ is cyclic. ■

1.2. **nth Power Residues and a Connection to Finite Fields.** In this section, we focus on proving the following important result. Let $n \in \mathbb{Z}^+$ and let $|\mathbb{F}| = q$ so $|\mathbb{F}^*| = q - 1$.

Theorem 1.7. *Let $\alpha \in \mathbb{F}^*$. Then the equation $x^n = \alpha$ has solutions if and only if $\alpha^{(q-1)/d} = 1$, where $d = \gcd(n, q-1)$. If there indeed are solutions, then there are exactly d solutions.*

In order to understand the proof of the prior result in the context of finite fields, we begin by proving a proposition for which the prior result is a generalization. Recall that for $m, n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$, we define a to be an *nth power residue modulo m* if $x^n \equiv 1 \pmod m$ is solvable and a is a solution.

Proposition 1.8. *If $m \in \mathbb{Z}^+$ has primitive roots and $\gcd(a, m) = 1$, then a is an nth power residue modulo m if and only if $a^{\phi(m)/d} \equiv 1 \pmod m$, where $d = \gcd(n, \phi(m))$.*

In order to prove this result, we must recall some facts in elementary number theory. Recall that the set of residue classes modulo m is denoted by $\mathbb{Z}/m\mathbb{Z}$. This is in fact a ring, but we will not prove it here. The set of all representatives for the residue classes of $\mathbb{Z}/m\mathbb{Z}$ is the complete set of residues modulo m.

Perhaps the most elementary study of congruences can be summarized in linear congruences of the form $ax \equiv b \pmod m$. In particular, we are interested in determining the solvability of linear congruences of this form. For some interesting perspective, the number of solutions to a linear congruence is the value of n in an n-tuple $(a_1, \ldots, a_n)$ such that $f(a_1, a_2, \ldots, a_n) \equiv 0 \pmod m$ for a linear congruence $f(x_1, x_2, \ldots, x_n) \equiv 0 \pmod m$ in n variables. Uniqueness of such an n-tuple is assumed, so that if there exists some n-tuple $(b_1, \ldots, b_n)$ that also satisfies the polynomial equation, it must be the exact same n-tuple.

As we move forward, we will begin by looking at linear congruences in one variable.

Proposition 1.9. *Let $d = \gcd(a, m)$. The linear congruence $ax \equiv b \pmod{m}$ has solutions if and only if $d|b$. Moreover, if $d|b$, then there are exactly d solutions. Furthermore, if x_0 is a solution, then all other solutions can be written in the form $x_0 + m', \ldots, x_0 + (d-1)m'$.*

Proof. To preface the proof, we need the following remark. We let $d = \gcd(a, m)$. We also set $a' = a/d$ and $m' = m/d$. Then $\gcd(a', m') = 1$ since a' and m' are in their ultimately reduced forms.

We prove the biconditional first. We begin with the forward direction. Let x_0 be a solution to the linear congruence. Then it satisfies the relation $ax_0 - b = my_0$ for some $y_0 \in \mathbb{Z}$. Then by the opening remark in this proof, we have $b = ax_0 - my_0 = da'x_0 - dm'y_0 = d(a'x_0 - m'y_0)$; thus $d|b$. We now prove the backward direction. Suppose that $d|b$. By Bézout's Lemma, there must exist integers x_0' and y_0' such that $ax_0' - my_0' = d$. If we let some $c = b/d$ and multiply both sides by c, we obtain $a(x_0'c) - m(y_0'c) = b$. Letting $x_0 = cx_0'$ and $y_0 = cy_0'$, we can write $ax_0 - b = m(y_0)$ or $ax_0 - my_0 = b$, which gives the linear congruence a solution.

We now prove that there are exactly d solutions to the congruence $ax \equiv b \pmod{m}$. Suppose that both x_0 and x_1 are solutions such that $ax_0 \equiv b \pmod{m}$ and $ax_1 \equiv b \pmod{m}$. This implies that $a(x_1 - x_0) \equiv 0 \pmod{m}$. Therefore, for two distinct pairs a, m and a', m' we have $m|a(x_1 - x_0)$ and $m'|a'(x_1 - x_0)$ respectively. The second statement implies that $m'|x_1 - x_0$ by our opening remark; in other words, for some $k \in \mathbb{Z}$ we have $x_1 = x_0 + km'$. As we vary the value of k from 0 to $d - 1$, we see that there are incongruent solutions in the form $x_0, x_0+m', \ldots, x_0+(d-1)m'$. Suppose that another solution to $ax \equiv b \pmod{m}$ is $x_1 = x_0+km'$. By the division algorithm, there exist $r, s \in \mathbb{Z}$ such that $k = rd+s$ where $0 \leq s < d$. Substituting, this gives $x_1 = x_0 + (rd + s)m' = x_0 + sm' + rm$. Since $x_1 = x_0 + km'$, we must have $r = 0$, so $k = s$. Since s runs from 0 to $d - 1$, there are thus exactly d solutions. ■

This establishes the solvability of linear congruences. The equation $ax \equiv b \pmod{m}$ is equivalent to writing the equivalence relation $[a]x = [b]$ in the ring $\mathbb{Z}/m\mathbb{Z}$. By Proposition 1.9, the congruence has solutions if and only if $d|b = 1$, which is equivalent to when $\gcd(a, m) = 1$[3]. Thus, $[a]$ is a unit if and only if $\gcd(a, m) = 1$. A special fact about $\mathbb{Z}/m\mathbb{Z}$ is that there are exactly $\phi(m)$ such units. If we let $m = p$ be prime, then all residue classes in $\mathbb{Z}/p\mathbb{Z}$ are units, and we can prove that, in both the multiplicative and additive cases, $\mathbb{Z}/p\mathbb{Z}$ is a field.

With this result, Euler's Theorem can be proven using the elementary fact that a residue class is a unit if, when multiplied with another residue class, yields the [1] residue class modulo m.

Theorem 1.10 (Euler's Theorem)**.** *If $\gcd(a, m) = 1$, then*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

An immediate corollary for prime m is Fermat's Little Theorem, which is used widely in elementary number theory.

Corollary 1.11 (Fermat's Little Theorem)**.** *If p prime and $p \nmid a$, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

We are becoming carried away with ourselves with these results. In a final step before our proof of Proposition 1.8, we note that much like our proof of Theorem 1.6, we were studying the existence of an x that acts as a generator for $\mathbb{F}^*$. Now we consider the analogue over $U(\mathbb{Z}/n\mathbb{Z})$, the group of units of the integers modulo n. It can be shown that if p prime, $U(\mathbb{Z}/p\mathbb{Z})$ is cyclic; the proof is essentially identical to the proof of Theorem 1.6. We say that a is a *primitive root modulo p* if $p - 1$ is the smallest integer such that $a^{p-1} \equiv 1 \pmod{p}$[4]. Now we proceed to prove Proposition 1.8.

[3]We say that the residue class $[a]$ is a *unit* if and only if it satisfies $[a]x = 1$, or if $ax \equiv 1 \pmod{m}$ has solutions.

[4]We also define an integer a to be a *primitive root* modulo p prime if its residue class $[a]$ generates $U(\mathbb{Z}/p\mathbb{Z})$, the group of units of $\mathbb{Z}/p\mathbb{Z}$.

Proof of Proposition 1.8. To begin, let g be a primitive root modulo m, and let $a = g^b$ and $x = a^y$. Then the nth-degree congruence $x^n \equiv 1 \pmod{m}$ is equivalent to $a^{yn} \equiv g^{yn} \equiv g^b \pmod{m}$. The second equivalence can be taken due to the fact that we assumed g to be a primitive root modulo m. Simplifying, we have $g^{ny-b} \equiv 1 \pmod{m}$. Since g is a primitive root, this only occurs if $ny-b$ is some multiple of $\phi(m)$ by Euler's Theorem. Therefore $ny - b \equiv k\phi(m)$ for $k \in \mathbb{Z}$ so $ny \equiv b \pmod{\phi(m)}$. This is a linear congruence and is solvable if and only if $d|b$ by Proposition 1.9. To show the forward direction of this proposition, let $d|b$. Then $a^{\phi(m)/d} \equiv g^{(b\phi(m))/d} \equiv g^{l\phi(m)} \pmod{m}$ for some integer constant l, or $g^{l\phi(m)} \equiv 1 \pmod{m}$. To show the backward direction, let $a^{\phi(m)/d} \equiv 1 \pmod{m}$. Then $g^{(b\phi(m))/d} \equiv 1 \pmod{m}$, which only occurs when b/d is an integer. This only occurs if $d|b$. Therefore $d|b$, and we have proven both directions. ■

Notice also that since the linear congruence is solvable, $d = \gcd(n, \phi(m))$, and there are exactly d solutions. This deduction is necessary in the proof of Theorem 1.7. We now return to our proof of Theorem 1.7.

Proof of Theorem 1.7. The statement of the theorem appears very similar to that of Proposition 1.8. To begin, let γ be a generator of the cyclic group $\mathbb{F}^*$. As in Proposition 1.8, we let $\alpha = \gamma^a$, and $x = \gamma^y$. Then the equivalence relation $x^n = \alpha$ is equivalent to $\gamma^{yn} = \gamma^a$. We can reduce this equivalence to a congruence by removing the base of γ as follows. Dividing both sides by γ^b, we have $\gamma^{ny-b} = 1$. Similar to the proof of Proposition 1.8, and due to the fact that we defined γ to be a generator of $\mathbb{F}^*$, we must have that $ny - b$ is an integer multiple of $q-1$, the order of the multiplicative group of the finite field. Therefore $ny - b = k(q-1)$ so $ny \equiv b \pmod{q-1}$. As in Proposition 1.8, this is a linear congruence, and we can apply Proposition 1.9 as follows.

The congruence is solvable if and only if $d|a$. Suppose first that $d|a$. Then $\alpha^{(q-1)/d} \equiv \gamma^{(a(q-1))/d} \equiv \gamma^{r(q-1)}$ for some integer constant r. Since r must be an integer, $\gamma^{r(q-1)} = 1$. To prove the backward direction, let $\alpha^{(q-1)/d} = 1$. Then $\gamma^{(a(q-1))/d} = 1$, which is only possible if $d|a$, as γ is a generator of $\mathbb{F}^*$. Therefore $d|a$ and we have proven both directions. ■

Notice that in this result, since the linear congruence is solvable, the number of solutions is given by $d = \gcd(n, q-1)$ by Proposition 1.9, and we are done.

Remark 3. In relation to nth power residues, it is also interesting consider what might happen to the number of solutions to the equation $x^n = \alpha$ for $\alpha \in \mathbb{F}^*$ with varying values for d. If $\gcd(n, q-1) = 1$, then there is only 1 unique solution to the equation $x^n = \alpha$. Alternatively, if $n|q-1$ instead, then there are exactly $\gcd(n, q-1) = \frac{q-1}{n}$ solutions to $x^n = \alpha$, and there are n solutions if $\alpha = \beta^n$ for some $\beta \in \mathbb{F}^*$.

1.3. **Structure of Finite Fields.** Now that we have surveyed the multiplicative group of a finite field, we might be interested in determining further characteristics of finite fields and their structural properties, especially in regard to their construction. Most notably, in this section we determine the order of a finite field and show how finite fields have a very intuitive relationship with their subfields. These results prepare us in proving the existence of finite fields later.

Proposition 1.12. *Let $\mathbb{F}$ be a finite field. The integer multiples of the identity form a subfield of $\mathbb{F}$ that is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for p a prime.*

Proof. As a means of standardizing notation, we use e as the identity of the multiplicative group of $\mathbb{F}$ given as $\mathbb{F}^*$ in this proof. Define ϕ as a mapping of the integers to the finite field $\mathbb{F}$ that takes every $n \in \mathbb{Z}$ to some ne, or the integer multiples of the multiplicative identity of $\mathbb{F}$. This is a ring homomorphism because the original operation is preserved, and we are operating under ϕ from the ring of integers to $\mathbb{F}$. It is not difficult to show that ϕ is bijective and satisfies $\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$. The resulting image, namely the nes, form a finite subring of $\mathbb{F}$. More specifically, since $\mathbb{Z}$ commutes, it is also a nonzero commutative ring, or an

integral domain. The kernel of the homomorphism is thus $\text{Ker}(\phi) = \{n \in \mathbb{Z} | \phi(n) = e\}$. In this way, the kernel is a nonzero prime ideal, meaning that either n or e must belong to the finite subring and naturally the integral domain. Thus, by Theorem 0.3, the field $\mathbb{Z}/p\mathbb{Z}$ of the integers modulo p a prime (Note: the set $p\mathbb{Z}$ is exactly the aforementioned $\text{Ker}(\phi)$ because it is a prime ideal of $\mathbb{Z}$) must be isomorphic to the image of ϕ, or $\text{im}(\phi)$, in the mapping from $\mathbb{Z}$ to $\mathbb{F}$. ■

Now that we have proven a fact about the finite field and its relation to the field $\mathbb{Z}/p\mathbb{Z}$, we further explore properties of $\mathbb{F}$ in determining its order. This brings us to the following result.

Proposition 1.13. *The number of elements in a finite field is a power of a prime. Namely, a finite field over a vector space with dimension n has order p^n.*

Proof. From linear algebra, we know that every field can be expressed as a finite-dimensional vector space over each of its subfields, or in this case, every field is a finite-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$. We will not prove this here as it lies beyond the scope of this paper, but the result is critical in our proof of this result.

Let n be the dimension of the vector space and let $\omega_1, \omega_2, \ldots, \omega_n$ be a basis of $\mathbb{F}$. By the construction of a finite-dimensional vector space, every element in $\mathbb{F}$ has a unique representation as a linear combination of all vectors in the basis and elements of $\mathbb{Z}/p\mathbb{Z}$, namely as $a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n$ where $a_i \in \mathbb{Z}/p\mathbb{Z}$ for all $1 \leq i \leq n$. Since the field $\mathbb{Z}/p\mathbb{Z}$ has prime order p, we know that there are exactly p possible inputs for each a_i. This gives us p^n total linear combinations of the basis, so the order of $\mathbb{F}$ is p^n. ■

As we continue studying $\mathbb{F}$, we introduce a definition. Let e represent the multiplicative identity of a finite field $\mathbb{F}$. We define the *characteristic* of a finite field $\mathbb{F}$ to be the minimum element p to satisfy $pe = 0$, where 0 is the additive identity. As we have seen before, p must be a prime as it is the only possible integer that satisfies the isomorphism in Proposition 1.12. An important fact about the characteristic is that when applied to *any* element of the finite field, it yields the additive identity. In other words, if there is some $\alpha \in \mathbb{F}$, then $p\alpha = p(\alpha e) = (pe)\alpha = 0 \cdot \alpha = 0$ by the commutativity of $\mathbb{F}$. This leads us to the following result.

Proposition 1.14. *If a finite field $\mathbb{F}$ has characteristic p, then for $\alpha, \beta \in \mathbb{F}$ and some $d \in \mathbb{Z}^+$,*

$$(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d}.$$

Proof. We prove this by induction on d. In the base case where $d = 1$, this is obvious as $(\alpha + \beta)^p = \sum_{r=0}^{p} \binom{p}{r} \alpha^{p-r}\beta^r$. Expanding, we have

$$\alpha^p + \binom{p}{1}\alpha^{p-1}\beta + \binom{p}{2}\alpha^{p-2}\beta^2 + \cdots + \binom{p}{p-1}\alpha\beta^{p-1} + \beta^p.$$

Since $\mathbb{F}$ has characteristic p, each multiple of p must be equivalent to the additive identity. In other words, since p divides each binomial coefficient where $i = 1, 2, \ldots, p-1$ (this can be proven using simple facts about the binomial coefficient), their multiples equate to the additive identity. Therefore we have $(\alpha + \beta)^p = \alpha^p + \beta^p$.

Assume that this relation holds for some $d = k$. Then $(\alpha + \beta)^{p^k} = \alpha^{p^k} + \beta^{p^k}$. We wish to prove that it holds for $d = k + 1$. As a result of the inductive hypothesis, we have

$$\begin{aligned}
((\alpha + \beta)^{p^k})^p &= (\alpha^{p^k} + \beta^{p^k})^p \\
(\alpha + \beta)^{p^{k+1}} &= \sum_{r=0}^{p} \binom{p}{r} (\alpha^{p^k})^{p-r} (\beta^{p^k})^p \\
&= \sum_{r=0}^{p} \binom{p}{r} (\alpha^{p^k})^p (\alpha^{p^k})^{-r} (\beta^{p^k})^p \\
&= \alpha^{p^{k+1}} + \binom{p}{1} \alpha^{p^{k+1}} \alpha^{-p^k} \beta^{p^{k+1}} + \cdots + \binom{p}{p-1} \alpha^{p^{k+1}} \alpha^{-p^k(p-1)} \beta^{p^{k+1}} + \beta^{p^{k+1}} \\
&= \alpha^{p^{k+1}} + \beta^{p^{k+1}},
\end{aligned}$$

where intermediate terms in the binomial expansion vanish modulo p since $\mathbb{F}$ has characteristic p. ■

Now that we have information about binomial powers and the order of finite fields, we may be interested in determining not only properties of $\mathbb{F}$ but of subfields of the finite field $\mathbb{F}$ for which $\mathbb{Z}/p\mathbb{Z}$ is the scalar field. For the sake of the following results, we will denote such fields as $\mathbb{E}$. Let n be the order of $\mathbb{F}$ and d be the dimension of $\mathbb{E}$. It is possible to show, using techniques of field extensions and algebraic extensions, that $d|n$. We will instead provide an alternate proof that $d|n$ using finite fields. The underlying concept suggests that there is one and only one intermediate subfield $\mathbb{E}$ corresponding to each divisor d of n. In order to prove this we begin with the following elementary results.

Lemma 1.15. *Let $\mathbb{F}$ be a field. Then for $x^l - 1, x^m - 1 \in \mathbb{F}[x]$ we have that $x^l - 1 | x^m - 1$ if and only if $l|m$.*

Proof. Suppose that $l \nmid m$, or that $m = ql + r$ for some remainder $r \in [0, 1)$ and divisor $q \in \mathbb{Z}$. Then,

$$\frac{x^m - 1}{x^l - 1} = \frac{x^{ql} x^r - 1}{x^l - 1} = \frac{x^{ql} - 1}{x^l - 1} x^r + \frac{x^r - 1}{x^l - 1}.$$

By polynomial division, the first term on the *RHS* can be written as the polynomial $x^r((x^l)^{q-1} + (x^l)^{q-2} + \cdots + x^l + 1)$. The remaining quotient can be seen to be 0 if and only if $r = 0$, as it evaluates to $0/(x^l - 1) = 0$. Therefore the *RHS* is a polynomial if and only if $r = 0$, which occurs if and only if $l|m$, so we are done. ■

Remark 4. This result is also true for positive integers in place of x and can be summarized as follows: if $a \in \mathbb{Z}^+$, then $a^l - 1 | a^m - 1$ if and only if $l|m$. We will not prove it here as the proof is identical to that of Lemma 1.15.

Now that we have these results about divisibility, we can prove the relation between $\mathbb{F}$ and its subfields.

Theorem 1.16. *Let $\mathbb{F}$ be a finite field of dimension n over $\mathbb{Z}/p\mathbb{Z}$. Then the subfields of $\mathbb{F}$ have an injection with the divisors d of n.*

Proof. Let $\mathbb{E}$ be a field of dimension d over the field $\mathbb{Z}/p\mathbb{Z}$. Furthermore, let the finite field $\mathbb{F}$ have dimension n such that $\mathbb{E}$ is a subfield of $\mathbb{F}$. In this proof we wish to show that $d|n$.

To begin, notice that by Proposition 1.13, we know that $\mathbb{E}$ must have an order of a power of a prime, namely p^d, since the dimension of $\mathbb{E}$ is d. We can verify this by counting all possible linear combinations with respect to some basis, just as in the proof of Proposition 1.13. Since the subfield $\mathbb{E}$ has order p^d, its multiplicative group $\mathbb{E}^*$ therefore must have order $p^d - 1$. By the

definition of the multiplicative group, exactly $p^d - 1$ elements satisfy the polynomial equation $x^{p^d-1} - 1 = 0$ where x is some arbitrary variable. Now, considering the multiplicative group $\mathbb{F}^*$, we can see that it similarly has exactly $p^n - 1$ elements satisfying $x^{p^n-1} - 1 = 0$. Therefore $x^{p^d-1} - 1 | x^{p^n-1} - 1$. By Lemma 1.15, we know that this implies $p^d - 1 | p^n - 1$, and furthermore, by Remark 4, this implies that $d|n$.

Now that we have shown that $d|n$, we must prove that there is an injection between the subfields of $\mathbb{F}$ and the divisors of n. In order for an injection to exist, there must be a correspondence such that if $f(x) = f(y)$ for $x, y \in \mathbb{E}$ an arbitrary subfield of $\mathbb{F}$, then $x = y$ for f a function from $\mathbb{E}$ of $\mathbb{F}$ to the divisors of n. We show this relationship in the following. To begin, suppose that $d|n$ again, as we will use this fact. Now let $\mathbb{E} = \{\alpha \in \mathbb{F} | \alpha^{p^d} = \alpha\}$. By constructing the subfield $\mathbb{E}$ in this way, we are constructing all subfields such that all elements α in the finite field $\mathbb{E}$ are also in $\mathbb{F}$, just as we observed in Corollary 1.2 with the requirement that $\alpha \in \mathbb{F}$ be in $\mathbb{E}$ if and only if α satisfies the equation $\alpha^{p^d} = \alpha$. In order to ensure that this construction is valid, we must prove that $\mathbb{E}$ is indeed a field. In other words, the following properties must be true for any $\alpha, \beta \in \mathbb{E}$:

(1) $(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d} = \alpha + \beta$,
(2) $(\alpha\beta)^{p^d} = \alpha^{p^d}\beta^{p^d} = \alpha\beta$,
(3) $(\alpha^{-1})^{p^d} = (\alpha^{p^d})^{-1} = \alpha^{-1}$ for $\alpha \neq 0$.

Property (1) follows immediately from Proposition 1.14 since $\mathbb{E}$ also has characteristic p, and then by our initial construction of elements in $\mathbb{E}$. Properties (2) and (3) are trivial as they are inherent properties of $\mathbb{F}$ with the exception of the construction of $\mathbb{E}$.

We now determine the order of $\mathbb{E}$. By the very construction of $\mathbb{E}$, we know that $\mathbb{E}$ is the set of solutions to the polynomial equation $x^{p^d} - x = 0$. By Remark 4, since $d|n$, we know that $p^d - 1 | p^n - 1$, and similarly by Lemma 1.15, we must also have $x^{p^d-1} - 1 | x^{p^n-1} - 1$. Consequently $x^{p^d} - x | x^{p^n} - x$. Since $\mathbb{E}$ comprises the solutions to $x^{p^d} - x = 0$, we thus have that $x^{p^d} - x$ is exactly the $f(x)$ described by Corollary 1.4. Furthermore, the order of $\mathbb{E}$ is exactly the roots of $x^{p^d} - x$, so the order of $\mathbb{E}$ is p^d. Therefore $\mathbb{E}$ must have dimension d over $\mathbb{Z}/p\mathbb{Z}$ by applying Proposition 1.13.

To finish the proof, we must show that each divisor d of n corresponds to a unique subfield of $\mathbb{F}$. To do this, let $\mathbb{E}'$ be another subfield of $\mathbb{F}$ of dimension d over $\mathbb{Z}/p\mathbb{Z}$. Then by our previous workings, every element of $\mathbb{E}'$ must satisfy $x^{p^d} - x = 0$, and these are the elements that do. However, we constructed $\mathbb{E}$ in the same way, so the solutions to $x^{p^d} - x = 0$ must coincide, i.e. $\mathbb{E} = \mathbb{E}'$. ■

These results establish some basic properties of finite fields. We are now concerned with whether such a finite field can exist.

1.4. **The Existence of Finite Fields.** Now that we have shown the construction and some properties of finite fields, we may ask another question: given some number p^n where $n \in \mathbb{Z}^+$, does there exist some finite field with exactly p^n elements? This is largely what we will investigate here, summarized in the following theorem.

Theorem 1.17. *Let $n \geq 1$ be an integer and let p be prime. Then there must exist a finite field with exactly p^n elements.*

We first need to prove some ring-theoretic facts, and then we will return to proving results for the theorem. We stated that $k[x]$ was a Euclidean domain for some arbitrary field k. By Theorem 0.1, $k[x]$ is a PID. We say that some polynomial $p(x) \in k[x]$ is *irreducible* if some polynomial $q(x)$ divides $p(x)$, then $q(x)$ must either be a constant multiple of $p(x)$ or is a constant. In this

way, irreducible polynomials are analogous to prime numbers in $\mathbb{Z}$. We now need to prove the following results.

Lemma 1.18. *If A is an ideal of a ring R and contains a unit (1), then $A = R$.*

Proof. We prove this by double inclusion. Since A is an ideal of R, by definition it is true that $A \subseteq R$. We need to show that $R \subseteq A$. Let $a \in A$ and $r \in R$. Since A is an ideal, we know that $ar = ra \in R$ for all $r \in R$. Since A contains 1, it must be true that $1r = r1 \in R$ for all $r \in R$, namely that $r \in A$ for all $r \in R$, which means that $R \subseteq A$. Therefore $R = A$, and we are done. ■

Proposition 1.19. *Let R be a commutative ring with unity and let A be an ideal of R. Then the quotient ring R/A is a field if and only if A is maximal.*

Proof. We begin by proving the forward direction. Let the quotient ring R/A be a field. Let B be an ideal of R such that $A \subseteq B$. Furthermore, consider some $b \in B$ but $b \notin A$. Then $b + A$ is a nonzero element of the field R/A, and by the definition of a field, there must exist another element $c + A$ such that $(b + A)(c + A) = 1 + A$, or the multiplicative identity of R/A. Since $b \in B$, it must be true by the definition of an ideal that any multiple $bc \in B$. We then have $1 + A = (b + A)(c + A) = bc + A$. Therefore $1 - bc \in A \subseteq B$, so $1 - bc + bc = 1 \in B$. By Lemma 1.18, we have that A is a maximal ideal.

We now prove the backward direction. Suppose that A is a maximal ideal and there exists some $b \in R$ but $b \notin A$. To ensure that the quotient ring R/A is a field, we need only show that $b + A$ has a multiplicative inverse because the other properties of a field are trivial. Consider the set $B = \{br+a | r \in R, a \in A\}$. We can show that B is an ideal of R as follows. First, to prove the first condition for B to be an ideal, consider distinct $r, a \in R$ such that we have two elements $br_1 + a_1$ and $br_2 + a_2$. Then we can see $br_1 + a_1 + br_2 + a_2 = b(r_1 + r_2) + (a_1 + a_2) \in B$ by the construction of B. Next, consider some element $r' \in R$. Then $(br + a)r' = brr' + ar' = b(rr') + r'a \in B$ again by the construction of B. Therefore B is an ideal of R. Since A was assumed to be maximal, in the construction of B as an ideal of R we then have that $B = R$. Then the unit 1 is an element of B. Let $1 = bc + a'$ for some $a' \in A$. Then we may write $1 + A = bc + a' + A = bc + A = (b + A)(c + A)$, so we have shown that $b + A$ has a multiplicative inverse, namely $c + A$. ■

This leads us to the following result about the existence of polynomials with roots in a field. Recall that an *irreducible* polynomial in $k[x]$ for some arbitrary field k is equivalent to the notion of a prime in $\mathbb{Z}$.

Proposition 1.20. *Let k be an arbitrary field, and also let $f(x) \in k[x]$ be an irreducible polynomial. There exists some field K containing k and an element $\alpha \in K$ such that α is a root of $f(x)$, or $f(\alpha) = 0$.*

Proof. We showed above that $k[x]$ is a PID. Since $f(x)$ is an irreducible polynomial, the ideal given by $(f(x))$ generated by $f(x)$ is a maximal and principal ideal (while also being a proper ideal), meaning that it is one of the largest ideals of $k[x]$. By Proposition 1.19, the quotient ring $k[x]/(f(x))$ is a field since $(f(x))$ is a maximal ideal. Let $K' = k[x]/(f(x))$. This field runs through all $a(x) \in k[x]$ and combines each $a(x)$ with the entire ideal $(f(x))$, thereby generating the group of cosets $\{a(x) + (f(x)) | a(x) \in k[x]\}$. Let ϕ be the homomorphism that maps $k[x]$ to K' by mapping each element of $k[x]$ to its respective coset modulo $(f(x))$. For example, if $a_1(x) \in k[x]$ then ϕ would take $a_1(x)$ to its unique coset in the group of cosets. Now consider the following diagram.

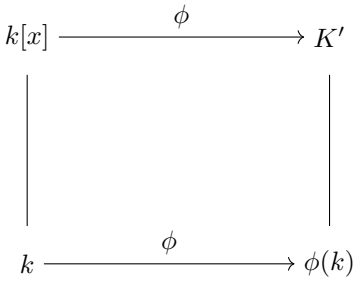

Figure 2. Illustration of the homomorphism ϕ over two analogues

In this diagram, we naturally have the mapping from $k[x]$ to K' described before. However, to simplify the proof, we are also considering the mapping via ϕ that similarly maps elements from the previously defined field k to its cosets, defined as $\phi(k) = \{a + (f(x))|a \in k\}$. It is obvious that k is a subfield of $k[x]$, and it is also clear that since for all $a \in k$ it is also true that all $a(x) \in k[x]$ with coefficients a, $\phi(k)$ is a subfield of K'.

We claim that $\phi(k)$ is isomorphic to k. To prove this, we need to show that the mapping via ϕ is injective and that it preserves the operation. It is clear that the operation is preserved due to the fact that we are transitioning between k and the group of cosets with respect to the ideal $(f(x))$. We need only show that the map is injective. Consider some $a \in k$. If $\phi(a) = 0$, then $a \in (f(x))$ because this means that for all a, it is true that $a + (f(x)) = 0$, or that $a = -(f(x))$, namely that $a \in (f(x))$. Suppose that $a \neq 0$. Therefore a must be a unit and cannot be an element of $(f(x))$ as that would contradict the construction of the ideal. Therefore $a = 0$. Thus, if $\phi(a) = 0$, then $a = 0$, satisfying the condition for ϕ to be an injection.

Since ϕ is an isomorphism attached to k, we can identify k with $\phi(k)$ instead, meaning that we are now considering K' to be an extension of k using the isomorphism via ϕ. In other words, K' contains a subfield, namely the aforementioned $\phi(k)$, that is isomorphic to k. Therefore we can relabel K' as K containing k, as this is the field that we desired to construct.

To complete the proof, we wish to bring this to context in polynomials. Let α be the coset of x in K, namely the coset $\phi(x) = x + (f(x)) = \alpha$. Then $0 = \phi(f(x)) = f(\phi(x)) = f(\alpha)$. The second and third equivalence can be seen to be true by considering a simple example. For the sake of simplicity, we consider the monic polynomial $x^2 \in k[x]$. After evaluating each composition, we see that $\phi(f(x)) = f(\phi(x)) = x^2 + (x^4)$. The equivalence can be generalized by considering the general form of a polynomial $a(x) \in k[x]$ with $\deg(a(x)) = n$ and evaluating each composition accordingly.

Therefore α is a root of $f(x)$ in K. ■

In the following, we denote this field K exactly as $k(\alpha)$, where k is an arbitrary field. Let $k[\alpha]$ denote the ring of polynomials in α with coefficients belonging to the field k. We have the following. The α described below is exactly the roots of $f(x)$.

Proposition 1.21. *The elements $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ form a vector space basis for the finite-dimensional vector space $k(\alpha)$ over k, where k is the same arbitrary field and n is the degree of $f(x)$ described in the previous proposition.*

We omit the proof as it lies beyond the scope of this paper.

We briefly introduced field extensions and the degree of a field extension in the preliminary section. Proposition 1.21 shows that if we wish to find a field extension $[k(\alpha) : k] = n$ of degree n, it is sufficient to construct an irreducible polynomial $f(x) \in k[x]$ with $\deg(f) = n$. In other words, we need only produce such a polynomial to show that a finite field with prime power order exists.

As we proceed, we will prove a powerful result, due to Gauss, that there exists an irreducible polynomial of every degree in the polynomial ring obtained by adjoining the finite field $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ with x. This polynomial ring can be denoted with $\mathbb{Z}/p\mathbb{Z}[x]$, but we will use the notation $\mathbb{F}_p[x]$ instead. First, notice that in $\mathbb{F}_p[x]$ there are finitely many polynomials of any degree, ranging from 0 to $p-1$. This is obvious because there are a finite number of combinations of elements in $\mathbb{F}_p$ that can form a polynomial.

In the following, we let $F_d(x)$ denote the product of all monic irreducible polynomials in $\mathbb{F}_p[x]$. The following result ultimately states that the polynomial $x^{p^n} - x$ can be factored into a product of monic irreducible polynomials with respect to degrees that are divisors of n.

Proposition 1.22.

$$x^{p^n} - x = \prod_{d|n} F_d(x).$$

Proof. First, we must prove that the product $F_d(x)$ contains only unique monic irreducible polynomials. We do this by supposing that if some arbitrary monic irreducible $f(x)$ divides $x^{p^n} - x$, then $f(x)^2$ cannot divide $x^{p^n} - x$. We show this as follows. Suppose $f(x)^2$ does indeed divide $x^{p^n} - x$. Then there must exist another monic irreducible $g(x)$ such that $x^{p^n} - x = f(x)^2 g(x)$. Differentiating each side with respect to x, we obtain

$$p^n x^{p^n - 1} - 1 = 2f(x)f'(x)g(x) + f(x)^2 g'(x).$$

Since $\mathbb{F}_p[x]$ has characteristic p, we set $p = 0$. Therefore

$$-1 = 2f(x)f'(x)g(x) + f(x)^2 g'(x) = f(x)[2f'(x) + f(x)g'(x)].$$

This shows that $f(x)|1$, which, when $f(x)$ is a monic irreducible, is impossible. Therefore $f(x)^2 \nmid x^{p^n} - x$.

We now only need to show that if $f(x)$ is a monic irreducible polynomial with $\deg(f) = d$, then it divides $x^{p^n} - x$ if and only $d|n$. Let $K = \mathbb{Z}/p\mathbb{Z}(\alpha)$ be the field mentioned earlier, where α is a root of $f(x)$ as described in Proposition 1.20. Since $\deg(f) = d$, we know that K has order p^d by Proposition 1.13. Therefore all elements of K are roots of $x^{p^d} - x$, i.e. satisfy the polynomial equation $x^{p^d} - x = 0$.

We first prove the forward direction. Assume, WLOG, that $f(x)|x^{p^n} - x$, or that there exists another monic irreducible $g(x) \in \mathbb{F}_p[x]$ that divides $x^{p^n} - x$. Then we need to show that $\alpha^{p^n} = \alpha$ for some arbitrary root $\alpha \in K$. Suppose that $\alpha_1 = a_1\alpha_1^{d-1} + a_2\alpha_1^{d-2} + \cdots + a_{d-1}\alpha_1 + a_d$ is some arbitrary element of K. Then, plugging into the equivalence $\alpha^{p^n} = \alpha$ for α, by Proposition 1.14,

$$\begin{aligned}(a_1\alpha_1^{d-1} + a_2\alpha_1^{d-2} + \cdots + a_{d-1}\alpha_1 + a_d)^{p^n} &= a_1(\alpha_1^{p^n})^{d-1} + a_2(\alpha_1^{p^n})^{d-2} + \cdots a_{d-1}(\alpha_1^{p^n}) + a_d \\ &= a_1\alpha_1^{d-1} + a_2\alpha_1^{d-2} + \cdots + a_{d-1}\alpha_1 + a_d.\end{aligned}$$

Therefore every element of K satisfies the polynomial equation $x^{p^n} - x = 0$. By the construction of K, its elements satisfy the polynomial equation $x^{p^d} - x = 0$, so it must also be true that $x^{p^d} - x | x^{p^n} - x$. By Lemma 1.15, this implies that $d|n$, thus proving the forward direction.

We now proof the backward direction. Assume that $d|n$. We again have that an arbitrary root $\alpha \in K$ satisfies $\alpha^{p^d} = \alpha$. Since $f(x)$ is the monic irreducible with α as a root, we have $f(x)|x^{p^d} - x$. By Lemma 1.15 again, since $d|n$, we have $x^{p^d} - x | x^{p^n} - x$, and by transitivity $f(x)|x^{p^n} - x$, thus proving the proposition. ∎

Now that we have proven that such a factorization of $x^{p^n} - x$ exists, we want to prove something about the number of monic irreducibles of a given degree in $\mathbb{F}_p[x]$. We let N_d denote the number of monic irreducibles of degree d. We have the following.

Corollary 1.23.

$$p^n = \sum_{d|n} dN_d.$$

Proof. We equate the degrees of the *LHS* and *RHS* of Proposition 1.22. Since the degree of the *RHS* is the sum of the number of monic irreducibles of degree d multiplied by each divisor of n, the result follows. ■

This gives us the following due to Möbius Inversion.

Corollary 1.24.

$$N_n = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right)p^d.$$

Proof. We use Theorem 0.11. Let the arithmetic function $f(n) = nN_n$ and let its summatory function be $F(n) = p^n$. By the inversion formula, we can write this as

$$nN_n = \sum_{d|n} \mu\left(\frac{n}{d}\right)p^d$$

$$N_n = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right)p^d.$$

■

This gives us the following due to Gauss.

Proposition 1.25. *For each integer $n \geq 1$, there exists an irreducible polynomial of degree n in $\mathbb{F}_p[x]$.*

Proof. Expanding the sum on the *RHS* of Corollary 1.24 (and excluding the intermediate terms due to the fact that the divisors are arbitrary for an arbitrary non-prime n), we obtain

$$N_n = \frac{1}{n}(p^n - \cdots + p\mu(n)).$$

Notice that the expression $(p^n - \cdots + p\mu(n))$ is never 0 since the first term is p^n and all remaining terms are a prime factor of either 1 or -1 as given in the definition of the Möbius function. This implies that with respect to the degree n, there exists at least 1 irreducible with that degree. ■

Since we have proven that there is an irreducible of every degree, we have shown that there exists a finite field with p^n elements, thereby proving Theorem 1.17.

We have only provided a brief overview of the algebra and number theory required for the study of finite fields, but existing research and current research on finite fields is highly relevant to many areas of ongoing mathematics research. The study of finite fields is also interesting in its own right. In the next section we give a proof of quadratic reciprocity using finite fields.

1.5. **Another Proof of the Law of Quadratic Reciprocity.** The following proof of quadratic reciprocity is an expanded version of a proof of quadratic reciprocity using quadratic Gauss sums due to Hausner published in 1961; see [Hau61]. While this proof relies heavily on quadratic Gauss sums, the fundamental argument of the proof we present relies largely on the existence of finite fields of prime power order to define a modified quadratic Gauss sum, and we take full advantage of properties of finite fields. The proof is as follows.

Proof of Theorem 0.6 using finite fields. Consider distinct odd primes p and q. Obviously, we have $\gcd(p, q) = 1$. Therefore, there exists some integer n such that $q^n \equiv 1 \pmod{p}$. For example, $n - 1$ might satisfy this congruence, which is a special case of Corollary 1.11. Now let $\mathbb{F}$ be some finite field of dimension n over $\mathbb{Z}/q\mathbb{Z}$ (recall from earlier that we are able to do this as we are treating $\mathbb{F}$ as a vector space for which $\mathbb{Z}/q\mathbb{Z}$ is a scalar field). It is well-known that since q is an odd prime, $\mathbb{Z}/q\mathbb{Z}$ is a field. Therefore the multiplicative group $\mathbb{F}^*$ is cyclic and has order $|\mathbb{F}| - 1 = q^n - 1$. Since $\mathbb{F}^*$ is cyclic, it must have a generator. Let γ be one such generator, and let $\lambda = \gamma^{(q^n-1)/p}$. In other words, λ has order p, since p is the least integer such that $\lambda^p = 1$ by Corollary 1.11.

We now define an analogue to the quadratic Gauss sum. Let

$$\tau_a = \sum_{t=0, a\in\mathbb{Z}}^{p-1} \left(\frac{t}{p}\right)\lambda^{at}.$$

Similar to quadratic Gauss sums, we will denote the case when $a = 1$ as simply τ. Like the proof of quadratic reciprocity using quadratic Gauss sums in section 4.4 of [CR22], we will need two identities. Namely,

(1)
$$\tau_a = \left(\frac{a}{p}\right)\tau,$$

(2)
$$\tau^2 = (-1)^{\frac{p-1}{2}}\overline{p}.$$

In (2), we let $\overline{p}$ be the coset of p in $\mathbb{Z}/q\mathbb{Z}$. We first prove (1). Consider the case where $a \equiv 0 \pmod{p}$. This can clearly be shown to be true since $\sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \cdot 1 = 0$. The second case is when $a \not\equiv 0 \pmod{p}$. We follow the proof procedure used for Proposition 0.8, and ultimately we can prove the result by expanding the *RHS* of (1) and proceeding with the same approach as in [CR22]. To prove (2) we follow the proof procedure for Proposition 0.9. We leave the details of the proof to the reader, which can also be found in [CR22]. The proof involves evaluating the particular sum

$$\sum_{a=0}^{p-1} \tau_a\tau_{-a}$$

in two different ways.

Notice that in (2), $\overline{p}$ denotes the coset of p in $\mathbb{Z}/q\mathbb{Z}$. In other words, it is comprised of all elements $p + q\mathbb{Z}$. Note that if some number is a square modulo q, then that is equivalent to stating that the coset consists of square elements. As with the proof of quadratic reciprocity using quadratic Gauss sums, we denote $p^* = (-1)^{(p-1)/2}p$. Then we can rewrite (2) as $\tau^2 = \overline{(-1)^{(p-1)/2}p} = \overline{p^*}$. Therefore, the coset p^* is a square modulo q, i.e. p^* is a quadratic residue modulo q, so $(\frac{p^*}{q}) = 1$. Note that this is satisfied if and only if $\tau \in \mathbb{Z}/q\mathbb{Z}$. By Corollary 1.2, this biconditional statement is true if and only if

(1)
$$\tau^q = \tau.$$

Notice further that we are able to use Corollary 1.2 because obviously $\mathbb{Z}/q\mathbb{Z} \subset \mathbb{F}$. If we evaluate τ^q, since all intermediate terms reduce to 0 modulo q,

$$\tau^q = \left(\sum_{t\in\mathbb{F}_p} \left(\frac{t}{p}\right)\lambda^t\right)^q = \sum_{t\in\mathbb{F}_p} \left(\frac{t}{p}\right)\lambda^{qt} = \tau_q.$$

Applying (1), we can see that this is the same as $\tau_q = (\frac{q}{p})\tau$. Clearly, the only case where $\tau_q = \tau$ is when $(\frac{q}{p}) = 1$. If we work our way back to the statement of this biconditional, we have $(\frac{p^*}{q}) = 1$ if and only if $(\frac{q}{p}) = 1$, i.e.

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

As with the standard proof of quadratic reciprocity using quadratic Gauss sums, by Theorem 0.7, we can write this equivalence as

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

which is equivalent to the statement of Theorem 0.6. ■

Many proofs of quadratic reciprocity using Gauss sums exist, and this is one such proof that utilizes few facts from algebraic number theory. In the proof given by Hausner, finite fields are referred to instead as Galois fields and are denoted as $GF(q)$ where q denotes order. For our purposes, as proven in Proposition 1.13, we are dealing primarily with $GF(p^k)$ for $k \in \mathbb{Z}^+$. Many similar proofs of quadratic reciprocity published during this period utilize similar notation.

2. Multiplicative Characters

In this section we study multiplicative characters. The main motivation for studying multiplicative characters is to generalize quadratic residue symbols - which we referred to as Legendre symbols - to higher degree residue symbols. While this section provides a general overview of nth degree residue symbols, the case when $n = 3$ will be the primary consideration of this paper.

2.1. Definitions and Some Basic Results.

One of the most elementary examples of a multiplicative character is the Legendre symbol (a/p), as it can be thought of as a function of the coset of a modulo p a prime. We define a multiplicative character as follows, where we denote the integers modulo p given as $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$ for the sake of simplicity.

Definition 17 (Multiplicative Character)**.** We define a multiplicative character on a field $\mathbb{F}_p$ with p elements as some mapping χ from the multiplicative group $\mathbb{F}_p^*$ to the nonzero complex numbers that satisfies the property that for all $a, b \in \mathbb{F}_p^*$,

$$\chi(ab) = \chi(a)\chi(b).$$

Once we are more familiar with the basic definitions of multiplicative characters, we will refer to them as "characters" instead. One concrete notion of the multiplicative character is the trivial multiplicative character, which naturally has properties that map every element of $\mathbb{F}_p^*$ to the multiplicative identity; namely, for a mapping ε, we have $\varepsilon(a) = 1$ for all $a \in \mathbb{F}_p^*$. To study multiplicative characters in more depth, it is possible to consider the additive identity in the definition of the trivial and nontrivial multiplicative characters. Namely, if we let some character $\chi \neq \varepsilon$, then we can define $\chi(0) = 0$, and $\varepsilon(0) = 1$. We now prove the following results about multiplicative characters.

Proposition 2.1. *Let χ be some multiplicative character and $a \in \mathbb{F}_p^*$. Then*

1. $\chi(1) = 1$,
2. $\chi(a)$ *is a* $(p-1)$*st root of unity,*
3. $\chi(a^{-1}) = (\chi(a))^{-1} = \overline{\chi(a)}$ *(where a bar denotes conjugation).*

Proof. To prove (1), we have from our definition of χ that $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$. Since χ is a map to nonzero complex numbers, the only value for $\chi(1)$ that satisfies this relation is the complex number 1, so $\chi(1) = 1$.

For (2), some complex number a is a $(p-1)$st root of unity if $a^{p-1} = 1$. Thus, following from (1), we have $1 = \chi(1) = \chi(a^{p-1}) = (\chi(a))^{p-1}$. Therefore $\chi(a)$ is a $(p-1)$st root of unity.

Finally, for (3), following again from the definition of χ, we have $1 = \chi(1) = \chi(a^{-1}a) = \chi(a^{-1})\chi(a)$. Therefore $\chi(a^{-1}) = \chi(a)^{-1}$, and also, since $\chi(a)$ is a $(p-1)$st root of unity, meaning that $\chi(a)$ evaluates to 1, its modulus must be 1. From the fact that $x\overline{x} = 1$ for some $x \in \mathbb{C}$, we have that $\chi(a)^{-1} = \overline{\chi(a)}$. ∎

Many properties of the Legendre symbol can offer good intuition for many of the following results that we develop regarding multiplicative characters. Said properties were developed more precisely in the preliminary section of [CR22].

Proposition 2.2. *Let χ be a multiplicative character. If $\chi \neq \varepsilon$, the trivial multiplicative character, then $\sum_{t\in\mathbb{F}_p} \chi(t) = 0$. Otherwise, the sum is p.*

Proof. The last assertion is as follows. Since t runs through all elements of $\mathbb{F}_p$, we must have

$$\sum_{t\in\mathbb{F}_p} \chi(t) = \sum_{t\in\mathbb{F}_p} \varepsilon(t) = p.$$

To prove the first assertion, we assume otherwise. Let there exist some $a \in \mathbb{F}_p^*$ such that $\chi(a) \neq 1$, or χ does not map a to 1, hence χ nontrivial. Let the desired sum be $T = \sum_{t\in\mathbb{F}_p} \chi(t)$. Then we may write

$$\chi(a)T = \sum_{t\in\mathbb{F}_p} \chi(a)\chi(t) = \sum_{t\in\mathbb{F}_p} \chi(at).$$

This equates to T itself as at runs through the exact same number of elements from $\mathbb{F}_p$ as t does, so $\chi(a)T = T$. Then $T(\chi(a) - 1) = 0$. We stated that necessarily $\chi(a) \neq 1$, so $T = 0$, and we are finished. ∎

Remark 5. An important fact about characters is that they form a group. Necessarily, for two nontrivial characters χ and λ, the function $\chi\lambda$ is the map that takes some $a \in \mathbb{F}_p^*$ to $\chi(a)\lambda(a)$. In order for $\chi\lambda$ to be a character it must be true that the map of the composition is a homomorphism, namely that for all $x, y \in \mathbb{F}_p^*$, we have $\chi\lambda(xy) = \chi\lambda(x)\chi\lambda(y)$. Another property of the group of characters is that if χ is some character, then χ^{-1} is the map that takes some $a \in \mathbb{F}^*$ to $\chi(a)^{-1}$, serving as a sort of reverse image mapping. This can be shown to be a character by similarly proving that it is a homomorphism. Finally, it is clear that the identity element of the group is the trivial character ε.

The fact that characters form a group is fundamental to later results. We need the following result.

Theorem 2.3. *The multiplicative group of $\mathbb{Z}/p\mathbb{Z}$, namely in our notation, $\mathbb{F}_p^*$, is cyclic.*

The proof is nearly identical to the proof of Theorem 1.6, but simpler due to the fact that we are dealing with the integers modulo p. We now show that the group of characters also forms a cyclic group of order $p - 1$.

Theorem 2.4. *The group of characters form a cyclic group of order $p - 1$. Furthermore, for some $a \in \mathbb{F}_p^*$ with $a \neq 1$, then there exists a character χ such that $\chi(a) \neq 1$.*

Proof. This theorem asserts that the characters form a cyclic group, so just as before, it is necessary to show that there exists a generator that, when raised to the $(p-1)$st power, yields the identity, namely ε. We first show that the order of the group is $p - 1$. By Theorem 2.3, $\mathbb{F}_p^*$

is cyclic. Let some $g \in \mathbb{F}_p^*$ be a generator. Then every $a \in \mathbb{F}_p^*$ can be represented as a power of g. Then $a = g^l$ for some exponent l. If χ is a character on $\mathbb{F}_p^*$, then it is true that $\chi(a) = \chi(g)^l$. What this shows is that the the character χ is restricted explicitly by the value of $\chi(g)$, the character acting on the generator. By Proposition 2.1, we know that $\chi(g)$ is a $(p-1)$st root of unity. Furthermore, by the definition of prime roots of unity, there are exactly $p-1$ roots. Therefore, the character group has order at most $p-1$.

Now we proceed to show the existence of a generator on the group of characters to show that it is cyclic. Define some function λ as $\lambda(g^k) = e^{2\pi i(\frac{k}{p-1})}$. The function λ is well-defined; this can be verified by considering its properties as a function. Furthermore, λ is also a character because it possesses the property that

$$\lambda(g^k) = \underbrace{\lambda(g)\cdots\lambda(g)}_{k} = \underbrace{e^{\frac{2\pi i}{p-1}}\cdots e^{\frac{2\pi i}{p-1}}}_{k} = \left(e^{\frac{2\pi i}{p-1}}\right)^k = e^{\frac{2k\pi i}{p-1}},$$

thus satisfying the multiplicative property of the character. If we want to show that the group is cyclic, we need to show that $p-1$ is the smallest integer n such that $\lambda^n = \varepsilon$. If $\lambda^n = \varepsilon$, then we must have $\lambda^n(g) = \varepsilon(g) = 1$ for some g. Alternatively, we also have $\lambda^n(g) = (\lambda(g))^n = (e^{\frac{2\pi i}{p-1}})^n = e^{\frac{2n\pi i}{p-1}}$. For this to be equivalent to 1, we must have that $p-1|n$. For some a, we have $\lambda^{p-1}(a) = \lambda(a)^{p-1} = \lambda(a^{p-1}) = 1$, which is only possible if $\lambda^{p-1} = \varepsilon$. Repeating this process, we can show that $\varepsilon, \lambda, \ldots, \lambda^{p-2}$ are distinct, and thus combined with the the fact that the group has a maximum order of $p-1$, we have that the group of characters is cyclic with generator λ.

Finally, to prove the final part, let there be some $a \in \mathbb{F}_p^*$ with $a \neq 1$. Then a can be represented as a power of the generator g, so $a = g^l$, with $p-1|l$. Then applying λ to a we have $\lambda(a) = \lambda(g^l) = \lambda(g)^l = (e^{\frac{2\pi i}{p-1}})^l = \lambda(g)^l = e^{\frac{2l\pi i}{p-1}}$. Since $p-1 \nmid l$, it must be true that $\lambda(a) \neq 1$, so we are done. ∎

As an analogue to Proposition 2.2 and as a result of Theorem 2.4, we can also consider summing over all characters and evaluating each one at a fixed variable from $\mathbb{F}_p^*$. This gives us the following proposition.

Proposition 2.5. *Let $a \in \mathbb{F}_p^*$ with $a \neq 1$. Then $\sum_\chi \chi(a) = 0$ over all characters χ.*

Proof. Let us denote the sum above with $S = \sum_\chi \chi(a)$. Since we assumed that $a \neq 1$, Theorem 2.4 asserts that there must exist some other character λ such that $\lambda(a) \neq 1$. Then we have

$$\lambda(a)S = \lambda(a)\sum_\chi \chi(a) = \sum_\chi \lambda(a)\chi(a) = \sum_\chi \lambda\chi(a)$$

by our discussion in Remark 5. Note that $\lambda\chi$ runs over an equivalent number of characters as χ from the group of characters, so we can assert that $\sum_\chi \lambda\chi(a) = S$ as we defined earlier. Therefore $\lambda(a)S = S$, so $(\lambda(a)-1)S = 0$, which since $\lambda(a) \neq 1$, is only possible if $S = 0$. ∎

2.2. **Gauss Sums.** As we have mentioned before, the multiplicative character generalizes the notion of the Legendre symbol. Similarly, it also generalizes the notion of a quadratic Gauss sum to the notion of a general Gauss sum. We define the Gauss sum as follows.

Definition 18 (Gauss Sum)**.** Let χ be some character on $\mathbb{F}_p$ and let $a \in \mathbb{F}_p$. Let

$$g_a(\chi) = \sum_{t\in\mathbb{F}_p} \chi(t)\zeta_p^{at},$$

where $\zeta_p = e^{2i\pi/p}$ is a pth root of unity. We say that $g_a(\chi)$ is a Gauss sum on $\mathbb{F}_p$ belonging to the character χ.

With this definition, we can see that a each Gauss sum is over a unique character, so we are dealing with sums of a singular character evaluated at all values of $\mathbb{F}_p$ equipped with an additional parametrization of t. We examine some basic properties of the Gauss sum.

Lemma 2.6. *The following are true.*

(1) *If $a \neq 0$ and $\chi \neq \varepsilon$, then $g_a(\chi) = \overline{\chi(a)} g_1(\chi)$.*
(2) *If $a \neq 0$ and $\chi = \varepsilon$ then $g_a(\varepsilon) = 0$.*
(3) *If $a = 0$ and $\chi \neq \varepsilon$, then $g_a(\chi) = 0$.*
(4) *If $a = 0$ and $\chi = \varepsilon$, then $g_a(\chi) = p$.*

Proof. Let us begin by proving (1). Let $a \neq 0$ and $\chi \neq \varepsilon$. Then

$$\chi(a) g_a(\chi) = \chi(a) \sum_{t \in \mathbb{F}_p} \chi(t) \zeta_p^{at} = \sum_{t \in \mathbb{F}_p} \chi(a)\chi(t)\zeta_p^{at} = \sum_{t \in \mathbb{F}_p} \chi(at)\zeta_p^{at} = g_1(\chi).$$

Then $\chi(a) g_a(\chi) = g_1(\chi)$, so $g_a = g_1(\chi)\chi(a)^{-1} = \chi(a^{-1}) g_1(\chi) = \overline{\chi(a)} g_1(\chi)$.

We now prove (2). Let $a \neq 0$ but $\chi = \varepsilon$. Since ε maps all $a \in \mathbb{F}_p$ to 1, we have

$$g_a(\varepsilon) = \sum_{t \in \mathbb{F}_p} \varepsilon(t) \zeta_p^{at} = \sum_{t \in \mathbb{F}_p} \zeta_p^{at}.$$

Recall that $\mathbb{F}_p$ is the integers modulo p, so t runs through all residue class representatives. Namely, it goes from $t = 0$ to $p - 1$. Therefore $\sum_{t \in \mathbb{F}_p} \zeta_p^{at} = \sum_{t=0}^{p-1} \zeta_p^{at}$. Since $a \neq 0$, we consider two cases: (a) when $a \equiv 0 \pmod p$ and (b) when $a \not\equiv 0 \pmod p$. Considering (a), if $a \equiv 0 \pmod p$, then for some $k \in \mathbb{Z}$, we have $\zeta_p^a = (e^{2i\pi/p})^{kp} = e^{2ki\pi} = 1$ for all values of k. Then $\sum_{t=0}^{p-1} (\zeta_p^a)^t = 1 + \cdots + 1 = p$. We now consider (b). If $a \not\equiv 0 \pmod p$, then we can evaluate the sum as a finite geometric series. Then

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

We know that $\zeta_p^{ap} = 1$ for all p prime, so $\frac{\zeta_p^{ap} - 1}{\zeta_p^a - 1} = 0/(\zeta_p^a - 1) = 0$.

To prove (3), let $a = 0$ and $\chi \neq \varepsilon$. Then $g_0(\chi) = \sum_{t \in \mathbb{F}_p} \chi(t) = 0$ by Proposition 2.2.

To prove (4), let both $a = 0$ and $\chi = \varepsilon$. Then $g_0(\varepsilon) = \sum_{t \in \mathbb{F}_p} \varepsilon(t) = \underbrace{1 + \cdots + 1}_{p} = p$. ∎

In our proof of (2), we split the evaluation of the sum into two cases with dependence on the value of a. This result can be summarized as follows.

Lemma 2.7.

$$\sum_{t=0}^{p-1} \zeta_p^{at} = \begin{cases} p, & a \equiv 0 \pmod p, \\ 0, & a \not\equiv 0 \pmod p. \end{cases}$$

Suppose we wish to determine the absolute value of the Gauss sum if the character is nontrivial. In prior literature it is possible to compute the value of the quadratic Gauss sum as well as its sign. Though we do not humor the intricacies of that proof as they lie beyond the scope of the paper, we compute the value of the general Gauss sum in Lemma 2.10. The following simple result is useful in proving the lemma and following results.

Corollary 2.8 (Corollary to Lemma 2.7)**.**

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

Proof. The proof follows by considering each case and evaluating accordingly. ∎

2.3. **Jacobi Sums.** The theory of Jacobi sums extends far beyond what we will discuss here, specifically in regard to solving Diophantine equations, but basic properties of the Jacobi sum will be useful later. We define a Jacobi sum as follows.

Definition 19 (Jacobi Sum)**.** Let χ and λ be two characters on $\mathbb{F}_p$. Then we define a Jacobi sum over χ and λ to be

$$J(\chi,\lambda)=\sum_{\substack{a+b=1\\ a,b\in\mathbb{F}_p}}\chi(a)\lambda(b),$$

where $a,b\in\mathbb{F}_p$.

The following theorem relates Jacobi sums to Gauss sums.

Theorem 2.9. *Let χ and λ be characters such that neither is the trivial character ε. Then*

(1) $J(\varepsilon,\varepsilon)=p$,
(2) $J(\varepsilon,\chi)=0$,
(3) $J(\chi,\chi^{-1})=-\chi(-1)$,
(4) *If the composition $\chi\lambda\neq\varepsilon$, then*

$$J(\chi,\lambda)=\frac{g(\chi)g(\lambda)}{g(\chi\lambda)}.$$

Proof. Note that $x,y\in\mathbb{F}_p$ in the following.

(1) follows from the fact that for all α we have $\varepsilon(\alpha)=1$, so that $J(\varepsilon,\varepsilon)=\sum_{a+b=1}\chi(a)\lambda(b)=\sum_{a+b=1}1=p$ since $\mathbb{F}_p$ has order p.

For (2), we have $J(\varepsilon,\chi)=\sum_{a+b=1}\varepsilon(a)\chi(b)=\sum_{a+b=1}\chi(b)$, which equates to 0 as an extension of the result in Proposition 2.2.

For (3), we have

$$J(\chi,\chi^{-1})=\sum_{a+b=1}\chi(a)\chi^{-1}(b)=\sum_{\substack{a+b=1,\\ b\neq 0}}\chi(ab^{-1})=\sum_{a\neq 1}\chi\bigg(\frac{a}{1-a}\bigg).$$

Let $q=\sum_{a\neq 1}\chi(\frac{a}{1-a})$. With the constraint that $c\neq 1$, we can express $a=\frac{c}{1+c}$. As the value of a runs over the entire field $\mathbb{F}_p$, with the exception that $a\neq 1$, simultaneously c also varies over $\mathbb{F}_p$, with the exception that $c\neq 1$. Therefore, by Proposition 2.1 we can take the sum

$$J(\chi,\chi^{-1})=\sum_{c\neq -1}\chi(c)=\sum_{c}\chi(c)-\sum_{c=-1}\chi(c)=-\chi(-1).$$

For (4), we have

$$\begin{aligned}g(\chi\lambda)=g(\chi)g(\lambda)&=\bigg(\sum_{x}\chi(x)\zeta^{x}\bigg)\bigg(\sum_{y}\lambda(x)\zeta^{y}\bigg)\\&=\sum_{x,y}\chi(x)\lambda(y)\zeta^{x+y}\\&=\sum_{t\in\mathbb{F}_p}\bigg(\sum_{x+y=t}\chi(x)\lambda(y)\bigg)\zeta^{t}.\end{aligned}$$

We consider two cases for the value of t. If $t=0$, then, choosing to sum over x and by the fact that the composition $\chi\lambda\neq\varepsilon$, clearly

$$\sum_{x+y=0}\chi(x)\lambda(y)=\sum_{x}\chi(x)\lambda(-x)=\sum_{x}\lambda(-1)\chi(x)\lambda(x)=\lambda(-1)\sum_{x}\chi\lambda(x)=0$$

by Proposition 2.2. In the case that $t \neq 0$, define two new elements x' and y' as $x = tx'$ and $y = ty'$. Then, if we have $x + y = t$, then substituting we have $tx' + ty' = t$, so that $x' + y' = 1$. Therefore

$$\begin{aligned}\sum_{x+y=t} \chi(x)\lambda(y) &= \sum_{x'+y'=1} \chi(tx')\lambda(ty') = \sum_{x'+y'=1} \chi(t)\lambda(t)\chi(x')\lambda(y') = \sum_{x'+y'=1} \chi\lambda(t)\chi(x')\lambda(y') \\ &= \chi\lambda(t)J(\chi,\lambda).\end{aligned}$$

If we substitute this into our evaluation of $g(\chi)g(\lambda)$, then we have

$$g(\chi)g(\lambda) = \sum_{t\in\mathbb{F}_p} \chi\lambda(t)J(\chi,\lambda)\zeta^t = J(\chi,\lambda)\sum_{t\in\mathbb{F}_p} \chi\lambda(t)\zeta^t = J(\chi,\lambda)g(\chi\lambda).$$

Setting this equal to $g(\chi)g(\lambda)$ and dividing by $g(\chi\lambda)$, we have

$$J(\chi,\lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}.$$

■

Before we can proceed, we require several technical lemmas. We have the following.

Lemma 2.10. *If $\chi \neq \varepsilon$ is a nontrivial character, then $|g(\chi)|^2 = p$.*

Proof. The proof is very similar to proofs regarding the quadratic Gauss sum discussed in [CR22]. We want to evaluate the sum

$$\sum_{a\in\mathbb{F}_p} g_a(\chi)\overline{g_a(\chi)}$$

in two different ways. We first want to evaluate the argument of the sum. Assume that $a \neq 0$. By (1) of Lemma 2.6, we can write

$$\overline{g_a(\chi)} = \overline{\chi(a^{-1})g(\chi)} = \chi(a)\overline{g(\chi)}.$$

Taking the conjugate, we also have $g_a(\chi) = \chi(a^{-1})g(\chi)$. Multiplying,

$$\chi(a)\overline{g(\chi)}\chi(a^{-1})g(\chi) = \overline{g(\chi)}g(\chi) = |g(\chi)|^2.$$

Since $\sum_{a\in\mathbb{F}_p}$ sums over all elements of the finite field $\mathbb{F}_p$ except $a = 0$, we consider this quantity $p - 1$ times, so

$$\sum_{a\in\mathbb{F}_p} g_a(\chi)\overline{g_a(\chi)} = (p-1)|g(\chi)|^2.$$

Similarly, considering two parameters x and y and writing the argument of the sum as a double sum, we have

$$g_a(\chi)\overline{g_a(\chi)} = \sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p} \chi(x)\overline{\chi(y)}\zeta^{ax-ay}.$$

Summing over all elements of $\mathbb{F}_p$ and applying Corollary 2.8 we have

$$\begin{aligned}\sum_{a\in\mathbb{F}_p}\sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p} \chi(x)\overline{\chi(y)}\zeta^{ax-ay} &= pp^{-1}\sum_{a\in\mathbb{F}_p}\sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p} \chi(x)\overline{\chi(y)}\zeta^{ax-ay}p \\ &= p\sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p} \chi(x)\overline{\chi(y)}\zeta^{ax-ay}\delta(x,y)\end{aligned}$$

where $\delta(x,y)$ denotes the Kronecker delta. If $x \not\equiv y \pmod p$ then the double sum will equate to 0, so we consider when $x \equiv y \pmod p$. If this is true, then the argument of the sum will run over exactly $p - 1$ elements, so that

$$p\sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p} \chi(x)\overline{\chi(y)}\zeta^{ax-ay}\delta(x,y) = p(p-1).$$

Equating our two evaluations, we have

$$(p-1)|g(\chi)|^2 = p(p-1)$$
$$|g(\chi)|^2 = p,$$

so we are done. ■

It is important to notice that the same result holds when $g(\overline{\chi})$ is considered instead, i.e. $|g(\overline{\chi})|^2 = p$. This is evident in the following.

Corollary 2.11.

$$g(\chi)g(\overline{\chi}) = \chi(-1)p.$$

Proof. Note first that $\chi(-1) = \overline{\chi(-1)}$ since both values equate to ± 1. Taking the conjugate of the equivalence given in Lemma 2.10, we have

$$\overline{\overline{g(\chi)}} = \overline{\chi(-1)g(\overline{\chi})}$$
$$g(\chi) = \chi(-1)\overline{g(\overline{\chi})}$$
$$g(\chi)g(\overline{\chi}) = \chi(-1)\overline{g(\overline{\chi})}g(\overline{\chi}) = \chi(-1)|g(\overline{\chi})|^2 = \chi(-1)p,$$

thereby proving the result. ■

The following result is general for characters, but will be useful when considering the relation between Gauss sums and Jacobi sums.

Theorem 2.12. *It is well known that there exist an infinite number of primes of the form* $p \equiv 1 \pmod{n}$ *since all primes are odd. As such, let* χ *be a character of order* $n > 2$*. Then*

$$g(\chi)^n = \chi(-1)p(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2}).$$

Proof. We can express (4) of Theorem 2.9 as $J(\chi,\chi)g(\chi\cdot\chi) = g(\chi)g(\chi)$. This gives $g(\chi)^2 = J(\chi,\chi)g(\chi^2)$. In the $n = 3$ case, multiply both sides by $g(\chi)$ and we have

$$g(\chi)^3 = J(\chi,\chi)g(\chi)g(\chi^2) = J(\chi,\chi)J(\chi,\chi\cdot\chi)g(\chi^3) = J(\chi,\chi)J(\chi,\chi^2)g(\chi^3).$$

We can continue multiplying the *LHS* and *RHS* by $g(\chi)$, so eventually, we have the $(n-1)$th case, so that

$$g(\chi)^{n-1} = J(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2})J(\chi,\chi^{n-1}).$$

Notice, however, by the fact that characters form a cyclic group, that $g(\chi)^{n-1} = g(\chi)^n g(\chi)^{-1} = g(\chi)^{-1} = g(\overline{\chi})$. Therefore we have $g(\chi)g(\chi^{n-1}) = g(\chi)g(\overline{\chi}) = \chi(-1)p$ by Corollary 2.11. Multiplying both sides of the equation above by $g(\chi)$, we have

$$g(\chi)^n = \chi(-1)p(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2}),$$

so we are done. ■

What follows from this is a corollary concerning the relationship between the cubic Gauss sum and the Jacobi sum.

Corollary 2.13. *Let* χ *be the cubic character. Then*

$$g(\chi)^3 = pJ(\chi,\chi).$$

Proof. This is a special case of Theorem 2.12. Take $n = 3$. Then, since -1 is clearly a cube, namely $\chi(-1) = \chi((-1)^3) = 1$, we have

$$g(\chi)^3 = \chi(-1)pJ(\chi,\chi) = pJ(\chi,\chi).$$

■

These results will be of utmost importance later when we seek to prove cubic reciprocity.

3. Cubic Reciprocity

Whereas quadratic reciprocity resides in $\mathbb{Z}$, cubic reciprocity resides in $\mathbb{Z}[\omega]$, the Eisenstein integers. In order to state and then prove cubic reciprocity, it is necessary to take a step back and examine characteristics of the ring $\mathbb{Z}[\omega]$. We will begin our examination by looking at the prime elements and units of $\mathbb{Z}[\omega]$.

3.1. **Units and Primes in $\mathbb{Z}[\omega]$.** We say that some ω is a cube root of unity, and that the set $\mathbb{Z}[\omega]$ contains complex number elements of the form $\alpha = a + b\omega$ for $a, b \in \mathbb{Z}$. It is in fact true that $\mathbb{Z}[\omega]$ is a ring. In our case, we consider when $\omega = -1/2 + i\sqrt{3}/2$.

We say that the *norm* of α, written as $N\alpha$, is the product of α and its conjugate, namely $N\alpha = \alpha\overline{\alpha} = a^2 - ab + b^2$. We may now consider the prime elements and units of $\mathbb{Z}[\omega]$. Note that this is possible explicitly because there inherently exists a notion of unique factorization in $\mathbb{Z}[\omega]$, and therefore we are able to consider the supposed "building blocks" of the ring. By means of notational convention, we denote $\mathbb{Z}[\omega] = D$.

Proposition 3.1. *Some $\alpha \in D$ is a unit of D if and only if $N\alpha = 1$. Furthermore, the units of D are $1, -1, \omega, -\omega, \omega^2, -\omega^2$.*

Proof. We prove the backward direction first. If $N\alpha = 1$, then by the definition of the norm, $\alpha\overline{\alpha} = 1$, which implies that α must be a unit.

To prove the reverse direction, suppose that α is a unit. By the definition of the unit, this must mean there exists some $\beta \in D$ such that $\alpha\beta = 1$. Therefore $N\alpha N\beta = 1$. However, since $N\alpha$ and $N\beta$ must be integers, in order for their product to be 1, they must both be 1. Therefore $N\alpha = 1$.

We now determine the units of D. Suppose that $\alpha = a + b\omega \in D$ is a unit. Then by definition of the norm we have $1 = a^2 - ab + b^2$. We may rewrite this as $4 = 4a^2 - 4ab + 4b^2$, or $4 = 4a^2 - 4ab + b^2 + 3b^2$ so $4 = (2a - b)^2 + 3b^2$. If we observe this Diophantine equation, we can see that there are only two sets of possible solutions. We write them as follows.

(1) $2a - b = \pm 1, b = \pm 1$,
(2) $2a - b = \pm 2, b = 0$.

We need to solve all 6 possible pairs of equations for a and b. The first is $2a - b = 1$ and $b = 1$. Then $a = b = 1$. The second is $2a - b = -1$ and $b = -1$. Then $a = b = -1$. The third is $2a - b = 1$ and $b = -1$. Then $a = 0$ and $b = -1$. The fourth is $2a - b = -1$ and $b = 1$. Then $a = -1$ and $b = 1$. The fifth is $2a - b = 2$ and $b = 0$. Then $a = 1$ and $b = 0$. The final is $2a - b = -2$ and $b = 0$. Then $a = -1$ and $b = 0$. Plugging these into the expression for α, we have the units $1 + \omega, -1 - \omega, -\omega, \omega, 1, -1$. An identity asserts that $\omega^2 + \omega + 1 = 0$, so rewriting, we can express the first two units as $-\omega^2$ and ω^2 respectively. ∎

Now that we have determined the units, we begin to observe characteristics of prime elements in $\mathbb{Z}[\omega]$.

Remark 6. Note that primes in $\mathbb{Z}$ are not necessarily prime in D. For example, consider the prime 7. We can express it as $7 = (3+\omega)(2-\omega) = 6 - 3\omega + 2\omega - \omega^2 = 6 - \omega - \omega^2 = 7$. Therefore, in order to distinguish between integer primes and primes in D, we refer to primes in D as primes and primes in $\mathbb{Z}$ as *rational primes*.

Proposition 3.2. *Let π be a prime in D. Then there is some rational prime p such that $N\pi = p$ or p^2. If $N\pi = p$ then π is not associate to a rational prime, and if $N\pi = p^2$ then π is associate to a rational prime.*

Proof. By the definition of the norm, we must have that $N\pi = \pi\overline{\pi} = n > 1$. Clearly, by the fundamental theorem of arithmetic, n is a product of rational primes. Therefore $\pi | p$ for some rational prime p. Since $\pi | p$, there exists some $\gamma \in D$ such that $p = \pi\gamma$. Then we may write

$N\pi N\gamma = N\pi\gamma = Np = p(p) = p^2$. For this equality to be true we must have either $N\pi = p^2$ with $N\gamma = 1$ or that $N\pi = N\gamma = p$. We consider the first case. If $N\pi = p^2$ and $N\gamma = 1$, then γ must be a unit of D, so π is associate to p. In the second case, suppose that π is associate to some other rational prime $q \in \mathbb{Z}$, with u a unit. Then we must have $\pi = uq$. Then $N\pi = Nuq = NuNq = 1(q)(q) = q^2$. Clearly, a rational prime cannot be a square of another rational prime, so π must not be associate to a rational prime. Thus we are done. ■

Proposition 3.3. *If there is some $\pi \in D$ such that $N\pi = p$ where p is a rational prime, then π is a prime in D.*

Proof. Assume that π is not prime in D. Then we can express π as a product of primes $\rho, \gamma \in D$, such that for $N\rho, N\gamma > 1$, we have $p = N\pi = N\rho\gamma = N\rho N\gamma$. However, since p is itself prime in $\mathbb{Z}$, this argument is not possible. Therefore π is prime in D. ■

Now that we have shown several properties of primes and units in D, we might be interested in classifying its primes.

Theorem 3.4. *Let p and q be rational primes.*

1. *If $q \equiv 2 \pmod 3$ then q is prime in D.*
2. *If $p \equiv 1 \pmod 3$, then $p = N\pi = \pi\overline{\pi}$, where π is a prime in D.*
3. *$3 = -\omega^2(1-\omega)^2$, and $1-\omega$ is prime in D.*

Proof. We begin by proving (1). Suppose that p is not a rational prime. Then we can write $p = \pi\gamma$ for $\pi, \gamma \in D$ and $N\pi, N\gamma > 1$. Then taking the norm of both sides, we have $Np = N\pi N\gamma$ so $p^2 = N\pi N\gamma$. Therefore we can write $N\pi = p$. Let $\pi \in D$ be of the from $\pi = a + b\omega$. Then we may write $N\pi = a^2 - ab + b^2 = p$. Using the same factorization in Proposition 3.1, we have $4p = (2a-b)^2 + 3b^2$. Reducing modulo 3, we have $p \equiv (2a-b)^2 \pmod 3$. If $3 \nmid p$, then it must be true that $p \equiv 1 \pmod 3$ because 1 is the only integer such that it is a nonzero square modulo 3. In other words, 1 is a quadratic residue modulo 3. If we again look at $a^2 - ab + b^2$ and substitute all pairs (a, b) where $a, b \in \mathbb{Z}/3\mathbb{Z}$, we can see that it is impossible for $a^2 - ab + b^2 \equiv 2 \pmod 3$. Note that no prime is congruent to 0 modulo 3. Therefore there must exist some rational prime $q \equiv 2 \pmod 3$ that is prime in D.

We now prove (2). Suppose that $p \equiv 1 \pmod 3$. Using Theorem 0.6, we have

$$\begin{aligned}\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) &= (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} \\ &= (-1)^{\frac{p-1}{2}+\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1.\end{aligned}$$

Therefore, -3 is a quadratic residue modulo 3, meaning that there exists some $a \in \mathbb{Z}$ such that $a^2 \equiv -3 \pmod 3$. We may rewrite this as $pb = a^2 + 3$ for some $b \in \mathbb{Z}$. Factorizing, we have that p divides $pb = (a - \sqrt{-3})(a + \sqrt{-3}) = (a + 1 + 2\omega)(a - 1 - 2\omega)$. Since D is a UFD, by the class inclusions mentioned in Remark 2, D is also an integral domain. Therefore an analogue of Euclid's lemma applies, so p must divide one of the factors. Assume that p is a prime. Since $p \neq 2$, it cannot divide the first factor. Furthermore, $2/p$ is rational, and so it cannot divide the second factor. Therefore p is not prime and can be expressed as $p = \pi\gamma$ for $\pi, \gamma \in D$ nonunits (as this guarantees that one is not associate to the other). Therefore, taking the norm of both sides, we have $p^2 = N\pi\gamma = N\pi N\gamma$, so that $p = N\pi = \pi\overline{\pi}$.

We now prove (3). Note that we can factorize $x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$. Therefore since $x^3 - 1 = (x-1)(x^2 + x + 1)$, we have that $x^2 + x + 1 = (x-\omega)(x-\omega^2)$. Letting $x = 1$, we have $3 = (1-\omega)(1-\omega^2) = (1-\omega)(1-\omega)(1+\omega) = (1+\omega)(1-\omega)^2$. Recalling that $1 + \omega = -\omega^2$,

we have $3 = -\omega^2(1-\omega)^2$. Taking the norm of both sides, we obtain

$$\begin{aligned} 3(3) &= N(-\omega^2)N(1-\omega)^2 \\ 9 &= N(\omega^3)N(1-\omega)^2 \\ 3 &= N(1-\omega), \end{aligned}$$

so we are done. ■

Now that we are equipped with information about prime and unitary elements of $\mathbb{Z}[\omega]$, we are prepared to introduce the second most important theorem in this paper.

3.2. **The Residue Class Ring $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ Is a Finite Field for π Prime.** In this subsection, we prove the most important connections between finite fields and reciprocity and outline why we needed to survey finite fields in so much depth. Much like in section 4.1 of [CR22], it is useful to think about notions of congruence in D as well. Let $\alpha, \beta, \gamma \in D$ with γ nonzero and a nonunit. Then we say that $\alpha \equiv \beta \pmod{p}$ if $\gamma | \alpha - \beta$. Note that this definition is very similar to the definition of congruence in $\mathbb{Z}$. Each residue class modulo γ may be combined in a quotient ring of the form $D/\gamma D$. To see how this is analogous to the conventional construction of a quotient ring, notice that $D/\gamma D$ runs through moduli $0, 1, 2, \ldots, \gamma - 1$, with each residue class forming a set of congruent numbers in D, much like how $\mathbb{Z}/n\mathbb{Z}$ runs through moduli $0, 1, 2, \ldots, n-1$. We refer to such a quotient ring as a *residue class ring modulo* γ. We now prove an important property of residue class rings.

Theorem 3.5. *Let some $\pi \in D$ be a prime. Then the residue class ring $D/\pi D$ is a finite field with $N\pi$ elements.*

Proof. In order to prove that $D/\pi D$ is a finite field, we need to first prove that it is a field, and then show that it has a finite number of elements; in this case, exactly $N\pi$. The second part of the proof requires that we consider all possible cases in Theorem 3.4.

We begin by showing that $D/\pi D$ is a field. Clearly, properties such as commutativity, transitivity, etc. natural to fields are present in $D/\pi D$. We need only show the existence of a unit in $D/\pi D$. Let there exist some $\alpha \in D$ with the property that $\alpha \not\equiv 0 \pmod{\pi}$. Since $D/\pi D$ is a commutative ring, it is an integral domain. Therefore for some elements $\beta, \gamma \in D$ it is possible to write $1 = \beta\alpha + \gamma\pi$. Reducing both sides modulo π, we have $\alpha\beta \equiv 1 \pmod{\pi}$. If we rewrite this congruence as an equality, we have that $[\alpha\beta] = [\alpha][\beta] = 1$, which is the requirement for $[\alpha]$ to be a unit in $D/\pi D$. Therefore $D/\pi D$ is a field.

We now prove that $D/\pi D$ has $N\pi$ elements by considering all possible cases of Theorem 3.4. We begin by supposing that $q \equiv 2 \pmod{3}$, where $q \in \mathbb{Z}$ is a rational prime. In order to show that there are $N\pi$ elements, we need to show that there is a complete set of coset, or residue class, representatives that has cardinality $N\pi$. Therefore, we need to show that the set $\{a+b\omega | 0 \leq a < q \wedge 0 \leq b < q\}$ is a complete set of coset representatives for D/qD with cardinality $Nq = q^2$. Suppose that there is some $\mu = m + n\omega \in D$ for $m, n \in \mathbb{Z}$. Then by the division algorithm, we can express $m = qs + a$ and $n = qt + b$, where $s, t, a, b \in \mathbb{Z}$ with the constraint that $a, b \in [0, q)$. By our definition of μ, it is clear that μ belongs to its own residue class modulo q, namely $\mu \equiv a + b\omega \pmod{q}$. We want to show that every coset representative μ can be constructed in this form, and is unique. Suppose that for $0 \leq a, b, a', b' < q$ that $a + b\omega \equiv a' + b'\omega \pmod{q}$. Rearranging, we have that

$$\begin{aligned} a - a' + b\omega - b'\omega &\equiv 0 \pmod{q} \\ (a - a') + (b - b')\omega &\equiv 0 \pmod{q} \\ \frac{a - a'}{q} + \frac{b - b'}{q}\omega &\in D. \end{aligned}$$

By the definition of elements of D, this means $(a-a')/q$ and $(b-b')/q$ are both integers, but since they are rational it is only possible if $a=a'$ and $b=b'$, thus proving uniqueness.

Now we show that this is true when $p \equiv 1 \pmod 3$ is a rational prime, and $p = \pi\overline{\pi} = N\pi$. Much like the first part of the proof, we want to show that a set is a complete set of coset representatives, but alternatively in the form $\{0, 1, 2, \ldots, p-1\}$ with cardinality $p = N\pi$. Begin by letting $\pi = a+b\omega$ be a prime. By the definition of the norm, $p = a^2-ab+b^2$, and it is obvious that $p \nmid b$. Let there exist $\mu = m+n\omega \in D$. Then there must exist some $c \in \mathbb{Z}$ such that $cb \equiv n \pmod p$. Then we have $\mu - c\pi \equiv m+n\omega-c(a+b\omega) \equiv m+n\omega-ac-bc\omega \equiv m-ac+(n-bc)\omega \equiv m-ac \pmod p$. Therefore it is also true that $\mu \equiv m-ca \pmod p$ by taking both sides modulo π. This shows that every element of D is congruent to a rational integer modulo π. Now we need to show modulo π, these elements correspond to one of $\{0, 1, 2, \ldots, p-1\}$. Let some $l \in \mathbb{Z}$. Then by the division algorithm we can write $l = sp+r$ for $s, r \in \mathbb{Z}$ and $0 \leq r < p$. Therefore $l \equiv r \pmod p$, and in fact $l \equiv r \pmod \pi$. Since we showed earlier that every element of D is congruent to a rational integer modulo π, this argument demonstrates that all elements of D are congruent to exactly one of $\{0, 1, 2, \ldots, p-1\}$ modulo p instead. Now we need only prove that these coset representatives are unique. Suppose that for $r, r' \in \mathbb{Z}$ and $0 \leq r, r' < p$, there is a congruence $r \equiv r' \pmod \pi$. Then $r-r' = \pi\gamma$ for some arbitrary $\gamma \in D$. Then taking the norm, we have $(r-r')^2 = N\pi\gamma = pN\gamma$. Then $p|(r-r')^2$, and so $p|(r-r')$. This implies that $r \equiv r' \pmod p$. Since we initially stated that r and r' are least residues modulo p, they are not only equivalent modulo p, but further satisfy $r = r'$, thus proving uniqueness.

The final case is when an element of D has a norm of 3. Proposition 3.3 guarantees that $1-\omega$ is prime in D because 3 is prime in $\mathbb{Z}$. In other words, since part (3) of Theorem 3.4 asserts that $1-\omega$ is prime in D, the residue class ring $D/(1-\omega)D$ contains exactly $N(1-\omega) = 3$ elements. Since $\pi = 1-\omega$, we will be proving this modulo $(1-\omega)$. To see what these cosets look like, we must determine what the elements of $D/(1-\omega)D$ are. Notice that since this is a residue class ring, we are taking the elements from the ideal $(1-\omega)D$ and combining them with the elements of D to form the set of coset representatives $\{r+(1-\omega)D | r \in D\}$. The three coset representatives are $0, 1$ and 2, so the respective cosets are $0+D/(1-\omega)D, 1+D/(1-\omega)D$, and $2+D/(1-\omega)D$. ■

The significance of the above result is that it allows us to consider elements of the ring $D/\pi D$ for π prime in such a way to be a finite field, which is a fundamental fact when studying cubic reciprocity considering many of the results that we derived in section 1.

3.3. **Statement of Cubic Reciprocity.** Now that we have formed the connection between finite fields and the residue class ring $D/\pi D$ for π prime, we can begin familiarizing ourselves with characteristics of the finite field. Since $D/\pi D$ is a finite field with order $N\pi$, its multiplicative group $(D/\pi D)^*$ has order $N\pi - 1$. Theorem 1.6 asserts that $(D/\pi D)^*$ must be cyclic, so with it we have a useful analogue in $D/\pi D$ to Fermat's Little Theorem, namely

Theorem 3.6 (Analogue to Fermat's Little Theorem in $D/\pi D$)**.** *If π is a prime and $\pi \nmid \alpha$, then*

$$\alpha^{N\pi-1} \equiv 1 \pmod \pi.$$

The proof of this follows similarly to Corollary 1.11, where instead we consider the residue classes modulo π and use the fact that $(D/\pi D)^*$ is cyclic.

In order to consider higher reciprocity, we must consider cases where $N\pi \neq 3$, namely, when $N\pi > 3$. Specifically, if $N\pi \neq 3$, then the residue classes formed by $1, \omega$ and ω^2 would necessarily be distinct, unlike if $N\pi = 3$. We show this as follows.

Suppose that $N\pi \neq 3$ in all following cases. Then suppose that ω and 1 belong to the same residue class, i.e. $\omega \equiv 1 \pmod \pi$. Then $\pi|1-\omega$. However, we showed before that $1-\omega$ is a prime element of $D/\pi D$, so it must be true that π is associate to $1-\omega$, i.e. there exists some unit u such

that $\pi = u(1-\omega)$. Taking the norm of both sides, we have $N\pi = NuN(1-\omega) = N(1-\omega) = 3$, but we assumed that $N\pi \neq 3$, so this is a contradiction. Therefore ω and 1 belong to distinct residue classes modulo π. We can repeat this for 1 and ω^2, and finally for ω and ω^2. For the first one, we assume that $\omega^2 \equiv 1 \pmod{\pi}$. Then $\pi|1-\omega^2$, so for some unit u, we have $\pi = u(1-\omega^2)$. Notice that $-\omega^2 = -\omega$, so $\pi = u(1-\omega)$. Taking the norm of both sides, we have $N\pi = NuN(1-\omega) = N(1-\omega) = 3$, but this is a contradiction, so $\omega^2 \not\equiv 1 \pmod{\pi}$. The same procedure can be done to show the distinctness of the remaining two residue classes.

Taking these three distinct residue class representatives, we have a cyclic group of order 3, namely $\{1, \omega, \omega^2\}$. By Theorem 0.2, this cyclic group divides the order of the group for which it is a subgroup, namely $|(D/\pi D)^*| = N\pi - 1$. Therefore $3|N\pi - 1$. Alternatively, if $\pi = q$ is some rational prime, then taking the norm of both sides, we have $N\pi = q^2$. Then $q^2 \equiv 1 \equiv N\pi \pmod{3}$. Proposition 3.3 asserts the existence of some other prime p such that $N\pi = p$, so $q^2 \equiv p \equiv 1 \pmod{3}$, which is the same as $3|p-1$. This leads us to the following result.

Proposition 3.7. *Let π be a prime with $N\pi \neq 3$ and $\pi \nmid \alpha$. Then there must exist a unique integer $m = 0, 1, 2$ such that*

$$\alpha^{\frac{N\pi-1}{3}} \equiv \omega^m \pmod{\pi}.$$

Proof. Rearranging the statement of Theorem 3.6, we have $\alpha^{N\pi-1} - 1 \equiv 0 \pmod{\pi}$, so $\pi|\alpha^{N\pi-1} - 1$. Factoring the *LHS*, we have

$$\alpha^{N\pi-1} - 1 = (\alpha^{\frac{N\pi-1}{3}} - 1)(\alpha^{\frac{N\pi-1}{3}} - \omega)(\alpha^{\frac{N\pi-1}{3}} - \omega^2)$$

so $\pi|(\alpha^{\frac{N\pi-1}{3}} - 1)(\alpha^{\frac{N\pi-1}{3}} - \omega)(\alpha^{\frac{N\pi-1}{3}} - \omega^2)$. As we discussed prior to this proof, it must be true that $3|N\pi - 1$ for each element of the cyclic group $\{1, \omega, \omega^2\}$. If π divided more than one factor, then the first and intermediate terms would no longer satisfy the property that $3|N\pi - 1$. Therefore, π must divide exactly one of the factors. Therefore, considering each factor, we have $\pi|(\alpha^{\frac{N\pi-1}{3}} - 1)$, $\pi|(\alpha^{\frac{N\pi-1}{3}} - \omega)$, and $\pi|(\alpha^{\frac{N\pi-1}{3}} - \omega^2)$. Naturally, it follows that for distinct integer values m running from 0 to 2, we have $\alpha^{\frac{N\pi-1}{3}} \equiv \omega^m \pmod{\pi}$. ∎

We now proceed to define the cubic residue character. Note the following.

Remark 7. While the vertical notation (a/p) is preferable for the Legendre symbol and there does exist a vertical cubic residue symbol $(\alpha/\pi)_3$, we instead use a shorthand as we will be writing it many times. Therefore, we denote the cubic residue character with $\chi_\pi(\alpha)$ to represent the cubic character of α modulo π.

Definition 20 (Cubic residue character)**.** Let $N\pi \neq 3$. We say that the cubic residue character of α modulo π is defined as

(1) $\chi_\pi(\alpha) = 0$ if $\pi|\alpha$,
(2) $\alpha^{\frac{N\pi-1}{3}} \equiv \chi_\pi(\alpha) \pmod{\pi}$ where

$$\chi_\pi(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is a cubic residue,} \\ \omega \text{ or } \omega^2 & \text{otherwise.} \end{cases}$$

Recall that the Legendre symbol outputted solutions to the equation $x^2 - 1 = 0$, so naturally, the cubic residue character outputs solutions to the equation $x^3 - 1 = 0$, roots of which are cube roots of unity. Note that both symbols can also output 0. We first prove an important property that the congruence of two cubic characters modulo π implies their equality, and follow by proving some other properties of the cubic residue character.

Lemma 3.8. *Let $\pi \in D$ be a prime. Then suppose that there exist some $a, b \in \{0, 1, \omega, \omega^2\}$ with the property that $a \equiv b \pmod{\pi}$. Then $a = b$.*

Proof. Notice that if $a \equiv b \pmod{\pi}$, then by the definition of congruence we can write $a-b = \pi\gamma$, where $\gamma \in D$. For $a = b$, the *RHS* must reduce to 0 modulo π.

We begin by taking the differences of each possible pair in the set $\{0, 1, \omega, \omega^2\}$. We obtain $-1, 1, -\omega, \omega, -\omega^2, \omega^2, 1-\omega, \omega-1, 1-\omega^2, \omega^2-1, \omega-\omega^2, \omega^2-\omega$. If we apply the identity $1+\omega+\omega^2 = 0$ we can reduce these differences to $-1, 1, -\omega, \omega, -1-\omega, 1+\omega, 1-\omega, \omega-1, 2+\omega, -2-\omega, 2\omega+1, -2\omega-1$. We want to show that these differences are always a multiple of some prime π.

To do this, it is sufficient to show that each of these differences is either prime or irreducible. If an element of D is a unit, then it is irreducible. Proposition 3.1 asserts that the units of D are $1, -1, \omega, -\omega, \omega^2, -\omega^2$, so when congruent modulo π these elements will also be equivalent. Part (3) of Theorem 3.4 asserts that $1-\omega$ is prime in D, so by the same argument, $-1-\omega$ is also prime in D. Furthermore, by applying the identity $1+\omega+\omega^2 = 0$, notice that $-1-\omega = \omega^2$ and $1+\omega = -\omega^2$, which are both units. Finally, applying Proposition 3.3, we need only check that the norm of the 4 differences is prime in $\mathbb{Z}$. We have $N(2+\omega) = N(-2-\omega) = 2^2 - 2(1) + 1 = 3$, which is prime in $\mathbb{Z}$. Similarly, $N(1+2\omega) = N(-1-2\omega) = 1^2 - 2(1) + 2^2 = 3$, which is also prime in $\mathbb{Z}$.

Therefore if each element is congruent to every other element modulo π, they must be equal. ∎

Proposition 3.9. *The following are true.*

(1) $\chi_\pi(\alpha) = 1$ *if and only if the congruence* $x^3 \equiv \alpha \pmod{\pi}$ *is solvable, namely, if* α *is a cubic residue modulo* π*, or* $\pi \nmid \alpha$.

(2)
$$\alpha^{\frac{N\pi-1}{3}} \equiv \chi_\pi(\alpha) \pmod{\pi}.$$

(3)
$$\chi_\pi(\alpha\beta) = \chi_\pi(\alpha)\chi_\pi(\beta).$$

(4) *If* $\alpha \equiv \beta \pmod{\pi}$*, then*
$$\chi_\pi(\alpha) = \chi_\pi(\beta).$$

Proof. To prove (1), consider Theorem 1.7. Let $\mathbb{F} = D/\pi D$, so that $\mathbb{F}^* = (D/\pi D)^*$. Furthermore, let $q = N\pi$ and $n = 3$ as we are dealing with a cubic. Therefore the congruence $x^3 \equiv \alpha \pmod{\pi}$ is solvable if and only if $\alpha^{(N\pi-1)/\gcd(3,N\pi-1)} \equiv 1 \pmod{\pi}$. This is solvable because $N\pi - 1$ is always divisible by the possible values of $\gcd(3, N\pi-1) = 1$ or 3, and 1 is always a cubic residue modulo π. Furthermore, there is either one solution or three solutions depending on the value of $\gcd(3, N\pi-1)$. This is the same idea as what is described in Remark 3 but applied to $D/\pi D$ instead.

(2) follows from the definition of the cubic residue character.

For (3) and (4) we use Lemma 3.8. To show (3), we have
$$\chi_\pi(\alpha\beta) \equiv (\alpha\beta)^{\frac{N\pi-1}{3}} \equiv \alpha^{\frac{N\pi-1}{3}}\beta^{\frac{N\pi-1}{3}} \equiv \chi_\pi(\alpha)\chi_\pi(\beta) \pmod{\pi}.$$
By Lemma 3.8, we have $\chi_\pi(\alpha\beta) = \chi_\pi(\alpha)\chi_\pi(\beta)$.

To show (4), notice that if $\alpha \equiv \beta \pmod{\pi}$, then
$$\chi_\pi(\alpha) \equiv \alpha^{\frac{N\pi-1}{3}} \equiv \beta^{\frac{N\pi-1}{3}} \equiv \chi_\pi(\beta) \pmod{\pi}.$$
By Lemma 3.8, we then have $\chi_\pi(\alpha) = \chi_\pi(\beta)$. ∎

We will now study cubic characters and their function, as the proof of cubic reciprocity requires the use of cubic Gauss sums.

Proposition 3.10. *The following are true.*

(1) $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$.

(2) $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$.

Proof. By definition, $\chi_\pi(\alpha) \in \{0, 1, \omega, \omega^2\}$. Squaring each one, we have $0, 1, \omega^2 = \omega$, and $\omega^4 = \omega^2$, all of which are equivalent to their conjugate.

To prove the second property, recall by Proposition 3.9 that $\alpha^{(N\pi-1)/3} \equiv \chi_\pi(\alpha) \pmod{\pi}$. Conjugating both sides, we have

$$\overline{\alpha}^{(N\overline{\pi}-1)/3} \equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}.$$

Notice that $\overline{\alpha}^{(N\overline{\pi}-1)/3} \equiv \chi_{\overline{\pi}}(\overline{\alpha}) \pmod{\overline{\pi}}$, but $N\overline{\pi} = N\overline{\pi} = N\pi$, so this is just $\chi_{\overline{\pi}}(\overline{\alpha}) \equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}$. By Lemma 3.8, we thus have $\chi_{\overline{\pi}}(\overline{\alpha}) = \overline{\chi_\pi(\alpha)}$. ■

From this we have the following corollary.

Corollary 3.11. *The following are true for a rational integer q.*

(1) $\chi_q(\overline{\alpha}) = \chi_q(\alpha^2)$.
(2) *If n is a rational integer coprime to q, then $\chi_q(n) = 1$.*

Proof. Since q is also a rational integer, it is obvious that $\overline{q} = q$. Therefore, by Proposition 3.10, we have $\chi_q(\overline{\alpha}) = \chi_{\overline{q}}(\overline{\alpha}) = \overline{\chi_q(\alpha)} = \chi_q(\alpha)^2 = \chi_q(\alpha^2)$.

To prove (2), notice similarly that $\overline{n} = n$. Therefore following the same procedure as (1) we have $\chi_q(n) = \chi_{\overline{q}}(\overline{n}) = \overline{\chi_q(n)} = \chi_q(n)^2$. It is impossible for $\chi_q(n)$ to be 0 as $n \nmid q$, so it must be that $\chi_q(n) = 1$. In this way, this corollary asserts that n is a cubic residue modulo q if both are rational integers. ■

Remark 8. As a special case of the law of cubic reciprocity, consider two primes $q_1 \neq q_2$ such that $q_1 \equiv q_2 \equiv 2 \pmod 3$. Then $\chi_{q_1}(q_2) = \chi_{q_2}(q_1)$. This is a special case of cubic reciprocity where both the modulus and argument are rational integers.

In order to state the general case, we need to extend this result to all prime elements in D.

Definition 21 (Primary)**.** Let $\pi \in D$ be prime. Then π is *primary* if $\pi \equiv 2 \pmod 3$.

We know that π is either rational or not rational. In the rational case, the previous discussion in Remark 8 applies. If π is not rational, then we consider when $\pi = a + b\omega$, namely when $a \equiv 2 \pmod 3$ and $b \equiv 0 \pmod 3$. Naturally, there exist 6 possible associates for every element π of D, as the 6 units of D act as multiplicative identities. However, it is necessary to derive a result that removes the ambiguity concerning which associate can be used for each element of D.

Lemma 3.12. *Let $N\pi = p \equiv 1 \pmod 3$. Exactly one associate of π is primary.*

Proof. Express $\pi = a + b\omega$ for $a, b \in \mathbb{Z}$. Then the associates of π are given as (1) π, since there is some unit u such that $\pi = u\pi$, (2) $\omega\pi$, since ω is a unit and $\pi = u(\omega\pi)$ for some unit u, (3) $\omega^2\pi$, since ω^2 is also a unit and $\pi = u(\omega^2\pi)$ for some unit u, (4) $-\pi$, for the same reason as (1), (5) $-\omega\pi$ for the same reason as (2), and (6) $-\omega^2\pi$ for the same reason as (3).

With all of these associates for π, we can now express each in terms of a and b. Namely, in order, we have

(1) $a + b\omega$,
(2) $\omega(a + b\omega) = a\omega + b\omega^2 = a\omega + b(-1 - \omega) = -b + (a - b)\omega$,
(3) $\omega^2(a + b\omega) = a\omega^2 + b\omega^3 = a(-1 - \omega) + b = (b - a) - a\omega$,
(4) $-a - b\omega$,
(5) $-\omega(a + b\omega) = -(-b + (a - b)\omega) = b + (b - a)\omega$,
(6) $-\omega^2(a + b\omega) = -((b - a) - a\omega) = (a - b) + a\omega$.

Among these we must determine the primary associate. Recall that $N\pi = p = a^2 - ab + b^2$. In this expression, only one of a and b is divisible by 3 since π is primary. Therefore, we proceed by assuming, WLOG, that $a \not\equiv 0 \pmod 3$. Then we further assume that $a \equiv 2 \pmod 3$. With these assumptions, we have that $p = a^2 - ab + b^2 \implies p \equiv 1 \equiv 2^2 - 2b + b^2 \pmod 3 \implies -3 \equiv$

$b(b-2) \equiv 0 \pmod 3$. We now consider two cases for b. If $3|b$, then we have $a \equiv 2 \pmod 3$ and $b \equiv 0 \pmod 3$, such that $\pi \equiv 2 \pmod 3$ and so $a + b\omega$ is primary. If $b \equiv 2 \pmod 3$, then we must also have $a \equiv 2 \pmod 3$, so $\pi \equiv 2 + 2\omega \equiv b + (b-a)\omega \pmod 3$. Therefore $b + (b-a)\omega$ is primary.

Now all that remains is to prove uniqueness. Let $a + b\omega$ be primary. This only occurs when $b \equiv 0 \pmod 3$, so looking at (2), it is clear that $-b + (a-b)\omega$ cannot be primary. The same is true for (3). For (4), notice that $b \equiv 0 \pmod 3$ implies that $\pi \equiv -a \equiv -2 \equiv 1 \pmod 3$, so $-a - b\omega$ is not primary. For (5), the argument is identical to (2). For (6), the argument is identical to (3). ■

Now we are equipped to state cubic reciprocity.

Theorem 3.13 (The Law of Cubic Reciprocity)**.** *Let π_1 and π_2 be primary. Furthermore, let $N\pi_1, N\pi_2 \neq 3$ with $N\pi_1 \neq N\pi_2$. Then*

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1).$$

In words, if π_1 and π_2 are primary with different norms not equal to 3, then π_1 is a cubic residue modulo π_2 if π_2 is a cubic residue modulo π_1, and π_1 is a cubic nonresidue modulo π_2 if π_2 is a cubic nonresidue modulo π_1.

This theorem requires that we consider 3 scenarios. The first scenario requires that we consider whether each π is rational or not. Namely, when both π_1 and π_2 are rational, when one of π_1 and π_2 is rational and the other is complex (i.e. in D), and when both π_1 and π_2 are complex. In Remark 8, we showed that the first case is trivial. We will also consider special cases of cubic reciprocity, namely when the input of the cubic character is either a unit, which we consider in the first supplement, or a special prime, which we consider in the second supplement. The first supplement is easily provable, but the second is a little more difficult.

3.4. **Supplements to Cubic Reciprocity.** We first consider cubic reciprocity when the inputs are the units, namely $1, \omega$, and ω^2 and their negatives. Clearly, $(-1)^3 = -1$, so -1 is always a cubic residue modulo any π prime, i.e. $\chi_\pi(-1) = 1$. By (2) of Proposition 3.9, we have that $\chi_\pi(\omega) = \omega^{\frac{N\pi-1}{3}}$. Therefore, the cubic character of units can be stated as follows.

Theorem 3.14 (First supplement to the Law of Cubic Reciprocity)**.** *Let ω be a cube root of unity. Then*

$$\chi_\pi(\omega) = \omega^{\frac{N\pi-1}{3}} = \begin{cases} 1 & \text{if } N\pi \equiv 1 \pmod 9, \\ \omega & \text{if } N\pi \equiv 4 \pmod 9, \\ \omega^2 & \text{if } N\pi \equiv 7 \pmod 9. \end{cases}$$

Proof. This is not difficult to show by considering each case. ■

Notice that in the identity $1 + \omega + \omega^2 = 0$, we can write $\omega^2 = -1 - \omega$. Therefore the final case requires us to consider the cubic residue character $\chi_\pi(1-\omega)$, where $1-\omega$ is also a prime in D as shown in Theorem 3.4. The proof is divided into two separate cases, specifically when the modulus is a rational prime $\pi = q$ and when the modulus is a non-rational prime π. The first case is easily considered, but the second case requires us to consider more about primary elements in D.

Theorem 3.15 (Second supplement to the Law of Cubic Reciprocity)**.** *Let $N\pi \neq 3$. If $\pi = q$ is rational, then write $q = 3m - 1$. If π is primary with $\pi \in D$ then write $\pi = a + b\omega$ and take $a = 3m - 1$. Then*

$$\chi_\pi(1-\omega) = \omega^{2m}.$$

Proof of Theorem 3.15 when $\pi = q$ is rational. This supplement requires us to consider two different cases. The first case is when $\pi = q$ is a rational prime, and the second is when $\pi = a + b\omega$ is non-rational. We consider the case where $\pi = q$ is a rational prime in this proof.

First notice that $(1-\omega)^2 = 1 - 2\omega + \omega^2 = -1 - \omega + 1 - 2\omega = -3\omega$. Therefore by definition of a character, $\chi_q((1-\omega)^2) = \chi_q(-3\omega) = \chi_q(-3)\chi_q(\omega)$. By Corollary 3.11, since we know that $\pi = q$ is a rational prime, and since $\gcd(-3, q) = 1$, we can write $\chi_q(\overline{-3}) = \chi_q(-3) = 1$. Taking $\pi = q$ to be a rational prime in Theorem 3.14, and since $N\pi = Nq = q^2$, we can write $\chi_q(\omega) = \omega^{(N\pi-1)/3} = \omega^{(q^2-1)/3}$. If we square both sides and notice that χ_q is inherently a cube root of unity then by Corollary 3.11 we have

$$\begin{aligned}(\chi_q(1-\omega)^2)^2 = \chi_q(1-\omega)^4 = (\chi_q(1-\omega))^3\chi_q(1-\omega) = \chi_q(1-\omega)\\ = \omega^{\frac{2}{3}\cdot\frac{q^2-1}{3}}.\end{aligned}$$

We now evaluate the *RHS*. Let $q = 3m - 1$. Then $q^2 - 1 = (3m-1)^2 - 1 = 9m^2 - 6m$. Therefore the exponent of the *RHS* is $2/3(9m^2 - 6m) = 6m^2 - 4m$. Reducing this modulo 3 because we are dealing with all possible powers of ω - namely, the cube roots of unity - we have $6m^2 - 4m \equiv -4m \equiv 2m \pmod 3$. Substituting, we have $\chi_q(1-\omega) = \omega^{2m}$, which is our desired result. ∎

The second case requires that we investigate some facts about primary elements in D. We begin with the following lemma.

Lemma 3.16. *Let α and β be two primary elements in D. Then $-\alpha\beta$ is primary.*

Proof. Let $\alpha = a + b\omega$ and $\beta = c + d\omega$. By definition of primary, we have $\alpha \equiv 2 \pmod 3$ and $\beta \equiv 2 \pmod 3$. For some $s, t \in \mathbb{Z}$, let $\alpha = 3s + 2$ and $\beta = 3t + 2$. Taking the product, we have

$$\begin{aligned}-\alpha\beta = -(3s+2)(3t+2) = -(9st + 6s + 6t + 4) &\equiv -4 \pmod 3\\ &\equiv 2 \pmod 3.\end{aligned}$$

Therefore $-\alpha\beta$ is primary. ∎

This can in fact be extended to a product of any number primary elements. This gives us a sort of primary factorization for primary elements in D.

Corollary 3.17. *Let $\gamma_1, \gamma_2, \ldots, \gamma_n \in D$ be primary. Then $(-1)^{n-1}\gamma_1\gamma_2\cdots\gamma_n$ is also primary.*

Proof. We prove this with induction. When $n = 2$, we have $(-1)^1\gamma_1\gamma_2$, which is primary by Lemma 3.16. Assume that this holds for some $n = k$. Then $(-1)^{k-1}\gamma_1\gamma_2\cdots\gamma_k$ is primary. We want to show that $(-1)^k\gamma_1\gamma_2\cdots\gamma_k\gamma_{k+1}$ is primary. Notice that

$$(-1)^k\gamma_1\gamma_2\cdots\gamma_k\gamma_{k+1} = (-1)(-1)^{k-1}\gamma_1\gamma_2\cdots\gamma_k(\gamma_{k+1}) = -(\gamma_{k+1})((-1)^{k-1}\gamma_1\gamma_2\cdots\gamma_k).$$

We know that γ_{k+1} is primary, so by Lemma 3.16, the product is also primary. ∎

This primary factorization allows us to consider the set of primaries as a UFD. In other words, if $\gamma \in D$ is some primary element, then we can write $\gamma = (-1)^{k-1}\gamma_2\gamma_2\cdots\gamma_k$, where, as in $\mathbb{Z}$, the γ_is need not be distinct primary primes elements.

Proof of Theorem 3.15 when π is a non-rational prime. We can now prove the second case of Theorem 3.15. Let $\pi = a + b\omega$ be a primary non-rational prime. This is only possible when $a \equiv 2 \equiv -1 \pmod 3$ and $b \equiv 0 \pmod 3$. For $m, n \in \mathbb{Z}$, let $a = 3m - 1$ and $b = 3n$. By definition, a is primary. If a is non-prime, then Corollary 3.17 asserts that for some sequence of primary primes a_i, we can write $a = (-1)^{n-1}a_1a_2\cdots a_n$. WLOG, we assume that a is a primary rational prime because we can choose any such a_i to be our a. By extension, we can say that $a + b$ is also a primary rational prime. Furthermore, since a and b are nonzero and we assumed π to be complex, it is also true that $\gcd(a, a+b) = \gcd(b, a+b) = \gcd(a, a+bw)$.

Notice that

$$\frac{Na-1}{3} = \frac{(3m-1)^2-1}{3} \equiv 2m \pmod 3. \tag{1}$$

Furthermore, notice that

$$a + b\omega \equiv b\omega \pmod a. \tag{2}$$

Notice that

$$\begin{aligned} a + b\omega &\equiv 0 \pmod \pi \\ a - a\omega + a\omega + b\omega &\equiv 0 \pmod \pi \\ a - a\omega &\equiv -(a+b)\omega \pmod \pi. \end{aligned} \tag{3}$$

We have the following. Recall that we defined $N\pi = p = a^2 - ab + b^2$, so

$$\begin{aligned} p &= a^2 - ab + b^2 \\ &= (3m-1)^2 - (3m-1)(3n) + (3n)^2 \\ \frac{p-1}{3} &= 3m^2 - 2m - 3mn + 3n^2 \\ &\equiv -2m + n \pmod 3. \end{aligned} \tag{4}$$

Finally, we have the following.

$$\begin{aligned} a + b &\equiv 0 \pmod{a+b} \\ a + b\omega &\equiv b\omega - b \pmod{a+b} \\ a + b\omega &\equiv -b(1-\omega) \pmod{a+b}. \end{aligned} \tag{5}$$

Using these results, we can compute the following. We use $\pi = a + b\omega$. Since a is a rational primary, by Remark 8, we can write

$$\begin{aligned} \chi_{a+b\omega}(1-\omega) &= \chi_a(b)\chi_{a+b\omega}(1-\omega) \\ &= \chi_a(b\omega^3)\chi_{a+b\omega}(1-\omega) \\ &= \chi_a(\omega^2)\chi_a(b\omega)\chi_{a+b\omega}(1-\omega). \end{aligned}$$

By (2), we can expand $\chi_a(\omega)^2\chi_a(a+b\omega)\chi_{a+b\omega}(1-\omega) = \omega^{\frac{2(Na-1)}{3}}\chi_{a+b\omega}(a)\chi_{a+b\omega}(1-\omega)$.

Combining (1) and (3) and then simplifying, we have

$$\begin{aligned} \omega^{2m}\chi_{a+b\omega}(a(1-\omega)) &= \omega^{2m}\chi_{a+b\omega}(-(a+b)\omega) \\ &= \omega^{2m}\chi_{a+b\omega}(-1)\chi_{a+b\omega}(\omega)\chi_{a+b\omega}(a+b) \\ &= \omega^{2m}(1)\omega^{\frac{N\pi-1}{3}}\chi_{a+b\omega}(a+b). \end{aligned}$$

Applying properties of the cubic character, (4), and (5), we have

$$\omega^{2m-2m+n}\chi_{a+b}(a+b\omega) = \omega^n\chi_{a+b}(-b(1-\omega)) = \omega^n\chi_{a+b}(1-\omega).$$

It is not difficult to verify the following by evaluating each part individually and simplifying.

$$\frac{2(N(a+b)-1)}{3} \equiv 2(m+n) \pmod 3. \tag{6}$$

Leading toward the final result and recalling that $(1-\omega)^2 = -3\omega$, we have

$$\begin{aligned}\chi_{a+b\omega}(1-\omega) = \omega^n\chi_{a+b}(1-\omega) = \omega^n\chi_{a+b}(1-\omega)^4 &= \omega^n(\chi_{a+b}(1-\omega)^2)^2\\ &= \omega^n\chi_{a+b}(-3\omega)^2\\ &= \omega^n(1)^2(1)^2\chi_{a+b}(\omega)^2\\ &= \omega^n(\omega^{\frac{N(a+b)-1)}{3}})^2.\end{aligned}$$

By (6), this is equivalent to writing $\omega^n\omega^{2(m+n)} = \omega^{2m+3n} = \omega^{2m}\omega^{3n} = \omega^{2m}$, which is what we wanted to prove. ■

In section 3.6, we will also introduce a special supplement of cubic reciprocity, namely the cubic character of 2 modulo π. We now proceed to prove cubic reciprocity.

3.5. **Proof of Cubic Reciprocity.** Before continuing with the proof, we need to make some preliminary statements regarding $D/\pi D$. We let $\pi \in D$ be a prime such that $N\pi = p \equiv 1 \pmod 3$. We showed earlier that $D/\pi D$ is a finite field with characteristic p, so naturally, it contains the field $\mathbb{Z}/p\mathbb{Z}$ as well. Both fields have p elements. Therefore, it is useful to define an isomorphism between $D/\pi D$ and $\mathbb{Z}/p\mathbb{Z}$. Namely, we have a bijection, where we map residue classes from $\mathbb{Z}/p\mathbb{Z}$ to their complex counterparts in $D/\pi D$. In this way, we are mapping the coset of some residue class in $\mathbb{Z}/p\mathbb{Z}$ to some other coset in $D/\pi D$. This isomorphism allows us to extend the cubic character χ_π to not only $D/\pi D$, but $\mathbb{Z}/p\mathbb{Z}$ as well. This means that the properties of the cubic character in $D\pi D$ are also valid in $\mathbb{Z}/p\mathbb{Z}$, allowing us to consider cubic Gauss sums $g_a(\chi_\pi)$ as well as cubic Jacobi sums $J(\chi_\pi, \chi_\pi)$ on $\mathbb{Z}/p\mathbb{Z}$. This realization is ultimately what allows us to prove cubic reciprocity, and explains why we investigated $D/\pi D$ so thoroughly.

Moving on, we need to prove some important properties about the Jacobi sum that relate directly to cubic reciprocity. We first have the following.

Lemma 3.18.

$$1^k + 2^k + 3^k + \cdots + (p-1)^k = \sum_{l=1}^{p-1} l^k \equiv \begin{cases} 0 & \text{if } p-1 \not\equiv 0 \pmod k \\ -1 & \text{if } p-1 \equiv 0 \pmod k. \end{cases}$$

Proof. The proof can follow by considering $[g]$ to be a primitive root of $(\mathbb{Z}/p\mathbb{Z})^*$, and noticing that it is identical to considering the complete set of representatives $\{[0],[1],[2],\ldots,[p-1]\}$, we can evaluate the sum over the entire finite field and evaluate each congruence depending on whether $p-1|k$ or $p-1 \nmid k$. ■

Proposition 3.19. *Let π be primary. Then*

$$J(\chi_\pi, \chi_\pi) = \pi.$$

Proof. Let there exist some other primary number π' such that $J(\chi_\pi, \chi_\pi) = \pi'$. By the definition of π we must have $N\pi = \pi\overline{\pi} = p = \pi'\overline{\pi}'$, since the norm of every primary element π is p. Therefore either $\pi|\pi'$ or $\pi|\overline{\pi}'$. However, since all prime elements are primary, each prime is coprime to every other prime, implying that we must have either $\pi = \pi'$ or $\pi = \overline{\pi}'$. We need to show that the second equation is not possible in order to show that π is unique and that there is only one such primary element.

We begin by writing out the cubic Jacobi sum. Then for some x that runs over $\mathbb{Z}/p\mathbb{Z}$, we have

$$J(\chi_\pi, \chi_\pi) = \sum_x \chi_\pi(x)\chi_\pi(1-x).$$

By Proposition 3.10, we can rewrite each character so that

$$\sum_x \chi_\pi(x)\chi_\pi(1-x) \equiv \sum_x x^{\frac{p-1}{3}}(1-x)^{\frac{p-1}{3}} \pmod \pi.$$

Notice that the degree of this polynomial is $\deg(f(x)) = 2((p-1)/3) < p-1$. Obviously, this means that $p-1 \nmid \deg(f(x))$. Analogously, by Lemma 3.18, and since x runs over all elements of $\mathbb{Z}/p\mathbb{Z}$, we can assert that

$$\sum_x x^{\frac{p-1}{3}}(1-x)^{\frac{p-1}{3}} \equiv 0 \pmod{p}.$$

Equivalence modulo p can be extended to equivalence modulo π. Therefore we can make the assertion that

$$\sum_x \chi_\pi(x)\chi_\pi(1-x) \equiv \sum_x x^{\frac{p-1}{3}}(1-x)^{\frac{p-1}{3}} \equiv J(\chi_\pi, \chi_\pi) = \pi' \equiv 0 \pmod{\pi}.$$

By definition of congruence, $\pi|\pi'$, which is impossible unless $\pi = \pi'$ since π and π' are both primary. ■

A simple corollary follows by substituting this result into Corollary 2.13 as follows.

Corollary 3.20.

$$g(\chi_\pi)^3 = p\pi.$$

Proof. By Corollary 2.13, we know that $g(\chi)^3 = pJ(\chi,\chi)$. Take the character to be the cubic character. Then by Proposition 3.19, we have $g(\chi_\pi)^3 = p\pi$. ■

We need a final fact about the Jacobi sum. The significance of the following result is that it allows us to make the assertion that the Jacobi sum $J(\chi,\chi)$ is a primary prime in D. In fact, since $J(\chi,\chi)$ is indeed primary, we have $J(\chi,\chi)\overline{J(\chi,\chi)} = p$, i.e. $J(\chi,\chi)$ has norm p. First, we must utilize a fact about algebraic integers. Let Ω denote the set of algebraic integers.

Lemma 3.21. *Let $\omega_1, \omega_2 \in \Omega$ and $p \in \mathbb{Z}$ be prime. Then*

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

Proof. The proof follows by expanding the *LHS* with the Binomial Theorem and noticing that all intermediate terms reduce to 0 modulo p. ■

In the following, assume that $\pi \in D$ is primary.

Proposition 3.22. *If $J(\chi,\chi) = a + b\omega$ where $\omega \in \mathbb{Z}[\omega]$, then $a \equiv -1 \pmod 3$ and $b \equiv 0 \pmod 3$.*

Proof. It is well known that the algebraic integers form a ring. Working with congruences in Ω and using Lemma 3.21 as well as the fact that $\chi(t)$ is a cubic character, we have

$$g(\chi)^3 = \left(\sum_{t\in\mathbb{F}_p} \chi(t)\zeta_3^t\right)^3 \equiv \sum_{t\in\mathbb{F}_p} \chi(t)^3\zeta_3^{3t} \pmod{3}.$$

Clearly $\chi(0) = 0$, and since $\chi(t)$ is a cubic character, $\chi(t)^3 = 1$ for nonzero t. Therefore

$$\sum_{t\in\mathbb{F}_p} \chi(t)^3\zeta_3^{3t} = \sum_{t\neq 0} \zeta_3^{3t} = \sum_{t\neq 0} e^{2\pi i t} = -1.$$

By Corollary 3.20, we have

$$g(\chi)^3 = pJ(\chi,\chi) \equiv a + b\omega \equiv -1 \pmod{3}.$$

Alternatively, consider the conjugate $\overline{\chi}$. By Proposition 3.10, we have that $\overline{g(\chi)} = g(\overline{\chi})$. Again applying Corollary 3.20, we have

$$g(\overline{\chi})^3 = pJ(\overline{\chi},\overline{\chi}) \equiv a + b\overline{\omega} \equiv -1 \pmod{3}.$$

Equating these equations modulo 3, we have

$$\begin{aligned}(a+b\omega)-(a+b\overline{\omega}) &\equiv -1-(-1) \pmod 3\\ b(\omega-\overline{\omega}) &\equiv 0 \pmod 3\\ b\left(\frac{-1+i\sqrt{3}}{2}-\frac{-1-i\sqrt{3}}{2}\right) &\equiv 0 \pmod 3\\ b\left(\frac{2i\sqrt{3}}{2}\right)=bi\sqrt{3} &\equiv 0 \pmod 3\\ -3b^2 &\equiv 0 \pmod 9.\end{aligned}$$

This implies that $3|b$, i.e. $b \equiv 0 \pmod 3$. Therefore $a+b\omega \equiv a \equiv -1 \equiv 2 \pmod 3$. ■

With all of these results, we are now sufficiently equipped to prove cubic reciprocity.

Proof of The Law of Cubic Reciprocity (Theorem 3.13). As indicated before, this is a proof by cases. In order to prove the full law, we need to consider when one of π_1 and π_2 is complex and the other is rational, and when both are complex.

We first prove the case when one is complex and the other is rational. In other words, we need to show that if $\pi_1 = q \equiv 2$ and $\pi_2 = \pi$ a primary with $N\pi = p$, then $\chi_\pi(q) = \chi_q(\pi)$. Begin by taking the expression in Corollary 3.20 and raising the *LHS* and *RHS* to a power of $(q^2-1)/3$. This results in the equivalence $g(\chi_\pi)^{((q^2-1)/3)\cdot 3} = g(\chi_\pi)^{q^2-1} = (p\pi)^{(q^2-1)/3}$. Take this equality modulo q, so by properties of the cubic character, we have $g(\chi_\pi)^{q^2-1} \equiv \chi_q(p\pi) \pmod q$. Notice that the *RHS* of the congruence can be expressed as $\chi_q(p\pi) = \chi_q(p)\chi_q(\pi)$. Clearly, since p and q are coprime, by Lemma 3.11, $\chi_q(p) = 1$. Therefore we can rewrite the congruence as

$$\begin{aligned}g(\chi_\pi)^{q^2-1} &\equiv \chi_q(p)\chi_q(\pi) \pmod q\\ g(\chi_\pi)^{q^2} &\equiv \chi_q(\pi)g(\chi_\pi) \pmod q.\end{aligned}$$

Now we can examine the *LHS*. If we expand the Gauss sum of the *LHS*, we have

$$g(\chi_\pi)^{q^2} = \left(\sum_{t\in\mathbb{F}_p} \chi_\pi(t)\zeta^t\right)^{q^2}.$$

The intermediate terms of this sum will have some form of q as a factor, so if we take this modulo q, we are left with

$$g(\chi_\pi)^{q^2} \equiv \sum_{t\in\mathbb{F}_p} \chi_\pi(t)^{q^2}\zeta^{q^2t} \pmod q.$$

Notice that $q \equiv 2 \pmod 3 \implies q^2 \equiv 1 \pmod 3$. Also, since $\chi_\pi(t)$ is a cube root of 1, meaning that is is a cube root of unity, we can express the *RHS* as a Gauss sum so that we can simplify to $g(\chi_\pi)^{q^2} \equiv g_{q^2}(\chi_\pi) \pmod q$. By Lemma 2.6 and since $\overline{q^2} = q^{-2}$ and $\chi_\pi(q^3) = 1$, the *RHS* in fact becomes $g_{q^2}(\chi_\pi) = \chi_\pi(q^{-2})g(\chi_\pi) = \chi_\pi(q^{-2})\chi_\pi(q^3)g(\chi_\pi) = \chi_\pi(q)g(\chi_\pi)$. Thus, setting the two equations equal to each other, we have the expression

$$\chi_\pi(q)g(\chi_\pi) \equiv \chi_q(\pi)g(\chi_\pi) \pmod \pi.$$

Notice that $g(\chi_\pi)g(\overline{\chi_\pi}) = \chi_\pi(-1)p = p$ by Corollary 2.11, so multiplying both sides by $g(\overline{\chi_\pi})$ we have

$$\begin{aligned}\chi_\pi(q)g(\chi_\pi) &\equiv \chi_q(\pi)g(\chi_\pi) \pmod q\\ \chi_\pi(q)p &\equiv \chi_q(\pi)p \pmod q\\ \chi_\pi(q) &\equiv \chi_q(\pi) \pmod q.\end{aligned}$$

By Lemma 3.8, this means that $\chi_\pi(q) = \chi_q(\pi)$.

Now we need to show that this is true when both π_1 and π_2 are non-rational. In this case, we have that the norm of both must be congruent to 1 modulo 3, i.e. $N\pi_1 = p_1 \equiv 1 \pmod 3$ and $N\pi_2 = p_2 \equiv 1 \pmod 3$. (Note in some way that this is a result of Lemma 3.4) Let some $\gamma_1 = \overline{\pi_1}$ and some $\gamma_2 = \overline{\pi_2}$. By Lemma 3.12, we know that exactly one associate of each p_1 or p_2 is primary, so we call them γ_1 and γ_2. Then $p_1 = \pi_1\gamma_1$ and $p_2 = \pi_2\gamma_2$. We approach this problem in a similar way to when one prime is rational and the other is complex. Take the expression in Corollary 3.20, and write it as $g(\chi_{\gamma_1})^3 = p_1\gamma_1$. Raising the *LHS* and *RHS* to a power of $(N\pi_2 - 1)/3$ or $(p_2 - 1)/3$ and taking the expression modulo π_2, we obtain

$$\begin{aligned}(g(\chi_{\gamma_1})^3)^{\frac{p_2-1}{3}} = g(\chi_{\gamma_1})^{\pi_2-1} = (p_1\gamma_1)^{\frac{p_2-1}{3}} &\equiv \chi_{\pi_2}(p_1\gamma_1) \pmod{\pi_2}\\ g(\chi_{\gamma_1})^{p_2}g(\chi_{\gamma_1})^{-1} &\equiv \chi_{\pi_2}(p_1\gamma_1) \pmod{\pi_2}\\ g(\chi_{\gamma_1})^{p_2} &\equiv g(\chi_{\gamma_1})\chi_{\pi_2}(p_1\gamma_1) \pmod{\pi_2}.\end{aligned}$$

We can simplify the *LHS*. Notice that

$$g(\chi_{\gamma_1})^{p_2} = \left(\sum_{t\in\mathbb{F}_p}\chi_{\gamma_1}(t)\zeta^t\right)^{p_2} \equiv \sum_{t\in\mathbb{F}_p}\chi_{\gamma_1}(t)^{p_2}\zeta^{p_2 t} \pmod{\pi_2}$$

since the intermediate terms are all congruent to 0 modulo π_2, and disappear after reduction. Notice that this is also a Gauss sum, namely $g_{p_2}(\chi_{\gamma_1})$, so $g(\chi_{\gamma_1})^{p_2} \equiv g_{p_2}(\chi_{\gamma_1}) \pmod{\pi_2}$. Notice that by Lemma 2.6 and Corollary 3.11, and since $\overline{p_2} = p_2$, the *RHS* of this congruence can be equivalently written as $g_{p_2}(\chi_{\gamma_1}) = \chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1})$. If we equate this to the expression derived above, then we have

$$\chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1}) \equiv g(\chi_{\gamma_1})\chi_{\pi_2}(p_1\gamma_1) \pmod{\pi_2}$$

Recall again that $g(\chi_1)\overline{g(\chi_{\gamma_1})} = p$, so multiplying both sides by $\overline{g(\chi_{\gamma_1})}$, and by Lemma 3.8 , we have

$$\begin{aligned}\chi_{\gamma_1}(p_2^2)p &\equiv p\chi_{\pi_2}(p_1\gamma_1) \pmod{\pi_2}\\ \chi_{\gamma_1}(p_2^2) &\equiv \chi_{\pi_2}(p_1\gamma_1) \pmod{\pi_2}\\ \chi_{\gamma_1}(p_2^2) &= \chi_{\pi_2}(p_1\gamma_1). \qquad (1)\end{aligned}$$

We now seek to evaluate the the same thing, but instead using the relation $g(\chi_{\pi_2})^3 = p_2\gamma_2$. Raising the *LHS* and *RHS* to a power of $(N\pi_1 - 1)/3$ or $(p_1 - 1)/3$ and taking the expression modulo π_1, we obtain

$$\begin{aligned}(g(\chi_{\pi_2})^3)^{\frac{p_1-1}{3}} &= (p_2\pi_2)^{\frac{p_1-1}{3}}\\ g(\chi_{\pi_2})^{p_1-1} &\equiv \chi_{\pi_1}(p_2\pi_2) \pmod{\pi_1}\\ g(\chi_{\pi_2})^{p_1} &\equiv \chi_{\pi_1}(p_2\pi_2)g(\chi_{\pi_2}) \pmod{\pi_1}.\end{aligned}$$

Evaluating the *LHS* of this congruence, notice that by using the same facts about Gauss sums as before we have

$$g(\chi_{\pi_2})^{p_1} = \left(\sum_{t\in\mathbb{F}_p}\chi_{\pi_2}(t)\zeta^t\right)^{p_1} \equiv \sum_{t\in\mathbb{F}_p}\chi_{\pi_2}(t)^{p_1}\zeta^{p_1 t} \pmod{\pi_1}.$$

This is also a Gauss sum, so we can write $g(\chi_{\pi_2})^{p_1} = g_{p_1}(\chi_{\pi_2}) = \chi_{\pi_2}(p_1^2)g(\chi_{\pi_2})$ since $\overline{p_1} = p_1$. Equating this to the equation derived above, we now have

$$\begin{aligned}\chi_{\pi_2}(p_1^2)g(\chi_{\pi_2}) &\equiv \chi_{\pi_1}(p_2\pi_2)g(\chi_{\pi_2}) \pmod{\pi_1}\\ \chi_{\pi_2}(p_1^2)p &\equiv \chi_{\pi_1}(p_2\pi_2)p \pmod{\pi_1}\\ \chi_{\pi_2}(p_1^2) &\equiv \chi_{\pi_1}(p_2\pi_2) \pmod{\pi_1}. \qquad (2)\end{aligned}$$

We have evaluated the cases for both π_1 and π_2, but now we are interested in relating them. We want to evaluate $\chi_{\gamma_1}(p_2^2)$. Notice that by (1) of Corollary 3.11 again, we can rewrite this as $\chi_{\gamma_1}(p_2^2) = (\chi_{\gamma_1}(p_2))^2 = \overline{\chi_{\gamma_1}(p_2)}$. Since $\overline{\gamma_1} = \overline{\overline{\pi_1}} = \pi_1$, and since $\overline{p_2} = p_2$, we have $\overline{\chi_{\gamma_1}(p_2)} = \chi_{\pi_1}(p_2)$, so

$$\chi_{\gamma_1}(p_2^2) = \chi_{\pi_1}(p_2). \tag{3}$$

Now we are able to finish the proof.

We compute the following. We have

$$\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1) = \chi_{\pi_1}(\pi_2)\chi_{\gamma_1}(p_2^2), \tag{4}$$

which follows by substituting (1). Using (3), we have that

$$\chi_{\pi_1}(\pi_2)\chi_{\gamma_1}(p_2^2) = \chi_{\pi_1}(\pi_2\chi_{\pi_1}(p_2) = \chi_{\pi_1}(p_2\pi_2).$$

By (2), we can write this as

$$\begin{aligned} \chi_{\pi_2}(p_1^2) &= \chi_{\pi_2}(p_1\pi_1\gamma_1) \\ &= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\gamma_1). \end{aligned} \tag{5}$$

Equating the *LHS* of (4) to (5) and dividing both sides by $\chi_{\pi_2}(p_1\gamma_1)$, we have

$$\begin{aligned} \chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1) &= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\gamma_1) \\ \chi_{\pi_1}(\pi_2) &= \chi_{\pi_2}(\pi_1), \end{aligned}$$

which is the statement of cubic reciprocity. ■

3.6. **Cubic Character of 2.** Now that we have proven cubic reciprocity, we might be interested in investigating what values might be cubic residues. The special case that we will consider in particular is the even prime 2. We will not prove the final result as it uses facts about Jacobi sums that lie beyond the scope of this paper, but a detailed proof may be found in Chapter 10 of [Rou12]. To begin, we have the following result about special rational primes.

Proposition 3.23. *If $q \equiv 2 \pmod 3$ is a rational prime, then every integer is a cubic residue modulo q.*

Proof. We begin by assuming that $q \equiv 2 \pmod 3$ is a rational prime. Since q is rational, we can work in the integers modulo q, namely $\mathbb{Z}/q\mathbb{Z}$. We define a group homomorphism $\phi : (\mathbb{Z}/q\mathbb{Z})^* \to (\mathbb{Z}/q\mathbb{Z})^*$ with the mapping $\phi(k) = k^3$ for some $k \in (\mathbb{Z}/q\mathbb{Z})^*$. By Theorem 0.3,

$$(\mathbb{Z}/q\mathbb{Z})^*/\mathrm{Ker}(\phi) \approx \mathrm{Im}(\phi).$$

We determine the kernel of ϕ. Clearly, it is only possible for some $k \in \mathrm{Ker}(\phi)$ if $k^3 = 1$, i.e. ϕ maps k to the identity of $(\mathbb{Z}/q\mathbb{Z})^*$, which is 1. However, Theorem 2.3 asserts that the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^*$ is cyclic with order $q-1$. But, $3 \nmid q-1$, so naturally the relation $k^3 = 1$ is possible if and only if $k = 1$, as it maps to the identity. Thus $\mathrm{Ker}(\phi)$ is trivial, in that it only contains one element, so that

$$|\mathrm{Im}(\phi)| = |(\mathbb{Z}/q\mathbb{Z})^*/\mathrm{Ker}(\phi)| = |(\mathbb{Z}/q\mathbb{Z})^*|/1 = |(\mathbb{Z}/q\mathbb{Z})^*|.$$

This satisfies the condition for ϕ to be surjective, so due to the mapping ϕ defined earlier, every element of $(\mathbb{Z}/q\mathbb{Z})^*$ is a perfect cube, i.e. every integer is a cubic residue modulo q. ■

Proposition 3.24. *The cubic congruence $x^3 \equiv 2 \pmod \pi$ where $\pi \in D$ is prime is solvable if and only if $\pi \equiv 1 \pmod 2$, i.e. if and only if $a \equiv 1 \pmod 2$ and $b \equiv 0 \pmod 2$ in $\pi = a + b\omega$.*

Proof. If $\pi = q$ is some primary rational prime, then Proposition 3.23 asserts that every integer is a perfect cube, so every integer is a cubic residue modulo q a primary rational prime. Therefore we need to prove that this result is true for a non-rational primary prime π. Let $\pi = a + b\omega$ be a primary prime. By Theorem 3.13, we have that $\chi_\pi(2) = \chi_2(\pi)$. We evaluate the *RHS* of this equality. We have

$$\pi^{\frac{N(2)-1}{3}} = \pi^{(4-1)/3} = \pi \equiv \chi_2(\pi) \pmod 2.$$

By Proposition 3.9, $\chi_2(\pi) = 1$, i.e. π is a cubic residue modulo 2, if and only if the congruence $x^3 \equiv \pi \pmod 2$ is solvable. This congruence is solvable, however, if and only if $\pi \equiv 1 \pmod 2$, because otherwise x would have to be complex and thus the congruence unsolvable. Therefore $\chi_2(\pi) = 1$ if and only if $\pi \equiv 1 \pmod 2$. Similarly, we have that $\chi_\pi(2) = 1$ if and only if $\pi \equiv 1 \pmod 2$. In either case, we thus the congruence $x^3 \equiv 2 \pmod \pi$ is solvable if and only if $\pi \equiv 1 \pmod 2$. ■

With this result, we can prove a condition for the solvability of $x^3 \equiv 2 \pmod p$, which allows us to characterize the cubic character of 2. Notice that Proposition 3.24 asserts that the modulus must be a rational primary prime such that $a \equiv 1 \pmod 2$ and $b \equiv 0 \pmod 2$. We use this fact concerning the modulus in the proof of the following due to Gauss.

Theorem 3.25. *Let $p \equiv 1 \pmod 3$. Then the congruence $x^3 \equiv 2 \pmod p$ is solvable if and only if there exist $C, D \in \mathbb{Z}$ such that $p = C^2 + 27D^2$.*

Proof. The proof may be found in Chapter 10 of [Rou12]. ■

4. A Brief Survey of Biquadratic Reciprocity

While Carl Friedrich Gauss had published 8 proofs of quadratic reciprocity by his death, he stated, without proof, cubic and biquadratic reciprocity. Though Gauss did not provide proofs, he stated that their proofs likely involved Gauss sums, a new technique for proving higher reciprocity laws. The proof of cubic reciprocity given in Section 3 is exactly using cubic Gauss sums. In this section we aim to introduce the fundamentals of the Gaussian integers $\mathbb{Z}[i]$ and outline the biquadratic reciprocity law.

4.1. **The Statement of Biquadratic Reciprocity.** As explained in the introduction, there are many connections between cubic and biquadratic reciprocity in that they both utilize finite fields. Throughout the rest of this section we let $D = \mathbb{Z}[i]$ denote the Gaussian integers. If some $\alpha \in D$ then $(\alpha) = \alpha D$ is the principal ideal generated by α. This is useful in defining the residue class ring later. It is well known that D is a Euclidean domain, i.e. there exists a Euclidean algorithm over D. Therefore, an analogue of Euclid's lemma applies such that if $\pi \in D$ is some irreducible element and $\alpha, \beta \in D$, then $\pi | \alpha\beta$ implies that $\pi | \alpha$ or $\pi | \beta$.

There is also a norm function over D so that $N\alpha = \alpha\overline{\alpha}$. Some $\alpha \in D$ is a unit if and only if $N\alpha = 1$. Suppose that $\alpha = a + bi$ is a unit. Then $\alpha | 1$, so for some $\beta \in D$ we have $\alpha\beta = 1$. Taking norms, we have $N\alpha\beta = N(1) = 1$. Now suppose that $N\alpha = 1$. Then by the definition of the norm $a^2 + b^2 = 1$. This is possible only if either a or b is 0, in which case the units of D are ± 1 and $\pm i$.

Let $\pi \in D$ be an irreducible.

Theorem 4.1. *The residue class ring $D/\pi D$ is a finite field with $N\pi$ elements.*

Proof. The proof of this fundamental result is very similar to Theorem 3.5. In this proof we use more facts about irreducibles in D. ■

A natural corollary as an analogue to Fermat's Little Theorem easily follows.

Corollary 4.2. *If $\pi \nmid \alpha$ then $\alpha^{N\pi - 1} \equiv 1 \pmod \pi$.*

The following is very similar to Proposition 3.7, and the proof is ultimately identical with consideration for $\mathbb{Z}[i]$ instead.

Proposition 4.3. *If $\pi \nmid \alpha$ and the ideal $(\pi) \neq (1+i)$ (the significance of this is due to the fact that $1+i$ is irreducible in D), then there exists a unique integer $j = 0, 1, 2, 3$ such that*

$$\alpha^{\frac{N\pi-1}{4}} \equiv i^j \pmod{\pi}.$$

As such, the biquadratic character is defined as follows.

Definition 22. If π is irreducible and $N\pi \neq 2$, for $\pi \nmid \alpha$ the biquadratic character of α is defined as $\chi_\pi(\alpha) = i^j$ where the value of j is determined exactly by Proposition 4.3. If $\pi|\alpha$ then we define $\chi_\pi(\alpha) = 0$.

With this definition we can state biquadratic reciprocity.

Theorem 4.4 (The Law of Biquadratic Reciprocity)**.** *Let $\pi, \lambda \in D$ be relatively prime primary elements. Then*

$$\chi_\pi(\lambda)\chi_\lambda(\pi) = (-1)^{\frac{N\lambda-1}{4}\cdot\frac{N\pi-1}{4}}.$$

While the statement of biquadratic reciprocity is more complex than cubic reciprocity, the mechanisms in its proof are fundamentally identical to that of cubic reciprocity. However, to full prove this result, it is necessary to prove consistently more results regarding Jacobi sums than we have in this paper. Full coverage of biquadratic reciprocity and its details can be found in chapter 9 of [IRR90].

4.2. **Higher Reciprocity.** As mentioned in the introduction, Eisenstein reciprocity was the first generalized reciprocity law. However, before obtaining generalized reciprocity, many attempts were made to generalize reciprocity beyond cubic and biquadratic reciprocity. Gauss (who was the first to state potential results for higher reciprocity), Jacobi, and Eisenstein made multiple attempts to no avail. In 1839, Jacobi stated - without proof - special cases of higher reciprocity for 5th, 8th, and 12th degrees, but he was unable to consider more general laws; see [Jac39]. The reason for the difficulty in generalizing reciprocity laws beyond 3rd and 4th degrees is that most sets of complex integers adjoined with increasing roots of unity fail to contain an analogue to the Euclidean Algorithm and do not form a UFD. The cases we have considered in this paper both rely on the fact that $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$ have the aforementioned properties. The existence of these properties allows us to consider their residue class rings and proceed from there.

Acknowledgements

The author would like to thank Dr. Tamar Avineri at the North Carolina School of Science and Mathematics for being a wonderfully supportive reviewer for this paper throughout the revision process; the author would also like to thank Dr. Tamar Avineri for insightful and useful conversations regarding mathematics and number theory. The author would further like to thank Dr. Simon Rubinstein-Salzedo for helpful insights and suggestions on numerous proofs throughout this paper. Finally, the author would like to thank Dr. Frank Thorne at the University of South Carolina for agreeing to endorse him on the arXiv.

References

[Col77] Mary Joan Collison. The origins of the cubic and biquadratic reciprocity laws. *Archive for History of Exact Sciences*, 17(1):63–69, 1977.

[CR22] Matias Carl Relyea. *Proofs and Applications of Quadratic Reciprocity*. Academia.edu, 2022.

[Gal02] Joseph A Gallian. *Contemporary Abstract Algebra*. Houghton Mifflin Company, 5th edition, 2002.

[Hau61] Alvin Hausner. On the quadratic reciprocity theorem. *Arch. Math.*, 12(1):182–183, dec 1961.

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

[Jac39] C.G.J. Jacobi. Ueber die complexen primzahlen, welche in der theorie der reste der 5ten, 8ten und 12ten potenzen zu betrachten sind. *Journal für die reine und angewandte Mathematik*, 1839(19):314–318, 1839.

[Rou12] Suzanne Rousseau. *Quadratic and Cubic Reciprocity*. EWU Masters Thesis Collection, 2012.