THE QUADRATIC AND CUBIC CHARACTERS OF 2

MATIAS C. RELYEA

Abstract. The solvability of the cubic congruence $x^3 \equiv 2 \pmod{p}$ is referred to as the *cubic character of 2*. In evaluating the cubic character of 2, we introduce the Eisenstein integers, Gauss and Jacobi sums, and the law of cubic reciprocity. We motivate this proof by giving ample historical information surrounding the early development of higher reciprocity laws as well as Gauss' proof of the solvability of the quadratic congruence $x^2 \equiv 2 \pmod{p}$; conventionally the *quadratic character of 2*. We simultaneously outline other relevant contributions by Fermat, Euler, Legendre, Jacobi, and Eisenstein.

From the Beginning

Many elementary number theory texts cover everything up to quadratic reciprocity and rarely anything further pertaining to reciprocity laws. While it is true that higher reciprocity laws such as cubic, biquadratic, Eisenstein, or even Artin reciprocity are rooted in mechanics that need a sufficient amount of algebraic number theory, their special cases are approachable with only a few additional ideas from algebra. In a similar way, the history of reciprocity laws from their origin is undoubtedly rich, hence Lemmermeyer's book [1]. It is illuminating to understand this rich history before encountering a modern treatment of reciprocity laws. In this paper, we are concerned with determining the solvability of the cubic congruence $x^3 \equiv 2 \pmod{p}$ using Gauss and Jacobi sums and an elementary representation of primes. We will also use Gauss' approach to solving the quadratic congruence $x^2 \equiv 2 \pmod{p}$ as the foundation for how our story develops. We do this while considering the nuance of historical contributions from Fermat, Euler, Gauss, Legendre, Jacobi, and Eisenstein.

The law of quadratic reciprocity is perhaps the most well-known theorem of elementary number theory, and it is typically the first major result encountered by most students in a first course. Many refer to the law as the pinnacle of elementary number theory; even Carl Friedrich Gauss, who gave the first proofs of the law, referred to it as the "Theorema Aureum", or the "Golden Theorem". The main theorem is as follows, where (a/p) denotes the Legendre symbol.

Theorem 1 (The Law of Quadratic Reciprocity)**.** *Let $p, q \in \mathbb{Z}$ be odd primes. Then*

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

While there exist multiple forms of the law, this form, which was first expressed by Adrien-Marie Legendre, is certainly the most elegant. Gauss proved this magnificent result a total of 8 times. When the law was initially stated, there were also two supplementary laws. In this paper, we are most interested in the second.

Theorem 2 (Second Supplement to Theorem 1)**.** *Let p be an odd prime. Then*

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

Date: October 2024.

This theorem concerns the solvability of the quadratic congruence $x^2 \equiv 2 \pmod p$, and its proof is infrequently touched upon in many elementary number theory classes. The solvability of this congruence is referred to as the *quadratic character of 2*; the reason for this language will be explained later. It is one of the two main results that we are interested in proving in a part of this paper.

Gauss determines the quadratic character of 2 in *Disquisitiones Arithmeticae* [2] and proves it using induction. While the conventional proof seen in most number theory texts uses Gauss' Lemma and a combinatorial argument, Gauss' inductive proof informs us exactly how he approached numerous other laws concerning residues and nonresidues (most notably, quadratic reciprocity). We give Gauss' proof from *Disquisitiones* in the next section.

Even fewer introductory university classes cover special cases of higher reciprocity. Nonetheless, we can still use elementary results to get a taste of the consequences of cubic reciprocity by considering the solvability of the special cubic congruence $x^3 \equiv 2 \pmod p$. The solvability of this congruence is referred to as the *cubic character of 2.* After proving quadratic reciprocity, Gauss took interest in higher reciprocity. In particular, he closely studied the solvability of congruences of the form $x^3 \equiv a \pmod p$ and $x^4 \equiv a \pmod p$; respectively, these are known as cubic and biquadratic reciprocity. Despite Gauss' fascination with these congruences, his theorems on cubic and biquadratic residues were only conjecture. In his second monograph in which he also considered biquadratic reciprocity, Gauss stated in a footnote - his only published reference to cubic residues - that

> [t]he theory of cubic residues must be based in a similar way on a consideration of numbers of the form $a+bh$ where h is an imaginary root of the equation $h^3-1=0$, say $h=(-1+\sqrt{-3})/2$, and similarly the theory of residues of higher powers leads to the introduction of other imaginary quantities [3] (translated [4, pg. 84]).

As we know it today, the value "h" that Gauss was referring to is ω, a cube root of unity, and the set of numbers of the form $a + bh$ is now known as the Eisenstein integers. Gauss' speculation came to no fruition, and it wasn't until 1844 that cubic reciprocity was first proven by Gotthold Eisenstein, who also happened to be one of Gauss' students. There is, however, some debate regarding whether Gauss was able to eventually produce a proof of the law in posthumous publications containing notes before or after Eisenstein published his manuscripts. In June of 1844, after reading Eisenstein's manuscripts on cubic reciprocity, Gauss even invited Eisenstein to his home in Göttingen to discuss them. The proof that Eisenstein produced used primary numbers and the residue class ring $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$, where π was some prime element of $\mathbb{Z}[\omega]$, as well as cubic Gauss sums, which Gauss had developed several years earlier.

In perfect analogy with the Legendre symbol, we let $(\alpha/\pi)_3$ be the cubic character of α for some prime element π and α an arbitrary element of $\mathbb{Z}[\omega]$. The law of cubic reciprocity can be stated as follows.

Theorem 3 (The Law of Cubic Reciprocity)**.** *Let π_1 and π_2 be primary elements of $\mathbb{Z}[\omega]$. Furthermore, let the norms $N\pi_1, N\pi_2 \neq 3$ with $N\pi_1 \neq N\pi_2$. Then*

$$(\pi_1/\pi_2)_3 = (\pi_2/\pi_1)_3.$$

The proof of cubic reciprocity is by no means simple and may be found completely in [5] as well as in chapter 9 of [6]. We cannot make clear enough the importance of finite fields to cubic reciprocity, and there are many relevant results. Most notably, we have

Theorem 4. *The multiplicative group of a finite field is cyclic.*

This result is the building block for any construction using finite fields that we have, and it can be proven using Möbius inversion. This result also has other far-reaching consequences, both elementary and complex[1].

While the main supplements of cubic reciprocity concern prime elements of the Eisenstein integers, the case of 2 is still incredibly nuanced. Concerning the cubic character of 2, Gauss wrote, in his posthumously published *Werke VIII*, that

> 2 is a cubic residue or nonresidue of a prime number p of the form $3n+1$, according to whether p is representable by the form $xx + 27yy$ or $4xx + 2xy + 7yy$ [7] (translated [4, pg. 85]).

The form $xx + 27yy$ is very similar to the form of primes in a result concerning the cubic character of 2 conjectured by Leonhard Euler between 1748 and 1750. At the time, a well known result of Pierre de Fermat - a consequence of his theorem on the sum of two squares - was that if $p \equiv 1 \pmod 3$, then for $a, b \in \mathbb{Z}$, the representation $p = a^2 + 3b^2$ was unique up to sign. Using intuition from Fermat's theorem, Euler stated, among other cubic characters of $3, 5, 6, 7$, and 10, that $(2/p) = 1$ if and only if $3|b$, where p was in the aforementioned representation $a^2 + 3b^2$ (see chapter 7 of [1]). This result is the main theorem of this article, and its formal proof is laid out in the final section. The main theorem is as follows.

Theorem 5. *If $p \equiv 1 \pmod 3$, then the cubic congruence $x^3 \equiv 2 \pmod p$ is solvable if and only if there exist integers C and D such that $p = C^2 + 27D^2$.*

While this result *was* conjectured by Euler as a result of his "genius", he did not provide a proof. Even though Theorem 5 was eventually proven by Gauss in notes that were published posthumously, this paper aims to illuminate the historical nuance of contributions from other mathematicians leading up to Gauss' work on the cubic character of 2, and more generally on cubic and biquadratic reciprocity.

The Quadratic Character of 2

Let us take a brief look at Gauss' evaluation of the quadratic character of 2.

Notice that (2) of Theorem 2 alternatively states that if $p \equiv \pm 1 \pmod 8$, then 2 is a quadratic residue modulo p, and if $p \equiv \pm 3 \pmod 8$, then 2 is a quadratic nonresidue. Gauss' statement of this result in *Disquisitiones* divides the entire result into multiple articles, but it is unsurprising considering this was how he addressed numerous problems. In condensed form, Gauss states the following.

Theorem 6 (Gauss' equivalent statement to (2) in Theorem 2 [2])**.** *Let $n \in \mathbb{Z}$.*

(1) $+2$ *will be a nonresidue,* -2 *a residue of all prime numbers of the form* $8n + 3$*,*
(2) $+2$ *and* -2 *will both be nonresidues of all prime numbers of the form* $8n + 5$*,*
(3) -2 *is a nonresidue,* $+2$ *a residue of all prime numbers of the form* $8n + 7$*,*
(4) 2 *and* -2 *are residues of all prime numbers of the form* $8n + 1$*.*

The concept of Gauss' proof is, as Gauss states, by "induction". However, it is more accurate to describe his proof as by strong induction with a flavor of contradiction.

Proof of Theorem 6. Let $n \in \mathbb{Z}$ in the following. We will be proving each part individually.

We prove (1) and (2) first. The first thing to notice is that if a composite number is of the form either $8n + 3$ or $8n + 5$, then it must involve some prime factor that is of either the form $8n+3$ or $8n+5$. Otherwise, the composite numbers would instead be in the form $8n+1$ or $8n+7$.

[1] A good elementary application of this result is that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. It is well known that $\mathbb{Z}/p\mathbb{Z}$ is a finite field. Since $\mathbb{Z}/p\mathbb{Z}$ is a finite field, by Theorem 4 its multiplicative group, $(\mathbb{Z}/p\mathbb{Z})^\times$, is cyclic with order $p-1$. Using this definition, Fermat's Little Theorem also becomes a direct corollary.

In general, no number of the form $8n+3$ or $8n+5$ can have 2 as a quadratic residue. Gauss states that there is no number of either form less than 100 such that 2 is a residue. The choice of 100 is arbitrary, and we could have just as easily chosen 97 or 235. Now we suppose that there are numbers of this form such that 2 is a residue, and we let the least be t. This t must be of the form $8n+3$ or $8n+5$. Clearly, 2 will be a residue of t but a nonresidue of everything less than t. By definition, $2 \equiv a^2 \pmod{t}$. There must exist an $a < t$ such that this is true. Rearrange, so $a^2 = 2 + tu$ for some integer u. Then $tu = a^2 - 2$. Notice that a^2 is in the form $8n+1$. Then tu is of the form $= 8n+1-2 = 8n-1$. Thus u will be of the form $8n+3$ or $8n+5$, depending on whether t is in the form $8n+5$ or $8n+3$ respectively. However, $a^2 = 2 + tu$ also implies that $2 \equiv a^2 \pmod{u}$, or 2 is a residue of u. Clearly, $u < t$, so there is a contradiction.

The proof of (3) is similar. Every composite number of the form $8n+5$ or $8n+7$ must involve a prime factor of either form, so -2 cannot be a residue of a number of the form $8n+5$ or $8n+7$. Suppose on the contrary that some did exist, with t as the least. We repeat the procedure and arrive at the congruence $-2 = a^2 - tu$. If $a < t$ and odd, then u will be of the form $8n+5$ or $8n+7$, depending on whether t is of the form $8n+7$ or $8n+5$ respectively. However, $a^2 + 2 = tu$ implies that $-2 \equiv a^2 \pmod{u}$, or -2 is a residue of u. Clearly, $u < t$, so there is a contradiction.

The case for (4) is trickier. Instead of using the strong induction approach, Gauss makes a clever deduction using congruences. We begin by letting $8n+1$ be some prime and a be a primitive root modulo $8n+1$. Since a is a primitive root modulo $8n+1$, we know that $a^{(8n+1)-1} = a^{8n} \equiv 1 \pmod{8n+1}$. We can factor the left-hand-side as $(a^{4n})^2 \equiv 1 \pmod{p}$. This is only possible if $a^{4n} \equiv \pm 1 \pmod{8n+1}$, but we take the negative part. Therefore $a^{4n} \equiv -1 \pmod{8n+1}$, or $a^{4n}+1 \equiv 0 \pmod{8n+1}$. Adding $2a^{2n}$ to both sides, we obtain $a^{4n}+2a^{2n}+1 \equiv 0 \pmod{8n+1}$, and after factoring, we obtain $(a^{2n}+1)^2 \equiv 2a^{2n} \equiv \pmod{8n+1}$. Alternatively, we subtract $2a^{2n}$ from both sides. After factoring, we obtain $(a^{2n}-1)^2 \equiv -2a^{2n} \pmod{8n+1}$. In either case, we have that $\pm 2a^{2n}$ are both quadratic residues. In other words,

$$\left(\frac{\pm 2a^{2n}}{8n+1}\right) = \left(\frac{\pm 2}{8n+1}\right)\left(\frac{a^{2n}}{8n+1}\right) = \left(\frac{\pm 2}{8n+1}\right)\left(\frac{(a^n)^2}{8n+1}\right) = \left(\frac{\pm 2}{8n+1}\right) = 1.$$

Therefore both 2 and -2 are quadratic residues modulo $8n+1$. ■

It is worth noting that Gauss didn't use Legendre symbols, as they were not introduced until 1798, when Legendre first formally defined them[2].

Example. As an example, say we want to determine whether there are solutions to the quadratic congruence $x^2 \equiv 2 \pmod{11}$. We can evaluate this as $(2/11) = (-1)^{\frac{11^2-1}{8}} = (-1)^{15} = -1$, so there is no solution. If we instead implement Theorem 6, we see that 11 is of the form $8(1)+3$, so 2 must be a nonresidue, which is equivalent.

Eisenstein Integers, Gauss and Jacobi Sums, and the Uniqueness of a Representation of Primes

Gauss also had considerations for the quadratic characters of other special integers in *Disquisitiones*, most using similar ideas of induction. Overall, these proofs cannot be described as anything more than elementary. Yet, these investigations were quintessential to the expansion of reciprocity laws in the early 19th century.

Gauss had already given various proofs for the quadratic characters of special integers and proved quadratic reciprocity in two different ways - one by induction and the other by quadratic

[2]While Gauss managed to prove the quadratic character of 2 using induction, Legendre was focused on the quadratic character of 2 using techniques stemming from quadratic forms, a technique that Gauss succeeded in implementing in his proof of quadratic reciprocity in *Disquisitiones*. Legendre's proof differs drastically from Gauss', but it is interesting nonetheless (see [8] for a detailed overview).

forms, yet - he was unsatisfied and continued to pursue more proofs. In his second memoir, Gauss stated that he

> ... sought to add more and more proofs of the already-known theorems on quadratic residues, in the hope that from these many different methods, one or another could illuminate something in the related circumstances [3] (translated [9, pg. 333]).

At the time, Gauss was thinking extensively about cubic and biquadratic reciprocity and believed that the key to confronting these "mysteries of the higher arithmetic" was intimately related to quadratic reciprocity. Gauss presented his 6th proof of quadratic reciprocity in 1807, and it used a new technique. In Gauss' words,

> ... the sixth proof calls upon a completely different and most subtle principle, and gives a new example of the wonderful connection between arithmetic truths that at first glance seem to lie very far from one another [3] (translated [9, pg. 333]).

In writing this proof, Gauss defined the notion of a quadratic Gauss sum[3]. While Gauss was ultimately unable to apply his newfound quadratic "Gauss" sum to proofs of cubic and biquadratic reciprocity, his formulations of the Gauss sum were used by many of his colleagues and students, most notably by Eisenstein in his successful attempts at proving higher reciprocity laws.

The idea surrounding Gauss sums is surprisingly difficult to motivate. In fact, they are so difficult to motivate within the scope of this article that we only offer some insight into how they were developed, but in messing with the technical details, we will take its conceptual foundations for granted. In this section, we are largely concerned with proving the uniqueness of primes of the form described in Theorem 5. On the way, we will take a look at Gauss sums and Jacobi sums and some of their fundamental properties.

As indicated by Gauss, and as mentioned earlier in [3], considerations of cubic congruences would likely involve complex numbers with a cube root of unity. Before we prove the elegant properties of Gauss sums, we are first inclined to formally investigate the Eisenstein integers.

The Eisenstein Integers. The most significant difference between quadratic reciprocity and higher reciprocity is the use of complex numbers. Whereas quadratic reciprocity can be expressed in elementary terms over $\mathbb{Z}$, higher reciprocity (specifically Eisenstein reciprocity) is expressed over the m-th cyclotomic field $\mathbb{Q}[\zeta_m]$ for an integer $m > 1$. The focus of this paper is on cubic reciprocity, which takes arguments from the ring $\mathbb{Z}[\omega]$, the Eisenstein integers. Every Eisenstein integer can be expressed in the form $a + b\omega$, where a and b are integers and $\omega = \zeta_3$ is a cube root of unity. We take ω to be $-1/2 + i\sqrt{3}/2$.

The most important property of the ring $\mathbb{Z}[\omega]$ is that it forms a unique factorization domain, or UFD. It is possible to show that since $\mathbb{Z}[\omega]$ is a UFD, it is also a Euclidean domain. Since $\mathbb{Z}[\omega]$ is a Euclidean domain, there need exist a norm function over $\mathbb{Z}[\omega]$ that takes elements of $\mathbb{Z}[\omega]$ and outputs elements of $\mathbb{Z}$. Let $\alpha = a + b\omega$. It happens that the norm over $\mathbb{Z}[\omega]$ is defined such that $N\alpha = \alpha\overline{\alpha} = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2$, and we will prove that this norm is uniquely expressible for some a and b in Proposition 14.

Necessarily, the ring $\mathbb{Z}[\omega]$ contains prime and unit elements. To determine the unitary elements of $\mathbb{Z}[\omega]$, we let $a + b\omega$ be a unit. Therefore, its norm must be 1, so determining the units amounts to determining the pairs of values of a and b such that $N(a + b\omega) = a^2 - ab + b^2 = 1$. It is

[3]Chapter 6 of Ireland and Rosen's book [6] brilliantly provides a modern proof of quadratic reciprocity using quadratic Gauss sums. It turns out that quadratic Gauss sums are so powerful that they also offer an incredibly comprehensive proof of the quadratic character of 2, requiring only some theorems regarding algebraic integers. A proof can be found in the same chapter.

important to note that $\mathbb{Z}[\omega]$ also contains $\mathbb{Z}$, so to distinguish between elements of each set, we say that prime elements of $\mathbb{Z}$ are "rational primes" and prime elements of $\mathbb{Z}[\omega]$ are just "primes"[4].

Now that we have a grasp of the basics of the Eisenstein integers, we will redirect ourselves toward considering some results concerning the Gauss sum and Jacobi sum. These results are technical and time-consuming, but most results are analogues to results concerning quadratic Gauss sums and follow general yet still similar proofs. Before we may take a look, however, we need to define a special symbol that characterizes (no pun intended) all residue symbols.

Multiplicative Characters. We are already familiar with the quadratic residue symbol, or the Legendre symbol (a/p). This symbol behaves in a simple way: you choose some integer a, and you map it to either $-1, 0$, or 1. In this way, the Legendre symbol is a map between the integers and the set $\{-1, 0, 1\}$. In the case of $n = 3$, the inputs can now be Eisenstein integers, with outputs as 0 and the cube roots of unity, or $\{0, 1, \omega, \omega^2\}$. As we continue increasing n, the domain and codomain expand even further. In general, this map can be defined as some mapping from the multiplicative group of a finite field to specific nonzero complex numbers. This is what we meant by "character". Throughout the rest of this paper, the finite field that we refer to is $\mathbb{Z}/p\mathbb{Z}$, but we write it as $\mathbb{F}_p$ and denote its multiplicative group as $\mathbb{F}_p^\times$. More formally,

Definition 1 (Multiplicative character)**.** We define the *multiplicative character* on a finite field $\mathbb{F}_p$ with p elements to be a mapping χ from the multiplicative group $\mathbb{F}_p^\times$ to the nonzero complex numbers such that for all $a, b \in \mathbb{F}_p^\times$,

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

An important remark regarding the multiplicative character is needed.

Remark 1. A character is a group homomorphism. An important fact is that multiplicative characters form a group with an identity character, ε, that maps all elements to the multiplicative identity. We refer to this character as the trivial character, and it satisfies $\varepsilon(a) = 1$ for all $a \in \mathbb{F}^\times$. Even more surprisingly, the group of characters is cyclic, a result that is worth convincing oneself of.

Multiplicative characters are the building blocks for reciprocity laws. Though applications of the multiplicative character are more prevalent in other areas of number theory, they are particularly interesting in reciprocity laws because of how well they describe residue symbols - in turn, this lets us construct some really interesting theory. We will start by looking at some general properties of the multiplicative character.

Since χ is a map that takes in elements of $\mathbb{F}_p^\times$, we are interested in what happens if we put in different elements $a \in \mathbb{F}_p^\times$. First and foremost, we would hope that a multiplicative character maps the identity to itself. In fact, we can write $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$, so the only possible value of $\chi(1)$ is 1, which indeed maps the identity to itself. As for any element a, it turns out that $\chi(a)$ is just a $(p-1)$st root of unity. This is because $a^{p-1} = 1$, so $1 = \chi(1) = \chi(a^{p-1}) = (\chi(a))^{p-1}$. From these two facts, it is also possible to show that $\chi(a^{-1}) = (\chi(a))^{-1} = \overline{\chi(a)}$.

An interesting fact about the Legendre symbol is that the sum of all Legendre symbols with arguments ranging from 0 to $p-1$ is 0. Perhaps a little unsurprisingly, the general multiplicative character satisfies the same property, as we see in the following.

Proposition 7. *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.*

[4]It is worth noting an important identity of cube roots of unity: $1 + \omega + \omega^2 = 0$.

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 $a\in\mathbb{F}_p^\times$ such that $\chi(a)\neq 1$, or χ does not map a to 1, hence χ is 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. ∎

We now turn our attention to Gauss and Jacobi sums.

Gauss and Jacobi Sums. We begin this technical subsection with a definition.

Definition 2 (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.

An important note is that by notational convention, when $a=1$, we write $g_1(\chi)=g(\chi)$. The next lemma provides us with a useful relationship between the Gauss sum and the character.

Lemma 8. *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 $g_a(\varepsilon)=0$.*

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

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: (1) when $a\equiv 0\pmod p$ and (2) when $a\not\equiv 0\pmod p$. Considering (1), 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 (2). 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 $\frac{\zeta_p^{ap}-1}{\zeta_p^a-1}=0/(\zeta_p^a-1)=0$. ∎

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 rewritten in the following form.

Lemma 9.
$$\sum_{t=0}^{p-1} \zeta_p^{at} = \begin{cases} p, & a \equiv 0 \pmod p, \\ 0, & a \not\equiv 0 \pmod p. \end{cases}$$

An easy corollary follows, where we denote the Kronecker delta with $\delta(x, y)$. The proof can follow by evaluating cases when either $x \equiv y \pmod p$ or $x \not\equiv y \pmod p$.

Corollary 10 (Corollary to Lemma 9)**.**
$$p^{-1} \sum_{t=0}^{p-1} \zeta_p^{t(x-y)} = \delta(x, y).$$

This is all we will need regarding the Gauss sum.

Now we define the Jacobi sum, which is a generalization of the Gauss sum. Gauss sums were briefly mentioned in *Disquisitiones* by Gauss, but Jacobi sums only surfaced in 1827 when Carl Gustav Jacob Jacobi sent a letter to Gauss with his work[5]. We begin with its definition.

Definition 3 (Jacobi sum)**.** Let χ and λ be two characters on $\mathbb{F}_p$. Then we define the *Jacobi sum* over χ and λ to be
$$J(\chi, \lambda) = \sum_{\substack{a+b=1 \\ a, b \in \mathbb{F}_p}} \chi(a)\lambda(b).$$

The defining property of the Jacobi sum is its relationship with the Gauss sum.

Proposition 11. *Let χ and λ be characters such that neither is the trivial character ε. Then if the composition $\chi\lambda \neq \varepsilon$,*
$$J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}.$$

Proof. To begin, we have
$$\begin{aligned} g(\chi\lambda) = g(\chi)g(\lambda) = \left(\sum_x \chi(x)\zeta^x\right)\left(\sum_y \lambda(x)\zeta^y\right) &= \sum_{x,y} \chi(x)\lambda(y)\zeta^{x+y} \\ &= \sum_{t \in \mathbb{F}_p} \left(\sum_{x+y=t} \chi(x)\lambda(y)\right)\zeta^t. \end{aligned}$$

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 $\chi\lambda \neq \varepsilon$,
$$\sum_{x+y=0} \chi(x)\lambda(y) = \sum_x \chi(x)\lambda(-x) = \sum_x \lambda(-1)\chi(x)\lambda(x) = \lambda(-1)\sum_x \chi\lambda(x) = 0$$
by Proposition 7. In the case that $t \neq 0$, we 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 $x' + y' = 1$. Therefore
$$\sum_{x+y=t} \chi(x)\lambda(y) = \sum_{x'+y'=1} \chi(tx')\lambda(ty') = \sum_{x'+y'=1} \chi(t)\lambda(t)\chi(x')\lambda(y') = \sum_{x'+y'=1} \chi\lambda(t)\chi(x')\lambda(y'),$$

[5]The theory of Jacobi sums is rich, and this richness can be seen on a very high level in chapter 4 of [1]. A more modern approach to motivating Jacobi sums can be seen through determining the number of solutions to the Diophantine equation $x^n + y^n = 1$, which is assessed with good rigor in chapter 8 of [6].

which equates to $\chi\lambda(t)J(\chi,\lambda)$. If we substitute this into our evaluation of $g(\chi)g(\lambda)$, then we have

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

Dividing both sides by $g(\chi\lambda)$, we thus have

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

■

The following result determines the value of the general Gauss sum, and we will then use it to determine the value of the Jacobi sum.

Lemma 12. *If $\chi \neq \varepsilon$ is a nontrivial character, then $|g(\chi)|^2 = p$.*

Proof. The main idea for the proof is to evaluate the sum

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

in two different ways and set the evaluations equal to one another. We will first evaluate the argument contained within the sum. Assume that $a \neq 0$. By (1) of Lemma 8, 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 and rearranging, we have

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

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 contained within the sum as a double sum, we have

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

Summing over all elements of $\mathbb{F}_p$ and applying Corollary 10, we have

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

If $x \not\equiv y \pmod{p}$ then the double sum will equate to 0 as $\delta(x,y)$ will certainly be 0, and by Proposition 7 the sum of all multiplicative characters over $\mathbb{F}_p$ is 0. Therefore we consider when $x \equiv y \pmod{p}$. If this is true, then every term except when $x \equiv y \pmod{p}$ will be counted, leaving a total of $p-1$ terms. Since $x \equiv y \pmod{p}$, necessarily $\zeta^{ax-ay} = 1$, so

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

Equating our two evaluations, we have

$$\begin{aligned}(p-1)|g(\chi)|^2 &= p(p-1) \\ |g(\chi)|^2 &= p,\end{aligned}$$

so we are done. ∎

Given the relation between the Gauss and Jacobi sum in Proposition 11 and the value of the Gauss sum in Lemma 12, it is only natural that we ask what the value of the Jacobi sum is.

Corollary 13 (Corollary to Proposition 11)**.** *Let χ and λ be nontrivial multiplicative characters. If their composition $\chi\lambda \neq \varepsilon$, then $|J(\chi, \lambda)| = \sqrt{p}$.*

Proof. We apply Proposition 11. Take the absolute value of both sides to obtain

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

By Lemma 12, $g(\chi) = \sqrt{p}$ for any character χ, so this is just $(\sqrt{p})^2/\sqrt{p} = \sqrt{p}$. ∎

If we recall that the norm of an Eisenstein integer is $a^2 - ab + b^2$, we will see a resemblance in the following result. It turns out that the uniqueness of the representation of the norm of an Eisenstein integer is crucial to proving the uniqueness of the representation of p in Theorem 5.

Proposition 14. *If $p \equiv 1 \pmod 3$, then there exist integers a and b such that we can write $p = a^2 - ab + b^2$.*

Proof. Since multiplicative characters form a cyclic group of order p by our discussion in Remark 1, there must be some generator element, say $\chi(a)$, that satisfies $\chi(a)^{p-1} = 1$. Here, we are dealing with characters that have order 3.

Since each character is of order 3, they must be roots of the polynomial equation $x^3 = 1$, i.e. they must be cube roots of unity, taking on values $1, \omega$, and ω^2. Therefore

$$J(\chi, \chi) = \sum_{u+v=1} \chi(u)\chi(v) = \sum_{u+v=1} \chi(uv)$$

must be an Eisenstein integer, and may be expressed in the form $J(\chi, \chi) = a + b\omega$, where $a, b \in \mathbb{Z}$. Recall that the norm of any Eisenstein integer in $\mathbb{Z}[\omega]$ is $N(a + b\omega) = a^2 - ab + b^2$. Taking the absolute value of both sides and recalling Corollary 13, we thus have

$$\begin{aligned} |a + b\omega| &= |J(\chi, \chi)| = \sqrt{p} \\ N(a + b\omega) &= N(\sqrt{p}) \\ a^2 - ab + b^2 &= (\sqrt{p})^2 = p, \end{aligned}$$

which is what we wanted to show. ∎

Consider the following example.

Example. Suppose that $p = 61 \equiv 1 \pmod 3$. Then a possible pair for a and b is $(9, 5)$, because $(9)^2 - (9)(5) + (5)^2 = 81 - 45 + 25 = 61$.

We are now prepared to prove the final result of this section. The proof for uniqueness can be completed by considering each case, but we give the much more approachable proof of existence in favor of its implications.

Theorem 15. *If $p \equiv 1 \pmod 3$, then there exist unique integers A and B that are determined up to sign such that $4p = A^2 + 27B^2$.*

Proof. We want to manipulate the expression $a^2 - ab + b^2$ to be in a unique form. Proposition 14 guarantees the existence of such integers a and b. Notice that even if a and b are positive, the expression is not unique because

$$\begin{aligned} a^2 - ab + b^2 &= (b - a)^2 - (b - a)b + b^2 \\ &= a^2 - a(a - b) + (a - b)^2, \end{aligned}$$

both of which are in the form $x^2 - xy + y^2$ for $x, y \in \mathbb{Z}$. We will manipulate this expression such that it is unique. Recall that $p = a^2 - ab + b^2$. Then

$$4p = 4a^2 - 4ab + 4b^2 = (2a-b)^2 + 3b^2 = (2b-a)^2 + 3a^2 = (a+b)^2 + 3(a-b)^2. \tag{0.1}$$

For this to be in the form that we want, we require $a - b$ to be a multiple of 3, or $3|a - b$. Otherwise, either $3|a$ or $3|b$, but not both. Suppose that $3 \nmid a$ and $3 \nmid b$. We then consider two cases: (1) when $a \equiv 1 \pmod 3$ and $b \equiv 2 \pmod 3$ and (2) when $a \equiv 2 \pmod 3$ and $b \equiv 1 \pmod 3$. Let $k, l \in \mathbb{Z}$. In the first case, we have

$$\begin{aligned}(3k+1)^2 - (3k+1)(3l+2) + (3l+2)^2 &= 9k^2 + 6k + 1 - 9kl - 6k - 3l - 2 + 4 \\ &= 9k^2 + 6k - 9kl - 6k - 3l + 9l^2 + 12l + 3 \\ &\equiv 0 \pmod 3.\end{aligned}$$

The second case follows similarly. Both cases show that $a^2 - ab + b^2 = p \equiv 0 \pmod 3$, which is impossible. Therefore $3|a - b$. Let $a - b = 3B$ and $a + b = A$. Substituting this into Equation (0.1), we obtain

$$4p = A^2 + 3(3B)^2 = A^2 + 27B^2,$$

which is in the form that we wanted. ■

Let us consider an example.

Example. Suppose that $p = 61$, so $61 \equiv 1 \pmod 3$. Theorem 15 asserts that there exist integers A and B such that $4(61) = 244 = A^2 + 27B^2$. By trial and error, we can see that when $A = 1$ and when $B = 3$, we have $244 = 1^2 + 27(3)^2 = 1 + 243 = 244$. This representation is unique up to sign, as $A = -1$ and $B = -3$ also satisfy the equality.

Theorem 15 is also central to proving Euler's other conjectures for the cubic residuacity of small primes $p \equiv 1 \pmod 3$ in the form a^2+3b^2. As known by Gauss, Lagrange (who contributed to numerous results concerning quadratic residues using quadratic forms), and others, this result is rooted in the study of binary quadratic forms, an area that initially developed from Fermat's theorem on the sum of two squares and was studied rigorously by Gauss in *Disquisitiones*[6].

The Law of Cubic Reciprocity

While we cannot contain the full breadth of cubic reciprocity in this paper, it is an integral part of what we will use to evaluate the cubic character of 2, and only needs some more algebra. Cubic reciprocity occurs over the residue class ring $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$, where π is some prime element of $\mathbb{Z}[\omega]$. It turns out that this residue class ring is also a finite field with exactly $N\pi$ elements, and thus it retains properties that we need; for instance its multiplicative group $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^\times$ contains $N\pi - 1$ elements, and by our discussion in Theorem 4 from earlier, it is cyclic. In summary,

Theorem 16. *The finite field $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ contains $N\pi$ elements.*

This finite field is also unique in that it has a notion of congruence modulo a complex prime π, and the division algorithm applies.

One important classifying result for primes in $\mathbb{Z}[\omega]$ is that if the norm of some Eisenstein integer is a rational prime, then the Eisenstein integer must also be prime. To show this, we use contradiction. Suppose that π is not prime in $\mathbb{Z}[\omega]$. Since it's not prime, without loss of generality, we can express it as a product of two non-unitary primes, say ρ and γ, so $\pi = \rho\gamma$. If we take the norm of both sides, we have $N\pi = p = N\rho\gamma = N\rho N\gamma$. However, since ρ and γ are

[6]More of the richness regarding how binary quadratic forms paint a more complete picture of the development of both cubic and biquadratic residues can be found in section 4 of [4].

non-unitary, each of their norms must be greater than 1. So, $N\rho N\gamma$ must also be greater than 1, which is impossible since p is a rational prime. Therefore π is prime.

For example, let $\pi = 3+\omega$, so $N(3+\omega) = 3^2 - 3(1) + 1 = 7$, which is prime. Therefore $3+\omega$ is prime and has no representation in terms of other primes. In summary,

Lemma 17. *If $\pi \in \mathbb{Z}[\omega]$ has the property that its norm $N\pi = p$ a rational prime, then π is prime in $\mathbb{Z}[\omega]$.*

An interesting implication of this result is that, by the definition of the norm and Proposition 14, the norm of each prime Eisenstein integer is uniquely expressible in terms of its components as a rational prime, or for some rational prime p we have $N\pi = N(a+b\omega) = p = a^2 - ab + b^2$. We will use this representation in our proof of Theorem 5.

We give an example of the residue class ring $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$.

Example. Consider the prime $3+\omega$. We already showed that $3+\omega$ is prime. We are looking at the residue class ring $\mathbb{Z}[\omega]/(3+\omega)\mathbb{Z}[\omega]$. This ring contains $N(3+\omega) = 7$ elements. It is possible to compute all 7 elements of this ring using brute force (i.e. considering all pairs (a,b) where $a,b \in \{0,\ldots,2\}$), but we will not do this. Note also that in this definition of the residue class ring, the prime $3+\omega$ acts as a modulus, so only one coset representative modulo $3+\omega$ is in the ring.

If we recall our discussion in Footnote 1, we can naturally suspect that there exists an analogous form to Fermat's Little Theorem over $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$. Indeed, since $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ is a finite field, its multiplicative group is cyclic. So, for some generator element $\alpha \in \mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$, all elements must satisfy

$$\alpha^{N\pi-1} \equiv 1 \pmod{\pi} \tag{0.2}$$

for $\pi \nmid \alpha$. This can be referred to as the analogue to Fermat's Little Theorem over $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$, and it is the fundamental equation for defining the cubic residue character.

Just as with quadratic characters, we need a corresponding cubic character. Note that since the quadratic character outputs solutions to the polynomial equation $x^2 = 1$, the cubic character outputs solutions to the polynomial equation $x^3 = 1$; namely, the cube roots of unity, $1, \omega$, and ω^2.

Definition 4 (Cubic residue character)**.** Let $N\pi \neq 3$ and $\alpha \in \mathbb{Z}[\omega]$. We say that the *cubic residue character of α modulo π* is defined as

(1) $(\alpha/\pi)_3 = 0$ if $\pi|\alpha$,
(2) $\alpha^{\frac{N\pi-1}{3}} \equiv (\alpha/\pi)_3 \pmod{\pi}$ where

$$(\alpha/\pi)_3 = \begin{cases} 1 & \text{if } \alpha \text{ is a cubic residue,} \\ \omega \text{ or } \omega^2 & \text{otherwise.} \end{cases}$$

The cubic character behaves nearly exactly like the Legendre symbol. Most importantly, there is multiplicativity, so for $\alpha, \beta \in \mathbb{Z}[\omega]$, we have

$$(\alpha\beta/\pi)_3 = (\alpha/\pi)_3(\beta/\pi)_3. \tag{0.3}$$

A proof follows by using Equation (0.2) and the definition of the cubic character. The most important definition over $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ in relation to cubic reciprocity is that of primary elements.

Definition 5 (Primary number)**.** Suppose that $\pi \in \mathbb{Z}[\omega]$ is prime. We say that π is *primary* if $\pi \equiv 2 \pmod{3}$.

Eisenstein defined primary numbers to give a stronger notion of primality over $\mathbb{Z}[\omega]$. One can verify that the product of primary numbers and the complex conjugate of a primary number remain primary. In fact, $\mathbb{Z}[\omega]$ is a UFD explicitly because there exists a unique primary factorization constructed from primary numbers. With these definitions, we would then be able to state the law of cubic reciprocity as in Theorem 3.

An important discussion concerning cubic reciprocity and its relationship with biquadratic reciprocity and the formulation of the cubic and biquadratic character of 2 is now due. While cubic reciprocity wasn't proven until 1844, the biquadratic law was proven nearly a decade earlier by Jacobi in a sequence of lectures given in Königsberg from 1836-1837 (see [1, pg. 200]). The reason for this nearly one decade gap between proofs is still widely debated, but it seems that the cubic law might have been easier than the biquadratic law: in a letter from Jacobi to Legendre in 1827, Jacobi wrote,

> Mr. Gauss presented to the Society of Göttingen two years ago a first memoir on the theory of biquadratic residues, which is much easier than the theory of cubic residues [10] (translated [1, pg. 224]).

Evidently, the biquadratic character of 2 was proven by Gauss in his first monograph of biquadratic reciprocity [11], which was published in 1828, far before his derivation of the cubic character of 2.

An example of applying cubic reciprocity is helpful to consider, though it should be noted that cubic characters are far more tedious to compute than Legendre symbols.

Example. [7]As an example, suppose we wish to determine the solvability of the congruence $x^3 \equiv (3-\omega) \pmod 5$. Note that this is valid because $N(3-\omega) = 13$ is prime. This amounts to evaluating the symbol $(3-\omega/5)_3$. The modulus is already primary, but we need to make the argument primary. Recall that the units of $\mathbb{Z}[\omega]$ are $\pm1, \pm\omega, \pm\omega^2$. We want to find some u such that $u(3-\omega) \equiv 2 \pmod 3$. After some trial and error, we use Footnote 4 to find that $\omega^2(3-\omega) = 3\omega^2 - 1 = -4 - 3\omega \equiv 2 \pmod 3$. Therefore $(3-\omega/5)_3 = (\omega^2/5)_3(-4-3\omega/5)_3$. By Theorem 3, this is $(\omega^2/5)_3(5/-4-3\omega)_3$. We want to reduce 5 modulo $-4-3\omega$. Using rules of complex numbers, we see that $5/(-4-3\omega) = (-20-15\omega^2)/13$. This fraction is approximately greater than $-1+\omega = -2-\omega^2$ using Footnote 4, so we reduce 5 by this multiple of $-4-\omega$. We obtain $5 - (-4-3\omega)(-2-\omega^2) = 2\omega^2$. Evaluating the final symbol, we have

$$\begin{aligned}\left(\frac{3-\omega}{5}\right)_3 &= \left(\frac{\omega^2}{5}\right)_3^{-1}\left(\frac{2\omega^2}{-4-3\omega}\right)_3 = \left(\frac{\omega^2}{5}\right)_3^{-1}\left(\frac{\omega^2}{-4-3\omega}\right)_3\left(\frac{2}{-4-3\omega}\right)_3 \\ &= \left(\frac{\omega^2}{5}\right)_3^{-1}\left(\frac{\omega}{-4-3\omega}\right)_3^2\left(\frac{-4-3\omega}{2}\right)_3 = \left(\frac{\omega}{5}\right)_3^{-2}\left(\frac{\omega}{-4-3\omega}\right)_3^2\left(\frac{\omega}{2}\right)_3 \\ &= (\omega^{\frac{N(5)-1}{3}})^{-2}(\omega^{\frac{N(-4-3\omega)-1}{3}})(\omega^{\frac{N(2)-1}{3}}) = (\omega^2)^{-2}(\omega)(\omega)^2 = \omega^{-1} = \omega^2.\end{aligned}$$

Therefore there is no solution to the congruence $x^3 \equiv (3-\omega) \pmod 5$.

The Cubic Character of 2

Whereas the quadratic character of 2 determines the solvability of $x^2 \equiv 2 \pmod p$ for an odd prime p, the cubic character of 2 determines the solvability of $x^3 \equiv 2 \pmod \pi$, where $\pi \in \mathbb{Z}[\omega]$ is a prime. Given that cubic reciprocity occurs over both Eisenstein primes and rational primes, the cubic character of 2 can be considered for both prime and non-prime moduli. We will first take a look at a neat result for rational primes.

---

[7]This computation features a number of identities that we will not state here. For those who wish to follow carefully, statements and proofs of the identities can be found in chapter 9 section 4 of [6] and section 3 of [5]

A Neat Rational Case. In our first case, we suppose that the modulus π is some rational prime q. Furthermore, since we deduced that π must be primary, we let $q \equiv 2 \pmod 3$. This gives us the following generalization that, while not particularly helpful in considering the general case, is immensely powerful when considering the cubic character of only rational integers.

Proposition 18. *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 $\phi : (\mathbb{Z}/q\mathbb{Z})^\times \to (\mathbb{Z}/q\mathbb{Z})^\times$ with the mapping $\phi(k) = k^3$ for some $k \in (\mathbb{Z}/q\mathbb{Z})^\times$. By the First Isomorphism Theorem,

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

We now determine the kernel of ϕ. For an element k to be contained within $\mathrm{Ker}(\phi)$, the map induced by ϕ must yield 1, the identity of $(\mathbb{Z}/q\mathbb{Z})^\times$. In other words, $k^3 = 1$ iff $k \in \mathrm{Ker}(\phi)$. However, Footnote 1 asserts that the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic and has 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

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

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

The implications of this result are beautifully simple. We look at an example.

Example. Suppose that the modulus is 11, because $11 \equiv 2 \pmod 3$. Proposition 18 tells us that every integer must be a cubic residue modulo 11. Since we are dealing modulo 11, every least residue $0, 1, \ldots, 10$ must be a cubic residue. We have

$$\begin{array}{lll} 0^3 \equiv 0 \pmod{11} & 1^3 \equiv 1 \pmod{11} & 2^3 \equiv 8 \pmod{11} \\ 3^3 \equiv 5 \pmod{11} & 4^3 \equiv 9 \pmod{11} & 5^3 \equiv 4 \pmod{11} \\ 6^3 \equiv 7 \pmod{11} & 7^3 \equiv 2 \pmod{11} & 8^3 \equiv 6 \pmod{11} \\ 9^3 \equiv 3 \pmod{11} & 10^3 \equiv 10 \pmod{11}. & \end{array}$$

Notice that each integer in the finite field $\mathbb{Z}/11\mathbb{Z}$ is represented, so every element is a cubic residue modulo 11, and we get that $(2/q)_3 = 1$ for free whenever $q \equiv 2 \pmod 3$.

The Complex Cases. The remaining cases are more difficult. Since Proposition 18 shows us that 2 is always a cubic residue modulo a rational prime, we consider the case where the modulus is a complex prime of the form $a + b\omega$.

The first result we will prove eliminates consideration of most complex elements in the final result. The first important step is noticing that the congruence $x^3 \equiv 2 \pmod \pi$, where $\pi \in \mathbb{Z}[\omega]$ is prime, is solvable if and only if every congruence $x^3 \equiv 2 \pmod{\pi'}$ is also solvable, where π' denotes an associate[8] of π. To differentiate between π and its associates, we can assume that π is primary.

Lemma 19. *The cubic congruence $x^3 \equiv 2 \pmod \pi$, where $\pi \in \mathbb{Z}[\omega]$ 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 $b \equiv 0 \pmod 2$.*

Proof. Let $\pi = a + b\omega$ be a primary prime. By Theorem 3, we have that $(2/\pi)_3 = (\pi/2)_3$. We evaluate the right-hand-side of this equality. By the definition of the cubic character,

$$\pi^{\frac{N(2)-1}{3}} = \pi^{(4-1)/3} = \pi \equiv (\pi/2)_3 \pmod 2.$$

[8]Recall that in a commutative ring R, two elements $r, s \in R$ are *associate* if there is some unitary element $u \in R$ such that $us = r$. In this case, we are asserting that there exists some $u \in \mathbb{Z}[\omega]$ such that $\pi = u\pi'$.

Notice that $(\pi/2)_3 = 1$, 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 π would no longer be prime if $\pi \equiv 0 \pmod 2$. Therefore $(\pi/2)_3 = 1$ if and only if $\pi \equiv 1 \pmod 2$. Similarly, we have that $(2/\pi)_3 = 1$ if and only if $\pi \equiv 1 \pmod 2$. In either case, we thus have that the congruence $x^3 \equiv 2 \pmod \pi$ is solvable if and only if $\pi \equiv 1 \pmod 2$. ■

The importance of Lemma 19 is that it reduces the problem to only considering some rational cases, so it is fundamental to proving Theorem 5. We are now in the final stretch. Euler's conjectures regarding the cubic residuacity of special integers only appeared posthumously in his *Tractatus* [12], which was published in 1849, despite the fact that the contents were originally written between 1748 and 1750. The history of who initially proved the rule is complex, as Gauss produced many relevant notes that were published posthumously. However, Gauss did manage to evaluate the cubic and biquadratic characters of 2 in his sketches [13] using the incredibly important ideas from Theorem 15, just as we do now.

Proof of Theorem 5. Let $\pi = a + b\omega$ be prime. By the definition of the norm, $N\pi = p = a^2 - ab + b^2$, where $a, b \in \mathbb{Z}$. We start by proving the forward direction by supposing that the cubic congruence $x^3 \equiv 2 \pmod p$ is solvable. Since π is associate to p, we know that $x^3 \equiv 2 \pmod \pi$ must also be solvable. So, by Proposition 19, $\pi \equiv 1 \pmod 2$. Notice that this implies that in the expression $a + b\omega$, a must be odd and b must be even.

Let us examine $p = a^2 - ab + b^2$. Multiplying both sides by 4, we obtain $4p = 4a^2 - 4ab + 4b^2 = 4a^2 - 4ab + b^2 + 3b^2$. Notice that we can factor the right-hand-side, yielding $4p = (2a - b)^2 + 3b^2$. Let us set $A = 2a - b$ and $B = b/3$. Plugging these in, we obtain

$$4p = A^2 + 3(3B)^2 = A^2 + 27B^2.$$

By Theorem 15, this representation is unique, in that both A and B are unique integers up to sign. We require that b be an integer, so it must be a multiple of both 2 and 3. Let $m, n \in \mathbb{Z}$, so $b = 2m \cdot 3n$. Therefore $B = 6mn/3 = 2mn$, which must be even. Since $4p = A^2 + 27B^2$, we also know that $A^2 + 27B^2$ must be even, which further requires A to be even. Substitute $C = A/2$ and $D = B/2$, which are both necessarily integers. Therefore $p = C^2 + 27D^2$, proving the forward direction.

We now prove the backward direction. We follow the same procedure, undoing what we did in the forward direction. Suppose that there exist $C, D \in \mathbb{Z}$ such that $p = C^2 + 27D^2$. Multiplying both sides by 4, we have

$$4p = 4C^2 + 4 \cdot 27D^2 = (2C)^2 + 27(2D)^2.$$

Again, by Theorem 15, there must exist some unique integer $B = \pm 2D$, which implies that B is even. Consequently b must also be even, implying that $b \equiv 0 \pmod 2$; necessarily, $\pi \equiv 1 \pmod 2$ since π is prime. Therefore by the backward direction of Proposition 19, the cubic congruence $x^3 \equiv 2 \pmod \pi$ is solvable. We now need to show that this extends further to modulus a rational prime p.

Theorem 16 shows that the residue class ring $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ contains exactly $N\pi = p$ elements. Therefore, among all elements of $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$, there must exist some $k \in \mathbb{Z}$ such that $k^3 \equiv 2 \pmod \pi$. By definition of congruence, this means $\pi|(k^3 - 2)$. By our discussion preceding Footnote 8, it must also be true that $\pi'|(k^3 - 2)$, where π' is some associate of π. Since $\pi\pi' = p$, we have $p|(k^3 - 2)^2$, so $p|(k^3 - 2)$. Rewriting, this implies that $k^3 \equiv 2 \pmod p$, or k is a solution to the cubic congruence $x^3 \equiv 2 \pmod p$. ■

Notice that this result is only applicable when considering moduli greater than or equal to 28, since $C^2 + 27D^2 \geq 28$ when $C, D \geq 1$.

Example. In this first example we examine the case where the modulus is 29. Notice that there is no ordered pair (A, B) such that $29 = A^2 + 27B^2$. Therefore there is no solution to the congruence $x^3 \equiv 2 \pmod{29}$.

Example. In this second example we let the modulus be 259. Since $259 = 4^2 + 27(3^2)$, there must exist a solution to the cubic congruence $x^3 \equiv 2 \pmod{259}$, so $(2/259)_3 = 1$.

Acknowledgements

The author would like to thank Dr. Tamar Avineri at the North Carolina School of Science and Mathematics for providing immense support throughout the writing and revision of this paper.

References

[1] F. Lemmermeyer. *Reciprocity Laws: From Euler to Eisenstein.* Springer Monographs in Mathematics. Springer Berlin Heidelberg, 2000.

[2] Carl Friedrich Gauß. *Disquisitiones Arithmeticae: Engl. Ed.* Springer, 1986.

[3] Biblioteca Provinciale and Reale Biblioteca di Marina. *Werke Carl Friedrich Gauss: 2.* Königlichen Gesellschaft der Wissenschaften, 1863.

[4] D.A. Cox. *Primes of the Form x2+ny2: Fermat, Class Field Theory, and Complex Multiplication.* Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 2013.

[5] Matias Carl Relyea. On finite fields and higher reciprocity, 2024.

[6] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*, volume 84. Springer Science & Business Media, 1990.

[7] Carl Friedrich Gauß. *Werke: Vol. 8*, volume 8. Teubner, 1900.

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

[9] Jeremy Gray. *A History of Abstract Algebra: From Algebraic Equations to Modern Algebra.* Springer, 2018.

[10] C G J Jacobi. *Letter to Legendre of 5.* New York; Berlin, 1827.

[11] Carl Friedrich Gauß. Theoria residuorum biquadraticorum -commentatio prima. *Werke (Göttingen: Königlichen Gesellschaft der Wissenschaften, 1876)*, pages 65–92, 1876.

[12] Leonhard Euler. *Tractatus de numerorum doctrina capita XVI, quae supersunt.* Euler Archive - All Works, 1849.

[13] Carl Friedrich Gauß. Notizen über cubische und biquadratische reste. *Nachlaß*, 1900.

Matias C. Relyea is a senior at the North Carolina School of Science and Mathematics. Currently, he is most interested in number theory, but he hopes to widen his knowledge of other areas of mathematics. In his free time, Matias enjoys playing the violin and TeXnique.