RINGS OF INTEGERS, GAUSS-JACOBI SUMS, AND THEIR APPLICATIONS

CHAOFAN CHEN

Abstract. In this paper we shall explore the structure of the ring of algebraic integers in any quadratic extension of the field of rational numbers $\mathbb{Q}$, develop the concepts of Gauss and Jacobi sums, and apply the theory of algebraic integers and that of Gauss-Jacobi sums to solving problems involving power congruences and power sums as well as to proving the quadratic and cubic reciprocity laws. In particular, we shall address the problem of when a rational prime (that is, a prime in $\mathbb{Z}$) stays a prime in the ring of algebraic integers in any quadratic extension of $\mathbb{Q}$, discuss when a rational prime can be written as the sum of two squares, and find the number of solutions to congruence equations of the form $x^n + y^n \equiv 1 \bmod p$ when $n = 2$ or 3.

Contents

1. Introduction

The concept of ordinary integers 0, ± 1, ± 2, ± 3, ..., is a familiar one. Observe that each ordinary integer r is a root to the polynomial $x - r$, which is monic with

Date: August 8, 2012.

ordinary integer coefficients. It will then be natural for us to extend the concept of ordinary integers and define algebraic integers as complex numbers which are roots to some monic polynomial with ordinary integer coefficients. Thus, algebraic integers include more than just ordinary integers; for example, $i = \sqrt{-1}$ is an algebraic integer because it is a root to the polynomial $x^2 + 1$.

Now, consider the set $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$. It is easy to check that all the elements of the set are algebraic integers, for any $a + bi \in \mathbb{Z}[i]$ is a root to the polynomial $x^2 - 2a + (a^2 + b^2)$, and that the set $\mathbb{Z}[i]$ forms a ring under ordinary addition and multiplication of complex numbers. We call $\mathbb{Z}[i]$ the ring of Gaussian integers.

We observe that an ordinary prime number $p \in \mathbb{Z}$ has the property that if p divides ab for a, $b \in \mathbb{Z}$, then p divides a or p divides b (Here, p divides $x \in \mathbb{Z}$ means $x = qp$ for some $q \in \mathbb{Z}$). Of course, we can extend both the concepts of divisibility and of prime elements to $\mathbb{Z}[i]$, by defining an element $p \in \mathbb{Z}[i]$ to be prime when p satisfies the property that if p divides ab for a, $b \in \mathbb{Z}[i]$, then p divides a or p divides b (Here, p divides $x \in \mathbb{Z}[i]$ means $x = qp$ for some $q \in \mathbb{Z}[i]$). We will then discover that 2 is no longer a prime in $\mathbb{Z}[i]$, for 2 divides the product of $1 + i$ and $1 - i$ but divides neither of them individually in $\mathbb{Z}[i]$. On the other hand, 3 is a prime in both $\mathbb{Z}$ and $\mathbb{Z}[i]$. This observation leads to an interesting question: When does a prime number in $\mathbb{Z}$ stay a prime in $\mathbb{Z}[i]$? More generally, when does a prime number in $\mathbb{Z}$ stay a prime in the ring of algebraic integers in any quadratic extension of $\mathbb{Q}$? To avoid confusion, we shall speak of primes in $\mathbb{Z}$ as rational primes.

Another interesting (and classical) question in number theory is under what conditions a rational prime can be written as the sum of squares of two integers in $\mathbb{Z}$. If we define the norm of a Gaussian integer $a + bi \in \mathbb{Z}[i]$ by $N(a + bi) = a^2 + b^2$, the question above is equivalent to under what conditions a rational prime is the norm of some Gaussian integer. It turns out that a rational prime p is the sum of squares of two integers in $\mathbb{Z}$ if and only if $p = 2$ or $p \equiv 1 \bmod 4$, as we shall see.

Of course, besides the ring of Gaussian integers $\mathbb{Z}[i]$, there are other rings of algebraic integers. Let $\omega = \frac{-1+\sqrt{-3}}{2}$ throughout this paper. The ring $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ will be of particular interest to us, as the law of cubic reciprocity will be stated in terms of cubic characters of primary elements in $\mathbb{Z}[\omega]$. To prove the law of cubic reciprocity, we shall develop the concepts of Gauss and Jacobi sums, which will also be used to prove the law of quadratic reciprocity and to count the number of solutions to congruence equations of the form $x^n + y^n \equiv 1 \bmod p$ when $n = 2$ or 3.

2. Finite Fields and Multiplicative Characters

2.1. **Finite Fields.** We shall begin by investigating some of the properties of finite fields. In particular, we shall prove that the number of elements in a finite field is some positive integral power of a rational prime, and that the multiplicative group of a finite field is cyclic.

Theorem 2.1. *The number of elements in a finite field is some positive integral power of a rational prime.*

Proof. Let F be a finite field. Define the map $\varphi : \mathbb{Z} \to F$ by $\varphi(k) = k1_F$ where 1_F denotes the multiplicative identity of F. Then φ is a ring homomorphism. The image of φ, $\varphi(\mathbb{Z})$ is a (finite) subring of the finite field F; in particular it

must be an integral domain. Since we have $\varphi(\mathbb{Z}) \cong \mathbb{Z}/ker\varphi$, $\mathbb{Z}/ker\varphi$ is an integral domain, so $ker\varphi$ is a prime ideal in $\mathbb{Z}$. Thus, we have $ker\varphi = p\mathbb{Z}$, and consequently $\varphi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ for some rational prime p. Note that we have $\varphi(\mathbb{Z}) = \{k1_F : k \in \mathbb{Z}\}$, so we have proved that the integer multiples of the (multiplicative) identity of a finite field F forms a subfield of F isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some rational prime p.

We shall identify $\mathbb{Z}/p\mathbb{Z}$ with the image of φ, $\varphi(\mathbb{Z})$, in F and think of F as a finite dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$. Let n be the dimension and $\{x_1, ..., x_n\}$ be a basis of F over $\mathbb{Z}/p\mathbb{Z}$. Then every element $x \in F$ can be written uniquely in the form $a_1x_1 + ... + a_nx_n$ with $a_i \in \mathbb{Z}/p\mathbb{Z}$. It then follows that F has p^n elements. □

Let 0 and 1 denote the additive and multiplicative identities (respectively) of a finite field F, and let p be the least positive integer such that $p1 = 0$. The first part of the proof of Theorem 2.1 tells us that p must be a prime number. It is called the characteristic of F. For all $x \in F$, we have $px = p(1x) = (p1)x = 0x = 0$. This observation leads to the following proposition.

Proposition 2.2. *If F has characteristic p, then $(a + b)^{p^d} = a^{p^d} + b^{p^d}$ for all a, $b \in F$ and all positive integers d.*

Proof. For $d = 1$, we have

$$(a + b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k}b^k + b^p = a^p + b^p$$

because p divides $\binom{p}{k}$ for $1 \leq k \leq p - 1$.

Now suppose that $(a + b)^{p^d} = a^{p^d} + b^{p^d}$ is true for some $d \geq 1$. It then follows $(a + b)^{p^{d+1}} = ((a + b)^{p^d})^p = (a^{p^d} + b^{p^d})^p = (a^{p^d})^p + (b^{p^d})^p = a^{p^{d+1}} + b^{p^{d+1}}$. The induction is complete. □

Let F be a finite field with q elements. The multiplicative group $F^\times$ of F is $F - \{0\}$, and has $q - 1$ elements. Thus every element $x \in F^\times$ satisfies $x^{q-1} = 1$, and every element $x \in F$ satisfies $x^q = x$. To show that $F^\times$ is cyclic, we will prove a stronger result that every finite subgroup of the multiplicative group of a field is cyclic (Our main reference is [3]). We need the following lemmas before we proceed.

Lemma 2.3. *Let G be a group and let g, $h \in G$ be commuting elements of finite orders m, n respectively with $(m, n) = 1$. Then we have $|gh| = mn$.*

Proof. We have $(gh)^{mn} = (g^m)^n(h^n)^m = 1$, where 1 denotes the identity of G, so $l = |gh|$ divides mn. Then we have $g^l = h^{-l} \in \langle g\rangle \cap \langle h\rangle = \{1\}$, so m and n both divide l. It then follows, from $(m, n) = 1$, that mn divides $l = |gh|$. Thus, we have $|gh| = mn$. □

Lemma 2.4. *Let G be a finite abelian group, and let $m = max\{|g| : g \in G\}$. Then $|g|$ divides m for every $g \in G$.*

Proof. Let $h \in G$ have order m, and let g be any element of G. Let $m = \prod_{i=1}^n {p_i}^{r_i}$ be the prime factorization of m in $\mathbb{Z}$. If there exists a rational prime p which divides $|g|$ but not m, then G contains an element x of order p. Since we have $(p, m) = 1$, by Lemma 2.3, we have $|xh| = pm > m$, which contradicts the maximality of m. Thus, every rational prime divisor of $|g|$ must be a divisor of m. Suppose now that there exists i with ${p_i}^r$ dividing $|g|$ and $r > r_i$. Then G contains an element of order ${p_i}^r$ and an element of order $m/{p_i}^{r_i}$. Since we have $({p_i}^r, m/{p_i}^{r_i}) = 1$, by

Lemma 2.3, G contains an element of order $mp_i^{r-r_i} > m$, which again contradicts the maximality of m. Thus, every rational prime power divisor of $|g|$ divides m, so $|g|$ divides m. □

We are now ready to prove that every finite subgroup of the multiplicative group of a field is cyclic, and consequently the multiplicative group of a finite field is cyclic.

Theorem 2.5. *Every finite subgroup of the multiplicative group of a field is cyclic.*

Proof. Let G be a finite subgroup of the multiplicative group of a field F. Then G is a finite abelian group. Let $m = max\{|g| : g \in G\}$. By Lemma 2.4, we have $g^m = 1$ for every $g \in G$. Thus, every element of G is a root to the polynomial $x^m - 1$, which has at most m roots in F, so we have $|G| \leq m$. On the other hand, by Lagrange's Theorem, m divides $|G|$, so we have $m \leq |G|$. It follows $|G| = m$. Since G contains an element of order $|G|$, G must be cyclic. □

Corollary 2.6. *The multiplicative group of a finite field is cyclic.*

Let F be a finite field. The fact that $F^\times$ is cyclic allows us to give a criterion for deciding when $x^n = a$ ($a \in F^\times$) has solutions in $F^\times$, as we shall see.

Lemma 2.7. *Let a, $m \in \mathbb{Z}$ and $d = (a, m)$. For $b \in \mathbb{Z}$, the congruence $ax \equiv b$ mod m has solutions if and only if d divides b. If d divides b, then there are exactly d solutions which are not equivalent mod m.*

Proof. If x_0 is a solution, then we have $ax_0 - b = my_0$ for some integer y_0, which gives $ax_0 - my_0 = b$. Since d divides both a and m, it follows that d divides $ax_0 - my_0 = b$.

Conversely, suppose that d divides b. Since we have $d = (a, m)$, there exist integers x_0' and y_0' such that $ax_0' - my_0' = d$. Let $c = b/d$. Then we have $a(x_0'c) - m(y_0'c) = dc = b$. Let $x_0 = x_0'c$ and we clearly have $ax_0 \equiv b \bmod m$.

Suppose that d divides b. To show that $ax \equiv b \bmod m$ has exactly d solutions, suppose that x_0 and x_1 are solutions, i.e. they satisfy $ax_0 \equiv b \bmod m$ and $ax_1 \equiv b \bmod m$, which imply $a(x_1 - x_0) \equiv 0 \bmod m$. Thus, m divides $a(x_1 - x_0)$, and consequently $\frac{m}{d}$ divides $\frac{a}{d}(x_1 - x_0)$. Note that $\frac{a}{d}$ and $\frac{m}{d}$ are relatively prime. It then follows that $\frac{m}{d}$ divides $x_1 - x_0$, so we have $x_1 = x_0 + k\frac{m}{d}$ for some integer k. On the other hand, any integer of the form $x_0 + k\frac{m}{d}$ is a solution, since we have $a(x_0 + k\frac{m}{d}) = ax_0 + mk\frac{a}{d} \equiv b \bmod m$. Also, the solutions x_0, $x_0 + \frac{m}{d}$, ..., $x_0 + (d-1)\frac{m}{d}$ are not equivalent, for if we have $x_0 + r\frac{m}{d} \equiv x_0 + s\frac{m}{d} \bmod m$ for some nonnegative integers r, s with $r \neq s$ and r, $s \leq d - 1$, then m would divide $|r - s|\frac{m}{d}$, and we would have $\frac{|r-s|}{d} \in \mathbb{Z}$, which is impossible. Now let $x_1 = x_0 + k\frac{m}{d}$ be another solution. Then there are integers q and r such that $k = qd + r$ and $0 \leq r \leq d - 1$. Thus, we have $x_1 = x_0 + r\frac{m}{d} + qm \equiv x_0 + r\frac{m}{d} \bmod m$. We have shown that x_0, $x_0 + \frac{m}{d}$, ..., $x_0 + (d-1)\frac{m}{d}$ are all the solutions, so there are exactly d solutions which are not equivalent mod m. □

Proposition 2.8. *Let F be a finite field with q elements, and let $a \in F^\times$. Then $x^n = a$ has solutions if and only if $a^{(q-1)/d} = 1$, where $d = (n, q - 1)$. If there are solutions, then there are exactly d solutions.*

Proof. We have shown that $F^\times$ is cyclic. Let g be a generator of $F^\times$ and set $a = g^b$ and $x = g^y$. Then $x^n = a$ is equivalent to the congruence $ny \equiv b \bmod q - 1$. The result follows by applying Lemma 2.7. □

To conclude our discussion on finite fields, we shall prove the following proposition, using the fact that the multiplicative group of a finite field is cyclic.

Proposition 2.9. *For all integers k and rational primes p, we have $1^k + 2^k + ... + (p-1)^k \equiv 0$ mod p if $p-1$ does not divide k, and -1 mod p if $p-1$ divides k.*

Proof. Let g be a generator of $F_p^\times$, so g has order $p-1$. By identifying 1, 2, ..., $p-1$ as elements of $(\mathbb{Z}/p\mathbb{Z})^\times \cong F_p^\times$ and letting $i = g^{r_i}$ for all integers i with $1 \leq i \leq p-1$, we have

$$1^k + 2^k + ... + (p-1)^k = (g^{r_1})^k + (g^{r_2})^k + ... + (g^{r_{p-1}})^k = \sum_{i=1}^{p-1} (g^k)^{r_i} = \sum_{j=0}^{p-2} (g^k)^j.$$

Note that we also have

$$(g^k - 1)\sum_{j=0}^{p-2} (g^k)^j = \sum_{j=0}^{p-2} g^{k(j+1)} - g^{kj} = g^{k(p-1)} - g^0 = 1 - 1 = 0$$

in F_p. Suppose that $p-1$ does not divide k in $\mathbb{Z}$. Then we have $g^k \neq 1$ in F_p, so we must have $\sum_{j=0}^{p-2} (g^k)^j = 0$ in F_p, which is equivalent to $1^k + 2^k + ... + (p-1)^k \equiv 0$ mod p. If $p-1$ divides k in $\mathbb{Z}$, then we have $1^k + 2^k + ... + (p-1)^k = 1 + 1 + ... + 1 = p - 1 = -1$ in F_p, which is equivalent to $1^k + 2^k + ... + (p-1)^k \equiv -1$ mod p. □

2.2. **Multiplicative Characters.** We shall now introduce multiplicative characters which will later be used to define Gauss and Jacobi sums.

Definition 2.10. Let F_p denote a finite field with p elements, where p is a rational prime. A multiplicative character χ on F_p is a group homomorphism from $F_p^\times$ to $\mathbb{C}^\times$, i.e. it satisfies $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in F_p^\times$.

An example of a multiplicative character is the trivial multiplicative character ϵ defined by $\epsilon(a) = 1$ for all $a \in F_p^\times$.

It is often useful to extend the domain of a multiplicative character to all of F_p. If $\chi \neq \epsilon$, we do this by defining $\chi(0) = 0$. For the trivial character ϵ, we define $\epsilon(0) = 1$.

The following proposition summarizes some basic properties of multiplicative characters.

Proposition 2.11. *Let χ be a multiplicative character on F_p, ϵ be the trivial character, and $a \in F_p^\times$. Then*
(a) $\chi(1) = 1$.
(b) $\chi(a)$ is a $(p-1)$st root of unity.
(c) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.
(d) $\sum_{t \in F_p} \chi(t) = 0$ for $\chi \neq \epsilon$, and $\sum_{t \in F_p} \epsilon(t) = p$.

Proof. (a) Since we have $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$ and $\chi(1) \neq 0$, we must have $\chi(1) = 1$.

(b) For all $a \in F_p^\times$, we have $a^{p-1} = 1$, which implies that $1 = \chi(1) = \chi(a^{p-1}) = \chi(a)^{p-1}$.

(c) For all $a \in F_p^\times$, we have $1 = \chi(1) = \chi(aa^{-1}) = \chi(a)\chi(a^{-1})$, which implies $\chi(a^{-1}) = \chi(a)^{-1}$. Since we have $|\chi(a)| = 1$ by part (b), we have $\chi(a)\overline{\chi(a)} = |\chi(a)|^2 = 1$, which implies $\overline{\chi(a)} = \chi(a)^{-1}$.

(d) Suppose $\chi \neq \epsilon$. In this case there is an $a \in F_p^\times$ such that $\chi(a) \neq 1$. Let $T = \sum_{t \in F_p} \chi(t)$. Then we have $\chi(a)T = \sum_{t \in F_p} \chi(a)\chi(t) = \sum_{t \in F_p} \chi(at) = T$, which gives $(\chi(a) - 1)T = 0$, but $\chi(a) - 1 \neq 0$, so we must have $T = 0$. It is clear that $\sum_{t \in F_p} \epsilon(t) = \sum_{t \in F_p} 1 = p$. □

The multiplicative characters on F_p form a group by means of the following definitions: (1) If χ and λ are multiplicative characters on F_p, then $\chi\lambda$ is the map given by $\chi\lambda(a) = \chi(a)\lambda(a)$ for all $a \in F_p^\times$. (2) If χ is a multiplicative character on F_p, χ^{-1} is the map given by $\chi^{-1}(a) = \chi(a)^{-1}$. It is not difficult to verify that $\chi\lambda$ and χ^{-1} defined above are multiplicative characters on F_p and that these definitions make the set of multiplicative characters on F_p into a group. The identity of this group is the trivial character ϵ.

Theorem 2.12. *The group of multiplicative characters on F_p is a cyclic group of order $p-1$. For any $a \in F_p^\times$ with $a \neq 1$, there is a character χ on F_p with $\chi(a) \neq 1$.*

Proof. We have shown that $F_p^\times$ is a cyclic group of order $p-1$. Let g be a generator of $F_p^\times$. If a is any element of $F_p^\times$ and χ is a multiplicative character on F_p, then we have $a = g^l$ for some $l \in \mathbb{Z}$ and $\chi(a) = \chi(g)^l$. This shows that χ is completely determined by the value of $\chi(g)$. Since $\chi(g)$ is a $(p-1)$st root of unity, and since there are exactly $p-1$ of these, it follows that the group of multiplicative characters on F_p has order at most $p-1$.

Now define a function $\lambda : F_p^\times \to \mathbb{C} - \{0\}$ by $\lambda(g^k) = e^{2\pi i(k/(p-1))}$. It is not difficult to check that λ is well defined and is a multiplicative character. Suppose $\lambda^n = \epsilon$. Then we have $\lambda^n(g) = \epsilon(g) = 1$. However, we also have $\lambda^n(g) = \lambda(g^n) = e^{2\pi i(n/(p-1))}$. It follows that $p-1$ divides n. Since we have $\lambda^{p-1}(a) = \lambda(a^{p-1}) = \lambda(1) = 1$, we have $\lambda^{p-1} = \epsilon$. It then follows that λ is a character of order $p-1$, and that ϵ, λ, λ^2, ..., λ^{p-2} are all distinct. Since there are at most $p-1$ characters on F_p, ϵ, λ, λ^2, ..., λ^{p-2} must be all the characters on F_p. Thus, the group of multiplicative characters is a cyclic group of order $p-1$, with λ as a generator.

For any $a \in F_p^\times$ with $a \neq 1$, we have $a = g^l$ and $p-1$ does not divide l. Consequently, we have $\lambda(a) = \lambda(g^l) = e^{2\pi i(l/(p-1))} \neq 1$. □

Corollary 2.13. *Let $a \in F_p^\times$ with $a \neq 1$, and G be the group of multiplicative characters on F_p. Then we have $\sum_{\chi \in G} \chi(a) = 0$.*

Proof. Let $S = \sum_{\chi \in G} \chi(a)$. Since we have $a \neq 1$, there is a character λ on F_p with $\lambda(a) \neq 1$. Then we have $\lambda(a)S = \sum_{\chi \in G} \lambda(a)\chi(a) = \sum_{\chi \in G} \lambda\chi(a) = S$. Thus, we have $(\lambda(a) - 1)S = 0$ and consequently $S = 0$. □

Multiplicative characters are useful in the study of power congruences. To illustrate this, consider the equation $x^n = a$ for $a \in F_p^\times$. By Proposition 2.8, we know that it has solutions if and only if $a^{(p-1)/d} = 1$, where $d = (n, p-1)$, and that if there are solutions, then there are exactly d solutions. We shall now derive a formula for the number of solutions in F_p of the equation $x^n = a$ where $a \in F_p$ using characters. For simplicity, we shall assume that n divides $p-1$, and in this case we have $d = (n, p-1) = n$.

Proposition 2.14. *Let $a \in F_p^\times$ and suppose that n divides $p-1$. If $x^n = a$ has no solutions in F_p, then there is a character χ such that $\chi^n = \epsilon$ and $\chi(a) \neq 1$.*

Proof. Let g and λ be the same as in Theorem 2.12. Set $\chi = \lambda^{(p-1)/n}$. Then we have $\chi^n = \lambda^{p-1} = \epsilon$. Now, we have $\chi(g) = \lambda^{(p-1)/n}(g) = \lambda(g^{(p-1)/n}) = e^{2\pi i/n}$, and $a = g^l$ for some $l \in \mathbb{Z}$. Since $x^n = a$ has no solutions in F_p, n does not divide l and consequently $\chi(a) = \chi(g)^l = e^{2\pi i(l/n)} \neq 1$. □

For $a \in F_p$, let $N(x^n = a)$ denote the number of solutions in F_p of the equation $x^n = a$.

Proposition 2.15. *If n divides $p-1$, then we have $N(x^n = a) = \sum_{\chi^n=\epsilon} \chi(a)$.*

Proof. We shall first show that there are exactly n characters of order dividing n. Let χ be a character of order dividing n, and g be a generator of $F_p^\times$. Since the value of $\chi(g)$ must be an nth root of unity, there are at most n characters of order dividing n. Now the character χ given by $\chi(g) = e^{2\pi i/n}$ is a character of order n, and it follows that ϵ, χ, χ^2, ..., χ^{n-1} are n distinct characters of order dividing n.

To prove the formula, note that $x^n = 0$ has one solution in F_p, namely, $x = 0$. Now, it is not difficult to see that $\sum_{\chi^n=\epsilon} \chi(0) = 1$ since we have $\epsilon(0) = 1$ and $\chi(0) = 0$ for $\chi \neq \epsilon$.

Now suppose $a \neq 0$. Suppose, furthermore, that $x^n = a$ has solutions in F_p. Then Proposition 2.8 tells us that there are exactly $d = (n, p-1) = n$ solutions. Let b be an element of F_p with $b^n = a$. For all characters χ on F_p with $\chi^n = \epsilon$, we have $\chi(a) = \chi(b^n) = \chi^n(b) = \epsilon(b) = 1$. Thus, we have $\sum_{\chi^n=\epsilon} \chi(a) = n$, which is equal to $N(x^n = a)$ in this case.

Finally, suppose that $x^n = a$ has no solution in F_p ($a \neq 0$). We must show $\sum_{\chi^n=\epsilon} \chi(a) = 0$. Let $R = \sum_{\chi^n=\epsilon} \chi(a)$. By the proposition above, there is a character ρ with $\rho^n = \epsilon$ and $\rho(a) \neq 1$. Then we have $\rho(a)R = \sum_{\chi^n=\epsilon} \rho(a)\chi(a) = \sum_{\chi^n=\epsilon} \rho\chi(a) = R$, which gives $(\rho(a) - 1)R = 0$ and consequently $R = 0$. □

2.3. **An Example of Multiplicative Characters: The Legendre Symbol.** We shall now introduce the Legendre symbol, which is a multiplicative character of order 2 on F_p.

Definition 2.16. Let a and m be two integers with $(a, m) = 1$. Then a is a quadratic residue mod m if the congruence $x^2 \equiv a \bmod m$ has a solution. Otherwise a is a quadratic nonresidue mod m.

Definition 2.17. Let p be an odd rational prime. The Legendre symbol, denoted by $\left(\frac{a}{p}\right)$, equals 1 if a is a quadratic residue mod p, -1 if a is a quadratic nonresidue mod p, and 0 if p divides a.

The following proposition summarizes some properties of the Legendre symbol.

Proposition 2.18. *Let a, $b \in \mathbb{Z}$, and p be an odd rational prime. Then*
(a) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$; in particular, we have $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.
(b) $a \equiv b \bmod p$ implies $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
(c) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Proof. (a) If p divides a, then we have $a^{(p-1)/2} \equiv 0 = \left(\frac{a}{p}\right) \bmod p$. Suppose that p does not divide a. Then we have $a^{p-1} \equiv 1 \bmod p$, which gives $(a^{(p-1)/2} + 1)(a^{(p-1)/2} - 1) = a^{p-1} - 1 \equiv 0 \bmod p$. Thus, we have $a^{(p-1)/2} \equiv \pm 1 \bmod p$. By

Proposition 2.8, $a^{(p-1)/2} \equiv 1 \bmod p$ if and only if the congruence $x^2 \equiv a \bmod p$ has a solution, i.e. if and only if a is a quadratic residue mod p. This establishes $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$. Letting $a = -1$, we have $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

(b) Part (b) is obvious from the definition.

(c) By part (a), we have $\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p$. Thus, we have $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p$, which implies $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. □

Corollary 2.19. *Let p be an odd rational prime. Then -1 is a quadratic residue mod p if and only if $p \equiv 1$ mod 4.*

Proof. -1 is a quadratic residue mod p if and only if $(-1)^{(p-1)/2} = \left(\frac{-1}{p}\right) = 1$ if and only if $(p-1)/2$ is even if and only if $p \equiv 1 \bmod 4$. □

Corollary 2.20. *Let p be an odd rational prime. Then there are $(p-1)/2$ quadratic residues mod p and as many quadratic nonresidues mod p.*

Proof. Proposition 2.8 implies that $a^{(p-1)/2} \equiv 1 \bmod p$ has $(p-1)/2$ solutions. Thus, there are $(p-1)/2$ quadratic residues mod p and $(p-1)-((p-1)/2) = (p-1)/2$ quadratic nonresidues mod p. □

Proposition 2.18(b) allows us to regard the Legendre symbol $\left(\frac{a}{p}\right)$ as a function of the coset of a mod p, and consequently as a function on F_p. Proposition 2.18(c) then allows us to regard the Legendre symbol as a multiplicative character on F_p. Note that for all $a \not\equiv 0 \bmod p$, we have $\left(\frac{a}{p}\right)^2 = 1$. This, together with Corollary 2.20, implies that the Legendre symbol is a character of order 2.

Proposition 2.21. *Let p be an odd rational prime. Then we have $\sum_{t=0}^{p-1}\left(\frac{t}{p}\right) = 0$.*

Proof. This is a special case of Proposition 2.11(d). □

The law of quadratic reciprocity is stated in terms of the Legendre symbol: Let p and q be odd rational primes. Then we have $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{((p-1)/2)((q-1)/2)}$.

Two proofs will be given in Section 5.

3. Field Extensions and Rings of Integers

In this section, we shall solve two of the questions we have posed in the Introduction: (1) When does a prime number in $\mathbb{Z}$ stay a prime in the ring of algebraic integers in any quadratic extension of $\mathbb{Q}$? (2) Under what conditions can a rational prime be written as the sum of squares of two integers in $\mathbb{Z}$?

3.1. Field Extensions.

Definition 3.1. (1) K is an extension field of F, denoted by K/F, if K is a field containing the subfield F. (2) The degree of a field extension K/F is the dimension of K as a vector space over F. (3) K is a quadratic extension of F if the degree of the field extension K/F is 2.

We shall now give a characterization of quadratic extensions of $\mathbb{Q}$, as follows:

Proposition 3.2. *If K is a quadratic extension of $\mathbb{Q}$, then we have $K = \mathbb{Q}(\sqrt{d})$ for some square-free ordinary integer d.*

Proof. Let β be any element of K not contained in $\mathbb{Q}$. Then β is a root to a polynomial $f(x)$ of degree at most 2 in $\mathbb{Q}[x]$. Now, $f(x)$ cannot be of degree 1, since β is not an element of $\mathbb{Q}$ by assumption. It follows that $f(x)$ must be of degree 2, and that $\mathbb{Q}(\beta)$ is a quadratic extension of $\mathbb{Q}$; since we have $\mathbb{Q} \subset \mathbb{Q}(\beta) \subseteq K$, we must have $K = \mathbb{Q}(\beta)$.

Suppose $f(x) = ax^2 + bx + c$ ($a \neq 0$). Then the quadratic formula tells us $\beta = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$. (Here b^2-4ac is not a square in $\mathbb{Q}$ and $\sqrt{b^2-4ac}$ denotes a root to the polynomial $x^2-(b^2-4ac)$ in K.) Consequently, we have $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\sqrt{b^2-4ac})$. Conversely, we have $\sqrt{b^2-4ac} = \pm(b+2a\beta)$, which gives $\mathbb{Q}(\sqrt{b^2-4ac}) \subseteq \mathbb{Q}(\beta)$. Thus, we have $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{b^2-4ac})$; since $\sqrt{b^2-4ac} = y\sqrt{d}$ for some nonzero $y \in \mathbb{Q}$ and some square-free ordinary integer d, we have $\mathbb{Q}(\sqrt{b^2-4ac}) = \mathbb{Q}(\sqrt{d})$. The proof is now complete. □

For the rest of the paper, we shall define the norm $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ (where d is a square-free ordinary integer) by $N(\gamma) = \gamma\gamma'$ where $\gamma' = a - b\sqrt{d}$ for all $\gamma = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ (Note that $\gamma' = \overline{\gamma}$ is the complex conjugate of γ when d is a negative integer in $\mathbb{Z}$). It is easy to check that N is multiplicative, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$.

3.2. **Rings of Algebraic Integers in Extension Fields of $\mathbb{Q}$.** We shall now extend the concept of ordinary integers and define algebraic integers in an extension field of $\mathbb{Q}$. Let K be an extension field of $\mathbb{Q}$.

Definition 3.3. An element $\alpha \in K$ is an algebraic integer if α is a root to some monic polynomial with coefficients in $\mathbb{Z}$.

The set of all algebraic integers in an extension field of $\mathbb{Q}$ forms a ring. To prove this, we need a lemma.

Lemma 3.4. *Suppose that α belongs to a ring R in K that is a finitely generated $\mathbb{Z}$ module. Then α is an algebraic integer.*

Proof. Let R be a ring which is also the $\mathbb{Z}$ module generated by g_1, ..., g_n. Then for each $i \in \mathbb{Z}$ with $1 \leq i \leq n$, we have $\alpha g_i = \sum_{j=1}^{n} c_{ij} g_j$ for some $c_{ij} \in \mathbb{Z}$. Let g denote the column vector with entries g_i. Then we have $\alpha g = Mg$ where M is the $n \times n$ matrix with entries c_{ij}. Thus, α is an eigenvalue of M in K, and satisfies the characteristic polynomial of M, which is a monic polynomial with coefficients in $\mathbb{Z}$. □

Theorem 3.5. *The set of all algebraic integers in K, denoted by $\mathcal{O}_K$, forms a ring (an integral domain, in fact).*

Proof. Let α and β be algebraic integers in K. Suppose $\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0 = 0$ and $\beta^m + b_{m-1}\beta^{m-1} + ... + b_1\beta + b_0 = 0$ with a_i, $b_j \in \mathbb{Z}$. Let R be the set of all $\mathbb{Z}$ linear combinations of $\alpha^i\beta^j$ with i, $j \in \mathbb{Z}$, $0 \leq i < n$ and $0 \leq j < m$. Then R is a ring in K that is a finitely generated $\mathbb{Z}$ module. Since $\alpha + \beta$ and $\alpha\beta$ belong to R, by the lemma above, we conclude that $\alpha + \beta$ and $\alpha\beta$ are algebraic integers in K. □

We can extend the concept of congruence from $\mathbb{Z}$ to $\mathcal{O}_K$, as follows: If γ_1, γ_2 and λ are elements of $\mathcal{O}_K$ with $\lambda \neq 0$, we say that γ_1 is congruent to γ_2 mod λ ($\gamma_1 \equiv \gamma_2$ mod λ) if we have $\gamma_1 - \gamma_2 = \delta\lambda$ for some $\delta \in \mathcal{O}_K$. The following proposition gives a useful property of congruences in $\mathcal{O}_K$.

Proposition 3.6. *Let ω_1, ω_2 be any elements of $\mathcal{O}_K$ and p be a rational prime. Then we have $(\omega_1+\omega_2)^p \equiv \omega_1^p + \omega_2^p \mod p$.*

Proof. We have

$$(\omega_1+\omega_2)^p = \omega_1^p + \sum_{k=1}^{p-1} \binom{p}{k} \omega_1^{p-k}\omega_2^k + \omega_2^p.$$

Since p divides $\binom{p}{k}$ for $1 \leq k \leq p-1$ and $\mathcal{O}_K$ is a ring, we have the desired result. □

To illustrate the usefulness of the notion of congruence in a ring of algebraic integers, we shall compute $\left(\frac{2}{p}\right)$ where p is an odd rational prime.

Proposition 3.7. *Let p be an odd rational prime. Then we have $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.*

Proof. Let $\zeta = e^{2\pi i/8}$. Then we have $(\zeta^4+1)(\zeta^4-1) = \zeta^8 - 1 = 0$, which implies $\zeta^4 = -1$. Consequently, we have $\zeta^2 + \zeta^{-2} = \zeta^4\zeta^{-2} + \zeta^{-2} = -\zeta^{-2} + \zeta^{-2} = 0$, and $(\zeta+\zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = 2$.

Let $\tau = \zeta + \zeta^{-1}$. Note that both ζ and τ are algebraic integers in $\mathbb{C}$. We may thus work with congruences in the ring of algebraic integers in $\mathbb{C}$.

Now, since $\tau^{p-1} = (\tau^2)^{(p-1)/2} = 2^{(p-1)/2} \equiv \left(\frac{2}{p}\right) \mod p$, we have $\tau^p \equiv \left(\frac{2}{p}\right)\tau \mod p$. By Proposition 3.6, we also have $\tau^p = (\zeta+\zeta^{-1})^p \equiv \zeta^p + \zeta^{-p} \mod p$. Since $\zeta^8 = 1$, we have $\zeta^p + \zeta^{-p} = \zeta + \zeta^{-1} = \tau$ for $p \equiv \pm 1 \mod 8$ and $\zeta^p + \zeta^{-p} = \zeta^3 + \zeta^{-3}$ for $p \equiv \pm 3 \mod 8$. Note that we have $\zeta^3 = \zeta^4\zeta^{-1} = -\zeta^{-1}$ and $\zeta^{-3} = -\zeta$, so we have $\zeta^p + \zeta^{-p} = -(\zeta+\zeta^{-1}) = -\tau$ for $p \equiv \pm 3 \mod 8$. Thus, we have $\zeta^p + \zeta^{-p} = (-1)^{(p^2-1)/8}\tau$, and consequently $\left(\frac{2}{p}\right)\tau \equiv (-1)^{(p^2-1)/8}\tau \mod p$; multiplying both sides of the congruence relation by τ, we obtain $\left(\frac{2}{p}\right)2 \equiv (-1)^{(p^2-1)/8}2 \mod p$, which implies $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$. □

We shall now present two important properties of algebraic integers. The first proposition establishes the existence of a minimal polynomial for each algebraic integer (in fact, for each algebraic number, which is a root to some polynomial in $\mathbb{Q}[x]$), and the second gives a simple criterion for α to be an algebraic integer in terms of the minimal polynomial for α.

Proposition 3.8. *If α is an algebraic number then α is a root to a unique monic irreducible polynomial $f(x) \in \mathbb{Q}[x]$. Furthermore, if we have $g(x) \in \mathbb{Q}[x]$, $g(\alpha) = 0$, then $f(x)$ divides $g(x)$.*

Proof. Let $f(x)$ be a monic polynomial in $\mathbb{Q}[x]$ of the smallest degree for which α is a root. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$. For any $g(x) \in \mathbb{Q}[x]$ with $g(\alpha) = 0$, if $f(x)$ does not divide $g(x)$, then we have $(f(x), g(x)) = 1$ and consequently $f(x)s(x) + g(x)t(x) = 1$ for some polynomials $s(x)$, $t(x) \in \mathbb{Q}[x]$. However, we also have $f(\alpha)s(\alpha) + g(\alpha)t(\alpha) = 0 \neq 1$. Thus, we must have $f(x) \mid g(x)$. Uniqueness of $f(x)$ now follows immediately. □

The polynomial $f(x)$ defined in the above proposition is called the minimal polynomial of α. Thus, a minimal polynomial for an algebraic number α is a monic polynomial in $\mathbb{Q}[x]$ of the smallest degree for which α is a root; it is irreducible in $\mathbb{Q}[x]$, is unique and has the property that if $g(x)$ is a polynomial in $\mathbb{Q}[x]$ with $g(\alpha) = 0$, then $f(x)$ divides $g(x)$.

Proposition 3.9. *An element α in some field extension K of $\mathbb{Q}$ is an algebraic integer if and only if α is a root of some nonzero polynomial in $\mathbb{Q}[x]$ and its minimal polynomial has coefficients in $\mathbb{Z}$. In particular, the algebraic integers in $\mathbb{Q}$ are the ordinary integers $\mathbb{Z}$.*

Proof. If α is a root of some nonzero polynomial in $\mathbb{Q}[x]$ and its minimal polynomial has coefficients in $\mathbb{Z}$, then α is an algebraic integer by definition. Conversely, suppose that α is an algebraic integer. Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ of the smallest degree having α as a root. If $f(x)$ were reducible in $\mathbb{Q}[x]$, then $f(x)$ would be reducible in $\mathbb{Z}[x]$ and we would have $f(x) = g(x)h(x)$ for some monic polynomials $g(x)$, $h(x) \in \mathbb{Z}[x]$ of degree at least one but smaller than the degree of $f(x)$ (This is a special case of a result known as Gauss' Lemma, which states that if R is a unique factorization domain with field of fractions F and $f(x) \in R[x]$ is reducible in $F[x]$, then $f(x)$ is reducible in $R[x]$; for a proof of Gauss' Lemma, see [2] pp. 303-304). Consequently, α would be a root of either $g(x)$ or $h(x)$, contradicting the minimality of the degree of $f(x)$. Hence, $f(x)$ is irreducible in $\mathbb{Q}[x]$, and it is the minimal polynomial of α. It then follows that the minimal polynomial of α has coefficients in $\mathbb{Z}$. Finally, the minimal polynomial of $\alpha = a/b \in \mathbb{Q}$ (a/b reduced to the lowest terms and $b > 0$) is $x - (a/b)$. Hence, α is an algebraic integer if and only if $b = 1$. This shows that the algebraic integers in $\mathbb{Q}$ are the ordinary integers $\mathbb{Z}$. □

We shall now determine the ring of algebraic integers in any quadratic extension $\mathbb{Q}(\sqrt{d})$ (where $d \in \mathbb{Z}$ is square-free) of $\mathbb{Q}$.

Proposition 3.10. *Let $d \in \mathbb{Z}$ be a square-free integer. The ring of algebraic integers in $\mathbb{Q}(\sqrt{d})$ (known as the quadratic integer ring) is $\mathbb{Z}[\alpha]$ where $\alpha = \sqrt{d}$ if $d \equiv 2$ or $3 \bmod 4$, and $\alpha = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \bmod 4$.*

Proof. Since α satisfies $\alpha^2 - d = 0$ for $d \equiv 2$ or $3 \bmod 4$ and $\alpha^2 - \alpha + (1-d)/4 = 0$ for $d \equiv 1 \bmod 4$, it follows that α is an algebraic integer, so $\mathbb{Z}[\alpha]$ is contained in the ring of algebraic integers in $\mathbb{Q}(\sqrt{d})$. To show that $\mathbb{Z}[\alpha]$ is the full ring of algebraic integers in $\mathbb{Q}(\sqrt{d})$, we let $\gamma = a + b\sqrt{d}$ with a, $b \in \mathbb{Q}$, and suppose that γ is an algebraic integer. If $b = 0$, then we have $\gamma = a \in \mathbb{Q}$ and consequently $\gamma \in \mathbb{Z} \subseteq \mathbb{Z}[\alpha]$. If $b \neq 0$, the minimal polynomial of γ is $x^2 - 2ax + (a^2 - b^2 d)$. Then the proposition above tells us that $2a$ and $a^2 - b^2 d$ are both elements of $\mathbb{Z}$. Then we have $4(a^2 - b^2 d) = (2a)^2 - (2b)^2 d \in \mathbb{Z}$, which implies $(2b)^2 d \in \mathbb{Z}$. Since $d \in \mathbb{Z}$ is square-free, we must have $2b \in \mathbb{Z}$. Write $a = x/2$ and $b = y/2$ for some x, $y \in \mathbb{Z}$. Since we have $a^2 - b^2 d \in \mathbb{Z}$, we must have $x^2 - y^2 d \equiv 0 \bmod 4$. Since 0 and 1 are the only squares mod 4 and d is not divisible by 4, the only possibilities are the following:

(1) $d \equiv 2$ or $3 \bmod 4$ and x, y are both even, or

(2) $d \equiv 1 \bmod 4$ and x, y are both even or both odd.

In case (1), we have a, $b \in \mathbb{Z}$ and $\gamma \in \mathbb{Z}[\sqrt{d}] = \mathbb{Z}[\alpha]$. In case (2), we have $\gamma = a + b\sqrt{d} = r + s\alpha$ with $r = (x-y)/2 \in \mathbb{Z}$ and $s = y \in \mathbb{Z}$, so again $\gamma \in \mathbb{Z}[\alpha]$. Thus, we conclude that the ring of algebraic integers in $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\alpha]$. □

For the rest of the paper, let $\mathbb{Z}[\alpha]$ denote the quadratic integer ring as in the proposition above. Recall that a prime element p in an integral domain R is one which satisfies the property that if p divides ab for a, $b \in R$, then p divides a or

p divides b. In the language of ideals, p is a prime element of R if it satisfies the property that $ab \in (p)$ implies $a \in (p)$ or $b \in (p)$. We have seen that a rational prime needs not be a prime in $\mathbb{Z}[\alpha]$. To answer the question when a rational prime stays a prime in $\mathbb{Z}[\alpha]$, we shall give a simple criterion in terms of the Legendre symbol.

Proposition 3.11. *Let p be an odd rational prime. For any prime ideal P in $\mathbb{Z}[\alpha]$, define $P' = \{\gamma' : \gamma \in P\}$.*
(a) If $\left(\frac{d}{p}\right) = -1$, then we have $(p) = P$ for some prime ideal P in $\mathbb{Z}[\alpha]$ (In this case, we say that p is inert).
(b) If $\left(\frac{d}{p}\right) = 1$, then we have $(p) = PP'$ and $P \neq P'$ for some prime ideal P in $\mathbb{Z}[\alpha]$ (In this case, we say that p splits).
(c) If $\left(\frac{d}{p}\right) = 0$, then we have $(p) = P^2$ for some prime ideal P in $\mathbb{Z}[\alpha]$ (In this case, we say that p ramifies).

Proof. (a) Suppose $\left(\frac{d}{p}\right) = -1$. Let $f(x)$ be the minimal polynomial of α. Note that we have $f(x) = x^2 - d$ for $d \equiv 2$ or $3 \bmod 4$, and $f(x) = x^2 - x + (1-d)/4$ for $d \equiv 1 \bmod 4$, and $f(x)$ is reducible in $F_p[x]$ if and only if d is a quadratic residue mod p. Thus, $f(x)$ is irreducible in $F_p[x]$, which means that $(f(x))$ is a prime ideal in $F_p[x]$. It then follows that $\mathbb{Z}[\alpha]/(p) \cong F_p[x]/(f(x))$ is an integral domain, and consequently, (p) is a prime ideal in $\mathbb{Z}[\alpha]$.

(b) Suppose $\left(\frac{d}{p}\right) = 1$. Then we have $a^2 \equiv d \bmod p$ for some $a \in \mathbb{Z}$. Note that we have $(p, a+\sqrt{d})(p, a-\sqrt{d}) = (p)(p, a+\sqrt{d}, a-\sqrt{d}, (a^2-d)/p)$. Since $(p, a+\sqrt{d}, a-\sqrt{d}, (a^2-d)/p)$ contains p and $2a$ which are relatively prime in $\mathbb{Z}$, $(p, a+\sqrt{d}, a-\sqrt{d}, (a^2-d)/p)$ contains 1 and is consequently the whole ring $\mathbb{Z}[\alpha]$. Thus, we have $(p, a+\sqrt{d})(p, a-\sqrt{d}) = (p)$. If $(p, a+\sqrt{d}) = (p, a-\sqrt{d})$, then $(p, a+\sqrt{d})$ would contain p and $2a$, and would be the whole ring $\mathbb{Z}[\alpha]$. Consequently, (p) would be the whole ring $\mathbb{Z}[\alpha]$, which is impossible. Setting $P = (p, a+\sqrt{d})$, we have the desired result.

(c) Suppose $\left(\frac{d}{p}\right) = 0$. Note that we have $(p, \sqrt{d})^2 = (p)(p, \sqrt{d}, d/p)$. Since $(p, \sqrt{d}, d/p)$ contains p and d/p which are relatively prime in $\mathbb{Z}$ (because $d \in \mathbb{Z}$ is square-free), $(p, \sqrt{d}, d/p)$ contains 1 and is consequently the whole ring $\mathbb{Z}[\alpha]$. Thus, we have $(p, \sqrt{d})^2 = (p)$. Setting $P = (p, \sqrt{d})$, we have the desired result. □

The case where $p = 2$ requires separate treatment.

Proposition 3.12. *Let $p = 2$. For any prime ideal P in $\mathbb{Z}[\alpha]$, define P' in the same way as in the proposition above.*
(a) If $d \equiv 5 \bmod 8$, then we have $(2) = P$ for some prime ideal P in $\mathbb{Z}[\alpha]$.
(b) If $d \equiv 1 \bmod 8$, then we have $(2) = PP'$ and $P \neq P'$ for some prime ideal P in $\mathbb{Z}[\alpha]$.
(c) If $d \equiv 2$ or $3 \bmod 4$, then we have $(2) = P^2$ for some prime ideal P in $\mathbb{Z}[\alpha]$.

Proof. (a) Suppose $d \equiv 5 \bmod 8$. Then we have $d \equiv 1 \bmod 4$. Let $f(x)$ be the minimal polynomial of $\alpha = (1+\sqrt{d})/2$. Then we have $f(x) = x^2 - x + (1-d)/4 = x^2 - x + 1$ in $F_2[x]$. Note that $f(x) = x^2 - x + 1$ is irreducible in $F_2[x]$, which means that $(f(x))$ is a prime ideal in $F_2[x]$. It then follows that $\mathbb{Z}[\alpha]/(2) \cong F_2[x]/(f(x))$ is an integral domain, and consequently, (2) is a prime ideal in $\mathbb{Z}[\alpha]$.

(b) If $d \equiv 1 \bmod 8$, we have $d \equiv 1 \bmod 4$ and $(2,(1+\sqrt{d})/2)(2,(1-\sqrt{d})/2) = (2)(2,(1+\sqrt{d})/2,(1-\sqrt{d})/2,(1-d)/8)$. Note that $(2,(1+\sqrt{d})/2,(1-\sqrt{d})/2,(1-d)/8)$ contains $1 = (1+\sqrt{d})/2 + (1-\sqrt{d})/2$, and is consequently the whole ring $\mathbb{Z}[\alpha]$. Thus, we have $(2,(1+\sqrt{d})/2)(2,(1-\sqrt{d})/2) = (2)$. If $(2,(1+\sqrt{d})/2) = (2,(1-\sqrt{d})/2)$, then $(2,(1+\sqrt{d})/2)$ would contain 1, and we would have $(2) = \mathbb{Z}[\alpha]$, which is impossible. Setting $P = (2,(1+\sqrt{d})/2)$, we have the desired result.

(c) Suppose $d \equiv 2 \bmod 4$. Note that we have $(2,\sqrt{d})^2 = (2)(2,\sqrt{d},d/2)$. Since $(2,\sqrt{d},d/2)$ contains 2 and $d/2$ which are relatively prime in $\mathbb{Z}$, $(2,\sqrt{d},d/2)$ contains 1 and is consequently the whole ring $\mathbb{Z}[\alpha]$. Thus, we have $(2,\sqrt{d})^2 = (2)$. Setting $P = (2,\sqrt{d})$, we have the desired result.

Suppose $d \equiv 3 \bmod 4$. Note that we have $(2,1+\sqrt{d})^2 = (2)(2,1+\sqrt{d},\frac{(1+\sqrt{d})^2}{2}) = (2)(2,1+\sqrt{d},\frac{1+d}{2}+\sqrt{d})$. Since $(2,1+\sqrt{d},\frac{1+d}{2}+\sqrt{d})$ contains 2 and $\frac{1-d}{2} = (1+\sqrt{d}) - (\frac{1+d}{2}+\sqrt{d})$, which are relatively prime in $\mathbb{Z}$, $(2,1+\sqrt{d},\frac{1+d}{2}+\sqrt{d})$ contains 1 and is consequently the whole ring $\mathbb{Z}[\alpha]$. Thus, we have $(2,1+\sqrt{d})^2 = (2)$. Setting $P = (2,1+\sqrt{d})$, we have the desired result. □

To conclude our discussion on quadratic integer rings, we shall use the norm defined on quadratic extensions of $\mathbb{Q}$ to characterize the units in quadratic integer rings.

Proposition 3.13. *The element γ is a unit in $\mathbb{Z}[\alpha]$ if and only if $N(\gamma) = \pm 1$.*

Proof. Suppose $N(\gamma) = \pm 1$. Then we have $\gamma\gamma' = \pm 1$, so $\pm\gamma' = \gamma^{-1}$. Since $\pm\gamma'$ lies in $\mathbb{Z}[\alpha]$, we see that γ is a unit in $\mathbb{Z}[\alpha]$.

Suppose that γ is a unit in $\mathbb{Z}[\alpha]$. Then there exists a $\delta \in \mathbb{Z}[\alpha]$ satisfying $\gamma\delta = 1$. Thus, we have $N(\gamma)N(\delta) = 1$. Since $N(\gamma)$ and $N(\delta)$ are ordinary integers, we must have $N(\gamma) = \pm 1$. □

3.3. **The Ring of Gaussian Integers $\mathbb{Z}[i]$.** Let $i = \sqrt{-1}$. The ring of Gaussian integers $\mathbb{Z}[i]$ is the ring of algebraic integers in the quadratic extension $\mathbb{Q}(\sqrt{-1})$ of $\mathbb{Q}$. The elements of $\mathbb{Z}[i]$ are complex numbers of the form $a + bi$ with a, $b \in \mathbb{Z}$. If $\gamma = a + bi$ is an element of $\mathbb{Z}[i]$, then the complex conjugate of γ is $\overline{\gamma} = a - bi$, and the norm of γ (defined on $\mathbb{Q}(\sqrt{-1})$ as in Section 3.1) is $N(\gamma) = \gamma\overline{\gamma} = a^2 + b^2$. We shall now use Propositions 3.11, 3.12 and 3.13 to characterize the prime elements and the units in $\mathbb{Z}[i]$.

Proposition 3.14. *Let p be a rational prime. If $p \equiv 3$ mod 4, then p is inert in $\mathbb{Z}[i]$. If $p \equiv 1$ mod 4, then p splits in $\mathbb{Z}[i]$. Finally, 2 ramifies in $\mathbb{Z}[i]$.*

Proof. If $p \equiv 3 \bmod 4$, we have $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = -1$; consequently, by Proposition 3.11, p is inert in $\mathbb{Z}[i]$.

If $p \equiv 1 \bmod 4$, we have $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = 1$; consequently, by Proposition 3.11, p splits in $\mathbb{Z}[i]$.

Finally, we have $-1 \equiv 3 \bmod 4$; consequently, by Proposition 3.12, 2 ramifies in $\mathbb{Z}[i]$. □

Proposition 3.15. *The element $\gamma \in \mathbb{Z}[i]$ is a unit if and only if $N(\gamma) = 1$. The units in $\mathbb{Z}[i]$ are 1, -1, i, and $-i$.*

Proof. The first assertion follows from Proposition 3.13 and the observation that $N(\gamma)$ is a nonnegative integer for all $\gamma \in \mathbb{Z}[i]$.

Now suppose that $\gamma = a+bi$ is a unit in $\mathbb{Z}[i]$. Then we have $N(\gamma) = a^2+b^2 = 1$. The only possibilities are $a = \pm 1$ and $b = 0$, or $a = 0$ and $b = \pm 1$. It then follows that the units in $\mathbb{Z}[i]$ are 1, -1, i, and $-i$. □

Recall that a Euclidean domain R is an integral domain with the property that there is a function $\eta : R - \{0\} \to \mathbb{Z}_{\geq 0}$ such that if a and b are two elements of R with $b \neq 0$, then there exist q, $r \in R$ satisfying $a = qb + r$ and either $r = 0$ or $\eta(r) < \eta(b)$. We shall now prove that $\mathbb{Z}[i]$ is a Euclidean domain, and make use of the fact that Euclidean domains are principal ideal domains (PIDs).

Proposition 3.16. *The ring of Gaussian integers $\mathbb{Z}[i]$ is a Euclidean domain.*

Proof. Let N denote the norm on $\mathbb{Q}(\sqrt{-1})$. Let $\gamma = a + bi$ and $\delta = c + di$ be two elements of $\mathbb{Z}[i]$ with $\delta \neq 0$.

Then we have $\frac{\gamma}{\delta} = r + si$ for some r, $s \in \mathbb{Q}$. Choose integers m and n satisfying $|r - m| \leq \frac{1}{2}$ and $|s - n| \leq \frac{1}{2}$. Set $\rho = m + ni$. Then we have $\rho \in \mathbb{Z}[i]$ and $N(\frac{\gamma}{\delta} - \rho) = (r-m)^2 + (s-n)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$.

Set $\tau = \gamma - \rho\delta$. Then we have $\tau \in \mathbb{Z}[i]$ and either $\tau = 0$ or $N(\tau) = N(\delta(\frac{\gamma}{\delta} - \rho)) = N(\delta)N(\frac{\gamma}{\delta} - \rho) \leq \frac{1}{2}N(\delta) < N(\delta)$. Thus, N makes $\mathbb{Z}[i]$ into a Euclidean domain. □

Theorem 3.17. *(Fermat's Theorem on sums of squares) A rational prime p is the sum of the squares of two integers in $\mathbb{Z}$, i.e. $p = a^2 + b^2$ for some a, $b \in \mathbb{Z}$, if and only if $p = 2$ or $p \equiv 1 \mod 4$.*

Proof. Note that $p = 2$ or $p \equiv 1 \mod 4$ if and only if p ramifies or splits in $\mathbb{Z}[i]$ (Proposition 3.14), if and only if $p = \gamma\delta$ for some nonunits γ, $\delta \in \mathbb{Z}[i]$ (Here, we uses the fact that $\mathbb{Z}[i]$ is a PID). If $p = \gamma\delta$ for some nonunits γ, $\delta \in \mathbb{Z}[i]$, then we have $p^2 = N(p) = N(\gamma)N(\delta)$; since $N(\gamma) \neq 1$ and $N(\delta) \neq 1$, we must have $p = N(\gamma) = a^2 + b^2$ for some a, $b \in \mathbb{Z}$. Conversely, if $p = a^2 + b^2$ for some a, $b \in \mathbb{Z}$, then we have $p = (a + bi)(a - bi)$, and both $a + bi$ and $a - bi$ are nonunits in $\mathbb{Z}[i]$. The desired result now follows. □

The same reasoning can be used to characterize the rational primes p which can be written as $p = a^2 + 2b^2$ for some a, $b \in \mathbb{Z}$. Instead of $\mathbb{Z}[i]$, we shall now work with $\mathbb{Z}[\sqrt{-2}]$. Like $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$ is also a Euclidean domain, and consequently a PID. We shall now prove that a rational prime p can be written as $p = a^2 + 2b^2$ for some a, $b \in \mathbb{Z}$ if and only if $p = 2$, or $p \equiv 1 \mod 8$, or $p \equiv 3 \mod 8$, or $p \equiv 1 \mod 16$, or $p \equiv 11 \mod 16$, as follows:

Note that $p = 2$, or $p \equiv 1 \mod 8$, or $p \equiv 3 \mod 8$, or $p \equiv 1 \mod 16$, or $p \equiv 11 \mod 16$ if and only if $p = 2$, or $\frac{p-1}{2} + \frac{p^2-1}{8} = \frac{(p-1)(p+5)}{8}$ is an even integer in $\mathbb{Z}$, if and only if $p = 2$, or $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} + \frac{p^2-1}{8}} = 1$, if and only if p ramifies or splits in $\mathbb{Z}[\sqrt{-2}]$, if and only if $p = \gamma\delta$ for some nonunits γ, $\delta \in \mathbb{Z}[\sqrt{-2}]$. If $p = \gamma\delta$ for some nonunits γ, $\delta \in \mathbb{Z}[\sqrt{-2}]$, then we have $p^2 = N(p) = N(\gamma)N(\delta)$; since $N(\gamma) \neq 1$ and $N(\delta) \neq 1$, we must have $p = N(\gamma) = a^2 + 2b^2$ for some a, $b \in \mathbb{Z}$. Conversely, if $p = a^2 + 2b^2$ for some a, $b \in \mathbb{Z}$, then we have $p = (a + b\sqrt{-2})(a - b\sqrt{-2})$, and both $a + b\sqrt{-2}$ and $a - b\sqrt{-2}$ are nonunits in $\mathbb{Z}[\sqrt{-2}]$. The desired result now follows.

In general, the question whether a rational prime p can be written as $p = a^2+nb^2$ for some $a, b \in \mathbb{Z}$ is much more difficult to answer, and the technique used above to characterize the rational primes p which can be written as $p = a^2+b^2$ or $p = a^2+2b^2$ for some $a, b \in \mathbb{Z}$ cannot be generalized for an arbitrary ordinary integer n, because it relies on the fact that $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\sqrt{-2}]$ are PIDs, but $\mathbb{Z}[\sqrt{-n}]$ is, in general, not necessarily a PID. For example, $\mathbb{Z}[\sqrt{-5}]$ is not a PID, and the above technique cannot be used to characterize the rational primes p which can be written as $p = a^2 + 5b^2$.

3.4. **The Ring $\mathbb{Z}[\omega]$.** Let $\omega = \frac{-1+\sqrt{-3}}{2}$. Note that we have $\omega^2 = \frac{-1-\sqrt{-3}}{2} = \overline{\omega}$ and $1 + \omega + \omega^2 = 0$, and 1, ω and ω^2 are the three cubic roots of unity. The ring $\mathbb{Z}[\omega] = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is the ring of algebraic integers in the quadratic extension $\mathbb{Q}(\sqrt{-3})$ of $\mathbb{Q}$. The elements of $\mathbb{Z}[\omega]$ are complex numbers of the form $a + b\omega$ with $a, b \in \mathbb{Z}$. Let $\gamma = a + b\omega \in \mathbb{Z}[\omega]$, and $\overline{\gamma}$ denote the complex conjugate of γ. Then the norm of γ (defined on $\mathbb{Q}(\sqrt{-3})$ as in Section 3.1) is $N(\gamma) = \gamma\overline{\gamma} = a^2 - ab + b^2$. We shall prove that $\mathbb{Z}[\omega]$ is also a Euclidean domain, and use Propositions 3.11, 3.12 and 3.13 again to investigate the units and the prime elements in $\mathbb{Z}[\omega]$. For notational convenience we shall set $D = \mathbb{Z}[\omega]$.

Proposition 3.18. *D is a Euclidean domain.*

Proof. Let N denote the norm on $\mathbb{Q}(\sqrt{-3})$. Let γ and δ be two elements of D with $\delta \neq 0$. Then we have $\frac{\gamma}{\delta} = \frac{\gamma\overline{\delta}}{\delta\overline{\delta}} = r + s\omega$ for some $r, s \in \mathbb{Q}$. We have used the facts that $\delta\overline{\delta} = N(\delta)$ is a positive integer and that $\gamma\overline{\delta}$ lies in D since both γ and $\overline{\delta}$ are elements of D and D is a ring.

Choose $m, n \in \mathbb{Z}$ with $|r - m| \leq \frac{1}{2}$ and $|s - n| \leq \frac{1}{2}$. Set $\rho = m + n\omega$. Then we have $\rho \in D$ and $N(\frac{\gamma}{\delta}-\rho) = (r-m)^2-(r-m)(s-n)+(s-n)^2 \leq \left(\frac{1}{2}\right)^2+\frac{1}{2}\frac{1}{2}+\left(\frac{1}{2}\right)^2 = \frac{3}{4}$.

Set $\tau = \gamma - \rho\delta$. Then we have $\tau \in D$ and either $\tau = 0$ or $N(\tau) = N(\delta(\frac{\gamma}{\delta} - \rho)) = N(\delta)N(\frac{\gamma}{\delta} - \rho) \leq \frac{3}{4}N(\delta) < N(\delta)$. Thus, N makes D into a Euclidean domain. □

Proposition 3.19. *The element $\gamma \in D$ is a unit if and only if $N(\gamma) = 1$. The units in D are 1, -1, ω, $-\omega$, ω^2, and $-\omega^2$.*

Proof. The first assertion follows from Proposition 3.13 and the observation that $N(\gamma)$ is a nonnegative integer for all $\gamma \in D$.

Now suppose that $\gamma = a+b\omega$ is a unit in D. Then we have $N(\gamma) = a^2-ab+b^2 = 1$ and consequently $(2a - b)^2 + 3b^2 = 4$. There are two possibilities:

(1) $2a - b = \pm 1$ and $b = \pm 1$, or

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

Solving the six pairs of equations, we see $\gamma = 1$, -1, ω, $-\omega$, $-1 - \omega = \omega^2$ or $1+\omega = -\omega^2$. It then follows that the units in D are 1, -1, ω, $-\omega$, ω^2, and $-\omega^2$. □

The following propositions characterize the prime elements of $\mathbb{Z}[\omega]$.

Proposition 3.20. *If π is a prime in D, then there is a rational prime p such that $N(\pi) = p$ or p^2. In the former case, π is not an associate to a rational prime; in the latter case π is associate to p.*

Proof. Since π is a prime in D, we have $N(\pi) = \pi\overline{\pi} = n$ for some $n \in \mathbb{Z}$ with $n > 1$. Since n is a product of rational primes, π divides p for some rational prime p. Suppose $p = \pi\gamma$ for some $\gamma \in D$. Then we have $N(\pi)N(\gamma) = N(p) = p^2$. Thus,

we must have $N(\pi) = p$, or $N(\pi) = p^2$ and $N(\gamma) = 1$. In the former case, if we had $\pi = uq$ for some unit $u \in D$ and some rational prime q, then we would have $p = N(\pi) = N(u)N(q) = q^2$, which is impossible. Thus, π is not an associate to a rational prime. In the latter case, since γ is a unit, π is associate to p. □

Proposition 3.21. *If $\pi \in D$ satisfies $N(\pi) = p$ where p is a rational prime, then π is a prime element of D.*

Proof. If π were not prime in D, π would be reducible in D (since D is a Euclidean domain), so we could write $\pi = \rho\gamma$ for some $\rho, \gamma \in D$ with $N(\rho) > 1$ and $N(\gamma) > 1$. Then we would have $p = N(\pi) = N(\rho)N(\gamma)$, which is impossible since p is a rational prime. Thus, π is a prime element of D. □

Proposition 3.22. *Let p be a rational prime. If $p \equiv 2 \mod 3$, then p is a prime element of D. If $p \equiv 1 \mod 3$, then we have $p = \pi\overline{\pi}$, where π is prime in D. Finally we have $3 = -\omega^2(1-\omega)^2$, and $1-\omega$ is prime in D.*

Proof. Suppose $p \equiv 2 \bmod 3$. If p is odd, then by the law of quadratic reciprocity (which is stated in Section 2 and will be proved in Section 5), we have

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

and consequently, by Proposition 3.11, p is a prime element of D. If $p = 2$, since $-3 \equiv 1 \bmod 4$ and $-3 \equiv 5 \bmod 8$, by Proposition 3.12, 2 is a prime element of D.

Suppose $p \equiv 1 \bmod 3$. A similar calculation shows $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$. By Proposition 3.11, we have $(p) = PP'$; since D is a PID, we have $P = (\pi)$ and $P' = (\gamma)$ for some $\pi, \gamma \in D$ with $N(\pi) > 1$ and $N(\gamma) > 1$. Consequently, we have $p = u\pi\gamma$ for some unit $u \in D$, and $p^2 = N(p) = N(\pi)N(\gamma)$, which implies $p = N(\pi) = \pi\overline{\pi}$.

Finally, since $x^2+x+1 = (x-\omega)(x-\omega^2)$, setting $x = 1$, we have $3 = (1-\omega)(1-\omega^2) = (1+\omega)(1-\omega)^2 = -\omega^2(1-\omega)^2$. Since $3^2 = N(3) = N(-\omega^2)N((1-\omega)^2) = (N(1-\omega))^2$, we must have $N(1-\omega) = 3$. By Proposition 3.21, $1-\omega$ is prime in D. □

We need a notion of primary primes to eliminate the ambiguity caused by the fact that every nonzero element of D has six associates.

Definition 3.23. If π is a prime element of D, we say that π is primary if $\pi \equiv 2 \bmod 3$.

If $\pi = a + b\omega$ is a complex prime, the definition above is equivalent to $a \equiv 2 \bmod 3$ and $b \equiv 0 \bmod 3$.

Proposition 3.24. *Let π be a prime element of D with $N(\pi) = p \equiv 1 \mod 3$. Among the associates of π exactly one is primary.*

Proof. Let $\pi = a + b\omega$. The associates of π are π, $-\pi$, $\omega\pi$, $-\omega\pi$, $\omega^2\pi$ and $-\omega^2\pi$, which, in terms of a and b, are
(a) $a + b\omega$,
(b) $-a - b\omega$,
(c) $-b + (a - b)\omega$,
(d) $b + (b - a)\omega$,
(e) $(b - a) - a\omega$, and
(f) $(a - b) + a\omega$.

Since we have $p = a^2 - ab + b^2$, not both a and b are divisible by 3. By comparing (a) and (d), we may assume that 3 does not divide a. By considering (a) and (b), we may assume $a \equiv 2 \bmod 3$. Under these assumptions, $p = a^2 - ab + b^2$ implies $1 \equiv 4 - 2b + b^2 \bmod 3$, which gives $b(b-2) \equiv 0 \bmod 3$. If $b \equiv 0 \bmod 3$, then $a + b\omega$ is primary. If $b \equiv 2 \bmod 3$, then $b + (b - a)\omega$ is primary.

To show the uniqueness of a primary prime among its associates, suppose that $a + b\omega$ is primary. Then we have $a \equiv 2 \bmod 3$ and $b \equiv 0 \bmod 3$. Since we have $-a \equiv 1 \bmod 3$, $-b \equiv 0 \bmod 3$ and $b \equiv 0 \bmod 3$, (b), (c) and (d) are not primary. Since we have $-a \equiv 1 \bmod 3$ and $a \equiv 2 \bmod 3$, (e) and (f) are not primary. □

Let $\lambda \neq 0$ be a nonunit in D. Just as in $\mathbb{Z}$, the congruence classes mod λ in D can be made into a ring $D/\lambda D$, called the residue class ring mod λ.

Proposition 3.25. *Let $\pi \in D$ be a prime. Then $D/\pi D$ is a finite field with $N(\pi)$ elements.*

Proof. We shall first prove that $D/\pi D$ is a field. Note that $D/\pi D$ is an integral domain. Let γ be an element of D with $\gamma \not\equiv 0 \bmod \pi$. Since D is a Euclidean domain, there exist δ, $\rho \in D$ with $\gamma\delta + \pi\rho = 1$, which gives $\gamma\delta \equiv 1 \bmod \pi$. This shows that every nonzero element of $D/\pi D$ is a unit. Thus, $D/\pi D$ is a field.

To show that $D/\pi D$ has $N(\pi)$ elements, we shall consider three cases:

(1) Suppose that $\pi = q$ is a rational prime congruent to 2 mod 3. We claim that $\{a + b\omega : a, b \in \mathbb{Z}, 0 \leq a < q, 0 \leq b < q\}$ gives a complete set of representatives mod q. This will establish that D/qD has $q^2 = N(q)$ elements. Let $\mu = m + n\omega \in D$. Then we have $m = qs + a$ and $n = qt + b$ for some s, a, t, $b \in \mathbb{Z}$ with $0 \leq a, b < q$, and $\mu \equiv a + b\omega \bmod q$. Now, suppose $a + b\omega \equiv a' + b'\omega \bmod q$ with $0 \leq a, b, a', b' < q$. Then we have $((a - a')/q) + ((b - b')/q)\omega \in D$, implying $(a - a')/q \in \mathbb{Z}$ and $(b - b')/q \in \mathbb{Z}$. This is possible only if we have $a = a'$ and $b = b'$.

(2) Suppose that π is a prime element of D with $\pi\overline{\pi} = N(\pi) = p$, where p is a rational prime congruent to 1 mod 3. We claim that $\{0, 1, ..., p-1\}$ gives a complete set of representatives mod π. This will establish that $D/\pi D$ has $p = N(\pi)$ elements. Let $\pi = a + b\omega$. Since $p = N(\pi) = a^2 - ab + b^2$, p does divide b (for otherwise p would divide π and $\overline{\pi}$, and p would be a unit in D, which is impossible). Let $\mu = m + n\omega$. Then there exists some $c \in \mathbb{Z}$ with $cb \equiv n \bmod p$, and we have $\mu - c\pi \equiv m - ca \bmod p$, so $\mu \equiv m - ca \bmod \pi$. Thus, every element of D is congruent to an ordinary integer mod π. For each $l \in \mathbb{Z}$, we have $l = ps + r$ for some s, $r \in \mathbb{Z}$ with $0 \leq r < p$. Thus, we have $l \equiv r \bmod p$, so $l \equiv r \bmod \pi$. We have shown that every element of D is congruent to an element of $\{0, 1, ..., p-1\}$ mod π. Now, suppose $r \equiv r' \bmod \pi$ with r, $r' \in \mathbb{Z}$ and $0 \leq r, r' < p$. Then we have $r - r' = \pi\gamma$ for some $\gamma \in D$, and $(r - r')^2 = pN(\gamma)$, which implies that p divides $r - r'$, i.e. $r \equiv r' \bmod p$. Consequently, we must have $r = r'$.

(3) Suppose $\pi = 1-\omega$. Then we have $N(\pi) = 3$. We claim that $\{0, 1, 2\}$ gives a complete set of representatives mod π. This will establish that $D/\pi D$ has $3 = N(\pi)$ elements. Let $\mu = m + n\omega$. Then we have $\mu + n\pi = m + n$, so $\mu \equiv m + n \bmod \pi$. Thus, every element of D is congruent to an ordinary integer mod π. To show that every element of D is congruent to an element of $\{0, 1, 2\}$ mod π, and that 0, 1 and 2 are distinct residues mod π, we use the same technique as in case (2), with p replaced by 3. □

Corollary 3.26. *Let π be a prime element of D. The multiplicative group $(D/\pi D)^\times$ of $D/\pi D$ is cyclic with order $N(\pi) - 1$. Consequently, if π does not divide $\gamma \in D$, then we have $\gamma^{N(\pi)-1} \equiv 1$ mod π.*

Corollary 3.27. *Let π be a prime element of D with $N(\pi) \neq 3$, and γ be an element of D such that π does not divide γ. Then the residue classes of 1, ω, ω^2 are distinct in $D/\pi D$, and there is a unique integer $m = 0$, 1 or 2 such that $\gamma^{(N(\pi)-1)/3} \equiv \omega^m$ mod π.*

Proof. To see that the residue classes of 1, ω, ω^2 are distinct in $D/\pi D$, suppose, first, $\omega \equiv 1 \bmod \pi$. Then π would divide $1-\omega$, and since $1-\omega$ is prime in D, π and $1-\omega$ would be associate, and we would have $N(\pi) = N(1-\omega) = 3$, a contradiction. Suppose $\omega^2 \equiv 1 \bmod \pi$. Then π would divide $1 - \omega^2 = (1+\omega)(1-\omega)$. Since π is prime in D and π does not divide $1-\omega$, π would have to divide $1 + \omega = -\omega^2$, but this is impossible since $-\omega^2$ is a unit. Finally, suppose $\omega^2 \equiv \omega \bmod \pi$. Then π would divide $\omega - \omega^2 = \omega(1-\omega)$. Since π is a prime in D and π does not divide $1-\omega$, π would have to divide ω, but this is again impossible since ω is a unit.

We know that π divides $\gamma^{N(\pi)-1}-1 = (\gamma^{(N(\pi)-1)/3}-1)(\gamma^{(N(\pi)-1)/3}-\omega)(\gamma^{(N(\pi)-1)/3}-\omega^2)$. Since π is prime in D, it must divide at least one of the three factors; on the other hand, π can divide at most one of the three factors, since if it divided two factors, it would divide the difference. Thus, π divides exactly one of the three factors. The desired result now follows. □

On the basis of Corollary 3.27 we can define the cubic residue character as follows:

Definition 3.28. Let π be a prime element of D with $N(\pi) \neq 3$. For all $\gamma \in D$, the cubic residue character of γ mod π, $\left(\frac{\gamma}{\pi}\right)_3$, is given by
(a) $\left(\frac{\gamma}{\pi}\right)_3 = 0$ if π divides γ.
(b) $\left(\frac{\gamma}{\pi}\right)_3 \equiv \gamma^{(N(\pi)-1)/3} \bmod \pi$, with $\left(\frac{\gamma}{\pi}\right)_3 = 1$, ω or ω^2, if π does not divide γ.

The cubic residue character plays an analogous role in the theory of cubic residues as the Legendre symbol plays in the theory of quadratic residues. For the rest of this paper, let $\chi_\pi(\gamma) = \left(\frac{\gamma}{\pi}\right)_3$ denote the cubic residue character of γ mod π for all $\gamma \in D$. The following proposition summarizes some of the properties of the cubic residue character.

Proposition 3.29. *Let π be a prime element of D with $N(\pi) \neq 3$. Then for all γ, $\delta \in D$, we have*
(a) $\chi_\pi(\gamma) = 1$ if and only if $x^3 \equiv \gamma$ mod π is solvable, i.e. if and only if γ is a cubic residue mod π.
(b) $\chi_\pi(\gamma) \equiv \gamma^{(N(\pi)-1)/3}$ mod π.
(c) $\chi_\pi(\gamma) = \chi_\pi(\delta)$ if $\gamma \equiv \delta$ mod π.
(d) $\chi_\pi(\gamma\delta) = \chi_\pi(\gamma)\chi_\pi(\delta)$.

(e) $\overline{\chi_\pi(\gamma)} = \chi_\pi(\gamma)^2 = \chi_\pi(\gamma^2)$.
(f) $\overline{\chi_\pi(\gamma)} = \chi_{\overline{\pi}}(\overline{\gamma})$.

Proof. (a) This is a special case of Proposition 2.8 with $F = D/\pi D$, $q = N(\pi)$, $a = \gamma$, and $n = 3$.

(b) This is immediate from the definition.

(c) If $\gamma \equiv \delta \bmod \pi$, we have $\chi_\pi(\gamma) \equiv \gamma^{(N(\pi)-1)/3} \equiv \delta^{(N(\pi)-1)/3} \equiv \chi_\pi(\delta) \bmod \pi$, which implies $\chi_\pi(\gamma) = \chi_\pi(\delta)$.

(d) Since we have $\chi_\pi(\gamma\delta) \equiv (\gamma\delta)^{(N(\pi)-1)/3} \equiv \gamma^{(N(\pi)-1)/3}\delta^{(N(\pi)-1)/3} \equiv \chi_\pi(\gamma)\chi_\pi(\delta) \bmod \pi$, we must have $\chi_\pi(\gamma\delta) = \chi_\pi(\gamma)\chi_\pi(\delta)$.

(e) $\chi_\pi(\gamma)$ is by definition 0, 1, ω, or ω^2, and each of these squared is equal to its complex conjugate.

(f) Since we have $\chi_\pi(\gamma) \equiv \gamma^{(N(\pi)-1)/3} \bmod \pi$, we must also have $\overline{\chi_\pi(\gamma)} \equiv \overline{\gamma}^{(N(\pi)-1)/3} = \overline{\gamma}^{(N(\overline{\pi})-1)/3} \equiv \chi_{\overline{\pi}}(\overline{\gamma}) \bmod \overline{\pi}$, which implies $\overline{\chi_\pi(\gamma)} = \chi_{\overline{\pi}}(\overline{\gamma})$. □

Proposition 3.29 allows us to regard the cubic residue character as a multiplicative character of order 3 on $D/\pi D$.

Corollary 3.30. *Let q be a rational prime with $q \equiv 2$ mod 3. Then we have $\chi_q(\overline{\gamma}) = \chi_q(\gamma^2)$ and $\chi_q(n) = 1$ if $n \in \mathbb{Z}$ is relatively prime to q. In particular, if $q_1 \neq q_2$ are two rational primes congruent to 2 mod 3, then q_1 and q_2 are prime elements of D and we have $\chi_{q_1}(q_2) = \chi_{q_2}(q_1)$.*

Proof. Since q is a rational prime with $q \equiv 2 \bmod 3$, q is prime in D and we have $\overline{q} = q$. Consequently, we must have $\chi_q(\overline{\gamma}) = \chi_{\overline{q}}(\overline{\gamma}) = \overline{\chi_q(\gamma)} = \chi_q(\gamma^2)$. Since we have $\overline{n} = n$, we must have $\chi_q(n) = \chi_q(\overline{n}) = \chi_q(n)^2$; if $n \in \mathbb{Z}$ is relatively prime to q, we have $\chi_q(n) \neq 0$, which implies $\chi_q(n) = 1$.

If $q_1 \neq q_2$ are two rational primes congruent to 2 mod 3, then q_1 and q_2 are prime elements of D and they are relatively prime to each other in $\mathbb{Z}$; consequently, we must have $\chi_{q_1}(q_2) = 1$ and $\chi_{q_2}(q_1) = 1$, and the desired result follows immediately. □

Corollary 3.30 gives a special case of the law of cubic reciprocity. We shall now state the general law:

Let π_1, $\pi_2 \in D$ be primary primes with $N(\pi_1)$, $N(\pi_2) \neq 3$ and $N(\pi_1) \neq N(\pi_2)$. Then we have $\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$.

A proof will be given in Section 6.

4. Gauss and Jacobi Sums

In this section, we shall develop the concepts of Gauss and Jacobi sums, which will be used later to find the number of solutions to congruence equations of the form $x^n + y^n \equiv 1 \bmod p$ when $n = 2$ or 3, and to prove the laws of quadratic and cubic reciprocity.

4.1. **Gauss Sums.**

Definition 4.1. Let $\zeta = e^{2\pi i/p}$ be a pth root of unity, χ be a multiplicative character on F_p, and a be any element of F_p. Define $g_a(\chi) = \sum_{t \in F_p} \chi(t)\zeta^{at}$. Then $g_a(\chi)$ is called a Gauss sum on F_p belonging to the character χ.

When χ is the Legendre symbol, $g_a(\chi)$ is called a quadratic Gauss sum, and will be denoted simply as g_a. Thus, we have $g_a = \sum_{t\in F_p} \left(\frac{t}{p}\right) \zeta^{at}$.

To prove some of the properties of Gauss sums, we need a lemma.

Lemma 4.2. *$\sum_{t=0}^{p-1} \zeta^{at}$ is equal to p if $a \equiv 0 \mod p$; otherwise it is zero.*

Proof. If $a \equiv 0 \mod p$, we have $\zeta^a = 1$, so $\sum_{t=0}^{p-1} \zeta^{at} = \sum_{t=0}^{p-1} 1 = p$. If $a \not\equiv 0 \mod p$, we have $\zeta^a \neq 1$ and $\sum_{t=0}^{p-1} \zeta^{at} = (\zeta^{ap} - 1)/(\zeta^a - 1) = 0$. □

Corollary 4.3. *$p^{-1} \sum_{t=0}^{p-1} \zeta^{t(x-y)} = \delta(x, y)$, where $\delta(x, y) = 1$ if $x \equiv y \mod p$ and $\delta(x, y) = 0$ if $x \not\equiv y \mod p$.*

The following propositions summarize the properties of Gauss sums. Again, ϵ denotes the trivial character on F_p.

Proposition 4.4. *If $a \neq 0$ and $\chi \neq \epsilon$, we have $g_a(\chi) = \chi(a^{-1})g_1(\chi)$. If $a \neq 0$ and $\chi = \epsilon$, we have $g_a(\epsilon) = 0$. If $a = 0$ and $\chi \neq \epsilon$, we have $g_0(\chi) = 0$. If $a = 0$ and $\chi = \epsilon$, we have $g_0(\epsilon) = p$.*

Proof. Suppose $a \neq 0$ and $\chi \neq \epsilon$. Then we have $\chi(a)g_a(\chi) = \chi(a) \sum_{t\in F_p} \chi(t)\zeta^{at} = \sum_{t\in F_p} \chi(at)\zeta^{at} = g_1(\chi)$, so $g_a(\chi) = \chi(a)^{-1}g_1(\chi) = \chi(a^{-1})g_1(\chi)$.

If $a \neq 0$, we have $g_a(\epsilon) = \sum_{t\in F_p} \epsilon(t)\zeta^{at} = \sum_{t\in F_p} \zeta^{at} = 0$, by Lemma 4.2.

Now, for all characters χ on F_p, we have $g_0(\chi) = \sum_{t\in F_p} \chi(t)\zeta^{0t} = \sum_{t\in F_p} \chi(t)$, which is equal to 0 if $\chi \neq \epsilon$, and is equal to p if $\chi = \epsilon$, by Proposition 2.11(d). □

Corollary 4.5. $g_a = \left(\frac{a}{p}\right) g_1$.

From now on we shall denote $g_1(\chi)$ simply as $g(\chi)$ and g_1 simply as g.

Proposition 4.6. *If $\chi \neq \epsilon$, we have $|g(\chi)| = \sqrt{p}$.*

Proof. We shall evaluate $\sum_{a\in F_p} g_a(\chi)\overline{g_a(\chi)}$ in two ways.

If $a \neq 0$, then by Proposition 4.4, we have $g_a(\chi) = \chi(a^{-1})g(\chi)$ and $\overline{g_a(\chi)} = \overline{\chi(a^{-1})g(\chi)} = \chi(a)\overline{g(\chi)}$, so $g_a(\chi)\overline{g_a(\chi)} = \chi(a^{-1})\chi(a)g(\chi)\overline{g(\chi)} = g(\chi)\overline{g(\chi)} = |g(\chi)|^2$. Since $g_0(\chi) = 0$, we have $\sum_{a\in F_p} g_a(\chi)\overline{g_a(\chi)} = (p-1)\,|g(\chi)|^2$.

On the other hand, we have

$$g_a(\chi)\overline{g_a(\chi)} = \sum_{x\in F_p} \sum_{y\in F_p} \chi(x)\overline{\chi(y)}\zeta^{a(x-y)}.$$

By Corollary 4.3, we have

$$\sum_{a\in F_p} g_a(\chi)\overline{g_a(\chi)} = \sum_{x\in F_p} \sum_{y\in F_p} \chi(x)\overline{\chi(y)}\delta(x, y)p = (p-1)p.$$

Thus, we have $(p-1)\,|g(\chi)|^2 = (p-1)p$, which gives the desired result. □

Corollary 4.7. *$g(\chi)g(\overline{\chi}) = \chi(-1)p$; in particular, $g^2 = (-1)^{(p-1)/2}p$.*

Proof. Since $\overline{g(\chi)} = \sum_{t\in F_p} \overline{\chi(t)}\zeta^{-t} = \overline{\chi(-1)} \sum_{t\in F_p} \overline{\chi(-t)}\zeta^{-t} = \chi(-1)g(\overline{\chi})$, we have $g(\overline{\chi}) = \chi(-1)\overline{g(\chi)}$, so $g(\chi)g(\overline{\chi}) = \chi(-1)g(\chi)\overline{g(\chi)} = \chi(-1)p$. Letting χ be the Legendre symbol, we have $g^2 = (-1)^{(p-1)/2}p$. □

4.2. **Jacobi Sums.**

Definition 4.8. Let χ_1, χ_2, ..., χ_r be characters on F_p. A Jacobi sum is defined by the formula

$$J(\chi_1, \chi_2, ..., \chi_r) = \sum_{t_1+...+t_r=1} \chi_1(t_1)\chi_2(t_2)...\chi_r(t_r).$$

It is useful to define another sum

$$J_0(\chi_1, \chi_2, ..., \chi_r) = \sum_{t_1+...+t_r=0} \chi_1(t_1)\chi_2(t_2)...\chi_r(t_r).$$

Some properties of Jacobi sums are given in the following propositions.

Proposition 4.9. *Let $\chi_1, \chi_2, ..., \chi_r, \chi$ be characters on F_p, and ϵ denote the trivial character.*
(a) $J_0(\epsilon, \epsilon, ..., \epsilon) = J(\epsilon, \epsilon, ..., \epsilon) = p^{r-1}$.
(b) $J_0(\chi_1, \chi_2, ..., \chi_r) = J(\chi_1, \chi_2, ..., \chi_r) = 0$, if some but not all of the χ_i are trivial.
(c) $J(\chi, \chi^{-1}) = -\chi(-1)$, if χ is nontrivial.
(d) Suppose $\chi_r \neq \epsilon$. Then $J_0(\chi_1, \chi_2, ..., \chi_r)$ is equal to 0 if $\chi_1\chi_2...\chi_r$ is nontrivial, and is equal to $\chi_r(-1)(p-1)J(\chi_1, \chi_2, ..., \chi_{r-1})$ if $\chi_1\chi_2...\chi_r$ is trivial.

Proof. (a) Note that there are p^{r-1} distinct r-tuples $(t_1, t_2, ..., t_r)$ satisfying $t_1 + t_2 + ... + t_r = 0$. Thus, we have $J_0(\epsilon, \epsilon, ..., \epsilon) = \sum_{t_1+...+t_r=0} 1 = p^{r-1}$. The same reasoning shows $J(\epsilon, \epsilon, ..., \epsilon) = p^{r-1}$.

(b) Suppose that χ_1, χ_2, ..., χ_s are nontrivial and χ_{s+1}, χ_{s+2}, ..., χ_r are trivial. Then we have

$$\begin{aligned} J_0(\chi_1, \chi_2, ..., \chi_r) &= \sum_{t_1+...+t_r=0} \chi_1(t_1)\chi_2(t_2)...\chi_r(t_r) \\ &= \sum_{t_1, t_2..., t_{r-1}} \chi_1(t_1)\chi_2(t_2)...\chi_s(t_s) \\ &= p^{r-s-1} \left(\sum_{t_1} \chi_1(t_1)\right)\left(\sum_{t_2} \chi_2(t_2)\right)...\left(\sum_{t_s} \chi_s(t_s)\right) \\ &= 0. \end{aligned}$$

The same reasoning shows $J(\chi_1, \chi_2, ..., \chi_r) = 0$.

(c) Note that we have

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

Setting $c = \frac{a}{1-a}$, we have

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

(d) Note that we have

$$J_0(\chi_1, \chi_2, ..., \chi_r) = \sum_s \left(\sum_{t_1+...+t_{r-1}=-s} \chi_1(t_1)...\chi_{r-1}(t_{r-1})\right)\chi_r(s).$$

Since χ_r is nontrivial, we have $\chi_r(0) = 0$, and we may assume $s \neq 0$ in the above sum. For $s \neq 0$, define t_i' by $t_i = -st_i'$. Then we have

$$\sum_{t_1+...+t_{r-1}=-s} \chi_1(t_1)...\chi_{r-1}(t_{r-1}) = \chi_1\chi_2...\chi_{r-1}(-s) \sum_{t_1'+...+t_{r-1}'=1} \chi_1(t_1')...\chi_{r-1}(t_{r-1}')$$
$$= \chi_1\chi_2...\chi_{r-1}(-s)J(\chi_1, ..., \chi_{r-1}).$$

Combining these results, we have

$$J_0(\chi_1, \chi_2, ..., \chi_r) = \chi_1\chi_2...\chi_{r-1}(-1)J(\chi_1, ..., \chi_{r-1}) \sum_{s\neq 0} \chi_1\chi_2...\chi_r(s).$$

The desired result follows since $\sum_{s\neq 0} \chi_1\chi_2...\chi_r(s)$ is equal to 0 if $\chi_1\chi_2...\chi_r$ is nontrivial, and is equal to $p-1$ if $\chi_1\chi_2...\chi_r$ is trivial. □

Corollary 4.10. *Let χ be a nontrivial character. Then we have*
(a) $J(\epsilon, \epsilon) = p$.
(b) $J(\epsilon, \chi) = 0$.

Proposition 4.11. *Suppose that $\chi_1, \chi_2, ..., \chi_r$ are nontrivial characters on F_p and $\chi_1\chi_2...\chi_r$ is also nontrivial. Then we have*

$$g(\chi_1)g(\chi_2)...g(\chi_r) = J(\chi_1, \chi_2, ..., \chi_r)g(\chi_1\chi_2...\chi_r).$$

Proof. For $t \in F_p$, define $\psi(t) = \zeta^t$. Then we have $\psi(x + y) = \psi(x)\psi(y)$ and $g(\chi) = \sum_{t\in F_p} \chi(t)\psi(t)$. Now,

$$g(\chi_1)g(\chi_2)...g(\chi_r) = \left(\sum_{t_1} \chi_1(t_1)\psi(t_1)\right) ... \left(\sum_{t_r} \chi_r(t_r)\psi(t_r)\right)$$
$$= \sum_s \left(\sum_{t_1+...+t_r=s} \chi_1(t_1)\chi_2(t_2)...\chi_r(t_r)\right)\psi(s).$$

If $s = 0$, then by Proposition 4.9(d), we have

$$\sum_{t_1+...+t_r=s} \chi_1(t_1)\chi_2(t_2)...\chi_r(t_r) = 0.$$

For $s \neq 0$, define t_i' by $t_i = st_i'$, and then we have

$$\sum_{t_1+...+t_r=s} \chi_1(t_1)\chi_2(t_2)...\chi_r(t_r) = \chi_1\chi_2...\chi_r(s) \sum_{t_1'+...+t_r'=1} \chi_1(t_1')\chi_2(t_2')...\chi_r(t_r')$$
$$= \chi_1\chi_2...\chi_r(s)J(\chi_1, \chi_2, ..., \chi_r).$$

Combining these results, we have

$$g(\chi_1)g(\chi_2)...g(\chi_r) = J(\chi_1, \chi_2, ..., \chi_r) \sum_{s\neq 0} \chi_1\chi_2...\chi_r(s)\psi(s)$$
$$= J(\chi_1, \chi_2, ..., \chi_r)g(\chi_1\chi_2...\chi_r).$$

□

Corollary 4.12. *Suppose that $\chi_1, \chi_2, ..., \chi_r$ are nontrivial characters on F_p but $\chi_1\chi_2...\chi_r$ is trivial. Then we have*

$$g(\chi_1)g(\chi_2)...g(\chi_r) = \chi_r(-1)pJ(\chi_1, \chi_2, ..., \chi_{r-1})$$

and

$$J(\chi_1, \chi_2, ..., \chi_r) = -\chi_r(-1)J(\chi_1, \chi_2, ..., \chi_{r-1}).$$

If $r = 2$, *set* $J(\chi_1) = 1$.

Proof. By Proposition 4.11, we have

$$g(\chi_1)g(\chi_2)...g(\chi_{r-1}) = J(\chi_1, \chi_2, ..., \chi_{r-1})g(\chi_1\chi_2...\chi_{r-1}).$$

Multiply both sides of the equation by $g(\chi_r)$. The desired result follows since we have $g(\chi_1\chi_2...\chi_{r-1})g(\chi_r) = g(\chi_r^{-1})g(\chi_r) = g(\overline{\chi_r})g(\chi_r) = \chi_r(-1)p$.

Note that when $r = 2$, the second equation is equivalent to Proposition 4.9(c).

Suppose $r > 2$. Using the same reasoning as in the proof of Proposition 4.11 with the hypothesis that $\chi_1\chi_2...\chi_r$ is trivial, we have

$$g(\chi_1)g(\chi_2)...g(\chi_r) = J_0(\chi_1, \chi_2, ..., \chi_r) + J(\chi_1, \chi_2, ..., \chi_r)\sum_{s\neq 0}\psi(s).$$

Note that we have $\sum_s \psi(s) = 0$, so $\sum_{s\neq 0}\psi(s) = 0 - \psi(0) = -1$. By Proposition 4.9(d), we have $J_0(\chi_1, \chi_2, ..., \chi_r) = \chi_r(-1)(p-1)J(\chi_1, \chi_2, ..., \chi_{r-1})$. Also, we have $g(\chi_1)g(\chi_2)...g(\chi_r) = \chi_r(-1)pJ(\chi_1, \chi_2, ..., \chi_{r-1})$. Combining these results, we have

$$\begin{aligned} J(\chi_1, \chi_2, ..., \chi_r) &= J_0(\chi_1, \chi_2, ..., \chi_r) - g(\chi_1)g(\chi_2)...g(\chi_r) \\ &= -\chi_r(-1)J(\chi_1, \chi_2, ..., \chi_{r-1}). \end{aligned}$$

□

Corollary 4.13. *If* χ, λ, *and* $\chi\lambda$ *are nontrivial characters, then we have*

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

Proposition 4.14. *Suppose that* $\chi_1, \chi_2, ..., \chi_r$ *are nontrivial.*
If $\chi_1\chi_2...\chi_r$ *is nontrivial, then we have*

$$|J(\chi_1, \chi_2, ..., \chi_r)| = p^{(r-1)/2}.$$

If $\chi_1\chi_2...\chi_r$ *is trivial, then we have*

$$|J_0(\chi_1, \chi_2, ..., \chi_r)| = (p-1)p^{(r/2)-1}$$

and

$$|J(\chi_1, \chi_2, ..., \chi_r)| = p^{(r/2)-1}.$$

Proof. We know $|g(\chi)| = \sqrt{p}$ for any nontrivial character χ. Thus, if $\chi_1\chi_2...\chi_r$ is nontrivial, by Proposition 4.11, we have

$$|J(\chi_1, \chi_2, ..., \chi_r)| = \frac{|g(\chi_1)|...|g(\chi_r)|}{|g(\chi_1...\chi_r)|} = (\sqrt{p})^{r-1} = p^{(r-1)/2}.$$

If $\chi_1\chi_2...\chi_r$ is trivial, by Proposition 4.9(d) and Corollary 4.12, we have

$$|J_0(\chi_1, \chi_2, ..., \chi_r)| = (p-1)\,|J(\chi_1, \chi_2, ..., \chi_{r-1})| = (p-1)p^{(r-2)/2} = (p-1)p^{(r/2)-1},$$

and

$$|J(\chi_1, \chi_2, ..., \chi_r)| = |J(\chi_1, \chi_2, ..., \chi_{r-1})| = p^{(r-2)/2} = p^{(r/2)-1}.$$

□

Corollary 4.15. *If* χ, λ, *and* $\chi\lambda$ *are nontrivial characters, then we have* $|J(\chi, \lambda)| = \sqrt{p}$.

Proposition 4.16. *Suppose that $n \in \mathbb{Z}$ is an ordinary integer with $n > 2$, and that p is a rational prime with $p \equiv 1 \ mod\ n$. Then there is a character of order n on F_p. Let χ be a character of order n on F_p. Then we have*

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

Proof. We know that the group of multiplicative characters on F_p is cyclic with order $p-1$. Let λ be a generator of the group. Since n divides $p-1$, the character $\lambda^{(p-1)/n}$ has order n. This proves existence.

Let χ be a character of order n on F_p. By Corollary 4.13, we have $g(\chi)^2 = J(\chi,\chi)g(\chi^2)$. Multiplying both sides of the equation by $g(\chi)$, we have $g(\chi)^3 = J(\chi,\chi)g(\chi^2)g(\chi) = J(\chi,\chi)J(\chi,\chi^2)g(\chi^3)$. Continuing in this way, we shall obtain

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

The desired result follows from multiplying both sides of the equation above by $g(\chi)$, since we have $g(\chi^{n-1})g(\chi) = g(\chi^{-1})g(\chi) = g(\overline{\chi})g(\chi) = \chi(-1)p$. □

Corollary 4.17. *If p is a rational prime with $p \equiv 1 \ mod\ 3$, then there is a cubic character on F_p. Let χ be a cubic character on F_p. Then we have $g(\chi)^3 = pJ(\chi,\chi)$.*

Proof. Set $n = 3$ in the proposition above. The desired result follows since we have $\chi(-1) = \chi((-1)^3) = \chi^3(-1) = 1$. □

The following proposition characterizes the Jacobi sum $J(\chi,\chi)$ when χ is a cubic character.

Proposition 4.18. *Suppose that p is a rational prime with $p \equiv 1 \ mod\ 3$, and that χ is a cubic character on F_p. Then we have $J(\chi,\chi) = a + b\omega$, where $\omega = \frac{-1+\sqrt{-3}}{2}$, for some a, $b \in \mathbb{Z}$ with $a \equiv -1 \ mod\ 3$ and $b \equiv 0 \ mod\ 3$.*

Proof. Since χ is a cubic character, the values of χ must be cubic roots of unity, i.e. the values of χ are in the set $\{1, \omega, \omega^2\}$. By the definition of Jacobi sums, we have $J(\chi,\chi) = \sum_{x+y=1} \chi(x)\chi(y)$, which is a $\mathbb{Z}$ linear combination of 1, ω, $\omega^2 = -1-\omega$, $\omega^3 = 1$ and $\omega^4 = \omega$. Thus, we have $J(\chi,\chi) = a + b\omega$ for some a, $b \in \mathbb{Z}$.

Note that we have

$$g(\chi)^3 = \left(\sum_t \chi(t)\zeta^t\right)^3 \equiv \sum_t \chi(t)^3\zeta^{3t} \, mod\, 3.$$

Since $\chi(0) = 0$ and $\chi(t)^3 = 1$ for $t \neq 0$, we have $\sum_t \chi(t)^3\zeta^{3t} = \sum_{t\neq 0} \zeta^{3t} = -1$. Thus, we have

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

Since $\overline{g(\chi)} = g(\overline{\chi})$, we also have

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

Consequently, we have $b(\omega - \overline{\omega}) \equiv 0 \bmod 3$, or $b\sqrt{-3} \equiv 0 \bmod 3$. It then follows that 9 divides $-3b^2$, so 3 divides b. Since 3 divides b and we have $a + b\omega \equiv -1 \bmod 3$, we must have $a \equiv -1 \bmod 3$. □

Corollary 4.19. *Suppose that p is a rational prime with $p \equiv 1 \ mod\ 3$. There exist A, $B \in \mathbb{Z}$ such that $4p = A^2 + 27B^2$ and $A \equiv 1 \ mod\ 3$.*

Proof. Since p is a rational prime with $p \equiv 1 \bmod 3$, there is a cubic character on F_p. Let χ be a cubic character on F_p. Then we have shown that $J(\chi, \chi) = a + b\omega$ for some a, $b \in \mathbb{Z}$ with $a \equiv -1 \bmod 3$ and $b \equiv 0 \bmod 3$. Set $A = 2a - b$ and $B = b/3$. Note that we have $A = 2a - b \equiv -2 \equiv 1 \bmod 3$.

Since $p = |J(\chi, \chi)|^2 = |a + b\omega|^2$, we have $p = a^2 - ab + b^2$. Thus, we have $4p = (2a - b)^2 + 3b^2 = A^2 + 27B^2$. □

4.3. **The Equations of the Form $x^n + y^n = 1$ in F_p for $n = 2$ or 3.** Let $N(x^n + y^n = 1)$ denote the number of solutions to equations of the form $x^n + y^n = 1$ in F_p. To illustrate the usefulness of Gauss and Jacobi sums, we shall use them to determine $N(x^n + y^n = 1)$ when $n = 2$ or 3.

Lemma 4.20. *Let p be an odd rational prime, and let $N(x^n = a)$ denote the number of solutions to the equation $x^n = a$ in F_p. Then we have $N(x^2 = a) = 1 + \left(\frac{a}{p}\right)$.*

Proof. This is a special case of Proposition 2.15. □

Proposition 4.21. *Let p be an odd rational prime. We have $N(x^2 + y^2 = 1) = p - (-1)^{(p-1)/2}$.*

Proof. Let χ denote the Legendre symbol mod p. Then we have $\chi^{-1} = \chi$, and

$$\begin{aligned}
N(x^2 + y^2 = 1) &= \sum_{a+b=1} N(x^2 = a)N(y^2 = b) \\
&= \sum_{a+b=1} \left(1 + \left(\frac{a}{p}\right)\right)\left(1 + \left(\frac{b}{p}\right)\right) \\
&= p + \sum_{a} \left(\frac{a}{p}\right) + \sum_{b} \left(\frac{b}{p}\right) + \sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \\
&= p + 0 + 0 + \sum_{a+b=1} \chi(a)\chi(b) \\
&= p + \sum_{a+b=1} \chi(a)\chi^{-1}(b) \\
&= p + J(\chi, \chi^{-1}) \\
&= p - \chi(-1) \\
&= p - (-1)^{(p-1)/2}.
\end{aligned}$$

□

Proposition 4.22. *Suppose that p is a rational prime with $p \equiv 2$ mod 3. Then we have $N(x^3 + y^3 = 1) = p$.*

Proof. It is clear that $x^3 = 0$ has exactly one solution in F_p, namely, $x = 0$. For each $a \in F_p^\times$, since $(3, p - 1) = 1$ and $a^{(p-1)/1} = a^{p-1} = 1$, by Proposition 2.8, $x^3 = a$ has exactly one solution in F_p. Thus, we have $N(x^3 = a) = 1$ for all $a \in F_p$, and

$$N(x^3 + y^3 = 1) = \sum_{a+b=1} N(x^3 = a)N(y^3 = b) = \sum_{a=0}^{p-1} 1 = p.$$

□

Proposition 4.23. *Suppose that p is a rational prime with $p \equiv 1$ mod 3. Then there are A, $B \in \mathbb{Z}$ with $4p = A^2 + 27B^2$. If we require $A \equiv 1$ mod 3, then A is uniquely determined, and we have $N(x^3 + y^3 = 1) = p - 2 + A$.*

Proof. We have proved the existence of A, $B \in \mathbb{Z}$ satisfying $4p = A^2 + 27B^2$ (Corollary 4.19). To show that A is uniquely determined if we require $A \equiv 1$ mod 3, we shall write

$$\begin{aligned} 4p &= A^2 + 27B^2 \\ &= (A + 3B\sqrt{-3})(A - 3B\sqrt{-3}) \\ &= (A + 3B(2\omega + 1))(A - 3B(2\omega + 1)) \\ &= (A + 3B + 6B\omega)(A - 3B - 6B\omega) \\ &= (A + 3B + 6B\omega)\overline{(A + 3B + 6B\omega)}. \end{aligned}$$

Since p is a rational prime with $p \equiv 1$ mod 3, by Proposition 3.22, we have $p = \pi\overline{\pi}$ for some prime element π of $\mathbb{Z}[\omega]$, and consequently, $4p = 2\pi\overline{2\pi}$. Note that there are 12 choices of π, because π and $\overline{\pi}$ each has six associates, and we can interchange π and $\overline{\pi}$. Since $\mathbb{Z}[\omega]$ is a UFD, there is at least one choice of π such that $A+3B+6B\omega = 2\pi$. Let such a π be equal to $x + y\omega$. Then we have $A + 3B + 6B\omega = 2x + 2y\omega$, i.e. $A+3B = 2x$ and $6B = 2y$ (or equivalently, $3B = y$). Consequently, we have $A \equiv 2x$ mod 3 and $y \equiv 0$ mod 3. If we require $A \equiv 1$ mod 3, then we have $2x \equiv 1$ mod 3, i.e. $x \equiv 2$ mod 3. It then follows that $\pi = x + y\omega$ must be a primary prime. There are only two primary primes among the 12 choices of π, and they are conjugate to each other. Suppose that $a+b\omega$ and $\overline{a + b\omega} = a-b-b\omega$ are the two primary primes such that $p = (a + b\omega)(a - b - b\omega)$. If $A + 3B + 6B\omega = 2(a + b\omega)$, then we have $A+3B = 2a$ and $6B = 2b$, which give $A = 2a-b$; if $A+3B+6B\omega = 2(a-b-b\omega)$, then we have $A + 3B = 2a - 2b$ and $6B = -2b$, which again give $A = 2a - b$. This shows that A is uniquely determined.

Since 3 divides $p - 1$, the proof of Proposition 2.15 shows that there are exactly 3 distinct characters ϵ, χ and χ^2 of order dividing 3, where ϵ is the trivial character and χ and χ^2 both have order 3, and the proposition itself tells us $N(x^3 = a) = 1 + \chi(a) + \chi^2(a)$. Note that we have $\chi(-1) = \chi((-1)^3) = \chi^3(-1) = 1$ and $\chi^2 = \chi^{-1} = \overline{\chi}$. We are now ready to compute $N(x^3 + y^3 = 1)$:

$$\begin{aligned} N(x^3 + y^3 = 1) &= \sum_{a+b=1} N(x^3 = a)N(y^3 = b) \\ &= \sum_{a+b=1} \sum_{i=0}^{2} \chi^i(a) \sum_{j=0}^{2} \chi^j(b) \\ &= \sum_{i=0}^{2} \sum_{j=0}^{2} \left(\sum_{a+b=1} \chi^i(a)\chi^j(b) \right) \\ &= p + J(\chi, \chi) + J(\chi^2, \chi^2) + J(\chi, \chi^2) + J(\chi^2, \chi) \\ &= p + J(\chi, \chi) + J(\overline{\chi}, \overline{\chi}) + 2J(\chi, \chi^{-1}) \\ &= p + J(\chi, \chi) + \overline{J(\chi, \chi)} - 2\chi(-1) \\ &= p - 2 + 2Re\, J(\chi, \chi). \end{aligned}$$

We have shown that $J(\chi, \chi) = a + b\omega$ for some a, $b \in \mathbb{Z}$ with $a \equiv -1$ mod 3 and $b \equiv 0$ mod 3. As in the proof of Corollary 4.19, set $A = 2a - b$ and $B = b/3$, and we

have $4p = A^2 + 27B^2$ and $A \equiv 1 \bmod 3$. Furthermore, we have shown that this A is unique. Now, since $Re\, J(\chi, \chi) = (2a - b)/2$, we have $2Re\, J(\chi, \chi) = 2a - b = A$. The proof is now complete. □

5. Law of Quadratic Reciprocity

In this section, we shall work with congruences in the ring of algebraic integers in $\mathbb{C}$, and also with Gauss and Jacobi sums, to give two proofs of the law of quadratic reciprocity.

Theorem 5.1. *Let p and q be odd rational primes. Then we have*

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

Proof. The first proof uses quadratic Gauss sums:

Let $g = \sum_{t \in F_p} \left(\frac{t}{p}\right)\zeta^t$ and $p* = (-1)^{(p-1)/2}p$. Then we have $g^2 = p*$, by Corollary 4.7. Let $q \neq p$ be another odd rational prime. Then we have

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

which gives

$$g^q \equiv \left(\frac{p*}{q}\right) g \bmod q.$$

We also have

$$g^q = \left(\sum_{t \in F_p} \left(\frac{t}{p}\right)\zeta^t\right)^q \equiv \sum_{t \in F_p} \left(\frac{t}{p}\right)^q \zeta^{qt} = g_q = \left(\frac{q}{p}\right) g \bmod q.$$

Thus, we have

$$\left(\frac{q}{p}\right) g \equiv \left(\frac{p*}{q}\right) g \bmod q.$$

Multiplying both sides of the congruence equation by g, we have

$$\left(\frac{q}{p}\right) p* \equiv \left(\frac{p*}{q}\right) p* \bmod q,$$

which implies

$$\left(\frac{q}{p}\right) \equiv \left(\frac{p*}{q}\right) \bmod q,$$

so

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

The second proof uses Gauss and Jacobi sums:

Let q be an odd rational prime not equal to p, and χ be the Legendre symbol mod p (i.e. $\chi(a) = \left(\frac{a}{p}\right)$. Then χ is a character of order 2 on F_p, and Corollary 4.12 implies

$$g(\chi)^{q+1} = \chi(-1)pJ(\chi, \chi, ..., \chi) = (-1)^{(p-1)/2}pJ(\chi, \chi, ..., \chi),$$

where there are q components in the Jacobi sum. Since $q+1$ is even and $\chi = \overline{\chi}$, we also have

$$\begin{aligned} g(\chi)^{q+1} &= (g(\chi)^2)^{(q+1)/2} = (g(\chi)g(\overline{\chi}))^{(q+1)/2} = (\chi(-1)p)^{(q+1)/2} \\ &= (-1)^{((p-1)/2)((q+1)/2)}p^{(q+1)/2}. \end{aligned}$$

Thus, we have

$$(-1)^{((p-1)/2)((q-1)/2)}p^{(q-1)/2} = J(\chi, \chi, ..., \chi).$$

Now, $J(\chi, \chi, ..., \chi) = \sum_{t_1+t_2+...+t_q=1} \chi(t_1)\chi(t_2)...\chi(t_q)$. If $t = t_1 = t_2 = ... = t_q$, then we have $t = q^{-1}$ and $\chi(t_1)\chi(t_2)...\chi(t_q) = \chi(q^{-1})^q = \chi(q^{-1}) = \chi(q)$. If not all the t_i's are equal, then there are q different q-tuples obtained from $(t_1, t_2, ..., t_q)$ by cyclic permutation, and the corresponding terms $\chi(t_1)\chi(t_2)...\chi(t_q)$ of the sum all have the same value. Thus, we have

$$(-1)^{((p-1)/2)((q-1)/2)}p^{(q-1)/2} \equiv \chi(q) \, mod \, q.$$

Since $p^{(q-1)/2} \equiv \left(\frac{p}{q}\right) \bmod q$ and $\chi(q) = \left(\frac{q}{p}\right)$, we have

$$(-1)^{((p-1)/2)((q-1)/2)} \left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right) \, mod \, q,$$

which gives

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

□

6. Law of Cubic Reciprocity

Set $D = \mathbb{Z}[\omega]$. Let π be a complex prime with $N(\pi) = p \equiv 1 \bmod 3$ for some rational prime p. Since $D/\pi D$ is a finite field with $N(\pi) = p$ elements, we have $D/\pi D \cong F_p$ and we may identify the two fields. This identification allows us to consider the cubic residue character mod π, χ_π, as a cubic character on F_p. Thus, we may work with the Gauss sums $g_a(\chi_\pi)$ and the Jacobi sum $J(\chi_\pi, \chi_\pi)$.

If χ is any cubic character on F_p, we have proved $g(\chi)^3 = pJ(\chi, \chi)$ and $J(\chi, \chi) = a + b\omega$ for some a, $b \in \mathbb{Z}$ with $a \equiv -1 \bmod 3$ and $b \equiv 0 \bmod 3$, which, since we have $J(\chi, \chi)\overline{J(\chi, \chi)} = |J(\chi, \chi)|^2 = p$, implies that $J(\chi, \chi)$ is a primary prime in D of norm p.

To prove the law of cubic reciprocity, we need the following lemma. Let p be a rational prime, and π be a primary prime with $N(\pi) = p \equiv 1 \bmod 3$. Then we have

Lemma 6.1. $J(\chi_\pi, \chi_\pi) = \pi$.

Proof. Let $J(\chi_\pi, \chi_\pi) = \pi'$, where π' is a primary prime in D of norm p. Since $\pi\overline{\pi} = p = \pi'\overline{\pi'}$, we have $\pi \mid \pi'$ or $\pi \mid \overline{\pi'}$. Since all the primes involved are primary, we must have $\pi = \pi'$ or $\pi = \overline{\pi'}$. By the definition of Jacobi sums, we have

$$J(\chi_\pi, \chi_\pi) = \sum_{x \in F_p} \chi_\pi(x)\chi_\pi(1-x) \equiv \sum_{x \in F_p} x^{(p-1)/3}(1-x)^{(p-1)/3} \, mod \, \pi.$$

Now, Proposition 2.9 implies

$$\sum_{x\in F_p} x^{(p-1)/3}(1-x)^{(p-1)/3} = \sum_{k=0}^{(p-1)/3} (-1)^k \binom{(p-1)/3}{k} \left(\sum_{x=1}^{p-1} x^{((p-1)/3)+k}\right) \equiv 0 \, mod \, p.$$

Thus, we have $J(\chi_\pi, \chi_\pi) \equiv 0 \bmod \pi$, i.e. $\pi \mid \pi'$, so $\pi = \pi'$. □

Corollary 6.2. $g(\chi_\pi)^3 = p\pi$.

Proof. $g(\chi_\pi)^3 = pJ(\chi_\pi, \chi_\pi) = p\pi$. □

We are now ready to prove the law of cubic reciprocity.

Theorem 6.3. *Let π_1, $\pi_2 \in D$ be primary primes with $N(\pi_1)$, $N(\pi_2) \neq 3$ and $N(\pi_1) \neq N(\pi_2)$. Then we have $\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$.*

Proof. We have shown that if $q_1 \neq q_2$ are two rational primes congruent to 2 mod 3, then q_1 and q_2 are prime elements in D and we have $\chi_{q_1}(q_2) = \chi_{q_2}(q_1)$ (Corollary 3.30). We shall now consider the case in which we have $\pi_1 = q \equiv 2 \bmod 3$ and $\pi_2 = \pi$ with $N(\pi) = p \equiv 1 \bmod 3$, where p and q are rational primes.

Since $g(\chi_\pi)^3 = p\pi$, we have $g(\chi_\pi)^{q^2-1} = (p\pi)^{(q^2-1)/3} \equiv \chi_q(p\pi) \bmod q$. Since $\chi_q(p) = 1$ (Corollary 3.30), we have

$$g(\chi_\pi)^{q^2} \equiv \chi_q(\pi) g(\chi_\pi) \, mod \, q.$$

On the other hand, we have

$$g(\chi_\pi)^{q^2} = \left(\sum_t \chi_\pi(t)\zeta^t\right)^{q^2} \equiv \sum_t \chi_\pi(t)^{q^2}\zeta^{q^2 t} = \sum_t \chi_\pi(t)\zeta^{q^2 t} = g_{q^2}(\chi_\pi) \, mod \, q,$$

where we have used $q^2 \equiv 1 \bmod 3$ and the fact that χ_π is a cubic character. By Proposition 4.4, we have $g_{q^2}(\chi_\pi) = \chi_\pi(q^{-2}) g(\chi_\pi) = \chi_\pi(q) g(\chi_\pi)$. Combining these results, we have

$$\chi_\pi(q) g(\chi_\pi) \equiv \chi_q(\pi) g(\chi_\pi) \, mod \, q.$$

Multiplying both sides of the congruence equation by $\overline{g(\chi_\pi)}$, we have

$$\chi_\pi(q) p \equiv \chi_q(\pi) p \, mod \, q,$$

where we have used $g(\chi_\pi)\overline{g(\chi_\pi)} = p$. Thus, we have

$$\chi_\pi(q) \equiv \chi_q(\pi) \, mod \, q,$$

which implies

$$\chi_\pi(q) = \chi_q(\pi).$$

It remains to consider the case in which we have two complex primes π_1 and π_2 with $N(\pi_1) = p_1 \equiv 1 \bmod 3$ and $N(\pi_2) = p_2 \equiv 1 \bmod 3$, where p_1 and p_2 are rational primes. Let $\gamma_1 = \overline{\pi_1}$ and $\gamma_2 = \overline{\pi_2}$. Then γ_1 and γ_2 are primary primes, and we have $p_1 = \pi_1\gamma_1$ and $p_2 = \pi_2\gamma_2$.

Since $g(\chi_{\gamma_1})^3 = p_1\gamma_1$, we have $g(\chi_{\gamma_1})^{p_2-1} = (p_1\gamma_1)^{(p_2-1)/3}$, and consequently,

$$g(\chi_{\gamma_1})^{p_2-1} \equiv \chi_{\pi_2}(p_1\gamma_1) \, mod \, \pi_2,$$

or equivalently,

$$g(\chi_{\gamma_1})^{p_2} \equiv \chi_{\pi_2}(p_1\gamma_1) g(\chi_{\gamma_1}) \, mod \, \pi_2,$$

On the other hand, we have

$$g(\chi_{\gamma_1})^{p_2} = \left(\sum_t \chi_{\gamma_1}(t)\zeta^t\right)^{p_2} \equiv \sum_t \chi_{\gamma_1}(t)^{p_2}\zeta^{p_2 t} = \sum_t \chi_{\gamma_1}(t)\zeta^{p_2 t} = g_{p_2}(\chi_{\gamma_1})\, mod\, \pi_2,$$

where we have used $p_2 \equiv 1 \bmod 3$ and the fact that χ_{γ_1} is a cubic character. By Proposition 4.4, we have $g_{p_2}(\chi_{\gamma_1}) = \chi_{\gamma_1}(p_2^{-1})g(\chi_{\gamma_1}) = \chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1})$. Combining these results, we have

$$\chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1}) \equiv \chi_{\pi_2}(p_1\gamma_1)g(\chi_{\gamma_1})\, mod\, \pi_2.$$

Multiplying both sides of the congruence equation by $\overline{g(\chi_{\gamma_1})}$, we have

$$\chi_{\gamma_1}(p_2^2)p_1 \equiv \chi_{\pi_2}(p_1\gamma_1)p_1\, mod\, \pi_2,$$

where we have used $g(\chi_{\gamma_1})\overline{g(\chi_{\gamma_1})} = p_1$. Thus, we have

$$\chi_{\gamma_1}(p_2^2) \equiv \chi_{\pi_2}(p_1\gamma_1)\, mod\, \pi_2,$$

which implies

$$\chi_{\gamma_1}(p_2^2) = \chi_{\pi_2}(p_1\gamma_1).$$

The same reasoning, beginning with $g(\chi_{\pi_2})^3 = p_2\pi_2$, and then raising both sides of the equation to the power $(p_1 - 1)/3$ and taking congruences mod π_1, shows

$$\chi_{\pi_2}(p_1^2) = \chi_{\pi_1}(p_2\pi_2).$$

We also need the relation $\chi_{\gamma_1}(p_2^2) = \chi_{\overline{\pi_1}}(\overline{p_2^2}) = \overline{\chi_{\pi_1}(p_2^2)} = \chi_{\pi_1}(p_2^2)^2 = \chi_{\pi_1}(p_2)$, which follows from Proposition 3.29(e), (f). Since we have

$$\begin{aligned}
\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1) &= \chi_{\pi_1}(\pi_2)\chi_{\gamma_1}(p_2^2) \\
&= \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2) \\
&= \chi_{\pi_1}(p_2\pi_2) \\
&= \chi_{\pi_2}(p_1^2) \\
&= \chi_{\pi_2}(p_1\pi_1\gamma_1) \\
&= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\gamma_1)
\end{aligned}$$

and $\chi_{\pi_2}(p_1\gamma_1) \neq 0$, we have the desired result. □

7. Conclusion

As we can see, the concepts of algebraic integers and of Gauss and Jacobi sums are extremely powerful; indeed, they can be used to solve a wide range of problems in number theory.

Acknowledgments. It is a pleasure to thank my mentor, Daniel Le, for his guidance and support.

References

[1] K. Ireland and M. Rosen. A Classical Introduction to Modern Number Theory. Second Edition. Springer-Verlag New York, Inc. 1972. 1982. 1990.
[2] D. Dummit and R. Foote. Abstract Algebra. Third Edition. John Wiley and Sons, Inc. 2004.
[3] S. Rankin. A finite subgroup of the multiplicative group of a field is cyclic. http://www.math.uwo.ca/~srankin/courses/4123/2011/finite_subgroup_field_cyclic.pdf.