PRIMES OF THE FORM $x^2 + ny^2$

ISAAC CHAN-OSBORN
EULER CIRCLE

Abstract. Fermat created three theorems classifying primes of the form $x^2 + ny^2$ for $n = 1, 2, 3$. We will prove and expand these results using quadratic reciprocity, quadratic forms, and the class group. This paper explores the question and solves it for many values of n.

1. Introduction

A well known theorem categorizes the primes that are $x^2 + y^2$ for integers x and y.

Theorem 1.1. *When p is an odd prime and x and y are integers,*

$$p = x^2 + y^2 \iff p \equiv 1 \bmod 4.$$

The forwards direction is direct by mod 4 considerations, but the backwards direction is more interesting. This was known by Fermat, although its first proof was published by Euler. Fermat also knew that

Theorem 1.2. *When p is an odd prime and x and y are integers,*

$$p = x^2 + 2y^2 \iff p \equiv 1, 3 \bmod 8$$

$$p = x^2 + 3y^2 \iff p \equiv 0, 1 \bmod 3.$$

He also conjectured a similar hypothesis for $x^2 + 5y^2$, claiming that for primes $p, q \equiv 3, 7 \bmod 20$ it is true that

$$pq = x^2 + 5y^2$$

for some x and y.

These results are interesting on their own, but they prompt us to generalize to arbitrary n. This leads to the question

Question 1.3. *For a given n, which primes p can be expressed as $x^2 + ny^2$ for some integers x, y?*

This is a very rich question with a very deep answer.

Theorem 1.4 (Final Result)**.** *Let n be a positive integer. Then there is a polynomial $f_n(x)$ such that for a prime p not dividing n or the discriminant of $f_n(x)$ we have that*

$$p = x^2 + ny^2 \iff \begin{cases} \left(\dfrac{-n}{p}\right) = 1 \text{ and} \\ f_n(x) \equiv 0 \bmod p \text{ has a solution.} \end{cases}$$

Date: June 2025.

We will not prove this theorem, but we will dive into this question and tackle it for some specific n. Our treatment of this question will use Legendre's theorem of quadratic forms, genus theory, quadratic reciprocity and its extensions. We will first show the case $n = 1$, which will provide insight into the result for general n. We will then categorize the p that divide $x^2 + ny^2$ using quadratic reciprocity. Using quadratic forms will enable us to further study $x^2 + ny^2$, and we will solve the "convenient" numbers n. Then we briefly discuss the class group of forms, and this theory will give results such as Fermat's conjecture on $pq = x^2 + 5y^2$. We will conclude studying the rings $\mathbb{Z}[e^{2i\pi/3}]$ and $\mathbb{Z}[i]$, fully solving $n = 27$ and $n = 64$. Note that the case $n = 4$ is trivially equivalent to $n = 1$ since at least one of x, y is even. As such we will ignore it throughout the paper. We will also ignore the case $p = 2$ since it is uninteresting.

2. Fermat, Euler, Descent and Reciprocity

We will begin by proving (1.1). The first known proof of the case when $n = 1$ is attributed to Euler, and we present a modified form of his proof.

The forwards direction is obvious by mod 4, but the backwards direction takes more consideration. There are two steps which combine to imply that

$$p \equiv 1 \bmod 4 \implies p = x^2 + y^2 :$$

- Descent: If $p | x^2 + y^2, \gcd(x, y) = 1$ then $p = x^2 + y^2$ for some x, y.
- Reciprocity: If $p \equiv 1 \bmod 4$ then $p | x^2 + y^2, \gcd(x, y) = 1$.

The descent step uses the ancient identity

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 = (ac - bd)^2 + (ad + bc)^2. \tag{2.1}$$

This means that the product of two sums of squares is a sum of squares. Then, we use the lemma

Lemma 2.1. *If N and q can be written as the sum of relatively prime squares where q is a prime and $q|N$, then N/q is also the sum of two relatively prime squares.*

Proof. Let $N = a^2 + b^2$ for relative prime a, b and $q = x^2 + y^2$ for relatively prime x, y. Then,

$$q | x^2 N - a^2 q = x^2(a^2 + b^2) - a^2(x^2 + y^2) = (xb - ay)(xb + ay).$$

Then, $q | xb - ay$ or $q | xb + ay$. Note that we can change the sign of a freely, so assume that $q | xb - ay$ and $xb - ay = dq$ for an integer d. Then,

$$\begin{aligned} x | xb - dx^2 &= xb - d(x^2 + y^2) + dy^2 \\ &= xb - dq + dy^2 \\ &= ay + dy^2 = (a + dy)y \end{aligned}$$

and because $\gcd(x, y) = 1$ we have that $x | a + dy$. Then, let $a + dy = cx$ so that

$$N = a^2 + b^2 = (cx - dy)^2 + (dx + cy)^2 = (x^2 + y^2)(c^2 + d^2) = q(c^2 + d^2),$$

using (2.1). Note that c and d are relatively prime, proving the lemma. ∎

To finish the descent, let $p | a^2 + b^2$ for some relatively prime a, b. Shift a and b by multiples of p until $|a|, |b| < p/2$. Divide by any common factor so that a and b are relatively prime. Now, we know that $N < p^2/2$ and $\gcd(a, b) = 1$, so we can use (2.1) on a prime divisor q of N. Note that if q is the sum of two squares, then so is N/q. Divide by all such prime factors. Now, if p is not the sum of two squares, take the smallest prime factor q of N. Since $N < p^2/2$, we have that $q < p$. Then, we do the same thing but with q, perpetually getting smaller primes. By descent, this is a contradiction, and p is the sum of two squares.

We can generalize descent using the generalization of (2.1)

$$(a^2 + nb^2)(c^2 + nd^2) = (ac \pm nbd)^2 + n(ad \mp bc)^2. \tag{2.2}$$

While $n = 1, 2,$ and 3 satisfy the property

$$p|x^2 + ny^2, \gcd(x, y) = 1 \implies p = x^2 + ny^2,$$

this unfortunately fails for $n = 5$. Although $7|49 = 2^2 + 5 \cdot 3^2$ we can see that 7 cannot be written as $x^2 + 5y^2$. The reason for this failure is that $|a|, |b| < p$ no longer implies $a^2 + ny^2 < p^2$, and so the smallest prime divisor of N can be greater than p.

The reciprocity step took Euler much more time to find.

Theorem 2.2. *When p is an odd prime then $p \equiv 1 \bmod 4 \implies p|x^2 + y^2, \gcd(x, y) = 1$.*

Proof. Let $p = 4k + 1$, and we can write

$$(x^{2k} - 1)(x^{2k} + 1) \equiv 0 \bmod p$$

when $x \not\equiv 0 \bmod p$ by Fermat's Little Theorem. Whenever $x^{2k} \not\equiv 1 \bmod p$, we must have that $x^{2k} \equiv -1 \bmod p$. Since $x^{2k} - 1$ is a polynomial of degree $2k$, it has at most $2k < p$ distinct roots, and thus there is some x such that $p|x^2 + 1$, as desired. ■

3. Quadratic Reciprocity and the Legendre and Jacobi symbols

We can generalize the reciprocity step using quadratic reciprocity.

Recall the Legendre symbol $\left(\dfrac{a}{p}\right)$, which is defined for a prime p and integer a.

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ if } p|a \\ 1 \text{ if } a \text{ is a quadratic residue } \bmod p \\ -1 \text{ otherwise.} \end{cases}$$

Using this notation, we can find that

Lemma 3.1. *Let p be an odd prime relatively prime to n. Then,*

$$p|x^2 + ny^2, \gcd(x, y) = 1 \iff \left(\frac{-n}{p}\right) = 1$$

where $\left(\dfrac{-n}{p}\right)$ is the Legendre symbol.

Proof. Note that

$$\begin{aligned} &x^2 + ny^2 \equiv 0 \bmod p \\ \iff\ &x^2 \equiv -ny^2 \bmod p \\ \iff\ &\frac{x^2}{y^2} \equiv -n \bmod p \end{aligned}$$

since y is relatively prime to p and thus has an inverse mod p. Then, $p|x^2 + ny^2 \implies \left(\frac{-n}{p}\right) = 1$, and the opposite direction is true because

$$x^2 \equiv -n \bmod p \implies x^2 + n \cdot 1^2 \equiv 0 \bmod p.$$

■

Now, it remains to categorize the primes for which $\left(\frac{-n}{p}\right) = 1$. This is at the heart of quadratic reciprocity, and Euler spent a lot of time studying this. To do this, we first look at special cases of the Legendre symbol. Euler conjectured the following cases of $\left(\frac{n}{p}\right)$ for an odd prime p not dividing n :

Theorem 3.2 (Conjecture of Euler)**.**

$$\left(\frac{3}{p}\right) = 1 \iff p \equiv \pm 1 \bmod 12$$
$$\left(\frac{5}{p}\right) = 1 \iff p \equiv \pm 1, \pm 9 \bmod 20$$
$$\left(\frac{7}{p}\right) = 1 \iff p \equiv \pm 1, \pm 9, \pm 25 \bmod 28.$$

For $n = 3, 5, 7$ its seems that

$$\left(\frac{n}{p}\right) = 1 \iff p \equiv \pm\alpha^2 \bmod 4n$$

where α is an odd integer. Unfortunately, Euler also found that

$$\left(\frac{6}{p}\right) = 1 \iff p \equiv \pm 1, \pm 5 \bmod 24$$
$$\left(\frac{10}{p}\right) = 1 \iff p \equiv \pm 1, \pm 3, \pm 9, \pm 14 \bmod 40$$
$$\left(\frac{14}{p}\right) = 1 \iff p \equiv \pm 1, \pm 5, \pm 9, \pm 11, \pm 13, \pm 25 \bmod 56$$

which are not all squares mod $4n$. However, $3, 5, 7$ are prime while $6, 10, 14$ are composite. As such, one could guess that

Theorem 3.3. *If p and q are distinct odd primes then*

$$\left(\frac{q}{p}\right) = 1 \iff p \equiv \pm\alpha^2 \bmod 4q \textit{ for some odd integer } \alpha.$$

Surprisingly, this is equivalent to the statement of the Law of Quadratic Reciprocity.

Proposition 3.4 (Law of Quadratic Reciprocity)**.** *When p and q are distinct odd primes*

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

Claim 3.5. *When p and q are distinct odd primes the statement of (3.3) is equivalent to (3.4).*

Proof. Let $p^* = (-1)^{\frac{p-1}{2}} p$ so that (3.4) is equivalent to

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

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

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

by the properties of the Legendre Symbol

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

and

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

Then, since $\left(\frac{p^*}{q}\right), \left(\frac{q}{p}\right) \in \{-1, 1\}$ we can restate (3.4) as

$$\left(\frac{p^*}{q}\right) = 1 \iff \left(\frac{q}{p}\right) = 1$$

from which it remains to show that

$$\left(\frac{p^*}{q}\right) = 1 \iff p \equiv \pm\alpha^2 \bmod 4q.$$

This is true because

$$\left(\frac{p^*}{q}\right) = 1 \iff p^* \equiv \alpha^2 \bmod q$$

which is the case when $p \equiv 1 \bmod 4$ and $p \equiv \alpha^2 \bmod q$ or $p \equiv 3 \bmod 4$ and $p \equiv -\alpha^2 \bmod q$. ■

Quadratic reciprocity is well-known and we will not provide a proof of (3.4) here. While this is an important result, the prime case is only a subset of what we want, which is to categorize p for any N. To do this, we use the following lemma

Theorem 3.6. *Let $D \equiv 0, 1 \bmod 4$ be a nonzero integer. There is a unique homomorphism $\chi : (\mathbb{Z}/D\mathbb{Z}) \to \{-1, 1\}$ satisfying*

$$\chi(p) = \left(\frac{D}{p}\right) \text{ for odd primes } p \text{ not dividing } D$$

and

$$\chi(-1) = \begin{cases} 1 \text{ when } D > 0 \\ -1 \text{ when } D < 0 \end{cases}$$

Proof. We now use the Jacobi symbol, an extension of the Legendre symbol. For any integer N and odd integer n we define the Jacobi symbol as

$$\left(\frac{N}{n}\right) = \prod \left(\frac{N}{p_i}\right)^{a_i}$$

where $p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ is the prime factorization of n. We use the properties of the Jacobi symbol

$$M \equiv N \bmod n \implies \left(\frac{N}{n}\right) = \left(\frac{M}{n}\right)$$
$$\left(\frac{M}{n}\right)\left(\frac{N}{n}\right) = \left(\frac{MN}{n}\right)$$
$$\left(\frac{M}{mn}\right) = \left(\frac{M}{m}\right)\left(\frac{M}{n}\right)$$

which are true by definition and similar identities for the Legendre symbol. We will also use the crucial lemma

Lemma 3.7. *When $m = n \bmod D$ where m, n are positive and odd and $D \equiv 0, 1 \bmod 4$*

$$\left(\frac{D}{m}\right) = \left(\frac{D}{n}\right).$$

Proof. The proof uses the supplementary laws and quadratic reciprocity. For more details see [1] (17). ■

This implies that χ gives a well-defined homomorphism $\chi : (\mathbb{Z}/D\mathbb{Z})^* \to \{-1, 1\}$. We also know that there are infinitely many primes in each residue class of $(\mathbb{Z}/D\mathbb{Z})^*$ by Dirichlet's theorem, so this uniquely determines χ. ■

Corollary 3.8. *Now we can say that the following are equivalent when p is an odd prime not dividing an integer n and χ is the given homomorphism $\chi : (\mathbb{Z}/4n\mathbb{Z})^* \to \{-1, 1\}$ for $D = -4n$:*

(i) $p|x^2 + ny^2$ *where* $\gcd(x, y) = 1$.

(ii) $\left(\frac{-n}{p}\right)$*=1.*

(iii) $p \in \ker(\chi) \subseteq (\mathbb{Z}/-4n\mathbb{Z})^*$.

Proof. Follows from (3.6) and (3.1) ■

Now this concludes the reciprocity step, as we have characterized the primes for which $\left(\frac{-n}{p}\right) = 1$,

4. Lagrange's Quadratic forms

We begin the study of quadratic forms, or polynomials of the form $ax^2 + bxy + cy^2$ for integers a, b, c. With genus theory and the theory of reduced forms, we will be able to prove the result for many n.

We call a quadratic form $f(x, y)$ primitive if its coefficients are relatively prime. A quadratic form $f(x, y)$ represents an integer a if $a = f(x, y)$ has an integer solution. We will deal exclusively with primitive forms, as non-primitive forms represent primes trivially. We say that $f(x, y)$ properly represents a if x, y are relatively prime. Now the main question can be restated as: which primes p are represented by $x^2 + ny^2$?

We say that two forms f and g are equivalent when

$$f(x, y) = g(px + qy, rx + sy)$$

where $ps - qr = \pm 1$. Note that this means that the matrix $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ is invertible, so this forms an equivalence relation on quadratic forms. Note that equivalent forms represent the same numbers, and only primitive forms are equivalent to non-primitive forms. We say that two forms are properly equivalent if $ps - qr = 1$ and improperly equivalent if $ps - qr = -1$.

As an example, $ax^2 + bxy + cy^2$ and $ax^2 - bxy + cy^2$ are improperly equivalent by letting $(x, y) \mapsto (x, -y)$. However, we can't immediately say whether they are properly equivalent. We will see that sometimes this is the case, as in $2x^2 \pm 2xy + 3y^2$, but sometimes isn't, as in $3x^2 \pm 2xy + 5y^2$.

We can find a very nice relation between proper equivalence and proper representation

Lemma 4.1. *A form $f(x, y)$ properly represents an integer m if and only if $f(x, y)$ is properly equivalent to a form of the form $mx^2 + bxy + cy^2$.*

Proof. Assume that $f(p, q) = m$ where $\gcd(p, q) = 1$. Then, by Bézout's identity there are integers r, s such that $ps - qr = 1$. Then, $f(px + ry, qx + sy)$ is a quadratic form with x^2 coefficient $f(p, q) = m$, and thus $f(x, y)$ is properly equivalent to a form of the form $mx^2 + bxy + cy^2$. The converse is true, as $mx^2 + bxy + cy^2 = m$ when $(x, y) = (1, 0)$. ■

We say that the discriminant of a form $ax^2 + bxy + cy^2$ as $b^2 - 4ac$. Now, one can show that if the determinant of $f(x, y) = ax^2 + bxy + cy^2$ is D, then the discriminant D' of $g(x, y) = f(px + qy, rx + sy)$ satisfies

$$D' = (ps - qr)^2 D$$

by expansion. Moreover, when two forms are properly equivalent they have the same discriminant. The discriminant is important to the behavior of a form, as

$$4af(x, y) = (2ax + by)^2 - Dy^2.$$

If $D > 0$ then $f(x, y)$ represents both positive and negative integers, and we call it indefinite. If $D \leq 0$, then the form only represents nonnegative or nonpositive integers depending on the sign of a. If $f(x, y)$ represents only nonnegative integers, we call it positive definite, and if it only represents nonpositive integers we call it negative definite.

We also have that $D \equiv b^2 \bmod 4$, and so b is even if and only if $D \equiv 0 \bmod 4$, and odd when $D \equiv 1 \bmod 4$. All of these properties are preserved by equivalence.

We have the following condition for an integer m represented by a form of discriminant D.

Lemma 4.2. *Let $D \equiv 0, 1 \bmod 4$ be an integer and let m be an odd integer relatively prime to D. Then m is properly represented by a primitive form of discriminant D if and only if D is a quadratic residue* mod *m.*

Proof. If $f(x, y)$ properly represents m, we assume by (4.1) that $f(x, y) = mx^2 + bxy + cy^2$ for some b, c. Then, we have that $D = b^2 - 4mc$, which means that $D \equiv b^2 \bmod m$ and D is a quadratic residue mod m.

Now, let $D \equiv b^2 \bmod m$. Then, assume without loss of generality that $D \equiv b \bmod 2$ so that $D^2 \equiv b^2 \bmod 4m$. Then we can say that $D^2 - b^2 = -4mc \implies D^2 = b^2 - 4mc$ for some c, and thus $f(x, y) = mx^2 + bxy + cy^2$ has discriminant D, and it obviously properly represents m. We also know that $f(x, y)$ is primitive since m is relatively prime to D. ■

Corollary 4.3. *When n is an integer and p is an odd prime not dividing n, we have that $\left(\frac{-n}{p}\right) = 1$ if and only if n is properly represented by a form of discriminant $-4n$.*

Proof. This follows from (4.2) and the fact that $\left(\frac{-4n}{p}\right) = \left(\frac{-n}{p}\right)$. ■

Note the similarity to the reciprocity step and (3.1), as $x^2 + ny^2$ is a primitive form of discriminant $-4n$. However, there are too many primitive forms of discriminant $-4n$, so we cannot differentiate between them at this point. An example is $\left(\frac{-3}{13}\right) = 1$ and 13 is represented by the form $13x^2 + 12xy + 3y^2$ of discriminant -12. This doesn't give as much insight about $x^2 + 3y^2$. Now we look only at positive definite forms. We want to restrict our study to only a few simple forms of each discriminant. To do this, we turn to Lagrange's theory of reduced forms.

A primitive quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is reduced if

$$|b| \leq a \leq c \text{ and } b \geq 0 \text{ if } |b| = a \text{ or } a = c.$$

Note that we have $a, c > 0$.

With this, we can prove the following theorem

Theorem 4.4. *Every primitive positive definite form is properly equivalent to a reduced form. Moreover, this form is unique.*

Proof. We first show that every such form is properly equivalent to one satisfying $|b| \leq a \leq c$. To do this, take the form $f(x, y) = ax^2 + bxy + cy^2$ properly equivalent to the given one with $|b|$ as small as possible. If $a < |b|$ then

$$g(x, y) = f(x + my, y) = ax^2 + (2am + b)xy + (c + m^2)y^2$$

is properly equivalent to $f(x, y)$. Then, we can find m such that $|b + 2am| < |b|$, a contradiction. Thus we get that $|b| \leq a$ and by symmetry $|b| \leq c$. Then, if $a > c$ then we substitute $(x, y) \mapsto (-y, x)$ so that $a \geq c$. Now, it remains to show that this form is properly equivalent to a reduced one. It is only not reduced if $b < 0$ and $b = -a$ or $a = c$. Then, we have that $ax^2 - bxy + cy^2$ is reduced. To show that these two are equivalent, consider the substitutions

$$a = -b : (x, y) \mapsto (x + y, y) \quad \text{sends} \quad ax^2 + bxy + cy^2 \text{ to } ax^2 - bxy + cy^2$$
$$a = c : (x, y) \mapsto (-y, x) \quad \text{sends} \quad ax^2 + bxy + ay^2 \text{ to } ax^2 - bxy + ay^2.$$

Now we have shown that every primitive positive definite form is properly equivalent to a reduced form. It remains to show that no two reduced forms can be equivalent, or that this reduced form is unique.

This requires some observations about size. Note that if $f(x, y) = ax^2 + bxy + cy^2$ is reduced, then

$$f(x, y) = ax^2 + bxy + cy^2 \geq (a - |b| + c) \min(x^2, y^2).$$

Note that $f(1,0) = a$ and $f(0,1) = c$. Then, when $xy \neq 0$ we have that $f(x,y) \geq a - |b| + c \geq c \geq a$.

We first prove a simpler case: let $f(x,y)$ be a reduced form with $|b| < a < c$. Then we get the strict inequalities $a < c < f(x,y)$ whenever $xy \neq 0$. This means that the two smallest values that f represents are a and c. We also have that

$$f(x,y) = a \implies (x,y) = (\pm 1, 0)$$
$$f(x,y) = c \implies (x,y) = (0, \pm 1).$$

Then, let $g(x,y) = a'x^2 + b'xy + c'y^2$ be a different reduced form properly equivalent to $f(x,y)$. We have that the two smallest values represented by g are a and c because equivalent forms represent the same values. Then, we have that $a = a'$ and $c = c'$ because $a' < c'$. Then, because f and g have the same discriminant we must have that $b' = -b$. Then we want to show that $ax^2 + bxy + cy^2$ is not properly equivalent to $ax^2 - bxy + cy^2$. Assume for the sake of contradiction that

$$g(x,y) = f(px + qy, rx + sy)$$

where $ps - qr = 1$. We have that $a = g(1,0) = f(p,r)$ and $c = g(0,1) = f(q,s)$. This means that $(p,r) = (\pm 1, 0)$ and $(q,s) = (0, \pm 1)$, which implies that $f(x,y) = g(x,y)$.

We assume that $|b| < a < c$, so this argument fails when $|b| = a$ or $a = c$. A similar argument holds in these cases, and for more details see Scharlau and Opalka (36-38). ■

This solves the previous question of $2x^2 \pm 2xy + 3y^2$ and $3x^2 \pm 2xy + 5y^2$. While $2x^2 + 2xy + 3y^2$ is reduced, it is properly equivalent to $2x^2 - 2xy + 3y^2$ by (4.4), but $3x^2 \pm 2xy + 5y^2$ are both reduced and therefore not properly equivalent.

Now we can make the observation that

$$-D = 4ac - b^2 \geq 4a^2 - b^2 \geq 4a^2 - a^2 = 3a^2,$$

so

$$a \leq \sqrt{\frac{-D}{3}}.$$

This implies that a fixed D gives finitely many a in a reduced form, and therefore finitely many b and finitely many c because $D = b^2 - 4ac$. Thus there are a finite number of reduced forms of a given discriminant, a huge improvement. Now this means that there are finitely many primitive positive definite forms of discriminant D, up to proper equivalence. We let $h(D)$ denote this number. Here are some specific values of $h(D)$:

D	$h(D)$	Reduced Forms of Discriminant D
-4	1	$x^2 + y^2$
-8	1	$x^2 + 2y^2$
-12	1	$x^2 + 3y^2$
-20	2	$x^2 + 5y^2, 2x^2 + 2xy + 3y^2$
-28	1	$x^2 + 7y^2$
-56	4	$x^2 + 14y^2, 2x^2 + 7y^2, 3x^2 \pm 2xy + 5y^2.$

Note that $x^2 + ny^2$ is always a reduced form of discriminant $-4n$. As such, we look to use the theory we've built to attack the problem.

Lemma 4.5. *For a positive integer n and an odd prime p, $\left(\frac{-n}{p}\right) = 1$ if and only if n is represented by one of the $h(-4n)$ reduced forms of discriminant $-4n$.*

Proof. Follows from (4.4) and (4.3). ■

Now we notice that for $n = 1, 2, 3, 7$ it is necessarily true that p being represented by a reduced form of discriminant $-4n$ means that p is represented by x^2+ny^2, because $h(-4n) = 1$. Thus the primes p for which $p = x^2 + ny^2$ are exactly the primes p for which $\left(\frac{-n}{p}\right) = 1$. Using the previous work on reciprocity solves Fermat's Theorems for $n = 1, 2, 3$ completely. We then ask

Question 4.6. *For which positive integers n is $h(-4n)$ equal to 1?*

The answer to this question was conjectured by Gauss as a subset of the Class Number Problem and proven by Landau much later.

Theorem 4.7 (Landau)**.** *The positive integers n for which $h(-4n) = 1$ are $1, 2, 3, 4$, and 7.*

Proof. The main idea is to construct other reduced forms for other n. For more details see [1] (31). Categorizing all negative D for which $h(D) = 1$ is related to Gauss's Class Number Problem and is much more complicated. For further ideas when $h(-4n) > 1$, we turn to genus theory. ■

5. Genus Theory and the Principal Genus

We can now separate quadratic forms by looking at the values they represent mod $4n$. For example, we know that primes p that are $1, 3, 7, 9 \bmod 20$ satisfy $\left(\frac{-5}{p}\right) = 1$ and are represented by $x^2 + 5y^2$ or $2x^2 + 2xy + 3y^2$ by (4.3) However, one can show by computation that $p = x^2 + 5y^2 \implies p \equiv 1, 9 \bmod 20$ and $p = 2x^2 + 2xy + 3y^2 \implies p \equiv 3, 7 \bmod 20$ because these two forms represent different values. Thus, the primes that are $x^2 + 5y^2$ are those that are $1, 9 \bmod 20$.

The idea is that we can say that two forms are in the same genus if they represent the same values in $(\mathbb{Z}/4n\mathbb{Z})^*$. Note that equivalent forms lie in the same genus, and thus we can think of each genus being composed of equivalence classes.

We begin by defining the principal form of a negative discriminant D as

$$x^2 - \frac{D}{4}y^2 \quad \text{if} \quad D \equiv 0 \bmod 4$$
$$x^2 + xy + \frac{1-D}{4} \quad \text{if} \quad D \equiv 1 \bmod 4.$$

For $D = -4n$, this is simply $x^2 + ny^2$.

In fact, one can describe the values represented by the principal form as follows:

Theorem 5.1. *Let $D \equiv 0, 1 \bmod 4$ be a negative integer and let χ be the function described in (3.6). Then:*

(i) The values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by the principal genus form a subgroup $H \subseteq \ker(\chi)$.
(ii) The values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by a form $f(x, y)$ of discriminant D form a coset of H in $\ker(\chi)$.

Proof. First we show that if $m \in (\mathbb{Z}/D\mathbb{Z})^*$ is represented by the principal form $x^2 + ny^2$ then it lies in the kernel of χ. Let m be odd. To do this, note that $m = b^2m'$ where m' is properly represented by $x^2 + ny^2$. Then, we have that D is a quadratic residue mod m', so $D = x^2 + km'$ for some x, k. Then,

$$\chi(m) = \left(\frac{D}{m}\right) = \left(\frac{D}{b^2m'}\right) = \left(\frac{D}{m'}\right) = \left(\frac{x^2 - km'}{m'}\right) = 1,$$

as desired. When m is even, the proof is more complicated, and more details can be found in [1] (45).

Then, it follows by (2.2) that H is closed under multiplication when $D \equiv 0 \bmod 4$. To show that H is a subgroup and that the represented values of any form are a coset of H takes more work, and can be found in [1] (35). ■

We can actually extend this to show that

Theorem 5.2. *Let $D \equiv 0, 1 \bmod 4$ be negative and let H be defined as in (5.1) and H' be a coset of H. When p is an odd prime not dividing D then $p \in H'$ if and only if p is represented by a reduced form in the genus of H', where we define the genus of H' as the genus of forms that represents H'.*

This is a powerful result and the main result of our study of genus theory so far. Using this, we can show that the principal genus, or the genus containing the principal form satisfies

Corollary 5.3. *Let n be a positive integer and p an odd prime not dividing n. Then p can be represented by a reduced form in the principal genus if and only if*

$$p \equiv b^2 \text{ or } b^2 + n \bmod 4n$$

for some integer b.

This follows from the fact that $x^2 + ny^2$ represents x^2 or $x^2 + n$ depending on the sign of y. The best case is when the principal genus consists of only one class, this means that (5.3) completely solves the problem. This happens when $n = 5$, as the principal genus only has one form. For $n = 6, 10, 13, 15, 21$ we get the similar results

$$\begin{aligned}
p = x^2 + 6y^2 &\iff p \equiv 1, 7 \bmod 24 \\
p = x^2 + 10y^2 &\iff p \equiv 1, 9, 11, 19 \bmod 40 \\
p = x^2 + 13y^2 &\iff p \equiv 1, 9, 17, 25, 29, 49 \bmod 52 \\
p = x^2 + 15y^2 &\iff p \equiv 1, 19, 31, 49 \bmod 60 \\
p = x^2 + 21y^2 &\iff p \equiv 1, 25, 37 \bmod 84.
\end{aligned}$$

This theory also gives insight into Fermat's conjecture and Lagrange's theorem about pq mentioned previously.

Proposition 5.4 (Lagrange)**.** *When p, q are primes congruent to $3, 7 \bmod 20$, then $pq = x^2 + 5y^2$ for some x, y.*

Since any $p \equiv 3, 7 \bmod 20$ can be represented as $2x^2 + 2xy + 3y^2$, it simply remains to show that the product of two numbers of the form $2x^2 + 2xy + 3y^2$ is of the form $x^2 + 5y^2$. This can be shown by the identity

$$(2x^2 + 2xy + 3y^2)(2w^2 + 2wz + 3z^2) = (2xz + xw + yz + 3yw)^2 + 5(xw - yz)^2.$$

Several other theorems conjectured by Fermat and Euler can be shown in a similar manner.

Legendre was motivated to generalize the previous identity, which resulted in his theory of composition.

We can say that for two forms $f(x, y)$ and $g(x, y)$ with discriminant D that the form $F(x, y)$ of discriminant D is their composition if

$$f(x, y)g(w, z) = F(B_1(x, y, w, z), B_2(x, y, w, z))$$

where B_1, B_2 are bilinear forms of the form

$$B_i(x, y, w, z) = a_i xw + b_i xz + c_i yw + d_i yz.$$

Thus $x^2 + 5y^2$ is the composition of $2x^2 + 2xy + 3y^2$ and itself. One important property of composition is that if $f(x, y)$ represents m and $g(x, y)$ represents m' then their composition represents mm'. Legendre showed that any two forms of the same discriminant can be composed, and moreover there are exactly four forms that are their composition.

Although Legendre continued to work with this theory of composition, there are problems with this approach. The primary issue is that composition is multivalued, and we need to somehow uniformly define composition in a way that preserves proper equivalence.

6. Dirichlet Composition, Class Group, and Convenient Numbers

Gauss and Dirichlet both took approaches to fix this issue. We will focus on Dirichlet's work on making composition consistent.

Lemma 6.1. *Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ have the same discriminant D and assume that $\gcd\left(a, a', \frac{b+b'}{2}\right) = 1$. Note that $D \equiv b^2 \equiv b'^2 \bmod 4$ and thus b and b' have the same parity. There is a unique integer $B \bmod 2aa'$ such that*

$$B \equiv b \bmod 2a$$

$$B \equiv b' \bmod 2a'$$

$$B^2 \equiv D \bmod 4aa'.$$

Proof. See [1] (48) for details. ■

Dirichlet's definition of composition uses $f(x, y), g(x, y), D$ as above. Then if $f(x, y)$ and $g(x, y)$ are primitive positive definite forms then their Dirichlet composition is

$$F(x, y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2$$

where B is from (6.1). One can show that this is a composition as defined previously, and a proof can be found at [1]. It is also true that this Dirichlet composition is primitive.

We can now introduce the class group.

Theorem 6.2. *Let $D \equiv 0, 1 \bmod 4$ be negative and let $C(D)$ be the set of classes of properly equivalent primitive reduced positive definite forms of discriminant D. Then, $C(D)$ is an abelian group with order $h(-D)$ and binary operation Dirichlet composition so that the identity is the principal class and the inverse of $ax^2 + bxy + cy^2$ is the class with $ax^2 - bxy + cy^2$. We call this the class group of D.*

From this many properties follow, and they are listed in more detail in [1] (50). Together, we can come back to our discussion of $x^2 + ny^2$ and use them to prove that

Theorem 6.3. *For a positive integer n the following are equivalent:*

(i) Every genus of forms of discriminant $-4n$ has exactly one class.
(ii) Every reduced form $ax^2 + bxy + cy^2$ of discriminant $-4n$ has $a = c, a = b,$ or $b = 0$.
(iii) Two forms with discriminant $-4n$ are properly equivalent if they are equivalent.
(iv) The class group $C(-4n)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$ for some integer m.
(v) The class number $h(-4n) = 2^{\mu-1}$ where μ is defined in terms of the number of odd prime factors of n and $n \bmod 4$.

This is a combination of genera, composition, the class group, and everything we've done with quadratic forms so far. It makes sense to ask for which n this is true. Gauss found 65 numbers satisfying this property. They arose to him not because of $p = x^2 + ny^2$ but because of Euler's definition of a convenient number.

We can define Euler's notion of a convenient number as follows:

Definition 6.4. A convenient number is one such that for any odd number m relatively prime to n, if the equation $m = x^2 + ny^2$ only has one solution up to sign of x, y, then m is prime.

These numbers were helpful to Euler because they allowed him to find large primes. For example, 1848 is convenient and Euler found that

$$197^2 + 1848 \cdot 100^2 = 185,818,809$$

is a prime, which is impressive for the tools of Euler's time.

Gauss connected the convenient numbers and those satisfying (6.3) by observing that

Theorem 6.5. *Let n be a positive integer. Then, n is convenient if and only if every genus of forms with discriminant $-4n$ consists of only one class.*

These convenient numbers are indeed convenient, as they are fully solvable by (5.3). Unfortunately, genus theory gives great help for the 65 known convenient numbers, but it is also known that there are at most 66 convenient numbers. Of the other cases, sometimes it partially helps but sometimes it does not help at all. For example, $n = 27$ has all three reduced forms lying in the same genus, while $n = 14$ separates them partially.

To fully explore general n requires much more theory and can be found in [1] in Cox's further discussion of class field theory. We will now turn to the two concrete cases $n = 27$ and $n = 64$, and will study them using the Eisenstein and Gaussian integers.

7. Cubic Reciprocity and $x^2 + 27y^2$

We will turn towards the case $n = 27$ and study cubic reciprocity in the ring of Eisenstein integers $\mathbb{Z}[\omega]$ where

$$\omega = \frac{-1+\sqrt{3}}{2} = e^{\frac{2i\pi}{3}}.$$

Some useful properties of ω are that $\overline{\omega} = \omega^2 = -1 - \omega$ and

$$\overline{a + b\omega} = a + b\omega^2 = a - b - b\omega$$

where $\overline{a + b\omega}$ denotes complex conjugation. We define the norm function

$$N(a + b\omega) = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2.$$

We also have that for Eisenstein integers $\alpha = a + b\omega, \beta = c + d\omega$ the norm function is multiplicative, or

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

This is direct by expansion, as

$$\begin{aligned} N(\alpha\beta) &= N(ac - bd + (bc + ad - bd)\omega) \\ &= (ac - bd)^2 - (ac - bd)(bc + ad - bd) + (bc + ad - bd)^2 \\ &= (a^2 - ab + b^2)(c^2 - cd + d^2) \\ &= N(\alpha)N(\beta), \end{aligned}$$

as desired.

Claim 7.1. *We have that for Eisenstein Integers α, β where $\beta \neq 0$ there are Eisenstein Integers γ, δ such that*

$$\alpha = \gamma\beta + \delta, N(\delta) < N(\beta).$$

Proof. Extend the norm function $N(\alpha)$ to $\mathbb{Q}(\omega)$ so that it is still multiplicative. Then,

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{\alpha\overline{\beta}}{N(\beta)} \in \mathbb{Q}(\omega)$$

so that $\frac{\alpha}{\beta} = r + s\omega$ with $r, s \in \mathbb{Q}$. Then, let r_1, s_1 be integers defined as $r_1 = \lfloor r + \frac{1}{2} \rfloor$ and $s_1 = \lfloor s + \frac{1}{2} \rfloor$ so that $|r - r_1| \leq \frac{1}{2}$ and $|s - s_1| \leq \frac{1}{2}$. We claim that it suffices to choose $\gamma = r_1 + s_1\omega$. Then, $\delta = \alpha - \gamma\beta$. Then,

$$N(\delta) < N(\beta) \iff N(\delta/\beta) < 1,$$

but $\delta/\beta = (r - r_1) + (s - s_1)\omega$, which has norm

$$(r - r_1)^2 + (s - s_1)^2 - (r - r_1)(s - s_1) < 1$$

because $|r - r_1| \leq \frac{1}{2}$ and $|s - s_1| \leq \frac{1}{2}$. ■

This means that $\mathbb{Z}[\omega]$ is a Euclidean domain. Some properties follow from this:

Corollary 7.2. *We find that $\mathbb{Z}[\omega]$ is a PID (principal ideal domain) and a UFD (universal factorization domain).*

Proof. We can show that every Euclidean domain is a PID. We define a PID as a domain such that every ideal is principal, or formed by the multiples of some element of the domain. Now, let I be an ideal of Euclidean domain D, and let α be a nonzero element of minimal norm in I. Then, for any element $\gamma \in I$ we have that $\gamma = \alpha\beta + \delta$ for some β, δ such that $N(\delta) < N(\alpha)$. This means that $\delta = 0$ by minimality, and thus $\alpha|\gamma$ for all elements $\gamma \in I$. It similarly follows that $\alpha|\gamma \implies \gamma \in I$.

A PID has some useful properties.

Corollary 7.3 (Ascending Chain Condition). *If there is no infinite chain of ideals in D*

$$I_1 \subsetneq I_2 \subsetneq I_3 \cdots$$

such that each properly contains the previous then D satisfies the ascending chain condition. Every PID satisfies the ascending chain condition.

Proof. Assume that there is an infinite chain of ideals

$$I_1 \subsetneq I_2 \subsetneq I_3 \cdots .$$

Then, let $I = \cup_{n=1}^{\infty} I_n$. It is easy to show that I is a subring of D; furthermore I is an ideal of D. This means that I is generated by an element α of D. Then there is some n such that $\alpha \in I_n$, and it holds that for all $k \geq n$ we have that $I_k = I$ because I_k must be the ideal generated by α. ■

Proposition 7.4. *The following are equivalent for nonzero $\alpha \in D$ when D is a PID*

1. *α is irreducible.*
2. *α is prime (a nonunit element α is prime if $\alpha | \beta\gamma \implies \alpha | \beta$ or $\alpha | \gamma$).*
3. *αD is a prime ideal (an ideal I of D is prime if $\beta\gamma \in I \implies \beta \in I$ or $\gamma \in I$).*
4. *αD is a maximal ideal (an ideal I of D is maximal if I is not a subset of any ideal in D besides D).*

Proof. It is obvious that (2) $\iff$ (3). Then, assume that α is irreducible in D and that $\langle \alpha \rangle$ is not maximal, or

$$\langle \alpha \rangle \subsetneq \langle \beta \rangle \subsetneq D$$

for some $\beta \in D$ with $\beta \neq \alpha$. Then,

$$\alpha \in \langle \beta \rangle \implies \beta | \alpha,$$

so β is a unit. This means that $\langle \beta \rangle = D$, a contradiction. Then, to show that (4) $\implies$ (1), assume that $\langle \alpha \rangle$ is maximal in D and $\alpha = \beta\gamma$ when β and γ aren't units. Then,

$$\langle \alpha \rangle \subsetneq \langle \beta \rangle \neq D,$$

so we can conclude that $\langle \alpha \rangle$ is maximal if and only if α is irreducible.

Then, we need to show that α being irreducible is equivalent to α being prime. To do this, let $\alpha | \beta\gamma$ where α is irreducible. Then, $\beta\gamma = \alpha\delta$ for some δ. Assume that $\alpha \nmid \beta$ Then, take the smallest ideal containing $\langle \alpha \rangle$ and $\langle \beta \rangle$. Because $\langle \alpha \rangle$ is maximal, this is D, and therefore contains 1. This means that $1 = \alpha x + \beta y$ for some x, y. Multiply both sides by γ so that $\gamma = \alpha\gamma x + \alpha y$, so $\alpha | \gamma$. Thus irreducibles are prime. To show that primes are irreducible, assume that α is prime and reducible. Then, $\alpha = \gamma\beta$ where γ and β aren't units. Assume that $\alpha | \gamma$. Then, $\gamma = \delta\alpha$ and then $\alpha = \alpha\delta\beta$, so β is a unit, a contradiction. Thus, primes are irreducible. ■

Now, to define a UFD we first define units, associates, and irreducibles.

1. A unit of D is an element of D with an inverse in D.
2. An associate β of $\alpha \in D$ is a number such that $\beta = \gamma\alpha$ where γ is a unit of D.
3. A nonunit α of D is irreducible if $\alpha = \beta\gamma$ for $\beta, \gamma \in D$ implies that β or γ is a unit.

A domain D is a UFD if every nonzero nonunit α can be written as a product of irreducibles that is unique up to ordering and associates. It is actually true that a PID is a UFD, but we do not need this fact.

To show that $\mathbb{Z}[\omega]$ is a UFD, note by strong induction on norm that every nonunit nonzero element of D can be written as the product of irreducibles. Then, assume that an element α can be written as a product of irreducibles as

$$\alpha = \beta_1\beta_2 \cdots \beta_n = \gamma_1\gamma_2 \cdots \gamma_k$$

where $k \geq n$. Then, since every irreducible is prime we have that $\beta_1 | \gamma_i$ for some i, and thus $\beta_1 = \gamma_i u_1$ where u_1 is a unit. Divide by β_1, β_2 until we get that

$$1 = u_1 u_2 \cdots u_n \gamma_{n+1} \gamma_{n+2} \cdots \gamma_k.$$

Now we can see that there must be 0 remaining factors γ_i, and so this product of irreducibles is unique up to ordering and associates. Thus $\mathbb{Z}[\omega]$ is a UFD. ■

Now it makes sense to categorize the elements of $\mathbb{Z}[\omega]$ that are units and primes.

Claim 7.5. *It holds that*

(i) An Eisenstein integer α is a unit if and only if $N(\alpha) = 1$.
(ii) The units in $\mathbb{Z}[\omega]$ are $\pm 1, \pm\omega, \pm\omega^2$.

Proof. Note that if α is a unit then α is invertible and so there is an Eisenstein integer β such that $\alpha\beta = 1 \implies N(\alpha)N(\beta) = 1$. Since $N(\alpha)$ is a positive integer, $N(\alpha) = 1$. Then, assume $N(\alpha) = 1$. Then,

$$\frac{1}{\alpha} = \frac{\overline{\alpha}}{N(a)} = \overline{\alpha} \in \mathbb{Z}[\omega],$$

as desired.

Note that $\pm 1, \pm\omega, \pm\omega^2$ all have norm 1. Letting $\alpha = a + bi$ we have that

$$N(\alpha) = a^2 - ab + b^2 = 1.$$

Now, $a^2 - ab + b^2$ is between $(a-b)^2$ and $(a+b)^2$, so one of them is 0 or 1. If $(a \pm b)^2 = 0$ then $a = \pm b$. Then, $2a^2 \pm a^2 = 1 \implies (a, b) = (\pm 1, \mp 1)$ and we get $1 - \omega = \omega^2$ and $\omega - 1 = -\omega^2$. If $(a \pm b)^2 = 1$ then $ab = 0$ and we get $\alpha = 1, -1, \omega, -\omega$. Putting this together, the units of $\mathbb{Z}[\omega]$ are

$$\pm 1, \pm\omega, \pm\omega^2.$$

■

Lemma 7.6. *If $\alpha \in \mathbb{Z}[\omega]$ and $N(\alpha)$ is prime then α is prime in $\mathbb{Z}[\omega]$.*

Proof. Obvious by (7.5) and the multiplicativity of the norm. ■

Proposition 7.7. *For a prime $p \in \mathbb{Z}$*

(i) If $p = 3$ then $3 = -\omega^2(1-\omega)^2$ and $1 - \omega$ is a prime.
(ii) If $p \equiv 1 \bmod 3$ then $p = \pi\overline{\pi}$ where π and $\overline{\pi}$ are non-associate primes in $\mathbb{Z}[\omega]$.
(iii) If $p \equiv 2 \bmod 3$ then p is a prime in $\mathbb{Z}[\omega]$.

We also have that this covers all primes in $\mathbb{Z}[\omega]$ up to associates.

Proof. We have that $N(1-\omega) = 3$, so $1 - \omega$ is prime, proving (i). Then, if $p \equiv 1 \bmod 3$ then $\left(\frac{-3}{p}\right) = 1$ and thus p can be represented with a reduced form of discriminant -3, or $x^2 + xy + y^2$. This means that $p = a^2 - ab + b^2$ for some a, b. Then,

$$p = (a + b\omega)(a + b\omega^2) = \pi\overline{\pi}$$

where $\pi = a + b\omega$. Now, $N(\pi) = N(\overline{\pi}) = p$, so both are primes. Now to show that they are non-associate, consider

$$\beta = \frac{\pi}{\overline{\pi}} = \frac{a + b\omega}{a + b\omega^2} = \frac{a^2 + b^2\omega^2 + 2ab\omega}{p} = \frac{a^2 - b^2}{p} + \frac{2ab - b^2}{p}\omega.$$

If we want this to be a unit, we need $p|a^2-b^2$ and $p|2ab-b^2$. If $p|b$ then $p|a$ then $p^2|a^2-ab+b^2$, which is impossible. Thus, $p|2a-b$ and $p|a-b$ or $p|a+b$. Either way, $p|a$, a contradiction.

Note that $\alpha\beta = p$ where $p \equiv 2 \bmod 3$ and neither α and β are units in $\mathbb{Z}[\omega]$ implies that $N(\alpha)N(\beta) = N(p) = p^2$. Thus $N(\alpha) = N(\beta) = p$, which is impossible because

$$a^2 - ab + b^2 = (a+b)^2 - 3ab \equiv 0, 1 \bmod 3.$$

Now we show that every Eisenstein prime π is an associate to one of those listed above. Then, $\pi\overline{\pi}$ is an integer and can thus be factored into integer primes. However, each of these integer primes can be factored into Eisenstein primes as above, and because $\mathbb{Z}[\omega]$ is a UFD the result follows. ■

Since $\pi\mathbb{Z}[\omega]$ is maximal when π is a prime, it is well known that $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ is a field.

Theorem 7.8. *When π is an Eisenstein prime, the quotient ring $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ is a finite field with $N(\pi)$ elements. It is also true that $N(\pi) = p$ or $N(\pi) = p^2$ for some integer prime p with*

(i) If $p = 3$ or $p \equiv 1 \bmod 3$ then $N(\pi) = p$ and $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega] \cong \mathbb{Z}/p\mathbb{Z}$
(ii) If $p \equiv 2 \bmod 3$ then $N(\pi) = p^2$ and $\mathbb{Z}/p\mathbb{Z}$ is isomorphic to the unique subfield of order p in $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$

Proof. This follows from the fact that $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ is a finite ring when $\pi \in \mathbb{Z}[\omega]$. ■

We say that $\alpha \equiv \beta \bmod \pi$ whenever $\pi|\alpha - \beta$.

Corollary 7.9 (Analogue of Fermat's Little Theorem)**.** *If $\pi \in \mathbb{Z}[\omega]$ is a prime that doesn't divide $\alpha \in \mathbb{Z}[\omega]$ then*

$$\alpha^{N(\pi)-1} \equiv 1 \bmod \pi.$$

Proof. We know that $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$ is a finite group with $N(\pi)-1$ elements, and the result follows. ■

Now we can define the cubic Legendre symbol $\left(\frac{\alpha}{\pi}\right)_3$. Let π be a prime not dividing 3. Then, because $N(\pi) \equiv 0, 1 \bmod 3$ and (7.7) it is clear that $N(\pi) \equiv 1 \bmod 3$. Then, for any $\alpha \not\equiv 0 \bmod \pi$ we have that $\alpha^{(N(\pi)-1)/3}$ is a solution of

$$x^3 - 1 = (x-1)(x-\omega)(x-\omega^2) \equiv 0 \bmod \pi,$$

so

$$\alpha^{(N(\pi)-1)/3} \equiv 1, \omega, \omega^2 \bmod \pi$$

because $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ is a ring and has no zero divisors. These are distinct modπ because $1-\omega \not\equiv 0 \bmod \pi$. It follows that we can define the cubic Legendre symbol

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{(N(\pi)-1)/3} \equiv 1, \omega, \omega^2 \bmod \pi. \tag{7.1}$$

Akin to quadratic reciprocity, it is easy to see that from (7.1) that

$$\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$$

and $\alpha = \beta \bmod \pi$ implies that

$$\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3.$$

Now because the well known fact that the multiplicative group of any finite field is cyclic, we can see that

$$\begin{aligned}\left(\frac{\alpha}{\pi}\right)_3 = 1 &\iff \alpha^{(N(\pi)-1)/3} \equiv 1 \bmod \pi \\ &\iff x^3 \equiv \alpha \bmod \pi \text{ has a solution in } \mathbb{Z}[\omega].\end{aligned}$$

Now, we have one more definition before we can state the law of cubic reciprocity. A primary prime π in $\mathbb{Z}[\omega]$ is one such that $\pi \equiv \pm 1 \bmod 3$. Note that for any prime π not dividing 3, 2 of its associates are primary.

Theorem 7.10 (Law of Cubic Reciprocity)**.** *Let π and θ be primary primes of unequal norm. Then,*

$$\left(\frac{\theta}{\pi}\right)_3 = \left(\frac{\pi}{\theta}\right)_3.$$

Proof. The proof of this fact involves Jacobi sums and can be found at [2] (115). ■

Note that (7) is the most elegant of the reciprocity laws. The requirement that π is primary is similar to the requirement that $p > 0$ in quadratic reciprocity. Similar to the supplements of quadratic reciprocity, there are supplements to cubic reciprocity for $1-\omega$ and ω. Take a prime π that is $-1 \bmod 3$ and let $\pi = a + b\omega$ where $a = 3m-1$ and $b = 3n$. Then,

$$\begin{aligned}\left(\frac{\omega}{\pi}\right)_3 &= \omega^{m+n} \\ \left(\frac{1-\omega}{\pi}\right)_3 &= \omega^{2m}\end{aligned} \tag{7.2}$$

Proof. The first line of (7.2) is simple to prove, but the second requires more ingenuity and was first proven by Eisenstein. A proof can be found in [2] (136). ■

Cubic reciprocity seems applicable to studying primes of the form $x^2 + 27y^2$, but we want to work in the integers, while the cubic Legendre symbol only applies to Eisenstein integers.

Question 7.11. *For a prime p and integer a when does*

$$x^3 \equiv a \bmod p$$

have a solution?

When $p = 3$ $a^3 \equiv a \bmod p$, so every residue is a cubic residue. When $p \equiv 2 \bmod 3$ we have that $3 \nmid p-1$ and every residue is a cubic residue. However, if $p \equiv 1 \bmod 3$ it isn't as simple. We can write $p = \pi\overline{\pi}$ for an Eisenstein prime π, so by (7.8) we can take the the isomorphism from $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ to $\mathbb{Z}/p\mathbb{Z}$. This means that

$$x^3 \equiv a \bmod p \text{ is solvable in } \mathbb{Z} \iff \left(\frac{a}{\pi}\right)_3 = 1. \tag{7.3}$$

Now we can solve a special case of our equation.

Theorem 7.12. *Let p be a prime. Then $p = x^2 + 27y^2$ has a solution in the integers if and only if $p \equiv 1 \bmod 3$ and 2 is a cubic residue mod p.*

Proof. Assume that $p = x^2 + 27y^2$. Then, $p \equiv 1 \bmod 3$ so we need to show that 2 is a cubic residue mod p. Let $\pi = x + 3\sqrt{-3}y = x + 3(2\omega + 1)y$ since $\sqrt{-3} = 2\omega + 1$ so $p = \pi\overline{\pi}$ and by (7.3)

$$x^3 \equiv 2 \bmod p \text{ is solvable in } \mathbb{Z} \iff \left(\frac{2}{\pi}\right)_3 = 1.$$

However, since $N(2) = 4$ we have that

$$\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3 \equiv \pi \bmod 2$$

by (7) and (7.1). Thus the problem is reduced to showing that $\pi \equiv 1 \bmod 2$. Now, note that

$$\pi \equiv x + 6\omega y + 3y \equiv x + y \bmod 2,$$

which is 1 because x and y have opposite parity.

For the other direction, suppose that p is a prime with $p \equiv 1 \bmod 3$ and 2 is a cubic residue mod$p$. Then we again write $p = \pi\overline{\pi}$ where π is a primary prime. This means that $\pi = a + 3b\omega$ for some a, b. Then,

$$4p = 4\pi\overline{\pi} = 4(a^2 - 3ab + 9b^2) = (2a - 3b)^2 + 27b^2.$$

If b is even, then the problem is solved. Now, we know that 2 is a cubic residue mod$p$. We know from earlier that

$$\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3 \equiv \pi \bmod 2,$$

so $\pi \equiv 1 \bmod 2$. This means that $a + 3b\omega \equiv 1 \bmod 2$ so a is odd and b is even. Thus p can be written as $x^2 + 27y^2$. ■

8. Biquadratic Reciprocity and $x^2 + 64y^2$

Now we move from $\mathbb{Z}[\omega]$ to the Gaussian integers $\mathbb{Z}[i]$ where $i^2 = -1$. Many properties of this ring are the same as in $\mathbb{Z}[\omega]$, and their proofs will be omitted. We use the norm function $N(a + bi) = a^2 + b^2 = (a + bi)(a - bi)$. Similar to before, $\mathbb{Z}[i]$ is a Euclidean domain, a PID, and a UFD. The details are omitted. Just like we did with $\mathbb{Z}[\omega]$, we classify the units and primes in $\mathbb{Z}[i]$.

Proposition 8.1. *When z is a Gaussian integer*

(i) z is a unit if and only if $N(z) = 1$.
(ii) The units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.

The proof is similar to before, and as such we omit it.

Proposition 8.2. *Let p be an integer prime. Then,*

(i) If $p = 2$ then $1 + i$ and $1 - i$ are associate primes and $2 = (1 + i)(1 - i) = -i(1 + i)^2$.
(ii) If $p \equiv 1 \bmod 4$ then there is a Gaussian prime π such that $p = \pi\overline{\pi}$.
(iii) If $p \equiv 3 \bmod 4$ then p is prime in $\mathbb{Z}[i]$.

All primes in $\mathbb{Z}[i]$ are associate to one of those listed above.

Proof. For (ii) note that $p \equiv 1 \bmod 4$ means that $a^2 + b^2 = p$ has a solution. Then, $\pi = a + bi$ has norm $N(\pi) = a^2 + b^2 = p$ and is therefore prime. Similarly $a - bi$ is prime. Now if $\pi\theta = p$ for nonunit π and θ and prime $p \equiv 3 \bmod 4$ then $N(\pi)N(\theta) = p^2$, and both are p which is a contradiction by the case $n = 1$. Showing that every prime is associate to one of those listed above is fairly straightforward. ■

We have the similar analogue to Fermat's Little Theorem. If π is a prime in $\mathbb{Z}[i]$ and doesn't divide $\alpha \in \mathbb{Z}[i]$ then

$$\alpha^{N(\pi)-1} \equiv 1 \bmod \pi.$$

Gaussian integers are well known and often used in many texts, but were actually introduced by Gauss to study biquadratic reciprocity. We define the biquadratic Legendre symbol for a prime π not associate to $1+i$ $\left(\frac{\alpha}{\pi}\right)_4$ as the fourth root of unity satisfying

$$\alpha^{(N(\pi)-1)/4} \equiv \left(\frac{\alpha}{\pi}\right)_4 \bmod \pi.$$

We also have that

$$\left(\frac{\alpha}{\pi}\right)_4 = 1 \iff x^4 \equiv a \bmod \pi \text{ has a solution in } \mathbb{Z}[i].$$

In $\mathbb{Z}[i]$, a prime π is primary if $\pi \equiv 1 \bmod 2+2i$, and every prime not associate to $1+i$ has exactly one associate that is primary.

Theorem 8.3 (Law of Biquadratic reciprocity)**.** *If θ and π are distinct primary primes in $\mathbb{Z}[i]$ then*

$$\left(\frac{\theta}{\pi}\right)_4 = \left(\frac{\pi}{\theta}\right)_4 (-1)^{(N(\pi)-1)(N(\theta)-1)/16}.$$

Proof. Given in [2] (123-127). ■

There are also the supplementary laws for a primary prime $\pi = a + bi$

$$\begin{aligned} \left(\frac{i}{\pi}\right)_4 &= i^{-(a-1)/2} \\ \left(\frac{1+i}{\pi}\right)_4 &= i^{(a-b-1-b^2)/4}. \end{aligned} \tag{8.1}$$

The first line is easy, but the second is more challenging. For a proof, see Ireland and Rosen (311). Now we can prove the case of $n = 64$.

Theorem 8.4. *(i) If $\pi = a + bi$ is a primary prime in $\mathbb{Z}[i]$ then*

$$\left(\frac{2}{\pi}\right)_4 = i^{ab/2}$$

(ii) A prime p can be represented as $x^2 + 64y^2$ if and only if $p \equiv 1 \bmod 4$ and 2 is a biquadratic residue $\bmod p$.

Proof. We can show that $(i) \implies (ii)$. To do this, let $p \equiv 1 \bmod 4$ be a prime. We write $p = \pi\overline{\pi}$ when $\pi = a+bi$ is a primary prime. We must have that a is odd and b is even because π is primary. We know that $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[i]/\pi\mathbb{Z}[i]$ and thus (i) shows that 2 is a biquadratic residue if and only if $8|b$, from which (ii) follows.

To prove (i), we use the supplementary laws (8.1). Then,

$$\left(\frac{2}{\pi}\right)_4 = \left(\frac{i}{\pi}\right)_4^3 \left(\frac{1+i}{\pi}\right)_4^2 = i^{-3(a-1)/2} \cdot i^{(a-b-1-b^2)/2} = i^{-a+1-(b+b^2)/2}.$$

We want to show that $-2a+2-(b+b^2) \equiv ab \bmod 8$. This can be easily verified for a primary prime. Thus, we have proven the case when $n = 64$. ■

9. Acknowledgements

I would like to acknowledge David Cox for his wonderful book *Primes of the Form* x^2+ny^2, which is the source of much of the content in this paper. I would also like to thank Simon Rubenstein-Salzedo and Jacob Swenberg at Euler Circle for their help with this class and my paper.

References

[1] David A. Cox. *Primes of the form* $x^2 + ny^2$*: Fermat, class field theory, and complex multiplication*, volume 34 of *Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts.* Wiley-Interscience, 1989.

[2] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory.* Springer Science+Business Media New York, 1990.