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

SOUNAK BAGCHI

Abstract. In this article, we characterize primes of the form $x^2 + ny^2$ for integers x and y and a fixed integer n. We tackle small cases of n brought about by conjectures of Fermat. We also touch upon Lagrange's theory of quadratic forms, and cover special cases using cubic reciprocity and biquadratic reciprocity. We end off with the main theorem of the paper that allows to answer our guiding question for all positive values of n.

1. Introduction and History

The Central Question. What primes p can be expressed in the form $x^2 + ny^2$ for a fixed integer n, where x and y are integers?

We generally deal with positive integers n when considering this central question. Negative integers n give us the theory of Pell Equations, which is much more well-established.

Euler and Fermat were some of the first mathematicians to truly examine this problem. The case for $n = 1$ is named after Fermat, and his conjectures about the cases $n = 1, 2, 3$ were proven by Euler. The ideas of genus theory and quadratic forms by Lagrange and Legendre were present at the time this problem was being explored. However, it was really Gauss who showed how these ideas could be put to use, along with quadratic reciprocity.

Gauss also used cubic reciprocity on the case $p = x^2 + 27y^2$ and biquadratic reciprocity on the case $p = x^2 + 64y^2$. Gauss also made the connection between these high forms of reciprocity and genus theory, specifically separating forms in the same genus.

Before we start our discussion, it makes sense to look at the main result we are trying to prove, and recognize at each step how we are building up to our main result.

Theorem 1.1. *Let $n > 0$ be an integer. Then there is an irreducible monic polynomial $f_n(x) \in \mathbb{Z}[x]$ of degree $h(-4n)$ such that, if an odd prime p divides neither n nor the discriminant of $f_n(x)$, then*

$$p = x^2 + ny^2 \iff \begin{cases} (-n/p) = 1 \text{ and } f_n(x) \equiv 0 \text{ (mod p)} \\ \text{has an integer solution} \end{cases}$$

And so, we begin!

2. Cases

We first consider the canonical example for $n = 1$ of $p = x^2 + y^2$ where x and y are integers and p is an odd prime. We'll follow Euler's proof, which is the most instructive about tackling primes for other values of n.

Note that the quadratic residues in modulo 4 are $0, 1$. Since p can be written as a sum of two squares, it follows that $p \equiv 0, 1, 2 \pmod 4$. Since p is an odd prime, we must have

$$p = x^2 + y^2 \implies p \equiv 1 \pmod 4. \qquad (1)$$

But is the converse true? It is, albeit much harder to prove. We'll show it in a two-step process.

Theorem 2.1.1. (*Descent.*) If $p \mid a^2 + b^2$ for $\gcd(a, b) = 1$, then p can be written as a sum of two squares.

To prove this, we need a smaller lemma.

Lemma 2.1.2. Suppose that N is a sum of two relatively prime squares, and a prime $q = x^2 + y^2$ divides N. Then N/q can be written as a sum of two relatively prime squares as well.

Proof: Let $N = a^2 + b^2$. Note that

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

is divisible by q since $q \mid N$. Hence, $q \mid xb-ay$ or $q \mid xb+ay$. Assume WLOG that $q \mid xb-ay$, as we can change the sign of a. We then get

$$xb - ay = dq$$

for some integer d.

We now claim that $x \mid a + dy$. Since $\gcd(x, y) = 1$ this is equivalent to proving that

$$x \mid y(a + dy).$$

But note that

$$y(a + dy) = ay + dy^2 = xb - dq + dy^2 = xb - d(x^2 + y^2) + dy^2 = x(b - dx)$$

so $x \mid y(a+dy)$, and thus $x \mid a+dy$. So, set $cx = a+dy$ for some integer c. Then $a = cx-dy$. Now, note that $cxy = xb - dx^2$ and so $b = cy + dx$. This gives us

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

so N/q is a sum of two integer squares. ■

Note that Lemma 2.1.2 is essentially the converse of the identity

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

i.e. the product of two sums of squares is a sum of squares itself.

Now, we have what we need to finish the Descent Step.

Proof of Theorem 2.1.1. Choose p to be an odd prime that divides $N = x^2+y^2$ for some N. Assume that $|x| < \frac{p}{2}$ and $|y| < \frac{p}{2}$; otherwise, they can be changed by multiples of p to fit this range, since $p \mid x^2 + y^2$ if either x, y are changed by a multiple of p. Then, $N < \frac{p^2}{4} + \frac{p^2}{4} = \frac{p^2}{2}$.

Since $p \mid N$, it follows that all other prime divisors of N are less than p, as $\frac{N}{p} < \frac{p}{2}$ and all other prime divisors of N divide $\frac{N}{p}$. Since we shifted x and y, it's not necessarily true that $\gcd(x, y) = 1$, but since $|x|, |y| < \frac{p}{2}$ it follows that $p \nmid \gcd(x, y)$. Thus, we can make the assumption that $\gcd(x, y) = 1$ by dividing both x and y by $\gcd(x, y)$ and taking a new N that is still less than $\frac{p^2}{2}$.

Now, let q be a prime divisor of N not equal to p. If, for all primes q dividing N less than p, q can be written as a sum of squares, then using Lemma 2.1.2 over all primes q gives us that p is a sum of two squares, since p divides into N at most 1 time. Otherwise, if for some prime q dividing N, q is not a sum of two squares, we can repeat the argument for q. Since $q < p$, we get an infinite decreasing sequence of positive primes, which is not possible.

Hence, the Descent Step concludes. ■

Theorem 2.1.3. (*Reciprocity.*) If $p \equiv 1 \pmod 4$, then $p \mid a^2 + b^2$ with $\gcd(a, b) = 1$.

Proof: Write $p = 4k + 1$. Note that, from Fermat's Little Theorem,

$$x^{4k} - 1 \equiv 0 \pmod p \iff (x^{2k} - 1)(x^{2k} + 1) \equiv 0 \pmod p.$$

If $p \nmid x^{2k} - 1$ for some x, then $p \mid x^{2k} + 1$, so p divides a sum of relatively prime squares. Thus, for contradiction's sake, assume $p \mid x^{2k} - 1$ for all x not congruent to 0 mod p. However, $x^{2k} - 1$ over $\mathbb{F}_p$ is a polynomial of degree $2k$, and hence can have at most $2k < p - 1$ roots. So, there exists some (in fact multiple) x with $p \mid x^{2k} + 1$, proving the claim. ■

Combining Theorems 2.1.1 and 2.1.3, along with (1), we get the following theorem:

Theorem 2.1.4. (*Fermat's Two Squares Theorem.*) For an odd prime p, we have

$$p \equiv 1 \ (\text{mod } 4) \iff p = x^2 + y^2 \quad (x, y \in \mathbb{Z}).$$

According to Cox, Euler used a similar method to tackle the cases of $n = 2$ and $n = 3$. He found that

$$\begin{aligned} p \equiv 1, 3 \ (\text{mod } 8) &\iff p = x^2 + 2y^2 \quad (x, y \in \mathbb{Z}) \\ p \equiv 1 \ (\text{mod } 3) \text{ or } p = 3 &\iff p = x^2 + 3y^2 \quad (x, y \in \mathbb{Z}) \end{aligned}$$

In particular, the Descent steps that he used were:

- If $p \mid x^2 + 2y^2, \gcd(x, y) = 1$ then p is of the form $a^2 + 2b^2$ for $a, b \in \mathbb{Z}$
- If $p \mid x^2 + 3y^2, \gcd(x, y) = 1$ then p is of the form $a^2 + 3b^2$ for $a, b \in \mathbb{Z}$

The Reciprocity steps that he used were:

- If $p \equiv 1, 3 \pmod 8$, then $p \mid x^2 + 2y^2, \gcd(x, y) = 1$
- If $p \equiv 1 \pmod 3$, then $p \mid x^2 + 3y^2, \gcd(x, y) = 1$

The natural question to ask is: does this generalize for all n? If it did, this paper would be much shorter. Since this isn't a short paper, we'll show how this doesn't generalize.

Note that the Descent Step for $n = 1$ uses the fact that

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

In fact, this generalizes for all n, through the identity

$$(a^2 + nb^2)(c^2 + nd^2) = (ac + nbd)^2 + n(ad - bc)^2.$$

The problem that arises, however, is that the Descent conjecture itself just isn't true for general n. For example, consider the case for $n = 5$:

$$\text{If } p \mid x^2 + 5y^2, \gcd(x, y) = 1 \text{ then } p \text{ is of the form } a^2 + 5b^2 \text{ for } a, b \in \mathbb{Z}$$

Taking $x = 1$ and $y = 2$, note that $3 \mid 1^2 + 5 \cdot 2^2 = 21$. However, 3 cannot be written in the form of $a^2 + 5b^2$ for integers a, b.

As it turns out, to fix this "Descent" step, we will need more advanced tools, namely Lagrange's Theorem on quadratic forms, which we'll cover later.

For now, let's focus on perfecting the Reciprocity Step. We essentially want a set of residues $a_1, a_2, \ldots$ so that the following statement holds:

$$p \equiv a_1, a_2, \ldots \pmod{n} \iff p \mid x^2 + ny^2, \gcd(x, y) = 1$$

This is rather easily generalizable. Define the standard **Legendre Symbol** $\left(\frac{a}{p}\right)$ to be

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & p \nmid a \text{ and a is a quadratic residue modulo p} \\ -1 & p \nmid a \text{ and a is a quadratic nonresidue modulo p} \end{cases}$$

Now, reciprocity can be restated as follows:

Theorem 2.1.5. For $n > 0$ and odd primes $p \nmid n$, we have

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

Proof: The forward direction is fairly elementary. Note that

$$x^2 + ny^2 \equiv 0 \text{ (mod p)} \iff -n \equiv \frac{x^2}{y^2} \equiv \left(\frac{x}{y}\right)^2 \pmod{p}.$$

This is legal since $y \not\equiv 0$ (mod p), as otherwise $x \equiv 0 \pmod{p}$ and $\gcd(x, y) \neq 1$. So, $-n$ is a square modulo p, hence the forward direction is proved.

For the backwards direction, write

$$-n \equiv a^2 \text{ (mod p)}.$$

Thus, we must find a solution (x, y) in modulo p such that

$$x^2 - a^2y^2 \equiv 0 \text{ (mod p)} \iff (x - ay)(x + ay) \equiv 0 \text{ (mod p)},$$

where $x, y \not\equiv 0$ (mod p). Then, it suffices to fix $x = 1$ and choose y to be the inverse of a modulo p, though many other solutions exist, of course.

Both directions have been proved, hence we're done. ■

It's interesting to note that Euler himself was not so aware of the notion of quadratic residues[1] at the time of his writing, so the argument for Theorem 2.1.5, albeit rather elementary, was difficult for him to find. In fact, it was this general Reciprocity Step that led Euler to find his larger result of **Quadratic Reciprocity**, which he discovered in 1783.

Theorem 2.1.6. For odd primes p and q with $p \neq q$,

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

This can also be restated as

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{If } p \text{ or } q \text{ is 1 mod 4} \\ -1 & \text{otherwise.} \end{cases}$$

Despite not discovering Quadratic Reciprocity explicitly when looking at this problem, Euler made some conjectures on his own relating to this problem, specifically:

$$\left(\frac{-3}{p}\right) \iff p \equiv 1, 7 \text{ (mod 12)}$$

$$\left(\frac{-5}{p}\right) \iff p \equiv 1, 3, 7, 9 \text{ (mod 20)}$$

$$\left(\frac{-7}{p}\right) \iff p \equiv 1, 9, 11, 15, 23, 25 \text{ (mod 28)}$$

In particular, these three cases correspond to the cases $n = 3, 5, 7$ in our problem.

3. Quadratic Forms

Lagrange first introduced the concept of Quadratic Forms in two variables

$$f(x, y) = ax^2 + bxy + cy^2, \quad a, b, c \in \mathbb{Z}$$

Along with quadratic forms, Lagrange introduced discriminants, reduced forms, and equivalence.

As it turns out, Lagrange's Theory on reduced forms gives us a solution for the Descent Step we are looking for. Then, along with the Reciprocity Step, this will give the answer to our central question for some cases n.

[1] Cox gives an amusing timeline detailing the evolution of Euler's terminology between 1744 and 1751 regarding quadratic residues.

3.1. **Introductory Quadratic Forms.** Now, we present some definitions.

Definition 3.1.1. We say that a binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is **primitive** if $\gcd(a, b, c) = 1$.

Note that every binary quadratic form is a multiple of a primitive binary quadratic form, so we will primarily consider primitive binary quadratic forms. Moreover, we will simply refer to quadratic forms in the future without using the word "binary", as we assume all future quadratic forms are in two variables.

Definition 3.1.2. We say that an integer m is **represented** by a quadratic form $f(x, y)$ if there exists $a, b \in \mathbb{Z}$ such that $f(a, b) = m$. Moreover, if a, b exist with $\gcd(a, b) = 1$, we say that m is **properly represented** by $f(x, y)$.

Hence, the central question becomes: what primes are represented by the quadratic form $x^2 + ny^2$, for fixed n?

Defintion 3.1.3. Two quadratic forms $f(x, y)$ and $g(x, y)$ are **equivalent** if there are integers p, q, r, s for which

$$f(x, y) = g(px + qy, rx + sy), \qquad ps - qr = \pm 1.$$

If $ps - qr = 1$, then f and g are properly equivalent, and if $ps - qr = -1$, then f and g are improperly equivalent.

As expected, there is a relationship between proper representation and proper equivalence.

Lemma 3.1.4. A form $f(x, y)$ properly represents an integer m if and only if $f(x, y) = ax^2 + bxy + cy^2$ is properly equivalent to a quadratic form $f(x, y) = mx^2 + b'xy + c'y^2$.

Proof: The reverse direction is simple, by taking $(x, y) = (1, 0)$.

To prove the forwards direction, we perform a bit of algebra. Let $f(p, q) = m$ for $\gcd(p, q) = 1$. From Bezout's, we can choose integers s, r with $ps - qr = 1$. Then, $f(x, y)$ is properly equivalent to $f(px + ry, qx + sy)$.

At the same time, if we consider the coefficient of x^2 in $f(px + ry, qx + sy)$, it is equal to

$$a(p^2) + b(pq) + c(q^2) = ap^2 + bpq + cq^2 = m.$$

Hence, the forward direction is proved as well. ■

Definition 3.1.5. The **discriminant** of a quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is $D = b^2 - 4ac$.

Note that the discriminant of properly equivalent quadratic forms are equal to each other. This can be confirmed manually, and is left as an exercise for the reader.

Moreover, note that the discriminant is always $0, 1 \pmod 4$ since

$$D = b^2 - 4ac \equiv b^2 \pmod 4$$

is a quadratic residue modulo 4.

Lemma 3.1.6. Let $D \equiv 0, 1 \pmod 4$ be an integer and let m be an odd integer relatively prime to D. Then m is properly represented by a primitive form with discriminant D if and only if D is a quadratic residue modulo m.

Proof: We prove the forward direction first. From Lemma 3.1.4, assume that $f(x, y) = mx^2 + bxy + cy^2$, since properly equivalent quadratic forms have the same discriminant. Then, we have $D = b^2 - 4mc$, so

$$D \equiv b^2 - 4mc \equiv b^2 \pmod m,$$

proving the forward direction.

For the backwards direction, suppose that $D \equiv b^2 \pmod m$ for some value of b. Since m is odd, assume D and b have the same parity - otherwise, replace b with $b + m$. Then, since $D \equiv 0, 1 \pmod 4$, it follows that

$$D \equiv b^2 \pmod{4m}.$$

Hence, $D = b^2 - 4mc$ for some value of c, and so the quadratic form $mx^2 + bxy + cy^2$ represents m and has discriminant D.

Moreover, since $\gcd(m, D) = 1$, it follows that $\gcd(m, b, c) = 1$, so this is proper representation by a primitive form, finishing the backwards direction. ■

The main purpose of Lemma 3.1.6 is one of it's corollaries.

Corollary 3.1.7. Let n be an integer and p be an odd prime that does not divide n. Then

$$\left(\frac{-n}{p}\right) \iff p \text{ is represented by a primitive form with discriminant -}4n.$$

Proof. This is a result of Lemma 3.1.6 along with basic properties of the Legendre Symbol, as $\left(\frac{-4n}{p}\right) = \left(\frac{-n}{p}\right)$. Since p being represented by a primitive form with discriminant $-4n$ is equivalent to $\left(-\frac{4n}{p}\right) = 1$, the result follows. ■

In the Descent Step of Euler's plan, he dealt with prime divisors of numbers of the form $x^2 + ny^2$. These primes satisfy $\left(\frac{-n}{p}\right) = 1$, and using Corollary 3.1.7, this means that they are represented by forms that have discriminant $-4n$.

However, the problem is that more than one form can have discriminant $-4n$. If we want our results to be truly meaningful, we want all of these forms to be equivalent to a very simple form, hopefully $x^2 + ny^2$.

We can do this using the next type of quadratic forms:

Definition 3.1.8. A primitive positive definite form $f(x, y) = ax^2 + bxy + cy^2$ (i.e. $f(x, y) > 0$ for all $(x, y) \neq (0, 0)$) is said to be **reduced** if

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

Corollary 3.1.9. The quadratic form $f(x, y) = x^2 + ny^2$ is always reduced.

The main theorem we can arrive it is the following:

Theorem 3.1.10. Every primitive positive definite form is properly equivalent to a unique reduced one.

We'll accept this without proof, as it does not require any advanced techniques[2]. To demonstrate the use of this theorem, consider the primitive positive definite forms $f(x, y) = 3x^2 + 2xy + 5y^2$ and $g(x, y) = 3x^2 - 2xy + 5y^2$. These forms are obviously equivalent since $f(x, y) = g(x, -y)$, and moreover they are both reduced. So, Theorem 3.9 implies that these forms are not properly equivalent.

On the other hand, consider $f(x, y) = 2x^2 + 2xy + 3y^2$ and $g(x, y) = 2x^2 - 2xy + 3y^2$. Note that only $f(x, y) = 2x^2 + 2xy + 3y^2$, since for both f and g, $a = |b|$. Hence, using Theorem 3.1.10, it follows that f and g are properly equivalent to each other.

The point of looking at reduced forms is that, for every reduced form with discriminant D, we have

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

from the inequalities $b^2 \leq a^2$ and $a \leq c$. Hence, we have

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

Hence, fixing a discriminant D, it follows that there are limited choices for a and subsequently limited choices for b through the inequality $|b| \leq a$. In addition to this, since

$$D = b^2 - 4ac,$$

there are also limited choices for c. Thus, for every discriminant D congruent to 0 or 1 modulo 4, there are a finite number of reduced quadratic forms with discriminant D.

In essence, what this gives us is that there a finite number of proper equivalence classes for a fixed discriminant D.

Definition 3.1.11. Let $h(D)$, the class number, denote the number of equivalence classes of primitive positive definite forms with discriminant D, with the equivalence relation being proper equivalence among quadratic forms.

[2] See Cox, Chapter 2.

As we discussed:

Corollary 3.1.12. $h(D)$ counts the number of reduced forms of discriminant D, and is thus finite.

Table 1. Reduced Forms for Certain Discriminants D [1].

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	$x^2 + 14y^2, 2x^2 + 7y^2, 3x^2 \pm 2xy + 5y^2$
-108	3	$x^2 + 27y^2, 4x^2 \pm 2xy + 7y^2$
-256	4	$x^2 + 64y^2, 4x^2 + 4xy + 17y^2, 5x^2 \pm 2xy + 13y^2$

As can be seen in the table above, for the values $n = 1, 2, 3$, the quadratic forms $x^2 + y^2, x^2 + 2y^2, x^2 + 3y^2$ are the only reduced forms with discriminant $-4n$. Hence, by using quadratic reciprocity, we can immediately find when the values $(-1/p), (-2/p), (-3/p)$ are equal to 1, and from there we can determine what primes are represented as $x^2 + ny^2$.

A similar thing occurs for $n = 7$; in fact, we have

$$p = x^2 + 7y^2 \iff p \equiv 1, 9, 11, 15, 23, 25 \pmod{28}$$

for odd primes p.

However, this only works because $h(-4n) = 1$ for the values $n = 1, 2, 3, 7$. This is not always true - for example, $h(-20) = 2$, as we can see in the figure. In fact, as it turns out:

Theorem 3.1.13. If n is a positive integer, then

$$h(-4n) \iff n = 1, 2, 3, 4, \text{ or } 7$$

Note that the case $n = 4$ is essentially the same as $n = 1$, since one of x or y is even (as p is odd).

This theorem is not very relevant for discussion, so we will omit a proof of it[3]. But this goes to show that we need a new strategy, as not all reduced forms with discriminant $-4n$ are unique.

3.2. **Genus Theory.** As we mentioned, we need new ideas to uniquely characterize x^2+ny^2 in the cases where $h(-4n) > 1$. As an example, for $n = 5$, we have

$$p \equiv 1, 3, 7, 9 \pmod{20} \iff \left(\frac{-5}{p}\right) = 1 \iff p = x^2 + 5y^2 \text{ or } p = 2x^2 + 2xy + 3y^2.$$

[3] See Cox, Chapter 2.

We need to find another way to separate these two forms.

This is precisely where genus theory comes into play. Consider our example with $n = 5$ as above. Note that

$$\begin{aligned} x^2 + 5y^2 &\quad \text{represents} \quad 1, 9 \qquad \pmod{20} \\ 2x^2 + 2xy + 3y^2 &\quad \text{represents} \quad 3, 7 \qquad \pmod{20} \end{aligned}$$

Another example is for $n = 14$:

$$\begin{aligned} x^2 + 14y^2, 2x^2 + 7y^2 &\quad \text{represents} \quad 1, 9, 15, 23, 25, 29 \qquad \pmod{56} \\ 3x^2 \pm 2xy + 5y^2 &\quad \text{represents} \quad 3, 5, 13, 19, 27, 45 \qquad \pmod{56} \end{aligned}$$

Together, these two examples illustrate that different reduced quadratic forms represent different residues in modulo D, their discriminant. As a result, it's not hard to see our next definition.

Definition 3.2.1. We say that two primitive positive definite forms, both with discriminant D, are part of the same **genus** if they represent the same values modulo D.

So, for example, in the above case for $D = -56$, $x^2 + 14y^2$ and $2x^2 + 7y^2$ would belong to the same genus, and in total there are two genera.

Now, consider the case $n = 5$ again. Using what we know about genera, we can conclude that

$$\begin{aligned} p = x^2 + 5y^2 &\iff p \equiv 1, 9 \pmod{20} \\ p = 2x^2 + 2xy + 3y^2 &\iff p \equiv 3, 7 \pmod{20} \end{aligned}$$

The top line, indeed, does give a full class of solutions for $n = 5$, as expected.

As we'll see, though, this is still not entirely sufficient since each genus can have more than one class of forms. In fact, it's not known how many such n exist where each genus has one class.

There is one more thing that we should cover, which essentially ties together our results. To understand this, we start with a lemma.

Lemma 3.2.2. Let $D \equiv 0, 1 \pmod 4$ be a nonzero integer. Then, there is a unique homomorphism $\chi : (\mathbb{Z}/D\mathbb{Z}) \to \{\pm 1\}$ such that $\chi([p]) = \left(\frac{D}{p}\right)$ for odd primes p that do not divide D. Further,

$$\chi[-1] = \begin{cases} 1 & \text{when D} > 0 \\ -1 & \text{when D} < 0. \end{cases}$$

We won't prove this here since it only requires familiarity with the Jacobi Symbol. However, χ does play a role in a very useful general theorem:

Theorem 3.2.3. Let $D \equiv 0, 1 \pmod 4$ be a negative integer, and let χ be the same homomorphism as defined in Lemma 3.2.2. Then, for an odd prime p that does not divide D, $[p]$ is in the kernel of χ if and only if p is represented by one of the $h(D)$ reduced forms of discriminant D.

Proof: By definition, note that $[p]$ is in the kernel of χ if and only if

$$\left(\frac{D}{p}\right) = 1.$$

Note from Lemma 3.1.6 that this is equivalent to being represented by a primitive positive definite form of discriminant D, and so we're done by Theorem 3.1.10. ■

What this tells us is that a congruence for a prime modulo D is all that is needed to determine whether a prime can be represented by a reduced form with discriminant D. It is much easier to work with reduced forms, and in fact quadratic reciprocity combined with reduced forms immediately gives us the solutions for $n = 1, 2, 3$.

We will also see in the next section how Theorem 3.2.3 becomes useful.

4. Biquadratic and Cubic Reciprocity

Here we grapple with the special cases of $x^2 + 27y^2$ and $x^2 + 64y^2$, which require the tools of biquadratic reciprocity and cubic reciprocity.

The ring associated with cubic reciprocity is the **Eisenstein Integers**, which are of the form

$$\mathbb{Z}[w] = \{a + b\omega;\ a, b \in \mathbb{Z}\}$$

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

The ring associated with biquadratic reciprocity is the **Gaussian Integers**, which are of the form

$$\mathbb{Z}[i] = \{a + bi;\ a, b \in \mathbb{Z}\}.$$

Of course, both the Gaussian and the Eisenstein Integers are subrings of the complex numbers, $\mathbb{C}$.

4.1. Cubic Reciprocity using $\mathbb{Z}[\omega]$.

First, we start with the norm in the Eisenstein integers. For an Eisenstein Integer $z = a + b\omega$, the norm of z is

$$N(z) = z \cdot \overline{z} = a^2 - ab + b^2,$$

where $\overline{z}$ is the conjugate of z in the complex numbers.

Note that the norm in the Eistenstein Integers is always nonnegative, just as the norm defined in the complex numbers is.

Corollary 4.1.1. The norm in $\mathbb{Z}[\omega]$ is multiplicative.

Proof: For Eisenstein Integers z_1 and z_2, we have

$$N(z_1 z_2) = z_1 z_2(\overline{z_1 z_2}) = z_1 \overline{z_1} z_2 \overline{z_2} = N(z_1)N(z_2).$$

■

Moreover, $\mathbb{Z}[\omega]$ has a "Division Algorithm" similar to the integers, and thus is a Euclidean ring. We can show this using the norm:

Theorem 4.1.2. For $a, b \in \mathbb{Z}[\omega]$, with $\beta \neq 0$, there exist $q, r \in \mathbb{Z}[\omega]$ with

$$a = bq + r \qquad \text{and} \qquad N(r) < N(b).$$

We accept this without proof[4].

As a result of this, via the standard definition, $\mathbb{Z}[\omega]$ is a **Euclidean Ring**.

In fact, as a result of this theorem:

Corollary 4.1.3. $\mathbb{Z}[\omega]$ is a PID (Principal Ideal Domain) and a UFD (Unique Factorization Domain).

Proof: Follows from $\mathbb{Z}[\omega]$ being a Euclidean Ring. ■

Now that we've established the Eisenstein Integers are a PID and a UFD, the next natural question to ask is: what are the units and the primes in $\mathbb{Z}[\omega]$?

Lemma 4.1.4.

- An element $a \in \mathbb{Z}[\omega]$ is a unit if and only if $N(a) = 1$.
- The units in $Z[\omega]$ are $\{\pm 1, \pm\omega, \pm\omega^2\}$.

Proof: These are quite simple to verify. The first follows from the fact that the norm is multiplicative, and the second follows by checking what elements in the Eisenstein Integers are on the unit circle. ■

We also have another corollary to partially describe the primes in $\mathbb{Z}[\omega]$.

Lemma 4.1.5. If $a \in \mathbb{Z}[\omega]$ and $N(a)$ is a prime in $\mathbb{Z}$, then a is prime in $\mathbb{Z}[\omega]$.

[4] See Cox, Chapter 4.

Proof: Suppose that $N(a) = p$ for some prime p, and for the sake of contradiction suppose that $a = xy$ where x and y are non-units. Then, from Lemma 4.1.4, $N(x), N(y) \neq 1$. But we have

$$N(x)N(y) = p$$

from multiplicity of norms. Since p is prime, one of $N(x), N(y)$ is equal to 1, a contradiction as desired. ■

We can also determine all of the integer primes in $\mathbb{Z}[\omega]$:

Theorem 4.1.6. If p is a prime in $\mathbb{Z}$, then:

- If $p = 3$, we have $3 = -\omega^2(1-\omega)^2$ and $1-\omega$ is prime in $\mathbb{Z}[\omega]$.
- If $p \equiv 1 \pmod 3$, there exists a prime $\pi \in \mathbb{Z}[\omega]$ with $\pi\overline{\pi} = p$, where π and $\overline{\pi}$ are non-associate (i.e. $\pi \cdot a \neq \overline{\pi}$ for any unit a).
- If $p \equiv 2 \pmod 3$, then p is also prime in $\mathbb{Z}[\omega]$.

Proof: The first property is a result of Lemma 4.1.5 since $N(1-\omega) = 3$.

For the second property, observe that $(\frac{-3}{p}) = 1$ for $p \equiv 1 \pmod 3$, and so p can be represented by a reduced quadratic form that has discriminant -3, through Theorem 3.2.3. It can be checked that the only reduced quadratic form with discriminant -3 is

$$f(x, y) = x^2 + xy + y^2,$$

so p can be written as $a^2 + ab + b^2$ and hence $ab - ab + b^2$. Then, letting $\pi = a + b\omega$, it follows that $\pi \cdot \overline{\pi} = a^2 - ab + b^2$. Moreover, both π and $\overline{\pi}$ have prime norms (i.e. $p = a^2 - ab + b^2$) and are thus prime themselves, by Lemma 4.1.5.

For the third property, note that the Eisenstein Norm

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

can only be 0 or 1 modulo 3, by casework on the values of a, b modulo 3. Now, FTSOC suppose that $p \equiv 2 \pmod 3$ factors as xy in $\mathbb{Z}[\omega]$. Then,

$$N(x)N(y) = p \equiv 2 \pmod 3.$$

But $N(x)$ and $N(y)$ can only be $0, 1$ in modulo 3, which is clearly impossible, so p is prime in $\mathbb{Z}[\omega]$. ■

In fact, a surprising corollary to this proof is the following:

Corollary 4.1.7. If π is a prime in $\mathbb{Z}[\omega]$ and $\pi \nmid \alpha$ with $\alpha \in \mathbb{Z}[\omega]$, then

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

Proof: Note that $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$ is a finite group that has $N(\pi) - 1$ elements. Hence, the result follows. ■

We will now give the statement of cubic reciprocity[5]. Multiple sources have proved it, and it's proof is not so relevant to the topic at hand itself. Before we display it, we need two more definitions.

Definition 4.1.8. We say that a prime p in $\mathbb{Z}[\omega]$ is **primary** if $p \equiv \pm 1 \pmod 3$.

For example, as we've seen already, all primes that are 2 modulo 3 in $\mathbb{Z}$ are primary primes in $\mathbb{Z}[\omega]$. A useful property of primary primes is that, for any prime π, exactly two of it's six associates $(\pm\pi, \pm\omega\pi, \pm\omega^2\pi)$ are primary. This makes it easy to work with primary primes, as they essentially represent all primes.

Definition 4.1.9. Denote the cubic Legendre Symbol $\left(\frac{a}{\pi}\right)_3$ for $a, \pi \in \mathbb{Z}[\omega]$ with π prime to indicate

$$\left(\frac{a}{\pi}\right)_3 = \begin{cases} 0 & \pi \mid a \\ 1 & \pi \nmid a \text{ and a is a cubic residue modulo } \pi \\ -1 & \pi \nmid a \text{ and a is a noncubic nonresidue modulo } \pi \end{cases}$$

As we can with general quadratic reciprocity, we can relate this to Corollary 4.1.7 through the following relationship:

Corollary 4.1.10. We have

$$a^{(N(\pi)-1)/3} \equiv \left(\frac{a}{\pi}\right)_3 \pmod{\pi}$$

for $a, \pi \in \mathbb{Z}[\omega]$ with π being prime.

Now:

Theorem 4.1.11. (*Cubic Reciprocity.*) For primary primes α and β that do not have norm equal to each other,

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

With cubic reciprocity out of the way, as well as it's underlying mechanisms, we are finally able to prove our general theorem for $n = 27$:

Theorem 4.1.12. Let p be a prime in $\mathbb{Z}$. Then $p = x^2 + 27y^2$ for $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod 3$ and 2 is a cubic residue modulo p.

Proof: First, we consider where $p = x^2 + 27y^2$. Then p is equivalent to 1 modulo 3, hence it suffices to show that 2 is a cubic residue modulo p. Now, let $\pi = x + \sqrt{-27}y = x + 3\sqrt{-3}y$, which is clearly an element of $\mathbb{Z}[\omega]$. Then, note that $p = \pi \cdot \overline{\pi}$. Moreover, $x \not\equiv 0 \pmod 3$ as otherwise p is not prime, so π is a primary prime. Thus, we have

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

[5] As Cox mentions, this is one of the simplest and most beautiful forms of reciprocity. It is much simpler than both quadratic and biquadratic reciprocity.

from Cubic Reciprocity. So, it suffices to show that

$$\left(\frac{\pi}{2}\right)_3 = 1,$$

which is the same as proving $\left(\frac{\pi}{2}\right)_3 \equiv \pi \pmod{2}$ from Corollary 4.1.10. Hence, it suffices to show that $\pi \equiv 1 \pmod{2}$.

Recall that $\pi = x + 3\sqrt{-3}y$, which can also be written as

$$\pi = x + 3y + 6y\omega.$$

So, it follows that $\pi \equiv x + 3y \equiv x + y \pmod{2}$. But for p to be prime, x and y have to be opposite parities, so it follows that $\pi \equiv 1 \pmod{2}$ and we're done.

In the reverse direction, suppose that $p \equiv 1 \pmod{3}$ is a prime and 2 is a cubic residue in modulo p. Then, write $p = \pi\overline{\pi}$ where π is a primary prime in $\mathbb{Z}[\omega]$. So, $\pi = a + 3b\omega$ for integers a, b. Then, note that

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

Note that, if b is even, then we are done. Since 2 is a cubic residue modulo p, this implies that $\pi \equiv 1 \pmod{2}$. Hence, $a + 3b\omega \equiv 1 \pmod{2}$, so a is odd and b is even, giving us what we want as desired. ■

4.2. **Biquadratic Reciprocity.** Most of our tactics for dealing ith $n = 27$ are similar for $n = 64$. We'll generally skim over most of the results rather than go in detail, since the proofs are quite similar.

We'll start off with a theorem similar to Theorem 4.1.6:

Theorem 4.2.1. If p is a prime in $\mathbb{Z}$, then:

- If $p = 2$ then $2 = i^3(1+i)^2$, where $1 + i$ is prime.
- If $p \equiv 1 \pmod{4}$, then there is a prime π so that $p = \pi\overline{\pi}$, where the primes π and $\overline{\pi}$ are not associates in $\mathbb{Z}[i]$.
- If $p \equiv 3 \pmod{4}$ then p remains prime in $\mathbb{Z}[i]$.

The proof is analogous to that of Theorem 4.1.6, so we omit it.

Similar to in cubic reciprocity, we also have our own version of Fermat's Little Theorem:

Corollary 4.2.2. If π is a prime in $\mathbb{Z}[i]$ and $\pi \nmid \alpha$ with $\alpha \in \mathbb{Z}[i]$, then

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

We also define the Legendre Symbol for biquadratic reciprocity as well.

Definition 4.2.3. Denote the quartic Legendre Symbol $\left(\frac{a}{\pi}\right)_4$ for $a, \pi \in \mathbb{Z}[\omega]$ to indicate

$$\left(\frac{a}{\pi}\right)_4 = \begin{cases} 0 & \pi \mid a \\ 1 & \pi \nmid a \text{ and a is a biquadratic residue modulo } \pi \\ -1 & \pi \nmid a \text{ and a is a biquadratic nonresidue modulo } \pi \end{cases}$$

As with quadratic and cubic reciprocity, we have the relation

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

Definition 4.2.4. We say that a prime π is **primary** if $\pi \equiv 1 \bmod (2+2i)$.

We include our statement of biquadratic reciprocity:

Theorem 4.2.5. (*Biquadratic reciprocity.*) For distinct primary primes π and θ in $\mathbb{Z}[i]$, we have

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

Now, we are ready for our final theorem for $n = 64$, which comes in two parts.

Theorem 4.2.6.

- If $\pi = a + bi$ is a primary prime in $\mathbb{Z}[i]$, then

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

- If p is prime, then $p = x^2 + 64y^2$ if and only if $p \equiv 1 \pmod 4$ and 2 is a biquadratic residue modulo p.

Sketch: The 2nd part is analogous to cubic reciprocity, but it turns out that the hard part is arriving at the 2nd part. We will show that the first part of the theorem implies the second.

If $p \equiv 1 \pmod 4$, then we can write $p = \pi\overline{\pi} = a^2 + b^2$, with $\pi = a + bi$ being a primary prime. (Remember - Fermat's Two Squares Theorem!)

Note that a is odd while b is even. Now, the idea is that $\mathbb{Z}/p\mathbb{Z}$ is isomorphic to $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$. This allows us to conclude that 2 is a biquadratic residue modulo p if and only if b is divisible by 8, from which the second part follows.

As for proving the first part, this is rather unrelated to our topic, but Dirichlet found a proof in 1857 using only quadratic reciprocity. ■

This concludes our handling of the special cases $n = 27$ and $n = 64$.

5. Final theorem[6]

Recall the main theorem that we wanted to prove:

Theorem 5.1.1. Let $n > 0$ be an integer. Then there is an irreducible monic polynomial $f_n(x) \in \mathbb{Z}[x]$ of degree $h(-4n)$ such that, if an odd prime p divides neither n nor the discriminant of $f_n(x)$, then

$$p = x^2 + ny^2 \iff \begin{cases} (-n/p) = 1 \text{ and } f_n(x) \equiv 0 \text{ (mod p)} \\ \text{has an integer solution} \end{cases}$$

It is important to note that this is a generalization of another theorem, provable using class field theory:

Theorem 5.1.2. Let $n > 0$ be a squarefree integer not congruent to 3 modulo 4. Then there is an irreducible monic polynomial $f_n(x)$ in $\mathbb{Z}[x]$ of degree $h(-4n)$ such that, if an odd prime p divides neither n nor the discriminant of $f_n(x)$, then

$$p = x^2 + ny^2 \iff \begin{cases} (-n/p) = 1 \text{ and } f_n(x) \equiv 0 \text{ (mod p)} \\ \text{has an integer solution} \end{cases}$$

Furthermore, $f_n(x)$ may be taken to be the minimal polynomial of a real algebraic integer α for which $L = K(\alpha)$ is the Hilbert Class Field of $K = \mathbb{Q}(\sqrt{-n})$.

Proof: See Chapter 5 of Cox for details.

The advantages of Theorem 5.1.1 are, of course, that it is more inclusive. For example, in the cases that Gauss studied with $n = 27, 64$ using cubic and biquadratic reciprocity, Theorem 5.1.1 can be applied whereas Theorem 5.1.2 cannot be.

The main purpose of this section is not to prove the theorem, but to understand the mechanisms behind it. To do this, we will introduce some definitions.

Definition 5.1.3. A number field K is a subfield of the complex numbers $\mathbb{C}$ that has finite degree over the rational numbers, $\mathbb{Q}$. We denote this degree as $[K : \mathbb{Q}]$.

Definition 5.1.4. We define $\mathcal{O}_K$ as the algebraic integers over K, i.e. the set of all $a \in K$ for which a is the root of some monic integer-coefficient polynomial.

We also refer to $\mathcal{O}_K$ as the ring of integers over K.

Now we introduce the topic of field extensions, which make up one the central lemmas that allow us to prove Theorem 5.1.1.

Definition 5.1.5. We say that a field L is a field extension of another field K if K is a subfield of L. We also denote the degree of the field extension as $[L : K]$. If $[L : K]$ is finite,

[6] The goal of this section is to completely resolve the problem for all values of n. This will require some class field theory; see Chapters 5,6,7 of Cox for more elaboration.

this is known as a finite field extension.

It's also important to discuss ideals, in particular prime ideals, which have their own set of special properties that make them interesting to deal with.

Definition 5.1.6. Let I be an ideal of a ring R. We say that I is a **prime ideal** if $ab \in I$ implies that $a \in I$ or $b \in I$, for $a, b \in R$.

Just as in the integers, for any ideal in the ring of integers in a number field K, it can be represented as a unique product of prime ideals, up to rearrangement.

Now we have set the stage for defining ramification. Suppose that I is a prime ideal of the algebraic integers $\mathcal{O}_K$. Then, consider a field extension L of K. Note that $I\mathcal{O}_L$ is an ideal and thus is the product of multiple different prime ideals, say

$$I\mathcal{O}_L = I_0^{e_0} I_1^{e_1} \dots I_j^{e_j}.$$

Then, the **ramification index** of the ideal I in the ideal I_n for some n is e_n (i.e. essentially the multiplicity). Moreover, if we consider the field extension $\mathcal{O}_L/I_n$ for some n, then the **inertial degree** f_n of I in I_n is the degree of this field extension.

We'll also formally define a Galois Extension, which is of interest here but is a hard construct to understand.

Definition 5.1.7. We say a field extension L/K is **normal** if, for every irreducible polynomial in K that has a root in L, the polynomial factors completely into linear factors.

Definition 5.1.8. We say a field extension is **separable** if, for all elements $\alpha \in L$, the minimal polynomial of α has no repeated roots (i.e. is separable).

Definition 5.1.9. A field extension L/K is a **Galois Extension** if it is both normal and separable.

Moreover, for a Galois Extension L/K, an ideal I of K ramifies if the ramification index of I is greater than 1, and is unramified otherwise (i.e. the ramification index is equal to 1).

Definition 5.1.10. Given a number field K, the **Hilbert Class Field** is a Galois Extension L over K so that L is the maximal unramified abelian extension over K. Hence, all unramified extensions over K lie in L.

Example 5.1.11. The Hilbert Class Field of the rationals, $\mathbb{Q}$, is just $\mathbb{Q}$ itself, since $\mathbb{Q}$ is a UFD.

The Hilbert Class Field is an example of a ring class field - in fact, it is the maximum ring class field of $\mathcal{O}_K$ for a ring K. This gives us what we need to understand Theorem 5.1.1.

The actual process for proving this theorem can be found in Chapter 9 of Cox's book, which requires a good understanding of class field theory and a functional understanding of Galois Theory.

6. Acknowledgements

I'd like to thank Dr. Simon Rubinstein-Salzedo and Emma Cardwell for their continual guidance in helping me write this paper. I'd also like to thank Justin Cheong and Siddharth Kothari for giving me suggestions on how to improve this paper.

The majority of this paper is based off of David Cox's excellent book *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication* [1].

7. References

[1] Cox, D.A.. (2013). Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication: Second Edition.