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

ADVAITH MOPURI

1. Abstract

This paper will, assuming only basic knowledge of group theory and number theory, present a proof of the criteria that a prime p must satisfy in order to have a representation in the form $x^2 + ny^2$ for integers x, y. To do so, we will go over quadratic reciprocity, quadratic forms, biquadratic/cubic reciprocity, the Hilbert class field, and basic class field theory.

2. Introduction

It is well known that for $x, y \in \mathbb{Z}$ and an odd prime p,

$$p = x^2 + y^2 \iff p \equiv 1 \bmod 4. \tag{2.1}$$

Is there a similar way that we can classify which primes[1] can be expressed in the form x^2+ny^2?

The groundwork to build such a classification was laid by mathematicians such as Fermat, Euler, Gauss, Lagrange, and Legendre. To begin, Fermat proposed theorems like the one at the beginning of this section, along with the following theorems for $x, y \in \mathbb{Z}$

$$p = x^2 + 2y^2 \iff p \equiv 1, 3 \bmod 8$$
$$p = x^2 + 3y^2 \iff p = 3 \text{ or } p \equiv 1 \bmod 3.$$

Euler was not only able to prove these theorems, but create some more unexpected theorems of his own, for example

$$x^2 + 5y^2 \iff p \equiv 1, 9 \bmod 20.$$

Additionally, Euler also discovered quadratic reciprocity, which is a fundamental part of the main result of this paper. Similary, both Lagrange and Legendre had their fair share of contributions to this topic, and we will explore all of them as we prove the first main result of this paper,

$$p = x^2 + ny^2 \iff \left(\frac{-n}{p}\right) = 1$$
$$\text{and } f_n(x) \equiv 0 \bmod p \text{ has an integer solution}$$

for squarefree $n \not\equiv 3 \bmod 4$, odd p, and a function f_n to be defined later in the text. p must also be such that it does not divide neither n nor the discriminant of f_n.

This is a preliminary result, which can actually be generalized to all values of n using genus theory and class field theory. This generalization will be the culmination of all the topics and proofs covered throughout the paper.

Date: June 2023.

[1]Here we are only considering odd primes p, as they make up the actually interesting parts of this problem

Acknowledgements

I would like to thank Simon Rubinstein-Salzedo and Annika Mauro, both of whom helped me during the writing of this paper.

3. Descent and Reciprocity

3.1. **A Classic Theorem of Fermat.** We begin our discussion of primes $p = x^2 + ny^2$ by considering a well known theorem of Fermat, shown in equation 2.1. This is the most basic nontrivial case of the the theorem which we are trying to prove, as it considers the smallest positive integer value of $n = 1$.

In order to prove this theorem, first note that the statement

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

is easily proven by noting that for any integer a, $a^2 \equiv 0, 1 \bmod 4$. This implies that for integers x, y, we have $x^2 + y^2 \equiv 0, 1, 2 \bmod 4$. But since p is an *odd* prime, $p \not\equiv 0, 2 \bmod 4$ which yields the desired result. So, we have successfully proven one direction of 2.1. However, the real diffculty lies in proving the converse of this theorem.

To do this, Euler used a method employing so-called *descent* and *reciprocity* steps. The goal of the descent step is to show that

$$\text{If } p|x^2 + y^2, \gcd(x, y) = 1, \text{ then } p \text{ can be written as } x^2 + y^2 \text{ for some possibly different } x, y$$

while the goal of the reciprocity step is to show that

$$\text{If } p \equiv 1 \bmod 4, \text{ then } p|x^2 + y^2, \gcd(x, y) = 1.$$

We begin the proof of Fermat's theorem with a lemma that will be aid in proving the descent step.

Lemma 3.1. *Let $N = a^2 + b^2$, with $\gcd(a, b) = 1$. Similarly, let q be a prime divisor of N such that $q = x^2 + y^2$ for x, y such that $\gcd(x, y) = 1$. Then, $\frac{N}{q}$ can also be weritten as the sum of two relatively prime squares.*

Proof. We have

$$\begin{aligned} x^2N - a^2q &= x^2(a^2 + b^2) - a^2(x^2 + y^2) \\ &= x^2b^2 - a^2y^2 = (xb + ay)(xb - ay). \end{aligned}$$

Since $q|N$, we must have that $q|x^2N - a^2q$ and since q is prime, this implies that

$$q|xb + ay \text{ or } q|xb - ay.$$

Now, we can assume that $q|xb - ay$, changing the sign of a if necessary to make this statement true. Thus, we have $xb - ay = dq$ for some integer d. Note that this implies $ay = xb - dq$.

We can now claim the following

Claim 3.2. *x divides $a + dy$*

This can easily be proven by noticing

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

This is clearly divisibly by x, and as x and y are relatively prime, we must have that $x|a+dy$. So, we can set $a + dy$ equal to cx for some integer c, which implies

$$a = cx - dy.$$

Plugging this back into the equation above yields that

$$b = dx + cy.$$

Now, we invoke another well known identity:

$$(x^2 + y^2)(z^2 + w^2) = (xz \pm yw)^2 + (xw \mp yz)^2$$

Using this identity in reverse yields

$$\begin{aligned} N = a^2 + b^2 &= (cx - dy)^2 + (dx + cy)^2 \\ &= (x^2 + y^2)(c^2 + d^2) \\ &= q(c^2 + d^2). \end{aligned}$$

As this is clearly a multiple of q, we have proven the lemma – we have that $\frac{N}{q} = c^2 + d^2$, and since we have $a = cx - dy$, $b = dx + cy$ with $\gcd(a, b) = 1$, we must also have $\gcd(c, d) = 1$. ■

Now, we can actually prove the descent and reciprocity steps.

Proof. To prove the descent step, we consider an odd prime p dividing $N = a^2 + b^2, a, b \in \mathbb{Z}$ such that p is the smallest prime dividing N that cannot be expressed as the sum of squares of 2 integers.

Notice that if multiples of p are added or subtracted from a and b, the fact $p|N$ still remains true. This can be seen simply by expanding $N = (a + mp)^2 + (b + np)^2$ and checking that all terms are multiples of p.

Since p is odd, we can continue adding/subtracting multiples of p to a, b until we have $|a| < \frac{p}{2}$ and $|b| < \frac{p}{2}$. This ensures that $N = a^2 + b^2 < \frac{p^2}{2}$. We can also divide out any common factors of a and b to ensure that $\gcd(a, b) = 1$.

Because N is also a multiple of p, we can use this bounding to show that $\frac{N}{p}$, the product of all prime factors of N other than p, must be less than $\frac{\frac{p^2}{2}}{p} = \frac{p}{2}$, which then implies that all other prime factors of N must be less than p (in fact, they must be less than $\frac{p}{2}$).

Then, due to the assumption that p is the smallest prime divisor of N that cannot be written as the sum of 2 squares, dividing out all prime factors of N that are smaller than p will simply yield another value that can be written as the sum of 2 squares by lemma 3.1.

However, since p is also the larges prime divisor of N, this implies that p can be written as the sum of two squares, a contradiction. This finishes the descent step.

Now, onto the reciprocity step. This step caused Euler a lot more trouble than the descent step in his original proof, but he eventually succeeded, employing the use of the calculus of finite differences. The proof presented here, however, is more modern.

By the assumptions in the reciprocity step, we have that $p \equiv 1 \bmod 4$, meaning that for some $k \in \mathbb{Z}$, $p = 4k + 1$. Thus, by Fermat's Little Theorem, we have

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

for all $x \not\equiv 0 \bmod p$. So, since p is prime, we have that $p|x^{2k} - 1$ or $p|x^{2k} + 1$. If $p \nmid x^{2k} - 1$ for even one value of x, then we have $p|x^{2k} + 1$, so p can be expressed as the sum of 2 relatively prime squares (namely, $(x^k)^2$ and 1^2) and we are done.

Thankfully, it is easy to show that at least one such value of x exists – $x^{2k} - 1$ is a polynomial over the finite field $\mathbb{F}_p$, so it has at most $2k < p - 1$ roots. Thus, there exists at least one nonzero value of $x \in \mathbb{F}_p$ such that $x^{2k} - 1 \not\equiv 0 \bmod p$, and we are finished.

Combining both the descent and the reciprocity step yields the desired conclusion. ■

Though it is quite amazing in and of itself, this proof is only for the case $n = 1$. What about larger values of n? At least for $n = 2, 3$, Euler used a similar descent-reciprocity approach as before. For $n = 2$,

$$\textit{Descent}\text{: If } p|x^2 + 2y^2, \gcd(x, y) = 1, \text{ then } p \text{ is of the form } x^2 + 2y^2 \text{ for some possibly different } x, y$$

$$\textit{Reciprocity}\text{: If } p \equiv 1, 3 \bmod 8, \text{ then } p|x^2 + 2y^2, \gcd(x, y) = 1$$

and for $n = 3$,

$$\textit{Descent}\text{: If } p|x^2 + 3y^2, \gcd(x, y) = 1, \text{ then } p \text{ is of the form } x^2 + 3y^2 \text{ for some possibly different } x, y$$

$$\textit{Reciprocity}\text{: If } p \equiv 1 \bmod 3, \text{ then } p|x^2 + 3y^2, \gcd(x, y) = 1$$

In each case, though, the reciprocity step became increasingly difficult for Euler to prove using the techniques mentioned thus far. To deal with this issue, we need to introduce quadratic/cubic/biquadratic reciprocity.

3.2. **Reciprocity.** It makes sense to continue addressing the problem $p = x^2 + ny^2$ with the descent-reciprocity approach given that it seems to be working decently well up till now (other than the difficulty of proving the reciprocity step, but that will be made easier using the techniques of this section).

3.2.1. *Quadratic Reciprocity.* For integer $n > 0$, the reciprocity step asks for congruence conditions in modular arithmetic that guarantee $p|x^2 + ny^2$. But what kind of conditions do we need?

Notice that in the 3 examples of the reciprocity step that are already provided, all the conditions can be written modulo $4n$. Thus, for any general n, we will also work modulo $4n$, and look for conditions $p \equiv a_1, a_2, \ldots, a_k \bmod 4n$ which imply $p|x^2 + ny^2, \gcd(x, y) = 1$.

In modern terms, these conditions are written in terms of the *Legendre symbol*, commonly denoted as $\left(\frac{a}{p}\right)$. This symbol is defined as follows

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

As always, a quadratic residue modulo p is a number in $\mathbb{Z}/p\mathbb{Z}$ that is congruent to a perfect square.

To see how this definition might be useful in our study of numbers of the form $x^2 + ny^2$, consider the following lemma

Lemma 3.3. *For a nonzero integer n and an odd prime p not dividing n, we have*

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

Proof. First, notice that $p|x^2 + ny^2 \iff x^2 + ny^2 \equiv 0 \bmod p$.

We begin the proof in the left-to-right direction. Note that we must have $y \not\equiv 0 \bmod p$. If this were not the case, then since $\gcd(x, y) = 1$, $x^2 + ny^2 \equiv x^2 \not\equiv 0 \bmod p$, meaning that the necessary condition does not hold. Since p is prime, this relation also implies that p and y are relatively prime, meaning that y has a multiplicative inverse modulo p.

Then, we have

$$\begin{aligned} & x^2 + ny^2 \equiv 0 \bmod p \\ \implies & x^2 + (y^{-1})^2 + n \equiv 0 \bmod p \\ \implies & (xy^{-1})^2 \equiv -n \bmod p \\ \implies & \left(\frac{-n}{p}\right) = -1 \end{aligned}$$

Proving the opposite (right-to-left) direction is just the same as this argument, except in reverse. ∎

Note that this formulation can also be rephrased in terms of *Euler's criterion.*

Lemma 3.4 (Euler's criterion)**.** *Let p be an odd prime and a a positive integer not divisible by p. Then,*

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

The proof of this lemma is also quite straightforward.

Proof. To begin, recall a well-known fact about the linear residues modulo p – exactly half of them are quadratic residues. Now, by Fermat's Little Theorem, we have

$$a^{p-1} \equiv 1 \bmod p$$
$$\implies a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$$

Now, if a is a quadratic residue mod p, then we have $a^2 \equiv x \bmod p$ for some x, which implies

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

However, if a is not a quadratic residue mod p, then we must show that $a^{\frac{p-1}{2}} \equiv -1 \bmod p$. To do this, consider the polynomial $x^{\frac{p-1}{2}} \equiv 1$ over $\mathbb{Z}/p\mathbb{Z}$. This polynomial clearly has at most $\frac{p-1}{2}$ roots, and since there are exactly $\frac{p-1}{2}$ quadratic residues modulo p, the roots of the polynomial must be exactly the set of quadratic residues. So, no non-quadratic residue can satisfy $a^{\frac{p-1}{2}} \equiv 1 \bmod p$, and since $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$, we must have the desired result. ∎

In terms of 3.3, this means that

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

Now, let us prove one final theorem of quadratic reciprocity. Though it is not directly related to lemma 3.3, it is interesting in its own right. We have:

Theorem 3.5. *For distinct odd primes p, q, we have*

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

Proof. The proof of this theorem is trivial by Euler's criterion and the simple fact that $p, q > 1$. ∎

Note that the right hand side of this theorem is only equal to 1 if both $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, and -1 otherwise. This formulation is equivalent to the following statement:

Corollary 3.6. *Let p, q be distinct odd primes. If $p \equiv 1 \bmod 4$ or $q \equiv 1 \bmod 4$, then*

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

Otherwise

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

Proof. The proof of this corollary is trivial by simply noting the exponent of -1 on the right hand side of 3.5. ∎

Using all these ideas, Euler was able to make some new conjectures of his own (though he did not express them in this exact manner and instead used more primitive notation)

$$\left(\frac{-3}{p}\right) \iff p \equiv 1, 7 \bmod 12$$
$$\left(\frac{-5}{p}\right) \iff p \equiv 1, 3, 7, 9 \bmod 28$$
$$\left(\frac{-7}{p}\right) \iff p \equiv 1, 9, 11, 15, 23, 25 \bmod 28$$

These 3 are of interest to us with regards to the problem at hand – they encompass Euler's work on the problems $p = x^2 + 3y^2, p = x^2 + 5y^2$, and $p = x^2 + 7y^2$.

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

These latter 3 conjectures are also interesting in their own right. Every number that appears seems to be of the form $\pm\beta^2$ for some odd β. In fact, it turns out that this observation is in fact equivalent to the statement of quadratic reciprocity in theorem 3.5.

3.2.2. *Eisenstein Integers and Cubic Reciprocity.* Now that we have shown how quadratic reciprocity is useful in the reciprocity step, we turn to higher reciprocity to provide more information in some special cases of n. One such form of higher reciprocity is cubic reciprocity.

In this section, the main theorem that we will aim to prove is

Theorem 3.7. *For prime p, $p = x^2 + 27y^2 \iff \begin{cases} p \equiv 1 \bmod 3, \\ 2 \text{ is a cubic residue modulo } p. \end{cases}$*

To do this, we must first extend our notion of the integers to the ring $\mathbb{Z}[\omega]$, consisting of all numbers of the form $a + b\omega, a, b \in \mathbb{Z}$ where $\omega = e^{\frac{2\pi i}{3}}$.

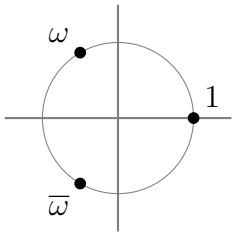

Figure 1. The cube roots of unity

We define the *norm* of a number $\alpha = a + b\omega$ as follows:

Definition 3.8 (Norm)**.** The norm of α is the nonnegative integer

$$N(\alpha) = \alpha\bar{\alpha} = a^2 - ab + b^2.$$

An important property of the norm over Eisenstein integers is that it is always congruent to 1 mod 3.

The norm function is also multiplicative, so we have

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

It also turns out that $\mathbb{Z}[\omega]$ is a Euclidean ring, so a modified version of the Euclidean algorithm will work on numbers over this ring. This property implies that $\mathbb{Z}[\omega]$ is a *principal ideal domain (PID)* and a *unique factorization domain (UFD)*.

To explain what this means, we first need a few definitions.

Definition 3.9 (Basic terminology)**.** Let R be an integral domain (a nonzero commutative ring with the property that the product of any two nonzero elements of R is nonzero). Then,

(1) $\alpha \in R$ is a unit if $\alpha\beta = 1$ for some $\beta \in R$. In other words, α has a multiplicative inverse in R.
(2) $\alpha, \beta \in R$ are associates if α is a unit times β.
(3) A nonunit $\alpha \in R$ is irreducible if $\alpha = \beta\gamma$ in R implies that β or γ is a unit.

Then R is a UFD if every nonunit $\alpha \neq 0$ can be written as a product of irreducibles, and given two such factorizations of α, each irreducible in the first factorization can be matched up in a one-to-one manner with an associate irreducible in the second. In simpler terms, factorization over R is unique up to order and associates.[2]

In fact, being a PID turns out to be a stronger property than simply being a UFD, so along with the previous properties, PIDs have the following one as well.

Lemma 3.10. *For α, β, γ in a PID, the following are equivalent*

(1) *α is irreducible,*
(2) *α is prime ($\alpha|\beta\gamma \implies \alpha|\beta$ or $\alpha|\gamma$).*

Now that we have gotten some basic properties out of the way, we can identify units and primes in $\mathbb{Z}[\omega]$.

The identification of units is aided greatly by the following lemma.

Lemma 3.11 (Norm of a unit)**.** *α is a unit if and only if $N(\alpha) = 1$.*

As it turns out, using 3.11 yields that the units in $\mathbb{Z}[\omega]$ are simply $\{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$.

Next, to identify primes, we make use of yet another lemma.

Lemma 3.12 (Norm of a prime)**.** *If $N(\alpha)$ is a prime in the integers for some $\alpha \in \mathbb{Z}[\omega]$, then α is a prime in $\mathbb{Z}[\omega]$.*

Proof. By property 3.10 of PIDs, it suffices to show that α is irreducible. We proceed by contradiction.

[2]These two sentences are taken from Cox's *Primes of the Form $x^2 + ny^2$*

Assume that α is reducible. In other words, $\alpha = \beta\gamma$ for nonunit $\beta, \gamma \in \mathbb{Z}[\omega]$. Then, due to the multiplicity of norm, we have

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

which is an equation over the integers. But since $N(\alpha)$ is prime, we must have that one of $N(\beta)$ and $N(\gamma)$ is 1. By 3.11, this implies that one of β, γ is a unit – a contradiction. ■

It turns out that by using this lemma, we have the following corollary.

Corollary 3.13. *All primes in* $\mathbb{Z}[\omega]$ *can be divided into* 3 *groups*

(1) $1 - \omega$,
(2) *Primes* $\pi \in \mathbb{Z}$ *with* $\pi \equiv 2 \bmod 3$,
(3) *Primes* $\pi \in \mathbb{Z}[\omega]$ *such that* $p = N(\pi)$ *is a prime equivalent to* 1 *modulo* 3.

Additionally, in the third case, we have that there is a natural isomorphism $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/\pi\mathbb{Z}$.

The Eisenstein primes can be plotted on the complex plane, yielding the graph below.

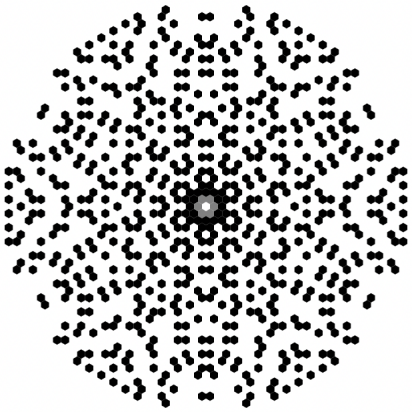

Figure 2. A plot of the Eisenstein primes on the complex plane

Finally, we have one more property of $\mathbb{Z}[\omega]$ that is of importance to us. So far, we have very frequently used the notion of taking numbers "*modulo* p" for $p \in \mathbb{Z}$. It makes sense, therefore, to extend this definition to the Eisenstein integers as well. Note that this extension is only possible because of the fact that $\mathbb{Z}[\omega]$ is a Euclidean ring.

To do so, we will need to introduce the idea of an *ideal* of a ring, as well as the definition of a *quotient ring*.

Definition 3.14 (Ideal)**.** An ideal $\mathfrak{i}$ is a subset of a ring R that is an additive group with the property that for any $x \in R$ and $y \in \mathfrak{i}$, both xy and yx are in $\mathfrak{i}$.

As an example consider the ring $\mathbb{Z}$ and the ideal $6\mathbb{Z}$. Now, we define a quotient ring.

Definition 3.15 (Quotient ring)**.** A quotient ring is a ring that is the quotient of a ring R and its ideal $\mathfrak{i}$, and is denoted as $A/\mathfrak{i}$. In general, a quotient ring is a set of equivalence classes, where x is equivalent to y if and only if $x - y \in \mathfrak{i}$.

We can now define the residues modulo a prime $\pi \in \mathbb{Z}[\omega]$ as a quotient ring

$$\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$$

with $N(\pi)$ elements. It turns out that this quotient ring is also a field. One corollary of this definition is:

Corollary 3.16. *If π is prime in $\mathbb{Z}[\omega]$ and does not divide $\alpha \in \mathbb{Z}[\omega]$, then*

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

Proof. The proof of this corollary is identical to the proof of Fermat's Little Theorem over the integers. We have that $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$ is a finite group with $N(\pi) - 1$ elements, and the desired conclusion follows. ■

Given these properties of the Eisenstein integers, we can finally begin to define cubic reciprocity. We do so using the generalized reciprocity symbol

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

Let π be a prime in $\mathbb{Z}[\omega]$ that does not divide 3. Since we have $3 = -\omega^2(1-\omega^2)$ with $-\omega^2$ being a unit, this can be rephrased as not allowing π to be an associate of $1-\omega$. Here, we ignore associates of $(1-\omega)^2$ since it is not prime. Using the definition of the Eisenstein primes provided in 3.13, it is easy to verify that $3|N(\pi)-1$.

Now, let $\alpha \in \mathbb{Z}[\omega]$ be some value not divisible by π. From 3.16, we have that $\alpha^{\frac{N(\pi)-1}{3}}$ is a root of the polynomial $x^3 \equiv 1 \bmod \pi$. But, we also have

$$\begin{aligned} x^3 &\equiv 1 \bmod \pi \\ \implies x^3 - 1 &\equiv 0 \bmod \pi \\ \implies (x-1)(x-\omega)(x-\omega^2) &\equiv 0 \bmod \pi \\ \implies \alpha^{\frac{N(\pi)-1}{3}} &\equiv 1, \omega, \omega^2 \bmod \pi \end{aligned}$$

Note that none of $1, \omega, \omega^2$ can be congruent modulo π. If this were the case, then it would imply $1 \equiv \omega \bmod \pi$, meaning that $1-\omega$ and π are associates, contrary to assumption. Then, we define the *cubic Legendre symbol* as the unique cube root of unity such that

Definition 3.17 (Cubic Legendre symbol)**.**

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \bmod \pi.$$

From this definition, some easily derived properties of the cubic Legendre symbol are

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

and

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

Now, in order to establish the link between cubic residues and cubic reciprocity, we use another fact of group theory – the multiplicative group of any finite field is cyclic. In particular, this means that $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$ is cyclic, which then implies

Lemma 3.18 (Cubic residues in Eisenstein integers)**.**

$$\left(\frac{\alpha}{\pi}\right)_3 = 1 \iff \alpha^{\frac{N(\pi)-1}{3}} \equiv 1 \bmod \pi \tag{3.1}$$

$$\iff x^3 \equiv \alpha \bmod \pi \text{ has a solution in } \mathbb{Z}[\omega]. \tag{3.2}$$

Let us next try to relate cubic reciprocity to the more natural idea of cubic residues mod p in $\mathbb{Z}$.

We break up this relation into 3 parts:

(1) $p \equiv 0 \bmod 3 \implies p = 3$
(2) $p \equiv 1 \bmod 3$
(3) $p \equiv 2 \bmod 3$.

In the first case, we have that Fermat's Little Theorem clearly implies $a^3 \equiv a \bmod 3$, so all residues modulo 3 are in fact cubic residues.

In the second case, let $p = \pi\bar{\pi} = N(\pi)$. By the third case of 3.13, we have that there is an isomorphism $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/\pi\mathbb{Z}$. Thus, for $p \nmid a$, lemma 3.18 guarantees

Lemma 3.19 (Cubic residues in the integers)**.**

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

Additionally, recall that exactly half of the values in $(\mathbb{Z}/p\mathbb{Z})^*$ are quadratic residues. Similarly, it turns out that exactly one-third of the values in $(\mathbb{Z}/p\mathbb{Z})^*$ are cubic residues (of course, this is only feasible since $p \equiv 1 \bmod 3$).

Finally, before we prove theorem 3.7, we need the following theorem.

Theorem 3.20. *If π and θ are primary primes in $\mathbb{Z}[\omega]$ of unequal norm, then*

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

Here, a primary prime is a prime π such that $\pi \equiv \pm 1 \bmod 3$. Note how simple this theorem is, even after all the complex numbers and other notation involved with cubic reciprocity!

Now we can begin the proof of the main result of this section.

$$p = x^2 + 27y^2 \iff \begin{cases} p \equiv 1 \bmod 3, \\ 2 \text{ is a cubic residue modulo } p. \end{cases}$$

Proof. We begin with the left-to-right direction of the proof.

Clearly, $27y^2$ is a multiple of 3, so we hav $x^2 + 27y^2 \equiv x^2 \bmod 3$. If $x \equiv 0 \bmod 3$, then $3|x^2 + 27y^2$, and since the right hand side of this divisibility is clearly greater than 3, there is no prime p that is equal to it. Thus, we have that x is not a multiple of 3, which implies that $p \equiv 1 \bmod 3$.

Now, it suffices to show that 2 is a cubic residue modulo p. Let $\pi = x + 3\sqrt{-3}y$ so that

$p = \pi\bar{\pi}$. Since $p \equiv 1 \bmod 3$, we have that π is a prime. Also, since $x \not\equiv 0 \bmod 3$, we can say that π is a primary prime. However, 2 is also a primary prime, so we have

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

by lemma 3.20. Thus, it is enough to show that $\left(\frac{\pi}{2}\right)_3 = 1$. To do this, note that by definition 3.17 and the fact $\frac{N(2)-1}{3} = 1$, we have

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

So now we only need to show that $\pi \equiv 1 \bmod 2$.

Since $\sqrt{-3} = 1 + 2\omega$, we have that $\pi = x + 3\sqrt{-3}y = x + 3y + 6\omega y$, which is clearly equivalent to $x + y$ modulo 2. But, x and y must have opposite parity since $p = x^2 + 27y^2$, and this yields the desired result.

Now, we prove the converse direction. We have that $p \equiv 1 \bmod 3$, so let $p = \pi\bar{\pi}$ with π being a primary prime in the Eisenstein integers. Then, we must have $\pi = a + 3b\omega$ for some integers a, b with $3 \nmid a$. This yields

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

Once we show that b is even, the desired result will obviously follow. To do this, we use the assumption that 2 is a cubic residue modulo p. Lemma 3.19 gives $\left(\frac{2}{\pi}\right)_3 = 1$ and then theorem 3.20 yields that $\left(\frac{\pi}{2}\right)_3 = 1$. But, similar to before, this implies that $\pi \equiv 1 \bmod 2$. This can be written as $a + 3b\omega \equiv 1 \bmod 2$, which implies a odd and b even, as required. ■

3.2.3. *Gaussian Integers and Biquadratic Reciprocity.* Now we can begin to address another major form of higher reciprocity, biquadratic reciprocity. Many of the concepts used will be the same as those used in cubic reciprocity, so this section will be relatively short. Still, this section aims to prove the following theorem:

Theorem 3.21. *For prime p, $p = x^2 + 64y^2$* $\iff$ $\begin{cases} p \equiv 1 \bmod 4 \\ 2 \textit{ is a biquadratic residue} \bmod p. \end{cases}$

To prove this theorem, we will once again need to extend our notion of the integers. However, instead of the Eisenstein integers, we will be considering the Gaussian integers, or $\mathbb{Z}[i]$. This ring consists of all numbers of the form $a + bi, a, b \in \mathbb{Z}$, with $i = \sqrt{-1} = e^{\frac{\pi i}{2}}$ as usual.

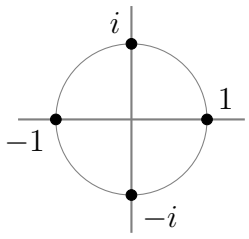

Figure 3. The fourth roots of unity

As with the Eisenstein integers, we can define the norm of $\alpha = a+bi$ as $N(\alpha) = \alpha\bar{\alpha} = a^2+b^2$. The norm function is still multiplicative.

Additionally, the Gaussian integers are a Euclidean ring, so the definitions in 3.9 still hold for $\mathbb{Z}[i]$, and lemmas 3.10 and 3.11 hold as well. In fact, lemma 3.12 holds as well but it turns out that primes not satisfying this condition also exist in $\mathbb{Z}[i]$. We can classify all primes in the following manner.

Corollary 3.22. *All primes in $\mathbb{Z}[i]$ can be divided into 3 groups*

(1) $1 + i$,
(2) *If $p \equiv 1 \bmod 4, p \in \mathbb{Z}$, then there is a prime $\pi \in \mathbb{Z}[i]$ such that $p = N(\pi) = \pi\bar{\pi}$, and the primes π and $\bar{\pi}$ are nonassociate in the Gaussian integers,*
(3) *If $p \equiv 3 \bmod 4, p \in \mathbb{Z}$, then p is also a Gaussian prime.*

It turns out that in the second case, when $p \equiv 1 \bmod 4$ and $p = \pi\bar{\pi}$, there exists an isomorphism $(\mathbb{Z}/p\mathbb{Z})^* \simeq (\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$.

We can also plot the Gaussian primes on the complex plane, yielding the beautiful image below.

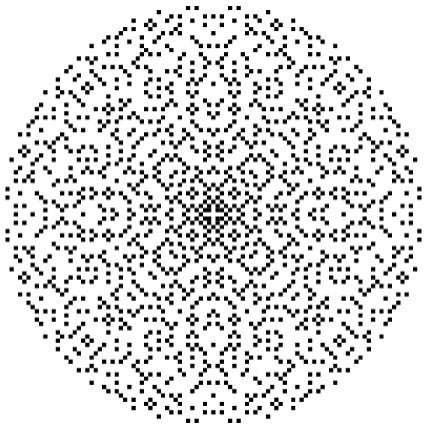

Figure 4. A plot of the Gaussian primes on the complex plane

Additionally, we have the following lemma which is a version of Fermat's Little Theorem over $\mathbb{Z}[i]$.

Lemma 3.23. *If π is prime in $\mathbb{Z}[i]$ and does not divide $\alpha \in \mathbb{Z}[i]$, then*

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

We can now define the biquadratic Legendre symbol. Given a prime $\pi \in \mathbb{Z}[i]$ not associate to 2 (since $2 = i^3(1+i)^2$, this is equivalent to π and $1+i$ being nonassociates), it can be proven that $1, -1, i, -i$ are all distinct modulo π and that $4|N(\pi) - 1$. Then, for α not divisible by π, the *biquadratic Legendre symbol* is defined to be the unique fourth root of unity such that

Definition 3.24 (Biquadratic Legendre symbol)**.**

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

Once again, this implies that the biquadratic reciprocity symbol is mutliplicative. Just as with the case of cubic reciprocity, we can also see that

$$\alpha^{\frac{N(\pi)-1}{4}} = 1 \iff x^4 \equiv \alpha \bmod \pi \text{ is solvable in } \mathbb{Z}[i].$$

Now, recall the second case of 3.22. We have the isomorphism $(\mathbb{Z}/p\mathbb{Z})^* \simeq (\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$., so we can consider $\mathbb{Z}/p\mathbb{Z}$ using the relation regarding biquadratic residues in Gaussian integers provided above. It turns out that $\mathbb{Z}/p\mathbb{Z}$ can be split into exactly 4 parts of equal size; one part consisting of biquadratic residues (where the symbol equals 1), one part of quadratic residues that are not biquadratic residues (symbol equals -1), and two parts of quadratic nonresidues (symbol equals $\pm i$).

We can also state a biquadratic reciprocity relation similar to theorem 3.20.

Note that in the Gaussian integers, we define a primary prime $\pi \in \mathbb{Z}[i]$ as one that satisfies $\pi \equiv 1 \bmod 2+2i$. It turns out that any prime not associate to $1+i$ has a unique associate that is primary. Now, we have

Theorem 3.25.

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

where θ and π are both primary primes in $\mathbb{Z}[i]$.

We also have 2 supplemental laws, stating

$$\left(\frac{i}{\pi}\right)_4 = i^{\frac{1-a}{2}}$$
$$\left(\frac{i+1}{\pi}\right)_4 = i^{\frac{a-b-b^2-1}{4}}$$

for primary prime $\pi = a+bi$. Using these facts, it is now possible to prove 3.21.

$$\text{For prime p, } p = x^2+64y^2 \iff \begin{cases} p \equiv 1 \bmod 4 \\ 2 \text{ is a biquadratic residue mod } p. \end{cases}$$

We begin by first proving a lemma

Lemma 3.26. *If $\pi \in \mathbb{Z}[i]$ is a primary prime, then*

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

Proof. This lemma follows from the supplemental laws stated above and the fact that $2 = i^3(1+i)^2$. Additionally, Dirichlet was able to find an elementary proof of this fact in 1857 using only quadratic reciprocity.

First, consider prime $p \in \mathbb{Z}$ with $p \equiv 1 \bmod 4$. Then, using theorem 2.1, we can write $p = a^2+b^2$ with a being odd and b being even. ∎

Now, we prove the main theorem.

Proof. First let $p \in \mathbb{Z}$ be a prime such that $p \equiv 1 \bmod 4$. Then we can write $p = \pi\bar{\pi}$, where $\pi = a + bi$ is a primary prime in the Gaussian integers. Note that this implies a odd and b even by the definition of primary primes in $\mathbb{Z}[i]$.

Now, we have $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}[i]/\pi\mathbb{Z}[i]$ since $p \equiv 1 \bmod 4$. Then by 3.26, we have that 2 is a biquadratic residue modulo p if and only if b is a multiple of 8. Letting $b = 8c$, we see that $p = \pi\bar{\pi} = a^2 + b^2 = a^2 + 64c^2$, and we are done. ∎

3.3. **Quadratic Forms.** Now that we have addressed methods of improving the reciprocity step of Euler's proofs, we can try to improve the descent step as well. As with the descent step in the case $n = 1$, the descent step for general n begins with the identity

$$(x^2 + ny^2)(z^2 + nw^2) = (xz \pm nyw)^2 + n(xw \mp yz)^2.$$

Proceeding with the descent step as in the case of theorem 2.1, we can conjecture that $p|x^2 + ny^2 \implies p = x^2 + ny^2$ for some (possibly different) x, y. However, this turns out to fail even for small values of n. For example,

$$21 = 1^2 + 5 \cdot 2^2, 3|21 \not\implies 3 = x^2 + 5y^2.$$

So if prime divisors of $x^2 + ny^2$ cannot themselves be represented in the form $x^2 + ny^2$ (again, for possibly different x, y), then how can they be represented? It turns out that Lagrange's theory of quadratic forms provides the tools necessary to address this question, and these are the tools that we will be addressing in this section.

3.3.1. *Basic Theory.* This section serves to cover some of the basic theory behind quadratic forms before we apply this theory to the problem $p = x^2 + ny^2$.

Definition 3.27 (Basic terminology)**.** We begin with a bit of basic terminology.

- A quadratic form is defined as $f(x, y) = ax^2 + bxy + cy^2$.
  - Such a form is called *primitive* if a, b, c are relatively prime.
- The *determinant* of a quadratic form $ax^2 + bxy + cy^2$ is defined as $D = b^2 - 4ac$.
- An integer m is said to be *represented* by $f(x, y)$ if
$$m = f(x, y)$$
has a solution for integer x, y.
  - If x, y are relatively prime, then m is said to be *properly represented*.
- We say that 2 forms $f(x, y)$ and $g(x, y)$ are *equivalent* if there exist integers p, q, r, and s such that
$$f(x, y) = g(px + qy, rx + sy)$$
and $ps - qr = \pm 1$.
  - This equivalence is called *proper* if $ps - qr = 1$, and improper otherwise.
  - Let $f(x, y)$ have discriminant D, and $g(x, y)$ have discriminant D'. Then, using $f(x, y) = g(px + qy, rx + sy)$ and doing some computation yields that $D = (ps - qr)^2 D'$, which implies that any two equivalent forms have the same discriminant.

Note that for the quadratic forms f and g to be equivalent, we must have $ps - qr = \pm 1$, which is equivalent to $\det \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) = \pm 1$. Thus, $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$ is in the group of 2×2 invertible integer matrices, also written as $\mathrm{GL}(2, \mathbb{Z})$. However, for proper equivalences, this matrix is in the

group $\mathrm{SL}(2,\mathbb{Z})$ which consists of 2×2 integer matrices with determinant 1.

It turns out that there is a very nice relation between properly represented values proper equivalences.

Lemma 3.28. *A form $f(x,y)$ properly represents an integer m if and only if $f(x,y)$ is properly equivalent to the form $mx^2 + Bxy + Cy^2$ for some $B, C \in \mathbb{Z}$.*

Proof. We begin by supposing that $f(p,q) = m$, for relatively prime integers p and q. Then, Bezout's lemma guarantees that there exist integers r and s with $pr - qs = 1$.

If $f(x,y) = ax^2 + bxy + cy^2$, then

$$\begin{aligned} f(px + ry, qx + sy) &= f(p,q)x^2 + (2apr + bps + brq + 2cqs)xy + f(r,s)y^2 \\ &= mx^2 + Bxy + Cy^2 \end{aligned}$$

which is of the desired form.

To prove the converse, simply consider $(x,y) = (1,0)$ over the form $mx^2 + Bxy + Cy^2$. ■

We now list a few more properties of the discriminant. Through simple computation, it is easy to see that the identity

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

is true. This means that for $D > 0$, f can take on both positive and negative values. Such a form is called *indefinite*. On the other hand, if $D < 0$, then f represents only positive or only negative values depending on the sign of a. Accordingly, such forms are called *positive definite* or *negative definite*. However, if $D = 0$, then f can take only nonnegative or only nonpositive values. Such forms are called *positive semidefinite* and *negative semidefinite*, respectively.

The discriminant D affects quadratic forms one other way; since $D = b^2 - 4ac$, it follows that b is even (resp. odd) if and only if $D \equiv 0$ (resp. 1) mod 4. We also have the following lemma regarding the discriminant.

Lemma 3.29. *Let $D \equiv 0, 1 \bmod 4$ be an integer and 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 modulo m.*

Proof. Since m is properly represented by some primitive form f, we can assume that $f(x,y) = mx^2 + bxy + cy^2$ by lemma 3.28.

Thus, we have $D = b^2 - 4mc$, which gives $D \equiv b^2 \bmod m$, which is exactly what we want to prove.

Conversely, if $D \equiv b^2 \bmod m$, then since m is odd, we can assume that D and b are the same parity, replacing b by $b+m$ if necessary. Then, $D \equiv 0, 1 \bmod 4$ implies that $D \equiv b^2 \bmod 4m$. So, $D = b^2 - 4mc$ for some integer c. So, $mx^2 + bxy + cy^2$ represents m properly and has discriminant D and the coefficients are all relatively prime to D since $\gcd(m, D) = 1$. ■

For the purposes of $p = x^2 + ny^2$, the most useful implementation of lemma 3.29 is the following corollary:

Corollary 3.30. *Let n be an integer and let p be an odd prime not dividing n. Then $\left(\frac{-n}{p}\right) = 1$ if and only if p is represented by a primitive form of discriminant $-4n$.*

Proof. The proof follows from lemma 3.29 because $-4n$ is a quadratic residue modulo p if and only if

$$\left(\frac{-4n}{p}\right) = \left(\frac{-n}{p}\right) = 1.$$

■

To see how this corollary is related to the descent step, recall lemma 3.3. Due to this lemma, we see that prime divisors p of $x^2 + ny^2$ can be represented by quadratic forms of discriminant $-4n$. The only issue with this is that there are too many quadratic forms that satisfy this condition.

For example, applying this corollary to $\left(\frac{-3}{13}\right) = 1$ yields that 13 is represented by the form $13x^2+12xy+3y^2$ with discriminant -12. But this does not provide us with that much information. In order for this corollary to be truly useful, we need to show that every quadratic form of a certain discriminant is equivalent to another, especially simple, form. Lagrange's theory of reduced forms does this beautifully.

Though we have been dealing with arbitrary quadratic forms for now, for the purposes of this text, we will now limit our scope to only positive definite forms. This not only covers the forms of interest to us (namely, $x^2 + ny^2$), but also simplifies our consideration of the theory of reduced forms.

Definition 3.31. A primitive positive definite form is considered to be *reduced* if

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

Of course, a and c are positive since the form is positive definite.

The theorem of interest to is is as follows:

Theorem 3.32. *Every primitive positive definite form is properly equivalent to a unique reduced form.*

Finally, in order to complete our treatment of reduced forms, we need to make one more observation. Suppose that $ax^2+bxy+cy^2$ is a reduced form of negative discriminant. Then, by the definition of a reduced form, we have that $b^2 \leq a^2, a \leq c$, which leads to

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

Thus, we have

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

For a fixed D, this means that there are only finitely many choices for a, and since $|b| \leq a$, there are only finitely many choices for b as well. Since $D = b^2 - 4ac$, the same is true for c, so there are only finitely many reduced forms of discriminant D.

Then, theorem 3.32 yields that there are only a finite number of proper equivalence classes as well. We say that two forms are of the same *class* if they are properly equivalent, and let $h(D)$ denote the number of such classes of primitive positive definite forms of discriminant D. Of course, this is just the same as the number of reduced forms. So, the following theorem is true:

Theorem 3.33. *Let $D < 0$ be fixed. Then the number $h(D)$ of classes of primitive positive definite forms of discriminant D is finite, and furthermore $h(D)$ is equal to the number of reduced forms of discriminant D.*

3.3.2. *Applications to $p = x^2 + ny^2$.* Using the theory from the previous section, we can now apply quadratic forms to the problem at hand. To begin, we have the following theorem:

Theorem 3.34. *Let n be a positive integer and p be an odd prime not dividing n. Then $\left(\frac{-n}{p}\right) = 1$ if and only if p is represented by one of the $h(-4n)$ reduced forms of discriminant $-4n$.*

Proof. This follows directly from corollary 3.30 and theorem 3.32. ■

Along with the fact that a number, say some prime p, can only be represented by a form of discriminant D if $\left(\frac{D}{p}\right) = 1$, we arrive at a result that allows for an analysis of primes p that can be represented by quadratic forms.

In the case of $n = 1, 2, 3, 4, 7$, it turns out that the only reduced form of discriminant $-4n$ is of the form $x^2 + ny^2$. This is exactly what we want – paired with theorem 3.34, we see that $p = x^2 + ny^2$ if and only if

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

Though it is quite computational, this theorem allows us to reprove the theorems of Euler and Fermat discussed at the end of section 3.1.

Other than for these specific values of n, the theory of quadratic forms pops up again and again throughout many other areas of math related to $p = x^2 + ny^2$.

4. A Solution for All n

In this section, we will explore the solution to $p = x^2 + ny^2$ for all n, in contrast to the work done in the last section.

A stepping stone to the promised theorem for all n is as follows:

Theorem 4.1. *Let $n > 0$ be a squarefree integer not congruent to 3 modulo 4. Then there is a monic irreducible 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*

$$p = x^2 + ny^2 \iff \left\{\left(\frac{-n}{p}\right) = 1 \text{ and } f_n(x) \equiv 0 \bmod p \text{ has an integer solution.}\right.$$

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 $K = \mathbb{Q}(\sqrt{-n})$.

While we will not prove this theorem, the concepts behind it will be explained in an effort to understand what it actually means.

We begin by defining a *number field* K to be a subfield of the complex numbers $\mathbb{C}$ which has a finite degree over $\mathbb{Q}$. The degree of K over $\mathbb{Q}$ is denoted $[K : \mathbb{Q}]$. For such a field K, we define the algebraic integers of K, $\mathcal{O}_K$, as the set of all $\alpha \in K$ which are the roots of a monic integer polynomial. The set $\mathcal{O}_k$ is often called the *ring of integers* of K.

Now, recall definition 3.14. A *prime ideal* is defined as follows:

Definition 4.2 (Prime ideal)**.** $\mathfrak{p}$ such that for all a, b, if $ab \in \mathfrak{p}$, $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

It turns out that for a number field K, any nonzero ideal $\mathfrak{a} \in \mathcal{O}_K$ can be represented as a product of prime ideals, with the decomposition being unique up to order. The prime ideals in the decomposition are exactly the prime ideals of $\mathcal{O}_K$ that contain $\mathfrak{a}$.

Next, we will introduce the idea of ramification and inertial degree. Consider a number field K and let L be a finite extension of K.

Definition 4.3 (Field extension)**.** A field extension is a pair of fields $K \subseteq L$, such that the operations of K are those of L restricted to K. In this case, L is an extension field of K and K is a subfield of L. The *degree* of the field extension is denoted by $[L : K]$, and extensions with finite degree are called *finite extensions*.

Note that $[L : K]$ is the number of left cosets of K in L.

Definition 4.4 (Left coset)**.** Let G be a group and H be a subgroup of G. Then the subset $aH = ah | h \in H \subseteq G$ is the left coset of H containing a.

Now, onto ramification. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$, and thus has a prime factorization which can be represented as

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1^{e_1}\mathfrak{B}_2^{e_2}\dots\mathfrak{B}_g^{e_g}.$$

Here, the $\mathfrak{B}_i$'s are the distinct primes of L containing $\mathfrak{p}$. Then, we have the following definitions:

Definition 4.5 (Ramification index)**.** The *ramification index* of $\mathfrak{p}$ in $\mathfrak{B}_i$ is the integer e_i.

Definition 4.6 (Inertial degree)**.** Each prime $\mathfrak{B}_i$ gives a field extension $\mathcal{O}_L/\mathfrak{B}_i$, whose degree is called the *inertial degree* f_i of $\mathfrak{p}$ in $\mathfrak{B}_i$.

It turns out that the sum of $e_i f_i$ from $i = 1$ to $i = g$ is simply the degree of the field extension L/K.

Of particular interest to us are *Galois extensions* L/K. The definition of a Galois extension is quite difficult to understand and most of the extensions that are used in the proofs of the following theorems are Galois extensions anyway, so we will just state a useful property of them here. For a Galois extension, all primes $\mathfrak{B}_i$ containing $\mathfrak{p}$ have the same ramification index e and the same inertial degree f. Thus, we have

$$efg = [L : K].$$

Given a Galois extension $K \subset L$, an ideal $\mathfrak{p}$ of K *ramifies* if $e > 1$, and is unramified if $e = 1$. If $\mathfrak{p}$ satisfies the stronger condition $e = f = 1$, then we say that $\mathfrak{p}$ *splits completely* in L.

Now, we define the *Hilbert class field* of a field K.

Definition 4.7 (Hilbert class field)**.** Given a number field K, there is a finite Galois extension L of K such that L is an unramified Abelian extension of K, and any unramified Abelian extension of K lies in L.

Here, an *Abelian* extension is one that is Galois and $\mathrm{Gal}(L/K)$ is abelian (i.e. commutative). Note that $\mathrm{Gal}(L/K)$ is the Galois group of the extension at hand, which consists of all automorphisms (self maps) of the extension.

Using the theory of the Hilbert class field along with the other class field theory shown so far, it is possible to show theorem 4.1 is true. This is done by showing that both the left and right hand sides of the "if and only if" in theorem 4.1 are equivalent to p splitting completely in the Hilbert class field of $\mathbb{Q}(\sqrt{-n})$. Here, $\mathbb{Q}(\sqrt{-n})$ is the set of all $a + b\sqrt{-n}$ for rational a, b. However, the proof is omitted here for the sake of brevity.

It turns out that by using *ring class fields*, a stronger variation of theorem 4.1 may be proven, which is the crown theorem of this paper.

Theorem 4.8. *Let $n > 0$ be an integer. Then there is a monic irreducible 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*

$$p = x^2 + ny^2 \iff \left\{ \left(\frac{-n}{p}\right) = 1 \text{ and } f_n(x) \equiv 0 \bmod p \text{ has an integer solution.} \right.$$

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 ring class field of order $\mathbb{Z}[\sqrt{-n}]$ in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-n})$.

Finally, if $f_n(x)$ is any monic integer polynomial of degree $h(-4n)$ for which the above equivalence holds, then $f_n(x)$ is irreducible over $\mathbb{Z}$ and is the minimal polynomial of a primitive element of the ring class field L described above.

At this point, every piece of notation used in this theorem has already been described except for the definition of a ring class field. We will define what such a field is, but will omit the proof of theorem 4.8, again for the sake of brevity.

Definition 4.9 (Ring class field)**.** Let $\mathcal{O}$ be an order of conductor f in an imaginary quadratic field K (one of the form $\mathbb{Q}(\sqrt{-n})$ for $n > 0$). Then, the ring class field of the order $\mathcal{O}$ is the unique Abelian extension L of K.

The conductor f is equivalent to the set $\mathrm{Ann}_K(L/K)$. Note that

$$\mathrm{Ann}_A(B) = a \in A | b \in B \text{ implies } ab = 0.$$

For such a ring class field, we have that all primes of K ramified in L must divide $f\mathcal{O}_K$.

With this, we finish our treatment of primes of the form $p = x^2 + ny^2$.

References

[1] John; Barile, Margherita; Renze and Eric W. Weisstein. Principal ideal domain.
[2] David A. Cox. *Primes of the Form $x^2 + ny^2$*. AMS Chelsea Publishing, 3 edition, 2022.
[3] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley and Sons, 3 edition, 2004.
[4] Rahmi Jackson and Eric W. Weisstein. Kernel.
[5] Todd; Moslehian, Mohammad Sal; Rowland and Eric W. Weisstein. Ideal.
[6] Todd Rowland. Prime ideal.
[7] Todd Rowland and Eric W. Weisstein. Galois extension.
[8] Harold M. Stark. *An Introduction to Number Theory*. MIT Press, 1 edition, 1970.
[9] Eric W. Weisstein. Algebraic number.
[10] Eric W. Weisstein. Eisenstein prime.
[11] Eric W. Weisstein. Gaussian prime.
[12] Eric W. Weisstein. Principal ideal.

[3] [2] [8] [4] [11] [10] [6] [12] [5] [1] [9] [7]