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

YIQIAO BAO

Abstract. We solve the $p = x^2 + ny^2$ problem using class group theory. We first introduce integer rings and some special properties of Dedekind domains. Then, we give a criterion for how principal ideals generated by prime numbers factor in integer rings. Finally, by using Minkowski's bound and by computing the ideal class group, we describe which odd prime numbers can be written in the form of $x^2 + ny^2$.

Contents

1. Introduction

Readers might be familiar to the following theorem of Fermat introduced in most undergraduate number theory courses: for an odd prime p, p is the sum of two squares if and only if p is equivalent to 1 modulo 4. That is,

$$p = x^2 + y^2 \text{ for some integers } x, y \Leftrightarrow p \equiv 1 \bmod 4.$$

This theorem leads us to consider a more general problem: which prime numbers can be written in the form of $x^2 + ny^2$ where x, y, n are integers?

Legendre gave a solution using Genus Theory. The form $x^2 + ny^2$ we are interested in is a special case of general quadratic forms $ax^2 + bxy + cy^2$. Genus Theory studies how prime integers are *represented by*, that is, can be written in the form of, these general quadratic forms. The discriminant of a quadratic form $ax^2 + bxy + cy^2$ is $D = b^2 - 4ac$. Then, the discriminant of $x^2 + ny^2$ is $-4n$. Each quadratic form of discriminant D is *equivalent* to a unique quadratic form with some special properties. These special forms are called *reduced* forms. For example, $x^2 + ny^2$ for a positive integer n is in the reduced form. Suppose one wants to find out which

Date: August 5, 2020.

primes can be written in the form of $x^2 + 5y^2$ whose discriminant is -20. Genus Theory suggested that any prime p satisfies

$$\left(\frac{-20}{p}\right) = 1 \tag{1.1}$$

if and only if it can be written in some reduced form with discriminant equal -20. If $p \equiv 3 \bmod 4$, we have

$$\left(\frac{-20}{p}\right) = \left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = -\left(\frac{5}{p}\right) = -\left(\frac{p}{5}\right) = 1.$$

Therefore, $p \equiv 2, 3 \bmod 5$. Together with the assumption $p \equiv 3 \bmod 4$, we have $p \equiv 3, 7 \bmod 20$. Similarly, if $p \equiv 1 \bmod 4$, we have

$$\left(\frac{-20}{p}\right) = \left(\frac{5}{p}\right) = 1.$$

Then $p \equiv 1, 4 \bmod 5$, suggesting $p \equiv 1, 9 \bmod 20$. In this way, we can narrow our choices down to 4 equivalence classes: a prime number p can be written in a quadratic form of discriminant -20 if and only if p is equivalent to 1,3,7,9 modulo 20. There are 2 reduced form of discriminant $D = -4n = -20$, namely x^2+5y^2 and $2x^2 + 2xy + 3y^2$ (see Cox[27, Theorem 2.13] for a proof). Hence, we still couldn't decide which primes of the four choices are represented by $x^2 + 5y^2$ and which are represented by $2x^2 + 2xy + 3y^2$ without some effort.

This paper will approach this problem with a different and less direct method. We will enlarge our scope and consider the operations in larger rings by using class field theory. Then, our main concern turns to the ideal generated by a prime integer p. By studying the properties of *integer rings* and how principal ideals (p) factor in these rings, we can find prime numbers of the form $x^2 + ny^2$ elegantly.

2. Basic Definitions

To begin with, I want to first introduce the idea of number field and ring of integers.

Definition 2.1. A number field K is a finite extension of $\mathbb{Q}$ inside $\mathbb{C}$.

Definition 2.2. Let the ring of integers $\mathcal{O}_K$ be the set containing any element α in K that satisfies $f(\alpha) = 0$ for some monic polynomial $f(x)$ with coefficients in $\mathbb{Z}$. Each element in $\mathcal{O}_K$ is called an algebraic integer.

For any algebraic integers $\alpha, \beta \in \mathcal{O}_K$, their sum and their product are also integral over $\mathbb{Z}$. Readers could refer to Neukirch *Algebraic Number Theory* [6, Proposition 2.2] for a proof. Hence the set of algebraic integers forms a ring $\mathcal{O}_K$. In fact, $\mathcal{O}_K$ is a Dedekind domain. Here are some important properties of a Dedekind domain that we will use in our discussions:

(1) $\mathcal{O}_K$ is integrally closed in K.
(2) Every non-zero prime ideal is maximal.

This paper will mainly focus on quadratic number fields. That is, number fields K of the form $\mathbb{Q}(\sqrt{N})$, where N is a square-free integer. Define the *discriminant* d_k of $K = \mathbb{Q}(\sqrt{N})$ as follows:

$$d_k = \begin{cases} N & \text{if } N \equiv 1 \bmod 4 \\ 4N & \text{otherwise} \end{cases}$$

Proposition 2.3. *The ring of integers $\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{N})$ can be written explicitly as*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\Big[\frac{1+\sqrt{N}}{2}\Big] & \text{if } N \equiv 1 \text{ mod } 4 \\ \mathbb{Z}[\sqrt{N}] & \text{otherwise} \end{cases} \tag{2.4}$$

Proof. For any element $\alpha \in K = \mathbb{Q}(\sqrt{N})$, α is of the form $r + s\sqrt{N}$ for some $r, s \in \mathbb{Q}$. There is a non-trivial automorphism of K that maps α to $\overline{\alpha} = r - s\sqrt{N}$. The trace and the norm of α are defined as follows.

$$T(\alpha) = \alpha + \overline{\alpha} = 2r, \tag{2.5}$$

$$N(\alpha) = \alpha\overline{\alpha} = r^2 - s^2 N. \tag{2.6}$$

Lemma 2.7. *For any $\alpha \in K$, α is integral if and only if $T(\alpha), N(\alpha) \in \mathbb{Z}$.*

Proof. First, consider the quadratic polynomial

$$f(x) = (x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}$$

. It admits α as a root. Hence, if the trace $T(\alpha) = \alpha + \overline{\alpha}$ and the norm $N(\alpha) = \alpha\overline{\alpha}$ are integers, the quadratic polynomial $f(x)$ has integer coefficients. By definition, α is integral over $\mathbb{Z}$.

Now assume α is integral over $\mathbb{Z}$. Since

$$f(x) = (x - \alpha)(x - \overline{\alpha}) = (x - r - s\sqrt{N})(x - r + \sqrt{N}) = x^2 - 2r \cdot x + r^2 - s^2 N$$

, $f(x)$ has rational coefficients. Thus, we can multiply $f(x)$ by some integer m to get a quadratic polynomial $\overline{f}(x)$ that has integer coefficients. Since the minimal polynomial of α, $f_\alpha(x)$, must divide $\overline{f}(x)$, $f_\alpha(x)$ is quadratic. By definition, $f_\alpha(x)$ is monic, while the leading coefficient of $\overline{f}(x)$ is m. Hence, $\overline{f}(x)$ is an m multiple of f_α. This shows f_α is exactly $f(x) = x^2 - 2r \cdot x + r^2 - s^2 N$, which means both the norm and the trace of α are integers. Therefore, for any $\alpha \in K$, $\alpha \in \mathcal{O}_K$ if and only if $T(\alpha), N(\alpha) \in \mathbb{Z}$.

□

Suppose $N \equiv 1 \bmod 4$. For any $\gamma \in \mathbb{Z}\Big[\frac{1+\sqrt{N}}{2}\Big]$, clearly $N(\gamma), T(\gamma) \in \mathbb{Z}$. Hence, γ is an algebraic integer. This shows $\mathbb{Z}\Big[\frac{1+\sqrt{N}}{2}\Big]$ is contained in $\mathcal{O}_K$. On the other hand, for any $\beta = r + s\sqrt{N} \in \mathcal{O}_K$, we must have $T(\beta), N(\beta) \in \mathbb{Z}$. That is, $2r$ and $r^2 - s^2 N$ are integers. Let $m = 2r \in \mathbb{Z}$, then

$$\frac{m^2}{4} - s^2 N \in \mathbb{Z},$$

or,

$$m^2 - 4s^2 N \equiv 0 \bmod 4.$$

If $m = 2r$ is even, s is an integer. We then have

$$\beta \in \mathbb{Z}[\sqrt{N}] \subseteq \mathbb{Z}\Big[\frac{1+\sqrt{N}}{2}\Big].$$

If m is odd, s is of the form $\frac{n}{2}$ where n is an odd integer. Thus,

$$\beta = \frac{m}{2} + \frac{n}{2}\sqrt{N} = \lfloor \frac{m}{2} \rfloor + \frac{1+\sqrt{N}}{2} \in \mathbb{Z}\Big[\frac{1+\sqrt{N}}{2}\Big].$$

Hence, the first case in the description (2.4) is proved. The second case is similar.

□

In fact, the two cases presented in Proposition 2.3 can be simplified into one case by using the discriminant of the number field.

Proposition 2.8. *Let $K = \mathbb{Q}(\sqrt{N})$ where N is any square-free integer. Then the ring of integers $\mathcal{O}_K$ can be written explicitly as*

$$\mathcal{O}_K = \mathbb{Z}\Big[\frac{d_K + \sqrt{d_K}}{2}\Big]. \tag{2.9}$$

By the definition of the norm of an element in $\mathbb{Q}(\sqrt{N})$ in (2.5) and (2.6), it can be seen that the norm function is multiplicative. That is, $N(\alpha\beta) = N(\alpha)N(\beta)$ for any $\alpha, \beta \in \mathbb{Q}(\sqrt{N})$. Also, the norm of an algebraic integer is also an integer. Suppose an algebraic integer b is a unit in $\mathcal{O}_K$. Then $N(bb^{-1}) = N(b)N(b^{-1}) = N(1) = 1$. This shows the norm of a unit element in $\mathcal{O}_K$ must be ± 1. The converse is also true. For an algebraic integer $b = r + s\sqrt{N}$ whose norm is ± 1, we have $r^2 - s^2N = 1$. Then $\overline{b} = r - s\sqrt{N}$ is the inverse of b.

For a general $\mathcal{O}_K$ and an ideal $\mathfrak{a}$ in $\mathcal{O}_K$, define the norm of $\mathfrak{a}$ to be

$$N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|. \tag{2.10}$$

By the Chinese Remainder Theorem,

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$$

for two ideals $\mathfrak{a}$ and $\mathfrak{b}$. If $K = \mathbb{Q}(\sqrt{N})$ and the ideal $\mathfrak{a}$ is a principal ideal generated by an element a, then the norm of $\mathfrak{a} = (a)$ is the absolute value of $N(a)$.

3. Unique Prime Factorization

Part of the motivation of studying Dedekind domains is to find the unique prime factorization of ideals. While the prime factorization for an integer is unique in $\mathbb{Z}$, this is not always the case in larger rings. For example, the ring of integers for the number field $K = \mathbb{Q}(\sqrt{-5})$ is $\mathbb{Z}(\sqrt{-5})$ by Proposition 1.4. There are two prime factorizations of the integer 6 in $\mathcal{O}_K$, namely

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \tag{3.1}$$

We will prove by contradiction that $3, 2, 1+\sqrt{-5}$, and $1-\sqrt{-5}$ are prime numbers in $\mathbb{Z}[\sqrt{-5}]$. If 3 is not a prime number, then we can find non-units $a, b \in \mathbb{Z}(\sqrt{-5})$ such that $ab = 3$, meaning

$$N(a)N(b) = N(3) = 9.$$

Since a, b are not units, their norms are not equal to ± 1. Thus

$$N(a) = N(b) = \pm 3$$

as norms of algebraic integers are again integers. However, $r^2 + 5s^2 = \pm 3$ does not have integer solutions, which means there is no element of the form $r + s\sqrt{-5} \in \mathcal{O}_K$ whose norm is 3. Therefore, 3 is a prime. Similarly, $2, 1+\sqrt{-5}, 1-\sqrt{-5}$ are primes. Furthermore, since $1 + \sqrt{-5}$ is not a unit multiple of either 2 or 3, (3.1) gives two ways to prime factor 6 in $\mathbb{Q}(\sqrt{-5})$.

However, if we consider the factorization of *ideals*, then the prime factorization is unique in Dedekind domains.

Theorem 3.2. *Suppose $\mathfrak{a}$ is a non-zero ideal in the Dedekind domain $\mathcal{O}_K$. Then there exists an unique prime factorization of $\mathfrak{a}$. That is,*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$$

where $\mathfrak{p}_i$ are prime ideals, unique up to permutation of indices.

Proof. Please refer to Lang [72, section 1.6] for a proof of the theorem. □

In our example, the ideal (6) can be factored into $(2)\cdot(3)$ or $(1+\sqrt{-5})\cdot(1-\sqrt{-5})$. We will later see that

$$(3) = \mathfrak{p}_1\mathfrak{p}_2, (2) = \mathfrak{p}_3^2,$$

for some distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$; and

$$(1 + \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3, (1 - \sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_3.$$

Thus the ideal (6) has a unique prime factorization into prime ideals.

The set of the ideals in $\mathcal{O}_K$ forms a monoid. In order to get a group structure, we introduce the idea of fractional ideals.

Definition 3.3. A fractional $\mathcal{O}_K$-ideal is a non-zero finitely generated $\mathcal{O}_K$-submodule of K.

Equivalently, fractional ideals are of the form $\alpha\mathfrak{a}$, where $\alpha \in K$ and $\mathfrak{a}$ is an ideal in $\mathcal{O}_K$. With this definition, we can generalize theorem 3.2:

Corollary 3.4. *For a fractional $\mathcal{O}_K$-ideal $\mathfrak{a}$, there exists a unique prime factorization*

$$\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_n^{s_n},$$

where s_i are integers, $\mathfrak{p}_i$ are distinct prime ideals in $\mathcal{O}_K$, $\mathfrak{p}_i$ and s_i are unique up to permutation of indices.

Proof. See Lang [72, section 1.6] for a proof. □

Thus, for any fractional ideal $\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_n^{s_n}$, we can always find a unique fractional ideal $\mathfrak{b} = \mathfrak{p}_1^{-s_1} \cdots \mathfrak{p}_n^{-s_n}$ such that $\mathfrak{ab} = \mathcal{O}_K$. We will use $\mathfrak{a}^{-1}$ to denote $\mathfrak{b}$. It's also clear that the product of two fractional ideals is again a fractional ideal. Hence, the set of all fractional ideals forms a group which will be denoted by I_K, with the identity element being $\mathcal{O}_K$ itself. The most important subgroup of our concern is the subgroup constructed by all principal fractional ideals, i.e., fractional ideals of the form $\alpha\mathcal{O}_K$ where α is an invertible element in K^*. We will denote this subgroup by P_K. Their quotient, I_K/P_K, is called the *ideal class group* and will be denoted by $C(O_K)$.

Proposition 3.5. *The ideal class group is a finite group.*

Proof. Please refer to Marcus [77, Corollary 2 to Theorem 35] for a proof. □

4. Ramification

Recall that in the previous section, it was stated that the ideal (3) can be factored into the product of two distinct prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ in the ring $\mathbb{Z}[\sqrt{-5}]$. This will be proved in the end of this section. Moreover, we will generalize this statement and show how an ideal generated by an arbitrary prime integer will factor in the ring of integers of a quadratic field $\mathbb{Q}(\sqrt{N})$. First, we will introduce the factorization behavior of a prime ideal in field extensions.

For a number field K, assume L/K is a finite field extension. Let $\mathfrak{p}$ be an arbitrary prime ideal in $\mathcal{O}_K$. Notice that $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$. As claimed in Theorem 3.4, there exists a unique prime factorization of $\mathfrak{p}\mathcal{O}_L$ in $\mathcal{O}_L$:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \tag{4.1}$$

where $\mathfrak{P}_i$ are distinct prime ideals in L. The positive integers e_i, also written as $e_{\mathfrak{P}_i|\mathfrak{p}}$, are called the ramification indices of $\mathfrak{p}$ in $\mathfrak{P}_i$. For any element $\alpha \in \mathfrak{p}$, α is in $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$. Hence, $\mathfrak{P}_i$ are ideals containing $\mathfrak{p}$. Since prime ideals are maximal in Dedekind domains, each $\mathfrak{P}_i$ gives a field extension $\mathcal{O}_L/\mathfrak{P}_i$ over $\mathcal{O}_K/\mathfrak{p}$. We call the degree of this field extension the *inertial degree* of $\mathfrak{p}$ in $\mathfrak{P}_i$, and denote it by f_i or $f_{\mathfrak{P}_i|\mathfrak{p}}$. Once we have these definitions, we can introduce the following theorems.

Theorem 4.2. *Suppose K is a number field and L is some finite field extension. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$, and let $e_1, \cdots, e_g$ be the ramification indices and $f_1, \cdots, f_g$ be the inertial degrees as defined above. Then we have*

$$\sum_{j=1}^{g} e_j f_j = [L : K]. \tag{4.3}$$

Theorem 4.4. *Suppose K is a number field; L/K is a Galois extension. Let $\mathfrak{p}$ be any prime ideal in $\mathcal{O}_K$. Then the Galois group $Gal(L/K)$ acts transitively on the prime ideals in $\mathcal{O}_L$ containing $\mathfrak{p}$.*

Readers can refer to Marcus [77, Theorem 21, Theorem 23] for proofs. These two theorems lay the foundation for the next theorem:

Theorem 4.5. *Suppose K is a number field; L/K is a Galois extension. If $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$, then the ramification indices are the same, i.e., $e_i = e_j$ for any i, j. Moreover, the inertial degrees are the same, i.e., $f_i = f_j$ for any i, j. We then have $efg = [L : K]$.*

Proof. Any element in $\mathrm{Gal}(L/K)$ maps algebraic integers in $\mathcal{O}_L$ to other algebraic integers. Suppose σ is an element in $\mathrm{Gal}(L/K)$. Since being integral is a Galois-invariant condition, $\sigma(\mathcal{O}_L) = \mathcal{O}_L$. Suppose $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$. Then

$$\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p})\sigma(\mathcal{O}_L) = \sigma(\mathfrak{p}\mathcal{O}_L) = \sigma(\mathfrak{P}_1)^{e_1} \cdots \sigma(\mathfrak{P}_g)^{e_g}.$$

Hence, $e_{\mathfrak{P}_i|\mathfrak{p}} = e_i = e_{\sigma(\mathfrak{P}_i)|\mathfrak{p}}$ for all i. By Theorem 4.4, we can always find an automorphism in $\mathrm{Gal}(L/K)$ that maps $\mathfrak{P}_i$ to $\mathfrak{P}_j$ for all i, j. Thus, $e_{\mathfrak{P}_i|\mathfrak{p}} = e_{\mathfrak{P}_j|\mathfrak{p}}$. That is, $e_i = e_j$ for all i, j. Similarly, $|\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}| = |\mathcal{O}_L/\sigma(\mathfrak{P}_i) : \mathcal{O}_K/\mathfrak{p}|$. That is, $f_{\mathfrak{P}_i|\mathfrak{p}} = f_{\sigma(\mathfrak{P}_i)|\mathfrak{p}}$. By the transitivity of the group action, $f_i = f_j$ for all i, j. Together with (4.3), we have $efg = [L : K]$ where g is the number of distinct prime ideals in the prime factorization of $\mathfrak{p}\mathcal{O}_L$. □

Now we see that the prime factorization of $\mathfrak{p}\mathcal{O}_L$ is of the form $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^e \cdots \mathfrak{P}_g^e$. If $e > 1$, then we say that the prime ideal $\mathfrak{p}$ *ramifies* in L. Otherwise, if $e = 1$, we say $\mathfrak{p}$ is *unramified*. Moreover, $\mathfrak{p}$ *splits* in L if both e and f are equal to 1.

This paper mainly focuses on prime factorization in a quadratic field $K = \mathbb{Q}(\sqrt{N})$. If for a prime integer p, the ideal $p\mathcal{O}_K$ factors into $\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_g^{e_g}$ where $\mathfrak{p}_i$ are distinct prime ideals in $\mathcal{O}_K$, then we must have $efg = 2$ where f is the degree of $\mathcal{O}_K/\mathfrak{p}_i$ over $\mathbb{Z}/(p)$. Therefore, there are only three cases:

(1) $g = 2, e = f = 1$. In this case, $p\mathcal{O}_K$ splits. That is, $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ for two distinct primes $\mathfrak{p}_1, \mathfrak{p}_2$.

(2) $f = 2, e = g = 1$. In this case, $p\mathcal{O}_K$ is a prime ideal.

(3) $e = 2, f = g = 1$. In this case, $p\mathcal{O}_K$ ramifies. That is, $p\mathcal{O}_K = \mathfrak{p}^2$ for a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$.

Proposition 4.6 below provides a specific criterion of how $p\mathcal{O}_K$ factors in $\mathcal{O}_K$ for a prime integer p. It is the main tool we will be using to find prime numbers of the form $x^2 + ny^2$.

Proposition 4.6. *Suppose K is a quadratic number field of the form $\mathbb{Q}(\sqrt{N})$ with discriminant d_K. Let p be a prime integer.*

(1) If $(\frac{d_K}{p}) = 0$, (that is, if $p|d_K$) then $p\mathcal{O}_K = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$.
(2) If $(\frac{d_K}{p}) = 1$, then $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ for some distinct non-trivial prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ in $\mathcal{O}_K$.
(3) If $(\frac{d_K}{p}) = -1$, then $p\mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$.

Proof. As proved in Proposition 2.3, the ring of integers for K is $\mathcal{O}_K = \mathbb{Z}\left[\frac{d_K+\sqrt{d_K}}{2}\right]$. Since

$$\frac{d_K + \sqrt{d_K}}{2} \cdot \frac{-d_K + \sqrt{d_K}}{2} = \frac{-d_K^2 + d_K}{4},$$

the quadratic polynomial

$$f(x) = x(x - d_K) - \frac{-d_K^2 + d_K}{4} = x^2 - xd_K - \frac{d_K - d_K^2}{4}$$

admits $\frac{d_K+\sqrt{d_K}}{2}$ as a root. (Notice that d_K is equivalent to 0 or 1 modulo 4, meaning $\frac{d_K-d_K^2}{4}$ is an integer. Thus $f(x)$ is indeed a polynomial in $\mathbb{Z}[x]$.) Hence, $\mathcal{O}_K = \mathbb{Z}[x]/(x^2 - xd_K - \frac{d_K-d_K^2}{4})$.

Now consider $\mathcal{O}_K/p\mathcal{O}_K$.

$$\begin{aligned}\mathcal{O}_K/p\mathcal{O}_K &= \mathbb{Z}[x]/(x^2 - xd_K - \frac{d_K - d_K^2}{4})\Big/p\big(\mathbb{Z}[x]/(x^2 - xd_K - \frac{d_K - d_K^2}{4})\big)\\ &= \mathbb{Z}[x]/p\mathbb{Z}[x]\Big/(x^2 - xd_K - \frac{d_K - d_K^2}{4})(\mathbb{Z}[x]/p\mathbb{Z}[x])\\ &= \mathbb{F}_p/(x^2 - xd_K - \frac{d_K - d_K^2}{4}).\end{aligned}$$

If in the first case, p divides d_K, then RHS becomes $\mathbb{F}_p/(x^2)$. The prime ideals are (x) and (x). It corresponds to (p) ramifies.

For the second case, assume the Legendre symbol $\left(\frac{d_K}{p}\right) = 1$. Then there exist some $a \in \mathbb{F}_p^*$ such that $a^2 = d_K$. We have

$$\begin{aligned}\mathbb{F}_p/(x^2 - xd_K - \frac{d_K - d_K^2}{4}) &= \mathbb{F}_p/(x^2 - xd_K - \frac{a^2 - d_K^2}{4})\\ &= \mathbb{F}_p/(x + \frac{-a - d_K}{2})(x + \frac{a - d_K}{2}).\end{aligned}$$

The two prime ideals are $(x + \frac{-a-d_K}{2})$ and $(x + \frac{a-d_K}{2})$, showing $p\mathcal{O}_K$ factors into two distinct prime ideals in $\mathcal{O}_K$.

For the third case, assume $\left(\frac{d_K}{p}\right) = -1$. Suppose $p\mathcal{O}_K$ is not a prime. Then $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ for some prime ideals $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathcal{O}_K$. Hence, $x^2 - xd_K - \frac{d_K - d_K^2}{4}$ also factors into two linear factors. Let them be $(x-\alpha)$ and $(x-\beta)$. Since $x^2 - xd_K - \frac{d_K - d_K^2}{4} = (x-\alpha)(x-\beta)$, we have

$$\alpha + \beta = d_K,\ \alpha\beta = -\frac{d_K - d_K^2}{4}.$$

Then

$$(\alpha - \beta)^2 = (\alpha+\beta)^2 - 4\alpha\beta = d_K^2 + 4(\frac{d_K - d_K^2}{4}) = d_K,$$

showing d_K is a square in $\mathbb{F}_p$, contradicting the assumption $\left(\frac{d_K}{p}\right) = -1$. Thus, $p\mathcal{O}_K$ cannot be factored into two primes. That is, $p\mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$. □

Back to our example in the second section. For $\mathcal{O}_K = \mathbb{Z}(\sqrt{-5})$, the discriminant $d_K = -20$. We want to find the prime factorization of (3) in $\mathcal{O}_K$. The Legendre symbol $\left(\frac{d_K}{p}\right) = \left(\frac{-20}{3}\right) = \left(\frac{1}{3}\right) = 1$. Thus $(3) = \mathfrak{p}_1\mathfrak{p}_2$ for two distinct prime ideals in $\mathbb{Z}(\sqrt{-5})$. But since $2|-20$, the ideal (2) ramifies and equals to the square of some prime ideal $\mathfrak{p}_3$. Now we have

$$\begin{aligned}
\mathcal{O}_K/(3) &= \mathbb{Z}[\sqrt{-5}]/(3) \\
&= \mathbb{Z}[x]/(x^2+5)\Big/3\mathbb{Z}[x]/(x^2+5) \\
&= \mathbb{F}_3[x]/(x^2+5) \\
&= \mathbb{F}_3[x]/(x^2-1) \\
&= \mathbb{F}_3[x]/(x+1)(x-1).
\end{aligned}$$

Hence, $(x+1)$ and $(x-1)$ are two prime ideals of $\mathbb{F}_3[x]/(x+1)(x-1)$. This corresponds to $(\sqrt{-5}+1, 3)$ and $(\sqrt{-5}-1, 3)$ being the prime ideals of $\mathcal{O}_K/(3)$. Therefore, $(\sqrt{-5}+1, 3)$ and $(\sqrt{-5}-1, 3)$ are exactly $\mathfrak{p}_1$ and $\mathfrak{p}_2$ whose product is (3). With similar methods, we will find out that $(\sqrt{-5}+1, 2)$ is the only prime ideal of $\mathcal{O}_K/(2)$, meaning $\mathfrak{p}_3 = (\sqrt{-5}+1, 2)$. Recall that $(6) = (2)\cdot(3) = (1+\sqrt{-5})\cdot(1-\sqrt{-5})$. Since $(2) = \mathfrak{p}_3^2$ and $(3) = \mathfrak{p}_1\mathfrak{p}_2$, it is natural that $(1+\sqrt{-5})$ and $(1-\sqrt{-5})$ correspond to $\mathfrak{p}_1\mathfrak{p}_3$ and $\mathfrak{p}_2\mathfrak{p}_3$. We can check that

$$\begin{aligned}
\mathfrak{p}_1\mathfrak{p}_3 &= (\sqrt{-5}+1, 3)\cdot(\sqrt{-5}+1, 2) \\
&= ((\sqrt{-5}+1)^2, 3(\sqrt{-5}+1), 2(\sqrt{-5}+1), 6) \\
&= ((\sqrt{-5}+1)^2, 3(\sqrt{-5}+1), 2(\sqrt{-5}+1), (\sqrt{-5}+1)\cdot(-\sqrt{-5}+1)) \\
&= (\sqrt{-5}+1).
\end{aligned}$$

Similarly, $\mathfrak{p}_2\mathfrak{p}_3 = (\sqrt{-5}-1)$.

5. Minkowski's Theorem

In section 3, we introduced the ideal class group $C(\mathcal{O}_K)$, which is the quotient of I_K by P_K. The size measures how far the number field is from a *Principal Ideal Domain* and in consequence gives us an idea of how ideals behave in the number field. For

example, if the ideal class group is trivial, then it means that $P_K = I_K$. That is, all the ideals in the number fields are principal. In this section, we will introduce Minkowski's Theorem, which provides a bound on the size of $C(\mathcal{O}_K)$.

Suppose K is a number field. There are $[K : \mathbb{Q}]$ number of $\mathbb{Q}$-embeddings from K to the complex field. Let r_1 denote the number of real embeddings. Since each complex embedding can be paired up with its conjugate, let $2r_2$ denote the number of complex embeddings. Then, $r_1 + 2r_2 = [K : \mathbb{Q}]$.

Theorem 5.1. *(Minkowski's bound) Suppose K is a number field of discriminant d_K. Then each element in the ideal class group $C(\mathcal{O}_K)$ can be represented by some integral ideal of norm less than or equal to*

$$M_K = \sqrt{|d_K|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}. \tag{5.2}$$

For example, $K = \mathbb{Q}(\sqrt{-5})$ is of degree 2 over $\mathbb{Q}$. The $\mathbb{Q}$-embeddings from K to the complex field are the trivial homomorphism and the conjugate homomorphism. Thus, $r_2 = 1$. The discriminant d_K equals -20 as shown previously. We calculate that

$$M_K = \sqrt{20}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n} = \sqrt{20}\left(\frac{4}{\pi}\right)\frac{2}{2^2} = 2.84\cdots < 3.$$

Hence, by Minkowski's Theorem, every element in $C(\mathcal{O}_K)$ can be represented by integral ideals of norm 1 or 2. Suppose $\mathfrak{p}$ is an ideal of norm 2. Then it is a prime ideal. (It cannot be factored into product of prime ideals as the norm function is multiplicative.) It is proved in the previous section that $(2) = \mathfrak{p}_3^2$ where $\mathfrak{p}_3 = (\sqrt{-5} + 1, 2)$. The norm of $\mathfrak{p}_3$ is 2 since $N((2)) = N(\mathfrak{p}_3)^2 = 4$. Thus, $\mathfrak{p}_3$ is the only integral ideal of norm less than or equal to the Minkowski's bound M_K. It is not a principal ideal. Therefore, the ideal class group is consisted of two elements, namely the identity and the element represented by $(\sqrt{-5} + 1, 2)$.

6. Primes Of The Form $x^2 + 5y^2$

In previous sections, we have introduced the ideal class group and ramification. However, we haven't shown why these are related to the main topic of this paper, primes of the form $x^2 + ny^2$ where n is a positive integer. This is where ramification and class field theory come in.

In the beginning of this paper, I introduced Legendre's method of using Genus Theory. The Legendre symbol in (1.1) might looks familiar to the readers, as it is the criterion for which ideals split in a ring of integers with discriminant -20 (recall Proposition 4.6). By arguments in section one, (p) splits in $\mathbb{Z}[\sqrt{-5}]$ if and only if $p \equiv 1, 3, 7, 9 \bmod 20$. That is, $(p) = \mathfrak{ab}$ for some prime ideals $\mathfrak{a}, \mathfrak{b}$. Since $N(p) = p^2 = N(\mathfrak{a})N(\mathfrak{b})$ and $\mathfrak{a}, \mathfrak{b}$ are not units, we must have $N(\mathfrak{a}) = N(\mathfrak{b}) = p$. Consider the following two cases:

(1) $\mathfrak{a}$ is a principal ideal. Then $\mathfrak{a}$ is generated by some element $a + b\sqrt{-5}$. Since the norm of $\mathfrak{a}$ is p, we have $a^2 + 5b^2 = p$.
(2) $\mathfrak{a}$ is not a principal ideal. Recall that at the end of section 5, it is shown that the class group of $\mathbb{Z}[\sqrt{-5}]$ has two elements. It suggests that $\mathfrak{a}$ times another non-principal ideal must be principal. Since $a^2 + 5b^2 = 2$ has no integer solution, any ideal $\mathfrak{p}$ of norm 2 cannot be a principal ideal. Then $\mathfrak{ap}$, an ideal of norm $2p$, is a principal ideal $(c + d\sqrt{-5})$ by argument of the size of the ideal class group. Therefore, $N(c + d\sqrt{-5}) = c^2 + 5d^2 = 2p$.

Here, notice that $c^2 + 5d^2$ is an even number, so either c and d are both even or they are both odd. Hence, we can write c as $c = d + 2k$ for some integer k. Then, the norm function becomes

$$\begin{aligned} 2p = c^2 + 5d^2 = (d+2k)^2 + 5d^2 = 4k^2 + 4dk + 6d^2, \\ \Leftrightarrow p = 2k^2 + 2dk + 3d^2. \end{aligned}$$

Notice that the two cases exactly correspond to the two reduced forms illustrated in the beginning of the section. Hence, we have proven that p can be represented by either $x^2 + 5y^2$ or $2x^2 + 2xy + 3y^2$ if p is equivalent to one of 1,3,7,9 modulo 20.

On the other hand, assume a prime p can be represented by $x^2 + 5y^2$. Since the square of an element is equivalent to either 1 or 0 modulo 4, p must be equivalent to 0 or 1 or 2 modulo 4. The cases $p \equiv 0, 2 \bmod 4$ are neglected as p is a prime (also, it's clear that $p = 2 = x^2 + 5y^2$ has no integer solution). Since the square of an element is equivalent to 0,1,4 modulo 5, p is equivalent to 0, 1, 4 modulo 5. The case $p \equiv 0 \bmod 5$ is neglected. Thus, p is equivalent to 1 or 9 modulo 20 if p can be represented by $x^2 + 5y^2$. Now assume $2p$ can be represented by $x^2 + 5y^2$ (which is equivalent to saying p can be represented by $2x^2 + 2xy + 3y^2$). Since $2p = x^2 + 5y^2$ must be even, it is equivalent to 2 modulo 4, and equivalent to 1 or 4 modulo 5. Then, we derive that p is equivalent to 3 or 7 modulo 20 if $2p$ can be represented by $x^2 + 5y^2$. Together with the above conclusion, a prime ideal (p) splits in $\mathbb{Z}[\sqrt{-5}]$ if and only if p can be represented by either $x^2 + 5y^2$ or $2x^2 + 2xy + 3y^2$. Moreover, a prime number p is of the form $x^2 + 5y^2$ if and only if $p \equiv 1$ or $9 \bmod 20$; p is of the form $2x^2 + 2xy + 3y^2$ if and only if $p \equiv 3$ or $7 \bmod 20$.

The proof is elegant because in the second case, we use the fact that the class group $C(\mathbb{Z}(\sqrt{-5}))$ has order 2. Only under this condition can we claim that the product of any two non-principal ideals is a principal ideal. By Minkowski's Theorem, as long as $M_K < 3$ and the ideal (2) ramifies in $\mathcal{O}_K$ for a number field $K = \mathbb{Q}(\sqrt{-N})$ where N a square-free positive integer, using class field theory to solve the $x^2 + Ny^2 = p$ problem will be similar to the above argument.

Below is an example where the order of $C(\mathcal{O}_K)$ is larger than 2.

Suppose our target equation is $p = x^2 + 14y^2$. Consider the ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$ of the number field $K = \mathbb{Q}(\sqrt{-14})$. Since -14 is not equivalent to 1 modulo 4, the discriminant $d_K = -56$. By Minkowski's Theorem, each element in the ideal class group $C(\mathcal{O}_K)$ can be represented by some integral ideal of norm less than or equal to

$$M_K = \sqrt{|-56|} \cdot \left(\frac{4}{\pi}\right) \cdot \frac{1}{2} < 5.$$

Thus, we only need to find all non-principal ideals of norm 2, 3 or 4. Since 2 divides the discriminant d_K, the ideal (2) ramifies. That is, $(2) = \mathfrak{p}_1^2$ for some prime ideal $\mathfrak{p}_1$ in $\mathbb{Z}[\sqrt{-14}]$. Notice that the norm of $\mathfrak{p}_1$ is 2 by the multiplicative property of the norm function. Since

$$\left(\frac{-14}{3}\right) = \left(\frac{1}{3}\right) = 1,$$

the ideal (3) splits. That is, $(3) = \mathfrak{p}_2\mathfrak{p}_3$ for some prime ideals $\mathfrak{p}_2, \mathfrak{p}_3$ of norm 3 in $\mathbb{Z}[\sqrt{-14}]$. Moreover, since $(4) = (2)^2 = \mathfrak{p}_1^4$, $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ are the only ideals that could possibly represent the elements in the ideal class group. Notice that

$$a^2 + 14b^2 = 2 \text{ and } a^2 + 14b^2 = 3$$

do not have integer solutions. This implies that there does not exist an element $\alpha \in \mathbb{Z}[\sqrt{-14}]$ such that $(\alpha) = \mathfrak{p}_i$ for $i = 1, 2, 3$. Hence, $\mathfrak{p}_i$ are non-principal ideals. Now, we want to know if any of these prime ideals are equivalent to each other in the ideal class group. By similar argument, we see that there is no principal ideal of norm 6. Thus, $\mathfrak{p}_1\mathfrak{p}_2$ or $\mathfrak{p}_1\mathfrak{p}_3$ are not the identity in the ideal class group. We have

$$\begin{aligned} \mathfrak{p}_2\mathfrak{p}_3 = (3) &\Rightarrow [\mathfrak{p}_2][\mathfrak{p}_3] = [\mathcal{O}_K] \\ &\Rightarrow [\mathfrak{p}_2] = [\mathfrak{p}_3]^{-1}. \end{aligned}$$

Moreover, since $[\mathfrak{p}_1][\mathfrak{p}_2] \neq [\mathcal{O}_K], [\mathfrak{p}_1][\mathfrak{p}_3] \neq [\mathcal{O}_K]$, the equivalence class $[\mathfrak{p}_1]$ is neither $[\mathfrak{p}_2]^{-1}$ nor $[\mathfrak{p}_3]^{-1}$, which is the same as saying

$$[\mathfrak{p}_1] \neq [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_3], [\mathfrak{p}_1] \neq [\mathfrak{p}_3]^{-1} = [\mathfrak{p}_2].$$

As for $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$, if $[\mathfrak{p}_2]$ is equivalent to $[\mathfrak{p}_3]$, then

$$[\mathfrak{p}_2] = [\mathfrak{p}_3] = [\mathfrak{p}_2]^{-1} \Rightarrow [\mathfrak{p}_2]^2 = [\mathcal{O}_K].$$

This means that $\mathfrak{p}_2^2$ is a principal ideal (β) for some $\beta \in \mathbb{Z}[\sqrt{-14}]$. The norm of (β) is 9. However, the equation

$$a^2 + 14b^2 = 9$$

only admits two solutions, corresponding to $\beta = \pm 3$. Since $(3) = \mathfrak{p}_2\mathfrak{p}_3$, and the prime factorization of an ideal is unique in a Dedekind domain, $(3) = (-3) \neq \mathfrak{p}_2^2$. In consequence, $[\mathfrak{p}_2]$ is not equivalent to $[\mathfrak{p}_3]$ in the ideal class group. Therefore, the ideal class group $C(\mathbb{Z}[\sqrt{-14}])$ has four elements, namely $e, [\mathfrak{p}_1], [\mathfrak{p}_2], [\mathfrak{p}_3]$. Moreover, since the order of both $\mathfrak{p}_2$ and $\mathfrak{p}_3$ is not 2, the ideal class group is isomorphic to Z_4.

For a prime number p, (p) splits in $\mathbb{Z}[\sqrt{-14}]$ if and only if the Legendre symbol $(\frac{-56}{p}) = 1$. Since

$$\left(\frac{-56}{p}\right) = \left(\frac{-14}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) \cdot \left(\frac{7}{p}\right),$$

we consider the following cases:

(1) $p \equiv 1 \bmod 8$.

$$\left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) \cdot \left(\frac{7}{p}\right) = \left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = 1 \tag{6.1}$$

if and only if $p \equiv 1, 2, 4 \bmod 7$. This leads to $p \equiv 1, 9, 25 \bmod 56$.

(2) $p \equiv 3 \bmod 8$.

$$\left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) \cdot \left(\frac{7}{p}\right) = \left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right) = 1 \tag{6.2}$$

if and only if $p \equiv 3, 5, 6 \bmod 7$. This leads to $p \equiv 3, 19, 27 \bmod 56$.

(3) $p \equiv 5 \bmod 8$.

$$\left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) \cdot \left(\frac{7}{p}\right) = -\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right) = 1 \tag{6.3}$$

if and only if $p \equiv 3, 5, 6 \bmod 7$. This leads to $p \equiv 5, 13, 45 \bmod 56$.

(4) $p \equiv 7 \bmod 8$.

$$\left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) \cdot \left(\frac{7}{p}\right) = -\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = 1 \tag{6.4}$$

if and only if $p \equiv 1, 2, 4 \bmod 7$. This leads to $p \equiv 15, 23, 39 \bmod 56$.

Since (p) splits for these cases, that is, $(p) = \mathfrak{ab}$ for some distinct prime ideals $\mathfrak{a}, \mathfrak{b} \in \mathbb{Z}[\sqrt{-14}]$, the norm of $\mathfrak{a}$ and $\mathfrak{b}$ are p. We examine whether or not $\mathfrak{a}$ is a principal ideal and have the following cases as in the previous example:

(1) Suppose $\mathfrak{a} = (\alpha)$ for some $\alpha = x + y\sqrt{-14} \in \mathbb{Z}[\sqrt{-14}]$ is principal. Then, since $N(\mathfrak{a}) = p = N(\alpha)$, we have $x^2 + 14y^2 = p$.

(2) Suppose $\mathfrak{a}$ is non-principal. Then in the ideal class group, $\mathfrak{a}$ can be represented by one of $\mathfrak{p}_1, \mathfrak{p}_2$ or $\mathfrak{p}_3$.

   (a) Suppose $\mathfrak{a}$ can be represented by $\mathfrak{p}_1$. Since the equivalence class $[\mathfrak{p}_1]^2$ is equal to $[\mathcal{O}_K]$, $\mathfrak{ap}_1$ is a principal ideal. Similar to the argument in (1), the norm of $\mathfrak{ap}_1$ is in the form of $x^2 + 14y^2$. Thus, $N(\mathfrak{ap}_1) = N(\mathfrak{a})N(\mathfrak{p}_1) = 2p = x^2 + 14y^2$. This means $x = 2m$ (for some integer m) is an even number. Then, $p = 2m^2 + 7y^2$.

   (b) Suppose $\mathfrak{a}$ can be represented by $\mathfrak{p}_2$ (respectively $\mathfrak{p}_3$). In consequence, $\mathfrak{ap}_3$ (resp. $\mathfrak{ap}_2$) is a principal ideal, implying $N(\mathfrak{ap}_3) = 3p$ (resp. $N(\mathfrak{ap}_2) = 3p$) is of the form $x^2 + 14y^2$. Since 3 divides $x^2 + 14y^2$, we must have either $x \equiv y \equiv 0 \bmod 3$ or $x \equiv y \equiv 1 \bmod 3$. However, if $x \equiv y \equiv 0$, 3 becomes a divisor of p, contradicting p is a prime. Thus, $x \equiv y \equiv 1 \bmod 3$. Then, we can write $x = 3m+1, y = 3n+1$ for some integers m, n. The expression then becomes

$$\begin{aligned} & 3p = (3m+1)^2 + 14(3m+1)^2 \\ \Leftrightarrow\ & p = 3m^2 + 2m + 5 + 42n^2 + 28n \\ \Leftrightarrow\ & p = 3(m-n)^2 + 2(m-n)(3n+1) + 5(3n+1)^2 \\ \Leftrightarrow\ & p = 3(n-m)^2 - 2(n-m)(3n+1) + 5(3n+1)^2. \end{aligned}$$

   Therefore, p is of the form $3x^2 \pm 2xy + 5y^2$.

The three cases listed above exactly correspond to the three reduced quadratic forms of discriminant -56 in Genus Theory.

Suppose in case (1), $p = x^2 + 14y^2$. Then, p is equivalent to x^2 modulo 7. In other words, the Legendre symbol $(\frac{p}{7}) = 1$. Since p is odd, x must also be odd. Then, x is equivalent to 1 modulo 8. Thus, p is equivalent to 1 or 7 modulo 8, corresponding to y being even or odd. This is exactly described by (6.1) and (6.4) above. Therefore, $p = x^2 + 14y^2$ implies p is equivalent to $1, 9, 15, 23, 25, 39$ modulo 56.

Similarly, suppose case (2)(a) is true, that is, $p = 2x^2 + 7y^2$. Then p is equivalent to $2x^2$ modulo 7. Since y must be odd, $7y^2$ is equivalent to 7 modulo 8, resulting in $p \equiv 1$ or 7 mod 8. This case coincides with the case $p = x^2 + 14y^2$, leading to p being equivalent to $1, 9, 15, 23, 25, 39$ modulo 56.

Now for the third case where $p = 3x^2 \pm 2xy + 5y^2$, or, $3p = x^2 + 14y^2$, we have $3p \equiv x^2 \bmod 7$ and $3p \equiv 1$ or 7 mod 8. Hence, p is equivalent to $2, 3$ or 5 modulo 7, and 3 or 5 modulo 8. This corresponds to cases (6.2) and (6.3), which implies p is equivalent to $3, 5, 13, 19, 27, 45$ modulo 56.

In summary, for an odd prime p,

$$\begin{aligned} \begin{cases} p = x^2 + 14y^2 \\ p = 2x^2 + 7y^2 \end{cases} \quad &\Leftrightarrow \quad p \equiv 1, 9, 15, 23, 25, 39 \bmod 56 \\ p = 3x^2 \pm 2xy + 5y^2 \quad &\Leftrightarrow \quad p \equiv 3, 5, 13, 19, 27, 45 \bmod 56. \end{aligned}$$

Acknowledgments

It's a pleasure to thank my mentor, Billy Lee, for being so inspiring, patient and resourceful when introducing me to class group theory and guiding me through this project. I would also like to thank professor May for organizing such an amazing REU program during this difficult pandemic period. Without him and all the fantastic instructors, this summer would never be so rewarding.

7. bibliography

References

[1] David A. Cox. Primes of the Form $x^2 + ny^2$. John Wiley & Sons, Inc., 2013.
[2] Serge Lang, Algebraic Number Theory, Springer-Verlag, Berlin, Heidelberg, and New York, 1986.
[3] D. Marcus, Number Fields, Springer-Verlag, Berlin, Heidelberg, and New York, 1977.
[4] J. Neukirch. Algebraic Number Theory. Springer-Verlag, Berlin, Heidelberg, and New York, 1999.