# AN INTRODUCTION TO GENUS THEORY AND PRIMES OF THE FORM $x^2 + ny^2$

AAHANA JAIN

**Abstract**

This is an expository paper on primes of the form $x^2 + ny^2$. We will start with the most basic case, then study Genus Theory to understand Quadratic Forms by sketching out examples. We will look at the Form Class Group and the Ideal Class Group and Quadratic Fields to see how it is related to the question at hand.

# Contents

**1 Important identities and properties** **3**

**2 Quadratic Reciprocity** **4**

2.1 Euler's Descent and Reciprocity steps . . . . . 4

2.2 Quadratic Reciprocity . . . . . 4

**3 Quadratic Forms** **5**

3.1 Primitve, reduced forms . . . . . 6

**4 Genus Theory** **9**

4.1 Genus Theory . . . . . 9

4.2 The Form Class Group . . . . . 13

**5 Examples of negative discriminant** **20**

5.1 $D = -495$ . . . . . 20

5.2 $D = -256$ . . . . . 20

5.3 $D = -40$ . . . . . 21
5.4 $D = -103$ . . . . . 21
5.5 $D = -2044$ . . . . . 22
5.6 $D = -3072$ . . . . . 22
5.7 $D = -111$ . . . . . 22
5.8 $D = -5120$ . . . . . 22
5.9 $D = -7007$ . . . . . 23

**6 Class Field Theory** **25**

6.1 Ring Theory: Pre-requisites . . . . . 25
6.2 Ideal Class Group . . . . . 29
6.3 Basic Ramification Theory . . . . . 33
6.4 Quadratic Fields . . . . . 34

# 1 Important identities and properties

1. $(a^2+b^2)(c^2+d^2) = (ac \pm bd)^2 + (ad \mp bc)^2$
2. $(x^2+ny^2)(z^2+nw^2) = (xz \pm nyw)^2 + n(xw \mp yz)^2$
3. Properties of the Legendre symbol:
   - $\left(\frac{MN}{m}\right) = \left(\frac{M}{m}\right)\left(\frac{N}{m}\right)$
   - $\left(\frac{M}{mn}\right) = \left(\frac{M}{m}\right)\left(\frac{M}{n}\right)$
4. Jacobi symbol: $\left(\frac{M}{m}\right) = \prod_{i=1}^{r}\left(\frac{M}{m_i}\right)$ and its properties:
   - $\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2}$
   - $\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}$
   - $\left(\frac{M}{m}\right) = (-1)^{(M-1)(m-1)/4}\left(\frac{m}{M}\right)$
   - **If $m \equiv n$ mod D, where m and n are odd positive and $D \equiv 0, 1$ mod 4, then**
     $$\left(\frac{D}{m}\right) = \left(\frac{D}{n}\right)$$

# 2 Quadratic Reciprocity

## 2.1 Euler's Descent and Reciprocity steps

We will start with the representation of an odd prime $x^2+ny^2$. The study of these forms resulted in the development of some interesting and important concepts in Number Theory. For instance, Euler discovered quadratic reciprocity through the manner of his proofs.

**Theorem 2.1.1** An odd prime $p$ can be written as the sum of two squares iff $p \equiv 1 \bmod 4$.

*Proof:* ($\Rightarrow$) Given $p = x^2 + y^2$, it is easy to prove $p \equiv 1 \bmod 4$ using congruence theory.

($\Leftarrow$) Given $p \equiv 1 \bmod 4$, we can prove that p can be written as the sum of two squares by proving the following steps (as written by Euler):

- Reciprocity step - If a prime $p = 1 \bmod 4$, $N = a^2 + b^2$, $gcd(a, b) = 1$, then $p|N$.
- Descent step - If $p|x^2+y^2$ and $gcd(x, y) = 1$, then p can be written as $x^2+y^2$.

## 2.2 Quadratic Reciprocity

We first begin with defining the Legendre symbol: Let $p$ be an odd prime number. An integer $a$ is a quadratic residue of $p$ if there is an integer x such that

$$a \equiv x^2 \pmod{p}$$

The Legendre Symbol $\left(\frac{a}{p}\right)$ is as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv p \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

This allows us to redefine $p \mid x^2 + y^2$ as follows:

**Lemma 2.2.1** Let n be a nonzero integer, p be an odd prime number such that $p \nmid n$. Then,

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

*Proof:* ($\Leftarrow$): $\left(\frac{-n}{p}\right) = 1 \Rightarrow x^2 \equiv -n \mod p \Rightarrow x^2 + n \cdot \frac{1}{2} \equiv 0 \mod p \Rightarrow p | x^2 + n \cdot \frac{1}{2}$.

($\Rightarrow$): $x^2 + ny^2 \equiv 0 \mod p$ and $\gcd(x, y) = 1$. Then $p|y$ implies $p|x$, impossible by $\gcd(x, y) = 1$. Thus $y$ is invertible modulo $p$, say $yz \equiv 1 \mod p$. Multiplying both sides of $x^2 + ny^2 \equiv 0 \mod p$ by $z^2$ gives $(xz)^2 + n \equiv 0 \mod p$, or $(xz)^2 \equiv -n \mod p$, so $\left(\frac{-n}{p}\right) = 1$.

# 3 Quadratic Forms

Quadratic forms are polynomials with the degree of each term being two. The most elementary quadratic form in two variables is

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

and this is **primitive** if all coefficients (a, b, c) are relatively prime.

## 3.1 Primitve, reduced forms

If $m = f(x, y)$ and gcd(x, y) = 1, then m is **properly represented** by f(x, y).

**Definition 3.1.1** If there exist integers $p, q, r, s$ such that $f(x, y) = g(px + qy, rx + sy)$ and $ps - qr = \pm 1$, then f(x, y) and g(x, y) are equivalent.

- $ps - qr = 1 \rightarrow$ proper equivalence.
- $ps - qr = -1 \rightarrow$ improper equivalence.

In other words, f and g are equivalent if $\exists\ A \in SL_2(\mathbb{Z})$ s. t. for

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$$

it holds that $g(x, y) = f(x', y')$.

Define discriminant $D$ of $f$ as $D = b^2 - 4ac$ and $D'$ of $g$. Then if $f$ and $g$ are equivalent, $D = (ps - qr)^2 D' \rightarrow D$ is constant in each equivalence class.

**Lemma 3.1.2** $f(x, y)$ properly represents an integer $m$ iff $f(x, y)$ is properly equivalent to the form $mx^2 + bxy + cy^2$ for $b, c \in \mathbb{Z}$.
*Proof:* Suppose that $f(p, q) = m$, where $p$ and $q$ are relatively prime. We can find integers $r$ and $s$ so that $ps - qr = 1$. If $f(x, y) = ax^2 + bxy + cy^2$, then,

$f(px + ry, qx + sy) = f(p, q)x^2 + (2apr + bps + brq + 2cqs)xy + f(r, s)y^2 = mx^2 + Bxy + Cy^2$ is of the desired form.

To prove the converse, note that $mx^2 + Bxy + Cy^2$ represents $m$ properly by taking $(x, y) = (1, 0)$.

**Lemma 3.1.3** Let $D \equiv 0, 1 \pmod 4$, $m$ be an odd integer relatively prime to $D$.

Then $m$ is properly represented by a primitive form of discriminant $D$ iff $D$ is a quadratic residue modulo $m$.
*Proof:* If $f(x, y)$ properly represents $m$, then by Lemma 4.1.2, we may assume that $f(x, y) = mx^2 + bxy + cy^2$. Thus $D = b^2 - 4mc$, and $D \equiv b^2 \mod m$ follows easily.

Conversely, suppose that $D \equiv b^2 \mod m$. Since $m$ is odd, we can assume that $D$ and $b$ have the same parity (replace $b$ by $b + m$ if necessary), and then $D \equiv 0, 1 \mod 4$ implies that $D \equiv b^2 \mod 4m$. This means that $D = b^2 - 4mc$ for some $c$. Then $mx^2 + bxy + cy^2$ represents $m$ properly and has discriminant $D$, and the coefficients are relatively prime since $m$ is relatively prime to $D$.

**Corollary 3.1.4** Let n be an integer and odd prime $p \nmid n$. Then $(-n/p) = 1$ iff $p$ is represented by a primitive form of discriminant $-4n$.

*As a result of this, any prime $p$ can be represented as $x^2 + ny^2$ (where $p \nmid n$), if* $\left(\frac{-n}{p}\right) = 1$.

To improve this corollary, a simple form has to be equivalent to every form corresponding to a discriminant. For this, define a primitive positive definite (definite forms are all of the same sign) form $f(x, y)$ to be *reduced* if

$$-|a| < b \leq |a| < |c|$$

or if

$$0 \leq b \leq |a| = |c|$$

**Theorem 3.1.5** Every primitive positive definite form is properly equivalent to a unique reduced form.
Following are some interesting results that come from the proof (see Cox [1, Theorem 2.8] of this theorem:

- The two forms $ax^2 \pm bxy + cy^2$ are properly equivalent.
- $f(x, y) \geq (a - |b| + c)\ \min(x^2, y^2)$, implying the following (Legendre's) observations:
  - a is the smallest nonzero value of $f(x, y)$
  - If $a < c$, c is the next smallest nonzero value of $f(x, y)$
  - Hence, the outer coefficients of a reduced form give the minimum values properly represented by any equivalent form.
- If f is a reduced form following the strict inequalities $|b| < a < c$, then
  - f(x, y) = a, gcd(x, y) = 1 $\Leftrightarrow (x, y) = \pm(1, 0)$
  - f(x, y) = c, gcd(x, y) = 1 $\Leftrightarrow (x, y) = \pm(0, 1)$
- $f(x, y) = g(x, y)$ if the forms are properly equivalent.

Suppose $ax^2 + bxy + cy^2$ is a *reduced* form of discriminant $D < 0$. Then $b^2 \leq a^2$, $a \leq c$,

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

Hence, $a \leq \sqrt{(-D/3)}$

**Observation:** $x^2 + ny^2$ is always a reduced form.

**Theorem 3.1.6** Denote the no. of classes of primitive positive definite forms of Discriminant $D$ as $h(D)$. Let $D < 0$ be fixed. Then, $h(D)$ is finite and equals the number of reduced forms of discriminant D.

# 4 Genus Theory

Genus Theory helps us classify binary quadratic forms into classes that represent certain values from $(\mathbb{Z}/D\mathbb{Z})^*$. All forms in a genus of the form discriminant D represent the same set of values modulo D.

In general, if the discriminant is of the form $D = -4n$, for an odd prime p not dividing D, $\left(\frac{-n}{p}\right) \iff$ a set of values from $(\mathbb{Z}/D\mathbb{Z})^*$, which are further classified to tell which genus represents which values.

**Example 4.1:** Consider $n = 14$. We have,

$$\left(\frac{-14}{p}\right) = 1 \iff p \equiv 1, 3, 4, 9, 13, 15, 19, 23, 25, 27, 39, 45$$

(mod 56). We can confirm this by calculating the Jacobi symbol for each p.

The reduced forms corresponding to discriminant $D = -56$ are $x^2 + 14y^2, 2x^2 + 7y^2, 3x^2 + 2xy + 5y^2, 3x^2 - 2xy + 5y^2$. We classify these four reduced forms into their respective genus (equivalence classes) as follows:

$$x^2 + 14y^2, 2x^2 + 7y^2 \text{ represent } p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}.$$
$$3x^2 \pm 2xy + 5y^2 \text{ represent } p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}.$$

We will study Genus Theory to understand these equivalence classes better.

## 4.1 Genus Theory

**Lemma 4.1.1:** If a nonzero integer $D \equiv 0, 1 \bmod 4$, There is a unique homomorphism $\chi : (\mathbb{Z}/D\mathbb{Z}) \to \pm 1$ such that $\chi([p]) = (D/p)$ for odd primes $p \nmid D$.
**Proof:** $\left(\frac{D}{m}\right) = \left(\frac{D}{n}\right)$ If $m \equiv n)$ mod D. Therefore, $\chi$ is a well-defined function as we can choose a representative $[m]$ such that it is odd and positive. The multiplicative properties of the Jacobi symbol show that it is a group homomor-

phism:

$$\chi([m])\chi([m']) = \left(\frac{D}{m}\right)\left(\frac{D}{m'}\right) = \left(\frac{D}{mm'}\right) = \chi([mm'])$$

**Theorem 4.1.2:** For an odd prime p not dividing $D$, $[p] \in ker(\chi)$ if and only if p is represented by one of the $h(D)$ reduced forms of discriminant $D$.

**Proof:** $[p] \in ker(\chi)$ if $(D/p) = 1$, which is equivalent to being represented by a form of discriminant D by the following Lemma:

**Lemma 4.1.3:** Let $D \equiv 0, 1 \pmod 4$ be an integer and $m$ be an odd integer relatively prime to $D$. Then $m$ is properly represented by a primitive form of $D$ if and only if $D$ is a quadratic residue modulo $m$:

**Proof:** ($\Rightarrow$) Since $f(x, y)$ properly represents m, then f can be written as $f(x, y) = mx^2 + bxy + cy^2$.

$$D = b^2 - 4mc \equiv b^2 \bmod m$$

Hence, $D$ is a quadratic residue modulo $m$.

($\Leftarrow$) Since $D$ is a quadratic residue modulo $m$, $D \equiv b^2$ mod m. Since m is odd, $D$ and $b$ have the same parity. Then $D \equiv 0, 1$ mod 4 implies $D \equiv 0, 1 \pmod{4m}$.

**Lemma 4.1.4:** Given a form $f(x, y) = (a, b, c)$ and an integer $M$, then $f(x, y)$ properly represents at least one number relatively prime to $M$.

**Proof:** Given a prime p, at least one of $f(1, 0), f(0, 1), f(1, 1)$ is prime to $p$. If both $f(1, 0) = a$ and $f(0, 1) = c$ is not prime to p, then $f(1, 1) = a + b + c$ must be prime to p as otherwise b is not prime to be, and $gcd(a, b, c) \neq 1 \rightarrow$ contradiction.

Now let the prime factors of M be $p_1, ..., p_r$. We can choose $(x_i, y_i) = (1, 0), (0, 1)$, or $(1, 1)$ such that $f(x_i, y_i) \not\equiv 0 \bmod p_i$. By the Chinese Remainder Theorem,

there are integers $x$ and $y$ such that $x \equiv x_i \bmod p_i$ and $y \equiv y_i \bmod p_i$ for all $i$. Then, for each $i$,

$$f(x, y) \equiv f(x_i, y_i) \not\equiv 0 \bmod p_i$$

**Lemma 4.1.5** The values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by the principal form of discriminant D form a subgroup $H \subset ker(\chi)$.

**Proof:** First we show that $H \subset ker(\chi)$. Let m be the number that is represented by a form of D, and m be prime to D. We can write $m = d^2m'$, where $m'$ is properly represented by $f(x', y')$. Then $\chi(m) = \chi(d^2m') = \chi(d)^2\chi(m') = \chi(m')$. Hence, we may assume m is properly represented by a form of D, which implies D is a quadratic residue modulo m and hence $[m] \in Ker(\chi)$.

1. **m is odd:** We can use the Jacobi symbol:

$$\chi([m]) = \left(\frac{D}{m}\right) = \left(\frac{b^2 - km}{m}\right) = \left(\frac{b^2}{m}\right) = \left(\frac{b}{m}\right)^2 = 1$$

2. **m is even:** We can write $m$ as $2m'$. Since $m$ is properly represented by a form of $D$, $f$ is equivalent to a form $f(x, y) = 2m'x^2 + bxy + cy^2$. Then discriminant $D = b^2 - 8m'c \Rightarrow D \equiv b^2 \Rightarrow D \equiv 1 \bmod 8$ (as D is odd). We know that $\chi([2]) = \left(\frac{2}{D}\right) = (-1)^{D^2-1}/8 = 1$. Let $m = 2^k$. Then

$$\chi([m]) = \chi([2])^k\chi([r]) = \chi([r])$$

Then, we show that H is closed under multiplication. For this, there are two cases:

1. $D \equiv 0$ **(mod 4):** Let $D = -4n$. Then the principal form of F is $x^2 + ny^2$. From the following, we can see that f is closed under multiplication:

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

2. $D \equiv 1$ **(mod 4):** The principal form is $x^2 + xy + \frac{1-D}{4}y^2$. Notice that

$$4(x^2 + xy + \frac{1-D}{4}y^2) \equiv (2x+y)^2 \text{ mod D.}$$

As $D$ is odd, 2 is invertible, i.e. $\exists r$ such that $2r \equiv 1$ (mod D). Hence, $x^2 + xy + \frac{1-D}{4}y^2 \equiv r^2(2x+y)^2 \equiv (2rx+ry)^2 \equiv (x+ry)^3$ mod D.
By setting y as 0 and letting x go from 1 to $D-1$, we see that $H$ is exactly the set of squares modulo $D$.

**Lemma 4.1.6:** The values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by $f(x,y)$ form a coset of $H$ in $ker(\chi)$.

**Proof:** Any primitive form $f(x,y)$ can represents at least one integer $m$ relatively prime to a given integer M (Lemma). Thus, let $f(x,y) = ax^2+bxy+cy^2$ represent some integer $m$ prime to $D$, so that it is properly equivalent to $g(x,y) = mx^2 + b'xy + c'y^2$. Hence, we may take a form f such that $a$ is prime to D. Since

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

(as H is the set of squares modulo $D$). Now we consider two cases:

1. $D \equiv 0$ **(mod 4):** Let $D = -4n$. Hence $a$ is odd and $b$ is even, so we can write $b = 2b'$. Then,

$$af(x,y) = (ax+b'y)^2 + ny^2$$

This is essentially the principal form of D and hence $\in H$. As $a$ is relatively prime to D and hence 4n, the values of $f$ in $(\mathbb{Z}/D\mathbb{Z})^*$ lie in the coset $[a]^{-1}H$.

2. $D \equiv 1$ **(mod 4):** Since $D$ is odd and relatively prime to a, 4a is invertible in $(\mathbb{Z}/D\mathbb{Z})^*$. Say $4at \equiv 1$ (mod D) $\in H$. Then $4a \in tH$. $(2ax+by)^2$ ranges over all values in H (since D is odd, b is also odd and $gcd(2a,b) = 1) \Rightarrow f$ assumes values that are the cosets of H.

**Definition 4.1.7:** The *genus* of $H'$ consists of all forms of discriminant $D$ which represent the values of $H'$ modulo $D$.

## 4.2 The Form Class Group

Let's define the Class Group, which forms a group under Dirichlet composition. First, we have the following lemma:

**Lemma 4.2.1:** Assume that f(x,y) = $ax^2+bxy+cy^2$ and g(x,y) = $a'x^2+b'xy+c'y^2$ have discriminant D and satisfy $gcd(a, a', (b + b')/2) = 1$ Then there is a unique integer B modulo 2aa' such that

$$B \equiv b \bmod 2a$$
$$B \equiv b' \bmod 2a'$$
$$B^2 \equiv D \bmod 4aa'$$

**Proof:** $B \equiv b \bmod 2a \Rightarrow B \equiv b \bmod a \Rightarrow B^2 \equiv b^2 \bmod a \Rightarrow B^2 \equiv D \bmod a$. Similarly, $B^2 \equiv D \bmod a'$. Therefore, $B^2 \equiv D \bmod aa'$

**Dirichlet composition:** With the above conditions, the composition of two forms $f(x, y)$ and $g(x, y)$ is the form $F(x, y) = aa'x^2+Bxy+\frac{B^2-D}{4aa'}y^2$. Following are its basic properties:

- $F(x, y)$ is a primitive positive definite form of discriminant D.
- F is a direct composition of $f(x, y)$ and $g(x, y)$.

**Theorem 4.2.2** Let negative $D \equiv 0, 1 \bmod 4$. Define $C(D)$ = set of classes of primitive positive definite forms of discriminant D. Then,

- $C(D)$ is a finite abelian group (called the Class Group) with the (well-defined) binary operation as Dirichlet composition and order = $h(D)$ (Class number).

- The identity element of $C(D)$ is the class containing the principal form.
- The inverse of the class containing $ax^2 + bxy + cy^2$ is the class containing $ax^2 - bxy + cy^2$ (also called opposite).

**Proof:**

1. **Well-defined binary operation:** Let $f = (a, b, c)$ and $g$ be two forms of the given type. $g$ can be properly equivalent to a form that properly represents an integer $a'$ relatively prime to $a$. Hence, the gcd condition is satisfied and this way Dirichlet composition is defined for any two such operations.

2. **Identity:** The principal form is the identity. Consider its composition with a form $f(x, y) = a'x^2 + b'xy + c'y^2$. It's leading coefficient $a = 1$ satisfies the gcd condition. Therefore, Dirichlet composition is defined. Clearly, B = b' is a solution of the congruences: ($b = 0$ if $D \equiv 0 \pmod 4$, $b = 0$ if $D \equiv 0 \pmod 4$)

   $$B \equiv b \pmod 2;\ B \equiv b' \pmod{2a'};\ B^2 \equiv D \pmod{4a'}$$

   The composition $F(x, y)$ then reduces to $f(x, y)$.

3. **Inverse:** The inverse of $(a, b, c)$ is $(a, -b, c) \sim (c, b, a)$. Since we are dealing with primitve forms, $gc(a, b, c) = 1$. We can apply Dirichlet's composition and B = b satisfies the necessary congruence conditions. The composed form is $F(x, y) = acx^2 + bxy + y^2$, which is equivalent to the principal form:

   (a) **b is even:** Say $b = 2B$. Let $x \mapsto -y, y \mapsto x + By$:

   $$ac(-y)^2 + 2B(-y)(x + By) + (x + By)^2 = x^2 + (ac - B^2)y$$

   (b) **b is odd:** Say $b = 2B + 1$. Let $x \mapsto -y, y \mapsto x + (B + 1)y$:

   $$ac(-y)^2+(2B+1)(-y)(x+(B+1)y)+(x+(B+1)y)^2 = x^2+xy(ac-B-B^2)y$$

4. **Associative:** First we will look at the composition $(f_1 \cdot f_2) \cdot f_3$. Consider the following three forms all with discriminant D:

$$f_1 = (a_1, b_1, c_1); f_2 = (a_2, b_2, c_2); f_3 = (a_3, b_4, c_3)$$

Now, let $B_1$ be such that:

$$B_1 \equiv b_1 \pmod{2a_1};$$
$$B_1 \equiv b_2 \pmod{2a_2};$$
$$B_1^2 \equiv D \pmod{4a_1a_2}$$

Then the composition $f_1 \cdot f_2 = F_1 = a_1a_2x^2 + B_1xy + \dfrac{B_1^2 - D}{4a_1a_2}y^2$.

Let $B_2$ satisfy:

$$B_2 \equiv b_3 \pmod{2a_3};$$
$$B_2 \equiv B_1 \pmod{2a_1a_2};$$
$$B_2^2 \equiv D \pmod{4a_1a_2a_3}$$

Then $(f_1 \cdot f_2) \cdot f_3 = F_2 = (a_1a_2a_3, B_2, \dfrac{B_2^2 - D}{4a_1a_2a_3})$.

Now, let's look at the composition $f_1 \cdot (f_2 \cdot f_3)$.

let $B_3$ be such that:

$$B_3 \equiv b_2 \pmod{2a_2};$$
$$B_3 \equiv b_3 \pmod{2a_3};$$
$$B_3^2 \equiv D \pmod{4a_2a_3}$$

Then the composition $f_1 \cdot f_2 = F_3 = a_2a_3x^2 + B_3xy + \dfrac{B_3^2 - D}{4a_2a_3}y^2$.

Let $B_4$ satisfy:

$$B_4 \equiv b_1 \pmod{2a_1};$$
$$B_4 \equiv B_3 \pmod{2a_2a_3};$$
$$B_4^2 \equiv D \pmod{4a_1a_2a_3}$$

Then $(f_1 \cdot f_2) \cdot f_3 = F_4 = (a_1a_2a_3, B_4, \dfrac{B_4^2 - D}{4a_1a_2a_3})$.

For associativity to hold, we have to check if $F_2 = F_4 \iff B_2 = B_4$, which can be seen from the aforementioned congruences.

**Commutative:** As Dirichlet composition is symmetric, the group is Abelian.

**Theorem 4.2.3:** Consider the map sending each equivalence class of $C(D)$ to the set of values it represents:

$$\Phi : C(D) \to Ker(\chi)/H$$

This is a group homomorphism.

**Proof:** Let $f$ and $g$ be two forms of discriminant D. As seen before, any two forms of $D$ can be composed by Dirichlet composition (the resultant is, say, $F$). Then $F$ represents values that are a product a product of the values represented by $f$ and $g$. Hence, $\Phi(F) = H'H''$.

**Genera:** Each fibre $\Phi^{-1}(H') for H' \in Ker(\chi)/H$ consists of all classes of forms of the genus of $H'$.

**Corollary 4.2.4:** Let $D$ be a discriminant. Then,

1. All genera of forms of discriminant $D$ consist of the same number of classes.
2. The number of genera is a power of 2.

**Proof:**

1. It is a standard fact in group theory that all 'fibres' (preimages $\Phi^{-1}(x), x \in Im(\Phi)$) contain the name number of elements. The fibre $\Phi^{-1}(x)$ coset of $ker(\Phi) = \Phi^{-1}(0)$. Since all cosets have the same cardinality, all genera consist of the same number of elements.

2. The group is abelian and consists only of elements whose square is the identity ($(+1)^2 = (-1)^2 = +1$)). Thus every element in $ker(\chi)/H$ has order $\leq 2$. From the structure theorem for finite Abelian groups, $ker(\chi)/H \simeq \pm 1^m$.

**Theorem 4.2.5:** Let $D \equiv 0, 1 \pmod 4$ be negative, and let $r$ be the number of odd primes dividing $D$. Define the number $\mu$ as follows:

1. $D \equiv 1$ **(mod 4):** $\mu = r$.
2. $D \equiv 0$ **(mod 4):**
   - $\mu = r$; $n \equiv 3 \pmod 4$
   - $\mu = r + 1$; $n \equiv 1, 2 \pmod 4$
   - $\mu = r + 1$; $n \equiv 4 \pmod 8$
   - $\mu = r + 1$; $n \equiv 0 \pmod 8$

Then,

1. There are $2^{\mu-1}$ genera of forms of discriminant D.
2. The principal genus (the genus containing the principal form) consists of the classes in $C(D)^2$, the subgroup of squares in the class group $C(D)$. Thus every form in the principal genus arises by duplication.

**Proof:** First, we define certain assigned characters. Let $p_1, ..., p_r$ be the distinct odd primes dividing D.

- $\chi_i(a) = \left(\frac{a}{p_i}\right)$; defined for $a$ prime to $p_i, i = 1, ..., r$.
- $\delta(a) = \left(\frac{-1}{a}\right)$; defined for $a$ odd
- $\epsilon(a) = \left(\frac{2}{a}\right)$; defined for $a$ odd

Then, the assigned characters are as follows: (The number of characters is the same as $\mu$).

| $n$ | assigned characters |
|---|---|
| $n \equiv 3 \bmod 4$ | $\chi_i$ |
| $n \equiv 1 \bmod 4$ | $\chi_i, \delta$ |
| $n \equiv 2 \bmod 8$ | $\chi_i, \delta\epsilon$ |
| $n \equiv 6 \bmod 8$ | $\chi_i, \epsilon$ |
| $n \equiv 4 \bmod 8$ | $\chi_i, \delta$ |
| $n \equiv 0 \bmod 8$ | $\chi_i, \delta, \epsilon$ |

From this, we get the following lemma:

**Lemma 4.2.6:** The homomorphism $\Psi : (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}^\mu$ is surjective, and its kernel is the subgroup $H$ of values represented by the principal form. Thus,

$$(\mathbb{Z}/D\mathbb{Z})^*/H \simeq \{\pm 1\}^\mu$$

Continuing the proof of the theorem:

1. $ker(\chi)$ has index 2 in $(\mathbb{Z}/D\mathbb{Z})^*$ from the first isomorphism theorem. Hence, with $H = ker(\chi)$ in Lemma 3.6, $(\mathbb{Z}/D\mathbb{Z})^*/H \simeq \{\pm 1\}^{\mu-1}$ and the order of $ker(\chi)/H$ is $2^{\mu-1}$, which is the number of genera.

2. Let $C = C(D)$. Since $\Phi : C \to ker(\chi)/H \simeq \{\pm 1\}^{\mu-1}$ is a homomorphism, $C^2 \subset ker(\Phi)$ and we have the induced map

   $$C/C^2 \to \{\pm 1\}$$

   Then, as done earlier, $C/C^2$ has elements $\leq 2$ in $C$, so it has order $2^{\mu-1}$. As $\Phi$ is surjective and both sides of the map have same order, $\Phi$ is an isomorphism.

Now, we can look at Example 4.1 in a different manner:

**Example 4.2.7** Consider $D = -56$. $56 = 2^3 \cdot 7$, hence its assigned characters are $\left(\frac{-1}{a}\right)$, $\left(\frac{2}{a}\right)$ and $\left(\frac{a}{7}\right)$. Following are its genera of forms:

| $\left(\frac{-1}{a}\right)$ | $\left(\frac{2}{a}\right)$ | $\left(\frac{a}{7}\right)$ | $((\mathbb{Z}/D\mathbb{Z})^*$ | Forms represented |
|---|---|---|---|---|
| 1 | 1 | 1 | [1, 9, 15, 23, 25, 39] | $(1,0,14),(2,0,7)$ |
| 1 | -1 | 1 | [3, 5, 13, 19, 27, 45] | $(3,\pm 2,5)$ |

# 5 Examples of negative discriminant

Here are a few examples of negative discriminant D and their genera, with their respective complete characters and the numbers they represent modulo D. This python code was used for the computations.

## 5.1 $D = -495$

$495 = 3^2 \cdot 5 \cdot 11$. Therefore the assigned characters are $\left(\frac{r}{3}\right), \left(\frac{r}{5}\right), \left(\frac{r}{11}\right)$.

| $\left(\frac{r}{3}\right)$ | $\left(\frac{r}{5}\right)$ | $\left(\frac{r}{11}\right)$ | $((\mathbb{Z}/D\mathbb{Z})^*$ | Forms represented |
|---|---|---|---|---|
| 1 | 1 | 1 | [1, 4, 16, 31, 34, 49, 64, 91, 124, 136, 166, 169, 181, 196, 199, 214, 229, 256, 289, 301, 331, 334, 346, 361, 364, 379, 394, 421, 454, 466] | $(1, 1, 124)$, $(4, \pm 1, 31)$, $(9, 9, 16)$ |
| 1 | 1 | 1 | [2, 8, 17, 32, 62, 68, 83, 98, 107, 128, 167, 173, 182, 197, 227, 233, 248, 263, 272, 293, 332, 338, 347, 362, 392, 398, 413, 428, 437, 458] | $(2, \pm 1, 62)$, $(8, \pm 7, 17)$ |
| 1 | 1 | 1 | [14, 26, 56, 59, 71, 86, 89, 104, 119, 146, 179, 191, 221, 224, 236, 251, 254, 269, 284, 311, 344, 356, 386, 389, 401, 416, 419, 434, 449, 476] | $(5, 5, 26)$, $(9, \pm 3, 14)$, $(11, 11, 14)$ |
| 1 | 1 | 1 | [7, 13, 28, 43, 52, 73, 112, 118, 127, 142, 172, 178, 193, 208, 217, 238, 277, 283, 292, 307, 337, 343, 358, 373, 382, 403, 442, 448, 457, 472] | $(7, \pm 3, 18)$, $(10, \pm 5, 13)$ |

## 5.2 $D = -256$

$256 = 2^8$. Therefore the assigned characters are $\left(\frac{-1}{a}\right)$ and $\left(\frac{2}{a}\right)$.

| $\left(\frac{-1}{a}\right)$ | $\left(\frac{2}{a}\right)$ | $((\mathbb{Z}/D\mathbb{Z})^*$ | Forms represented |
|---|---|---|---|
| 1 | 1 | [1, 9, 17, 25, 33, 41, 49, 57, 65, 73, 81, 89, 97, 105, 113, 121, 129, 137, 145, 153, 161, 169, 177, 185, 193, 201, 209, 217, 225, 233, 241, 249] | $(1,0,64),(4,4,17)$ |
| 1 | -1 | [5, 13, 21, 29, 37, 45, 53, 61, 69, 77, 85, 93, 101, 109, 117, 125, 133, 141, 149, 157, 165, 173, 181, 189, 197, 205, 213, 221, 229, 237, 245, 253] | $(5,\pm 2,13)$ |

## 5.3 $D = -40$

$40 = 2^3 \cdot 5$. Therefore the assigned characters are $\left(\frac{-1}{a}\right)$ and $\left(\frac{a}{5}\right)$.

| $\left(\frac{-1}{a}\right)$ | $\left(\frac{a}{5}\right)$ | $((\mathbb{Z}/D\mathbb{Z})^*$ | Forms represented |
|---|---|---|---|
| 1 | 1 | [1, 9, 11, 19] | $(1,0,10)$ |
| 1 | -1 | [7, 13, 23, 37] | $(2,0,5)$ |

## 5.4 $D = -103$

103 is prime. Therefore the assigned character is $\left(\frac{a}{103}\right)$.

| $\left(\frac{a}{103}\right)$ | $((\mathbb{Z}/D\mathbb{Z})^*$ | Forms represented |
|---|---|---|
| 1 | [1, 2, 4, 7, 8, 9, 13, 14, 15, 16, 17, 18, 19, 23, 25, 26, 28, 29, 30, 32, 33, 34, 36, 38, 41, 46, 49, 50, 52, 55, 56, 58, 59, 60, 61, 63, 64, 66, 68, 72, 76, 79, 81, 82, 83, 91, 92, 93, 97, 98, 100] | $(1,1,26)$, $(2,\pm 1,13)$, $(4,\pm 3,7)$ |

Following are a few examples with only the corresponding complete character:

## 5.5 $D = -2044$

$2044 = 2^2 \cdot 7 \cdot 73$. Therefore the assigned characters are $\left(\frac{a}{7}\right)$ and $\left(\frac{a}{73}\right)$.

| $\left(\frac{a}{7}\right)$ | $\left(\frac{a}{73}\right)$ | Forms represented |
|---|---|---|
| 1 | 1 | $(1,0,511),(8,\pm6,65),(16,\pm14,35),(23,\pm16,25)$ |
| 1 | -1 | $(7,0,73),(5,\pm4,103),(13,\pm6,40),(17,\pm8,31)$ |

## 5.6 $D = -3072$

$3072 = 2^{10} \cdot 3$. Therefore the assigned characters are $\left(\frac{-1}{a}\right)$, $\left(\frac{2}{a}\right)$, and $\left(\frac{a}{3}\right)$.

| $\left(\frac{-1}{a}\right)$ | $\left(\frac{2}{a}\right)$ | $\left(\frac{a}{3}\right)$ | Forms represented |
|---|---|---|---|
| 1 | 1 | 1 | $(1,0,768),(4,4,193),(16,\pm8,49)$ |
| -1 | -1 | 1 | $(3,0,256),(12,12,67),(19,\pm14,43)$ |
| -1 | 1 | 1 | $(7,\pm6,111),(28,\pm20,31)$ |
| 1 | -1 | 1 | $(13,\pm10,61),(21,\pm6,37)$ |

## 5.7 $D = -111$

$111 = 3 \cdot 37$. Therefore the assigned characters are $\left(\frac{a}{3}\right)$ and $\left(\frac{a}{37}\right)$.

| $\left(\frac{a}{3}\right)$ | $\left(\frac{a}{37}\right)$ | Forms represented |
|---|---|---|
| 1 | 1 | $(1,1,28),(3,3,10),(4,\pm1,7)$ |
| -1 | -1 | $(2,\pm1,14),(5,\pm3,6)$ |

## 5.8 $D = -5120$

$5120 = 2^{10} \cdot 5$. Therefore the assigned characters are $\left(\frac{-1}{a}\right)$, $\left(\frac{2}{a}\right)$, and $\left(\frac{a}{5}\right)$.

| $\left(\frac{-1}{a}\right)$ | $\left(\frac{2}{a}\right)$ | $\left(\frac{a}{3}\right)$ | Forms represented |
|---|---|---|---|
| 1 | 1 | 1 | $(1,0,1280),(4,4,321),(9,\pm 8,144),(16,\pm 8,81),(36,\pm 28,41)$ |
| -1 | -1 | -1 | $(3,\pm 2,427),(12,\pm 4,107),(27,\pm 8,48),(35,\pm 30,43)$ |
| 1 | -1 | 1 | $(5,0,256),(20,20,69),(21,\pm 2,61),(21,\pm 16,64),(29,\pm 10,45)$ |
| -1 | 1 | -1 | $(7,\pm 2,183),(15,\pm 10,87),(23,\pm 20,60),(28,\pm 12,47)$ |

## 5.9 $D = -7007$

$5120 = 7^2 \cdot 11 \cdot 13$. Therefore the assigned characters are $\left(\frac{a}{7}\right)$, $\left(\frac{a}{11}\right)$, and $\left(\frac{a}{13}\right)$.

| $\left(\frac{a}{7}\right)$ | $\left(\frac{a}{11}\right)$ | $\left(\frac{a}{13}\right)$ | Forms represented |
|---|---|---|---|
| 1 | 1 | 1 | $(1,1,1752),(4,\pm 1,438),(9,\pm 7,196),(16,\pm 15,113),$ $(22,\pm 11,81),(23,\pm 13,78),(36,\pm 7,49),(36,\pm 25,53)$ |
| 1 | -1 | -1 | $(2,\pm 1,876),(8,\pm 1,219),(11,11,162),(18,\pm 11,99),$ $(18,\pm 7,98),(32,\pm 17,57),(39,\pm 13,46),(44,\pm 33,46)$ |
| -1 | 1 | 1 | $(3,\pm 1,584),(12,1,146),(12,\pm 7,147),(26,\pm 13,69),$ $(27,\pm 11,66),(38,\pm 17,48),(38,\pm 21,49),(48,47,48)$ |
| -1 | -1 | -1 | $(6,\pm 5,293),(6,\pm 1,292),(13,\pm 13,138),(19,\pm 17,96),$ $(24,\pm 1,73),(24,\pm 17,76),(33,\pm 11,54),(41,\pm 39,52)$ |

This data of class numbers suggests the following relation:

**Statement:** Let $h(D)$ denote the class number of discriminant $D$ (= the number of primitive reduced quadratic forms of Discriminant $D$). Let $t \not\equiv 1, 5 \pmod 8$ and $t > 4$. Then,

1. *For odd t:* $\dfrac{h(-t^{k+2})}{h(-t^k)} = t$ for $k \geq 3$, $k$ is odd.
2. *For even t:* $\dfrac{h(-t^{k+2})}{h(-t^k)} = t$

   i if $t \equiv 0 \pmod 4$: $k \geq 1$

   ii if $t \equiv 2 \pmod 4$: $k \geq 2$

The above statement actually follows from Theorem 7.4 and 7.5 of Duncan Buell's Binary Quadratic Forms.

# 6 Class Field Theory

## 6.1 Ring Theory: Pre-requisites

A **Ring** R is a set together with 2 binary operations (+) and (x) satisfying:

- (R, +) is an abelian group.
- Multiplication ($R^{\times}$) is associative
- The Distributive laws hold, i.e.

$$(a+b)*c = (a*c)+(b*c)$$

- R is commutative if ($R^{\times}$) is commutative.
- R has an identity $1 \in R$ such that $1*a = a*1 = a$ for all $a \in R$

Following are some general definitions:

- If every nonzero element $a \in R$ has a multiplicative inverse, R is a *Division Ring/Skew Field.*
- A *field* is a commutative division ring.
- An element $u \in R$ is a a *unit* if it has a multiplicative inverse in R (i.e., there exists $\in R$ s.t. $uv = 1$). Group of units in $R = R^{\times}$.
- A nonzero element $a \in R$ is a *zero divisor* if $\exists b \in R$ s.t. either $ab = 0$ or $ba = 0$.
- A commutative ring with multiplicative identity $1 \neq 0$ (additive identity) and having no zero divisors, is an *integral domain.*

**Ideal:** Let R be a ring, I is a subset of R and $r \in R$. Define $rI = ra|a \in I$ and $Ir = ar|a \in I$. Then I is a left ideal if:

- I is a subring of R.
- I is closed under left multiplication by elements from R, i.e. $rI \subseteq I \forall r \in R$.

A right module is defined analagously.

**R-module:** Let R be a ring. A left R-module is a set M with:

1. A binary operation (+) on M under which it is an Abelian group.
2. An action of R on M (a map R x M $\to$ M) denoted by rm $\forall r, s \in R, m \in M$ satisfying:
   - $(r + s)m = rm + sm$
   - (rs)m = r(sm)
3. If the Ring has a 1, we also have

$$1m = m, \forall m \in M$$

In a left module, the elements appear on the left (as described above). For a right module, the elements will appear on the right.

**Prime Ideal:** A prime ideal is an ideal $I$ s.t. if $ab \in I$, then either $a \in I$ or $b \in I$.

**Field of Fractions:** Given an *integral domain* R and letting $R^\times = R - \{0\}$, define an equivalence relation on $R \times R^\times$ by letting $(n, d) \sim (m, b)$ when $nb = md$. Denote the equivalence class of (n, d) by $\frac{n}{d}$. Then, the field of fractions is the set Frac(R) $= R \times R^\times \sim$ with:

- Addition: $\frac{n}{d} + \frac{m}{b} = \frac{nb + md}{db}$
- Multiplication: $\frac{n}{d} \times \frac{m}{b} = \frac{nm}{db}$

This is the smallest field containing the integral domain $R$.

**Quadratic Field:** Let D be rational squarefree number. Define $\mathbb{Q}(\sqrt{D}) = a + b\sqrt{D} | a, b \in R$. $\mathbb{Q}(\sqrt{D})$ is a subring of $\mathbb{C}$ ($\mathbb{R}$ if $D > 0$.

**Algebraic Number Field (**$K$ is a subfield $= \mathbb{Q}[\sqrt{D}]$ of $\mathbb{C}$ whose degree over $\mathbb{Q}$ is finite (finite degree extension of rational numbers). The ring of integers $\mathcal{O}_K$ in $K$ is the set of algebraic integers in $K$. The **algebraic integers** of number field $\boldsymbol{K}$ are all $\alpha \in \boldsymbol{K}$ which are roots of a monic integer polynomial.

**Finite extension:** An extension field $F \subset K$ is called finite if the dimension of $K$ as a vector space over $F$ is finite. It is always algebraic.

Following are some important algebraic structures:

1. **Integral Domain:** An integral domain is a commutative ring with unity (identity element) in which the product of any two nonzero elements is nonzero.

2. **Principal Ideal Domain (PID):** A (PID) is an integral domain in which every ideal is a principal ideal, i.e. every ideal is generated by a single element.

3. **Unique Factorisation Domain (UFD)**: A (UFD) is an integral domain in which every nonzero non-unit element can be uniquely factored into irreducible (or prime) elements, up to units and order.

4. **Euclidean Domain**: A Euclidean domain is an integral domain equipped with a function (called the Euclidean norm) that behaves like a division algorithm, allowing the division of any two elements with a remainder.

**Theorem 6.1.1:** The following are equivalent for $\alpha \in \mathbb{C}$:

1. $\alpha$ is an algebraic integer;

2. The additive group of the ring $\mathbb{Z}[\alpha]$ is finitely generated;

3. $\alpha$ is a member of some subring of $\mathbb{C}$ having a finitely generated additive group;

4. $\alpha A \subset A$ for some finitely generated additive subgroup $A \subset \mathbb{C}$.

*Proof:* (1) $\Rightarrow$ (2): If $\alpha$ is a root of a monic polynomial over $\mathbb{Z}$ of degree $n$, then in fact the additive group of $\mathbb{Z}[\alpha]$ is generated by $1, \alpha, \ldots, \alpha^{n-1}$.

(2) $\Rightarrow$ (3) $\Rightarrow$ (4) trivially.

(4) $\Rightarrow$ (1): Let $a_1, \ldots, a_n$ generate $A$. Expressing each $\alpha a_i$ as a linear combination of $a_1, \ldots, a_n$ with coefficients in $\mathbb{Z}$, we obtain

$$\begin{pmatrix} \alpha a_1 \\ \vdots \\ \alpha a_n \end{pmatrix} = M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

where $M$ is an $n \times n$ matrix over $\mathbb{Z}$. Equivalently,

$$\Big(\alpha I - M\Big) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

is the zero vector, where $I$ denotes the $n \times n$ identity matrix. Since the $a_i$ are not all zero, it follows that $\alpha I - M$ has determinant 0. Hence, $\alpha$ is an eigenvalue of $M$. Expressing this determinant in terms of the $n^2$ coordinates of $\alpha I - M$, we obtain

$$\alpha^n + \text{lower degree terms} = 0.$$

Thus, we have produced a monic polynomial over $\mathbb{Z}$ having $\alpha$ as a root.

**Corollary 6.1.2:** If $\alpha$ and $\beta$ are algebraic integers, then so are $\alpha+\beta$ and $\alpha\beta$.

*Proof:* Since $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ have finitely generated additive groups, so does the

ring $\mathbb{Z}[\alpha, \beta]$.(If $\alpha_1$,..., $\alpha_m$ generate $\mathbb{Z}[\alpha]$ and $\beta_1$,..., $\beta_m$ generate $\mathbb{Z}[\beta]$, then the $mn$ products of $\alpha_k\beta_j$ generate $\mathbb{Z}[\alpha, \beta]$. Finally, $\mathbb{Z}[\alpha, \beta]$ contains $\alpha + \beta$ and $\alpha\beta$. By characterisation (3) of Theorem 6.1.2, this implies that they are algebraic integers.

## 6.2 Ideal Class Group

From here on, let $K$ be a number field and $\mathcal{O}_K$ be the ring of integers in K.

**Proposition 6.2.1:** $\mathcal{O}_K$ is:

1. A subring of C whose field of fractions is K.
2. A free Z-module of rank $[K : Q]$.

*Proof:*

1. i $\mathcal{O}_K$ *is a subring of* $\mathbb{C}$*:* We will use the **subring test** for this:

   *Let $S$ be a subset of a ring $(R, +, \cdot)$. Then $(S, +, \cdot)$ is a subring of $(R, +, \cdot)$ if and only if the following conditions hold:*
   *a. $S \neq \varnothing$.*
   *b. For all $x, y \in S$, $x + (-y) \in S$*
   *c. For all $x, y \in S$, $x \cdot y \in S$*
   *Proof:*
   **a. $\mathcal{O}_K$ is Non-Empty:** Since $\mathcal{O}_K$ is the ring of integers of the number field $K$, it contains at least the unity element 1. Therefore, $\mathcal{O}_K \neq \varnothing$.
   **b. Closure under Subtraction:** Let $x, y \in \mathcal{O}_K$. Since $x$ and $y$ are algebraic integers, their additive inverses $-x$ and $-y$ are also algebraic integers. Thus, $x+(-y)$ is an algebraic integer since the sum of algebraic integers is an algebraic integer (Corollary 5.1.2). Since $x + (-y) \in \mathbb{C}$ and $x + (-y) \in \mathcal{O}_K$, we have $x + (-y) \in \mathcal{O}_K$.

**c. Closure under Multiplication:** Let $x, y \in \mathcal{O}_K$. As before, since $x$ and $y$ are algebraic integers, their product $x \cdot y$ is also an algebraic integer (Corollary 5.1.2). Since $x \cdot y \in \mathbb{C}$ and $x \cdot y \in \mathcal{O}_K$, we have $x \cdot y \in \mathcal{O}_K$. Therefore $\mathcal{O}_K$ is a subring of $\mathbb{C}$.

ii *$K$ is the FoF of $\mathcal{O}_K$*: Let $L$ be the FoF of $\mathcal{O}_K \Rightarrow L \subseteq K$. Since $K$ is a number field, if $[K : L] > 1, \exists \alpha \in K \backslash L$ which is algebraic over $Q$. Then, there exists $d \in \mathbb{Z}$ such that $d\alpha$ is an algebraic integer $\Rightarrow d\alpha \in \mathcal{O}_K \subset L$. However, $d\alpha \notin L \rightarrow$ contradiction.

2. See Marcus [2, Corollary to Theorem 9] or Milne [4, Proposition 2.29]

**Corollary 6.2.2** If $K$ is a number field and $\mathfrak{a}$ is a non-zero ideal of $\mathcal{O}_K$, then the quotient using $\mathcal{O}_K/\mathfrak{a}$ is finite.

**Proof:** Let $\alpha \in \mathfrak{a}$. Then $\alpha$ satisfies $\alpha^m + \alpha^{n-1}a_1 + ... + a_n = 0$ with $a_i \in \mathbb{Z}$. $\Rightarrow a_n = -\alpha(\alpha^{n-1} + a_1\alpha^{n-2} + ... + a_{n-1} \in \mathfrak{a}$, since $\mathfrak{a}$ is a non-zero ideal. Therefore, $\mathfrak{a}$ contains a non-zero integer ($a_m = a$ (say)). From proposition 6.2.1, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n = [K : Q]$, and $\mathcal{O}_K/a\mathcal{O}_K \simeq \mathbb{Z}/a\mathbb{Z}$, which is finite. As $a \in \mathfrak{a}$, a natural surjection $\mathcal{O}_K/a\mathcal{O}_K \rightarrow \mathcal{O}_K/\mathfrak{a}$ exists and so $\mathcal{O}_K/\mathfrak{a}$ is also finite.

**Theorem 6.2.3** $\mathcal{O}_K$ is a Dedekind domain, which means that:

1. $\mathcal{O}_K$ is integrally closed in $K$, i.e., if $\alpha \in K$ satisfies a monic polynomial with coefficients in $\mathcal{O}_K$, then $\alpha \in \mathcal{O}_K$.

2. $\mathcal{O}_K$ is Noetherian, i.e., given any chain of ideals $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots$, there is an integer $n$ such that $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \ldots$.

3. Every nonzero prime ideal of $\mathcal{O}_K$ is maximal.

**Proof:**

1. See Mehrle [5, Example 3.56]

2. Since $\mathcal{O}_K/\mathfrak{a}$ is finite, there are only finitely many ideals containing $\mathfrak{a}$.

3. $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain (and therefore a field) as $\mathfrak{p}$ is prime. By definition, $\mathfrak{p}$ is maximal.

**Corollary 6.2.4:** If K is a number field, then any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ can be written as a product of prime ideals.

**Proof:** If $\mathfrak{a}$ is maximal, it is a prime ideal. Let's assume otherwise. Then there is some prime ideal $\mathfrak{p}_1$ containing it (as some maximal ideal contains $\mathfrak{a}$. Then we can write $\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}_1$, where $\mathfrak{a} \subseteq \mathfrak{a}_1$. Repeating this, we get $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2...\mathfrak{p}_n\mathfrak{a}_n$ and $\mathfrak{a} \subseteq \mathfrak{a}_1 \subseteq ... \subseteq \mathfrak{a}_n \subseteq \mathcal{O}_K$. As $\mathcal{O}_K$ is finitely generated, only a finite number of ideals can lie between $\mathfrak{a}$ and $\mathcal{O}_K$, at some point $\mathfrak{a}_k = \mathfrak{p}_k$ is prime.

We will now use *fractional ideals*, which are the nonzero finitely generated $\mathcal{O}_K$-submodules of $K$.

**Proposition 6.2.5:** Let $\mathfrak{a}$ be a fractional $\mathcal{O}_K$ ideal.

1. $\mathfrak{a}$ is invertible, i.e. there exists a fractional $\mathcal{O}_K$ ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}_K$.

2. $\mathfrak{a}$ can be written uniquely as a product $\mathfrak{a} = \prod_{i=1}^{r} p_i^{r_i}, r_i \in \mathbb{Z}$, where each $p_i$ is a distinct prime ideal of $\mathcal{O}_K$.

*Proof:*

1. Let $\mathfrak{a}^{-1} = \{x \in K : x\mathfrak{a} \subset \mathcal{O}_K$. The proof requires the following two parts:

   i *Every maximal ideal* $\mathfrak{p}$ *is invertible:* $x\mathfrak{p} \subset \mathcal{O}_K \Rightarrow \mathcal{O}_K \subset \mathfrak{p}^{-1}$. Let $a \in \mathfrak{p}, a \neq 0$. Choose r minimal such that there exists a product

   $$\mathfrak{p}_1...\mathfrak{p}_r \subset (a) \subset \mathfrak{p}$$

   Here $(a)$ is the ideal generated by $a = a\mathfrak{p}$. One of the prime ideals (say $\mathfrak{p}_1$ is contained in and equal to $\mathfrak{p}$ (as prime ideals are maximal).

Furthermore,

$$\mathfrak{p}_2 ... \mathfrak{p}_r \not\subset (a)$$

and therefore there exists $\mathfrak{b} \in \mathfrak{p}_2 ... \mathfrak{p}_r$ such that $b \notin (a)$. But $b\mathfrak{p} \subset (a) \Rightarrow b\mathfrak{a}^{-1}\mathfrak{p} \subset \mathcal{O}_K$. Since $\mathfrak{p}$ is maximal, either $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$ or $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$. But $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$ implies that $\mathfrak{p}^{-1}$ leaves a finitely generated $\mathfrak{o}$-module invariant, and hence is integral over $\mathfrak{o}$. This is impossible since $\mathfrak{o}$ is integrally closed. Hence $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$.

ii *Every non-zero ideal is invertible, by a fractional ideal:* Suppose this is not true. There exists a maximal non-invertible ideal $a$. We have just seen that $a$ cannot be a maximal ideal. Hence, $a \subseteq \mathfrak{p}$ for some maximal ideal $p$, and $a \sim p$. We get

$$\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{a}\mathfrak{a}^{-1} \subset \mathfrak{o}$$

Since $a$ is finitely generated, we cannot have $ap^{-1} = a$ (because $p^{-1}$ is not integral over $\mathfrak{o}$). Hence $ap^{-1}$ is larger than $a$, hence has an inverse, which, when multiplied by $p$, obviously gives an inverse for $a$, leading to a contradiction.

Since $\mathfrak{a}$ is a fractional ideal, it is non-zero, i.e., $\mathfrak{a} \neq \{0\}$. Therefore, $\mathfrak{a}$ is invertible.

2. This follows from Corollary 5.2.4.

**Proposition 6.2.6:** Let $I_K$ be the set of all prime ideals. Then,

1. $I_K$ is closed under multiplication and forms a group under that operation.
2. The set of principal fractional ideals $P_K$ (of the form $\alpha\mathcal{O}_K$) for some $\alpha \in K^*$ form a subgroup of $I_K$.

**Proof:**

1. We use the fact that $\mathfrak{a}$ *is a fractional ideal if and only if* $\mathfrak{a} = \alpha\mathfrak{b}$*, where* $\alpha \in K$ *and* $\mathfrak{b}$ *is an ideal of* $\mathcal{O}_K$*:* (for a proof, check Cox[Exercise 5.2].

   Now suppose $\alpha\mathfrak{a}$ and $\beta\mathfrak{b}$ are two fractional ideals, where $\mathfrak{a}, \mathfrak{b}$ are ideals of $\mathcal{O}_K$. Let $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$, so that $\mathfrak{c}$ is an $\mathcal{O}_K$-ideal. Then $(\alpha\mathfrak{a})(\beta\mathfrak{b}) = (\alpha\beta)(\mathfrak{a}\mathfrak{b}) = (\alpha\beta)(\mathfrak{c})$, which is a fractional ideal.

2. The set of principal fractional ideals $P_K$ is of the form $\alpha\mathcal{O}_K$ for some $\alpha \in K^*$. Clearly, it is a non-empty subset of $I_K$. For it to be a subgroup, we must satisfy the **subgroup criterion:** *Let $G$ be a group, and let $H \subset G$. Then $H < G$ if and only if for every pair of elements $g, h \in H$, the product $gh^{-1} \in H$.*

   Consider $\alpha, \beta \in K \Rightarrow \alpha\mathcal{O}_K, \beta\mathcal{O}_K \in P_K$. Then $(\alpha\mathcal{O}_K)(\beta^{-1}\mathcal{O}_K) = (\alpha\beta^{-1})\mathcal{O}_K \in P_K$ as $\alpha\beta^{-1} \in K$. Hence, $P_K$ is a subgroup of $I_K$.

The ***Ideal Class Group*** is defined as the quotient group $I_K/P_K$ and denoted by $C(\mathcal{O}_K)$. The order of this group is called the *Class number* and is denoted by $h(K)$.

## 6.3 Basic Ramification Theory

Suppose that $K$ is a number field, and let $L$ be a finite extension of $K$. 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 hence has a prime factorisation

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

where the $\mathfrak{P}_i$'s are the distinct primes of $L$ containing $\mathfrak{p}$. Following is some important related terminology:

- *Ramification index:* The integer $e_i$, also written $e_{\mathfrak{P}_i|\mathfrak{p}}$, is called the ramification index of $\mathfrak{p}$ in $\mathfrak{P}_i$.

- *Inertial degree:* Each prime $\mathfrak{P}_i$ containing $\mathfrak{p}$ also gives a residue field extension $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{P}_i$, and its degree, written $f_i$ or $f_{\mathfrak{P}_i|\mathfrak{p}}$, is the inertial degree of $\mathfrak{p}$ in $\mathfrak{P}_i$.

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 $e = f = 1$, we say that $\mathfrak{p}$ splits completely in $L$. Such a prime is unramified, and in addition $\mathfrak{p}\mathcal{O}_L$ is the product of $[L : K]$ distinct primes. $\mathfrak{p}$ is inert if it doesn't split at all.

## 6.4 Quadratic Fields

A quadratic field can be written uniquely in the form $K = \mathbb{Q}(\sqrt{N})$, where $N \neq 0, 1$ is a squarefree integer. The basic invariant of $K$ is its discriminant $d_K$, which is defined to be

$$d_K = \begin{cases} N, & \text{if } N \equiv 1 \mod 4, \\ 4N, & \text{otherwise.} \end{cases} \tag{2}$$

$d_K \equiv 0, 1 \mod 4$ and $K = \mathbb{Q}(\sqrt{d_K})$; hence a quadratic field is determined by its discriminant.

**Exercise 6.4.1:** Let's determine the integers in the quadratic field $K = \mathbb{Q}(\sqrt{N})$, where $N$ is a squarefree integer. Let $\alpha$ and $\alpha'$ denote the nontrivial automorphism of $K$.

(a) Given $\alpha = r + s\sqrt{N} \in K$, define the trace and norm of $\alpha$ to be

$$T(\alpha) = \alpha + \alpha' = 2r, \quad N(\alpha) = \alpha\alpha' = r^2 - s^2 N.$$

Then prove that for $\alpha, \beta \in K$,

$$T(\alpha + \beta) = T(\alpha) + T(\beta), \quad N(\alpha\beta) = N(\alpha)N(\beta).$$

*Solution:*

$$T(\alpha+\beta) = (\alpha+\beta)+(\alpha+\beta)' = \alpha+\beta+\alpha'+\beta' = \alpha+\alpha'+\beta+\beta' = T(\alpha)+T(\beta)$$

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

(b) Given $\alpha \in K$, prove that $\alpha \in \mathcal{O}_K$ if and only if $T(\alpha), N(\alpha) \in \mathbb{Z}$.
*Solution:*

$$f(x) = x^2 - T(\alpha)x + N(\alpha) = x^2 - (\alpha+\alpha')x + \alpha\alpha' = (x-\alpha)(x-\alpha')$$

Thus the roots of $f(x)$, which is a monic integer polynomial (as $T(\alpha), N(\alpha) \in \mathbb{Z}$), are $\alpha$ and $\alpha'$, showing that $\alpha, \alpha' \in \mathcal{O}_K$.

Conversely, if $\alpha \in \mathcal{O}_K$, then its minimal polynomial is $x^2 + cx + d \in \mathbb{Z}[x]$ and its other root is $\alpha'$. Thus $x^2 + cx + d = (x-\alpha)(x-\alpha') = x^2 - (\alpha+\alpha') + \alpha\alpha'$, so that $-c = \alpha + \alpha' = T(\alpha)$ and $d = \alpha\alpha' = N(\alpha)$ are both integers.

The next step is to describe the integers $\mathcal{O}_K$ of $K$. Writing $K = \mathbb{Q}(\sqrt{N})$, $N$ squarefree, one can show that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{N}], & N \not\equiv 1 \mod 4, \\ \mathbb{Z}[\frac{1+\sqrt{N}}{2}], & N \equiv 1 \mod 4, \end{cases} \tag{3}$$

Using the discriminant, this description of $\mathcal{O}_K$ may be written more elegantly as follows:

$$\mathcal{O}_K = \mathbb{Z}[\frac{\sqrt{d_K} + \sqrt{d_K}}{2}]. \tag{4}$$

Given $n > 0$, let $K$ be the imaginary quadratic field $\mathbb{Q}(\sqrt{-n})$. Then:

$$d_K = -4n \iff \mathcal{O}_K = \mathbb{Z}[\sqrt{-n}] \iff n \text{ is squarefree}, n \not\equiv 3(4) \tag{5}$$

We define the *Hilbert class field* $L$ of a number field $K$ as the maximal unramified Abelian extension of $K$.

Having defined all the requirements, we now state the two main theorems of this last section:

**Theorem 6.4.1:** Let $L$ be the Hilbert class field of $K = \mathbb{Q}(\sqrt{-n})$. Assume that $n$ is squarefree and $n \not\equiv 3 \mod 4$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$. If $p$ is an odd prime not dividing $n$, then

$$p = x^2 + ny^2 \iff p \text{ splits completely in } L.$$

**Theorem 6.4.2:** Let $n > 0$ be an integer such that $n$ is squarefree and $n \not\equiv 3 \mod 4$. 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

$$p = x^2 + ny^2 \iff \left(\frac{-n}{p}\right) = 1 \quad \text{and} \quad f_n(x) \equiv 0 \mod p \text{ has an integer solution.} \tag{6}$$

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

*Proof:* See [Cox, Theorem 5.1 and Theorem 5.26]

# Acknowledgements

I want to thank my project supervisor Professor Brundaban Sahu for giving me such an interesting topic to read about and providing me with mathematical guidance and materials to study the same.


# References


1. Cox, David. *Primes of the Form $x^2 + ny^2$*. John Wiley & Sons, Inc. 1989.
2. Marcus, Daniel A. *Number Fields*. Universitext, Springer-Verlag, New York-Heidelberg, 1977. MR0457396.
3. Lang, Serge. *Algebraic Number Theory*. Springer-Verlag, Berlin, Heidelberg, and New York, 1986.
4. Milne, James S. *Algebraic Number Theory (v3.08)*, Available at www.jmilne.org/math/, 2020
5. Mehrle, David. *Algebraic Number Theory*. Cornell University, Spring 2018.
6. Li, Che. *Introduction to Class Field Theory and Primes of the Form $x^2+ny^2$*.
7. Chang, Timo. *Number Fields, Exercise Solutions*.