The Class Number Problem*

Yukako Kezuka†

21st September, 2012

Abstract

The class number problem of Gauss asks for a complete list of imaginary quadratic fields with a given class number. In this project we will give a proof of the class number one problem, which states that there are exactly nine imaginary quadratic fields with class number one. We will follow Stark's presentation of Heegner's approach to the problem, which uses modular functions.

Contents

Introduction

In 1801, Gauss posed the following problems in his book *Disquisitiones Arithmeticae*:

1. *The class number $h(D) \to \infty$ as $D \to -\infty$.*
2. *There are exactly 9 imaginary quadratic fields with class number one, namely: $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ and $\mathbb{Q}(\sqrt{-163})$.*
3. *There are infinitely many real quadratic fields with class number one.*

The second problem is known as the class number one problem, and was settled independently by Heegner [9] in 1952, Baker [2] in 1966, and Stark [16] in 1967. Heegner was the first to prove this theorem, but sadly his proof was not accepted partly because it contained some minor mistakes.

*This essay was written as part of the assessment for the MSc Pure Mathematics course at the Department of Mathematics, Imperial College London.

†Email: yukako.kezuka@gmail.com

Heegner died before anyone really noticed what he had achieved. Stark formally filled in the gap in Heegner's proof in 1969. The general class number problem, as usually understood, asks for each $n \geqslant 1$ a complete list of imaginary quadratic fields with class number n.

The class number problem has a long and interesting history. Perhaps the subject goes back to Fermat, who stated in 1964 that for an odd prime p,

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

These were first proved by Euler in 1761 and 1763. Many other problems of similar form were solved in the 18^{th} century, and in 1773 Lagrange developed a general theory of binary quadratic forms

$$ax^2 + bxy + cy^2 \qquad (a, b, c \in \mathbb{Z}) \tag{0.1}$$

with discriminant

$$D = b^2 - 4ac \tag{0.2}$$

to handle the general problem of when an integer m can be written in the form

$$m = ax^2 + bxy + cy^2.$$

Legendre simplified Lagrange's work in his book of 1798. He proved the law of quadratic reciprocity assuming Dirichlet's theorem on primes in arithmetic progression, introduced the composition of two forms, and defined the well-known Legendre symbol. In 1801, Gauss published his *Disquitiones arithmeticae*, in which he defines the composition of two quadratic forms and proves that the equivalence classes of quadratic forms with a given discriminant form a finite group with composition as the group law. We should point out at this point that Gauss' definition of quadratic form is slightly different from Lagrange's in the sense that he considers the form

$$ax^2 + 2bxy + cy^2 \tag{0.3}$$

and defines the discriminant as

$$D = b^2 - ac. \tag{0.4}$$

In article 303 of the *Disquitiones*, he gives lists of discriminants with a given low class number and conjectures that his lists are complete. For the moment, let us stick to Gauss' notation and let $h(D)$ denotes the number of inequivalent forms of type (0.3). It is not widely known that with this notation, the class number one problem was first proved by Landau in 1902. This is due to the fact that Gauss' definitions (0.3) and (0.4) only deal with even discriminants in terms of the modern definitions (0.1) and (0.2).

Theorem 1.1 (Landau). Let D denote Gauss' discriminant. Then for $D = b^2 - ac < -7$ we have $h(D) > 1$.

This theorem is proved in Section 1. Now let us return to Lagrange's definitions (0.1) and (0.2), which are better suited to the modern theory of binary quadratic fields. Given a binary quadratic form $ax^2 + bxy + cy^2$ of discriminant D, we can associate to it an ideal

$$\left[a,\ \frac{-b + \sqrt{D}}{2}\right] = \left\{ax + \left(\frac{-b + \sqrt{D}}{2}\right) y\ :\ x, y \in \mathbb{Z}\right\}$$

in the quadratic field $K = \mathbb{Q}(\sqrt{D})$. Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent if they belong to the same class in the ideal class group of K (i.e. if there exists a principal fractional ideal (λ) of $\mathcal{O}_K$ such that

$\mathfrak{a} = \mathfrak{b}(\lambda)$). We will see in Section 2 that equivalent ideals correspond to equivalent forms of type (0.1). Moreover, we will define orders in a quadratic field and find a formula which relates $h(m^2d)$ and $h(d)$ given a negative discriminant d and a positive integer m.

To go further requires class field theory, which is discussed in Sections 3 and 4. In Section 3 we will give only a classical formulation of class field theory. At the end of this section we introduce the ring class field of an order in an imaginary quadratic field K, a special case being the Hilbert class field of K. We have a short section to introduce a more modern treatment of class field theory (in terms of adèles and idèles) in Section 4, which is not strictly necessary for the purpose of this project, but provides us with a very nice alternative way of looking at the results discussed in Section 3. In Section 5 we will study elliptic functions and the theory of complex multiplications, and then define the j-invariant which is a modular function and is one of the most important tools used in Heegner's proof. A crucial property of the the j-invariant which accounts for its name is that this value characterizes the lattices up to homothety, which is an equivalence relation on the lattices. An important consequence is that if we consider the ring of integers of an imaginary quadratic field as a lattice, then the j-invariant of $\mathcal{O}_K$ determines K uniquely. Another property of j is that if $\mathcal{O}$ be an order in an imaginary quadratic field K, then $j(\mathcal{O})$ is an algebraic integer and it generates the ring class field of $\mathcal{O}$ over K. In Section 6, we introduce the Weber functions, which are special modular functions Heegner used to prove the class number one problem.

We will give a very brief outline of Heegner's proof here. What we want to prove is that if d_K is a field discriminant such that $h(d_K) = 1$ then $d_K = -3, -4, -7, -8, -11, -19, -43, -67$ or -163. So assume d_K is a field discriminant such that $h(d_K) = 1$. Then we may also assume $d_K \equiv 1 \bmod 4$, because the case $d_K \equiv 0 \bmod 4$ is dealt by Landau's theorem. Now, in this case, genus theory gives that the form class group $Cl(d_K)$ has $2^{\mu-1}$ elements of order $\leqslant 2$, where μ is the number of primes dividing d_K. But since $h(d_K) = 1$ the form class group is trivial, so this tells us that $\mu = 1$, that is, $d_K = -p$ for a prime number p. There are two cases to consider, when $d_K \equiv 1 \bmod 8$ and when $d_K \equiv 5 \bmod 8$. When $d_K \equiv 1 \bmod 8$, then by applying the formula which relates $h(m^2d)$ and $h(d)$ with $d = d_K$ and $m = 2$ gives $h(4d_K) = h(d_K) = 1$. But using Landau's theorem again, we find that d_K must be -7. When $d_K \equiv 5 \bmod 8$, then the same method gives us $h(4d_K) = 3h(d_K) = 3$. Using the relation between the class number of an order and the degree of the ring class field, we get that $j(\sqrt{d_K})$ generates a cubic extension of $\mathbb{Q}$. On the other hand, using the Weber modular functions we can find a real number α which generates the same cubic extension, such that α^4 has the minimal polynomial

$$x^3 - \sqrt[3]{j(\tau_0)} - 16,$$

where $\tau_0 = \frac{3+\sqrt{d_K}}{2}$ and the cube root is chosen appropriately and is an integer. Note also that α^4 generates the same cubic extension, so by manipulating the minimal polynomial of α and comparing coefficients, the problem reduces to solvind the Diophantine equation

$$2X(X^3 + 1) = Y^2.$$

This has exactly 6 solutions, each of which gives rise to a value of $j(\tau_0)$. It turns out that these values correspond to the 6 imaginary quadratic fields we are left with. The idea is we calculate the j-invariant for the 6 imaginary quadratic fields. Then we find that the $j(\tau_0)$'s corresponding to the 6 solutions of the Diophantine equation are among the j-invariants corresponding to the 6 fields. Then using the fact that $j(\mathcal{O}_K)$ determines K uniquely, it follows that we now know all imaginary quadratic fields of class number one, and the proof is complete.

1 Quadratic Forms and the Form Class Group

Let us begin by giving basic definitions. It is well-known that a *quadratic form* over a ring R is a homogeneous polynomial of degree 2 in a number of variables with coefficients in R. In this project, by a quadratic form we shall mean a quadratic form in two variables x and y over $\mathbb{Z}$. We say that a form $f(x,y) = ax^2 + bxy + xy^2$ is *primitive* if $\gcd(a,b,c) = 1$. An integer m is *represented* by a form $f(x,y)$ if the equation

$$m = f(x,y) \tag{1.1}$$

has integer solutions for x and y. In particular, if x and y in (1.1) are coprime, we say that m is *properly represented* by $f(x,y)$. Given two forms $f(x,y)$ and $g(x,y)$, say they are *equivalent* if there exist integers p, q, r and s such that

$$g(x,y) = f(px+qy, rx+sy) \text{ and } ps - qr = \pm 1. \tag{1.2}$$

If $ps - qr = 1$ in (1.2), we say that $f(x,y)$ and $g(x,y)$ are *properly equivalent.*

Let K be a quadratic field. Then $K = \mathbb{Q}(\sqrt{N})$ for a unique squarefree integer $N \neq 0, 1$. Recall that the discriminant d_K of K is defined to be

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

When K is an imaginary quadratic field of discriminant $d_K < 0$, $h(d_K)$ is equal to the number of reduced forms of primitive positive definite quadratic forms of discriminant d_K (see Section 2).

We first show that if n is a positive integer and $h(-4n) = 1$, then $-4n = -4, -8, -12, -16$ or -28. It follows that if $d_K \equiv 0 \bmod 4$ is a field discriminant and $h(d_K) = 1$ then, $d_K = -4$ or -8.

A primitive positive definite quadratic form $(a,b,c) = ax^2 + bxy + cy^2$ is said to be *reduced* if $|b| \leqslant a \leqslant c$, and $b \geqslant 0$ if either $|b| = a$ or $a = c$. The discriminant of the form (a,b,c) is defined to be $b^2 - 4ac$.
Given a discriminant d, we have $-d = 4ac - b^2 \geqslant 3ac$ since for a reduced form (a,b,c) we have $b^2 \leqslant ac$. Hence $\frac{1}{3}|d| \geqslant ac \geqslant a^2 \geqslant b^2$ (note $d < 0$), and $a \geqslant 1$ since a is positive and $a, b, c \in \mathbb{Z}$ so it follows that c is bounded above by $\frac{1}{3}|d|$ and a and $|b|$ are bounded above by $\sqrt{|d|/3}$. Clearly a and c are bounded below by 1 and $-a < b \leqslant a < c$ implies that b in bounded below by $-\sqrt{|d|/3}$.
A procedure to list all the reduced forms with a given discriminant is as follows. d is congruent to 0 or 1 modulo 4, so let $b = d \bmod 2$. Then $d - b^2 \equiv 0 \bmod 4$ so let $c = (b^2 - d)/4$ and $a = 1$. Then (a,b,c) is a reduced form. So there is always at least one reduced form for a given discriminant. To find the rest, we can follow the procedure listed below.
Step 1. Set $b \leftarrow d \bmod 2$ and $B = \lfloor \sqrt{|d|/3} \rfloor$.
Step 2. Set $q \leftarrow (b^2 - d)/4$, $a \leftarrow \max\{2, b\}$.
Step 3. If $a \mid q$ then if $a = b$ or $a^2 = q$ or $b = 0$, let $c = q/a$ then (a,b,c) is a reduced form. If $a \mid q$ but non of the above applies, then similarly letting $c = q/a$ we have two reduced forms (a,b,c) and $(a,-b,c)$.
Step 4. Set $a \leftarrow a + 1$. If $a^2 \leqslant q$ go to step 3.
Step 5. Set $b \leftarrow b + 2$. If $b \leqslant B$ go to step 2, otherwise we have found all the reduced forms.

When the discriminant is even, the class number one problem can be solved using elementary methods. We now restate Theorem 1.1. The following argument is similar to the one due to Landau.

Theorem 1.1. *Let n be a positive integer. Then $h(-4n) = 1 \Leftrightarrow n = 1, 2, 3, 4$ or 7.*

Proof. We have $n \geqslant 1$, hence $x^2 + ny^2$ is a reduced form. We will show that if $n \notin \{1, 2, 3, 4, 7\}$ then $h(-4n) > 1$. Suppose first that n is not a prime power. Then n can be written $n = ac$ where $1 < a < c$ and $\gcd(a, c) = 1$, so $ax^2 + cy^2$ is another reduced form with discriminant $-4n$. Hence $h(-4n) > 1$ when n is not a prime power. Suppose next that $n = 2^r$. If $r \geqslant 4$ then $4x^2 + 4xy + (2^{r-2} + 1)y^2$ is a reduced form since $4 \leqslant 2^{r-2} + 1$ and is of discriminant $-4n$. Thus $h(-4n) > 1$ in this case. When $r = 3$, $-4n = -32$ and this has two reduced forms namely $x^2 + 8y^2$ and $3x^2 + 2xy + 3y^2$. Thus $h(-4n) > 1$ for $n = 2^r$, $r \geqslant 3$. This leaves us with the cases $n = 2$ and 4. Finally assume $n = p^r$ where p is an odd prime. If $n + 1$ is not a prime power, we can write $n + 1 = ac$ where $2 \leqslant a < c$ and $\gcd(a, c) = 1$. Then $ax^2 + 2xy + cy^2$ is a reduced form of discriminant $2^2 - 4ac = 4 - 4(n+1) = -4n$ so $h(-4n) > 1$. So suppose $n+1$ is also a prime power. But $n = p^r$ is odd so $n+1$ is even. Hence $n+1 = 2^s$ for some s. If $s \geqslant 6$, then $8x^2+6xy+(2^{s-3}+1)y^2$ is primitive and reduced of discriminant $-4n$ so $h(-4n) > 1$ when $s \geqslant 6$. The cases $s = 1, 2, 3, 4$ and 5 correspond to $n = 1, 3, 7, 15$ and 31 respectively. Now $n = 15$ is not a prime power so by the earlier argument $h(-4n) > 1$. When $n = 31$, $-4n = -124$ and this has a reduced forms $5x^2 \pm 2xy + 7y^2$ so $h(-4n) > 1$. This leaves us with the cases $n = 1, 3, 7$. Let us check that when $n = 1, 2, 3, 4, 7$ then $h(-4n) = 1$. When $n = 1, 2$, $|b| \leqslant \sqrt{\frac{|-4n|}{3}} \leqslant 1$ so $b \equiv 0 \bmod 2 \Rightarrow b = 0$ and n is not composite so x^2+ny^2 is the only reduced form. When $n = 3, 4, 7$, $|b| \leqslant \sqrt{\frac{|-4n|}{3}} \leqslant 3$ so $b \equiv 0 \bmod 2 \Rightarrow b = 0$ or ± 2. When $b = 0$, 3 and 7 are prime and although $4 = 2 \cdot 2$, $2x^2 + 2y^2$ is not a reduced form so $x^2 + ny^2$ is the only reduced form. So suppose now $|b| = 2$. If $n = 3$, then this means $4ac = 4 \cdot 3 + 2^2 = 16$ so $ac = 4$. But $a \leqslant c \Rightarrow (a, b, c) = (1, \pm 2, 4)$ or $(2, \pm 2, 2)$, none of which is a reduced form. If $n = 4$, then $4ac = 4 \cdot 4 + 2^2 = 20$, i.e. $ac = 5$. So $a \leqslant c \Rightarrow a = 1, c = 5$ but then $|b| > a$. If $n = 7$ then $4ac = 4 \cdot 7 + 2^2 = 32$ so $ac = 8$. Then $|b| \leqslant a \Rightarrow a \neq 1$ so $a = 2, c = 4$. But $(2, 2, 4)$ is not primitive. Hence $h(-4n) = 1$ if $n = 1, 2, 3, 4$ or 7, and this proves the theorem. □

We will show that the set $Cl(D)$ of equivalence classes of primitive positive definite forms of discriminant d forms an abelian group. In order to define multiplication of two classes, we need the following lemma, which is proved in [6] page 48.

Lemma 1.2. *Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ be quadratic forms of discriminant $D < 0$ such that $gcd(a, a', (b + b')/2) = 1$ (note b and b' have the same parity since f and g have the same discriminant and the parity of the discriminant of f (resp. g) only depends on b (resp. b') so $(b + b')/2$ is an integer). Then there exists an integer B such that*

$$B \equiv b \ mod \ 2a$$

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

$$B^2 \equiv D \ mod \ 4aa'$$

which is unique mod $2aa'$. □

Definition 1.3. Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ be primitive positive definite forms of discriminant $D < 0$ such that $\gcd(a, a', (b+b')/2) = 1$. Then the *Dirichlet composition* of $f(x, y)$ amd $g(x, y)$ is the form

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

where B is the integer detemined in Lemma 1.2.

We refer the reader to [6] page 50 for the proof of the following theorem, which shows that $Cl(D)$ indeed forms a group.

Theorem 1.4. *Let $D \equiv 0, 1 \ mod\ 4$ be negative and let $Cl(D)$ be the set of all equivalence classes of primitive positive definite forms of discriminant D, where two forms are in the same class if and only if they are properly equivalent. Then $Cl(D)$ is a finite abelian group with multiplication induced by Dirichlet composition, called the* form class group*. Furthermore, the identity element is the class containing the form*

$$\begin{aligned} x^2 - \frac{D}{4}y^2 \qquad & \text{if } D \equiv 0 \ mod\ 4 \\ x^2 + xy + \frac{1-D}{4}y^2 \qquad & \text{if } D \equiv 1 \ mod\ 4, \end{aligned} \tag{1.3}$$

and the inverse of the class containing the form $ax^2 + bxy + cy^2$ is the class containing the form $ax^2 - bxy + cy^2$. □

Remark 1.5. Alternatively, if $d_K < 0$ is a field discriminant then we can associate ideals of $K = \mathbb{Q}(\sqrt{d_K})$ with quadratic forms of discriminant d_K. Explicitly, given an ideal $\mathfrak{a} = [\alpha, \beta]$ of $\mathcal{O}_K$,

$$\frac{N(\alpha x + \beta y)}{N(\mathfrak{a})} = ax^2 + bxy + cy^2$$

is a quadratic form of discriminant d_K. Conversely, given a quadratic form (a, b, c) of discriminant d_K, the ideal $[a, (-b + \sqrt{d_K})/2]$ is an ideal in $\mathcal{O}_K$. Therefore we can define two forms to be equivalent if and only the ideals accociated with the forms are equivalent. This way, we can avoid defining the Dirichlet composition, c.f. Theorem 2.7.

Definition 1.6. Two quadratic forms of discriminant D are in the same *genus* if they represent the same values in $(\mathbb{Z}/D\mathbb{Z})^*$. Given D, the form described in (1.3) above is called the *principal form.* The genus containing the principal form is called the *principal genus.*

The following theorem draws attention to how genus theory is related to the theory of the form class group $Cl(D)$.

Theorem 1.7. *Let $D < 0$, $D \equiv 0, 1 \ mod\ 4$. Let r be the number of odd primes dividing D. Define μ as follows: if $D \equiv 1 \ mod\ 4$, then let $\mu = r$. If $D \equiv 0 \ mod\ 4$, write $D = -4n$ for $n > 0$, and:*

- *if $n \equiv 1, 2 \ mod\ 4$, let $\mu = r + 1$*
- *if $n \equiv 3 \ mod\ 4$, let $\mu = r$*
- *if $n \equiv 0 \ mod\ 8$, let $\mu = r + 2$*
- *if $n \equiv 4 \ mod\ 8$, let $\mu = r + 1$.*

Then:

(i) The form class group $Cl(D)$ has exactly $2^{\mu-1}$ elements of order $\leqslant 2$.

(ii) There are exactly $2^{\mu-1}$ genera of forms of discriminant D.

(iii) The principal genus consists of the classes in $Cl(D)^2$, the subgroup of squares in $Cl(D)$.

Proof. (sketch) The proof of (i) requires considering different cases all of which are similar and can be found in [12] pages 171–173. The idea of the proof of (ii) is the following: Let $Cl_0(D)$ denote the subgroup of $Cl(D)$ of elements of order $\leqslant 2$. Given D, we define μ *assigned characters* which give rise to a homomorphism $\psi : (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}^\mu$. This map ψ is surjective and its kernel turns out to be the subgroup H of values represented by the principal form. If we define $\chi : (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$ by sending $[p]$ to $\left(\frac{D}{p}\right)$ for $p \nmid D$ prime and $[-1]$ to 1 (resp. -1) when $D > 0$ (resp. $D < 0$), this extends

to give a homomorphism such that $\ker\chi$ has index 2 in $(\mathbb{Z}/D\mathbb{Z})^*$. So $\ker\chi/H$ has order $2^{\mu-1}$. Furthermore, sending a class to the coset of H defines a homomorphism $\phi : Cl(D) \to \ker\chi/H$ and we see that the order of $\phi(Cl(D))$ is the number of genera (ϕ sends a class to the coset of values it represents), so it suffices to prove $\phi(Cl(D)) = \ker\chi/H$. This can be done by showing that every congruence class in $\ker\chi$ contains a number represented by a form of discriminant D, which follows from Dirichlet's theorem on primes in arithmetic progression.
To prove (iii), notice that the squaring map gives a short exact sequence

$$0 \to Cl_0(D) \to Cl(D) \to Cl(D)^2$$

so the index $[Cl(D) : Cl(D)^2]$ equals the order of $Cl_0(D)$ and the map $Cl(D)/Cl(D)^2 \to \{\pm 1\}^{\mu-1}$ induced by ϕ is an isomorphism. Hence $Cl(D)^2 = \ker\phi$ which consists of the classes in the principal genus, hence the result follows. □

2 Orders in Imaginary Quadratic Fields

Notation. For a number field K and its ring of integers $\mathcal{O}_K$, we often say "a prime of $\mathcal{O}_K$" or "a prime of K" to mean "a nonzero prime ideal of $\mathcal{O}_K$". From now on, K and L denote number fields. $I(\mathcal{O}_K)$ denotes the group of all fractional ideals of $\mathcal{O}_K$, $P(\mathcal{O}_K)$ denotes the subgroup of $I(\mathcal{O}_K)$ consisting of principal fractional ideals and $Cl(\mathcal{O}_K) = \frac{I(\mathcal{O}_K)}{P(\mathcal{O}_K)}$ is the ideal class group.

We now introduce the concept of orders in a quadratic field K. We will see that in the case of imaginary quadratic fields, there is a nice relation between ideals in orders and quadratic forms. We will show that if $\mathcal{O}$ is an order then we can define the ideal class group $Cl(\mathcal{O})$, and it is isomorphic to the form class group $Cl(D)$ for $D < 0$ if $\mathcal{O}$ is chosen suitably. We begin with the definition:

Definition 2.1. An *order* $\mathcal{O}$ in a number field K is a subring $\mathcal{O} \subset K$ which is a finitely generated $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

It follows that $\mathcal{O}_K$ is an order in K and more importantly, any order $\mathcal{O}$ of K is contained in $\mathcal{O}_K$ (given $a \in \mathcal{O}$, multiplication by α gives a $\mathbb{Z}$-linear map, so it satisfies its characteristic polynomial by Cayley-Hamilton theorem, which shows that $\alpha \in \mathcal{O}_K$). Hence we call $\mathcal{O}_K$ the *maximal order* of K.

Note that if K is a quadratic field of discriminant d_K then we can write

$$\mathcal{O}_K = \left[1, \frac{d_K + \sqrt{d_K}}{2}\right].$$

Since $\mathcal{O}$ and $\mathcal{O}_K$ are free $\mathbb{Z}$-modules of rank 2, it follows that $[\mathcal{O}_K : \mathcal{O}] < \infty$. Hence we obtain the following lemma which gives a full description of orders in quadratic fields.

Lemma 2.2. *Let $\mathcal{O}$ be an order in a quadratic field K of discriminant d_K. Then we have*

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = \left[1, f\frac{d_K + \sqrt{d_K}}{2}\right]$$

where $f = [\mathcal{O}_K : \mathcal{O}]$.

Proof. We have $f\mathcal{O}_K \subset \mathcal{O}$ since $f = [\mathcal{O}_K : \mathcal{O}]$, so $\mathbb{Z} + f\mathcal{O}_K \subset \mathcal{O}$ follows. On the other hand, $[1, f\frac{d_K+\sqrt{d_K}}{2}]$ has index f in $\mathcal{O}_K = [1, \frac{d_K+\sqrt{d_K}}{2}]$, hence the result follows. □

Definition 2.3. Given an order $\mathcal{O}$ in a quadratic field K, $f = [\mathcal{O}_K : \mathcal{O}]$ is called the *conductor* of $\mathcal{O}$. Also, given a non-trivial automorphism σ of K and an order $\mathcal{O} = [\alpha, \beta]$, we define the *discriminant* of $\mathcal{O}$ to be the number

$$D = \det\begin{pmatrix} \alpha & \beta \\ \sigma(\alpha) & \sigma(\beta) \end{pmatrix}^2.$$

The discriminant is independent of the integral basis used and hence depends only on $\mathcal{O}$. The proof of this elementary fact is proved in the same way we prove that the discriminant of a number field is independent of the choice of integral basis, see [1] page 132. If we compute the discriminant D of $\mathcal{O}$ using the basis $\{1, f\frac{d_K+\sqrt{d_K}}{2}\}$, we get

$$D = \det \begin{pmatrix} 1 & f\frac{d_K+\sqrt{d_K}}{2} \\ 1 & f\frac{d_K-\sqrt{d_K}}{2} \end{pmatrix}^2 = (-f\sqrt{d_K})^2 = f^2 d_K. \tag{2.1}$$

Thus $d_K \equiv 0, 1 \bmod 4$ implies that $D \equiv 0, 1 \bmod 4$. Also, since $\frac{1}{f} \in \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{d_K})$, we see that $K = \mathbb{Q}(\sqrt{D})$, so the sign of D determines whether K is real or imaginary. In fact, D determines $\mathcal{O}$ uniquely and any nonsquare integer $D \equiv 0, 1 \bmod 4$ is the discriminant of an order in a quadratic field ; given $D \equiv 0, 1 \bmod 4$, write $D = f^2 d$ where f is a positive integer and $d \equiv 0, 1 \bmod 4$ is a squarefree integer. Then D is the discriminant of the order $\mathcal{O} = [1, f\frac{d+\sqrt{d}}{2}]$ in the quadratic field $\mathbb{Q}(\sqrt{d})$.

Example 2.4. The order $\mathbb{Z}[\sqrt{-n}]$ in $K = \mathbb{Q}(\sqrt{-n})$ has discriminant

$$D = \det \begin{pmatrix} 1 & \sqrt{-n} \\ 1 & -\sqrt{-n} \end{pmatrix}^2 = -4n$$

so equation (2.1) shows that

$$-4n = f^2 d_K.$$

Now we study the ideals of an order $\mathcal{O}$. The proofs of the results for $\mathcal{O}_K$ adapts easily to show that given a nonzero ideal $\mathfrak{a}$ in $\mathcal{O}$, the *norm* defined by $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$ is finite, $\mathcal{O}$ is Noetherian and has Krull dimension 1. It is also clear that if the conductor f of $\mathcal{O}$ is greater than 1, then $\mathcal{O}$ is not integrally closed, so that $\mathcal{O}$ is not a Dedekind domain. Hence the ideals of $\mathcal{O}$ may not have unique factorisation. To fix the situation, we introduce the concept of a proper ideal:

Definition 2.5. As of $\mathcal{O}_K$, a *fractional ideal* of $\mathcal{O}$ is a subset of K of the form $\alpha\mathfrak{a}$ where $\alpha \in K^*$ and $\mathfrak{a}$ is an ideal of $\mathcal{O}$, and a fractional ideal $\mathfrak{a}$ is *invertible* if there exists another fractional ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathcal{O}$. We say that a fractional ideal $\mathfrak{a}$ is *proper* if

$$\mathcal{O} = \{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\}.$$

The basic properties that we shall use later are that for $\alpha \in \mathcal{O}$, $\alpha \neq 0$ and proper ideals $\mathfrak{a}$, $\mathfrak{b} \subset \mathcal{O}$, we have:

$$N(\alpha\mathcal{O}) = N(\alpha) \tag{2.2}$$

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}) \tag{2.3}$$

The proofs of these properties can be found in [6] page 140. For quadratic fields, we have a nice result saying that the notions of proper and invertible coincide:

Proposition 2.6. *Let K be a quadratic field and let $\mathcal{O}$ be an order of K. Then a fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is proper if and only if it is invertible.*

Proof. Let $\mathfrak{a}$ be invertible, then $\mathfrak{ab} = \mathcal{O}$ for some fractional ideal $\mathfrak{b}$ of $\mathcal{O}$. Since $\mathcal{O} \subset \{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\}$ always holds ($\mathfrak{a}$ is an ideal), we need only show the other inclusion. Let $\beta \in K$ be such that $\beta\mathfrak{a} \subset \mathfrak{a}$. Then we have

$$\beta\mathcal{O} = \beta(\mathfrak{ab}) = (\beta\mathfrak{a})\mathfrak{b} \subset \mathfrak{ab} = \mathcal{O},$$

and $\beta \in \mathcal{O}$ follows. So $\mathfrak{a}$ is proper. Now let $\mathfrak{a}$ be a proper fractional ideal of $\mathcal{O}$. Note that $\mathfrak{a} = \beta\mathfrak{b}$ for some $\beta \in K^*$ and an ideal $\mathfrak{b}$ of $\mathcal{O}$ hence $\mathcal{O}/\mathfrak{b}$ is finite implies that $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank 2.

Hence we can write $\mathfrak{a} = [\gamma, \delta] = [1, h]$ for some $\gamma, \delta \in K$ and $h = \delta/\gamma$. Let $ax^2 + bx + c$ be the minimal polynomial of h, where a, b, and c are coprime integers.
Claim. $\mathcal{O} = [1, ah]$.
Proof of Claim. Note $(ah)^2 + b(ah) + c(ah) = 0$ so ah is an algebraic integer. Also for $\beta \in K$, see that

$$\begin{aligned}\beta[1,h] \subset [1,h] &\Leftrightarrow \beta \in [1,h] \text{ and } \beta h \in [1,h] \\ &\Leftrightarrow \beta = m + nh, m, n \in \mathbb{Z} \text{ and } \beta h = mh^2 + nh = mh + \frac{n}{a}(-bh - c)\end{aligned}$$

Since $\gcd(a, b, c) = 1$, it follows that $\beta h \in [1, h]$ if and only if $a \mid n$. Hence $\mathcal{O} = \{b \in K : \beta[1, h] \subset [1, h]\} = [1, ah]$ and thus the claim is proved.
Now let σ be a non-trivial automorphism of K. Then $\sigma(h)$ is the other root of ax^2+bx+c, and by the same argument as above, $\sigma(\mathfrak{a}) = \sigma(\alpha)[1, \sigma(h)]$ is a proper fractional ideal for $[1, a\sigma(h)] = [1, ah] = \mathcal{O}$. Then:

$$\begin{aligned}a\mathfrak{a}\sigma(\mathfrak{a}) = a\alpha\sigma(\alpha)[1,h][1,\sigma(h)] &= N(\alpha)[a, ah, a\sigma(h), ah\sigma(h)] \\ &= N(\alpha)[a, ah, -b, c] && \text{(using } h + \sigma(h) = -b/a,\ h\sigma(h) = c/a) \\ &= N(\alpha)[1, ah] && \text{(since } \gcd(a,b,c) = 1) \\ &= N(\alpha)\mathcal{O}\end{aligned}$$

So we have $\mathfrak{a}\left(\frac{a}{N(\alpha)}\sigma(\mathfrak{a})\right) = \mathcal{O}$, proving that $\mathfrak{a}$ is invertible. □

Given an order $\mathcal{O}$, let $I(\mathcal{O})$ denote the set of all proper fractional ideals of $\mathcal{O}$. Then Proposition 2.6 shows that $I(\mathcal{O})$ forms a group under multiplication. Let $P(\mathcal{O}) \subset I(\mathcal{O})$ denote the subgroup of all principal fractional ideals. As for $\mathcal{O}_K$, we call the quotient

$$Cl(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$$

the *ideal class group* of the order $\mathcal{O}$. The ideal class group $Cl(\mathcal{O})$ relates to the form class group $Cl(D)$ as follows:

Theorem 2.7. *Let $\mathcal{O}$ be the order of discriminant D in an imaginary quadratic field K, and let $f(x, y) = ax^2 + bxy + cy^2$ be a primitive positive definite quadratic form of discriminant D. Then:*

(i) $[a, (-b + \sqrt{D})/2]$ *is a proper ideal of* $\mathcal{O}$.

(ii) The map

$$f(x, y) \mapsto [a, (-b + \sqrt{D})/2]$$

induces an isomorphism $Cl(D) \xrightarrow{\sim} Cl(\mathcal{O})$.

(iii) A positive integer m is represented by $f(x, y)$ if and only if m is the norm of some ideal $\mathfrak{a}$ in the ideal class $[a, (-b + \sqrt{D})/2] + P(\mathcal{O})$ *in* $Cl(\mathcal{O})$. □

The proof can be found [6] pages 137–141.

Remark 2.8. In particular, the theorem above shows that $h(\mathcal{O}) = h(D)$ where $h(\mathcal{O}) = |Cl(\mathcal{O})|$.

Example 2.9. Here is an example to show that Theorem 2.7 does not necessarily hold for real quadratic fields. It is possible to define the form class group $Cl(d_K)$ for discriminants $d_K > 0$, although there will in general not exist only one reduced form per equivalence class. This can be fixed by changing the notion of *reduced* for positive discriminants. See [5] Chapter 5.6 for more

details. To show that Theorem 2.7 does not hold in general for positive discriminants, consider $K = \mathbb{Q}(\sqrt{3})$ and its maximal order $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$. Then $\mathcal{O}_K$ is a Euclidean field so a UFD, hence $Cl(\mathcal{O}_K)$ is trivial. On the other hand, we show that $\pm x^2 - 3y^2$, both of discriminant $d_K = 12$, are not properly equivalent, so that $Cl(d_K) \neq \{1\}$. To prove this, write $f(x, y) = x^2 - 3y^2$, $g(x, y) = -x^2 + 3y^2$ and suppose that these are properly equivalent. Then there exist $p, q, r, s \in \mathbb{Z}$ such that $g(x, y) = f(px + qy, rx + sy)$ and comparing the coefficients of x^2 on both sides yields $p^2 - 3r^2 = -1$, which has no solution mod 3 hence has no solution in $\mathbb{Z}$, a contradiction. Hence $Cl(\mathcal{O}_K) \ncong Cl(d_K)$.

Remark 2.10. There are ways to fix the situation above. We list two such ways below, for more details, see for example [5] Chapter 5.6.

1. Change the notion of equivalence of ideals. Replace the principal ideals $P(\mathcal{O})$ by $P^+(\mathcal{O})$ consisting of all principal ideals of positive norm. Define the *narrow ideal class group* $Cl^+(\mathcal{O}) = I(\mathcal{O})/P^+(\mathcal{O})$. It can then be shown that $Cl(D) \cong Cl^+(\mathcal{O})$ for any order of discriminant D in *any* quadratic field K, real or imaginary. In particular, if K is imaginary then we have $Cl^+(\mathcal{O}) = Cl(\mathcal{O})$, and the same is true for a real quadratic field K if $\mathcal{O}$ has a unit with norm -1. Otherwise, we have $|Cl^+(\mathcal{O})| = 2|Cl(\mathcal{O})|$.

2. Change the notion of equivalence of quadratic forms. Instead of proper equivalence, use *signed equivalence*, where two forms $f(x, y)$ and $g(x, y)$ are *signed equivalent* if there exists a matrix $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ such that

$$g(x, y) = \det \begin{pmatrix} p & q \\ r & s \end{pmatrix} \phi(px + qy, rx + sy).$$

   The set of signed equivalence classes forms a group which we denote by $Cl_S(D)$, then it can be shown that $Cl_S(D) \cong Cl(\mathcal{O})$.

It will be useful to find a way to relate proper ideals of an order $\mathcal{O}$ to ideals of the maximal order $\mathcal{O}_K$, since class field theory is almost always stated in terms of $\mathcal{O}_K$. In order to do this without encountering too much difficulty, we study ideals of $\mathcal{O}$ coprime to the conductor, which relate nicely to ideals of $\mathcal{O}_K$ as we will discover in Lemma 2.14:

Definition 2.11. Let $\mathcal{O}$ be an order of conductor f. We say that a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}$ is *prime* to f if $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$.

Here are some basic properties of ideals of $\mathcal{O}$ coprime to the conductor:

Proposition 2.12. *Let $\mathcal{O}$ be an order of conductor f, and let $\mathfrak{a}$ be an ideal of $\mathcal{O}$. Then:*

(i) $\mathfrak{a}$ is coprime to $f \Leftrightarrow gcd(N(\mathfrak{a}), f) = 1$.

(ii) $\mathfrak{a}$ is coprime to $f \Rightarrow \mathfrak{a}$ is proper.

Proof. To prove (i), consider the map $m : \mathcal{O}/\mathfrak{a} \mapsto \mathcal{O}/\mathfrak{a}$ which is multiplication by f. Then $\mathfrak{a} + f\mathcal{O} = \mathcal{O} \Leftrightarrow m_f$ is an isomorphim $\Leftrightarrow N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$ and f are coprime.
To show (ii), let $\mathfrak{a}$ be coprime to f and let $\beta \in K$ satisfy $\beta\mathfrak{a} \subset \mathfrak{a}$.We want to show $\beta \in \mathcal{O}$. Now,

$$\beta\mathcal{O} = \beta(\mathfrak{a} + f\mathcal{O}) \subset \mathfrak{a} + f\mathcal{O}_K$$

since $\beta\mathfrak{a} \subset \mathfrak{a}$ and $\mathcal{O} \subset \mathcal{O}_K$ and certainly $\beta \in \mathcal{O}_K$. However f is the conductor so $f\mathcal{O}_K \subset \mathcal{O}$, which means that $\beta\mathcal{O} \subset \mathfrak{a} + \mathcal{O} = \mathcal{O}$. Thus $\beta \in \mathcal{O}$, so $\mathfrak{a}$ is proper. □

It follows from Proposition 2.12 that ideals of $\mathcal{O}$ coprime to f lie in $I(\mathcal{O})$ and are closed under multiplication (if $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of $\mathcal{O}$ coprime to f, then $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ (2.3) and f are coprime), hence the fractional ideals they generate form a subgroup. This subgroup is denoted $I(\mathcal{O}, f) \subset I(\mathcal{O})$. We also have the subgroup $P(\mathcal{O}, f) \subset I(\mathcal{O}, f)$ generated by the principal ideals in $I(\mathcal{O}, f)$, i.e. of the form $\alpha\mathcal{O}$ where $N(\alpha\mathcal{O}) = N(\alpha)$ (2.2) is coprime to f.

Definition 2.13. For a positive integer m and an ideal $\mathfrak{a}$ of $\mathcal{O}_K$, say $\mathfrak{a}$ is *coprime to* m if $\mathfrak{a}+m\mathcal{O}_K = \mathcal{O}_K$.

This is equivalent to $\gcd(N(\mathfrak{a}), m) = 1$ (recall Proposition 2.12), so the set $I_K^m \subset I(\mathcal{O}_K)$ of fractional ideals generated by ideals of $\mathcal{O}_K$ coprime to m forms a subgroup in $I(\mathcal{O}_K)$. We are now ready to see how the ideals coprime to the conductor of $\mathcal{O}$ relate to ideals of $\mathcal{O}_K$:

Lemma 2.14. *Let $\mathcal{O}$ be an order of conductor f in an imaginary quadratic field K.*

(i) For an ideal $\mathfrak{a}$ of $\mathcal{O}_K$ coprime to f, $\mathfrak{a} \cap \mathcal{O}$ is an ideal of $\mathcal{O}$ coprime to f of the same norm.

(ii) For an ideal $\mathfrak{a}$ of $\mathcal{O}$ coprime to f, $\mathfrak{a}\mathcal{O}_K$ is an ideal of $\mathcal{O}_K$ coprime to f of the same norm.

(iii) I_K^f is isomorphic to $I(\mathcal{O}, f)$ via the isomorphism $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ whose inverse is given by $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$.

We refer the reader to [6] page 144 for the proof. We can now describe $Cl(\mathcal{O})$ in terms of the maximal order.

Proposition 2.15. *Let K be an imaginary quadratic field, and let $\mathcal{O}$ be an order of conductor f in K. Then there are natural isomorphisms*

$$Cl(\mathcal{O}) \cong I(\mathcal{O}, f)/P(\mathcal{O}, f) \cong I_K^f / P_{K,\mathbb{Z}}^f$$

where $P_{K,\mathbb{Z}}^f$ is the subgroup of $P(\mathcal{O}_K)$ generated by ideals of the form $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ satisfies $\alpha \equiv a \bmod f\mathcal{O}_K$ for some integer a coprime to f.

Proof. For the first isomorphism, consider the canonical map $I(\mathcal{O}, f) \to Cl(\mathcal{O})$. This map is surjective, since any primitive form represents numbers coprime to f so by Theorem 2.7 (iii) every ideal class in $Cl(\mathcal{O})$ contains a proper ideal whose norm is coprime to f. The kernel of this map is $I(\mathcal{O}, f) \cap P(\mathcal{O})$, and we claim that this is equal to $P(\mathcal{O}, f)$. It is clear that $I(\mathcal{O}, f) \cap P(\mathcal{O})$ contains $P(\mathcal{O}, f)$. To prove the converse, notice that an element of $I(\mathcal{O}, f) \cap P(\mathcal{O})$ is of the form $\alpha\mathcal{O} = \mathfrak{a}\mathfrak{b}^{-1}$, where $\alpha = \frac{a}{b} \in K^*$, $a, b \in \mathcal{O}$ (note $\mathrm{Frac}(\mathcal{O}) = K$ by definition of an order) and $\mathfrak{a} = a\mathcal{O}, \mathfrak{b} = b\mathcal{O}$. Let $n = N(\mathfrak{b})$ and let $\overline{\mathfrak{b}}$ denotes the conjugate of $\mathfrak{b}$, so that $N(\mathfrak{b})\mathcal{O} = n\mathcal{O} = \mathfrak{b}\overline{\mathfrak{b}}$. Then

$$n\alpha\mathcal{O} = \mathfrak{a}(n\mathfrak{b}^{-1}) = \mathfrak{a}\overline{\mathfrak{b}} \subset \mathcal{O}$$

and $N(n\alpha\mathcal{O}) = N(\mathfrak{a}\overline{\mathfrak{b}}) = N(\mathfrak{a})N(\overline{\mathfrak{b}}) = N(\mathfrak{a})N(\mathfrak{b})$ is coprime to n so $n\alpha\mathcal{O}$ is an ideal of $\mathcal{O}$ coprime to f. Also clearly $n\mathcal{O} \in P(\mathcal{O}, f)$ so $\alpha\mathcal{O} = n\alpha\mathcal{O}(n\mathcal{O})^{-1} \in P(\mathcal{O}, f)$, proving that $I(\mathcal{O}, f) \cap P(\mathcal{O}) = P(\mathcal{O}, f)$ and now the first isomorphism follows from the first isomorphism theorem.
To prove the second isomorphism, note that Lemma 2.14 (iii) tells us that the map $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$ gives an isomorphism $I(\mathcal{O}, f) \xrightarrow{\sim} I_K^f$. Let $P \subset I_K^f$ denote the image of $P(\mathcal{O}, f)$ under this map. It remains to prove $P = P_{K,\mathbb{Z}}^f$. We know $P(\mathcal{O}, f)$ is generated by the ideals $\alpha\mathcal{O}$ where $\alpha \in \mathcal{O}$ and $\gcd(N(\alpha), f) = 1$. Hence P is generated by the ideals $\alpha\mathcal{O}_K$ with $\alpha \in \mathcal{O}$ and $\gcd(N(\alpha), f) = 1$. Hence to show $P = P_{K,\mathbb{Z}}^f$ it suffices to prove that for $\alpha \in \mathcal{O}_K$,

$$\begin{aligned} &\alpha \equiv m \bmod f\mathcal{O}_K, m \in \mathbb{Z},\ \gcd(m, f) = 1 \\ &\Leftrightarrow \alpha \in \mathcal{O},\ \gcd(N(\alpha), f) = 1. \end{aligned} \tag{2.4}$$

If $\alpha \equiv m \bmod f\mathcal{O}_K$ for $m \in \mathbb{Z}$ coprime to f, then $\alpha = m + f\gamma$ for some $\gamma \in \mathcal{O}_K$. Hence $\overline{\alpha} = m + f\overline{\gamma}$, and $\overline{\gamma} \in \mathcal{O}_K$ so we also have $\overline{\alpha} \equiv m \bmod f\mathcal{O}_K$. So $\alpha\overline{\alpha} \equiv m^2 \bmod m\mathcal{O}_K$, so that $\alpha\overline{\alpha} - m^2 = f\delta$ for some $\delta \in \mathcal{O}_K$. But the LHS is an integer and so is f, hence $\delta \in \mathbb{Q}$. It follows that $\delta \in \mathbb{Z} = \mathbb{Q} \cap \mathcal{O}_K$, which gives $N(\alpha) \equiv m^2 \bmod f$. Hence $\gcd(N(\alpha), f) = \gcd(a^2, f) = 1$. But f is the conductor so we have $f\mathcal{O}_K \subset \mathcal{O}$, so $\alpha - m \equiv f\gamma$, $\gamma \in \mathcal{O}_K$ gives $\alpha = m + f\gamma \in \mathbb{Z} + f\mathcal{O}_K = \mathcal{O}$, giving $\alpha \in \mathcal{O}$.
Conversely, let $\alpha \in \mathcal{O}$ have norm coprime to f. Then $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ gives $\alpha = m + f\gamma$ for some $m \in \mathbb{Z}$, so $\alpha \equiv m \bmod f\mathcal{O}_K$. Then $N(\alpha) \equiv m^2 \bmod f$ as before, so the assumption $\gcd(N(\alpha), f) = 1$ implies $\gcd(a, f) = 1$ as required. □

Now we state one of the nicest applications of Proposition 2.15 which gives a formula for the class number $h(\mathcal{O})$ in terms of its conductor f and the class number of the maximal order $h(\mathcal{O}_K)$.

Theorem 2.16. *Let $\mathcal{O}$ be an order of conductor f in an imaginary quadratic field K. Then*

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right), \tag{2.5}$$

where p runs through the primes which divide f, $\left(\frac{d_K}{p}\right)$ denotes the Legendre symbol for an odd prime p and the Kronecker symbol for $p = 2$:

$$\left(\frac{d_K}{2}\right) = \begin{cases} 0 & \text{if } 2 \mid d_K \\ 1 & \text{if } d_K \equiv 1 \bmod 8 \\ -1 & \text{if } d_K \equiv 5 \bmod 8. \end{cases}$$

Moreover, $h(\mathcal{O}_K)$ always divides $h(\mathcal{O})$.

The following corollary is due to Gauss, and it gives a relation between the class numbers $h(m^2D)$ and $h(D)$:

Corollary 2.17. *Let D be a negative, $D \equiv 0, 1 \bmod 4$, and let m be a positive integer. Suppose $\mathcal{O}$ and $\mathcal{O}'$ are orders of discriminant D and m^2D respectably, and $\mathcal{O}'$ has index m in $\mathcal{O}$. Then,*

$$h(m^2D) = \frac{h(D)m}{[\mathcal{O}^* : \mathcal{O}'^*]} \prod_{p|m} \left(1 - \left(\frac{D}{p}\right)\frac{1}{p}\right).$$

Proof. Suppose $\mathcal{O}$ has conductor f, then $\mathcal{O}' \subset \mathcal{O}$ of index m has conductor mf. Then we can get the formula for $h(\mathcal{O}) = h(D)$ and $h(\mathcal{O}') = h(m^2D)$ using Theorem 2.16. Dividing $h(m^2D)$ by $h(D)$ gives

$$\frac{h(m^2D)}{h(D)} = \frac{m}{[\mathcal{O}^* : \mathcal{O}'^*]} \prod_{p|m} \left(1 - \left(\frac{D}{p}\right)\frac{1}{p}\right),$$

and the corollary follows. □

Theorem 2.16 also enables us to reduce the computation of $h(D)$ for $D < 0$, $D \equiv 0, 1 \bmod 4$ to the computation of $h(d_K)$. For $h(d_K)$ we have the classic formula

$$h(d_K) = \sum_{n=1}^{|d_K|-1} \left(\frac{d_K}{n}\right) n,$$

where $\left(\frac{d_K}{n}\right)$ denotes the Jacobi symbol. This formula is proved using analytic methods in [4] Chapter 5, Section 4.

Determining which orders have class number h remains a difficult problem even when h is small. The case $h = 1$ is what we call the class number one problem, and it is formulated in the following theorem:

Theorem 2.18. *(i) Let K be an imaginary quadratic field of discriminant d_K. Then*

$$h(d_K) = 1 \Leftrightarrow d_K = -3, -4, -7, -8, -11, -19, -43, -67, -163.$$

(ii) Let $D \equiv 0, 1 \bmod 4$, $D < 0$. Then

$$h(D) = 1 \Leftrightarrow D = -3, -4, -7, -8, -11, -12, -19, -27, -28, -43, -67, -163.$$

Remark 2.19. Here we only prove (i)⇒(ii). The proof of (i) is dealt with in Section 6.

Proof of (i) ⇒(ii). To see this, suppose $h(D) = 1$ where $D = f^2 d_K$. Then Theorem 2.16 and Remark 2.8 tells us $h(d_K) \mid h(D)$, giving $h(d_K) = 1$. Then (i) gives all the possibilities for d_K but we still need to find which conductors $f > 1$ can occur.
Case 1. $\mathcal{O}_K^* = \{\pm 1\}$.
If $f > 2$, then (2.5) gives

$$\begin{aligned} h(D) &= f \prod_{p \mid f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right) \\ &\geqslant p_1^{\alpha_1} \cdots p_n^{\alpha_n} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_n}\right) \qquad \text{(where } f = p_1^{\alpha_1} \cdots p_n^{\alpha_n}\text{)} \\ &= p_1^{\alpha_1 - 1} \cdots p_n^{\alpha_n - 1}(p_1 - 1) \cdots (p_n - 1) \\ &> 1 \end{aligned}$$

since $h(\mathcal{O}_K) = 1$ and $[\mathcal{O}_K^* : \mathcal{O}^*] = 1$, which contradicts the assumption $h(D) = 1$. One can check directly using (i) and Theorem 2.16 that $f = 2$ only happens when $d_K = -7$, i.e., $D = -28$.
Case 2. $\mathcal{O}_K^* \neq \{\pm 1\}$.
In the list (i), this case only happens if $d_K = -3$ or -4, in which case we have $\mathcal{O}_K^* = \{\pm 1, \frac{\pm 1 \pm \sqrt{3}}{2}\}$ and $\{\pm 1, \pm i\}$ respectably. Hence when $d_K = -3$ we can have $[\mathcal{O}_K^* : \mathcal{O}^*] = 1, 3$, then a similar argument as above yields $D = -27$. Similarly when $d_K = -4$, we can have $[\mathcal{O}_K^* : \mathcal{O}^*] = 1, 2$, then direct calculation yields $D = -12$. Hence we have (i) ⇒ (ii) as we claimed.

The proof of (i) was covered when the discriminant is even in Theorem 1.1, but when the discriminant is odd, the proof is *much* more difficult. In Section 4, we will study modular functions to give a complete proof of (i). □

3 Ring Class Fields

In this section, we will study abelian extension, i.e. a finite extension whose Galois group is abelian. The Čaboterev density theorem says, roughly speaking, that infinitely many primes gives the same Frobenius element; see Definition 3.3. This result is needed to prove that the Artin map is surjective. Other results proved by analytic technique include the famous Dirichlet's theorem on primes in arithmetic progressions. We will also see that it can be used to prove that a primitive positive definite quadratic form represents infinitely many prime numbers.

Definition 3.1. Let L/K be a Galois extention. Let $\mathfrak{B}$ be a prime of $\mathcal{O}_L$. Then define the *decomposition group* and *inertia group* of $\mathfrak{B}$ by

$$D_{\mathfrak{B}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{B}) = \mathfrak{B}\}$$

$$I_{\mathfrak{B}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(a) = a \bmod \mathfrak{B} \text{ for all } a \in \mathcal{O}_L\}.$$

Prime ideals of $\mathcal{O}_K$ are sometimes called *finite primes* to dinstinguish them from *infinite primes* which refer to the embeddings $K \to \mathbb{C}$. A real embedding is called a *real infinite prime* and a pair of complex conjugate embeddings is called a *complex infinite prime*. Given an extension L/K, let $\mathfrak{p}$ be a finite prime of K and let $\mathfrak{B}_\mathfrak{i}$ be a prime of L lying over $\mathfrak{p}$. We can write

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_i^{e_1} \cdots \mathfrak{B}_g^{e_g}$$

where $e_i \in \mathbb{Z}_{>0}$ and is called the *ramification index* of $\mathfrak{B}_i$. We say $\mathfrak{p}$ is *ramified* if $e_i > 1$ for some i and is *unramified* otherwise. If there is a unique prime $\mathfrak{B}$ lying over $\mathfrak{p}$ and with inertial degree 1,

then we say $\mathfrak{p}$ *ramifies totally* in L. Given an extension L/K, an infinite prime of K is *ramified* in L if it is real but it has an extension to L which is complex. It is *unramified* otherwise. An extension L/K is called *unramified* if it is unramified at all primes, finite or infinite.

Lemma 3.2. *Let L/K be a Galois extension, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ unramified in L. Let $\mathfrak{B}$ be a prime of $\mathcal{O}_L$ lying over $\mathfrak{p}$. Then there exists a unique element $\sigma \in \mathrm{Gal}(L/K)$ such that*

$$\sigma(a) \equiv a^{N(\mathfrak{p})} \ mod\ \mathfrak{B}$$

for all $a \in \mathcal{O}_L$, where $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ is the norm of $\mathfrak{p}$. □

Definition 3.3. The unique such σ in Lemma 3.2 is denote it by $\left(\frac{L/K}{\mathfrak{B}}\right)$.

Hence we have

$$\left(\frac{L/K}{\mathfrak{B}}\right)(a) \equiv a^{N(\mathfrak{p})} \bmod \mathfrak{B}$$

where $\mathfrak{p} = \mathfrak{B} \cap \mathcal{O}_K$ is a prime which is unramified in L. Some basic and useful properties of the of $\left(\frac{L/K}{\mathfrak{B}}\right)$ are as follows:

Corollary 3.4. *Let L/K be a Galois extension and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ which is unramified in L. Then for a prime $\mathfrak{B}$ of $\mathcal{O}_L$ containing $\mathfrak{p}$ and $\sigma \in \mathrm{Gal}(L/K)$, we have*

$$\left(\frac{L/K}{\sigma(\mathfrak{B})}\right) = \sigma\left(\frac{L/K}{\mathfrak{B}}\right)\sigma^{-1}$$

Proof. Let $\sigma \in \mathrm{Gal}(L/K)$ and $a \in \mathcal{O}_L$. Then

$$\left(\frac{L/K}{\mathfrak{B}}\right)(\sigma^{-1}(a)) \equiv (\sigma^{-1}(a))^{N(\mathfrak{p})} \bmod \mathfrak{B}$$

so applying σ on the left gives

$$\sigma\left(\frac{L/K}{\mathfrak{B}}\right)\sigma^{-1} \equiv a^{N(\mathfrak{p})} \bmod \sigma(\mathfrak{B}),$$

so we have $\sigma\left(\frac{L/K}{\mathfrak{B}}\right)\sigma^{-1} = \left(\frac{L/K}{\sigma(\mathfrak{B})}\right)$. □

It follows that $\left(\frac{L/K}{\mathfrak{B}}\right)$ is defined up to conjugacy by a knowledge of $\mathfrak{p}$. We write $\mathrm{Frob}_{\mathfrak{p}}$ for this conjugacy class. Moreover, if L/K is an abelian extension then $\mathrm{Frob}_{\mathfrak{p}}$ is a conjugacy class of size 1 (as $\left(\frac{L/K}{\sigma(\mathfrak{B})}\right) = \left(\frac{L/K}{\mathfrak{B}}\right)$ for all $\sigma \in \mathrm{Gal}(L/K)$ and for any two primes $\mathfrak{B}'$ and $\mathfrak{B}$ lying over $\mathfrak{p}$, there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{B}) = \mathfrak{B}'$), so in this case we can consider $\mathrm{Frob}_{\mathfrak{p}}$ as an element of $\mathrm{Gal}(L/K)$, and we call it the *Frobenius element*.

When L/K is an abelian extension, $\mathrm{Frob}_{\mathfrak{p}}$ is defined for all primes $\mathfrak{p}$ of $\mathcal{O}_K$ unramified in L/K. Then by multiplication, we can define the Frobenius element for any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$. Let $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i{}^{a_i}$ be a prime factorisation of $\mathfrak{a}$. Then define the Frobenius element for $\mathfrak{a}$ by

$$\mathrm{Frob}_{\mathfrak{a}} = \prod_{i=1}^{r} (\mathrm{Frob}_{\mathfrak{p}_i})^{a_i}.$$

To discuss more general results, we introduce the notion of a modulus in a number field:

Definition 3.5. A *modulus* for a number field K is a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

taken over all primes $\mathfrak{p}$ of K, finite or infinite, in which $n_{\mathfrak{p}}$ is a non-negative integer and $n_{\mathfrak{p}} = 0$ for for almost all primes $\mathfrak{p}$. Furthermore, $n_{\mathfrak{p}} = 0$ or 1 when $\mathfrak{p}$ is a real infinite prime and $n_{\mathfrak{p}} = 0$ when $\mathfrak{p}$ is a complex infinite prime.

A modulus may be considered as a product $\mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is the product of the finite primes appearing with positive exponent (i.e. an ideal of $\mathcal{O}_K$) and $\mathfrak{m}_\infty$ the product of distinct real infinite primes of K. Note that in a imaginary quadratic field, a modulus is just an ideal of $\mathcal{O}_K$.

Given a modulus $\mathfrak{m}$, let $I_K^{\mathfrak{m}}$ denote the group of all fractional ideals of $\mathcal{O}_K$ coprime to $\mathfrak{m}$ (this means coprime to $\mathfrak{m}_0$), and let $P_{K,1}^{\mathfrak{m}}$ denote subgroup of $I_K^{\mathfrak{m}}$ generated by the principal ideals $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ satisfies:

$$\alpha \equiv 1 \bmod \mathfrak{m}_0 \text{ and for every infinite prime } \sigma \text{ such that } \sigma \mid \mathfrak{m}_\infty \text{ we have } \sigma(\alpha) > 0.$$

A basic result is that $P_{K,1}^{\mathfrak{m}}$ has finite index in $I_K^{\mathfrak{m}}$ ([10] Chapter IV.1). A subgroup H of $I(\mathcal{O}_K)$ is called a *congruence subgroup* if there is a modulus $\mathfrak{m}$ such that

$$P_{K,1}^{\mathfrak{m}} \subset H \subset I_K^{\mathfrak{m}},$$

and the quotient

$$I_K^{\mathfrak{m}}/H$$

is called a *generalised ideal class group* for $\mathfrak{m}$.

The basic idea of class field theory is that the generalised ideal class groups are the Gaois groups of all abelian extensions of K, and the correspondence between these are provided by the *Artin map* of an abelian extension L/K.

Let L/K be an abelian extension, and let $\mathfrak{m}$ be a modulus which is a product of all primes of K ramified in L/K. Given a prime $\mathfrak{p}$ of K such that $\mathfrak{p} \nmid \mathfrak{m}$ (i.e. $\mathfrak{p}$ is a prime of K unramified in L/K), we have the Frobenius element $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$. This extends by multiplicativity to give a homomorphism

$$\begin{aligned} \Phi_{\mathfrak{m}} : I_K^{\mathfrak{m}} &\to \mathrm{Gal}(L/K) \\ \mathfrak{p} &\mapsto \mathrm{Frob}_{\mathfrak{p}}\,. \end{aligned}$$

This is called the *Artin map* for L/K and $\mathfrak{m}$.

The first theorem of class field theory states that $\mathrm{Gal}(L/K)$ is a generalised ideal class group for some modulus:

Theorem 3.6 (**Artin reciprocity thorem**). *Let L/K be an abelian extension, and let $\mathfrak{m}$ be a modulus divisible at least by all ramified primes of K. Then:*

(i) The Artin map Φ_m is surjective.

(ii) When the exponents of the prime divisors of $\mathfrak{m}$ are sufficiently large, $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$, and consequently the isomorphism

$$I_K^{\mathfrak{m}}/\ker\Phi_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Gal}(L/K)$$

shows that $\mathrm{Gal}(L/K)$ is a generalised ideal class group for the modulus $\mathfrak{m}$.

Proof. See [10], Chapter V, Theorem 5.7. □

Example 3.7. Let us consider the cyclotomic extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, where $m \geqslant 1$ is an integer and $\zeta_m = e^{2\pi i/m}$ is the primitive m th root of unity. Let $\mathfrak{m}$ be the modulus $m\infty$, where ∞ is the real infinite prime of $\mathbb{Q}$. Then all finite ramified primes of this extension divide m (this can be proved by by induction on the number of primes dividing m, see [13], Chapter 6, Theorem 6.4 for more details) so any prime not dividing $\mathfrak{m}$ is unramified in $\mathbb{Q}(\zeta_m)$ and the Artin map

$$\begin{aligned} \Phi_{\mathfrak{m}} : I_{\mathbb{Q}}^{\mathfrak{m}} &\to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^* \\ p &\mapsto \mathrm{Frob}_p \end{aligned}$$

is defined. We can describe $\Phi_{\mathfrak{m}}$ as follows: given $\left(\frac{a}{b}\mathbb{Z}\right) \in I_{\mathbb{Q}}$, where $a, b \in \mathbb{Z}$, $\frac{a}{b} > 0$ and $\gcd(a, m) = \gcd(b, m) = 1$, we have

$$\Phi_{\mathfrak{m}}\left(\frac{a}{b}\mathbb{Z}\right) = [a][b]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^*.$$

To see this, recall that Frob_p must satisfy the condition

$$\mathrm{Frob}_p(\zeta_m) \equiv \zeta_m^p \bmod \mathfrak{B}$$

where $\mathfrak{B}$ is a prime of $\mathcal{O}_{\mathbb{Q}(\zeta_m)}$ containing p, so Frob_p corresponds to p in $(\mathbb{Z}/m\mathbb{Z})^*$. It follows that

$$\ker \Phi_{\mathfrak{m}} = P_{\mathbb{Q},1}^{\mathfrak{m}}.$$

The following theorem is a fundamental result in class field theory which asserts that *every* generalised ideal class group is the Galois group of some abelian extension L/K.

Theorem 3.8 (**Takagi Existence Theorem**). *Let $\mathfrak{m}$ be a modulus of a number field K, and let H be a congruence subgroup for $\mathfrak{m}$, i.e., $P_{K,1}^{\mathfrak{m}} \subset H \subset I_K^{\mathfrak{m}}$. Then there is a unique abelian extension L/K all of whose ramified primes divide $\mathfrak{m}$, such that if*

$$\Phi_{\mathfrak{m}} : I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$$

is the Artin map of L/K, then $H = \ker(\Phi_{\mathfrak{m}})$.

Proof. See [10], Chapter V, Theorem 9.16. □

We can finally define the Hilbert class field. Let us apply the Existence Theorem 3.8 to the modulus $\mathfrak{m} = 1$, and note that $P_{K,1}^1 = P(\mathcal{O}_K)$ and $I_K^1 = I(\mathcal{O}_K)$. Then we can take $H = P(\mathcal{O}_K)$ to be a congruence group. Then Theorem 3.8 gives us a unique abelian unramified (since $\mathfrak{m} = 1$) extension L/K, such that the Artin map induces an isomorphism

$$Cl(\mathcal{O}_K) = I(\mathcal{O}_K)/P(\mathcal{O}_K) \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

This unique field L is the *Hilbert class field* of K. Its main property is the following:

Theorem 3.9. *The Hilbert class field L is the maximal unramified abelian extension of K.*

Proof. We leave the proof to [6] Chapter 8, Theorem 8.10. □

We will state some immediate consequences of Theorem 3.9.

Corollary 3.10. *Given a number field K, there exists a finite Galois extension L/K such that:*

(i) L/K is an unramified abelian extension.

(ii) Any unramified abelian extension of K lies in L.

Proof. Let L be the Hilbert class field of K and apply Theorem 3.9. □

Theorem 3.11 (**Artin reciprocity thorem for the Hilbert class field**). *Let L be the Hilbert class field of K. Then the Artin map*

$$\Phi : I(\mathcal{O}_K) \to \mathrm{Gal}(L/K)$$

is a surjective homomorphism and its kernel is exactly the principal ideals $P(\mathcal{O}_K)$, i.e. $Cl(\mathcal{O}_K) \cong \mathrm{Gal}(L/K)$.

Proof. This is just Theorem 3.6 applied to the Hilbert class field. □

From this we obtain the following corollary which is one of the main themes of class field theory:

Corollary 3.12 (**The Classification Theorem for unramified abelian extensions**). *Given a number field K, there is a bijection between unramified abelian extensions M/K and subgroups H of $Cl(\mathcal{O}_K)$. Furthermore, if the extension M/K corresponds to the subgroup $H \subset Cl(\mathcal{O}_K)$, then the Artin map induces an isomorphism*

$$Cl(\mathcal{O}_K)/H \xrightarrow{\sim} \mathrm{Gal}(M/K).$$

Recall from Theorem 2.7 that if $d_K < 0$, then there is a natural isomorphism between the form class group $Cl(d_K)$ and the ideal class group $Cl(\mathcal{O}_K)$. Hence by Theorem 3.11 we get that the Galois group $\mathrm{Gal}(L/K)$ of the Hilbert class field of an imaginary quadratic field K is isomorphic to the form class group $Cl(d_K)$.

Let us now talk about the Čebotarev density theorem which will help us prove that the Artin map is surjective in a very strong sense. But first, we need to define the Dirichlet density:

Definition 3.13. Let S be a set of finite primes of an algebraic number field K. Then the *Dirichlet density* of S is defined to be the real number

$$\delta(S) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{-\log(s-1)}$$

provided that the limit exists.

A basic property of the Dirichlet density is that if S has $\delta(S) \neq 0$ then S is an infinite set.

Now let L/K be a Galois extension, not necessarily abelian. In this case, given an unramified prime $\mathfrak{p}$ of K, different primes $\mathfrak{B}$ of L such that $\mathfrak{B} \mid \mathfrak{p}$ may give us different $\left(\frac{L/K}{\mathfrak{B}}\right)$, all of which are conjugate by Corollary 3.4. In fact they form a conjugacy class in $\mathrm{Gal}(L/K)$. Thus we can define $\mathrm{Frob}_{\mathfrak{p}}$ to be this conjugacy class in $\mathrm{Gal}(L/K)$. We can now state the Čebotarev density theorem:

Theorem 3.14 (**Čebotarev Density Theorem**). *Let L/K be a Galois extension, and let $\sigma \in \mathrm{Gal}(L/K)$ have conjugacy class $[\sigma]$ of size c. Define S to be the set of finite primes $\mathfrak{p}$ of K unramified in L/K satisfying $\mathrm{Frob}_{\mathfrak{p}} = [\sigma]$. Then*

$$\delta(S) = \frac{c}{|\mathrm{Gal}(L/K)|}.$$

Proof. See [10] Chapter V, Theorem 10.4. □

Notice that we have $\delta(S) > 0$ in Theorem 3.14 which tells us S must be an infinite set by the basic property of the Dirichlet density. In particular, we get the following corollary for abelian extension. Note that if L/K is an abelian extension, given any $\sigma \in \mathrm{Gal}(L/K)$ we have $[\sigma] = \{\sigma\}$ by Corollary 3.4.

Corollary 3.15. *Let L/K be an abelian extension, and let $\mathfrak{p}$ be a modulus divisible by all primes of K ramified in L/K. Then given any $\sigma \in \mathrm{Gal}(L/K)$, the set S of primes $\mathfrak{p}$ not dividing $\mathfrak{m}$ such that $\mathrm{Frob}_{\mathfrak{p}} = \sigma$ has density*

$$\delta(S) = \frac{1}{[L:K]}$$

Proof. Immediate from Theorem 3.14, since we have $|[\sigma]| = 1$ and $|Gal(L/K)| = [L : K]$ for any Galois extension L/K. □

In particular, this corollary shows that the set S in Corollary 3.15 is infinite since S has positive density, proving that the Artin map $\Phi_{\mathfrak{m}} : I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is not only surjective, but given $\sigma \in Gal(L/K)$ there are *infinitely many* $\mathfrak{p} \in I_K^{\mathfrak{m}}$ which map to σ via $\Phi_{\mathfrak{m}}$.

We conclude this section by introducing the ring class field. To define it, let $\mathcal{O}$ be an order of conductor f in an imaginary quadratic field K. Then we know

$$Cl(\mathcal{O}) \cong I_K^f / P_{K,\mathbb{Z}}^f \tag{3.1}$$

and that

$$P_{K,1}^f \subset P_{K,\mathbb{Z}}^f \subset I_K^f.$$

Hence $Cl(\mathcal{O})$ is a generalised ideal class group for the modulus $f\mathcal{O}_K$. By the Existence Theorem 3.8, this determines a unique abelian extension L/K. We call this L the *ring class field* of the order $\mathcal{O}$.

The basic properties of the ring class field L are the following:

1. All primes of K ramified in L must divide $f\mathcal{O}_K$.
2. The Artin map and the isomorphism (3.1) gived us

$$Cl(\mathcal{O}) \cong I_K^f / P_{K,\mathbb{Z}}^f \cong \mathrm{Gal}(L/K).$$

In particular, we get that the degree of L over K is the class number, i.e.

$$[L : K] = h(\mathcal{O}). \tag{3.2}$$

As an example of a ring class field, note that the ring class field for the maximal order $\mathcal{O}_K$ is the Hilbert class field of K.

4 Global Class Field Theory

Modern presentation of class field theory is given in terms of *idèles*. In this section, we will give the reader a sence of the important topics which have been left out in our discussion of class field theory, and restate some important results from the previous section in the modern language. The idèlic approach has some distinct advantages, as we will discover below.

Let K be a number field. A *place* of K is a class of equivalent valuations of K. There is a place for every non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ and for every equivalence class of embeddings $K \to \mathbb{C}$. The former is called a *finite place* and the latter is called an *infinite place*. The infinite places fall into two classes, the real and the complex ones. The real places are in bijection with the distinct embeddings $K \to \mathbb{R}$, and the complex places are in bijection with the pairs of conjugate non-real embeddings $K \to \mathbb{C}$. We write $v \nmid \infty$ if v is finite and $v \mid \infty$ if v is infinite, and we set $S_\infty = \{v \mid \infty\}$.

If $v \notin S_\infty$, let $\mathfrak{p}$ be the associated prime of $\mathcal{O}_K$ and let $\nu = \nu_\mathfrak{p}$ denote the corresponding valuation of K, i.e. for $x \in K^*$, let

$$\nu(x) = \text{powers of } \mathfrak{p} \text{ in the factorisation of } x\mathcal{O}_K \text{ as fractional ideals.}$$

Then define $|\cdot|_v$ in the following way.
If $v \notin S_\infty$, then

$$|x|_v = \begin{cases} \alpha^{\nu(x)} & \text{if } x \in K^* \\ 0 & \text{if } x = 0. \end{cases}$$

for a suitable α where $0 < \alpha < 1$ (we often take $\alpha = N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|^{-1}$, where $\mathfrak{p}$ is the prime of $\mathcal{O}_K$ associated with v). If v is real infinite and $\sigma : K \to \mathbb{R}$ is the corresponding embedding, then $|x|_v = |\sigma(x)|$ for $x \in K$. If v is complex infinite and $\sigma : K \to \mathbb{R}$ is one of the corresponding embeddings, then $|x|_v = |\sigma(x)|^2$ for $x \in K$.

Having normalised $|\cdot|_v$ in this way then $|x|_\mathfrak{p} = 1$ for almost all $\mathfrak{p}$ and $x \in K^*$. For each $\mathfrak{p}$, we also have the completion $K_\mathfrak{p}$ of K with respect to $|\cdot|_\mathfrak{p}$. If $p \notin S_\infty$, then $K_\mathfrak{p}$ is a $\mathfrak{p}$-adic number field, i.e. $[K_\mathfrak{p} : \mathbb{Q}_\mathfrak{p}] < \infty$. We write $\mathcal{O}_\mathfrak{p}$ for $\mathcal{O}_{K_\mathfrak{p}}$.

In place of ideals of a field, we will now study the idèles, originally known as ideal elements: a concept originated by Chevalley.

Definition 4.1. Let K be a number field. An *adèle* of K is a family $x = (x_v)$ of elements $x_v \in K_v$, where v runs over all places of K such that $|x_v|_v \leqslant 1$ for almost all v. The adèles form a ring, denoted by

$$\mathbb{A}_K \subset \prod_{v \text{ places of } K} K_v,$$

where addition and multiplication are defined componentwise. An *idèle* is a unit in this ring, i.e. an element in $\mathbb{A}_K^*$

Hence we have $\mathbb{A}_K^* = (\mathbb{A}_K^*)^{\mathrm{f}} \times (\mathbb{A}_K^*)^{\mathrm{inf}}$ where $(\mathbb{A}_K^*)^{\mathrm{f}} = \prod_{v \nmid \infty}{}' K_v^* \supset \prod_{v \nmid \infty} \mathcal{O}_v$ where $\prod'$ means the product consists of (x_v) such that $|x_v|_v = 1$ for almost all x_v, and $(\mathbb{A}_K^*)^{\mathrm{inf}} = \prod_{v|\infty} K_v^*$. The quotient group

$$C_K = (\mathbb{A}_K^*)/K^*$$

is called the *idèle class group.*

Definition 4.2. Given a finite extension L/K, we can define a norm map $N_{L/K} : \mathbb{A}_L^* \to \mathbb{A}_K^*$ as follows: Let M/K be the normal closure of L/K. Then $\mathbb{A}_L^*$ is the fixed module of $\mathbb{A}_M^*$ under $\mathrm{Gal}(M/L)$ (i.e. $\mathbb{A}_L^* = (\mathbb{A}_M^*)^{\mathrm{Gal}(M/L)}$) and

$$N_{L/K}(\alpha) = \prod_\sigma \sigma(\alpha) \text{ for } \alpha \in \mathbb{A}_L^*$$

where σ runs over a system of representatives of $\mathrm{Gal}(M/K) \Big/ \mathrm{Gal}(M/L)$. Then we have $\tau(N_{L/K}(\alpha)) = N_{L/K}(\alpha)$ for every $\tau \in \mathrm{Gal}(M/K)$, hence $N_{L/K}(\alpha) \in \mathbb{A}_K^*$.

We can now restate Theorem 3.6 using idèles.

Theorem 4.3. *Let L/K be an abelian extension. Then there is a map*

$$F_{L/K} : C_K \to \mathrm{Gal}(L/K)$$

which is surjective, with $\ker(F_{L/K}) = N_{L/K}(C_L)$*, i.e.*

$$\mathrm{Gal}(L/K) \cong ((\mathbb{A}_K^*)/K^*) \Big/ N_{L/K}((\mathbb{A}_L^*)/L^*)).$$

Thus the subgroups of C_K *of finite index are precisely the norm groups* $N_{L/K}(C_L)$*.*

The following theorem is a restatement of Theorem 3.8. In the idèle class group C_K, we consider the natural topology induced by the valuations of the completions K_v of K (an element of $\mathbb{A}_K^*$ has the form $\alpha = (\alpha_v)$ where $|\alpha_v|_v = 1$ for almost all places v. A sequence of idèles $\alpha^{(n)} = (\alpha_v^{(n)})$ is said to converge to α if it converges componentwise and if there exists an integer $N > 0$ such that $|\alpha_v^{-1}\alpha_v^{(n)}|_v = 1$ for $n > N$ and for all v). The idèle group is a locally compact topological group in this topology.

Theorem 4.4 (**The Existence Theorem for Global Class Field Theory**)**.** *Let* K *be a number field. Then there is a bijection between the finite abelian extensions* L/K *and the closed subgroups of finite index in* C_K *given by the map*

$$L \mapsto N_{L/K}(C_L).$$

If L/K *is associated to the subgroup* $\mathcal{N}$ *of* C_K*, then* L *is called the* class field *of* $\mathcal{N}$*.*

For each finite prime $\mathfrak{p}$ of a number field K, let

$$U_\mathfrak{p}^n = \{x \in \mathcal{O}_\mathfrak{p} : x \equiv 1 \bmod \mathfrak{p}^n\}$$

for $n > 0$ and let $U_\mathfrak{p}^0 = U_\mathfrak{p} = \mathcal{O}_\mathfrak{p}^*$. In addition, for a infinite prime $\mathfrak{p}$ define $U_\mathfrak{p}^1 = \mathbb{R}_+$, the positive reals, and $U_\mathfrak{p}^0 = \mathbb{R}^*$ if $\mathfrak{p}$ is real infinite, and $U_\mathfrak{p}^0 = \mathbb{C}^*$ if $\mathfrak{p}$ is complex infinite.

If $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}$ is a modulus, then for every idèle $\alpha = (\alpha_\mathfrak{p}) \in \mathbb{A}_K^*$ we write

$$\alpha \equiv 1 \bmod \mathfrak{m} \Leftrightarrow \alpha_\mathfrak{p} \equiv 1 \bmod \mathfrak{p}^{n_\mathfrak{p}} \text{ for all } \mathfrak{p}$$

and we consider the groups

$$(\mathbb{A}_K^*)^\mathfrak{m} = \{\alpha \in \mathbb{A}_K^* : \alpha \equiv 1 \bmod \mathfrak{m}\} = \prod_\mathfrak{p} U_\mathfrak{p}^{n_\mathfrak{p}}.$$

Definition 4.5. Given a modulus $\mathfrak{m}$, the group

$$C_K^\mathfrak{m} = (\mathbb{A}_K^*)^\mathfrak{m} K^*/K^* \subset C_K$$

is called the congruence subgroup mod $\mathfrak{m}$ of C_K. The factor group $C_K/C_K^\mathfrak{m}$ is called the *ray class group* mod $\mathfrak{m}$. The ray class field mod 1, C_K/C_K^1 is isomorphic to the ideal class group $I(\mathcal{O}_K)$.

Theorem 4.6. *The closed subgroups* $\mathcal{N}$ *of* C_K *of finite index (called the* norm groups*) are precisely the subgroups of* C_K *containing a congruence subgroup* $C_K^\mathfrak{m}$*.*

Proof. See [14] Theorem 7.3. □

The class field $K^\mathfrak{m}$ of the congruence subgroup $C_K^\mathfrak{m}$ is called the *ray class field* mod $\mathfrak{m}$. Its Galois group is isomorphic to the ray class group,

$$\mathrm{Gal}(K^\mathfrak{m}/K) \cong C_K/C_K^\mathfrak{m}.$$

In particular, the ray class field mod 1 is the *Hilbert class field* of K, and indeed we have

$$\mathrm{Gal}(K^1/K) \cong C_K/C_K^1 \cong I(\mathcal{O}_K).$$

5 Modular Functions and Complex Multiplication

In this section we will study the j-function and complex multiplication. A key role is played by the j-invariant of a lattice $\Lambda \subset \mathbb{C}$, and we will see that if $\mathcal{O}$ is an imaginary quadratic field, then its j-invariant $j(\mathcal{O})$ is an algebraic integer which generates the ring class field of $\mathcal{O}$ over K. This is often called the "First Main Theorem" of complex multiplication. But before we can get to the real depth of the subject, we need to learn about modular functions.

A *lattice* is an additive subgroup Λ of $\mathbb{C}$ generated by two elements $\omega_1, \omega_2 \in \mathbb{C}$ linearly independent over $\mathbb{R}$; we write $\Lambda = [\omega_1, \omega_2]$. Given a lattice, we can define an elliptic function:

Definition 5.1. An *elliptic function* for a lattice Λ is a function $f(z)$ defined on all of $\mathbb{C}$ except for isolated singularities, which satisfies

(i) $f(z)$ is meromorphic on $\mathbb{C}$.

(ii) $f(z+\omega) = f(z)$ for all $\omega \in \Lambda$.

Note that if $\Lambda = [\omega_1, \omega_2]$, (ii) is equivalent to saying

$$f(z+\omega_1) = f(z+\omega_2) = f(z) \text{ for all } z \in \mathbb{C}.$$

Thus an elliptic function is a doubly periodic meromorphic function, and elements of Λ are referred to as *periods*.

Elliptic functions depend on the lattice used, but sometimes different lattices can give basically the same elliptic functions. We say that the two lattices Λ and Λ' are *homothetic* if there exists a nonzero complex number λ such that $\Lambda' = \lambda\Lambda$. We note that homothety is an equivalence relation.

Before we can go further, we need to introduce the most important elliptic function, the *Weierstrass $\wp$-function* $\wp(z;\Lambda)$, which is defined as follows: given a lattice Λ and $z \in \mathbb{C} - \Lambda$, set

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

When it is clear which lattice we are using, we write $\wp(z)$ for $\wp(z;\Lambda)$. Subtracting $1/\omega^2$ from $1/(z-\omega)^2$ makes the summand roughly z/ω^3 (cf. [7] proof of Proposition 1.4.1), so the sum converges absolutely and uniformly on compact subsets of $\mathbb{C}$ away from Λ. Correcting the sum this way prevents the terms of the sum from being permuted when z is translated by a lattice element $\omega \in \Lambda$, so $\wp$ does not obviously have periods Λ. However, the derivative

$$\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}$$

clearly does have periods Λ, and combining this with the fact that $\wp$ is an even function shows that in fact $\wp$ has periods Λ as well. For $k > 2$ even, we can define functions of variable lattice,

$$G_k(\Lambda) = \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^k}.$$

When $\Lambda = [1, \tau]$, $\tau \in \mathcal{H}$, we write $\Lambda = \Lambda_\tau$. Then we have

$$G_k(\Lambda_\tau) = \sum_{(c,d)}{}' \frac{1}{(c\tau + d)^k}$$

where $\sum'$ means to sum over nonzero integer pairs $(c,d) \in \mathbb{Z}^2 - \{(0,0)\}$.

Proposition 5.2. *Let $\wp(z)$ be the Weierstrass $\wp$-function for the lattice Λ. Then*

(i) $\wp(z)$ satisfies the differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda),$$

where $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$.

(ii) $\wp(z)$ satisfies the addition law

$$\wp(z+w) = -\wp(z) - \wp(w) + \frac{1}{4}\left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}\right)^2$$

for z, w and $z + w \notin \Lambda$.

(iii) Let $\Lambda = [\omega_1, \omega_2]$ and let $\omega_3 = \omega_1 + \omega_2$. Then the cubic equation in (i) satisfied by $\wp$ and $\wp'$ is

$$y^2 = 4(x - e_1)(x - e_2)(x - e_3), \qquad e_i = \wp(\omega_i/2) \text{ for } i = 1, 2, 3.$$

Moreover, the right side has distinct roots.

In the case $\Lambda = [1, \tau]$, we write $g_i(\tau)$ for $g_i(\Lambda)$ for $i = 1, 2$. If we specialise to the case $z = w$ in (ii), then L'Hôpital's rule gives the following duplication formula:

$$\wp(2z) = -2\wp(z) + \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2. \tag{5.1}$$

However, the differential equation in (i) gives that

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$
$$\wp''(z) = 6\wp(z)^2 - (1/2)g_2$$

and substitution then gives

$$\wp(2z) = -2\wp(z) + \frac{(12\wp(z)^2 - g_2)^2}{16(4\wp(z)^3 - g_2\wp(z) - g_3)}.$$

Thus $\wp(2z)$ is a rational function in $\wp(z)$. In fact, one of the reasons why the $\wp$-functions are so important can be seen in the following:

Lemma 5.3. *Let Λ be a lattice. Then any elliptic function for Λ can be written as rational functions in $\wp(z)$ and $\wp'(z)$.*

Proof. See [6] page 218. □

Now, let us study how homothety affects elliptic curves. It is easy to see that if $f(z)$ is an elliptic function for Λ, then $f(\lambda z)$ is an elliptic function for $\lambda\Lambda$ for any nonzero complex number λ. Furthermore, the $\wp$-function transforms as follows:

$$\wp(\lambda z; \lambda\Lambda) = \lambda^{-2}\wp(z; \Lambda).$$

Given a lattice Λ, we set

$$\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2.$$

Notice that this is closely related to the discriminant Δ_F of the polynomial $F(x) = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ that appear in the differential equation for $\wp(z)$. In fact we have

$$\Delta(\Lambda) = 16\Delta_F. \tag{5.2}$$

Here is an important fact about $\Delta(\Lambda)$:

Proposition 5.4. $\Delta(\Lambda) \neq 0$ *for any lattice* $\Lambda \subset \mathbb{C}$.

Proof. It suffices to prove this for the case when $\Lambda = \Lambda_\tau$ for some $\tau \in \mathcal{H}$, since any lattice is homothetic to the one of that form, and it is easy to check using the definition of Δ and the homogeneity of g_2 and g_3 that $\Delta(\lambda\Lambda) = \lambda^{-12}\Delta(\Lambda)$. By part (iii) of Proposition 5.2, the cubic polynomial $p_\tau(x) = 4x^3 - g_2(\tau)x - g_3(\tau)$ has distinct roots. So by (5.2), we have $\Delta(\tau) \neq 0$. □

Definition 5.5. The *j-invariant* $j(\Lambda)$ of the lattice Λ is the complex number defined by

$$j(\Lambda) = 1728\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2} = 1728\frac{g_2(\Lambda)^3}{\Delta(\Lambda)}. \tag{5.3}$$

Note that $j(\Lambda)$ is always defined since $\Delta(\Lambda) \neq 0$ by Proposition 5.4. Remarkably, as we see in the following theorem, the j-invariant characterises the lattice Λ up to homothety:

Theorem 5.6. *Let* Λ *and* Λ' *be two lattices. Then* $j(\Lambda) = j(\Lambda')$ *if and only if* Λ *and* Λ' *are homothetic.*

Proof. By the definition of g_2 and g_3, it is clear that for any $\lambda \in \mathbb{C}^*$ we have

$$\begin{aligned} g_2(\lambda\Lambda) &= \lambda^{-4}g_2(\Lambda) \\ g_3(\lambda\Lambda) &= \lambda^{-6}g_3(\Lambda) \end{aligned} \tag{5.4}$$

and $j(\lambda\Lambda) = j(\Lambda)$ follows. The other direction is slightly longer, and is left to [6] pages 207–208. □

There is another way to think of the j-invariant which will be useful when we study modular functions:

Definition 5.7. Let $\mathcal{H} = \{\tau \in \mathbb{C} : Im(\tau) > 0\}$ denote the upper half plane and let $\tau \in \mathcal{H}$. Then define the *j-function* $j(\tau)$ by

$$j(\tau) := j(\Lambda_\tau).$$

The j-function plays an important role in the theory of complex multiplication. We begin with the observation that orders in imaginary quadratic fields give rise to a class of lattices: let $\mathcal{O}$ be an order in an imaginary quadratic field K, and let $\mathfrak{a}$ be a proper fractional ideal of $\mathcal{O}$. Then we know that we can write $\mathfrak{a} = [\omega_1, \omega_2]$ for some $\omega_1, \omega_2 \in K$. Also, ω_1 and ω_2 are linearly independent over $\mathbb{R}$ since K is imaginary quadratic ($\mathcal{O}$ contains a $\mathbb{Q}$-basis of K, hence an $\mathbb{R}$-basis of $\mathbb{C}$, since K is not contained in $\mathbb{R}$). It follows that $\mathfrak{a} = [\omega_1, \omega_2]$ is a lattice in $\mathbb{C}$, and consequently $j(\mathfrak{a})$ is defined. These complex numbers $j(\mathfrak{a})$ are called *singular moduli* and their properties will be explored later.

In order to simplify our discussion of complex multiplication, let us fix a lattice Λ. Recall that from Proposition 5.2 we could deduce that $\wp(2z)$ is a rational function in $\wp(z)$. It can be shown by induction that in general $\wp(nz)$ is a rational function in $\wp(z)$ for any positive integer n. Then the natural question to ask would be: are there any other complex numbers α for which $\wp(\alpha z)$ is a rational function in $\wp(z)$? The answer turns out to be rather surprising:

Theorem 5.8. *Let* Λ *be a lattice and let* $\wp(z)$ *be the* $\wp$*-function for* Λ*. Then for a complex number* $\alpha \in \mathbb{C} - \mathbb{Z}$*, the following are equivalent:*

(i) $\wp(\alpha z)$ *is a rational function in* $\wp(z)$*.*

(ii) $\alpha\Lambda \subset \Lambda$*.*

(iii) There is an order $\mathcal{O}$ *in an imaginary quadratic field* K *such that* $\alpha \in \mathcal{O}$ *and* Λ *is homothetic to a proper fractional ideal of* $\mathcal{O}$*.*

Moreover, if these conditions hold, then we can write

$$\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z))}$$

where $A(x)$ and $B(x)$ are coprime polynomials satisfying

$$\deg A = \deg B + 1 = [\Lambda : \alpha\Lambda] = N(\alpha).$$

Proof. (i) $\Rightarrow$ (ii). If (i) holds then there exist polynomials $A(x)$ and $B(x)$ such that

$$B(\wp(z))\wp(\alpha z) = A(\wp(z)). \tag{5.5}$$

Since $\wp(z)$ and $\wp(\alpha z)$ both have double poles at the origin, (5.5) gives us

$$\deg(A(x)) = \deg(B(x)) + 1. \tag{5.6}$$

Now take $\omega \in \Lambda$. Then since the poles of $\wp(z)$ are exactly the periods, it follows from (5.5) that $\wp(\alpha z)$ has a pole at ω, which then tells us that $\wp(z)$ has a pole at αz. This implies that $\alpha\omega \in \Lambda$, so that $\alpha\Lambda \subset \Lambda$.
(ii) $\Rightarrow$ (i). If $\alpha\Lambda \subset \Lambda$, then we have that $\wp(\alpha z)$ is an elliptic function for L then (i) follows immediately from Lemma 5.3.
(ii) $\Rightarrow$ (iii). We may assume wlog (by multiplying by a suitable $\lambda \in \mathbb{C}$) that $L = [1, \tau]$. Then $\alpha\Lambda \subset \Lambda$ means that $\alpha = a + b\tau$, $\tau = c + d\tau$ for some $a, b, c, d \in \mathbb{Z}$. This gives us

$$\tau = \frac{c + d\tau}{a + b\tau},$$

so τ satisfies the quadratic equation

$$b\tau^2 + (a - d)\tau - c = 0$$

and $b \neq 0$ since τ is non-real. Hence $K = \mathbb{Q}(\tau)$ is a quadratic field and

$$\mathcal{O} = \{\beta \in K : \beta\Lambda \subset \Lambda\}$$

is an order of K for which Λ is a proper fractional ideal of Λ, and clearly $\alpha \in \mathcal{O}$ so we are done.
(iii) $\Rightarrow$ (ii). This is clear.
For the last statement of the theorem, refer to [6] pages 210–211. □

This theorem together with Lemma 5.3 shows that if an elliptic function has multiplication by some $\alpha \in \mathbb{C}-\mathbb{R}$ (i.e. α satisfies conditions (i)-(iii) in Theorem 5.8), then it has multiplication by all elements in an order $\mathcal{O}$ in an imaginary quadratic field. Note that all elements in $\mathcal{O} - \mathbb{Z}$ are nonreal, which accounts for the name *complex multiplication*. Theorem 5.8 also tells us that complex multiplication is an intrinsic property of homothety classes of the lattices rather than elliptic functions. We can relate homothety classes of lattices and ideals class groups of orders in an imaginary quadratic field as follows:

Corollary 5.9. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K. Then there is a bijection between the ideal class group $Cl(\mathcal{O})$ and the homothety classes which have $\mathcal{O}$ as their full ring of complex multiplications. In particular, the class number $h(\mathcal{O})$ is the number of homothety classes of lattices having $\mathcal{O}$ as their full ring of complex multiplications.*

Proof. Let $\Lambda \subset \mathbb{C}$ be a lattice which has $\mathcal{O}$ as its full ring of complex multiplications. Then Theorem 5.8 implies that we can assume Λ is a proper fractional ideal of $\mathcal{O}$. Furthermore, two proper fractional ideals of $\mathcal{O}$ are homothetic if and only if they determine the same class in the $Cl(\mathcal{O})$: suppose $\mathfrak{a}$ and $\mathfrak{b}$ are two proper fractional ideals of $\mathcal{O}$. If they are homothetic, then $\mathfrak{b} = \lambda\mathfrak{b}$ for some $\lambda \in \mathbb{C}^*$ so we must have $\lambda \in K^*$ and hence $[\mathfrak{a}] = [\mathfrak{b}]$ in $Cl(\mathcal{O})$. Conversely, if $[\mathfrak{a}] = [\mathfrak{b}]$ in $Cl(\mathcal{O})$ then there exists a principal ideal $\lambda\mathcal{O} \in P(\mathcal{O})$, $\lambda \in K^* \subset \mathbb{C}$ such that $\mathfrak{b} = (\lambda\mathcal{O})\mathfrak{a} = \lambda\mathfrak{a}$, hence $\mathfrak{a}$ and $\mathfrak{b}$ are homothetic as lattices in $\mathbb{C}$. This proves the corollary. □

Example 5.10. Consider all lattices which have complex multiplication by $\sqrt{-5}$. This means we are dealing with an order $\mathcal{O}$ containing $\sqrt{-5}$ in the field $K = \mathbb{Q}(\sqrt{-5})$. But the only such order is the maximal order $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and the class number of $\mathcal{O}_K$ is $h(\mathcal{O}_K) = 2$. Hence the only lattices with complex multiplication by $\sqrt{-5}$ are $\mathcal{O}_K = [1, \sqrt{-5}]$ and $[2, 1 + \sqrt{-5}]$ up to homothety.

We also indicate how complex multiplication affects the j-invariant, since our ultimate goal involves j-invariant of the lattices.

Example 5.11. Let us consider the simplest cases. First consider the complex multiplication by i. Up to homothety, the only possible lattice which has complex multiplication by i is $\Lambda = [1, i]$. Note that we have $i\Lambda = [i, -1] = \Lambda$. Hence the homogeneity of $g_3(\Lambda)$ (5.4) gives

$$g_3(\Lambda) = g_3(i\Lambda) = i^{-6} g_3(\Lambda) = -g_3(\Lambda)$$

which implies $g_3(\Lambda) = 0$. Then the formula for $j(\Lambda)$ tells us $j(\Lambda) = j(i) = 1728$. Similarly, if $\Lambda = [1, \omega]$ where $\omega = e^{\frac{2\pi i}{3}}$, then again $\omega\Lambda = \Lambda$ and the homogeneity of $g_2(\Lambda)$ (5.4) gives

$$g_2(\Lambda) = g_2(\omega\Lambda) = \omega^{-4} g_2(\Lambda) = \omega^{-1} g_2(\Lambda)$$

so $g_2(\Lambda) = 0$. Then the formula for $j(\Lambda)$ gives us $j(\omega) = 0$.

Let us now study the j-function in detail. The properties of $j(\tau)$ are closely related to the action of the group $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane $\mathcal{H}$ which is defined as follows: given $\tau \in \mathcal{H}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, then

$$\gamma\tau = \frac{a\tau + b}{c\tau + d}.$$

Note that $\gamma\tau \in \mathcal{H}$ since an easy computation shows

$$\mathrm{Im}\left(\frac{a\tau + b}{c\tau + d}\right) = \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} |c\tau + d|^{-2} \mathrm{Im}(\tau)$$

and $\det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = 1$. This shows that the map defined above does define an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$, and we say that $\gamma\tau$ and τ are $\mathrm{SL}_2(\mathbb{Z})$-equivalent. The j-function has the following properties:

Theorem 5.12. *(i) $j(\tau)$ is a holomorphic function on $\mathcal{H}$.*

(ii) Given $\tau, \tau' \in \mathcal{H}$, we have $j(\tau) = j(\tau')$ if and only if $\tau' = \gamma\tau$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

(iii) $j : \mathcal{H} \to \mathbb{C}$ is surjective.

Proof. See [6] pages 221–225. □

One can define modular functions for any subgroup of $\mathrm{SL}_2(\mathbb{Z})$, but we concentrate on the subgroup

$$\Gamma_0(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod m \right\}$$

where $m \in \mathbb{Z}_{\geqslant 1}$. Note that $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$.

Given $B > 0$, let $\mathcal{H}_B$ denote the set of complex numbers with $\mathrm{Im} z > B$. Then map

$$\tau \mapsto e^{2\pi i \tau} = q(\tau)$$

defines a holomorphic map from $\mathcal{H}_B$ to the punctured open disc of radius $e^{-2\pi B}$. Furthermore, if $\mathcal{H}_B/T$ denotes the quotient space of $\mathcal{H}_B$ modulo translations by integers, then q induces an analytic isomorphism between $\mathcal{H}_B/T$ and the punctured open disc. Hence a meromorphic function f on $\mathcal{H}_B$

which has period 1, i.e. is invariant under T, induces a meromorphic function f^* on the punctured disc. Then we have that f^* is meromorphic at 0 if and only if there exists a positive integer N such that $f^*(q)q^N$ is bounded near 0. In this case, f^* has a Laurent expansion

$$f^*(q) = \sum_{n=-N}^{\infty} c_n q^n.$$

By abuse of notation in this case, we also write

$$f(q) = \sum_{n=-N}^{\infty} c_n q^n.$$

and say that f is *meromorphic at inifinity.*

For geometric reasons, a $\Gamma_0(m)$-equivalence class of the projective line $\mathbb{P}^1(\mathbb{Q})$ (viewed as the rational numbers $\mathbb{Q}$ together with the limit point ∞ of $\mathcal{H}$) is called a *cusp* of $\Gamma_0(m)$. The geometry motivating the term "cusp" is explained in [7] Chapter 2. When $m = 1$, i.e. when $\Gamma_0(m) = \mathrm{SL}_2(\mathbb{Z})$, all rational numbers are $\Gamma_0(m)$-equivalent to ∞ and so $\mathrm{SL}_2(\mathbb{Z})$ has only one cusp. However, if $m \neq 1$ then $\Gamma_0(m)$ is a proper subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and fewer points are $\Gamma_0(m)$-equivalent, meaning that $\Gamma_0(m)$ will have other cusps, represented by rational numbers. Notice that each $s \in \mathbb{Q}$ can be written $s = \gamma(\infty)$ for some $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, the number of cusps is at most the number of cosets $\Gamma_0(m)\gamma$ in $\mathrm{SL}_2(\mathbb{Z})$. It is also finite since $\Gamma_0(m)$ has a finite index in $\mathrm{SL}_2(\mathbb{Z})$. To see this notice that we have $\Gamma_0(m) \supset \Gamma(m) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \bmod m,\ \ b \equiv c \equiv 0 \bmod m \right\}$, which is the kernel of the canonical homomorphism

$$\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Since $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ is finite, $\Gamma(m)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of finite index. Hence it follows that $\Gamma_0(m)$ has a finite index in $\mathrm{SL}_2(\mathbb{Z})$.

Definition 5.13. A *modular function* for $\Gamma_0(m)$ is a function meromorphic on $\mathcal{H}$, invariant under $\Gamma_0(m)$ and meromorphic at all cusps.

Note that if f is a meromorphic function on $\mathcal{H}$ which is $\Gamma_0(m)$-invariant, and if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then $f(\gamma\tau)$ has period m. To see this, notice that $\tau + m = U\tau$ where $U = \left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)$ by the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$. An easy calculation shows that $\gamma U \gamma^{-1}$ has the $(2,2)$-entry $-c^2 m \equiv 0 \bmod m$, hence $\gamma U \gamma^{-1} \in \Gamma_0(m)$. So

$$f(\gamma(\tau + m)) = f(\gamma U \tau) = f(\gamma U \gamma^{-1} \gamma\tau) = f(\gamma\tau)$$

where the last equality uses the $\Gamma_0(m)$-invariance of f. It follows that if $q = q(\tau) = e^{2\pi i \tau}$, then $f(\gamma\tau)$ is a holomorphic function in $q^{1/m}$, defined for $0 < |q^{1/m}| < 1$.

The basic example of a modular function is the j-function. By Theorem 5.12 $j(\tau)$ is holomorphic on $\mathcal{H}$, invariant under $\mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(1)$ and the following shows that it has a q-expansion at infinity:

Theorem 5.14. *The q-expansion of $j(\tau)$ is*

$$j(\tau) = \frac{1}{q} + 744 + 196884q + \cdots = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n$$

where $c_n \in \mathbb{Z}$ for all $n \geqslant 0$.

Proof. See [11] 4.1. □

This theorem is the reason that the factor 1728 appears in the definition of the j-invariant: it is exactly the factor needed to guarantee that all of the coefficients of the q-expansion are integers without any common divisors. The remarkable fact is that modular functions for $\Gamma_0(m)$ are easily described in terms of the j-functions:

Theorem 5.15. *Let m be a positive integer. Then $j(\tau)$ and $j(m\tau)$ are modular functions for $\Gamma_0(m)$, and every modular function for $\Gamma_0(m)$ is a rational function of $j(\tau)$ and $j(m\tau)$.*

In particular, the above theorem tells us that $j(\tau)$ is a modular function of $\mathrm{SL}_2(\mathbb{Z})$, and every modular function for $\mathrm{SL}_2(\mathbb{Z})$ is a rational function in $j(\tau)$. See [6] pages 226–231 for the proof of this theorem. We state a special case. Say that a modular function is *holomorphic at infinity* if its q-expansion does not involve any negative powers of q.

Lemma 5.16. *(i) A holomorphic modular function for $\mathrm{SL}_2(\mathbb{Z})$ which is holomorphic at infinity is constant.*

(ii) A holomorphic modular function for $\mathrm{SL}_2(\mathbb{Z})$ is a polynomial in $j(\tau)$.

The next step is to introduce the *modular polynomial* $\Phi_m(X, Y)$. We first relate $\Gamma_0(m)$ to the set of matrices

$$C(m) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = m,\ a > 0,\ 0 \leqslant b < d,\ \gcd(a, b, c) = 1 \right\}.$$

The matrix $\sigma_0 = \left(\begin{smallmatrix} m & 0 \\ 0 & 1 \end{smallmatrix}\right) \in C(m)$ has two properties of interest: first, $\sigma_0\tau = m\tau$, and second, given $\sigma \in C(m)$, the set

$$(\sigma_0^{-1}\,\mathrm{SL}_2(\mathbb{Z})\sigma) \cap \mathrm{SL}_2(\mathbb{Z})$$

is a right coset of $\Gamma_0(m)$ in $\mathrm{SL}_2(\mathbb{Z})$. This induces a bijection between the right cosets of $\Gamma_0(m)$ and elements of $C(m)$. In the case $\sigma = \sigma_0$, we get the coset $\Gamma_0(m)$ itself. Moreover, this implies that $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(m)] = |C(m)|$. Let the right coset of $\Gamma_0(m)$ in $\mathrm{SL}_2(\mathbb{Z})$ be $\Gamma_0(m)\gamma_i$, $i = 1, ..., |C(m)|$. Then consider the following polynomial with a variable X:

$$\Phi_m(X, \tau) = \prod_{i=1}^{|C(m)|} (X - j(m\gamma_i\tau)).$$

We claim that this is a polynomial in X and $j(\tau)$. To see this, notice that the coefficients of $\Phi_m(X, \tau)$ are symmetric polynomials in the $j(m\gamma_i\tau)$'s, so they are certainly holomorphic. To check invariance under $\mathrm{SL}_2(\mathbb{Z})$, pick $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Then the cosets $\Gamma_0(m)\gamma_i\gamma$ are a permutation of the cosets $\Gamma_0(m)\gamma_i$, and since $j(m\tau)$ is invariant under $\Gamma_0(m)$, the $j(m\gamma_i\gamma\tau)$'s are a permutation of the $j(m\gamma_i\tau)$'s. Hence the coefficients of $\Phi_m(X, \tau)$ are $\mathrm{SL}_2(\mathbb{Z})$-invariant.

Next, we show that the coefficients are meromorphic at infinity. To see this, it suffices to expand in terms of $q^{1/m} = e^{2\pi i\tau/m}$ and show that there are only finitely many negative exponents. Given $\gamma_i \in \mathrm{SL}_2(\mathbb{Z})$, choose $\sigma \in C(m)$ corresponding to the right coset $\Gamma_0(m)\gamma_i$. This means $\sigma_0\gamma_i = \gamma\sigma$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, and hence $j(m\gamma_i\tau) = j(\sigma_0\gamma_i\tau) = j(\gamma\sigma\tau) = j(\sigma\tau)$ since $j(\tau)$ is $\mathrm{SL}_2(\mathbb{Z})$-invariant. Hence

$$j(m\gamma_i\tau) = j(\sigma\tau).$$

We know the q-expansion of $j(\tau)$ from Theorem 5.14, and if $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ then $\sigma\tau = (a\tau + b)/d$, so it follows that

$$q(\sigma\tau) = e^{2\pi i(a\tau+b)/d} = e^{2\pi ib/d} q^{a/d}.$$

Note also that if we set $\zeta_m = e^{2\pi i/m}$, we can write $q(\sigma\tau) = \zeta_m^{ab}(q^{1/m})^{a^2}$ since $ad = m$. This together with Theorem 5.14 gives the q-expansion

$$j(m\gamma_i\tau) = j(\sigma\tau) = \frac{\zeta_m^{-ab}}{(q^{1/m})^{a^2}} + \sum_{n=0}^{\infty} c_n \zeta_m^{abn} (q^{1/m})^{a^2 n}$$

where $c_n \in \mathbb{Z}$. This shows that the q-expansion of $j(m\gamma_i\tau)$ has only finitely many negative exponents. Since the coefficients of $\Phi_m(X, \tau)$ are polynomials in the $j(m\gamma_i\tau)$'s, they are meromorphic at infinity as required.

This proves that the coefficients of $\Phi_m(X, \tau)$ are holomorphic modular functions, and thus by Lemma 5.16, they are polynomials in $j(\tau)$. This means that there is a polynomial

$$\Phi_m(X, Y) \in \mathbb{C}[X, Y]$$

such that

$$\Phi_m(X, j(\tau)) = \prod_{i=1}^{|C(m)|} (X - j(m\gamma_i\tau)). \tag{5.7}$$

Definition 5.17. Let $\Phi_m(X, Y)$ be as above. The equation $\Phi_m(X, Y) = 0$ is called the *modular equation*, and we will call the polynomial $\Phi_m(X, Y)$ the *modular polynomial*.

We showed above that each $j(m\gamma_i\tau)$ can be written $j(\sigma\tau)$ for a unique $\sigma \in C(m)$, so we can also write the modular polynomial in the form

$$\Phi_m(X, j(\tau)) = \prod_{\sigma \in C(m)} (X - j(\sigma\tau)). \tag{5.8}$$

Some very important arithmetic properties of the modular polynomial $\Phi_m(X, Y)$ are given in the following theorem:

Theorem 5.18. *Let m be a positive integer.*

(i) $\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$.

(ii) $\Phi_m(X, Y)$ *is irreducible as a polynomial in* X.

(iii) $\Phi_m(X, Y) = \Phi_m(Y, X)$ *if* $m > 1$.

(iv) If p is a prime number, then $\Phi_p(X, Y) \equiv (X^p - Y)(X - Y^p) \bmod p\mathbb{Z}[X, Y]$.

Proof. These properties are straightforward consequences of the properties of the j-function, and the proof is left to [6] pages 231–234. □

Before we can apply the modular polynomial to complex multiplication, we need to understand the modular polynomial in terms of j-invariants of lattices.

Definition 5.19. Let Λ be a lattice. Then a *cyclic sublattice* of Λ of index m is a sublattice $\Lambda' \subset \Lambda$ such that $[\Lambda : \Lambda'] = m$ and the quotient Λ/Λ' is a cyclic group.

The basic idea is given in the following:

Theorem 5.20. *Let m be a positive integer, and let $u, v \in \mathbb{C}$. Then $\Phi_m(u, v) = 0$ if and only if there is a lattice Λ and a cyclic sublattice Λ' of index m such that $j(\Lambda') = u$ and $j(\Lambda) = v$.*

We will apply the modular polynomial to lattices with complex multiplication. It turns out that such lattices have some particularly interesting cyclic sublattices. To construct these, we introduce the notion of a *primitive* ideal.

Definition 5.21. Let $\mathcal{O}$ be an order. Then a proper ideal of $\mathcal{O}$ is *primitive* if it is not of the form $d\mathfrak{a}$ where $d > 1$ is an integer and $\mathfrak{a}$ is a proper ideal of $\mathcal{O}$. Similarly, say an element $\alpha \in \mathcal{O}$ is *primitive* if α is not of the form $d\beta$ where $d > 1$ and $\beta \in \mathcal{O}$.

Then primitive ideals are related to cyclic sublattices as follows:

Lemma 5.22. *Let $\mathcal{O}$ be an imaginary quadratic field, and let $\mathfrak{b}$ be a proper fractional ideal of $\mathcal{O}$. Then, given a proper ideal $\mathfrak{a}$ of $\mathcal{O}$, $\mathfrak{ab}$ is a sublattice of $\mathfrak{b}$ of index $N(\mathfrak{a})$. Moreover, $\mathfrak{ab}$ is a cyclic sublattice if and only if $\mathfrak{a}$ is a primitive ideal.*

Proof. We can assume that $\mathfrak{b} \subset \mathcal{O}$ after replacing $\mathfrak{b}$ by a multiple. We have an exact sequence

$$0 \to \mathfrak{b}/\mathfrak{ab} \to \mathcal{O}/\mathfrak{ab} \to \mathcal{O}/\mathfrak{b} \to 0$$

which implies that $|\mathfrak{b}/\mathfrak{ab}||\mathcal{O}/\mathfrak{b}| = |\mathcal{O}/\mathfrak{ab}|$, i.e., $[\mathfrak{b} : \mathfrak{ab}]N(\mathfrak{b}) = N(\mathfrak{ab}) = N(\mathfrak{ab})$. Hence we have $[\mathfrak{b} : \mathfrak{ab}] = N(\mathfrak{a})$ as claimed.
Now suppose $\mathfrak{b}/\mathfrak{ab}$ is not cyclic. Then by the structure theorem for finite abelian groups, it follows that $\mathfrak{b}/\mathfrak{ab}$ contains a subgroup isomorphic to $(\mathbb{Z}/d\mathbb{Z})^2$ for some $d > 1$. Hence there is a sublattice $\mathfrak{b}' \subset \mathfrak{b}$ containing $\mathfrak{ab}$ such that $\mathfrak{b}'/\mathfrak{ab} \cong (\mathbb{Z}/d\mathbb{Z})^2$. But $\mathfrak{b}'$ is a $\mathbb{Z}$-module of rank 2, so we must have $\mathfrak{ab} = d\mathfrak{b}'$, so that $\mathfrak{a} = d\mathfrak{b}'\mathfrak{b}^{-1}$. But $\mathfrak{b}'\mathfrak{b}^{-1} \subset \mathfrak{b}\mathfrak{b}^{-1} = \mathcal{O}$ since $\mathfrak{b}' \subset \mathfrak{b}$, so $\mathfrak{b}'\mathfrak{b}^{-1}$ is a proper ideal of $\mathcal{O}$. This shows that $\mathfrak{a}$ is not primitive. The converse is even easier and is left to the reader. See [6] page 237 for the details. □

If we apply this lemma in the case $\mathfrak{a}$ is a principal ideal $\mathfrak{a} = \alpha\mathcal{O}$, $\alpha \in \mathcal{O}$, we get that $\alpha\mathcal{O}$ is a primitive ideal of $\mathcal{O}$ if and only if α is a primitive element of $\mathcal{O}$. In particular, since we have $N(\alpha\mathcal{O}) = N(\alpha)$, we immediately get that if $\mathcal{O}$ and $\mathfrak{b}$ are as in Lemma 5.22, then given $\alpha \in \mathcal{O}$, $\alpha\mathfrak{b}$ is a sublattice of index $N(\alpha)$ and $\alpha\mathfrak{b}$ is a cyclic sublattice if and only if α is a primitive element of $\mathcal{O}$.

We can now state the main result of this section which unravels the strong connection between the j-invariant $j(\mathfrak{a})$ of a proper fractional ideal of $\mathcal{O}$ and the ring class field introduced at the end of section 3.

Theorem 5.23 (**The First Main Theorem of Complex Multiplication**)**.** *Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and let $\mathfrak{a}$ be a proper fractional ideal of $\mathcal{O}$. Then the j-invariant $j(\mathfrak{a})$ is an algebraic integer and $K(j(\mathfrak{a}))$ is the ring class field of $\mathcal{O}$.*

This theorem tells us a lot about the abelian extensions of an imaginary quadratic field:

Corollary 5.24. *Let K be an imaginary quadratic field. Then $K(j(\mathcal{O}_K))$ is the Hilbert class field of K.*

Proof. We know from section 3 that the Hilbert class field is the ring class field of $\mathcal{O}_K$, so we are done by Theorem 5.23. □

We will finish our discussion of ring class field and complex multiplication with the computation of the Frobenius element of a ring class field using j-invariants:

Theorem 5.25. *Let $\mathcal{O}$ be an order of an imaginary quadratic field K, and let L be the ring class field of $\mathcal{O}$. Then, given a proper fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ and a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, we have*

$$\mathrm{Frob}_p(j(\mathfrak{a})) = j(\overline{\mathfrak{p} \cap \mathcal{O}\alpha}).$$

It should be pointed out at this point that Theorem 5.25 can be restated in terms of ideal class group as follows:

Corollary 5.26. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and let L be the ring class field of $\mathcal{O}$. Then the map*

$$\begin{aligned} Cl(\mathcal{O}) &\xrightarrow{\sim} \mathrm{Gal}(L/K) \\ \mathfrak{a} &\longmapsto \sigma_{\mathfrak{a}} : j(\mathfrak{b}) \mapsto j(\overline{\mathfrak{a}}\mathfrak{b}) \end{aligned}$$

is an isomorphism.

6 Heegner's Proof of the Class Number One Problem

In this section, we will present Heegner's proof of the class number one problem.

Put

$$\gamma_2(\tau) = \sqrt[3]{j(\tau)} = 12\frac{g_2(\tau)}{\sqrt[3]{\Delta(\tau)}},$$

where we choose the unique cube root of $\Delta(\tau)$ which is holomorphic and real-valued on the imaginary axis. The existence of such a root follows from the fact that $\Delta(\tau)$ is nonvanishing and holomorphic on the simply connected domain $\mathcal{H}$, and it is real on the imaginary axis since we have $g_i(\overline{\tau}) = \overline{g_i(\tau)}$ for $i = 2, 3$. It follows that $\gamma_2(\tau)$ is the unique cube root of $j(\tau)$ which is real on the imaginary axis. The property of $\gamma_2(\tau)$ which is important for our purpose is given in the following theorem:

Theorem 6.1. *Let $3 \nmid D$ be the discriminant of an order $\mathcal{O} = [1, \tau_0]$ in an imaginary quadratic field K, where*

$$\tau_0 = \begin{cases} \sqrt{-m} & \text{if } D = -4m \equiv 0 \bmod 4 \\ \frac{3+\sqrt{-m}}{2} & \text{if } D = -m \equiv 1 \bmod 4. \end{cases}$$

Then $\gamma_2(\tau_0)$ is an algebraic integer and $K(\gamma_2(\tau_0))$ is the ring class field corresponding to $\mathcal{O}$. Moreover, $\mathbb{Q}(\gamma_2(\tau_0)) = \mathbb{Q}(j(\tau_0))$.

We refer the readers to [6] pages 249–255 for the proof of this theorem. We now introduce the *Weber modular functions* f, f_1 and f_2, studied by Heinrich Martin Weber (1842–1913). They are defined as follows.

$$\begin{aligned} f(\tau) &= q^{-1/48}\prod_{n=1}^{\infty}(1+q^{n-1/2}) \\ f_1(\tau) &= q^{-1/48}\prod_{n=1}^{\infty}(1-q^{n-1/2}) \\ f_2(\tau) &= \sqrt{2}q^{-1/24}\prod_{n=1}^{\infty}(1+q^n) \end{aligned}$$

where $q^{1/2} := e^{\pi i\tau}$. These functions are derived from the Dedekind η-function, which is defined by

$$\eta(\tau) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n).$$

In fact we have $f(\tau) = \zeta_{48}^{-1}\frac{\eta((\tau+1)/2)}{\eta(\tau)}$, $f_1(\tau) = \frac{\eta(\tau/2)}{\eta(\tau)}$ and $f_2(\tau) = \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)}$, where $\zeta_{48} = e^{2\pi i/48}$. Furthermore, the product expansions for the Weber functions give the following useful identities:

$$\begin{aligned} f(\tau)f_1(\tau)f_2(\tau) &= \sqrt{2} \\ f_1(2\tau)f_2(\tau) &= \sqrt{2}. \end{aligned} \tag{6.1}$$

There are deeper relations between $f(\tau), f_1(\tau), f_2(\tau), \eta(\tau), \gamma_2(\tau)$ and $\Delta(\tau)$ as we see in the following:

Theorem 6.2. *Given $\tau \in \mathcal{H}$, we have*

$$\gamma_2(\tau) = \frac{f(\tau)^{24} - 16}{f(\tau)^8} = \frac{f_1(\tau)^{24} + 16}{f_1(\tau)^8} = \frac{f_2(\tau)^{24} + 16}{f_2(\tau)^8}$$

and

$$\Delta(\tau) = (2\pi)^{12}\eta(\tau)^{24}.$$

Note that since $j(\tau) = \gamma_2(\tau)^3$, this gives some remarkable formulae for computing the j-function. Furthermore, using these formulae it can be shown that the q-expansions of $\gamma_2(\tau)$ and $j(\tau)$ have integer coefficients, and we can prove Theorem 5.14.

We will make use of the following transformation properties of $\eta(\tau)$ and the Weber functions later on:

Proposition 6.3. *Let $\zeta_n = e^{2\pi i/n}$ be a primitive n^{th} root of unity for a positive integer n, and let $\tau \in \mathcal{H}$. Then we have*

$$\begin{aligned} \eta(\tau + 1) &= \zeta_{24}\eta(\tau) \\ \eta(-1/\tau) &= \sqrt{-i\tau}\eta(\tau), \end{aligned}$$

where the square root is chosen to be positive on the imaginary axis. Moreover, we have

$$\begin{aligned} f(\tau + 1) &= \zeta_{48}^{-1} f_1(\tau) \\ f_1(\tau + 1) &= \zeta_{48}^{-1} f(\tau) \\ f_2(\tau + 1) &= \zeta_{24} f_2(\tau) \end{aligned}$$

and

$$\begin{aligned} f(-1/t) &= f(\tau) \\ f_1(-1/t) &= f_2(\tau) \\ f_2(-1/t) &= f_1(\tau). \end{aligned}$$

Proof. We only prove the proposition for $\eta(\tau)$, as the behavior of the Weber functions under the transformations are consequences of their definitions and the transformation properties of $\eta(\tau)$. Turning to $\eta(\tau)$, the formula for $\eta(\tau+1)$ is clear from its definition. For the transformation $\tau \mapsto -1/\tau$, recall from the proof of Proposition 5.4 that

$$\Delta(\lambda\tau) = \lambda^{-12}\Delta(\tau).$$

Therefore,

$$\Delta(-1/\tau) = \Delta([1, -1/\tau]) = \Delta(\tau^{-1}[1, \tau]) = \tau^{12}\Delta(\tau).$$

Using the formula $\Delta(\tau) = (2\pi)^{12}\eta(\tau)^{24}$ obtained in Theorem 6.2 and taking the 24^{th} root gives

$$\eta(-1/\tau) = \epsilon\sqrt{-i\tau}\eta(\tau)$$

for some root of unity ϵ, where the square root is chosen to be positive on the imaginary axis. By taking $\tau = i$ and noting $\eta(i) \neq 0$ since $\Delta(\tau) = (2\pi)^{12}\eta(\tau)^{24}$ and $\Delta(\tau) \neq 0$ for all $\tau \in \mathcal{H}$ by Proposition 5.4, we see that $\epsilon = 1$. □

A key fact we will use is that one can generate ring class fields using small powers of the Weber functions. Weber gave a long list of such theorems in [15], and Birch gave a modern proof in [3]. For our purpose, we will only state a special case of such results:

Theorem 6.4. *Let m be a positive integer such that $3 \nmid m$ and $m \equiv 3 \bmod 4$, and let $\mathcal{O} = [1, \sqrt{-m}]$ be an order in $K = \mathbb{Q}(\sqrt{-m})$. Then $f(\sqrt{-m})^2$ is an algebraic integer and $K(f(\sqrt{-m})^2)$ is the ring class field of $\mathcal{O}$.*

We are now ready to determinine completely all the imaginary quadratic fields with class number one, which turns out to be an application of the Weber functions:

Theorem 6.5 (**Class Number One Problem**). *Let K be an imaginary quadratic field of discriminant d_K. Then K has class number $h(d_K) = 1$ if and only if $d_K = -3, -4, -7, -8, -11, -19, -43, -67$ or -163.*

Recall that one consequence of this theorem is that it enables us to make a complete list of all discriminants D with $h(D) = 1$, as we found in Theorem 2.18.

Proof. We will follow Stark's presentation [16] of Heegner's argument. The case when d_K is even was proved using elementary methods in Theorem 1.1: we proved that if n is a positive integer, then $h(-4n) = 1$ if and only if $n = 1$, 2, 3, 4 or 7, which tells us that if d_K is a field discriminant such that $d_K \equiv 0 \bmod 4$ then $h(d_K) = 1$ if and only if $d_K = -4$ or -8. Hence, we may assume $d_K \equiv 1 \bmod 4$. Then Theorem 1.7 tells us that there are $2^{\mu-1}$ genera of discriminant d_K, where μ is the number of primes dividing d_K, and that the class group $Cl(d_K)$ has exactly $2^{\mu-1}$ elements of order $\leqslant 2$. Since $h(d_K) = 1$, we have exactly one element of order $\leqslant 2$ and this forces $\mu = 1$, i.e. $d_K = -p$ for some prime p such that $p \equiv 3 \bmod 4$ (since $d_K \equiv 1 \bmod 4$ by assumption).

If $d_K \equiv 1 \bmod 8$, i.e. $p \equiv 7 \bmod 8$, then applying Corollary 2.17 with $m = 2$ gives us

$$h(-4p) = 2h(-p)\left(1 - \left(\frac{-p}{2}\right)\frac{1}{2}\right) = h(-p) = 1.$$

Using Theorem 1.1 again, we find that the only prime number $p \equiv 7 \bmod 8$ such that $h(-4p) = 1$ is $p = 7$. Hence we are reduced to the case $d_K \equiv 5 \bmod 8$, i.e. $p \equiv 3 \bmod 8$, and we may assume $p \neq 3$. Then Corollary 2.17 again gives us

$$h(-4p) = 2h(-p)\left(1 - \left(\frac{-p}{2}\right)\frac{1}{2}\right) = 3h(-p) = 3. \tag{6.2}$$

We know by Theorem 5.23 that $L = K(j(\sqrt{-p}))$ is the ring class field of the order $\mathcal{O} = [1, \sqrt{-p}]$. To compute the degree of extension $[L : \mathbb{Q}]$, recall from (3.2) that the class number of an order is the degree of the corresponding ring class field over K. Also we have by Remark 2.8 $h(\mathcal{O}) = h(\mathrm{disc}(\mathcal{O})) = h(-4p)$ and $h(\mathcal{O}_K) = h(\mathrm{disc}([1, \frac{1+\sqrt{-p}}{2}])) = h(-p)$. Furthermore, $h(-p) = 1$ by assumption so the Hilbert Class Field of K is itself. Hence equation (6.2) gives us

$$[L : K] = \frac{h(\mathcal{O})}{h(\mathcal{O}_K)} = \frac{h(-4p)}{h(-p)} = 3.$$

This implies that $L = K(j(\sqrt{-p})) = \mathbb{Q}(\sqrt{-p}, j(\sqrt{-p}))$ has degree 3 over K, hence $\mathbb{Q}(\sqrt{-p}, j(\sqrt{-p}))$ is a degree 6 extension over $\mathbb{Q}$. We know that $[\mathbb{Q}(\sqrt{-p}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt{-p}, j(\sqrt{-p})) : \mathbb{Q}(j(\sqrt{-p}))] \leqslant 2$. But we know that j is real on the imaginary axis since g_2 and Δ are, so $\mathbb{Q}(\sqrt{-p}) \not\subset \mathbb{Q}(j(\sqrt{-p}))$. Hence it follows that $\mathbb{Q}(j(\sqrt{-p}))$ is a cubic extension of $\mathbb{Q}$. Moreover, Theorem 6.4 implies $f(\sqrt{-p})^2 \in K(j(\sqrt{-p}))$ and since $f(\sqrt{-p})^2$ is real (the product formula for $f(\tau)$ tells us that f is real on the imaginary axis), it generates the same cubic extension of $\mathbb{Q}$.

Set $\tau_0 = \frac{3+\sqrt{-p}}{2}$ and let $\alpha = \zeta_8 f_2(\tau_0)^2$. This relates to $f(\sqrt{-p})^2$ as follows. Recall from Theorem 6.1 that

$$f_1(2\tau_0)f_2(\tau_0) = \sqrt{2}$$

and by 6.3 we also have

$$f_1(2\tau_0) = f_1(3+\sqrt{-p}) = \zeta_{48}^{-3} f(\sqrt{-p}) = \zeta_{16}^{-1} f(\sqrt{-p}).$$

These formulae give $\frac{\sqrt{-2}}{f_2(\tau_0)} = \zeta_{16}^{-1} f(\sqrt{-p})$, from which we obtain $\alpha = \frac{2}{f(\sqrt{-p})^2}$. Hence we have $\mathbb{Q}(f(\sqrt{-p})^2) = \mathbb{Q}(\alpha)$. Note also that α^4 also generates the same cubic extension, since we have $\mathbb{Q} \subset \mathbb{Q}(\alpha^4) \subset \mathbb{Q}(\alpha)$ where $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a prime number, and clearly $\alpha^4 \notin \mathbb{Q}$ as α has a minimal polynomial of degree 3 over $\mathbb{Q}$.

Let us now study the minimal polynomial of α^4. Let $\mathcal{O} = [1, \tau_0]$. Then $h(\mathcal{O}) = h(-p) = 1$ and since $j(\mathcal{O}) = j(\tau_0)$ is an algebraic integer, this implies that $j(\tau_0)$ is an integer. Then by Theorem 6.1, $\gamma_2(\tau_0)$ is also an integer. But we have from Theorem 6.2

$$\gamma_2(\tau_0) = \frac{f_2(\tau_0)^{24} + 16}{f_2(\tau_0)^8}$$

so it follows that $\alpha^4 = (\zeta_8 f_2(\tau_0)^2)^4 = -f_2(\tau_0)^8$ is a root of the cubic equation

$$x^3 - \gamma_2(\tau_0)x - 16 = 0. \tag{6.3}$$

Since this is a monic cubic polynomial satisfied by α^4, and α^4 generates a cubic extension over $\mathbb{Q}$, it follows that this is the minimal polynomial of α^4 over $\mathbb{Q}$.

However, α also generates a cubic extension over $\mathbb{Q}$ and it is an algebraic integer (since α^4 satisfies $x^3 - \gamma_2(\tau_0)x - 16 = 0$, α satisfies $x^{12} - \gamma_2(\tau_0)x^4 - 16 = 0$) hence it satisfies an equation of the form

$$x^3 + ax^2 + bx + c = 0,$$

where $a, b, c \in \mathbb{Z}$. The idea is that this equation puts some very strong conditions that the equation for α^4 must satisfy. Moving the even degree terms to the right and squaring both sides gives

$$(x^3 + bx)^2 = (-ax - c)^2,$$

which means that α must satisfy

$$x^6 + (2b - a^2)x^4 + (b^2 - 2ac)x^2 - c^2 = 0.$$

Hence α^2 satisfies the cubic equation

$$x^3 + ex^2 + fx + g,$$

where $e = 2b - a^2$, $f = b^2 - 2ac$ and $g = -c^2$. Repeating the process, we see that α^4 satisfies the cubic equation

$$x^3 + (2f - e^2)x^2 + (f^2 - 2eg)x - g^2 = 0.$$

By the uniqueness of the minimal polynomial, this equation must equal (6.3). Comparing coefficients, we obtain

$$\begin{aligned} 2f - e^2 &= 0 \\ f^2 - 2eg &= -\gamma_2(\tau_0) \\ g^2 &= 16. \end{aligned} \tag{6.4}$$

The third equation of (6.4) gives $g = \pm 4$, and we also have $g = -c^2$, hence $g = -4$ and $c = \pm 2$. Moreover, changing α to $-\alpha$ leaves α^4 unchanged but takes a, b, c to $-a, b, -c$. Thus we may assume $c = 2$. Hence we have

$$\gamma_2(\tau_0) = -f^2 + 8e = -(b^2 - 4a)^2 - 8(2b - a^2).$$

It remains to determine the possibilities for a and b.

Note that first equation of (6.4) may be written

$$2(b^2 - 4a) = (2b - a^2)^2. \tag{6.5}$$

Expanding the bracket, we get $2b^2 - 8a = 4b^2 - 4a^2b + a^4$ and reducing this mod 2 gives $a \equiv 0 \bmod 2$. Then we have $a^4 \equiv 0 \bmod 4$ so reducing the equation mod 4 gives $2b^2 \equiv 0 \bmod 4$, i.e. $b \equiv 0 \bmod 2$. Hence we have that a and b are even. Now set $X = -a/2$ and $Y = (b - a^2)/2$. Then (6.5) gives

$$-8a + a^4 = 2(b - a^2)^2,$$

so dividing through by 8 we obtain that X and Y satisfy the Diophantine equation

$$2X(X^3 + 1) = Y^2. \tag{6.6}$$

This equation has exactly six integer solutions, corresponding to $p = 3, 11, 19, 43, 67$ and 163:

Proposition 6.6. *The only integer solutions of the Diophantine equation* $2X(X^3 + 1) = Y^2$ *are* $(X, Y) = (0, 0)$, $(-1, 0)$, $(1, \pm 2)$ *and* $(2, \pm 6)$.

Proof. Let (α, β) be an integer solution. Since α and $\alpha^3 + 1$ are coprime and α and β satisfy $2\alpha(\alpha^3 + 1) = \beta^2$, we must have $\pm(\alpha^3 + 1) = \gamma^2$ or $2\gamma^2$ for some $\gamma \in \mathbb{Z}$. Hence, (α, β) gives an integer solution to one of the following four Diophantine equations:

(i) $x^3 + 1 = y^2$

(ii) $x^3 + 1 = -y^2$

(iii) $x^3 + 1 = 2y^2$

(iv) $x^3 + 1 = -2y^2$

We deal with the cases (ii)–(iv) first, which are relatively elementary.

Case (ii) We work in $\mathbb{Z}[i]$. We know $\mathbb{Z}[i]$ is a UFD, and i is a unit in $\mathbb{Z}[i]$. If $x^3 = -(1 + y^2)$ then x must be odd, for if x is even then reducing the equation mod 8 gives $y^2 + 1 \equiv 0 \bmod 8$ which yields no solution. Hence $y + i$ and $y - i$ are coprime, since if a non-unit $z \in \mathbb{Z}[i]$ divides $y + i$ and $y - i$ then $z \mid 2i$ so $N(z) \mid 4$, so $N(z)$ is even, which contradicts $z \mid x^3$. By the fundamental theorem of algebra, $y + i$ and $y - i$ are both cubes in $\mathbb{Z}[i]$. Putting $y + i = (a + bi)^2$ and comparing coefficients gives $b(3a^2 - b^2) = 1$, hence $a = 0$ and $b = -1$. So $(x, y) = (-1, 0)$ is the only solution.

Case (iii) We work in $\mathbb{Z}[\omega]$, $\omega = e^{2\pi i/3}$, which is again a UFD. Note that if $\alpha, \gamma \in \mathbb{Z}$ satisfy $\alpha^3 + 1 = 2\gamma^2$ then $2\alpha(\alpha^3 + 1) = \beta^2$ gives $\alpha = \delta^2$ for some δ. So replacing x with x^2, let us look instead at the equation $x^6 + 1 = 2y^2$. Since the right hand side of the equation is even, it is easy to see that x must be odd. Note also that $x^6 + 1 = (x^2 + 1)(x^2 + \omega)(x^2 + \omega^2)$. Given $a, b \in \mathbb{Z}$ we have $N(a + b\omega) = a^2 - ab + b^2$ so $N(x^2 + 1) = x^4 + 2x^2 + 1$ and $N(x^2 + \omega) = N(x^2 + \omega^2) = x^4 - x^2 + 1$. If there exists a non-unit $a + b\omega \in \mathbb{Z}[\omega]$ dividing both $x^2 + 1$ and $x^2 + \omega$, then $a + b\omega \mid (x^2 + 1) - (x^2 + \omega) = 1 - \omega$ so $N(a + b\omega) \mid N(1 - \omega) = 3$. But $x^4 + 2x^2 + 1 \equiv 0 \bmod 3$ has no solution, which is a contradiction. Hence $x^2 + 1$ and $x^2 + \omega$, and similarly $x^2 + 1$ and $x^2 + \omega^2$ are coprime. Furthermore, 2 is prime in

$\mathbb{Z}[\omega]$ since there is no element in $\mathbb{Z}[\omega]$ of norm 2 (note $a^2-ab+b^2=2$ has no solution mod 2). Also, $x^2+\omega$ and $x^2+\omega^2$ are coprime because any divisor of these must also divide $\omega-\omega^2=1+2\omega$ which has norm 3, but $N(x^2+\omega)=x^4-x^2+1\equiv 0 \bmod 3$ has no solution. Therefore, by the fundamental theorem of algebra, one of the factors in $(x^2+1)(x^2+\omega)(x^2+\omega^2)$ must be $\pm$twice a square and the other two factors must be $\pm$squares in $\mathbb{Z}[\omega]$. But $x^2+1=\pm z^2$, $z\in\mathbb{Z}[\omega]$ implies $z\in\mathbb{Z}$ since $x\in\mathbb{Z}$, then $x^2+1=-z^2$ clearly has no solution and $x^2+1=z^2$ has no solution other than $(x,z)=(0,\pm 1)$, which is no good since x must be odd. Hence x^2+1 must be twice a square, and so we must have $x^2+\omega=\pm(a+b\omega)^2$ for some $a,b\in\mathbb{Z}$. If $x^2+\omega=(a+b\omega)^2$, comparing coefficients gives

$$\begin{cases} a^2-b^2=1 \\ b(2a-b)=1 \end{cases}$$

The second equation gives $(a,b)=(1,1)$ as the only solution, but this does not satisfy the first equation, hence we get a contradiction. If $x^2+\omega=-(a+b\omega)^2$, comparing coefficients gives

$$\begin{cases} a^2-b^2=-1 \\ b(2a-b)=-1 \end{cases}$$

and it is easy to see that $(a,b)=(0,\pm 1)$ are the only solutions. Hence $x^2+\omega=-\omega^2$, which yields $(x,y)=(\pm 1,\pm 1)$. Hence going back to the original equation, we see that the only solutions of $x^3+1=2y^2$ are $(x,y)=(1,\pm 1)$.

Case (iv) We work in $\mathbb{Z}[\sqrt{-2}]$, which is a UFD. If $x^3+1=-2y^2$, then the right hand side is even so x must be odd. We can write

$$x^3=-(1+2y^2)=-(1+\sqrt{-2}y)(1-\sqrt{-2}y),$$

where the factors are coprime: if $r\in\mathbb{Z}[\sqrt{-2}]$ is a non-unit which divides $1+\sqrt{-2}y$ and $1-\sqrt{-2}y$ then $r\mid(1+\sqrt{-2}y)+(1-\sqrt{-2}y)=2=-(\sqrt{-2})^2$. But $\sqrt{-2}$ is a prime in $\mathbb{Z}[\sqrt{-2}]$, so it follows that $2\mid N(x)$ which is a contradiction since x is odd. Hence it follows by the fundamental theorem of algebra that $1+\sqrt{-2}y$ and $1-\sqrt{-2}y$ are both cubes. Solving $1+\sqrt{-2}y=(a+b\sqrt{-2})^3$ for $a,b\in\mathbb{Z}$ yields

$$\begin{cases} a(a^2-6b^2)=1 \\ b(3a^2-2b^2)=y \end{cases}$$

The first equation tells us that $(a,b)=(1,0)$ is the only solution, then the second equation together with the relation $x^3+1=-2y^2$ give us $(x,y)=(1,0)$.

Case (i) Now we turn to (i). It is easy to spot that $(x,y)=(-1,0),(0,\pm 1)$ and $(2,\pm 3)$ are solutions of $x^3+1=y^2$. We will show that they are the only solutions. Let (x,y) be a rational solution, and write $x=a/b$, where $b>0$ and $\gcd(a,b)=1$. Assume also that $x\neq -1,0$ or 2, and set $c=a+b$. Since $\gcd(a,b)=1$, we have $\gcd(a,b,c)=1$. We will derive a contradiction from this. Since (x,y) is a solution, we have

$$\left(\frac{a}{b}\right)^3+1=y^2,$$

hence

$$b(a^3+b^3)=(b^2y)^2.$$

Also, note that we have

$$b(a^3+b^3)=bc(c^2-3bc+3b^2).$$

Hence $bc(c^2-3bc+3b^2)$ is a square. Moreover, $a\neq 0$ by assumption so $b\neq c$, and if we assume $c<0$ then $b>0$ implies $bc<0$, and $c^2-3bc+3b^2=c^2+3b(b-c)>0$ as $c^2, b-c>0$. So

$bc(c^2 - 3bc + 3b^2) < 0$, which is a contradiction since $bc(c^2 - 3bc + 3b^2)$ is a square. Hence $b, c > 0$.

Claim Let b, c be coprime positive integers such that $bc(c^2 - 3bc + 3b^2)$ is a square. Then we have either $b = c$ or $3 \mid c$.

Assume for now that the claim is true. Then we must have $3 \mid c$, so we can write $c = 3d$ and $3 \nmid b$. Substituting this, we obtain

$$bc(c^2 - 3bc + 3b^2) = 3^2 bd(b^2 - 3bd + 3d^2),$$

and since the left hand side is a square, $bd(b^2 - 3bd + 3d^2)$ is also a square. Since $3 \nmid b$, the claim implies $b = d$. But $\gcd(b, c) = 1$ and thus $\gcd(b, d) = 1$, so this implies $b = d = 1$, and hence $c = 3$. Therefore $x = a/b = 2$, which contradicts our assumption.

Thus it remains to prove the claim.

Proof of Claim. This follows Euler's argument, which uses infinite descent. Suppose, for a contradiction, that $b, c > 0$ are coprime integers such that $b \neq c$, $3 \nmid c$ and $bc(c^2 - 3bc + 3b^2)$ is a square. Then b and $c^2 - 3bc + 3b^2$ are coprime, for if $r \in \mathbb{Z}_{>1}$ divides b and $c^2 - 3bc + 3b^2$ then $r \mid c$, which contradicts $\gcd(b, c) = 1$. Noting $3 \nmid c$, we also see that c and $c^2 - 3bc + 3b^2$ are coprime. Since $b, c > 0$, by the fundamental theorem of algebra we can conclude that each of b, c and $c^2 - 3bc + 3b^2$ is a square. Write $c^2 - 3bc + 3b^2 = a^2$ for $a > 0$ and let $m, n > 0$ be such that $\gcd(b, c) = 1$ and $\frac{m}{n}b - c = a$. Then we have $c^2 - 3bc + 3b^2 = (\frac{m}{n}b - c)^2$. Then expanding the brackets gives

$$\frac{b}{c} = \frac{2mn - 3n^2}{m^2 - 3n^2}. \tag{6.7}$$

We consider two cases:

Case (a): $3 \nmid m$. In this case, we have that $2mn - 3n^2 = n(2m - 3n)$ and $m^2 - 3n^2$ are coprime, for if r is a prime common factor then $r \mid n$ and $r \mid m^2 - 3n^2$ implies $r \mid m$ which contradicts $\gcd(m, n) = 1$, so we must have $r \nmid n$ and $r \mid 2m - 3n$. Then $r \mid (2m - 3n)^2 - 4(m^2 - 3n^2) = 3n(4m - 7n)$ so $r \nmid 3, n$ implies $r \mid 4m - 7n$. Hence $r \mid 4(2m - 3n) - (4m - 7n) = n$, which is a contradiction. Hence we have either $(2mn - 3n^2, m^2 - 3n^2) = (b, c)$ or $(-b, -c)$. But if $m^2 - 3n^2 = -c$, then we have $m^2 \equiv 2 \bmod 3$ as c is a square such that $3 \nmid c$, which yields no solution. Hence we have

$$2mn - 3n^2 = b \quad \text{and} \quad m^2 - 3n^2 = c. \tag{6.8}$$

Then $3 \nmid m$ implies $3 \nmid c$. Also we can write $m^2 - 3n^2 = \left(\frac{p}{q}n - m\right)^2$ for $p, q > 0$ and $\gcd(p, q) = 1$. Note that we have $\frac{p}{q}n = \pm\sqrt{c} + m$ and we can choose the sign of $\sqrt{c}$ so that 3 does not divide the right hand side (if 3 divides both $\pm\sqrt{c} + m$ then $3 \mid 2m$, so $3 \mid m$, a contradiction) so we may assume $3 \nmid p$. Expanding the brackets gives $n^2\left(\frac{p^2}{q^2} + 3\right) = 2mn\frac{p}{q}$, so

$$\frac{m}{n} = \frac{p^2 + 3q^2}{2pq}. \tag{6.9}$$

Moreover, dividing $b = 2mn - 3n^2$ by n^2 and substituting the equation above, we obtain

$$\frac{b}{n^2} = \frac{p^2 - 3pq + 3q^2}{pq}.$$

Hence $pq(p^2 - 3pq + 3q^2) = \frac{b(pq)^2}{n^2}$, so that $pq(p^2 - 3pq + 3q^2)$ is a square. If $p = q$, then $\frac{m}{n} = \frac{4p^2}{2p^2} = 2$ by (6.9) so $\frac{c}{n^2} = 3 - \left(\frac{m}{n}\right)^2 = -1$ by (6.8), which is a contradiction since the left hand side is positive.

So $p \neq q$. Thus p and q satisfy the same conditions as b and c. Note that $q \mid n$ by definition so $q \mid b$. Hence $q < b$ unless $q = b$, in which case we also have $q = n$. But substituting this into (6.9) and using second equation of (6.8) gives $\frac{c}{q^2} = \frac{(p^2+3q^2)^2}{4p^2q^2} - 3$, so

$$p^2(4c - p^2) = 3q^2(3 - 2p^2).$$

So p must divide the right hand side, but $\gcd(p, 3) = 1$ and $\gcd(p, q) = 1$ so $p \mid 3 - 2p^2$, which gives $p \mid 3$, a contradiction. Hence $q < b$.

Case (b): $3 \mid m$. Then we can write $m = 3k$, so that (6.7) gives

$$\frac{b}{c} = \frac{6nk - 3n^2}{9k^2 - 3n^2} = \frac{n^2 - 2nk}{n^2 - 3k^2}. \tag{6.10}$$

Then $n^2 - 2nk$ and $n^2 - 3k^2$ are coprime, since if r is a prime factor then the argument of (a) implies $r \mid n - 2k$ and $n^2 - 3k^2$, and $r \nmid n$. But then $r \mid (n^2 - 3k^2) - (n - 2k)(n + 2k) = k^2$ so $r \mid k$, then this implies $r \mid n$ which is a contradiction. Then as in (a), reducing mod 3 implies that $n^2 - 3k^2$ and $n^2 - 2nk$ are positive. Hence we have

$$b = n^2 - 2nk \quad \text{and} \quad c = n^2 - 3k^2. \tag{6.11}$$

Since c is a square, we can write $n^2 - 3k^2 = \left(\frac{p}{q}k - n\right)^2$, where $p, q > 0$ and $\gcd(p, q) = 1$. Then as in (a), we may assume $3 \nmid p$. Also, expanding the brackets gives $k\left(\frac{p^2+3q^2}{q^2}\right) = 2n\frac{p}{q}$, so we have

$$\frac{n}{k} = \frac{p^2 + 3q^2}{2pq}. \tag{6.12}$$

Then dividing the first equation in (6.11) by n^2 and substituting (6.12), we obtain

$$\frac{b}{n^2} = \frac{p^2 - 4pq + 3q^2}{p^2 + 3q^2} = \frac{(p - q)(p - 3q)}{p^2 + 3q^2} \tag{6.13}$$

Therefore $(p - q)(p - 3q)(p^2 + 3q^2) = \frac{b(p^2+3q^2)^2}{n^2}$ is a square.

Let $t = |p - q|$ and $u = |p - 3q|$. Note that $p^2 + 3q^2 > 0$ and $(p - q)(p - 3q)(p^2 + 3q^2) > 0$, so t and u have the same sign. Hence we have $tu = (p - q)(p - 3q)$. Therefore, $u^2 - 3tu + 3t^2 = (p - 3q)^2 - 3(p - q)(p - 3q) + 3(p - q)^2 = p^2 - 3q^2$ and it follows that

$$(p - q)(p - 3q)(p^2 + 3q^2) = tu(u^2 - 3tu + 3t^2). \tag{6.14}$$

But $u \equiv \pm p \bmod 3$ and $3 \nmid p$ so $3 \nmid u$. Also $t \neq u$, otherwise $p - q = p - 3q$, i.e. $q = 0$. Moreover, t and u are positive by definition. It follows from (6.14) that t and u divided by their greatest common factor satisfy the same conditions as b and c. It remains to show that $t < b$. We consider the cases $t = q - p$ and $t = p - q$ separately.

If $t = q - p$, since $q \mid k$ by definition, we have $k \geqslant q = t + p > t$. But $b = n(n - 2k) \geqslant n \geqslant k$ so $b > t$ as required.

If $t = p - q$, we have $p > t$ and $u = p - 3q > 0$ so $p > 3q$, Hence $3k < p\left(\frac{k}{q}\right) = n \pm \sqrt{n^2 - 3k^2}$. But $p\left(\frac{k}{q}\right) = n - \sqrt{n^2 - 3k^2}$ implies $n - 3k > \sqrt{n^2 - 3k}$, then squaring both sides gives $3k(1 - 2n) + 9k^2 > 0$

so $2n-1<3k$. But we also have $b=n(n-2k)>0$ so $n>2k$. Hence $k=4k-3k<2n-3k<1$, which is a contradiction. Hence we must have

$$p\left(\frac{k}{q}\right)=n+\sqrt{n^2-3k^2}.$$

Write $\frac{k}{q}=l\geqslant 1$. If $l=1$, substituting $k=q$ in (6.12) gives $p^2+3q^2=2pn$, so $p\mid p^2+3q^2$. This implies $p\mid 3q^2$, which contradicts $3\nmid p$. Hence $l\geqslant 2$, that is, $k=ql\geqslant 2q$. Now let r be any prime dividing p. Then $r\nmid p^2+3q^2$, so (6.12) together with $\gcd(n,k)=1$ implies $\gcd(p^2+3q^2,2pq)=1$. Hence $k=2pq>p>t$, then as in the case $t=q-p$, $b\geqslant k$ implies $b>t$ as required.

Thus, given b and c satisfying the above condition, we can always find a pair of positive integers satisfying the same conditions, but with strictly smaller b. By infinite descent, no such b and c exist. This concludes the proof of claim, and hence the proof of proposition. □

Now that we know the solutions of (6.6), we can compute $a=-2X, b=4X^2+2Y$ and therefore $\gamma_2(\tau_0)=-(b^2-2ac)^2-8(2b-a^2)$. The values are listed in the following table:

X	Y	a	b	$\gamma_2(\tau_0)$
0	0	0	0	0
−1	0	2	4	−96
1	2	−2	8	−5280
1	−2	−2	0	−32
2	6	−4	28	−640320
2	−6	−4	4	−960

(6.15)

By Theorem 5.6, given imaginary quadratic fields K and K', we have $j(\mathcal{O}_K)=j(\mathcal{O}_{K'})$ if and only if $\mathcal{O}_K$ and $\mathcal{O}_{K'}$ are homothetic as lattices. But $\mathcal{O}_K=[1,w_K]$ and $\mathcal{O}_{K'}=[1,w_{K'}]$ where $w_K=\frac{d_K+\sqrt{d_K}}{2}$, hence we have $[1,w_K]=\lambda[1,w_{K'}]$ for some $\lambda\in\mathbb{C}$ so $\lambda=\alpha+\beta w_K$ and $\lambda w_{K'}=\gamma+\delta w_K$ for some $\alpha,\beta,\gamma,\delta\in\mathbb{Z}$. So we obtain $w_{K'}=\frac{\gamma+\delta w_K}{\alpha+\beta w_K}\in K=\mathbb{Q}(w_K)$. Hence $K'\subseteq K$, but K and K' have the same degree over $\mathbb{Q}$ so this implies $K=K'$. In particular, $j(\mathcal{O}_K)$ determines K uniquely. Therefore, it remains to compute the j-invariants (or γ_2, which is the cube root of j) for the six values of p and check that the values coincide with the those listed above in 6.15.

When $p=3$, we have $j(\mathcal{O}_K)=j(\tau_0)$ where $\tau_0=(-1+\sqrt{-3})/2=\omega$ and we computed $j(\omega)=0$ in Example 5.11. Turning to the cases $p=11,19,43,67$ or 163, let $\tau_0=(3+\sqrt{-p})/2$ as before. We want to compute $\gamma_2(\tau_0)$, which we can write in terms of Weber function $f_2(\tau_0)$:

$$\gamma_2(\tau_0)=f_2(\tau_0)^{16}+\frac{16}{f_2(\tau_0)^8}.$$

From (6.1), we know that

$$f_2(\tau_0)=\frac{\sqrt{2}}{f_1(2\tau_0)},$$

and then the transformation properties (6.3) imply

$$\begin{aligned}f_1(2\tau_0)=f_1(3+\sqrt{-p})&=\zeta_{48}^{-1}f(2+\sqrt{-p})\\&=\zeta_{48}^{-2}f_1(1+\sqrt{-p})\\&=\zeta_{48}^{-3}f(\sqrt{-p}).\end{aligned}$$

Combining these equations gives

$$f_2(\tau_0) = \frac{\sqrt{2}\zeta_{16}}{f(\sqrt{-p})},$$

and thus we obtain

$$\gamma_2(\tau_0) = \frac{256}{f(\sqrt{-p})^{16}} - f(\sqrt{-p})^8. \tag{6.16}$$

Now set $q = e^{-2\pi i\sqrt{-p}} = e^{-2\pi\sqrt{p}}$. Then the product expansion for the Weber function gives us

$$f(\sqrt{-p}) = q^{-1/48}\prod_{n=1}^{\infty}(1+q^{n-1/2}).$$

To estimate the infinite product, we use the inequality $1 + x < e^x$ for $x > 0$. This yields

$$1 < \prod_{n=1}^{\infty}(1+q^{n-1/2}) < \prod_{n=1}^{\infty} e^{q^{n-1/2}} = e^{\sqrt{q}/(1-q)}.$$

We can simplify the exponent by noting that $\sqrt{q}/(1-q) \leqslant \sqrt{q}/(1-e^{-2\pi}) < 1.002\sqrt{q}$ since $q \leqslant e^{-2\pi}$. Thus we have the following inequality for $f(\sqrt{-p})$:

$$q^{-1/48} < f(\sqrt{-p}) < q^{-1/48}e^{1.002\sqrt{q}}.$$

Applying this to (6.16), we get the bounds for $\gamma_2(\tau_0)$:

$$256q^{1/3} - q^{-1/6}e^{8.016\sqrt{q}} < \gamma_2(\tau_0) < 256q^{1/3}e^{-16.032\sqrt{q}} - q^{-1/6} \tag{6.17}$$

To see how sharp these bounds are, consider the difference

$$E = 256q^{1/3}(e^{-16.032\sqrt{q}} - 1) - q^{-1/6}(1 - e^{8.016\sqrt{q}}).$$

Then $q < e^{-2\pi}$ implies that $E < 0.25$. Therefore we obtain the formula

$$\gamma_2((3+\sqrt{-p})/2) = [-q^{-1/6} + 256q^{1/3}]$$

for $p = 11, 19, 43, 67$ and 163, where [ ] denotes the nearest integer function. Using a calculator, we can now compute the table for $\gamma_2(\tau_0)$:

d_K	p	τ_0	$\gamma_2(\tau_0)$
-3	3	$(1+\sqrt{-3})/2$	0
-11	11	$(3+\sqrt{-11})/2$	-32
-19	19	$(3+\sqrt{-19})/2$	-96
-43	43	$(3+\sqrt{-43})/2$	-960
-67	67	$(3+\sqrt{-67})/2$	-5280
-163	163	$(3+\sqrt{-163})/2$	-640320

(6.18)

Notice that the values of $\gamma_2(\tau_0)$ coinside with those computed in (6.15). It follows that we now know all imaginary quadratic fields of class number one. This proves the theorem. □

7 Beyond the Class Number One Problem

To conclude, let us see briefly the work that has been done on class numbers. We begin by restating the problems proposed by Gauss in his *Disquisitiones Arithmeticae*:

Conjecture 7.1 (Gauss). *1. The class number $h(D) \to \infty$ as $D \to -\infty$.*

2. Given a small positive integer n, Gauss gives lists of imaginary quadratic fields with class number n and believes them to be complete.

3. There are infinitely many real quadratic fields with class number one.

Very little progress was made on these conjectures until the 20^{th} century. Gauss' conjecture 1 was the first to be settled in 1934 by Heilbronn. In order to get a taste of how this was solved, we first need a few definitions. Given k, we can define *Dirichlet characters*, which are group characters

$$\chi : (\mathbb{Z}/k\mathbb{Z})^* \mapsto \mathbb{C}^*$$

satisfying $\chi(n+k) = \chi(n)\ \forall n \in \mathbb{Z}$, $\chi(mn) = \chi(m)\chi(n)\ \forall m, n \in \mathbb{Z}$ and $\chi(n) = 0$ for $\gcd(n, q) > 1$. There are $\phi(k)$ such characters $\chi \bmod k$. We can now define the *Dirichlet L-function*:

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

defined for $\mathrm{Re}(s) > 1$.

A remarkable connection between the Dirichlet L-function and the class number is illustrated in the following class number formula proved by Dirichlet in 1832.

Theorem 7.2 (**Dirichlet**). *Let $D < 0$ be a fundamental discriminant and let $\chi \bmod D$ be a real, odd, primitive (i.e. not induced by any character of smaller modulus) Dirichlet character. Then*

$$L(1, \chi) = 2\pi h(D)/w\sqrt{|D|},$$

where $w = 2$ for $D < -4$, $w = 4$ for $D = -4$ and $w = 6$ for $D = -3$.

Now, the *classical Riemann hypothesis* asserts that the only nontrivial zeros of the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ lie on the line $\mathrm{Re}(s) = 1/2$. Furthermore, if we replace $\zeta(s)$ by the formally similar, but much more general Dirichlet L-function $L(s, \chi)$ in the statement of the classical Riemann hypothesis, we get the *generalised Riemann hypothesis*. In 1918, a theorem was published which solves Gauss' conjecture 1 given the generalised Riemann hypothesis is true.

Theorem 7.3 (**Hecke**). *Let $D < 0$, and let $\chi \bmod D$ be an odd, real and primitive Dirichlet character. If $L(s, \chi) \neq 0$ for s real and $s > 1 - c/\log|D|$, then*

$$h(D) > c_1\sqrt{|D|}/\log|D|,$$

where $c, c_1 > 0$ are constants.

Hence, if the generalised Riemann hypothesis is true, the above theorem tells us that $h(D)$ grows with $|D|$, hence proves Gauss' conjecture 1. In 1933, Deuring proved the following unexpected and surprising result which supports Gauss' conjecture 1 but assumes the falsity of the classical Riemann hypothesis.

Theorem 7.4 (**Deuring**). *If the classical Riemann hypothesis is false, then* $h(D) \geqslant 2$ *for* $-D$ *sufficiently large.*

This result was improved by Mordell in 1934, who showed that in fact $h(D) \to \infty$ as $D \to -\infty$ if the classical Riemann hypothesis is false. In the same year, Heilbronn went a step further and proved:

Theorem 7.5 (**Heilbronn**). *If the generalised Riemann hypothesis is false, then* $h(D) \to \infty$ *as* $D \to -\infty$.

When combined with Hecke's theorem, we obtain an unconditional proof of Gauss' conjecture 1.

Theorem 7.6 (**Hecke–Deuring–Heilbronn**). $h(D) \to \infty$ *as* $D \to -\infty$.

This is one of the first instance of proof which first assumed that the generalised Riemann hypothesis was true and then that it was false, giving the same result in both cases!

On the other hand, Gauss' conjecture 3 which states that there are infinitely many real quadratic fields with class number one remains open. In fact, it is not even known whether there are infinitely many algebraic number fields with class number one. One way to approach this problem related to the theory of cyclotomic fields. Let μ_{p^∞} denote the group of all p-power roots of unity. Then it can be shown that

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \Delta \times \Gamma$$

where $\Delta \cong \mathbb{Z}/2\mathbb{Z}$ if $p = 2$ and $\Delta \cong (\mathbb{Z}/p\mathbb{Z})^\times$ otherwise, and $\Gamma \cong \mathbb{Z}_p$, the p-adic integers. Furthermore, if we let $\mathbb{Q}^{\mathrm{cyc},p}$ be the fixed field of Δ in $\mathbb{Q}(\mu_{p^\infty})$, then we have

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc},p}/\mathbb{Q}) = \Gamma \cong \mathbb{Z}_p.$$

More generally, given a number field F, a $\mathbb{Z}_p$-*extension* of F is a Galois extension F_∞/F with $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$. Let $\Gamma_n := p^n\Gamma \cong p^n\mathbb{Z}_p$, and let $F_n \subset F_\infty$ be the fixed field of Γ_n. Then we have $\mathrm{Gal}(F_n/F) \cong \mathbb{Z}/p^n\mathbb{Z}$. In 2009, Fukuda and Komatsu showed that the in the case $F = \mathbb{Q}$ and $p = 2$, $h(F_n)$ has no prime factor less than 1.1×10^8. In this case we have $F_n = \mathbb{Q}(2\cos(2\pi/2^{n+2}))$, a cyclotomic extension of $\mathbb{Q}$ of degree 2^n over $\mathbb{Q}$. Notice that to prove Gauss' conjecture 3, it suffices to prove $h(F_n) = 1$ for infinitely many n in the case $F = \mathbb{Q}$ and $p = 2$, so the above result is very promising. In fact, in 2010 the following question was posed:

Conjecture 7.7 (**Coates**). *For* $F = \mathbb{Q}$ *and* p *an arbitrary prime number,* $h(\mathcal{O}_{F_n}) = 1$ *for all* $n \geqslant 1$.

Now let us go back to Gauss' conjecture 2, and the general class number problem. First we mention that the class number two problem was also solved by Baker and Stark in 1971, and the class number h problems for h up to 100 were solved by 2004. In 1976 Goldfeld realised that the problem could be connected with the arithmetic of elliptic curves; if there is an elliptic curve of rank 3 and the Hasse–Weil L-function with zero of order 3 at $s = 1$ (which should be true, by the conjecture of Birch and Swinnerton-Dyer), then it yields an effective lower bound for $h(D)$.
To explain this in more detail, let us first define the Hasse–Weil L-function. To do this, let

$$E : y^2 = 4x^3 - ax - b \tag{7.1}$$

be an elliptic curve over $\mathbb{Q}$ with discriminant $a^3 - 27b^2$. Let $E(\mathbb{Q})$ denote, as usual, the group of rational points on E. Associated to E, we can define an integer N called the *conductor* of E, which is defined to be the product of all prime numbers dividing the discriminant Δ, and the powers of such a prime depends on the reduction of E at that prime. We can define the *Hasse–Weil L-function* associated with E:

$$L(E, s) = \prod_{p|N}(1 - t_p p^{-s})^{-1} \prod_{p\nmid N}(1 - t_p p^{-s} + p^{1-2s})^{-1}, \tag{7.2}$$

where

$$N_p = \text{Card}\{(x,y) \bmod p : y^2 \equiv 4x^3 - ax - b \bmod p\}$$

and

$$t_p = \begin{cases} p - N_p & \text{if } p \nmid N \\ \pm 1 \text{ or } 0 & \text{if } p \mid N \end{cases}$$

We can now state

Conjecture 7.8 (**Birch and Swinnerton-Dyer**). *If* $\text{rank}_{\mathbb{Z}}(E(\mathbb{Q})) = g$, *then*

$$L(E,s) \sim c_E(s-1)^g,$$

where $c_E \neq$ *is a constant. In particular, the rank of* $E(\mathbb{Q})$ *is equal to the order of the zero of* $L(E,s)$ *at* $s = 1$.

Goldfeld found in 1976 an effective lower bound for $h(D)$, provided the Birch and Swinnerton-Dyer conjecture holds for a suitable elliptic curve of rank 3. Notice that finiding a lower bound for $h(D)$ is an effective way of solving the general class number problem: given a positive integer h, if we can show that $h(D) > h$ for $D > m$, say, then we only need to compute $h(D)$ for $D \leqslant m$ to solve the class number h problem.

Theorem 7.9 (**Goldfeld**). *Let* E *be an elliptic curve over* $\mathbb{Q}$ *with Hasse–Weil L-function* $L(E,s)$. *Let* $\text{rank}_{\mathbb{Z}}(E(\mathbb{Q})) = g$ *and let* N *be the conductor of* E. *Let* $D < 0$ *be a squarefree discriminant such that* $\gcd(D,N) = 1$, *and let* $\chi \bmod D$ *be the real, odd, primitive Dirichlet character associated to the imaginary quadratic field* $\mathbb{Q}(\sqrt{D})$. *Choose* $\mu = 1, 2$ *so that* $\chi(-N) = (-1)^{g-\mu}$. *If* $L(E,s) \sim c_E(s-1)^g$ *for a constant* $c_E \neq 0$ *then*

$$h(D) > \frac{c}{g^{4g}N^{13}}(\log|D|)^{g-\mu-1}\exp\{-21\sqrt{g\log\log|D|}\}$$

where $c > 0$ *is a constant independent of* E.

Remark 7.10. There is a similar result for the case $\gcd(D,N) > 1$. This theorem reduces Gauss' conjecture 1 to finding an elliptic curve of rank 3 whose Hasse–Weil L-function has a triple zero at $s = 1$, as in this case the right hand side of the inequality diverges to infinity.

In 1983 Gross and Zagier proved that, for certain curves where the Hasse–Weil L-function has an odd order zero at $s = 1$, the first-order coefficient is related to *Heegner points* on the curve. Using this result, it can be shown that $L_{E_0}(s)$ has a triple zero at $s = 1$ where $E_0 : -139y^2 = x^3+4x^2-48x+80$ is an elliptic curve of rank 3. A better bound was found by Oesterlé in 1984:

Theorem 7.11 (**Oesterlé**).

$$h(D) > C(\log|D|)\prod_{p|D,\, p\neq D}\left(1 - \frac{[2\sqrt{p}]}{p+1}\right).$$

where $[2\sqrt{p}]$ *denotes the greatest integer smaller than or equal to* $2\sqrt{p}$, $C = 1/55$ *if* $5077 \nmid D$, *and* $C = 1/7000$ *otherwise.*

Oesterlé obtained this bound by computing the constant in Theorem 7.9 first by using the elliptic curve E_0, and then by using the elliptic curve of conductor 5077 found by Brumer and Kramer. To see concretely what this means, let us apply it to the class number three problem. For $h(D) = 3$, the above bound gives us

$$|D| \leqslant e^{165} < 10^{72}.$$

Combined with the bounds of Montgomery-Weinberger that

$$h(D) \neq 3 \text{ for } 907 < -D < 10^{2500},$$

it remains to check $h(D)$ for $D > -907$, and thus the class number three problem is solved. If the reader is interested, Serre [15] and Goldfeld [8] have pleasant articles summarising the work on the size of $h(D)$.

Acknowledgments

I am very grateful to my supervisor Professor Kevin Buzzard for many inspiring and insightful discussions. In particular, Section 4 of this project would not have existed if he had not introduced global class field theory to me.

References

[1] Saban Alaca and Kenneth S. Williams. *Introductory algebraic number theory*. Cambridge University Press, Cambridge, 2004.

[2] A. Baker. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika 13 (1966), 204-216; ibid. 14 (1967), 102-107; ibid.*, 14:220–228, 1967.

[3] B. J. Birch. Weber's class invariants. *Mathematika*, 16:283–294, 1969.

[4] A. I. Borevich and I. R. Shafarevich. *Number theory*. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20. Academic Press, New York, 1966.

[5] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[6] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[7] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[8] Dorian Goldfeld. Gauss's class number problem for imaginary quadratic fields. *Bull. Amer. Math. Soc. (N.S.)*, 13(1):23–37, 1985.

[9] Kurt Heegner. Diophantische Analysis und Modulfunktionen. *Math. Z.*, 56:227–253, 1952.

[10] Gerald J. Janusz. *Algebraic number fields*. Academic Press [A Subsidiary of Harcourt Brace Jovanovich, Publishers], New York-London, 1973. Pure and Applied Mathematics, Vol. 55.

[11] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[12] G. B. Mathews. *Theory of numbers*. 2nd ed. Chelsea Publishing Co., New York, 1961.

[13] James S. Milne. Algebraic number theory (v3.04), 2012. Available at www.jmilne.org/math/.

[14] Jürgen Neukirch. *Class field theory*, volume 280 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1986.

[15] Jean-Pierre Serre. $\Delta = b^2 - 4ac$. *Math. Medley*, 13(1):1–10, 1985.

[16] H. M. Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.*, 14:1–27, 1967.