ORDERS IN QUADRATIC IMAGINARY FIELDS OF SMALL CLASS NUMBER

JANIS KLAISE

Abstract. In 2003 M. Watkins [Wat03] solved the Gauss Class Number Problem for class numbers up to 100: given a class number h, what is the complete list of quadratic imaginary fields K with this class number? In this project we extend the problem by including non-maximal orders - subrings $\mathcal{O}$ of the ring of integers $\mathcal{O}_K$ that are also $\mathbf{Z}$-modules of rank 2 admiting a $\mathbf{Q}$-basis of K. These orders are more complicated than $\mathcal{O}_K$ since they need not be Dedekind domains. The main theoretical part is the class number formula linking the class numbers of $\mathcal{O}$ and $\mathcal{O}_K$. We give a complete proof of this and use it together with the results of Watkins to find the orders of class number $h = 1, 2, 3$ by solving the class number formula in a Diophantine fashion. We then describe a different algorithm that was suggested and implemented during the writing of this project and succesfully finds all orders of class number up to 100. Finally, we motivate the problem by its application to j-invariants in complex multiplication.

Contents

1. Introduction

Gauss in his *Disquisitiones Arithmeticae* [Gau86, §303-304] came up with several conjectures about imaginary quadratic fields (in the language of discriminants of integral binary quadratic forms). In particular, he gave lists of discriminants corresponding to imaginary quadratic fields with given small class number and believed them to be complete without proof. This became known as the Gauss Class Number Problem - for each $h \geq 1$ provide a complete list of imaginary quadratic fields with class number h. The case $h = 1$ was solved independently by Heegner [Hee52], Baker [Bak66] and Stark [Sta67]. Subsequently, $h = 2$ was solved again by Baker [Bak71] and Stark [Sta75]. The cases $h = 3$ and $h = 4$ were solved by Oesterlé [Oes85] and Arno [Arn92] respectively. Wagner [Wag96] solved the cases

Date: March 27, 2012.

$h = 5$, 6, 7 and Arno *et al.* [ARW98] solved the cases for $5 \leq h \leq 23$ odd. Finally, Watkins [Wat03] solved the problem for all $h \leq 100$. In this project we will extend these calculations to general *orders* of imaginary quadratic fields that correspond to *non-fundamental* discriminants (defined below).

Every quadratic field K has a discriminant d_K which is defined in terms of the integral basis of the ring of integers $\mathcal{O}_K$. The discriminants d_K are what we call *fundamental discriminants*:

Definition. An integer D is called a *fundamental discriminant* if either $D \equiv 1 \pmod 4$ and is squarefree or $D = 4d$ with $d \equiv 2, 3 \pmod 4$ with d squarefree.

Thus the fundamental discriminants are exactly the discriminants of quadratic fields.

It is well known that if $\mathbf{Q}\left(\sqrt{d}\right)$ is a quadratic field with d a squarefree integer and $\mathcal{O}_K = [1, w_K]$ is an integral basis, then if $d \not\equiv 1 \pmod 4$, the discriminant is $d_K = 4d$ and we can take $w_K = \sqrt{d}$ and if $d \equiv 1 \pmod 4$, then the discriminant is $d_K = d$ and we can take $w_K = \frac{1+\sqrt{d}}{2}$ (See for example [ST01, p. 62-63]or [Coh96, p. 223]). More succintly, we always have an integral basis $\mathcal{O}_K = [1, w_K]$ with $w_K = \frac{d_K+\sqrt{d_K}}{2}$.
Now Gauss originally included in his lists what we sometimes call *non-fundamental discriminants*. Together with the fundamental ones, they give a very easy description of what we mean by a discriminant in general:

Definition. An integer D is called a *discriminant* if $D \equiv 0, 1 \pmod 4$ and is non-square.

The question is, are these non-fundamental discriminants connected with quadratic fields in a similar way as the fundamental discriminants are (as discriminants of quadratic fields)? The answer is yes - they correspond to discriminants of *orders* in quadratic fields which will be the main objects of study in this project. There are many definitions of an order, some of which exclude certain properties and prove them later. Here we give a comprehensive definition that includes the properties we are interested in:

Definition. An *order* $\mathcal{O}$ of a quadratic field K is a subring $\mathcal{O} \subset \mathcal{O}_K$ that is also a free $\mathbf{Z}$-module of rank $2 = [K\colon \mathbf{Q}]$ so that it contains an integral basis of K.

In particular, we call $\mathcal{O}_K$ the *maximal order* since it contains every other order. Moreover, since both $\mathcal{O}$ and $\mathcal{O}_K$ are free $\mathbf{Z}$-modules of the same rank, we have that the index $f = [\mathcal{O}_K\colon \mathcal{O}]$ is finite. We call f the *conductor* of $\mathcal{O}$. Then if $\mathcal{O}_K = [1, w_K]$ as above, one can show that $\mathcal{O} = [1, fw_K]$ (See for example [Cox89, p. 133]).

Since an order $\mathcal{O}$ admits an integral basis of K, we can define the discriminant of $\mathcal{O}$ in exactly the same way as for $\mathcal{O}_K$ - the square of a 2×2 determinant with rows being the integral basis under the 2 automorphisms of the field K. In the same way as for $\mathcal{O}_K$, we can show that the discriminant of $\mathcal{O}$ is independent of the basis used and calculating it using the basis $[1, fw_K]$ gives the discriminant $D = f^2 d_K$

where d_K is the (fundamental) discriminant of $\mathcal{O}_K$.

So in fact every such discriminant D satisfies $D \equiv 0,\ 1 \pmod 4$ and so is consistent with our previous definition of a discriminant. But more is true. Any discriminant D is a discriminant of some order in a quadratic imaginary field; we summarize this in the following proposition:

Proposition. [Coh96, p. 224] *If K is a quadratic field of discriminant d_K then every order $\mathcal{O}$ of K has discriminant $D = f^2 d_K$ where $f \geq 1$ is an integer. Conversely, if $D \equiv 0,\ 1 \pmod 4$ and is squarefree, then $D = f^2 d_K$ uniquely for some fundamental discriminant d_K and there exists a unique order $\mathcal{O} \subset \mathbf{Q}(\sqrt{d_K})$ with discriminant D.*

In Section 2 we will develop a theory of ideals of $\mathcal{O}$ and arrive at a notion of the class group $C(\mathcal{O})$ of $\mathcal{O}$ analogously to the usual class group $C(\mathcal{O}_K)$ of the field K. The main result we derive is the following class number formula linking the class numbers of $\mathcal{O}$ and $\mathcal{O}_K$:

Theorem. [Cox89, p. 146]
Let $\mathcal{O}$ be the order of conductor f in an imaginary quadratic field K. Then

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)\, f}{\left[\mathcal{O}_K^\times : \mathcal{O}^\times\right]} \prod_{p \mid f} \left(1 - \left(\frac{d_K}{p}\right) \frac{1}{p}\right) \tag{1.1}$$

Furthermore, $h(\mathcal{O})$ is always an integer multiple of $h(\mathcal{O}_K)$.

Here $\left(\frac{d_K}{p}\right)$ is the Legendre-Kronecker symbol:

Definition. For an odd prime p, let $\left(\frac{d_K}{p}\right)$ be the Legendre symbol and for $p = 2$ define the Kronecker symbol:

$$\left(\frac{d_k}{2}\right) = \begin{cases} 0 & \text{if } 2 \mid d_K \\ 1 & \text{if } d_K \equiv 1 \pmod 8 \\ -1 & \text{if } d_K \equiv 5 \pmod 8 \end{cases} \tag{1.2}$$

Our aim is then to caclulate precisely which orders (or equivalently discriminants) have a given class number $h = h(\mathcal{O})$ up to $h \leq 100$.

In Section 3 we use the class number formula 1.1 and the Watkins table of fundamental discriminants [Wat03, p. 936] to explicitly solve the formula as a Diophantine equation for $(f,\ d_K)$ given $h(\mathcal{O}) = 1,\ 2,\ 3$.

In Section 4 we describe a different algorithm that was suggested and implemented during the course of writing this project. It succesfully finds all pairs $(f,\ d_K)$ given the desired class number $h(\mathcal{O}) = 1, \ldots 100$.

In the last section we motivate the problem of finding all discriminants of given class number by its application to j-invariants in the theory of complex multiplication.

2. The Class Number Formula

In order to prove the class number formula given above, we need to understand more about the theory of ideals in a non-maximal order $\mathcal{O}$. In particular, the difficulties arise because $\mathcal{O}$ is not a Dedekind domain, hence unique factorization of ideals into prime ideals fails and not every non-zero fractional ideal is invertible (so they don't form a group under multiplication). To retrieve these familiar properties characteristic of the maximal order $\mathcal{O}_K$ we need to restrict ourselves to smaller subsets of ideals $\mathfrak{a} \subset \mathcal{O}$ with some special properties.

Throughout this section we closely follow the book [Cox89, p. 132-150]. We reproduce the complete proof of the class number formula filling in the more important details left out in the book and cutting out the less important where possible.

Definition 1. An ideal $\mathfrak{a} \subset \mathcal{O}$ is called *proper* if $\mathcal{O} = \{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\}$.

Note that it is always true that $\mathcal{O} \subset \{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\}$ since $\mathfrak{a}$ is an ideal of $\mathcal{O}$, but equality need not occur.

We will use Definition 1 in the context of fractional ideals. Recall that a *fractional ideal* of $\mathcal{O}$ is a an $\mathcal{O}$-submodule $\mathfrak{a} \subset K$ such that there exists $r \in \mathcal{O} \setminus \{0\}$ with $r\mathfrak{a} \subset \mathcal{O}$. All of the fractional ideals take the form $\alpha\mathfrak{a}$ where $\alpha \in K^\times$ and $\mathfrak{a}$ is an ideal of $\mathcal{O}$ [Cox89, p. 135].

Recall also, that for the maximal order $\mathcal{O}_K$, the quotient $\mathcal{O}_K/\mathfrak{a}$ for any non-zero ideal $\mathfrak{a}$ is finite, so we can define the *norm* of and ideal to be $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$. The proof of the finiteness of the quotient adapts in the case of a non-maximal order $\mathcal{O}$, so our definition of a norm extends to all orders.

We know that all non-zero fractional ideals $\mathfrak{a}$ of $\mathcal{O}_K$ are *invertible* in the sense that there exists another fractional ideal $\mathfrak{b}$ of $\mathcal{O}_K$ such that $\mathfrak{ab} = \mathcal{O}_K$. We now show that the same is true in any order $\mathcal{O}$ if we restrict to proper fractional ideals. In fact, the notions of *proper* and *invertible* are equivalent.

Proposition 2. *Let $\mathcal{O}$ be an order of a quadratic field K and let $\mathfrak{a}$ be a fractional $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is proper $\iff$ $\mathfrak{a}$ is invertible.*

Proof. ($\Longleftarrow$) Suppose $\mathfrak{a}$ is invertible. Then there exists fractional $\mathcal{O}$-ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathcal{O}$. Now let $\beta \in K$ satisfy $\beta\mathfrak{a} \subset \mathfrak{a}$, then we have

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

so $\beta \in \mathcal{O}$ and hence $\mathfrak{a}$ is proper.

For the other implication we need a technical lemma.

Lemma 3. *Let $K = \mathbf{Q}(\tau)$ be a quadratic field and let $ax^2 + bx + c$ bet the minimal polynomial of τ with $gcd(a, b, c) = 1$. Then $[1, \tau]$ is a proper fractional ideal of the order $[1, a\tau] \subset K$.*

Proof. Note that $[1,\, a\tau]$ is indeed an order since $a\tau$ is an algebraic integer. Given $\beta \in K$, if $\beta\,[1,\,\tau] \subset [1,\,\tau]$, then this means $\beta \cdot 1 \in [1,\,\tau]$ and $\beta \cdot \tau \in [1,\,\tau]$. In other words we have

$$\begin{aligned} \beta &= m + n\tau \text{ for some} m,\, n \in \mathbf{Z} \\ \beta\tau &= m\tau + n\tau^2 = \frac{-cn}{a} + \left(\frac{-bn}{a} + m\right)\tau \end{aligned}$$

Since $\gcd(a, b, c) = 1$, we have $\beta\tau \in [1,\,\tau] \iff a \mid n$ and so $\{\beta \in K\colon \beta\,[1,\,\tau] \subset [1,\,\tau]\} = [1,\,a\tau]$. □

Using this we can prove the other implication.

($\Longrightarrow$) Suppose $\mathfrak{a}$ is proper. Note that $\mathfrak{a}$ is a $\mathbf{Z}$-module of rank 2 so we can write $\mathfrak{a} = [\alpha,\,\beta]$ for some $\alpha,\,\beta \in K$. Now define $\tau = \frac{\beta}{\alpha}$ so that $\mathfrak{a} = \alpha\,[1,\,\tau]$. Let $ax^2 + bx + c$ bet the minimal polynomial of τ with coprime coefficients. Then by Lemma 3, we must have $\mathcal{O} = [1,\,a\tau]$. Now consider the non-trivial automorphism of K taking τ to its conjugate $\tau\prime$. Since $\tau\prime$ is a root of the minimum polynomial, applying the lemma once more gives that $\mathfrak{a}' = \alpha'\,[1,\,\tau']$ is a fractional ideal of $[1,\,a\tau] = [1,\,a\tau'] = \mathcal{O}$. We will show that $\mathfrak{a}\mathfrak{a}' = \frac{N(\alpha)}{a}\mathcal{O}$ which shows that $\mathfrak{a}$ is invertible.

Note that

$$a\mathfrak{a}\mathfrak{a}' = a\alpha\alpha'\,[1,\,\tau]\,[1,\,\tau'] = N(\alpha)\,[a,\,a\tau,\,a\tau',\,a\tau\tau']$$

But we also have $\tau + \tau' = -b/a$ and $\tau\tau' = c/a$, so the above expression becomes

$$a\mathfrak{a}\mathfrak{a}' = N(\alpha)\,[a,\,a\tau,\,-b,\,c] = N(\alpha)\,[1,\,a\tau] = N(\alpha)\,\mathcal{O}$$

since $\gcd(a, b, c) = 1$.

□

In particular, this proposition also shows that in the maximal order $\mathcal{O}_K$ every non-zero fractional ideal is proper.

Now that we know that proper fractional ideals are invertible, we can define the ideal class group $C(\mathcal{O})$ of an order $\mathcal{O}$.

Definition 4. Let $\mathcal{O}$ be an order. Denote by $I(\mathcal{O})$ the set of all proper fractional. Then $I(\mathcal{O})$ is a group under multiplication and contains the principal $\mathcal{O}$-ideals denoted $P(\mathcal{O}) \subset I(\mathcal{O})$ as a subgroup. We define the *ideal class group* to be the quotient

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

Note that if $\mathcal{O} = \mathcal{O}_K$ is the maximal order, $C(\mathcal{O}_K)$ is the usual ideal class group of the number field K. From now on we will use the notation I_K and P_K for $I(\mathcal{O}_K)$ and $P(\mathcal{O}_K)$ respectively.

Next we state a major theorem relating integral binary quadratic forms to ideals. This is a classical result which allows to set up a $1-1$ correspondence between ideal classes in $C(\mathcal{O})$ and classes of forms as defined below. We are only interested in one application of this theorem, so we do not dwell on the details for long. The basic definitions and results are summarized below.

Definition 5. (Terminology of quadratic forms)

- A *binary integral quadratic form* is an expression of the form $f(x,y) = ax^2 + bxy + cx$ with $a, b, c \in \mathbf{Z}$.
- A form is said to be *primitive* if $\gcd(a,b,c) = 1$
- An integer m is *represented* by a form $f(x,y)$ if the equation $f(x,y) = m$ has an integer solution in x and y. In addition, if $\gcd(x,y) = 1$, then it is said that f represents m *properly*.
- Two forms $f(x,y)$ and $g(x,y)$ are said to be *(properly) equivalent* if there exist integers p, q, r, s with $f(x,y) = g(px+qy, rx+sy)$ and $ps - qr = 1$ and this gives an equivalence relation on the set of forms.
- A form f is said to be *positive definite* if $f(x,y) > 0$ for all x, y.
- The *discriminant* of a form is defined to be $D = b^2 - 4ac$.
- A primitive positive definite form $ax^2 + bx + c$ is said to be *reduced* if

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

Fact 6. *(Properties of quadratic forms)*

- *Equivalent forms have the same discriminant and the notion of positive definiteness is invariant under equivalence* [Cox89, p. 25]. *So define $C(D)$ to be the set of proper equivalence classes of primitive positive definite forms of discriminant D.*
- *Every primitive positive definite form is properly equivalent to a unique reduced form* [Cox89, p. 27].
- *There is a finite number of reduced forms of fixed discriminant D* [Cox89, p. 29]. *Thus $C(D)$ is finite and we write $h(D)$ for the number if classes of primitive positive definite forms of discriminant D.*
- *If $D \equiv 0, 1 \pmod 4$ is negative, then $C(D)$ can be made into an abelian group under certain composition rules for forms, called the form class group* [Cox89, p. 50].

Theorem 7. [Cox89, p. 137] *Let $\mathcal{O}$ be the order of discriminant D in an imaginary quadratic field K. Then*

1. *If $f(x,y) = ax^2 + bxy + cy^2$ is a primitive positive definite quadratic form of discriminant D, then $\left[a, \left(-b + \sqrt{D}\right)/2\right]$ is a proper ideal of $\mathcal{O}$.*
2. *The map $f(x,y) \longmapsto \left[a, \left(-b + \sqrt{D}\right)/2\right]$ induces an isomorphism between the form class grouo $C(D)$ and the ideal class group $C(\mathcal{O})$.*
3. *A positive integer m is represented by a form $f(x,y)$ iff m is the norm $N(\mathfrak{a})$ of some ideal $\mathfrak{a}$ in the corresponding ideal class in $C(\mathcal{O})$.*

It is not hard to come up with the idea of this correspondence between quadratic forms and ideals, the hard part of the theorem is checking all the details that come with this correspondence, for example, that equivalent forms are mapped to ideals in the same class, so the proof involves a lot of explicit calculations.

One immediate consequence of this theorem is that calculating the class number of an order $\mathcal{O}$ is equivalent to counting the number reduced forms of discriminant D. I have implemented this myself to see that it gives the correct results, however the actual algorithm is quite inefficient when compared to analytic methods.

For us, we are interested in applying part 3. of Theorem 7 to deduce the following fact about ideal classes in $C(\mathcal{O})$ which will play a crucial role in establishing the formula.

Proposition 8. *Let $\mathcal{O}$ be an order of an imaginary quadratic field. Given an integer $M \neq 0$, every ideal class in $C(\mathcal{O})$ contains a proper $\mathcal{O}$-ideal with norm relatively prime to M.*

Proof. We first show the following fact about quadratic forms. Given a primitve form $f(x,y) = ax^2 + bxy + cy^2$ with $gcd(a,b,c) = 1$ and an integer M, $f(x,y)$ properly represents numbers coprime to M. In other words, we can always find x, y coprime with $f(x,y)$ coprime to M. To see this, let p be a prime dividing M. Note that since$f(x,y)$ is primitive, p does not divide at least one of a, b, c. If $p \mid a$ and $p \mid c$, then $p \nmid b$ so taking x, y coprime to p will make $f(x,y)$ coprime to p. If on the other hand $p \nmid a$ (resp. $p \nmid c$), then take x, y with $p \nmid x$ and $p \mid y$ (resp. $p \mid x$ and $p \nmid y$) so that $f(x,y)$ is again coprime to M. Now, by the Chinese Remainder Theorem, we can choose x, y in this way for every prime $p \mid M$. At this point, if x, y are not coprime, divide through by any common factors.
Now we use part 3. of Theorem 7: since $f(x,y)$ represents numbers coprime to M, the corresponding ideal class to $f(x,y)$ contains ideals with norm coprime to M. □

In order to prove the formula, we need to translate proper $\mathcal{O}$-ideals in terms of $\mathcal{O}_K$-ideals. We do this through the concept of ideals prime to the conductor.

Definition 9. Let $\mathcal{O}$ be an order of conductor f and let $\mathfrak{a} \subset \mathcal{O}$ be a nonzero ideal. We say that $\mathfrak{a}$ is *prime to f* if $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$.

The following lemma summarizes give two important properties of such ideals.

Lemma 10. *Let $\mathcal{O}$ be an order of conductor f. Then*

1. *An $\mathcal{O}$-ideal $\mathfrak{a}$ is prime to f $\iff$ its norm $N(\mathfrak{a})$ is coprime to f.*
2. *Every $\mathcal{O}$-ideal prime to f is proper.*

Proof.

1. Define a map $m_f \colon \mathcal{O}/\mathfrak{a} \longrightarrow \mathcal{O}/\mathfrak{a}$ to be multiplication by f. Then we have
$$\mathfrak{a} + f\mathcal{O} = \mathcal{O} \iff m_f \text{ is surjective} \iff m_f \text{ is an isomorphism}$$
But by the classification of finite Abelian groups, m_f is an isomorphism $\iff$ f is coprime to the order $N(\mathfrak{a})$ of $\mathcal{O}/\mathfrak{a}$.
2. Let $\beta \in K$ satisfy $\beta\mathfrak{a} \subset \mathfrak{a}$. Then we have $\beta \in \mathcal{O}_K$ and
$$\beta\mathcal{O} = \beta(\mathfrak{a} + f\mathcal{O}) = \beta\mathfrak{a} + \beta f\mathcal{O} \subset \mathfrak{a} + f\mathcal{O}_K$$
But we also have $f\mathcal{O}_K \subset \mathcal{O}$ so that $\beta\mathcal{O} \subset \mathcal{O}$ giving $\beta \in \mathcal{O}$ proving $\mathfrak{a}$ is proper.

□

It follows from this lemma that $\mathcal{O}$-ideals prime to f form subset of $I(\mathcal{O})$ that is closed under multiplication. Thus we can the define the subgroup of fractional ideals they generate and denote it by $I(\mathcal{O}, f) \subset I(\mathcal{O})$ and as usual we also have the subgroup generated by the principal ideals deonted $P(\mathcal{O}, f) \subset I(\mathcal{O}, f)$. It turns out we can describe the class group $C(\mathcal{O})$ in terms of these two subgroups.

Proposition 11. *The inclusion $I(\mathcal{O},f)\subset I(\mathcal{O})$ induces an isomorphism*

$$I(\mathcal{O},f)/P(\mathcal{O},f)\cong I(\mathcal{O})/P(\mathcal{O})=C(\mathcal{O})$$

Proof. The map $I(\mathcal{O},f)\longrightarrow C(\mathcal{O})$ taking a fractional ideal prime to f to its ideal class is surjective by Proposition 8 and the kernel of this map is $I(\mathcal{O},f)\cap P(\mathcal{O})$. This clearly contains $P(\mathcal{O},f)$ so we need to show the other inclusion, then the result follows by the First Isomorphism Theorem.

An element of the kernel is a principal fractional ideal $\alpha\mathcal{O}=\mathfrak{a}\mathfrak{b}^{-1}$ with $\alpha\in K$ and $\mathfrak{a},\mathfrak{b}$ $\mathcal{O}$-ideals prime to f. Define $m=N(\mathfrak{b})$.Then we have $m\mathcal{O}=N(\mathfrak{b})\mathcal{O}=\mathfrak{b}\bar{\mathfrak{b}}$ so that $m\mathfrak{b}^{-1}=\bar{\mathfrak{b}}$. This gives us

$$m\alpha\mathcal{O}=\mathfrak{a}m\mathfrak{b}^{-1}=\mathfrak{a}\bar{\mathfrak{b}}\subset\mathcal{O}$$

which shows that $m\alpha\mathcal{O}\subset P(\mathcal{O},f)$. But then $\alpha\mathcal{O}=m\alpha\mathcal{O}\cdot(m\mathcal{O})^{-1}$ is in $P(\mathcal{O},f)$ as well. □

We now extend the definition of ideals prime to conductor to ideals of the maximal order $\mathcal{O}_K$. This will enable us to derive a relation between ideals of $\mathcal{O}$ prime to the conductor f and ideals of $\mathcal{O}_K$.

Definition 12. Let $m>0$ be an integer. An ideal $\mathfrak{a}\subset\mathcal{O}_K$ is *prime to* m if $\mathfrak{a}+m\mathcal{O}_K=\mathcal{O}_K$.

As in the Lemma 10, this is the same as saying $gcd(N(\mathfrak{a}),m)=1$. We can thus similarly define a subgroup of fractional ideals $I_K(m)\subset I_K$ generated by $\mathcal{O}_K$-ideals prime to m. The next proposition relates such ideals of $\mathcal{O}$ and $\mathcal{O}_K$.

Proposition 13. *Let $\mathcal{O}$ be an order of conductor f. Then*

1. *If $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal prime to f, then $\mathfrak{a}\cap\mathcal{O}$ is an $\mathcal{O}$-ideal prime to f of the same norm.*
2. *If $\mathfrak{a}$ is an $\mathcal{O}$-ideal prime to f, then $\mathfrak{a}\mathcal{O}_K$ is an $\mathcal{O}_K$-ideal prime to f of the same norm.*
3. *The map $\mathfrak{a}\longmapsto\mathfrak{a}\cap\mathcal{O}$ induces an isomorphism $I_K(f)\cong I(\mathcal{O},f)$ with an inverse map $\mathfrak{a}\longmapsto\mathfrak{a}\mathcal{O}_K$.*

Proof.

1. Let $\mathfrak{a}\subset\mathcal{O}_K$ be prime to f. Consider the composite map

   $$\mathcal{O}\hookrightarrow\mathcal{O}_K\longrightarrow\mathcal{O}_K/\mathfrak{a}$$

   This has kernel $\mathfrak{a}\cap\mathcal{O}$, so the map $\mathcal{O}/\mathfrak{a}\cap\mathcal{O}\longrightarrow\mathcal{O}_K/\mathfrak{a}$ is injective. So since $N(\mathfrak{a})$ is prime to f, so is $N(\mathfrak{a}\cap\mathcal{O})$ showing that $\mathfrak{a}\cap\mathcal{O}$ is prime to f. To see that the norms are equal, we show that the injective map is also surjective. Since $\mathfrak{a}$ is prime to f, multiplication by f gives an automorphism of $\mathcal{O}_K/\mathfrak{a}$ as in Lemma 10. But we also have $f\mathcal{O}_K\subset\mathcal{O}$, so the map is surjective.
2. Let $\mathfrak{a}\subset\mathcal{O}$ be prime to f. We have

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

   so that $\mathfrak{a}\mathcal{O}_K$ is prime to f. For norms see the argument in part 3.

(3) We prove 2 claims:

$$\mathfrak{a}\mathcal{O}_K \cap \mathcal{O} = \mathfrak{a} \text{ when } \mathfrak{a} \text{ is an } \mathcal{O}\text{-ideal prime to } f \tag{2.1}$$

$$(\mathfrak{a} \cap \mathcal{O})\,\mathcal{O}_K = \mathfrak{a} \text{ when } \mathfrak{a} \text{ is an } \mathcal{O}_K\text{-ideal prime to } f \tag{2.2}$$

We start with claim 2.1; if $\mathfrak{a}$ is an $\mathcal{O}$-ideal prime to f, then:

$$\begin{aligned}
\mathfrak{a}\mathcal{O}_K \cap \mathcal{O} &= (\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})\,\mathcal{O} \\
&= (\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})\,(\mathfrak{a} + f\mathcal{O}) \\
&\subset \mathfrak{a} + f\,(\mathfrak{a}\mathcal{O}_K \cap \mathcal{O}) \\
&\subset \mathfrak{a} + \mathfrak{a}f\mathcal{O}_K \\
&\subset \mathfrak{a} + \mathfrak{a}\mathcal{O} \\
&= \mathfrak{a}
\end{aligned}$$

The other inclusion is obvious so equality follows. For claim 2.2, if $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal prime to f, then:

$$\begin{aligned}
\mathfrak{a} = \mathfrak{a}\mathcal{O} &= \mathfrak{a}\,(\mathfrak{a} \cap \mathcal{O} + f\mathcal{O}) \\
&\subset (\mathfrak{a} \cap \mathcal{O})\,\mathcal{O}_K + f\mathfrak{a} \\
&\subset (\mathfrak{a} \cap \mathcal{O})\,\mathcal{O}_K + (\mathfrak{a} \cap \mathcal{O})\,\mathcal{O}_K
\end{aligned}$$

since $f\mathfrak{a} \subset f\mathcal{O}_K \subset \mathcal{O}$ and $f\mathfrak{a} \subset \mathfrak{a} \subset \mathcal{O}_K$ also. The other inclusion is again obvious, so equality follows. In particular, these two claims and part 1. give the norm statement in part 2. This also gives a bijection between $\mathcal{O}_K$-ideals and $\mathcal{O}$-ideals prime to f. This extends to an isomorphism $I_K(f) \cong I(\mathcal{O}, f)$ since the maps $\mathfrak{a} \longmapsto \mathfrak{a} \cap \mathcal{O}$ and $\mathfrak{a} \longmapsto \mathfrak{a}\mathcal{O}_K$ preserve multiplication.

□

Using this we can describe the group $C(\mathcal{O})$ purely in terms of the maximal order. To do this, we need to make one more definition - this time of a subgroup of $I_K(f)$.

Definition 14. Denote by $P_{K,\mathbf{Z}}(f)$ the subgroup of $I_K(f)$ generated by principal ideals $\alpha\mathcal{O}_K$ with $\alpha \in \mathcal{O}_K$ satisfying $\alpha \equiv a \pmod{f\mathcal{O}_K}$ for some integer a coprime to f.

Proposition 15. *Let $\mathcal{O}$ be an order of conductor f. Then there are isomorphisms*

$$C(\mathcal{O}) \cong I(\mathcal{O}, f)/P(\mathcal{O}, f) \cong I_K(f)/P_{K,\mathbf{Z}}(f)$$

Proof. The first isomorphism was proved in Proposition 11. By proposition 13, the map $\mathfrak{a} \longmapsto \mathfrak{a}\mathcal{O}_K$ induces an isomorphism $I(\mathcal{O}, f) \cong I_K(f)$ and under this isomorphism, $P(\mathcal{O}, f) \subset I(\mathcal{O}, f)$ maps to some subgroup $P \subset I_K(f)$. So we want to show that $P = P_{K,\mathbf{Z}}(f)$.
We first prove the following claim for $\alpha \in \mathcal{O}_K$:

$$\alpha \equiv a \pmod{f\mathcal{O}_K},\ a \in \mathbf{Z},\ gcd(a, f) = 1 \iff \alpha \in \mathcal{O},\ gcd(N(\alpha), f) = 1 \tag{2.3}$$

($\Longrightarrow$) If $\alpha \equiv a \pmod{f\mathcal{O}_K}$, then it follows that $N(\alpha) \equiv a^2 \pmod{f}$, so then $gcd(N(\alpha), f) = gcd\left(a^2, f\right) = 1$. Also, since $f\mathcal{O}_K \subset \mathcal{O}$, we have $\alpha \in \mathcal{O}$.
($\Longleftarrow$) Let $\alpha \in \mathcal{O} = [1, fw_K]$ have norm coprime to f. This means $\alpha \equiv a \pmod{f\mathcal{O}_K}$ for some $a \in \mathbf{Z}$. Since $gcd(N(\alpha), f) = 1$ and $N(\alpha) \equiv a^2 \pmod{f}$, we must have $gcd(a, f) = 1$.

Now, $P(\mathcal{O}, f)$ is generated by ideals $\alpha\mathcal{O}$ where $\alpha \in \mathcal{O}$ and $N(\alpha)$ is coprime to f, so P is generated by corresponding ideals $\alpha\mathcal{O}_K$ and by the claim this means $P = P_{K,\mathbf{Z}}(f)$. □

We need one last fact to prove the main theorem. This gives an expression for the number of units in a quotient of $\mathcal{O}_K$.

Proposition 16. *Let f be a positive integer. Then*

$$|\left(\mathcal{O}_K/f\mathcal{O}_K\right)^\times| = \Phi(f)\,\Phi_K(f) \tag{2.4}$$

$\Phi(f) = f\prod_{p|f}\left(1-\frac{1}{p}\right)$ *is the Euler Phi-function and* $\Phi_K(f) = f\prod_{p|f}\left(1-\left(\frac{d_K}{p}\right)\frac{1}{p}\right)$.

Proof. First we prove the following claim. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal. Then

$$|\left(\mathcal{O}_K/\mathfrak{p}^n\right)^\times| = N(\mathfrak{p})^n - N(\mathfrak{p})^{n-1} \tag{2.5}$$

Recall that the ideals of $\mathcal{O}_K/\mathfrak{p}^n$ are in $1-1$ correspondence with ideals I of $\mathcal{O}_K$ such that $\mathfrak{p}^n \subset I$. That is $I = \mathfrak{p}^k$ for $0 \leq k \leq n$ which gives $n+1$ ideals of $\mathcal{O}_K/\mathfrak{p}^n$:

$$\mathcal{O}_K/\mathfrak{p}^n,\ \mathfrak{p}/\mathfrak{p}^n,\ \ldots,\ \mathfrak{p}^{n-1}/\mathfrak{p}^n,\ 0$$

It is clear from this list that there is a unique maximal ideal, namely $\mathfrak{p}/\mathfrak{p}^n$. Since every non-unit of a non-zero ring lies in some maximal ideal, we have $[x] \in \mathcal{O}_K/\mathfrak{p}^n$ is a unit $\iff x \notin \mathfrak{p}$. This gives

$$|\left(\mathcal{O}_K/\mathfrak{p}^n\right)^\times| = |\,\mathcal{O}_K/\mathfrak{p}^n\,| - |\,\mathfrak{p}/\mathfrak{p}^n\,|$$

The first summand is simply $N(\mathfrak{p})^n$. To compute the second one, we use the Third Isomorphism Theorem:

$$|\,\mathfrak{p}/\mathfrak{p}^n\,| = \frac{|\,\mathcal{O}_K/\mathfrak{p}^n\,|}{|\,\mathcal{O}_K/\mathfrak{p}\,|} = \frac{N(\mathfrak{p})^n}{N(\mathfrak{p})} = N(\mathfrak{p})^{n-1}$$

which proves the claim.

Now let $\mathfrak{a} \subset \mathcal{O}_K$ be any ideal and consider its prime factorization $\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i^{n_i}$. By the Chinese Remainder Theorem we have

$$\mathcal{O}_K/\mathfrak{a} \cong \prod_{i=1}^r \left(\mathcal{O}_K/\mathfrak{p}_i^{n_i}\right)$$

Using this together with claim 2.5, we calculate

$$|\left(\mathcal{O}_K/\mathfrak{a}\right)^\times| = \prod_{i=1}^r |\,\mathcal{O}_K/\mathfrak{p}_i^{n_i}\,| = \prod_{i=1}^r N(\mathfrak{p}_i)^{n_i}\left(1-\frac{1}{N(\mathfrak{p}_i)}\right) = N(\mathfrak{a})\prod_{\mathfrak{p}|\mathfrak{a}}\left(1-\frac{1}{N(\mathfrak{p})}\right) \tag{2.6}$$

Now consider ideals of the form $\mathfrak{a} = p\mathcal{O}_K$ for a rational prime p. We want to rewrite formula 2.6 with these ideals. There are three cases:

(1) p splits so that $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 \neq \mathfrak{p}_2$ and $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$ so that $N(p\mathcal{O}_K) = p^2$ and

$$\prod_{\mathfrak{p}|p\mathcal{O}_K}\left(1-\frac{1}{N(\mathfrak{p})}\right) = \left(1-\frac{1}{p}\right)^2 = \left(1-\frac{1}{p}\right)\left(1-\frac{1}{p}\right)$$

(2) p is inert so that $p\mathcal{O}_K = \mathfrak{p}$ with $N(\mathfrak{p}) = p^2$ and

$$\prod_{\mathfrak{p}|p\mathcal{O}_K} \left(1 - \frac{1}{N(\mathfrak{p})}\right) = 1 - \frac{1}{p^2} = \left(1 - \frac{1}{p}\right)\left(1 + \frac{1}{p}\right)$$

(3) p is ramified so that $p\mathcal{O}_K = \mathfrak{p}^2$ with $N(\mathfrak{p}) = p$ so that again $N(p\mathcal{O}_K) = p^2$ and

$$\prod_{\mathfrak{p}|p\mathcal{O}_K} \left(1 - \frac{1}{N(\mathfrak{p})}\right) = \left(1 - \frac{1}{p}\right)$$

We can summarize the three cases in one single expression:

$$\prod_{\mathfrak{p}|p\mathcal{O}_K} \left(1 - \frac{1}{N(\mathfrak{p})}\right) = \left(1 - \frac{1}{p}\right)\left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right)$$

where $\left(\frac{d_K}{p}\right)$ is the Legendre symbol (Kronecker symbol for $p = 2$) so that it is equal to $+1$, -1, 0 in the cases $1. - 3.$ respectively [Cox89, p. 104].
Putting this all together, for a positive integer f, we have shown that

$$|\left(\mathcal{O}_K/f\mathcal{O}_K\right)^\times| = f^2 \prod \left(1 - \frac{1}{p}\right)\left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right) = \Phi(f)\,\Phi_K(f)$$

□

Finally, we come to the main theorem:

Theorem 17. [Cox89, p. 146]
Let $\mathcal{O}$ be the order of conductor f in an imaginary quadratic field K. Then

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)\, f}{\left[\mathcal{O}_K^\times : \mathcal{O}^\times\right]} \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right) \tag{2.7}$$

Furthermore, $h(\mathcal{O})$ is always an integer multiple of $h(\mathcal{O}_K)$.

Proof. We have proved so far that

$$\begin{aligned} h(\mathcal{O}) &= |\, C(\mathcal{O}) \,| = |\, I_K(f)/P_{K,\mathbf{Z}}(f) \,| \\ h(\mathcal{O}_K) &= |\, C(\mathcal{O}_K) \,| = |\, I_K/P_K \,| \end{aligned}$$

Also, $I_K(f) \subset I_K$ and $P_{K,\mathbf{Z}} \subset I_K(f) \cap P_K$ which induces a homomorphism $I_K(f)/P_{K,\mathbf{Z}}(f) \longrightarrow I_K/P_K$ with kernel $\left(I_K(f) \cap P_K\right)/P_{K,\mathbf{Z}}(f)$. Thus, the following sequence is exact:

$$0 \longrightarrow \left(I_K(f) \cap P_K\right)/P_{K,\mathbf{Z}}(f) \longrightarrow I_K(f)/P_{K,\mathbf{Z}}(f) \longrightarrow I_K/P_K \tag{2.8}$$

Also, $I_K(f)/P_{K,\mathbf{Z}}(f) \cong C(\mathcal{O})$ and $I_K/P_K \cong C(\mathcal{O}_K)$. By Proposition 8, every class in $C(\mathcal{O}_K)$ containts an $\mathcal{O}_K$-ideal with norm coprime to f. This makes the map $C(\mathcal{O}) \longrightarrow C(\mathcal{O}_K)$ surjective which shows that $h(\mathcal{O}_K) \mid h(\mathcal{O})$. In particular, using the sequence 2.8, we get

$$\frac{h(\mathcal{O})}{h(\mathcal{O}_K)} = |\left(I_K(f) \cap P_K\right)/P_{K,\mathbf{Z}}(f)\,|$$

We will calculate the order on the RHS relating this quotient to $\left(\mathcal{O}_K/f\mathcal{O}_K\right)^\times$.

Let $[\alpha] \in \left(\mathcal{O}_K/f\mathcal{O}_K\right)^\times$, then we have $\alpha\mathcal{O}_K + f\mathcal{O}_K = \mathcal{O}_K$, so $\alpha\mathcal{O}_K$ is prime to f, so lies in $I_K(f) \cap P_K$. Also, if $\alpha \equiv \beta \pmod{f\mathcal{O}_K}$, we can find $u \in \mathcal{O}$ so

that $u\alpha \equiv u\beta \pmod{f\mathcal{O}_K}$. So both $u\alpha\mathcal{O}_K$ and $u\beta\mathcal{O}_K$ lie in $P_{K,\mathbf{Z}}(f)$ and since $\alpha\mathcal{O}_K \cdot u\beta\mathcal{O}_K = \beta\mathcal{O}_K \cdot u\alpha\mathcal{O}_K$, the ideals $\alpha\mathcal{O}_K$ and $\beta\mathcal{O}_K$ lie in the same class in $(I_K(f) \cap P_K)/P_{K,\mathbf{Z}}(f)$. This means that the map

$$\begin{array}{rccl} \phi\colon & (\mathcal{O}_K/f\mathcal{O}_K)^\times & \longrightarrow & (I_K(f) \cap P_K)/P_{K,\mathbf{Z}}(f) \\ & [\alpha] & \longmapsto & [\alpha\mathcal{O}_K] \end{array}$$

is a well-defined homomorphism.

ϕ is surjective. Let $\alpha\mathcal{O}_K \in I_K(f) \cap P_K$. Then $\alpha\mathcal{O}_K = \mathfrak{a}\mathfrak{b}^{-1}$ for $\mathfrak{a}, \mathfrak{b}$ $\mathcal{O}_K$-ideals prime to f. Let $m = N(\mathfrak{b})$ and in Proposition 11 we saw that $\overline{\mathfrak{b}} = m\mathfrak{b}^{-1}$ so that $m\alpha\mathcal{O}_K = \mathfrak{a}\overline{\mathfrak{b}}$ giving $m\alpha \in \mathcal{O}_K$ and so $m\alpha\mathcal{O}_K$ is also an $\mathcal{O}_K$-ideal prime to f. Note that $m\mathcal{O}_K \in P_{K,\mathbf{Z}}(f)$, thus $[\alpha\mathcal{O}_K] = [m\alpha\mathcal{O}_K] = \phi([m\alpha])$ proving surjectivity.

Next we find the kernel of ϕ. We define the two maps

$$\begin{array}{rccl} d\colon & \{\pm 1\} & \longrightarrow & (\mathbf{Z}/f\mathbf{Z})^\times \times \mathcal{O}_K^\times \\ & \pm 1 & \longmapsto & ([\pm 1], \pm 1) \end{array} \tag{2.9}$$

$$\begin{array}{rccl} \psi\colon & (\mathbf{Z}/f\mathbf{Z})^\times \times \mathcal{O}_K^\times & \longrightarrow & (\mathcal{O}_K/f\mathcal{O}_K)^\times \\ & ([n], \epsilon) & \longmapsto & \left[n\epsilon^{-1}\right] \end{array} \tag{2.10}$$

We will use these to show that the following sequence is exact:

$$1 \longrightarrow \{\pm 1\} \xrightarrow{d} (\mathbf{Z}/f\mathbf{Z})^\times \times \mathcal{O}_K^\times \xrightarrow{\psi} (\mathcal{O}_K/f\mathcal{O}_K)^\times \xrightarrow{\phi} (I_K(f) \cap P_K)/P_{K,\mathbf{Z}}(f) \longrightarrow 1 \tag{2.11}$$

Now if n is an integer coprime to f and $\epsilon \in \mathcal{O}_K$, then $\psi([n], \epsilon) = n\epsilon^{-1} \pmod{f\mathcal{O}_K}$ so

$$\begin{array}{rcl} ([n], \epsilon) \in ker(\psi) & \Longleftrightarrow & n\epsilon^{-1} \equiv 1 \pmod{f\mathcal{O}_K} \\ & \Longleftrightarrow & \epsilon \equiv n \pmod{f\mathcal{O}_K} \\ & \Longleftrightarrow & \epsilon = \pm 1 \\ & \Longleftrightarrow & n = \pm 1 \pmod{f} \end{array}$$

Thus $ker(\psi) = ([\pm 1], \pm 1) = im(d)$.

By the definition of $P_{K,\mathbf{Z}}$, we immediately get $im(\psi) \subset ker(\phi)$. To show the other inclusion, let $[\alpha] \in ker(\phi)$. Thus $\alpha\mathcal{O}_K \in P_{K,\mathbf{Z}}$ which means $\alpha\mathcal{O}_K = \beta\mathcal{O}_K \cdot \gamma^{-1}\mathcal{O}_K$ for some β, γ satisfying $\beta \equiv b \pmod{f\mathcal{O}_K}$ and $\gamma \equiv c \pmod{f\mathcal{O}_K}$ with b, c coprime to f. This means $[b], [c] \in (\mathbf{Z}/f\mathbf{Z})^\times$. Now, $\alpha = \beta\gamma^{-1}\epsilon$ for some $\epsilon \in \mathcal{O}_K^\times$. Then

$$\begin{array}{rcl} \psi([b], 1) & = & b \pmod{f\mathcal{O}_K} = \beta \pmod{f\mathcal{O}_K} \\ \psi([c], \epsilon) & = & c\epsilon^{-1} \pmod{f\mathcal{O}_K} = \gamma\epsilon^{-1} \pmod{f\mathcal{O}_K} \\ \psi\left([b][c]^{-1}, \epsilon\right) & = & \beta\gamma^{-1}\epsilon \pmod{f\mathcal{O}_K} = [\alpha] \end{array}$$

We have shown that $\left([b][c]^{-1}, \epsilon^{-1}\right) \in (\mathbf{Z}/f\mathbf{Z})^\times \times \mathcal{O}_K^\times$ maps to $[\alpha] \in (\mathcal{O}_K/f\mathcal{O}_K)^\times$ proving the other inclusion.

Thus, by the exactness of 2.11, we have

$$|(I_K(f) \cap P_K)/P_{K,\mathbf{Z}}(f)| = \frac{|(\mathcal{O}_K/f\mathcal{O}_K)^\times || \{\pm 1\}|}{|(\mathbf{Z}/f\mathbf{Z})^\times \times \mathcal{O}_K^\times|}$$

We calculated in Proposition 16 that $|\left(\mathcal{O}_K/f\mathcal{O}_K\right)^\times| = \Phi(f)\,\Phi_K(f)$ and we also know that $\left(\mathbf{Z}/f\mathbf{Z}\right)^\times = \Phi(f)$. Thus

$$\frac{h(\mathcal{O})}{h(\mathcal{O}_K)} = |\left(I_K(f) \cap P_K\right)/P_{K,\mathbf{Z}}(f)| = \frac{\Phi_K(f)}{\left[\mathcal{O}_K^\times : \mathcal{O}^\times\right]}$$

proving the theorem. □

In the following section we use this formula to explicitly calculate all discriminants with class numbers $h = 1, 2, 3$. It is worth mentioning that there are analytic proofs of this theorem, using the analytic class number formula (See [Coh96, p. 233] for an outline). In addition, one can derive essentially the same formula for the number of elements in $C(\mathcal{O})$ for general number fields (not just imaginary quadratic) using canonical exact sequences, but calculating the orders of $\left(\mathcal{O}_K/f\mathcal{O}_K\right)^\times$ and $\left(\mathcal{O}/f\mathcal{O}\right)^\times$ is harder (See [Neu99, §12]).

3. Example Calculations.

We will make use the following well-known result about units in quadratic imaginary fields:

Proposition 18. [ST01, p. 77]
Let K be an imaginary quadratic field with discriminant d_K and the ring of integers $\mathcal{O}_K$. Then the group of units $\mathcal{O}_K^\times$ is as follows:

- $\mathcal{O}_K^\times = \left\{\pm 1, \pm\omega, \pm\omega^2\right\}$ for $d_K = -3$ and $\omega = e^{\frac{2\pi i}{3}}$
- $\mathcal{O}_K^\times = \{\pm 1, \pm i\}$ for $d_K = -4$
- $\mathcal{O}_K^\times = \{\pm 1\}$ for all other $d_K < 0$

Some observations:
If $\left|\mathcal{O}_K^\times\right| = 2$, then $\left[\mathcal{O}_K^\times : \mathcal{O}^\times\right] = 1$ since ± 1 are always units.
If $\left|\mathcal{O}_K^\times\right| = 4$, then $\left[\mathcal{O}_K^\times : \mathcal{O}^\times\right] = 2$ since $\pm i \notin [1, fi]$ for $f > 1$
If $\left|\mathcal{O}_K^\times\right| = 6$, then $\left[\mathcal{O}_K^\times : \mathcal{O}^\times\right] = 3$ since $\pm e^{\frac{2\pi i}{3}}, \pm e^{\frac{4\pi i}{3}} \notin \left[1, fe^{\frac{2\pi i}{3}}\right]$ for $f > 1$

Recall the integer valued function we first introduced in Proposition 16:

Definition 19. Define

$$\Phi_K(f) = f\prod_{p|f}\left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right) \tag{3.1}$$

So the problem of finding all orders of class number h reduces to solving

$$\Phi_K(f) = \frac{h(\mathcal{O})}{h(\mathcal{O}_K)}\left[\mathcal{O}_K^\times : \mathcal{O}^\times\right] \tag{3.2}$$

for (f, d_K) which uniquely determine the order $\mathcal{O}$ by its discriminant $D = f^2 d_K$.
In principle, if we wanted to find all orders of class number $h \leq 100$, we could solve $\Phi_K(f) = m$ for $m \leq 300$. But note that in the special cases where $\left[\mathcal{O}_K^\times : \mathcal{O}^\times\right] \neq 1$, we already know what d_K is and the job of finding f becomes easier.

We give a few useful properties of the function Φ_K.

Proposition 20. *Φ_K is multiplicative.*

Proof. Let $f = p_1^{e_1} \dots p_n^{e_n}$ be a prime decomposition of the conductor. Then

$$\begin{aligned}\Phi_K(f) &= f \prod_{p \mid f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right) \\ &= p_1^{e_1} \dots p_n^{e_n} \prod_{i=1}^{n} \left(1 - \left(\frac{d_K}{p_i}\right)\frac{1}{p_i}\right) \\ &= \prod_{i=1}^{n} p_i^{e_i} \left(1 - \left(\frac{d_K}{p_i}\right)\frac{1}{p_i}\right) \\ &= \Phi_K(p_i^{e_i})\end{aligned}$$

□

In particular, since $\Phi_K(p^e) = p^e\left(1 - \left(\frac{d_k}{p}\right)\frac{1}{p}\right) = p^{e-1}\left(p - \left(\frac{d_k}{p}\right)\right)$ we have the following properties:

$$\text{If } p^e \mid f, \text{ then } \begin{cases} p^{e-1} \mid \Phi(f) & \text{always} \\ p^e \mid \Phi_K(f) & \text{if } p \mid d \end{cases} \tag{3.3}$$

$$\text{If } p \mid f, \text{ then } p - \left(\frac{d_K}{p}\right) \mid \Phi_K(f) \tag{3.4}$$

Example 21. We find all orders of class number $h(\mathcal{O}) = 1$. Since $h(\mathcal{O}_K) \mid h(\mathcal{O})$ we immediately have $h(\mathcal{O}_K) = 1$. There are 9 maximal orders of class number 1 [Sta67] whose discriminants are:

$$-3, -4, -7, -8, -11, -19, -43, -67, -163 \tag{3.5}$$

If $\left[\mathcal{O}_K^\times : \mathcal{O}^\times\right] = 1$, need to solve $\Phi_K(f) = 1$. We consider a prime $p \mid f$.

Case 1: $\left(\frac{d_K}{p}\right) = 1 \implies (p-1) \mid 1 \implies p = 2 \implies d_K \equiv 1 \pmod 8 \implies d_K = -7$

Case 2: $\left(\frac{d_K}{p}\right) = -1 \implies (p+1) \mid 1$ is impossible

Case 3: $\left(\frac{d_K}{p}\right) = 0 \implies p \mid 1$ is impossible

So we have found one non-maximal order with $(f, d_K) = (2, -7)$ and discriminant $D = -28$.

If $\left[\mathcal{O}_K^\times : \mathcal{O}^\times\right] = 2$, need to solve $\Phi_K(f) = 2$ with $d_K = -4$.

Case 1: $\left(\frac{d_K}{p}\right) = 1 \implies (p-1) \mid 2 \implies p = 2$ or $p = 3$

If $p = 2$, then $\left(\frac{-4}{2}\right) = 0$ is false.

If $p = 3$, then $\left(\frac{-4}{3}\right) = -1$ is false.

Case 2: $\left(\frac{d_K}{p}\right) = -1 \implies (p+1) \mid 2$ is impossible

Case 3: $\left(\frac{d_K}{p}\right) = 0 \implies p \mid 2 \implies p = 2 \implies d_K = 0 \pmod 2$ is true

So we have an order with $(f, d_K) = (2, -4)$ and discriminant $D = -16$.

Lastly, if $\left[\mathcal{O}_K^\times : \mathcal{O}^\times\right] = 3$, need to solve $\Phi_K(f) = 3$ with $d_K = -3$.

Case 1: $\left(\frac{d_K}{p}\right) = 1 \Longrightarrow (p-1) \mid 3 \Longrightarrow p = 2 \Longrightarrow d_K \equiv 1 \pmod 8$ is false

Case 2: $\left(\frac{d_K}{p}\right) = -1 \Longrightarrow (p+1) \mid 3 \Longrightarrow p = 2 \Longrightarrow d_K \equiv 5 \pmod 8$ is true

Case 3: $\left(\frac{d_K}{p}\right) = 0 \Longrightarrow p \mid 3 \Longrightarrow p = 3 \Longrightarrow d_K \equiv 0 \pmod 3$ is true

So we have found another two orders with $(f, d_K) = (2, -3), (3, -3)$ and discriminants $D = -12, -27$ respectively.

This means that there are 13 orders of class number 1 of which 4 are non-maximal.

Example 22. To find the orders of class number $h(\mathcal{O}) = 2$ we must have $h(\mathcal{O}_K) = 1$ or $h(\mathcal{O}_K) = 2$. The 9 maximal orders of class number 1 are listed in 3.5. There are 18 maximal orders of class number 2 [Bak71] with discriminants as follows:

$$-15, -20, -24, -35, -40, -51, -52, -88, -91, -115, -123, \\ -148, -187, -232, -235, -267, -403, -427 \quad (3.6)$$

So if $h(\mathcal{O}_K) = 1$, then $\Phi_K(f) = 2\ (4, 6)$ depending on the size of the unit group. If $h(\mathcal{O}_K) = 2$, then $\Phi_K(f) = 1$ as the unit group has always size 2. We start with the latter case.

If $h(\mathcal{O}_K) = 2$, need to solve $\Phi_K(f) = 1$. Consider a prime $p \mid f$. We saw in Example 21 that the only solution is $f = 2$ with $d_K \equiv 1 \pmod 8$ which gives $d_K = -15$ and so an order with discriminant $D = -60$.

Now suppose $h(\mathcal{O}_K) = 1$ and the unit group has size 2. Need to solve $\Phi_K(f) = 2$.

Case 1: $\left(\frac{d_K}{p}\right) = 1 \Longrightarrow (p-1) \mid 2 \Longrightarrow p = 2$ or $p = 3$

If $p = 2$, then $\left(\frac{d_K}{2}\right) = 1 \Longrightarrow d_K \equiv 1 \pmod 8 \Longrightarrow d_K = -7$

$f = 2$, however, is impossible as $\Phi_K(2) = 1 \neq 2$.

$f = 4$ is also possible since $2^{2-1} = 2 \mid \Phi_K(f)$ by Property 3.3. Then indeed $\Phi_K(4) = 2$ and we have found an order with discriminant $D = -7 \cdot 4^2 = -112$.

If $p = 3$, then $\left(\frac{d_K}{3}\right) = 1 \Longrightarrow d_K \equiv 1 \pmod 3 \Longrightarrow d_K = -8, -11$. Indeed $\Phi_K(3) = 2$ which gives two orders with discriminants $D = -8 \cdot 3^2 = -72$ and $D = -11 \cdot 3^2 = -99$. Note that f cannot contain a higher power of 3 since $3^{2-1} = 3 \nmid \Phi_K(f)$.

We also have the possibility $f = 2 \cdot 3$. Then $d_K \equiv 1 \pmod 8, 1 \pmod 3 \Longrightarrow d_K \equiv 1 \pmod{24}$ which is not satisfied by any of the 9 fundamental discriminants.

Finally, $f = 2^2 \cdot 3$ is impossible as $\Phi_K(12) = 4 \neq 2$.

Case 2: $\left(\frac{d_K}{p}\right) = -1 \Longrightarrow (p+1) \mid 2$ is impossible

Case 3: $\left(\frac{d_K}{p}\right) = 0 \Longrightarrow p \mid 2 \Longrightarrow p = 2 \Longrightarrow d_K \equiv 0 \pmod 2 \Longrightarrow d_K = -8$. Indeed $\Phi_K(2) = 2$ which gives an order with discriminant $D = -8 \cdot 2^2 = -32$. By property 3.3, f cannot containt any higher power of 2.

Now suppose the unit group has size 4, i.e $d_K = -4$ and we want to solve $\Phi_K(f) = 4$.

Case 1: $\left(\frac{-4}{p}\right) = 1 \Longrightarrow (p-1) \mid 4 \Longrightarrow p = 2, 5$ but note that $\left(\frac{-4}{2}\right) = 0$ which is a contradiction. So $f = 5$ is the only possibility.

Case 2: $\left(\frac{-4}{p}\right) = -1 \Longrightarrow (p+1) \mid 4 \Longrightarrow p = 3$ and no higher power of 3 is possible.

Case 3: $\left(\frac{-4}{p}\right) = 0 \Longrightarrow p \mid 4 \Longrightarrow p = 2$ and so $f = 2, 2^2$ are possible.

So $\Phi_K(2) = 2 \neq 4$. $\Phi_K(3) = 4$ which gives an order with discriminant $D = -4 \cdot 3^2 = -36$. $\Phi_K(4) = 4$ which gives an order with discriminant $D = -4 \cdot 4^2 = -64$. Finally, $\Phi_K(5) = 4$ which gives an order with discriminant $D = -4 \cdot 5^2 = -100$. Note that we do not need to consider any other products f of the primes $2, 3, 5$ since $\Phi_K$is multiplicative so any such products will ensure $\Phi_K(f) > 4$.

Finally, suposse the unit group has size 6, i.e. $d_K = -3$ and we want to solve $\Phi_K(f) = 6$.

Case 1: $\left(\frac{-3}{p}\right) = 1 \Longrightarrow (p-1) \mid 6 \Longrightarrow p = 2, 3, 7$ but note that $\left(\frac{-3}{2}\right) = -1$ and $\left(\frac{-3}{3}\right) = 0$ which are contradictions. So $f = 7$ is the only possibility.

Case 2: $\left(\frac{-3}{p}\right) = -1 \Longrightarrow (p+1) \mid 6 \Longrightarrow p = 2, 5$ and $f = 2^2$ is also possible.

Case 3: $\left(\frac{-3}{p}\right) = 0 \Longrightarrow p \mid 6 \Longrightarrow p = 2, 3$ but again $\left(\frac{-3}{2}\right) = -1$ and so $f = 3$ is the only possibility.

We have $\Phi_K(7) = 6$ which gives an order of discriminant $D = -3 \cdot 7^2 = -147$.

$\Phi_K(2) = 3 \neq 6$.

$\Phi_K(4) = 6$ which gives an order of discriminant $D = -3 \cdot 4^2 = -48$.

$\Phi_K(5) = 6$ which gives and order of discriminant $D = -3 \cdot 5^2 = -75$.

$\Phi_K(3) = 3 \neq 6$.

Since Φ_K is multiplicative, we are done since any other product f of the primes $2, 3, 5$ will have $\Phi_K(f) > 6$.

To summarize, we have found 11 non-maximal ideals of class number 2 and there are no others. As a list (f, d_K):

$(2, -8), (2, -15), (3, -4), (3, -8), (3, -11), (4, -3), (4, -4), (4, -7), (5, -3), (5, -4), (7, -3)$

In particular, this calculation corrects an error in [**?**, p. 408] which gives an incomplete list of orders of class number 2, ommiting the order $(3, -8)$.

Notation: Write $p^e \| n$ to mean $p^e \mid n$ but $p^{e+1} \nmid n$.

The equation $\Phi_K(f) = m$ for m odd is particularly easy to solve since there are not a lot of options for the prime divisors of f.

If $\left(\frac{d_K}{p}\right) = 1$, then $(p-1) \mid m$ and so $p = 2 \| f$ if $d_K \equiv 1 \pmod 8$.

If $\left(\frac{d_K}{p}\right) = -1$, then $(p+1) \mid m$ and so $p = 2 \| f$ if $3 \mid m$ and $d_K \equiv 5 \pmod 8$.

If $\left(\frac{d_K}{p}\right) = 0$, then $p \mid m$ and so if $p^e \| m$ and $p \mid d_K$ then $p^d \| f$ for all $d \leq e$.

Example 23. We use this to find all orders of class number $h = 3$. There are 16 maximal orders of class number 3 [Oes85] with discriminants:

$$-23, -31, -59, -83, -107, -139, -211, -283, -307, -331, \\ -379, -499, -547, -643, -883, -907 \quad (3.7)$$

If $h(\mathcal{O}_K) = 3$, need to solve $\Phi_K(f) = 1$ and we know from Examples 21 and 22 that this gives $f = 2$ with $d_K \equiv 1 \pmod 8$. This corresponds to two orders with discriminants $D = -23 \cdot 2^2 = -92$ and $D = -31 \cdot 2^2 = -124$.

Next, if $h(\mathcal{O}_K) = 1$ and the unit group has size 2, this corresponds to $\Phi_K(f) = 3$. From the discussion above, $2 \| f$ iff $d_K = 1 \pmod 8$ or $d_K = 1 \pmod 5$ and $3 \| f$ iff $3 \mid d_K$. From 3.5, there are no d_K with unit group of size 2 and $3 \mid d_K$.

Also, if $d_K \equiv 1 \pmod 8$, then $\Phi_K(2) = 1 \neq 3$. On the other hand, if $d_K \equiv 5 \pmod 8$, then $\Phi_K(2) = 3$ as required. There are 5 such maximal orders which give rise to 5 non-maximal orders of conductor 2:

$(2, -11), (2, -19), (2, -43), (2, -67), (2, -163)$

Now suppose the unit group has size 4, i.e. $d_K = -4$ so we want to solve $\Phi_K(f) = 6$.\

Case 1: $\left(\frac{-4}{p}\right) = 1 \Longrightarrow (p-1) \mid 6 \Longrightarrow p = 2, 3, 7$ but none of these have $\left(\frac{-4}{p}\right) = 1$.

Case 2: $\left(\frac{-4}{p}\right) = -1 \Longrightarrow (p+1) \mid 6 \Longrightarrow p = 2, 5$ but none of these have $\left(\frac{-4}{p}\right) = -1$

Case 3: $\left(\frac{-4}{p}\right) = 0 \Longrightarrow p \mid 6 \Longrightarrow p = 2, 3$ but $\left(\frac{-4}{3}\right) = -1$ so only $f = 2, 2^2$ are possible.

However $\Phi_K(2) = 2$ and $\Phi_K(4) = 4$ so we do not get any new orders.

Finaly suppose the unit group has size 6, i.e. $d_K = -3$ so we want to solve $\Phi_K(f) = 9$.

From the discussion above for m odd, f has possible factors $2, 3, 9$ but no higher powers of either $2, 3$.

$\Phi_K(2) = 3 \neq 9$ and $\Phi_K(3) = 3 \neq 9$ but together they give $\Phi_K(6) = 9$, an order $(6, -3)$.

Also $\Phi_K(9) = 9$ which gives an order $(9, -3)$.

We have found 9 non-maximal orders of class number 3 and there are no others:

$(2, -11), (2, -19), (2, -23), (2, -31), (2, -43), (2, -67), (2, -163), (6, -3), (9, -3)$

These examples demonstrate that in principle it is possible to devise an algorithm that solves these Diophantine equations. It would be easy in the case $\Phi_K(f) = m$ where m is odd as already noted, but in the case m is even, more possibilities for the prime divisors of f need to be considered. Then several results for different m need to be combined in calculating the discriminants of any one order which makes this less straightforward. In the following section we describe a different algorithm

based on the idea of comparing $\Phi_K(f)$ with the Euler Phi function $\Phi(f)$ together with a lower bound to turn this into an exaustive search problem.

4. An Algorithm

In this section we look at the problem of finding all orders with a given class number from a different perspective which uses the class number formula derived in Section 2 as an upper bound for an exhaustive search. This algorithm was first suggested by Andrew V. Sutherland at MIT and later implemented in Sage by William Stein at the University of Washington. We give a description of the algorithm and the output in a condensed format listing the number of orders with given class number h and the maximum discriminant in absolute value for each h up to 100.

Recall the function $\Phi_K(f) = f\prod_{p|f}\left(1-\left(\frac{d_K}{p}\right)\frac{1}{p}\right)$ we defined earlier. This bears remarkable similarity to the Euler Phi function $\Phi(f) = f\prod_{p|f}\left(1-\frac{1}{p}\right)$. In fact, Proposition 16 and Theorem 17 show that these two functions are intimitely linked in proving the class number formula. Now let $(f,\, d_K)$ represent the order $\mathcal{O}$ with conductor f and discriminant $D = f^2 d_K$ where d_K is the fundamental discriminant of the maximal order $\mathcal{O}_K$ in which $\mathcal{O}$ lies. Also, let $w = \left[\mathcal{O}_K^\times : \mathcal{O}^\times\right]$. Changing notation so that $h(\mathcal{O}_K) = h(d_K)$ and $h(\mathcal{O}) = h\left(f^2 d_K\right)$ we have

$$h\left(f^2 d_K\right) = \frac{h(d_K)}{w}\Phi_K(f) \geq \frac{h(d_K)}{w}\Phi(f) > \frac{h(d_K)}{w}l(f) \tag{4.1}$$

where $l(f)$ is a lower bound for the Euler Phi function [Cla, p. 6] given by

$$l(f) = \begin{cases} \frac{f}{\left(1.79\log(\log(f)) + \frac{3}{\log(\log(f))}\right)} & \text{for } f \geq 2 \\ 0 & \text{for } f = 1 \end{cases}$$

Note that $l(f)$ is an increasing function of f

In addition to this we use the Watkins's table of fundamental discriminants [Wat03, p. 936] which gives a list with 100 entries $(h,\, d_K max,\, n)$ where h is the class number $h = 1, \ldots, 100$, $d_K max$ is the maximum fundamental discriminant (in absolute value) and n is the number of the fundamental discriminants of class number h.

The strategy is now clear. Given the maximum desired class number $hmax$ (in our case $hmax = 100$) we will use a double loop: the outer loop will run over the fundamental discriminants d_K while the inner loop will run over conductors f as long as $\frac{h(d_K)}{w}l(f) \leq hmax$ is satisfied. We will create a dictionary with keys h the class numbers and entries a list of $(f,\, d_K)$ representing orders of that class number. Here is the full description:

(1) Find the biggest fundamental discriminant (in absolute value) $d_K max$ in Watkins's table for h in the range $(1,\, hmax)$.
(2) Outer loop over fundamental discriminants d_K in the range $(-d_K max,\, -2)$, for each calculate $h(d_K)$.
(3) Inner loop over conductors f starting from $f = 1$ until $\frac{h(d_K)}{w}l(f) \leq hmax$ is satisfied.

(4) For each $(f,\, d_K)$ in the inner loop calculate $h = h\left(f^2 d_K\right)$.
(5) Test if $h \leq hmax$; if so, append $(f,\, d_K)$ to our dictionary with the key h.

The correctness and the termination of the algorithm follow from step 3. We know the bound on the fundamental discriminant $d_K max$ from the Watkins's table but the conductor f at first sight can be arbitrarily big. However, by the inequalities in 4.1 we only need to check f while $\frac{h(d_K)}{w} l\,(f) \leq hmax$ since otherwise $h = h\left(f^2 d_K\right) > hmax$ is out ouf our desired bound $hmax$. Since $l\,(f)$ is an increasing function of f, this means that the algorihtm will terminate in a finite number of steps.

The algorithm was run by John Cremona at the University of Warwick taking 19.5 hours to return a complete dictionary of orders with class number up to 100. There are a number of improvements to make the algorithm more efficient, however it is important to note that this was essentially a one-off calculation the results of which have been saved. Here we present a Watkins-style table of the total number of orders (maximal and non-maximal) and the biggest discriminant (in absolute value) for each class number $h \leq 100$:

h	#	large	h	#	large	h	#	large	h	#	large
1	13	163	26	227	103027	51	217	546067	76	1384	1086187
2	29	427	27	136	103387	52	1006	457867	77	236	1242763
3	25	907	28	623	126043	53	130	425107	78	925	1004347
4	84	1555	29	94	166147	54	812	532123	79	200	1333963
5	29	2683	30	473	137083	55	177	452083	80	3856	1165483
6	101	4075	31	83	133387	56	1812	494323	81	339	1030723
7	38	5923	32	1231	164803	57	237	615883	82	487	1446547
8	208	7987	33	158	222643	58	361	586987	83	174	1074907
9	55	10627	34	262	189883	59	144	474307	84	2998	1225387
10	123	13843	35	111	210907	60	2361	662803	85	246	1285747
11	46	15667	36	1306	217627	61	149	606643	86	555	1534723
12	379	19723	37	96	158923	62	386	647707	87	313	1261747
13	43	20563	38	284	289963	63	311	991027	88	2771	1265587
14	134	30067	39	162	253507	64	2919	693067	89	206	1429387
15	95	34483	40	1418	274003	65	192	703123	90	1516	1548523
16	531	35275	41	125	296587	66	861	958483	91	249	1391083
17	50	37123	42	596	301387	67	145	652723	92	1591	1452067
18	291	48427	43	123	300787	68	1228	819163	93	354	1475203
19	59	38707	44	911	319867	69	292	888427	94	600	1587763
20	502	58843	45	231	308323	70	704	821683	95	273	1659067
21	118	61483	46	330	462883	71	176	909547	96	7276	1684027
22	184	85507	47	117	375523	72	4059	947923	97	208	1842523
23	78	90787	48	2895	335203	73	137	886867	98	710	2383747
24	1042	111763	49	146	393187	74	474	951043	99	396	1480627
25	101	93307	50	445	389467	75	353	916507	100	2311	1856563

Using this table anyone who wishes to find all orders of a given class number h only needs to check all discriminants up to the largest one given in the table and the result can be double checked against the number of orders also given. If only fundamental discriminants are of concern, refer again to [Wat03, p. 936] for the

number of these.

There is a striking similarity between the third column of this table and the corresponding one in Watkins's table (listing the maximum *fundamental* discriminant in absolute value). In fact, these columns are identical except for 10 cases which are highlighted in the table (9 on which are curiously multiples of 163) . On closer scrutiny, it turns out that these 10 discriminants ar the *only* ones that are bigger than the fundamental bound given by Watkins. This means if Watkins had included non-fundamental discriminants in his calculations, he would have missed only 10 (!) discriminants which is a miniscule error taking into account the number of new discriminants we get when extending to non-fundamental ones. It is tempting to conjecture that for any clas number, there is at most one non-fundamental discriminant bigger (in absolute value) than the biggest fundamental one, but more data should be gathered. At present it seems out of reach unless people look into Watkins's method and optimize it to solve the problem for $h > 100$ in reasonable timeframes.

This concludes the main body of the project. We have found an answer to the problem we set out to solve with some collaboration. The next and final section is a bonus section which sets out to motivate the problem by its connection with complex multiplication of elliptic curves.

5. An Application to Complex Multiplication

In this section we will give a very brief survey of the Klein j-invariants which are important in the theory of complex multiplication for elliptic curves but also have connections with class field theory and have some very nice properties in connection with discriminants of given class number that we found in earlier sections. This should be considered as an informal introduction to the topic. For the initiated reader, a good reference is [Cox89, Ch. 3].

The j-invariant is defined as an invarinat of a *lattice* in $\mathbf{C}$:

Definition. [Cox89, p. 200] A *lattice* is an additive subgroup $L \subset \mathbf{C}$ generated by two complex numbers ω_1, ω_2 which ar linearly independent over $\mathbf{R}$. We write $L = [\omega_1, \omega_2]$.

We will also need *elliptic functions* defined for these lattices:

Definition. [Cox89, p. 200] An *elliptic functions* for a latice L is a function $f(z)$ defined on $\mathbf{C}$ (except for isolated singularities) such that

(1) $f(z)$ is meromorphic on $\mathbf{C}$.
(2) $f(z+\omega) = f(z)$ for all $\omega \in L$.

An important elliptic function that is used in defining j-invarinats is the Weierstrass $\wp$-function defined for a lattice L and $z \notin L$:

$$\wp(z; L) = \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right) \tag{5.1}$$

We will need two constants related this function to define j-invariants, so let

$$\begin{aligned} g_2(L) &= 60 \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega}^4 \\ g_3(L) &= 140 \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^6} \end{aligned}$$

In general, elliptic functions depend on the choice of lattice, but there exists a conveniet equivalence relation on lattices which means that equivalent lattices have basically the same elliptic functions:

Definition. [Cox89, p. 205] Two lattices L, L' are called *homothetic* if there exists $\lambda \in \mathbf{C} \setminus \{0\}$ so that $L' = \lambda L$.

The j-invariants first appear when classifying lattices up to homothety. Setting $\Delta(L) = g_2(L)^3 - 27 g_3(L)^2$ we can check this is non-zero for any lattice, so that we define:

Definition. [Cox89, p. 206] The j-invariant of a lattice L is the complex number

$$j(L) = 1728 \frac{g_2(L)^3}{\Delta(L)}$$

The following theorem makes it clear why these j-invariants matter:

Theorem. [Cox89, p. 206] *If L, L' are lattices in $\mathbf{C}$, then $j(L) = j(L') \iff L$ and L' are homothetic.*

What has this got to do with orders in imaginary quadratic fields? We know from our earlier results that if $\mathfrak{a} \subset \mathcal{O}$ is a proper fractional ideal of an order $\mathcal{O} \subset K$, then $\mathfrak{a} = [\alpha, \beta]$ for some $\alpha, \beta \in K$. Since K is a subset of $\mathbf{C}$ and it is an imaginary quadratic field, α and β are linearly independent over $\mathbf{R}$. So the ideal $\mathfrak{a} = [\alpha, \beta]$ gives a natural lattice in $\mathbf{C}$ so that $j(\mathfrak{a})$ is defined. We will see some remarkable properties of these numbers soon.

Time doesn't permit to discuss the theory of complex multiplication in full detail, but the idea is to ask the question for what complex numbers $\alpha \in \mathbf{C}$ we have that $\wp(\alpha z)$ is a rational function in $\wp(z)$? The answer [Cox89, p. 209] is surprising indeed: first of all, *any* elliptic function $f(z)$ is rational in $\wp(z)$ and $\wp'(z)$, and then if $f(\alpha z)$ is rational in $f(z)$ for some $\alpha \in \mathbf{C} \setminus \mathbf{R}$, it follows that this is true for elements of an entire *order* $\mathcal{O}$ in some imaginary quadratic field. This phenomenon is called *complex multiplication.*

Complex multiplication is an intrinsic property of the lattice and one can check that homothethy doesn't change this, so we can tlak about the homothety classes of lattices. We have the following beautiful result:

Corollary. [Cox89, p. 212] *Let $\mathcal{O}$ be an order in an imaginary quadratic field. There is a $1-1$ correspondence between the ideal class group $C(\mathcal{O})$ and the homothety classes of lattices with $\mathcal{O}$ as their full ring of complex multiplication.*

In particular, the class number $h(\mathcal{O})$ gives us the number of homothety classes of lattices with $\mathcal{O}$ as their full ring of complex multiplication. An example is in order. Consider, for example, lattices which have complex multiplication by $\sqrt{-3}$. This means that we have an order $\mathcal{O}$ containing $\sqrt{-3}$ in the field $K = \mathbf{Q}\left(\sqrt{-3}\right)$, so either $\mathcal{O} = \mathbf{Z}\left[\sqrt{-3}\right]$ or $\mathcal{O} = \mathbf{Z}\left[e^{2\pi i/3}\right]$. Both of these have class number 1, so up to homothety, the only lattices of this kind are $\left[1, \sqrt{-3}\right]$ and $\left[1, e^{2\pi i/3}\right]$.

Ultimately, we want to calculate j-invariants of lattices. This involves homogeinity properties of the constants g_2, g_3 defined earlier, so we will not cover this in detail. But as an example, consider complex multiplication by $i = \sqrt{-1}$. Up to homothety, the only lattice admitting this is $L = [1, i]$. To compute $j(L) = j(i)$, we note $iL = L$, so it follows by the Theorem above that $g_3(L) = g_3(iL) = i^{-6} g_3(L) = -g_3(L)$ so that $g_3(L) = 0$ and consequently $j(i) = 1728$.

These j-invariants, as already mentioned, have some remarkable properties. First of all, if we let $\tau \in \mathbb{H}$ be a complex number in the upper-half plane, we can define the j-function in the obvious way by $j(\tau) = j([1, \tau])$. Then for $q = e^{2\pi i \tau}$, we have a q-expansion of j with integer coefficients [Cox89, p. 297]:

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \\ + 20245856256q^4 + 333202640600q^5 + \dots \quad (5.2)$$

This is one reason why the factor 1728 appears in the definition of j-invariants - it is the smallest factor ensuring that all coefficients in the expanison are coprime integers.

The fundamental facts about j-invariants which give an even deeper insight into the connection with imaginary quadratic fields are as follow:

(1) If τ is a quadratic number (i.e τ is a root of $az^2+bz+c = 0$, $\gcd(a, b, c) = 1$, $D = b^2 - 4ac < 0$), then $j(\tau)$ is an algebraic integer.
(2) The degree of $j(\tau)$ is $h = h(D)$, the class number of the discriminant.
(3) There is a special case: $j(\tau) \in \mathbf{Q} \iff h(D) = 1$

Thus, if we wanted to compute the j-invariants of all 13 class number $h = 1$ orders, we could use the q-expansion in 5.2, summming up enough terms and taking the nearest integer value. As an example, for $\tau = i$, $q = e^{2\pi i^2} = e^{-2\pi}$ so that we have

$$\begin{aligned} \frac{1}{q} + 744 + 196884q &\approx 1647.16 \\ \dots + 21493760q^2 &\approx 1722.18 \\ \dots + 864299970q^3 &\approx 1727.75 \\ \dots + 20245856256q^4 &\approx 1727.99 \\ \dots + 333202640600q^5 &\approx 1727.99 \end{aligned}$$

so that indeed $j(i) = 1728$ provided we know something about the convergence of the q-expansion. Here we give a full table of j-invariants for class number $h = 1$ which is originally due to a scheme by Weber discussed in [Cox89, p. 260-263] but

one can easily get these by the series approximation we just saw in action. The 13 j-invariants are as follows:

D	τ	$j(\tau) = j(\mathcal{O})$
-3	$\frac{1+\sqrt{-3}}{2}$	0
-4	i	12^3
-7	$\frac{3+\sqrt{-7}}{2}$	-15^3
-8	$\sqrt{-2}$	20^3
-11	$\frac{3+\sqrt{-11}}{2}$	-32^3
-12	$\sqrt{-3}$	$54000 = 2^4 \cdot 3^3 \cdot 5^3$
-16	$2i$	66^3
-19	$\frac{3+\sqrt{-19}}{2}$	-96^3
-27	$\frac{1+3\sqrt{-3}}{2}$	$-12288000 = -2^{15} \cdot 3 \cdot 5^3$
-28	$\sqrt{-7}$	255^3
-43	$\frac{3+\sqrt{-43}}{2}$	-960^3
-67	$\frac{3+\sqrt{-67}}{2}$	-5280^3
-163	$\frac{3+\sqrt{-163}}{2}$	-640320^3

It is no coincidence that most of these numbers are perfect cubes, but we will not discuss this phenomenon here. But these j-invariants explain the apparently bizzare phenomenon of *almost integer* numbers. Consider $e^{\pi\sqrt{163}} = 640320^3 + 743.9999999999992507$. There is no reason why a transcendental number made up of seemingly arbitrary constants should be this close to a whole number. But the miracle turns out to be a simple consequence of complex multiplication. Let $z = \frac{1+\sqrt{-163}}{2}$ and consider the j-invariant $j(z) = -640320^3$ as already calculated. We also have $\frac{1}{q} = e^{-2\pi iz} = -e^{\pi\sqrt{163}}$ and $\mid q \mid \ll 1$, so in fact it is no surprise that $e^{\pi\sqrt{163}}$ is very close to $640320^3 + 744$. What is more interesting is that this example shows that the q-expansion converges very rapidly.

There are many more properties of j-invariants we have not discussed, in particular the connection to class field theory. In particular, if τ is a quadratic integer so that $\mathbf{Q}(\tau)$ is an imaginary quadratic field, it turns out that the field extension $\mathbf{Q}(\tau, j(\tau))$ is the Hilbert Class Field of $\mathbf{Q}(\tau)$ (i.e. the maximum abelian unramified extension of $\mathbf{Q}(\tau)$ - here *unramified* is rather technical, so we do not define it). In particular, since we know that for orders with class number $h = 1$ the j-invariants are integers, an immediate consequence is that if the ring of integers $\mathcal{O}_{\mathbf{Q}(\tau)}$ is a unique factorization domain, the field $\mathbf{Q}(\tau)$ is its own Hilbert Class Field.

References

[Arn92] S. Arno, *The Imaginary Quadratic Fields of Class Number 4*, Acta Arith. **40**, p.321-334, 1992.

[ARW98] S. Arno, M. L. Robinson, F. S. Wheeler, *Imaginary Quadratic Fields with Small Odd Class Number*, Acta. Arith. **83**, p.295-330, 1998.

[Bak66] A. Baker, *Linear Forms in the Logarithms of Algebraic Numbers I*, Mathematika **13**, p.204-216, 1996.

[Bak71] A. Baker, *Imaginary Quadratic Fields with Class Number 2*, Ann. Math. **94**, p.139-152, 1971.

[Cla] P. L. Clark, *Arithmetical Functions III: Orders of Magnitude*, http://math.uga.edu/~pete/4400arithmeticorders.pdf

[Cox89] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, John Wiley & Sons, Inc., New York, 1989.

[Coh96] H. Cohen, *A Course in Computational Algebraic Number Theory*, 3., corr. print., Springer-Verlag, Berlin Heidelberg New York, 1996.

[Cre92] J. E. Cremona, *Abelian Varieties with Extra Twist, Cusp Forms, and Elliptic Curves Over Imaginary Quadratic Fields*, Journal of the London Mathematical Society **45**, p.402-416, 1992.

[Gau86] C. F. Gauss, *Disquisitiones Arithmeticae*, reprint of 1966. ed. by Yale University Press, Springer-Verlag, New York Berlin Heidelberg Tokyo, 1986.

[Hee52] K. Heegner, *Diophantische Analysis und Modulfunktionen,* Math. Zeit. **56**, p.227-253, 1952.

[Neu99] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin Heidelberg New York, 1999.

[Oes85] J. Oesterlé, *Nombres de classes des corps quadratiques imaginaires*, Astérique **121-122**, p.309-323, 1985.

[Sta67] H. M. Stark, *A Complete Determination of the Complex Quadratic Fields of Class Number One*, Michigan Math. J. **14**, p.1-27, 1967.

[Sta75] H. M. Stark, *On Complex Quadratic Fields with Class Number Two*, Math. Comput. **29**, p.289-302, 1975.

[ST01] I. Stewart, D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, 3rd. ed., A K Peters Ltd., Natick, Massachusetts, 2001.

[Wag96] C. Wagner, *Class Number 5, 6, and 7*, Math. Comput. **65**, p.785-800, 1996.

[Wat03] M. Watkins, *Class Numbers of Imaginary Quadratic Fields*, Mathematics of Computation **73**, p.907-938, 2003.