Elliptic Curves with Complex Multiplication

Ivan Noden

Contents

1 Introduction **1**
1.1 Acknowledgements . . . 1

2 Elliptic Curves **1**
2.1 Definitions . . . 2
2.2 Group Law . . . 3
2.3 Maps Between Elliptic Curves . . . 4

3 Elliptic Functions **5**
3.1 Double Periodicity . . . 5
3.2 Lattices . . . 6
3.3 Properties of Elliptic Functions . . . 6
3.4 Weierstrass Function . . . 7

4 Uniformisation Theorem **11**
4.1 Homothety . . . 11
4.2 Modular Functions . . . 11
4.3 The j-invariant . . . 15
4.4 The j-invariant of Lattices and Elliptic Curves . . . 18
4.5 Correspondence of Maps . . . 21

5 Some Ideas from Class Field Theory **22**
5.1 Algebraic Number Fields . . . 22
5.2 Orders . . . 23
5.3 Splitting and Ramification of Primes . . . 26
5.4 Results of Class Field Theory . . . 28

6 Complex Multiplication **30**
6.1 Curves with CM . . . 30
6.2 Modular Functions for Subgroups . . . 31
6.3 The Modular Polynomial . . . 34
6.4 Roots of the Modular Polynomial . . . 36

7 Calculating Examples **38**
7.1 Class Number 1 . . . 38
7.2 Weber Functions . . . 39
7.3 Calculating $j(\sqrt{-14})$ . . . 42
7.4 Further Examples . . . 47

References **48**

1 Introduction

The study of algebraic number theory is primarily the study of algebraic number fields, that is finite extensions of the rationals. When studying field extensions, one of the most indispensable tools is that of the Galois group of the extension and the famous result of Kronecker-Weber tells us that every finite extension of $\mathbb{Q}$ with an abelian Galois group is contained in a field of the form $\mathbb{Q}(\zeta_n)$ where ζ_n is a primitive nth root of unity. One may then ask, given some number field K, does there exist a field L such that every abelian extension of K is a subfield of L? This explanatory note aims to partially answer that question in the case where $K = \mathbb{Q}(\sqrt{-m})$ for some square-free $m \in \mathbb{Z}_{>0}$, that is an imaginary quadratic field. To do so, we will develop the theory of elliptic curves with complex multiplication which provides us with a correspondence between certain sets of elliptic curves over $\mathbb{C}$ and the class group of an order in an imaginary quadratic field. This correspondence relies on values of the miraculous j-invariant, and it is $j(\tau)$, for some τ in the upper half plane that will generate the field L we are after. This result requires the machinery of class field theory, which we will not go into detail on. We will, however, build up enough understanding to motivate and grasp the statement of the theorems. Along the way, we will give a detailed account of the uniformisation theorem; delve into the study of modular functions; and end by proving some remarkable facts about the j-invariant, in particular that, if τ is an algebraic integer in an imaginary quadratic field, then $j(\tau)$ is also an algebraic integer.

The structure of this note is as follows. We open with Section 2 which very briefly recaps key definitions relating to elliptic curves, mainly to cement definitions and conventions. With Section 3, we study elliptic functions, in particular, the Weierstrass $\wp$-function, which we will show can be used to parameterise an elliptic curve isomorphic to a complex torus. The content of Section 4 then shows that every elliptic curve is one of this form and hence isomorphic to a complex torus. To prove this, we introduce modular functions and the j-invariant. We then take a brief aside in Section 5 to recap basic ideas of algebraic number theory and then cover some of the main results of class field theory, including the answer to the problem of abelian extensions of imaginary quadratic fields. These results are very useful in Section 6 where we introduce the notion of elliptic curves with complex multiplication and use them to show that $j(\tau)$ is an algebraic integer when τ is an algebraic integer in an imaginary quadratic field. Section 7 is then devoted to finding explicit values of $j(\tau)$ in these cases.

Whilst we aim to explain the majority of the theory needed, there are a few prerequisites required for understanding this text. Primarily, we recommend the reader be comfortable with the fundamentals of Galois theory, specifically the fundamental theorem. Also, it would be helpful if the reader were somewhat already familiar with the basic ideas of elliptic curves and algebraic number theory as we make extensive use of both and the recaps given do not go into a lot of detail.

1.1 Acknowledgements

The content of this document is based on the work done in a summer research project supervised by Assoc. Prof. Cecilia Busuioc of UCL. Its overall structure is loosely analogous to the one found in [Cox, 2013].

2 Elliptic Curves

In this section, we briefly recap some facts and definitions related to elliptic curves. For a fuller treatment (and for proofs) we refer the reader to [Silverman and Tate, 2015].

2.1 Definitions

Definition 2.1. An algebraic plane curve C over a field K is the zero set of a polynomial $f \in K[X,Y]$. That is,

$$C = \left\{(X,Y) \in K^2 : \ f(X,Y) = 0\right\}.$$

We will often write

$$C\colon \ f(X,Y) = 0$$

to mean C is an algebraic plane curve defined to be the zero set of f.

The degree of C is the degree of f.

In this text, we will only consider algebraic plane curves over $\mathbb{C}$ and so will simply say curve to mean an algebraic plane curve over $\mathbb{C}$.

When we want to work with curves, it is often convenient to work in a 'compactification' of $\mathbb{C}^2$ called the projective plane. A lot of geometric notions are 'nicer' in the projective plane than they are in the complex plane, for instance, distinct lines always meet at a point in the projective plane as opposed to parallel lines never meeting in the complex plane.

Definition 2.2. Define an equivalence relation on $\mathbb{C}^3 \setminus \{(0,0,0)\}$ by saying $(X_1,Y_1,Z_1) \sim (X_2,Y_2,Z_2)$ whenever there exists $\lambda \in \mathbb{C}^\times$ such that $X_1 = \lambda X_2$, $Y_1 = \lambda Y_2$ and $Z_1 = \lambda Z_2$. We then define the projective plane to be

$$\mathbb{P}^2 = \frac{\mathbb{C}^3 - \{(0,0,0)\}}{\sim}.$$

We denote the equivalence class of (X,Y,Z) in $\mathbb{P}^2$ by $(X : Y : Z)$. The degree of C is the degree of f.

Note that we cannot define curves in the projective plane in the obvious way, that is as the zero set of a polynomial in $\mathbb{C}[X,Y,Z]$. To see why, consider $f(X,Y,Z) = X^2 + Y^2 + Z^2 - 1 \in \mathbb{C}[X,Y,Z]$. Then $f(0,0,1) = 0$ but $(0:0:1) = (0:0:2)$ and $f(0,0,2) = 3$. Thus, f does not define a function on $\mathbb{P}^2$, and so we can't take its zero set. For this to work, we need restrictions on f.

Definition 2.3. We say a polynomial is homogenous if all of its terms are monomials of the same degree.

Suppose that $g \in \mathbb{C}[X,Y,Z]$ is homogenous of degree d. Then $g(\lambda X, \lambda Y, \lambda Z) = \lambda^d g(X,Y,Z)$ for all $\lambda \in \mathbb{C}^\times$ and hence it makes sense to say g is zero at some point in $\mathbb{P}^2$. This allows us to define projective plane curves over $\mathbb{C}$.

Definition 2.4. A projective plane curve C over a field K is the zero set of a homogenous polynomial $f \in K[X,Y,Z]$. That is,

$$C = \left\{(X : Y : Z) \in \mathbb{P}^2 : \ f(X,Y,Z) = 0\right\}.$$

We will say projective curve to mean projective plane curve over $\mathbb{C}$.

Let C be the curve defined by the polynomial $f \in \mathbb{C}[X,Y]$ of degree d. Note then that $g(X,Y,Z) = Z^d f(X/Z, Y/Z) \in \mathbb{C}[X,Y,Z]$ is homogenous of degree d and so defines a projective curve which we denote $\overline{C}$. Set $U = \left\{(X : Y : Z) \in \mathbb{P}^2 : \ Z \neq 0\right\} = \left\{(X : Y : 1) \in \mathbb{P}^2\right\}$ and see that we can identify C and $\overline{C} \cap U$ as this contains the zero set of $g(X,Y,1) = f(X,Y)$. Thus, for every curve we obtain a projective curve which contains it plus some extra points which are roots of $g(X,Y,0)$.

Definition 2.5. Let

$$C\colon \ f(X,Y) = 0$$

be a curve with f of degree d. The projective closure of C, denoted $\overline{C}$, is the zero set of $g(X,Y,Z) = Z^d f(X,Y)$. The polynomial g is known as the homogenisation of f. We call elements of the set

$$\left\{(X : Y : 0) \in \mathbb{P}^2 : \ g(X,Y,0) = 0\right\}$$

the points at infinity.

We will be primarily considered with a specific class of projective curves known as elliptic curves. These are a type of smooth projective curve.

Definition 2.6. We say the projective curve C defined by the homogenous polynomial $f \in K[X, Y, Z]$ is smooth if, for all $(X : Y : Z) \in C$, the partial derivatives of f evaluated at (X, Y, Z) are not all simultaneously zero.

Definition 2.7. An elliptic curve E over a field K is a smooth projective curve defined by a homogenous polynomial $f \in K[X, Y, Z]$ of degree 3. We will often write

$$E\colon\ g(X, Y) = 0$$

for some $g \in K[X, Y]$ of degree 3 to mean E is the projective closure of the curve defined by g.

Again, in this text, we will say elliptic curve to mean an elliptic curve over $\mathbb{C}$.

Theorem 2.8. *Let E be an elliptic curve. Under a suitable change of variables, E is the projective closure of the curve defined by*

$$Y^2 = X^3 + aX + b$$

for some $a, b \in \mathbb{C}$ with $4a^3 + 27b^2 \neq 0$. This is called the Weierstrass normal form.

Proof. See, for instance, [Silverman and Tate, 2015], Chapter 1.3. □

Suppose we have an elliptic curve

$$E\colon\ Y^2 = X^3 + aX + b.$$

Homogenising this equation yields $g(X, Y, Z) = Y^2Z - X^3 - aXZ^2 + bZ^3$ and hence the points at infinity of E is the set

$$\big\{(X : Y : 0) \in \mathbb{P}^2 :\ g(X, Y, 0) = X^3 = 0\big\} = \{(0 : 1 : 0)\}.$$

Hence, E is the curve defined by $Y^2 = X^3 + aX + b$ with the added 'point at infinity' $(0 : 1 : 0)$. Due to this, we tend to consider an elliptic curve as an algebraic curve defined by a polynomial of degree 3 along with this extra point $(0 : 1 : 0)$ denoted by O. It is often helpful to think of this point as lying 'infinitely' high up on the Y-axis.

2.2 Group Law

The conditions on f in the definition of an elliptic curve mean that the tangent line to the curve is well-defined at any point. We use this to define a group structure on an elliptic curve. We give a brief outline on the group operation, but the interested reader should consult [Silverman and Tate, 2015], Chapter 1 for a more detailed account.

Let P and Q be two points on an elliptic curve E. We define a line L as follows:

(i) if $P \neq Q$ then L is the line intersecting P and Q;

(ii) if $P = Q$ then L is the tangent line at P;

(iii) if $Q = \infty$ then L is the line through P perpendicular to the line $Y = 0$.

The line L will intersect E at a third point (it is possible that this point is also P, we must count multiplicities) which we call $P * Q$. We then reflect $P * Q$ in the line $Y = 0$, and we define this to be the point $P + Q$. We can then check that this defines an abelian group on E with ∞ as the identity.

2.3 Maps Between Elliptic Curves

We have now defined our objects of study so the natural next step is to define the morphisms between these objects. We will do so by defining maps between projective curves more generally. As projective curves are objects defined algebraically by polynomials, we should define the maps between them in terms of polynomials.

Let C and D be projective curves defined by $f \in \mathbb{C}[X,Y,Z]$ and $g \in \mathbb{C}[X,Y,Z]$ respectively. We will try to define a map $\varphi\colon C \to D$ in the most naive way by taking a triple of polynomials φ_1, φ_2 and φ_3 in $\mathbb{C}[X,Y,Z]$ and defining $\varphi(X:Y:Z) = (\varphi_1(X,Y,Z) : \varphi_2(X,Y,Z) : \varphi_3(X,Y,Z))$, then requiring this lands in D. This would be a bad definition as φ is not well-defined; it depends on the representative of $(X:Y:Z)$. However, suppose we require that φ_1, φ_2 and φ_3 are homogenous polynomials all of degree d. Then, if $\varphi_3(X,Y,Z)$ is non-zero, it is non-zero for every representative of $(X:Y:Z)$ and, in this case, we have

$$(\varphi_1(X,Y,Z) : \varphi_2(X,Y,Z) : \varphi_3(X,Y,Z)) = \left(\frac{\varphi_1(X,Y,Z)}{\varphi_3(X,Y,Z)} : \frac{\varphi_2(X,Y,Z)}{\varphi_3(X,Y,Z)} : 1\right).$$

Notice that

$$\frac{\varphi_i(\lambda X, \lambda Y, \lambda Z)}{\varphi_3(\lambda X, \lambda Y, \lambda Z)} = \frac{\lambda^d \varphi_i(X,Y,Z)}{\lambda^d \varphi_3(X,Y,Z)} = \frac{\varphi_i(X,Y,Z)}{\varphi_3(X,Y,Z)}$$

for $i \in \{1,2\}$ and all $\lambda \in \mathbb{C}^\times$. Thus, the value of

$$(\varphi_1(X,Y,Z) : \varphi_2(X,Y,Z) : \varphi_3(X,Y,Z))$$

does not depend on the representative of $(X:Y:Z)$ in these conditions. Of course, the same is true if either $\varphi_1(X,Y,Z)$ or $\varphi_2(X,Y,Z)$ is non-zero as well but what happens if all of them are zero? To deal with this, we will need to formalise some notation.

Definition 2.9. Define an equivalence relation on $\mathbb{C}(X,Y,Z) \setminus \{(0,0,0)\}$ by saying $(\psi_1,\psi_2,\psi_3) \sim (\rho_1,\rho_2,\rho_3)$ whenever there exists $\lambda \in \mathbb{C}(X,Y,Z)^\times$ such that $\psi_1 = \lambda\rho_1, \psi_2 = \lambda\rho_2$ and $\psi_3 = \lambda\rho_3$. We denote the equivalence class of (ψ_1,ψ_2,ψ_3) by $(\psi_1 : \psi_2 : \psi_3)$.

Now, suppose $\varphi_1(X,Y,Z) = \varphi_2(X,Y,Z) = \varphi_3(X,Y,Z) = 0$. Even when this is the case, we still have

$$(\varphi_1 : \varphi_2 : \varphi_3) = \left(\frac{\varphi_1}{\varphi_3} : \frac{\varphi_2}{\varphi_3} : 1\right).$$

Suppose there are some $\varphi_1', \varphi_2', \varphi_3' \in \mathbb{C}[X,Y,Z]$ all homogenouse of the same degree such that $\frac{\varphi_i(X,Y,Z)}{\varphi_3(X,Y,Z)} = \frac{\varphi_i'(X,Y,Z)}{\varphi_3'(X,Y,Z)}$ for all $i \in \{1,2\}$ and all $(X:Y:Z) \in C$, this is the same as saying that

$$\varphi_1\varphi_3' - \varphi_1'\varphi_3,\ \varphi_2\varphi_3' - \varphi_2'\varphi_3 \in (f).$$

Then $(\varphi_1 : \varphi_2 : \varphi_3)$ and $(\varphi_1' : \varphi_2' : \varphi_3')$ would define the same function on C but it could be that one of $\varphi_1'(X,Y,Z), \varphi_2'(X,Y,Z)$ or $\varphi_3'(X,Y,Z)$ is non-zero.

All of this discussion motivates the definition of a rational map.

Definition 2.10. Let C and D be projective curves defined by $f \in \mathbb{C}[X,Y,Z]$ and $g \in \mathbb{C}[X,Y,Z]$ respectively. A rational map $\varphi\colon C \dashrightarrow D$ is an equivalence class $(\varphi_1 : \varphi_2 : \varphi_3)$, with φ_1, φ_2 and φ_3 homogenous polynomials in $\mathbb{C}[X,Y,Z]$ of the same degree, not all of which are in (f), subject to the relation $(\varphi_1 : \varphi_2 : \varphi_3) \sim (\varphi_1' : \varphi_2' : \varphi_3')$ whenever all of $\varphi_1\varphi_2' - \varphi_1'\varphi_2, \varphi_1\varphi_3' - \varphi_1'\varphi_3$ and $\varphi_2\varphi_3' - \varphi_2'\varphi_3$ lie in the ideal (f), and such that $g(\varphi_1,\varphi_2,\varphi_3) \in (f)$.

We say φ is defined at $(X:Y:Z) \in C$ if any of $\varphi_1(X,Y,Z), \varphi_2(X,Y,Z)$ or $\varphi_3(X,Y,Z)$ are non-zero for some choice of representative $(\varphi_1 : \varphi_2 : \varphi_3)$.

A morphism of projective curves $\varphi\colon C \to D$ is a rational map defined at all points of C.

In the case of elliptic curves, morphisms are much simpler due to the following fact.

Theorem 2.11. *Let C be a smooth projective curve and D a projective curve. Then any rational map $C \dashrightarrow D$ is a morphism.*

Since elliptic curves have an added group structure, we want to consider morphisms that preserve this. For this, we use the following fact.

Theorem 2.12. *Let E_1 and E_2 be two elliptic curves with points at infinity O_1 and O_2 respectively. A morphism $\varphi\colon E_1 \to E_2$ is a group homomorphism if and only if $\varphi(O_1) = O_2$.*

This motivates the definition of an isogeny.

Definition 2.13. Let E_1 and E_2 be two elliptic curves with points at infinity O_1 and O_2 respectively. We call a morphism $\varphi\colon E_1 \to E_2$ with the property that $\varphi(O_1) = O_2$ an isogeny. We say φ is an isomorphism and that E_1 and E_2 are isomorphic if there exists an isogeny $\psi\colon E_2 \to E_1$ such that $\varphi \circ \psi$ and $\psi \circ \varphi$ are both the identity.

If we assume the elliptic curves E_1 and E_2 are written in Weierstrass normal form and $\varphi = (\varphi_1 : \varphi_2 : \varphi_3)\colon E_1 \to E_2$ is an isogeny, then, for all $(X : Y : Z) \in E_1$, $\varphi_3(X, Y, Z) = 0$ if and only if $(X : Y : Z) = (0 : 1 : 0)$ and we know that $\varphi(0 : 1 : 0) = (0 : 1 : 0)$. Set $U = \big\{(X : Y : Z) \in \mathbb{P}^2 : \ Z \neq 0\big\} = \{(X : Y : 1) \in \mathbb{P}^2\}$ and note that $E = E \cap U \cup \{(0 : 1 : 0)\}$. As φ is already determined on $(0 : 1 : 0)$, we need only define it on $E \cap U$. We know that, for $(X : Y : Z) \in E \cap U$, $\varphi_3(X, Y, Z) \neq 0$ so

$$\varphi(X : Y : Z) = \left(\frac{\varphi_1(X : Y : Z)}{\varphi_3(X : Y : Z)} : \frac{\varphi_2(X : Y : Z)}{\varphi_3(X : Y : Z)} : 1\right).$$

We can therefore identify φ with the tuple $\left(\frac{\varphi_1}{\varphi_3}, \frac{\varphi_2}{\varphi_3}\right)$.

3 Elliptic Functions

We begin our discussion with the study of elliptic functions, these are functions which are 'doubly periodic.' We say a function f is periodic if there exists some a such that $f(x) = f(x + a)$ for all x. The most obvious example is sin where $\sin(x) = \sin(x + 2\pi)$. Thus, to be doubly periodic, we want to consider functions f where $f(x) = f(x + a) = f(x + b)$ for some distinct a and b. We learn in the study of Fourier series that any periodic function, under suitable conditions, is equal to a convergent series whose terms are sums of sin and cos. In a similar vein, we will see that elliptic functions are all rational expressions in the Weierstrass $\wp$-function. It is the properties of this function in particular which will provide the link to elliptic curves.

For a more thorough discussion of these topics, we recommend the reader consult [Silverman, 2009].

3.1 Double Periodicity

There is a difficulty that arises when trying to give a precise definition of what a doubly periodic function should be, namely, how can we be sure a doubly periodic function isn't simply periodic? For instance, for all real numbers x, $\sin(x) = \sin(x + 2\pi) = \sin(x + 4\pi)$ but it would be ludicrous to claim that these are two distinct periods. The issue here is that both periods are integer multiples of some common divisor (in this case 2π).

More generally, let $f\colon \mathbb{R} \to \mathbb{R}$ be such that $f(x) = f(x + a) = f(x + b)$ where $a, b \in \mathbb{R}$ with $\frac{a}{b} \in \mathbb{Q}$. We can therefore choose some $p, q \in \mathbb{Z}$ coprime such that $\frac{a}{b} = \frac{p}{q}$. Letting $c = \frac{b}{q}$, we get

$$\frac{a}{c} = p, \qquad \frac{b}{c} = q$$

and hence $a = pc$ and $b = qc$. As p and q are coprime, we can find $h, k \in \mathbb{Z}$ such that $hp + kq = 1$ so $ha + kb = hpc + kqc = c$. It therefore follows that $f(x) = f(x + c)$ and the double periodicity of f is simply a consequence of this periodicity.

The other case then is if $\frac{a}{b}$ is irrational. It is beyond the scope of these notes, but it can then be show that f has periods dense in $\mathbb{R}$. Thus, assuming f is continuous, it must be constant.

To find more interesting cases than constant functions, we must turn to the complex numbers. Suppose $f\colon \mathbb{C} \to \mathbb{C}$ is continuous and that there exist $\omega_1, \omega_2 \in \mathbb{C}$ distinct such that $f(z) = f(z + \omega_1) = f(z + \omega_2)$ for all $z \in \mathbb{C}$. We want ω_1 and ω_2 to span $\mathbb{C}$ over $\mathbb{R}$, if not then $\omega_2 = \lambda\omega_1$ for some $\lambda \in \mathbb{R}$ and hence $\frac{\omega_1}{\omega_2} \in \mathbb{R}$ which has the same issues as when we were looking at real functions. If $\{\omega_1, \omega_2\}$ is indeed a basis for $\mathbb{C}$ over $\mathbb{R}$ then they cannot both be integer multiples of some common divisor and there is no reason why f should have to be constant. This therefore gives us a function which is 'truly' doubly periodic.

We are almost ready to define an elliptic function. The issue now is that there are far too many functions with this kind of doubly periodic behaviour, even limiting ourselves to continuous functions. To get a better grasp on the properties of these functions, we impose the condition that they are meromorphic.

Definition 3.1. An elliptic function is a meromorphic function $f\colon \mathbb{C} \to \mathbb{C}$ such that, for all $z \in \mathbb{C}$,

$$f(z) = f(z + \omega_1) = f(z + \omega_2)$$

where $\{\omega_1, \omega_2\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$.

3.2 Lattices

Suppose f is an elliptic function with periods ω_1 and ω_2. Note then that any $\mathbb{Z}$-linear combination of ω_1 and ω_2 are also periods of f. Hence, the periods of f are given by the set $\omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, this is a lattice in C.

Definition 3.2. A lattice Λ in $\mathbb{C}$ is an additive subgroup of $\mathbb{C}$ such that there exists a $\mathbb{Z}$-basis for Λ which is an $\mathbb{R}$-basis for $\mathbb{C}$.

It follows that every lattice can be written in the form $\omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, however, this form is not unique as, for instance, $\omega_1\mathbb{Z} + \omega_2\mathbb{Z} = \omega_1\mathbb{Z} + (-\omega_2)\mathbb{Z}$. We therefore often talk of a function being elliptic with respect to some lattice so that we don't have to fix a specific basis.

Definition 3.3. For a lattice Λ, we denote the set of all elliptic functions respect to Λ by $\mathbb{C}(\Lambda)$.

It is straightforward to see that $\mathbb{C}(\Lambda)$ is in fact a field with addition and multiplication defined pointwise.

If $f \in \mathbb{C}(\Lambda)$ then f is a well-defined meromorphic function on the space $\mathbb{C}/\Lambda$, a complex torus, so to study the behaviour of f on $\mathbb{C}$ as a whole, we need only look at its values on a set of coset representatives for $\mathbb{C}/\Lambda$.

Definition 3.4. A fundamental parallelogram for a lattice Λ is a set of the form

$$D = \{a + t_1\omega_1 + t_2\omega_2 : \ t_1, t_2 \in [0, 1)\}$$

where $a \in \mathbb{C}$ and $\{\omega_1, \omega_2\}$ is a $\mathbb{Z}$-basis for Λ. We let $\overline{D}$ denote the closure of D in $\mathbb{C}$.

3.3 Properties of Elliptic Functions

Let Λ be a lattice in $\mathbb{C}$; $f \in \mathbb{C}(\Lambda)$; and D a fundamental parallelogram for Λ. As f is determined by its values in D, we can use this to study its properties.

Proposition 3.5. *If f is holomorphic it is constant. If f has no zeroes it is constant.*

Proof. Suppose f is holomorphic. Note that

$$\sup_{z\in\mathbb{C}} |f(z)| = \sup_{z\in\overline{D}} |f(z)| .$$

As f is continuous and $\overline{D}$ is compact, $|f(z)|$ is bounded on $\overline{D}$ and hence on $\mathbb{C}$. Thus, by Liouville's theorem, f is constant.

Suppose f has no zeroes, then $\frac{1}{f} \in \mathbb{C}(\Lambda)$ and is holomorphic so is constant by the first part of this proof. Hence, f is constant. □

This tells us that, if f is not constant, it has at least a simple pole. We want to study the poles of f further, but first we introduce some notation.

Definition 3.6. Let $\operatorname{ord}_w(f)$ denote the order of f at $w \in \mathbb{C}$ and $\operatorname{res}_w(f)$ the residue of f at w.

Proposition 3.7.

$$\sum_{w\in D} \operatorname{ord}_w(f) = \sum_{w\in D} \operatorname{res}_w(f) = 0.$$

Proof. Note that we can choose D such that f has no poles on ∂D. Then, by Cauchy's Residue theorem,

$$\sum_{w\in D} \operatorname{res}_w(f) = \frac{1}{2\pi i}\int_{\partial D} f(z)\,\mathrm{d}z,$$

but this integral vanishes as f attains the same values on opposite sides of ∂D and these are traversed in opposite directions in the integral. Hence,

$$\sum_{w\in D} \operatorname{res}_w(f) = 0.$$

Observe that $f' \in \mathbb{C}(\Lambda)$ so $\frac{f'}{f} \in \mathbb{C}(\Lambda)$. By the first part,

$$\sum_{w\in D} \operatorname{res}_w\left(\frac{f'}{f}\right) = 0.$$

However, $\operatorname{res}_w\left(\frac{f'}{f}\right) = \operatorname{ord}_w(f)$ so the result follows. □

If f has only one simple pole at $w \in \mathbb{C}$, the above proposition implies $\operatorname{res}_w(f) = 0$ and so f is in fact holomorphic and hence constant. Thus, if f is not constant, it must have at least two poles, counting multiplicity.

Definition 3.8. The order of f is the number of poles of f counting multiplicity.

Therefore, the above implies the order of f is at least 2 or f is constant.

3.4 Weierstrass Function

It would be rather futile studying elliptic functions if we had no more examples than constants, so it is about time we tried to construct a non-trivial example. In the previous section, we deduced that any non-constant elliptic function must have an order of at least 2 and so the most obvious candidate to consider would be

$$f(z) = \sum_{w\in\Lambda} \frac{1}{(z-w)^2}.$$

Unfortunately, this series does not converge, so the function does not make sense. To ameliorate this, we introduce a 'fudge' factor to each term and define the Weierstrass $\wp$-function:

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\substack{w\in\Lambda \\ w\neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

This series does indeed converge absolutely and uniformly on compact subsets of $\mathbb{C}/\Lambda$ and so defines a meromorphic function on $\mathbb{C}$ with a double pole of residue zero at every point of Λ with no poles elsewhere (for a proof, see [Silverman, 2009], Theorem VI.3.1).

Importantly, one can also show that

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp_\Lambda, \wp'_\Lambda),$$

that is, every elliptic function with respect to Λ is a rational expression in $\wp_\Lambda$ and $\wp'_\Lambda$ (for a proof, see [Silverman, 2009] Theorem VI.3.2). If we can find some kind of algebraic relation between $\wp_\Lambda$ and $\wp'_\Lambda$, we will then be able to write

$$\mathbb{C}(\Lambda) \cong \frac{\mathbb{C}[X,Y]}{(f)}$$

for some $f \in \mathbb{C}[X,Y]$. This suggests that $\mathbb{C}(\Lambda)$ may be the ring of polynomial functions on some variety, but we already know that $\mathbb{C}(\Lambda)$ is the ring of meromorphic functions on $\mathbb{C}/\Lambda$ (a torus). It will turn out that f defines an elliptic curve, and we can then derive a correspondence between tori, elliptic curves and their morphisms.

To derive such an algebraic relation, it will be fruitful to find the Laurent expansion of $\wp_\Lambda(z)$ about $z = 0$, for this we use a trick. If $|x| < 1$ then recall

$$\frac{1}{1-x} = \sum_{n=1}^{\infty} x^n$$

and this convergence is uniform, so we can differentiate the series term by term to yield

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{1}{1-x}\right) = \frac{1}{(1-x)^2} = \sum_{n=1}^{\infty} n x^{n-1}.$$

Hence, if $w \neq 0$ and $|z| < |w|$, we have

$$\begin{aligned}
\frac{1}{(z-w)^2} - \frac{1}{w^2} &= \frac{1}{w^2}\left(\frac{1}{\left(1-\frac{z}{w}\right)^2} - 1\right) \\
&= \frac{1}{w^2}\left(-1 + \sum_{n=1}^{\infty} n \frac{z^{n-1}}{w^{n-1}}\right) \\
&= -\frac{1}{w^2} + \sum_{n=0}^{\infty} (n+1)\frac{z^n}{w^{n+2}} \\
&= \sum_{n=1}^{\infty} (n+1)\frac{z^n}{w^{n+2}}.
\end{aligned}$$

Letting $W = \min\{|w| : w \in \Lambda,\, w \neq 0\}$, if $|z| < W$ then we can substitute the above expression into $\wp_\Lambda$ to find

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\substack{w\in\Lambda \\ w\neq 0}} \left(\sum_{n=1}^{\infty} (n+1)\frac{z^n}{w^{n+2}} \right).$$

Observe that

$$\left|(n+1)\frac{z^n}{w^{n+2}}\right| \leq (n+1)\frac{z^n}{W^n}\left|\frac{1}{w}\right|^3,$$

so we have absolute convergence and so can exchange the order of summation. This leaves us with

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)\left(\sum_{\substack{w\in\Lambda\\ w\neq 0}}\frac{1}{w^{n+2}}\right)z^n.$$

Definition 3.9. The Eisenstein series of weight k for the lattice Λ is the series

$$G_k(\Lambda) = \sum_{\substack{w\in\Lambda\\ w\neq 0}}\frac{1}{w^k}.$$

If $k > 2$, the series $G_k(\Lambda)$ converges absolutely. We state this as a fact, but a proof can be found in, for instance, [Serre, 1973] Lemma VII.1. Observe that, if k is odd, $G_k(\Lambda) = 0$ and also note that, for any $k > 2$, $G_k(\lambda\Lambda) = \lambda^{-k}G_k(\Lambda)$ for all $\lambda \in \mathbb{C}$.

Using this notation, we find that the Laurent series for $\wp_\Lambda(z)$ about $z = 0$ is

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}(\Lambda)z^{2k}.$$

The idea now is to use powers of $\wp_\Lambda$ and $\wp'_\Lambda$ to find a Laurent series which has no terms with a negative exponent. This will give us a homolomorphic elliptic function which must be constant by Proposition 3.5, and so we can use this to find an algebraic relation between $\wp_\Lambda$ and $\wp'_\Lambda$.

Observe that

$$\begin{aligned}
\wp'_\Lambda(z) &= -2z^{-3} + 6G_4(\Lambda)z + 20G_6(\Lambda)z^3 + \cdots\\
\wp'_\Lambda(z)^2 &= 4z^{-6} - 24G_4(\Lambda)z^{-2} - 80G_6(\Lambda) + \cdots\\
\wp_\Lambda(z)^3 &= z^{-6} + 9G_4(\Lambda)z^{-2} + 15G_6(\Lambda) + \cdots.
\end{aligned}$$

So if we let

$$Q(z) = \wp'_\Lambda(z)^2 - 4\wp_\Lambda(z)^3 + 60G_4(\Lambda)\wp_\Lambda(z) + 140G_6(\Lambda)$$

then observe that the Laurent expansion of $Q(z)$ about $z = 0$ has all terms containing a positive power of z. We thus deduce that $Q(0) = 0$ and that $Q(z)$ is holomorphic at $z = 0$. Moreover, $Q \in \mathbb{C}(\Lambda)$ and Q is holomorphic away from Λ. It therefore follows that Q is holomorphic on $\mathbb{C}$ so, by Proposition 3.5, $Q(z) = 0$ for all $z \in \mathbb{C}$.

It is standard to define

$$g_2(\Lambda) = 60G_4(\Lambda), \qquad g_3(\Lambda) = 140G_6(\Lambda).$$

The above discussion shows that, for all $z \in \mathbb{C}$, $(\wp_\Lambda(z), \wp'_\Lambda(z))$ is a point on the cubic curve

$$E_\Lambda\colon\ Y^2 = 4X^3 - g_2(\Lambda)X - g_3(\Lambda).$$

Proposition 3.10. *For a lattice Λ, the curve*

$$E_\Lambda\colon\ Y^2 = 4X^3 - g_2(\Lambda)X - g_3(\Lambda)$$

is non-singular and hence an elliptic curve.

Proof. Let $\omega_1, \omega_2 \in \mathbb{C}$ be a basis for Λ and let $\omega_3 = \omega_1 + \omega_2$.

It is clear from the definition that $\wp_\Lambda$ is an even function so $\wp'_\Lambda$ is odd, hence

$$\wp'_\Lambda\left(\frac{\omega_i}{2}\right) = -\wp'_\Lambda\left(-\frac{\omega_i}{2}\right).$$

As $\wp'_\Lambda$ is elliptic with respect to Λ, we also know that

$$\wp'_\Lambda\left(-\frac{\omega_i}{2}\right) = \wp'_\Lambda\left(\frac{\omega_i}{2}\right).$$

From these two equalities, we deduce

$$\wp'_\Lambda\left(\frac{\omega_i}{2}\right) = -\wp'_\Lambda\left(\frac{\omega_i}{2}\right)$$

so

$$\wp'_\Lambda\left(\frac{\omega_i}{2}\right) = 0.$$

As $(\wp_\Lambda(z), \wp'_\Lambda(z))$ is a point on E_Λ for all $z \in \mathbb{C}$, we have found that the $\wp_\Lambda\left(\frac{\omega_i}{2}\right)$ are roots of

$$P(X) = 4X^3 - g_2(\Lambda)X - g_3(\Lambda).$$

To show E_Λ is non-singular, we will prove that these are three distinct roots.

Define

$$\psi_i(z) = \wp_\Lambda(z) - \wp_\Lambda\left(\frac{\omega_i}{2}\right).$$

Note that it is even so has at least a double zero at $z = \frac{\omega_i}{2}$. Also note that $\psi_i \in \mathbb{C}(\Lambda)$ and has order 2, so these can be the only zeros in an appropriate fundamental parallelogram by Proposition 3.7. In particular, $z = \frac{w_j}{2}$ is not a zero of ψ_i for $j \neq i$. This shows that the roots are distinct, completing the proof. □

We have therefore shown that the points $(\wp_\Lambda(z), \wp'_\Lambda(z))$ lie on the elliptic curve E_Λ. In fact, we can show that every point on E_Λ can be written in this form. This is a consequence of the following theorem, which we will not prove, that says $\mathbb{C}/\Lambda$ and E_Λ are isomorphic both as complex manifolds and as groups.

Theorem 3.11. *Let Λ be a lattice in $\mathbb{C}$ and E_Λ the elliptic curve*

$$E_\Lambda\colon\ Y^2 = 4X^3 - g_2(\Lambda)X - g_3(\Lambda).$$

Define the map

$$\phi\colon \mathbb{C}/\Lambda \to E_\Lambda$$

by

$$\phi(z) = \begin{cases} \infty & z = 0, \\ (\wp_\Lambda(z), \wp'_\Lambda(z)) & z \neq 0. \end{cases}$$

Then, ϕ is an isomorphism of complex manifolds and of groups.

Proof. See, for instance, [Silverman, 2009], Proposition VI.3.6. □

4 Uniformisation Theorem

In the previous section, we saw how the Weierstrass $\wp$-function can be used to provide a correspondence between lattices and some elliptic curves. The goal of this section is to show that every elliptic curve is isomorphic to one which corresponds to some lattice in this way. Furthermore, we can show that this lattice is unique up to some equivalence relation known as homothety. This provides a bijective correspondence between isomorphism classes of elliptic curves and lattices up to homothety.

The key idea to proving this fact is the use of the j-invariant, a numerical invariant which uniquely identifies both isomorphism classes of elliptic curves and lattices up to homothety.

4.1 Homothety

The idea of homothety is to identify lattices which 'look the same.' For instance, the lattices $\mathbb{Z} + i\mathbb{Z}$ and $2\mathbb{Z} + 2i\mathbb{Z}$ are distinct yet, if we visualise them on the complex plane, without labelling the axes, we have no way to tell them apart as they both have the same shape, their fundamental parallelograms are all square. This is because they are both a scaling of the other and the equivalence relation homothety takes this into account.

Definition 4.1. Let Λ_1 and Λ_2 be lattices in $\mathbb{C}$. We say Λ_1 and Λ_2 are homothetic, writing $\Lambda_1 \sim \Lambda_2$, if there exists some $\lambda \in \mathbb{C}$ with $\lambda \neq 0$ such that $\Lambda_1 = \lambda\Lambda_2$.

It is straightforward to verify that homothety is indeed an equivalence relation.

We want to be able to assign numerical invariants to lattices which respect the homothety relation. This seems a difficult task, so we loosen this restriction and introduce the notion of a lattice function.

Definition 4.2. Let **Latt** denote the set of all lattices in $\mathbb{C}$. A lattice function of weight $k \in \mathbb{Z}_{\geq 0}$ is a map $f\colon \mathbf{Latt} \to \mathbb{C}$ such that

$$f(\lambda\Lambda) = \lambda^{-k} f(\Lambda)$$

for all $\lambda \in \mathbb{C}$ and all $\Lambda \in \mathbf{Latt}$.

Example 4.1. We have already seen that the Eisenstein series of weight k is a lattice function of weight k as

$$G_k(\lambda\Lambda) = \sum_{\substack{w \in \lambda\Lambda \\ w \neq 0}} \frac{1}{w^k} = \sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{\lambda^k w^k} = \lambda^{-k} G_k(\Lambda).$$

Note that if f is a lattice function of weight k and g is a lattice function of weight l then $f \cdot g$ is a lattice function of weight $k + l$ and $\frac{f}{g}$ is a lattice function of weight $k - l$. Thus, if we find two lattice functions of the same weight, dividing them will yield a lattice function of weight 0, that is a function invariant under homothety. We could do this quite easily by considering, for instance, $\frac{G_8}{G_4^2}$ but there is very little we know about this function, even important facts such as is it constant? Where is it not defined? These questions are hard to answer as we don't have a good grasp on the space **Latt** on which it is defined. An idea then is to reinterpret lattice functions so that we can view them as functions on some nicer space, in particular as functions on

$$\mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im}(z) > 0\}.$$

4.2 Modular Functions

Let $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ be a lattice. Then Λ is homothetic to

$$\frac{1}{\omega_2}\Lambda = \mathbb{Z} + \frac{\omega_1}{\omega_2}\mathbb{Z}.$$

As

$$2\mathrm{Im}\left(\frac{\omega_1}{\omega_2}\right) = \frac{\omega_1}{\omega_2} - \frac{\overline{\omega}_1}{\overline{\omega}_2} = \frac{\omega_1\overline{\omega}_2 - \overline{\omega}_1\omega_2}{|\omega_2|},$$

we can assume $\frac{\omega_1}{\omega_2} \in \mathbb{H}$ by relabelling if necessary. This allows us to associate a point of $\mathbb{H}$ with each basis of $\{\omega_1, \omega_2\}$ of $\mathbb{C}$ over $\mathbb{R}$. We want to define some relation on $\mathbb{H}$ so that bases which define the same lattice Λ correspond to the same point modulo this relation. To do this, we use the following proposition.

Proposition 4.3. *Let*

$$M = \left\{(\omega_1, \omega_2) \in \mathbb{C}^2 : \omega_1, \omega_2 \neq 0, \mathrm{Im}\left(\frac{\omega_1}{\omega_2}\right) > 0\right\}$$

and let $(\omega_1, \omega_2), (\omega_1', \omega_2') \in M$. *Then* $\omega_1\mathbb{Z} + \omega_2\mathbb{Z} = \omega_1'\mathbb{Z} + \omega_2'\mathbb{Z}$ *if and only if*

$$\omega_1' = a\omega_1 + b\omega_2, \qquad \omega_2' = c\omega_1 + d\omega_2$$

where

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Proof. See, for instance, [Serre, 1973], Proposition VII.2. □

We thus define an action of $\mathrm{SL}_2(\mathbb{Z})$ on M by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\omega_1, \omega_2) = (a\omega_1 + b\omega_2, c\omega_1 + d\omega_2)$$

and the above proposition allows us to identify **Latt** with $\mathrm{SL}_2(\mathbb{Z})\backslash M$. We can also define an action of $\mathbb{C}^\times$ on M by

$$\lambda(\omega_1, \omega_2) = (\lambda\omega_1, \lambda\omega_2).$$

Then, we can identify $\mathbb{C}^\times\backslash M$ with $\mathbb{H}$ by the correspondence $(\omega_1, \omega_2) \to \frac{\omega_1}{\omega_2}$. In $\mathbb{C}^\times\backslash M$, every equivalence class has a representative of the form $(\tau, 1)$ with $\tau \in \mathbb{H}$ so, under this correspondence, the action of $\mathrm{SL}_2(\mathbb{Z})$ on M becomes the action on $\mathbb{H}$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\tau = \frac{a\tau + b}{c\tau + d}.$$

It thus follows that the map $\omega_1\mathbb{Z} + \omega_2\mathbb{Z} \mapsto \frac{\omega_1}{\omega_2}$ defines a bijection of $\mathbf{Latt}/\sim$ onto $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$.

How do we apply this to lattice functions? Let $f\colon \mathbf{Latt} \to \mathbb{C}$ be a lattice function of weight k and $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ with $(\omega_1, \omega_2) \in M$. Then

$$f(\Lambda) = f\left(\omega_2\left(\mathbb{Z} + \frac{\omega_1}{\omega_2}\mathbb{Z}\right)\right) = \omega_2^{-k} f\left(\mathbb{Z} + \frac{\omega_1}{\omega_2}\mathbb{Z}\right)$$

so define a function $g\colon \mathbb{H} \to \mathbb{C}$ such that

$$f(\omega_1\mathbb{Z} + \omega_2\mathbb{Z}) = \omega_2^{-k} g\left(\frac{\omega_1}{\omega_2}\right).$$

Then,

$$g(\tau) = f(\tau\mathbb{Z} + \mathbb{Z}) = f((a\tau + b)\mathbb{Z} + (c\tau + d)\mathbb{Z}) = (c\tau + d)^{-k} g\left(\frac{a\tau + b}{c\tau + d}\right)$$

for all

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

by Proposition 4.3. Now suppose we have a function $g\colon \mathbb{H} \to \mathbb{C}$ that satisfies this property and define

$$f(\omega_1\mathbb{Z} + \omega_2\mathbb{Z}) = \omega_2^{-k} g\left(\frac{\omega_1}{\omega_2}\right).$$

Then, f is independent of a choice of basis so is a well-defined function on **Latt** and

$$f(\lambda\omega_1\mathbb{Z} + \lambda\omega_2\mathbb{Z}) = \lambda^{-k} g\left(\frac{\lambda\omega_1}{\lambda\omega_2}\right) = \lambda^{-k} f(\omega_1\mathbb{Z} + \lambda\omega_2\mathbb{Z})$$

so f is a lattice function of weight k. This motivates the following definition.

Definition 4.4. We say a function $g\colon \mathbb{H} \to \mathbb{C}$ satisfies the modularity condition with weight k if, for all

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

we have

$$g\left(\frac{a\tau + b}{c\tau + d}\right) = (cz + d)^{-k} g(\tau)$$

for all $\tau \in \mathbb{H}$.

Proposition 4.5. *A function $g\colon \mathbb{H} \to \mathbb{C}$ satisfies the modularity condition with weight k if and only if $g(-1/\tau) = \tau^k g(\tau)$ and $g(\tau + 1) = g(\tau)$ for all $\tau \in \mathbb{H}$.*

Proposition 4.6. *Let*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Since $S, T \in \mathrm{SL}_2(\mathbb{Z})$, if g satisfies the modularity condition with weight k then $g(S\tau) = g(-1/\tau) = \tau^k g(\tau)$ and $g(T\tau) = g(\tau + 1) = g(\tau)$ as required.

For the other direction, recall the standard fact that S and T generate $\mathrm{SL}_2(\mathbb{Z})$. It is therefore enough to show that, if g satisfies the modularity condition with weight k for $\gamma_1, \gamma_2 \in \mathrm{SL}_2(\mathbb{Z})$ then it does for $\gamma_1\gamma_2$ and γ_1^{-1}. A straightforward calculation proves this to be true.

The above discussion provides a correspondence between lattice functions and functions that satisfy the modularity condition. Since functions on $\mathbb{H}$ are easier to study than functions on **Latt**. If we find a function which satisfies the modularity condition with weight 0 then this correspondence will yield a numerical invariant of lattices which is well-defined on **Latt**$/\sim$.

Functions satisfying the modularity condition with weight 0 are well-defined functions on the space $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. We will not get into the details, but this space is a Riemann surface which can be compactified by adding a point at infinity, $i\infty$. It is natural to then consider functions on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ which are holomorphic on the surface and at the point at infinity.

To make this last idea more precise, we note that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

so if f satisfies the modularity condition with any weight, $f(\tau+1)=f(\tau)$. Due to this fact, if we consider the map $\tau \mapsto q = e^{2\pi i \tau}$, which takes $\mathbb{H}$ to the punctured unit disk, then the function $g(q) = f\left(\frac{\log q}{2\pi i}\right)$ is well-defined and $f(t) = g(q)$. If f is holomorphic on $\mathbb{H}$ then g is holomorphic on the punctured unit disk so has a Laurent expansion about the origin. By abuse of notation, we write this Laurent expansion as

$$f(\tau) = \sum_{n\in\mathbb{Z}} a_n q^n$$

and often refer to it as a q-series. The map $\tau \mapsto q$ is such that $q \to 0$ as $\mathrm{Im}(\tau) \to \infty$ so, if the q-series only sums over non-negative integers then f can be extended to a holomorphic function at $q=0$ which we think of as a point at infinity in the imaginary axis. Similarly, if the q-series has only finitely many terms with negative exponents then we can consider f to be meromorphic at ∞.

These requirements motivate the following definition.

Definition 4.7. A modular function of weight k is a map $f\colon \mathbb{H} \to \mathbb{C}$ which satisfies the modularity condition with weight k; is meromorphic on $\mathbb{H}$; and is meromorphic at ∞, that is its q-series contains only finitely many terms with negative exponents. If f is holomorphic on $\mathbb{H}$ and at ∞, that is the q-series of f is summed only over non-negative integers, it is called a modular form. If f is a modular form and its q-series is summed only over positive integers it is called a cusp form.

Note that if we let $\mathrm{ord}_\infty(f) = \mathrm{ord}_0(g)$ where $g(q) = f\left(\frac{\log q}{2\pi i}\right)$ then a modular function has $\mathrm{ord}_\infty(f)$ finite; a modular form has $\mathrm{ord}_\infty(f) \geq 0$; and a cusp form has $\mathrm{ord}_\infty(f) \geq 1$.

Example 4.2. The Eisenstein series

$$G_k(\tau) = G_k(\mathbb{Z}+\tau\mathbb{Z}) = \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(m\tau+n)^k}$$

is a modular form of weight k. Its q-series is

$$G_k(\tau) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n\geq 1}\sigma_{k-1}(n)q^n$$

where

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} \text{ and } \sigma_r(m) = \sum_{\substack{d\in\mathbb{Z}_{\geq 1}\\ d|m}} d^r.$$

For a proof of this, see, for instance, [Serre, 1973], Proposition VII.8.

We often also consider the modular form $E_k = \frac{1}{2\zeta(k)}G_k$. If we recall the remarkable fact that

$$2\zeta(k) = -\frac{(2\pi i)^k}{k!}B_k$$

where B_k is defined so that

$$\frac{x}{e^x-1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}$$

then

$$E_k = 1 - \frac{2k}{B_k}\sum_{n\geq 1}\sigma_{k-1}(n)q^n.$$

In particular,

$$E_4 = 1 + 240q + 2160q^2 + 6720q^3 + \cdots$$
$$E_6 = 1 - 504q - 16632q^2 - 122976q^3 + \cdots$$

so we define

$$\Delta = \frac{E_4^3 - E_6^2}{1728} = q - 24q^2 + 252q^3 + \cdots$$

and this is a cusp form of weight 12.

The reason we have gone about defining modular functions is because we want to utilise what we know about the complex plane, holomorphic functions and so on to deduce properties of lattice functions. Now that we have the definitions set up, we are able to do that.

Theorem 4.8. *Let f be a modular function of weight k with $f \neq 0$. Write $\rho = e^{2\pi i/3}$. Then*

$$\operatorname{ord}_\infty(f) + \frac{\operatorname{ord}_i(f)}{2} + \frac{\operatorname{ord}_\rho(f)}{3} + \sum_{\substack{p \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \\ p \neq \infty, i, \rho}} \operatorname{ord}_p(f) = \frac{k}{12}.$$

This is known as the Valence Formula.

Proof. The formula is a corollary of the famous Riemann-Roch theorem. For a more elementary proof, see [Serre, 1973] Theorem VII.3. □

We use this formula to help us define a modular function. First, recall we defined

$$\Delta = \frac{E_4^3 - E_6^2}{1728} = q - 24q^2 + 252q^3 + \cdots$$

which is a cusp for of weight 12 with $\operatorname{ord}_\infty(\Delta) = 1$. By the Valence Formula,

$$1 + \frac{\operatorname{ord}_i(\Delta)}{2} + \frac{\operatorname{ord}_\rho(\Delta)}{3} + \sum_{\substack{p \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \\ p \neq \infty, i, \rho}} \operatorname{ord}_p(\Delta) = 1.$$

As Δ is holomorphic on $\mathbb{H}$, this therefore implies that Δ is non-zero on $\mathbb{H}$. Therefore,

$$j = \frac{E_4^3}{\Delta}$$

is holomorphic on $\mathbb{H}$; has a simple pole at infinity; and satisfies the modularity condition with weight 0. We thus have a modular function of weight 0, exactly what we were after!

4.3 The j-invariant

Definition 4.9. The j-invariant is the modular function of weight 0 defined by

$$j = \frac{E_4^3}{\Delta}.$$

One can check, using the q-series of the Eisenstein series, that

$$j = q^{-1} + 744 + \sum_{n=1}^{\infty} a_n q^n$$

where $a_n \in \mathbb{Z}$.

We will quickly cover some of the astonishing properties of the j-invariant as a modular function before we see how to apply it to lattices and elliptic curves.

Proposition 4.10. *The map $j\colon \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}$ is a bijection.*

Proof. Let $\lambda \in \mathbb{C}$ and define $f = j - \lambda$. We will show that f has a unique zero in $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. Note, f has a simple pole at ∞ and nowhere else so, by the Valence Formula

$$\frac{\mathrm{ord}_i(f)}{2} + \frac{\mathrm{ord}_\rho(f)}{3} + \sum_{\substack{p \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \\ p \neq \infty, i, \rho}} \mathrm{ord}_p(f) = 1.$$

The only non-negative integer solutions to this are given by

$$\left(\mathrm{ord}_i(f), \mathrm{ord}_\rho(f), \sum_{\substack{p \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \\ p \neq \infty, i, \rho}} \mathrm{ord}_p(f) \right) \in \{(2,0,0),\ (0,3,0),\ (0,0,1)\}.$$

This shows f has a unique zero. □

Definition 4.11. We let M_k denote the $\mathbb{C}$-vector space of modular forms of weight k. Let S_k denote the subspace of M_k of cusp forms.

Lemma 4.12. *(i) $M_k \cong S_k \oplus \mathbb{C}E_k$ for $k \geq 4$.*

(ii) $M_k = \{0\}$ for $k < 0$, $k = 2$ and k odd.

(iii) The map $M_{k-12} \to S_k$ defined by $f \mapsto \Delta f$ is an isomorphism.

(iv) $M_0 = \mathbb{C}$.

(v) For $k \in \mathbb{Z}_{\geq 0}$ with k even,

$$\dim M_k = \begin{cases} \left\lfloor \frac{k}{12} \right\rfloor, & k \equiv 2 \mod 12 \\ \left\lfloor \frac{k}{12} \right\rfloor + 1, & \text{otherwise.} \end{cases}$$

(vi) The set $\left\{ E_4^a E_6^b : a, b \in \mathbb{Z}_{\geq 0},\ 4a + 6b = k \right\}$ is a basis for M_k when $k \in \mathbb{Z}_{\geq} 0$ is even.

Proof. (i) Define $\phi\colon M_k \to \mathbb{C}$ by letting $\phi(f)$ be the constant term in the q-series of f. Then $\ker\phi = S_k$. See that $\dim(M_k/S_k) \leq 1$ and $E_k \in M_k - S_k$ for $k \geq 4$ so $M_k/S_k \cong \mathbb{C}E_k$. Thus, $M_k \cong S_k \oplus \mathbb{C}E_k$.

(ii) To show there are no modular forms of weight 2 or negative weight, simply use the Valence Formula. For odd weights, apply the modularity condition to $-I_2$.

(iii) We only need to show that division by Δ sends a cusp form to a modular form as this provides an inverse. If $g \in S_k$ then $\mathrm{ord}_\infty(g) \geq 1$ and $\mathrm{ord}_\infty(\Delta) = 1$ so $\mathrm{ord}_\infty\left(\frac{g}{\Delta}\right) \geq 0$. As Δ has no zeros elsewhere on $\mathbb{C}$, we see that $\frac{g}{\Delta} \in M_{k-12}$.

(iv) By the proof of the first part of this lemma, $M_0 = S_0 \oplus M_0/S_0$ and $\dim(M_0/S_0) \leq 1$ but, by the previous two parts, $S_0 \cong M_{-12} = \{0\}$ so $\dim M_0 \leq 1$but $\mathbb{C} \subset M_0$ so $M_0 = \mathbb{C}$.

(v) By the previous parts, $M_k = \mathbb{C}E_k$ for $k \in \{4, 6, 8, 10\}$; $M_0 = \mathbb{C}$; and $M_2 = \{0\}$ so the formula holds for $k \in \{0, 2, 4, 6, 8, 10\}$. Since $M_{k-12} \cong S_k$ and $M_k \cong S_k \oplus \mathbb{C}E_k$, increasing weight by 12 increases the dimension by 1, so the formula holds by induction.

(vi) By the previous part, this is true for $k \leq 12$. Now let n_k be the number of non-negative integer solutions to $4a + 6b = n_k$, and we can check that $n_k = \dim M_k$ for $k \in \{0, \ldots, 12\}$. See that $n_k = 1 + n_{k-12}$ so by induction and the dimension formula, $n_k = \dim M_k$ for $k \in \mathbb{Z}_{\geq 0}$ even, thus we only need to show linear independence. This is true for $k \leq 10$. If $k < 10$, suppose there exist $c_{a,b} \in \mathbb{C}$ such that

$$\sum_{\substack{a,b \in \mathbb{Z}_{\geq 0} \\ 4a+6b=k}} c_{a,b} E_4^a E_6^b = 0$$

Using the Valence Formula, we see that $E_6(i) = 0$ but $E_4(i) \neq 0$ so any term not containing E_6 must have a coefficient of 0. We can thus divide by E_6 and get a linear relation for weight $k - 6$. Applying induction then proves the $c_{a,b}$ are all zero.

□

Theorem 4.13. *The space of modular functions of weight* 0 *is* $\mathbb{C}(j)$*, that is, rational functions in* j*.*

Proof. Clearly, a rational function in j is a modular function. Now suppose f is a modular function of weight 0. Let S be the finite set of poles of f on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. For $w \in S$ let $o(w) = -\mathrm{ord}_w(f)$. Then

$$f(z) \prod_{w \in S} (j(z) - j(w))^{o(w)}$$

is a modular function of weight 0 which has no poles on $\mathbb{H}$. We can then choose $n \in \mathbb{Z}$ such that

$$F(z) = \Delta^n(z) f(z) \prod_{w \in S} (j(z) - j(w))^{o(w)}$$

is holomorphic at ∞ so $F \in M_{12n}$.

By Lemma 4.12, there are some $c_{a,b} \in \mathbb{Z}$ such that

$$F = \sum_{\substack{a,b \in \mathbb{Z}_{\geq 0} \\ 4a+6b=12n}} c_{a,b} E_4^a E_6^b.$$

Note that, if $4a + 6b = 12n$ then 3 divides a and 2 divides b so $a = 3A$ and $b = 2B$ for some $A, B \in \mathbb{Z}_{\geq 0}$. Then $12A + 12B = 12n$ so $A + B = n$. We then write

$$F = \sum_{\substack{a,b \in \mathbb{Z}_{\geq 0} \\ A+B=n}} c_{a,b} E_4^{3A} E_6^{2B}.$$

Since

$$\Delta = \frac{E_4^3 - E_6^2}{1728} \text{ and } j = \frac{E_4^3}{\Delta}$$

see that

$$j = \frac{E_6^2}{\Delta} + 1728.$$

Thus,

$$\frac{F}{\Delta^n} = \sum_{\substack{a,b \in \mathbb{Z}_{\geq 0} \\ A+B=n}} c_{a,b} \left(\frac{E_4^3}{\Delta}\right)^A \left(\frac{E_6^2}{\Delta}\right)^B = \sum_{\substack{a,b \in \mathbb{Z}_{\geq 0} \\ A+B=n}} c_{a,b} j^A (j - 1728)^B$$

is a rational function in j and so it follows that f is as well. □

This theorem essentially tells us that the field of meromorphic functions on the compactification of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is $\mathbb{C}(j)$.

4.4 The j-invariant of Lattices and Elliptic Curves

We previously found a correspondence between modular functions and lattice functions, so we can easily define $j(\Lambda)$ for $\Lambda \in \mathbf{Latt}$ by letting

$$j(\omega_1\mathbb{Z} + \omega_2\mathbb{Z}) = j\left(\frac{\omega_1}{\omega_2}\right)$$

and swapping the role of ω_1 and ω_2 if necessary. Also, recall that we identified $\mathbf{Latt}/\sim$ and $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. As we proved j is a bijection between $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ and $\mathbb{C}$ we thus also have a bijection between $\mathbf{Latt}/\sim$ and $\mathbb{C}$. In particular, this tells us that, for all $c \in \mathbb{C}$, there exists some $\Lambda \in \mathbf{Latt}$ such that $j(\Lambda) = c$. Moreover, if $j(\Lambda_1) = j(\Lambda_2)$ then Λ_1 is homothetic to Λ_2. Thus, j is a numerical invariant which allows us to classify lattice up to homothety.

Recall that for each lattice Λ, the torus $\mathbb{C}/\Lambda$ is isomorphic to the elliptic curve

$$E_\Lambda\colon\ Y^2 = 4X^3 - g_2(\Lambda)X - g_3(\Lambda).$$

Our idea now is to define $j(E)$ for any elliptic curve E such that $j(E_\Lambda) = j(\Lambda)$. If we then show that j classifies isomorphism classes of elliptic curves, we can start with the curve E, find a lattice Λ such that $j(\Lambda) = j(E)$, and then we will have proven that E is isomorphic to E_Λ and hence to $\mathbb{C}/\Lambda$, leading to a bijective correspondence between elliptic curves and complex tori.

We defined

$$j = \frac{E_4^3}{\Delta}.$$

Rewriting this explicitly in terms of the Eisenstein series we defined as lattice functions yields

$$\begin{aligned}
j &= 1728\frac{E_4^3}{E_4^3 - E_6^2} \\
&= 1728\frac{(2\zeta(4))^{-3}G_4^3}{(2\zeta(4))^{-3}G_4^3 - (2\zeta(6))^{-2}G_6^2} \\
&= 1728\frac{\frac{91125}{\pi^{12}}G_4^3}{\frac{91125}{\pi^{12}}G_4^3 - \frac{893025}{4\pi^{12}}G_6^2} \\
&= 1728\frac{364500G_4^3}{364500G_4^3 - 893025G_6^2} \\
&= \frac{1728}{16}\frac{27g_2^3}{27g_2^3 - 729g_3^2} \\
&= 108\frac{g_2^3}{g_2^3 - 27g_3^2}
\end{aligned}$$

where we recall that $g_2 = 60G_4$ and $g_3 = 140G_6$. Note that

$$E_\Lambda\colon\ Y^2 = 4X^3 - g_2(\Lambda)X - g_3(\Lambda)$$

is isomorphic to

$$E_\Lambda\colon\ Y^2 = X^3 - \frac{g_2(\Lambda)}{4}X - \frac{g_3(\Lambda)}{4}.$$

As any elliptic curve E can be written in the form

$$E\colon\ Y^2 = X^3 + aX + b$$

we can define

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}$$

and observe that

$$j(E_\Lambda) = 1728\frac{-\frac{1}{16}g_2(\Lambda)^3}{-\frac{1}{16}g_2^3 + \frac{27}{16}g_3^2} = 108\frac{g_2^3(\Lambda)}{g_2^3(\Lambda) - 27g_3^2(\Lambda)} = j(\Lambda)$$

as we desired. Note that, as E is non-singular, the quantity $4a^3 + 27b^2$ is non-zero so $j(E)$ is defined.

All that is left to show now is that if E_1 and E_2 are two elliptic curves then $j(E_1) = j(E_2)$ if and only if E_1 and E_2 are isomorphic. For this, we will need some basic facts about isogenies between elliptic curves.

Proposition 4.14. *Let E_1 and E_2 be elliptic curves over $\mathbb{C}$ and $\phi\colon E_1 \to E_2$ a non-constant isogeny. Then*

(i) ϕ is surjective;

(ii) there exist $u, v, s, t \in \mathbb{C}[x]$ with $\gcd(u, v) = \gcd(s, t) = 1$ such that

$$\phi(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$$

and u, v, s, t are unique up to scalar multiplication;

(iii) v and t have the same roots;

(iv) $\ker\phi$ consists of precisely those (x, y) where $v(x) = t(x) = 0$ and infinity so that $\ker\phi$ is finite;

(v) and if we let

$$\deg\phi = \max\{\deg u, \deg v\}$$

then $\deg\phi = |\ker\phi|$.

Proof. See, for example, [Sutherland, 2022b] □

Lemma 4.15. *Let*

$$E_1\colon\ Y^2 = X^3 + a_1X + b_1 \text{ and } E_2\colon\ Y^2 = X^3 + a_2X + b_2$$

be elliptic curves over $\mathbb{C}$. Then E_1 and E_2 are isomorphic if and only if there exists a $u \in \mathbb{C}$ with $u \neq 0$ such that

$$a_2 = u^4a_1 \text{ and } b_2 = u^6b_1.$$

Proof. Suppose E_1 and E_2 are isomorphic and $\phi\colon E_1 \to E_2$ an isomorphism. By Proposition 4.14, there exist $u, v, s, t \in \mathbb{C}[x]$ with $\gcd(u, v) = \gcd(s, t) = 1$ such that

$$\phi(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right).$$

As ϕ is injective, Proposition 4.14 tells us that v and t have no roots so are constant. We also know that $|\ker\phi| = 1 = \deg\phi$ so, as $\deg v = 0$, we have $\deg u = 1$. Thus, for some $A, B \in \mathbb{C}$ and $f \in \mathbb{C}[x]$, we can write

$$\phi(x, y) = (Ax + B, f(x)y).$$

If we substitute this into E_2 we find

$$f(x)^2y^2 = (Ax + B)^3 + a_2(Ax + B) + b_2$$

and hence

$$f(x)^2(x^3 + a_x + b_1) = (Ax + B)^3 + a_2(Ax + B) + b_2. \qquad (*)$$

Comparing degrees tells us $f(x) = c$ for some $c \in \mathbb{C}$. Comparing coefficients of x^2 yields $B = 0$ and comparing coefficients of x^3 yields $c^2 = A^3$. Substituting this all into $(*)$ gives us

$$A^3(x^3 + a_1x + b_1) = A^3x^3 + Aa_2x + b_2.$$

From which we deduce $a_2 = A^2a_1$ and $b_2 = A^3b_1$. Since $c^2 = A^3$, we know $A = \left(\frac{c}{A}\right)^2$ so let $u = \left(\frac{c}{A}\right)$, and we find $a_2 = u^4a_1$ and $b_2 = u^6b_1$ as required.

For the reverse direction, suppose we have a $u \in \mathbb{C}$ with $u \neq 0$ such that $a_2 = u^4a_1$ and $b_2 = u^6b_1$. Then, define $\phi\colon E_1 \to E_2$ by

$$\phi(x, y) = (u^2x, u^3y).$$

As $\deg \phi = 1 = |\ker \phi|$ and ϕ is not constant, by Proposition 4.14, ϕ is an isomorphism. □

Theorem 4.16. *Let E_1 and E_2 be elliptic curves. Then E_1 and E_2 are isomorphic if and only if $j(E_1) = j(E_2)$.*

Proof. We can write

$$E_1\colon\ Y^2 = X^3 + a_1X + b_1 \text{ and } E_2\colon\ Y^2 = X^3 + a_2X + b_2$$

First, suppose E_1 and E_2 are isomorphic. By Lemma 4.15, there exists some $u \in \mathbb{C}$ with $u \neq 0$ such that $a_2 = u^4a_1$ and $b_2 = u^6b_1$. Thus,

$$j(E_2) = 1728\frac{4a_2^3}{4a_2^3 + 27b_2^2} = 1728\frac{4u^{12}a_1^3}{4u^{12}a_1^3 + 27u^{12}b_2^2} = 1728\frac{4a_1^3}{4a_1^3 + 27b_1^2} = j(E_1).$$

Now, suppose $j(E_1) = j(E_2) = c$. We consider a few cases.

If $c = 0$ then $a_1 = a_2 = 0$ so simply choose $u \in \mathbb{C}$ such that $b_2 = u^6b_1$ and then $a_2 = u^4a_1$ as well. By Lemma 4.15, this means E_1 and E_2 are isomorphic.

If $c = 1728$ then $b_1 = b_2 = 0$ so again simply choose $u \in \mathbb{C}$ such that $a_2 = u^4a_1$ and the two curves are isomorphic.

Finally, if $c \notin \{0, 1728\}$ then we can rearrange

$$\frac{4a_1^3}{4a_1^3 + 27b_1^2} = \frac{4a_2^3}{4a_2^3 + 27b_2^2}$$

to get

$$a_1^3b_2^2 = a_2^3b_1^2. \tag{$*$}$$

Since $c \neq 0$, $a_1 \neq 0$ so let

$$u = \left(\frac{a_2}{a_2}\right)^{1/4}$$

and thus $a_2 = u^4a_1$. By $(*)$,

$$b_2^2 = \left(\frac{a_2}{a_1}\right)^3 b_1^2 = u^{12}b_1^2$$

so either $b_2 = u^6b_1$ or $b_2 = -u^6b_1$. In the former case, E_1 and E_2 are isomorphic by Lemma 4.15. In the latter case, replace u with iu, and we see E_1 and E_2 are isomorphic for the same reason. □

Thus, the j-invariant does everything we would like. If we have an elliptic curve E then by the surjectivity of j there exists some lattice Λ such that $j(\Lambda) = j(E)$. However, $j(\Lambda) = j(E_\Lambda)$ so $j(E_\Lambda) = j(E)$ and hence E_Λ and E are isomorphic. We already know E_Λ is isomorphic to $\mathbb{C}/\Lambda$ so this shows that E is isomorphic to $\mathbb{C}/\Lambda$. Moreover, any elliptic curve isomorphic to E is isomorphic to $\mathbb{C}/\Lambda$ and if there is another lattice Λ' such that E is isomorphic to $\mathbb{C}/\Lambda'$ then E is isomorphic to $E_{\Lambda'}$ and E_Λ so $j(E_\Lambda) = j(\Lambda) = j(\Lambda') = j(E_{\Lambda'})$ and thus Λ and Λ' are homothetic. We therefore have a bijective correspondence between isomorphism classes of elliptic curves and lattice up to homothety.

4.5 Correspondence of Maps

We have so far shown that we can identify isomorphism classes of elliptic curves and lattices up to homothety. To make this connection even stronger, we want to provide a correspondence between 'maps' between lattices and isogenies of elliptic curves. The question is, what is the best way to define 'maps' between lattices that makes this connection true but still a natural construction?

The key idea is to start with two elliptic curves E_1 and E_2 and recall that there are lattices Λ_1 and Λ_2 such that $E_1 \cong \mathbb{C}/\Lambda_1$ and $E_2 \cong \mathbb{C}/\Lambda_2$. Under this isomorphism, an isogeny $E_1 \to E_2$ corresponds to a holomorphic map $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ which fixes zero. An example of such a map is given by taking some $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 \subseteq \Lambda_2$ and then defining $\phi_\alpha \colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ by $\phi_\alpha(z) = \alpha z \mod \Lambda_2$. In the next proposition, we will show that all the holomorphic maps fixing zero have this form which allows us to associate isogenies to sets of the form $\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subseteq \Lambda_2\}$.

Proposition 4.17. *The association*

$$\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subseteq \Lambda_2\} \to \{\textit{holomorphic maps } \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \textit{ which fix zero.}\}$$

defined by

$$\alpha \mapsto \phi_\alpha,$$

where ϕ_α is as in the discussion above, is a bijection.

Proof. We first show it is an injection. Suppose $\phi_\alpha = \phi_\beta$ so, for all $z \in \mathbb{C}$ we have that $\alpha z \equiv \beta z \mod \Lambda_2$. Hence, the map $z \mapsto (\alpha - \beta)z$ sends $\mathbb{C}$ to Λ_2, but this is only possible if the map is constant. As $(\alpha - \beta)0 = 0$, the map must be the zero map so $\alpha = \beta$.

For surjectivity, suppose $\phi \colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ is holomorphic and $\phi(0) = 0$. It is a standard topological result that, as $\mathbb{C}$ is simply connected, there is a holomorphic map $f \colon \mathbb{C} \to \mathbb{C}$ with $f(0) = 0$ such that

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{f} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda_1 & \xrightarrow{\phi} & \mathbb{C}/\Lambda_2 \end{array}$$

commutes. Thus,

$$f(z + w) \equiv f(z) \mod \Lambda_2$$

for all $z \in \mathbb{C}$ and all $w \in \Lambda_1$. Hence, $f(z + w) - f(z) \in \Lambda_2$ for all $z \in \mathbb{C}$ which, again, is only possible if this map is independent of z. Thus, differentiating with respect to z, $f'(z + w) = f'(z)$ for all $w \in \Lambda_1$. This means f' is a holomorphic, elliptic function so, by Proposition 3.5, f' is constant. We can then write $f(z) = \gamma z + \delta$ for some $\gamma, \delta \in \mathbb{C}$, but $f(0) = 0$ so $\delta = 0$ and $f(z) = \gamma z$. Notice that $f(w) \equiv f(0) = 0 \mod \Lambda_2$ for all $w \in \Lambda_1$ so $\gamma\Lambda_1 \subseteq \Lambda_2$. Therefore, $\phi = \phi_\gamma$. □

We now not only have a correspondence between elliptic curves E_1 and E_2 with lattice Λ_1 and Λ_2 (up to isomorphism and homothety respectively) but also a correspondence between isogenies $E_1 \to E_2$ and the set $\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subseteq \Lambda_2\}$.

5 Some Ideas from Class Field Theory

We briefly depart from our main topic to discuss some basic ideas and results from algebraic number theory and class field theory. These results will be essential in order to achieve our aims but our far too broad and deep to receive a full treatment. We, therefore, will primarily state results without proof. For the interested reader, we recommend [Cox, 2013] and [Janusz, 1996]. Some familiarity with basic results in Galois theory will be helpful in understanding this section.

5.1 Algebraic Number Fields

We start by recapping some ideas of algebraic number fields and rings of algebraic integers.

Definition 5.1. An algebraic number field K is a finite field extension of $\mathbb{Q}$. The ring of algebraic integers in K, denoted $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. We call elements of any ring of this form an algebraic integer. A quadratic field is a degree 2 extension of $\mathbb{Q}$. We say a quadratic field is imaginary if it does not lie in $\mathbb{R}$.

Note that an algebraic number α is a root of a monic polynomial in $\mathbb{Z}[X]$ if and only if α is an algebraic integer. In particular, α is an algebraic integer if and only if its minimal polynomial (that is, the monic polynomial over $\mathbb{Q}$ of smallest degree of which α is a root) is in $\mathbb{Z}[X]$.

Definition 5.2. Let α be an algebraic integer. We define the degree of α to be the degree of its minimal polynomial.

Example 5.1. Let $d \in \mathbb{Z}$ be square-free with $d \neq 0, 1$. Then $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field (in fact, one can verify that all quadratic fields take this form). Also, one can check that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & d \equiv 1 \mod 4 \\ \mathbb{Z}[\sqrt{d}], & \text{otherwise.} \end{cases}$$

Algebraic integers are elements of $\mathbb{C}$ which can be 'algebraically described' by integers. For instance, $\sqrt{2}$ is a root of $x^2 - 2$ and whilst we can't find its value algebraically, we can say that it satisfies this polynomial. However, this alone can't distinguish $\sqrt{2}$ and $-\sqrt{2}$. Algebraically speaking, they are in some sense the same. We capture this notion by considering different embeddings of a number field K into $\mathbb{C}$.

Definition 5.3. Let K be an algebraic number field. An embedding of K in $\mathbb{C}$ is a homomorphism $K \to \mathbb{C}$.

Note that any embedding is automatically injective and fixes $\mathbb{Q}$. It is a standard result of Galois theory that any finite extension of $\mathbb{Q}$ has the form $\mathbb{Q}(\alpha)$ for some algebraic number α and this extension has degree equal to the degree of the minimal polynomial of α over $\mathbb{Q}$. Suppose $K = \mathbb{Q}(\alpha)$ is an algebraic number field of degree d and σ is an embedding of K. As σ fixes $\mathbb{Q}$, it is determined by where it sends α. Let m be the minimal polynomial of α. Note then that $m(\sigma(\alpha)) = \sigma(m(\alpha)) = 0$ so $\sigma(\alpha)$ is also a root of m. As m is irreducible over $\mathbb{Q}$, it must have distinct roots, and so we get d embeddings of K, all determined by which root of m that α is sent to. These embeddings are useful in giving us information about algebraic integers.

Definition 5.4. Let K be an algebraic number field and $\sigma_1, \ldots, \sigma_d$ the embeddings of K in $\mathbb{C}$. We define the norm of $\alpha \in K$ to be

$$N(\alpha) = \prod_{i=1}^{d} \sigma_i(\alpha).$$

Noting that $N(\alpha)$ is the constant term of the minimal polynomial of α (up to a sign), we see that $N(\alpha) \in \mathbb{Q}$ and, if $\alpha \in \mathcal{O}_K$ then $N(\alpha) \in \mathbb{Z}$. It is also clear that $N(\alpha\beta) = N(\alpha)N(\beta)$. From this we deduce that $\alpha \in \mathcal{O}_K$ is a unit if and only if $N(\alpha) = \pm 1$.

5.2 Orders

Recall Example 5.1. Here, we saw that $\mathbb{Z}[\sqrt{5}]$ is not the ring of algebraic integers of $\mathbb{Q}(\sqrt{5})$, yet it is still a very natural ring to consider. This motivates the definition of an order.

Definition 5.5. An order in a number field K is a finitely generated $\mathbb{Z}$-module contained in K which spans K as a $\mathbb{Q}$-vector space and is also a ring.

Note that this definition implies that, if $\mathcal{O}$ is an order in a number field K then $\mathcal{O}$ must be a $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$.

Example 5.2. For any number field K, $\mathcal{O}_K$ is an order.

In $\mathbb{Q}(\sqrt{5})$, $\mathbb{Z}[\sqrt{5}]$ is an order but note $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] \neq \mathbb{Z}[\sqrt{5}]$.

Let $\mathcal{O}$ be an order in K. As $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module, it is integral over $\mathbb{Z}$ so is contained in the integral closure of $\mathbb{Z}$ in K. That is, $\mathcal{O} \subseteq \mathcal{O}_K$. For this reason, $\mathcal{O}_K$ is referred to as the maximal order.

We will now consider some important invariants of an order, starting with the conductor.

Definition 5.6. The conductor of $\mathcal{O}$ is the largest ideal of $\mathcal{O}_K$ which is also an ideal of $\mathcal{O}$.

If $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field then recall that $\mathcal{O}_K = \mathbb{Z} + w_K\mathbb{Z}$ where

$$w_K = \begin{cases} \frac{1+\sqrt{d}}{2}, & d \equiv 1 \mod 4 \\ \sqrt{d}, & \text{otherwise.} \end{cases}$$

If $\mathcal{O}$ is an order in K, then, since $\mathcal{O}$ spans K as a $\mathbb{Q}$-vector space and $[K:\mathbb{Q}] = 2$, $\mathcal{O}$ must be a free $\mathbb{Z}$-module of rank 2. We know $\mathcal{O} \subseteq \mathcal{O}_K$ and $\mathcal{O}_K$ is also a free $\mathbb{Z}$-module of rank 2 so $\mathcal{O}_K/\mathcal{O}$ is finite. Let

$$f = \left|\frac{\mathcal{O}_K}{\mathcal{O}}\right|.$$

Note then that $f\mathcal{O}_K \subseteq \mathcal{O}$ and hence $\mathbb{Z} + f\mathcal{O}_K = \mathbb{Z} + fw_K\mathbb{Z} \subseteq \mathcal{O}$. Clearly $\mathbb{Z} + fw_k\mathbb{Z}$ has index f in $\mathcal{O}_K$, so it follows that $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$.

We thus know that $f\mathcal{O}_K$ is an ideal of $\mathcal{O}_K$ and $\mathcal{O}$; we claim this is the conductor. To see why, suppose for $\alpha \in \mathcal{O}_K$ we have $\alpha\mathcal{O}_K \subseteq \mathcal{O}$. Then f must divide α so $\alpha \in f\mathcal{O}_K$.

Another useful invariant is the discriminant.

Definition 5.7. Let K be an algebraic number field, $\{b_1, \ldots, b_n\}$ a basis of K, and $\sigma_1, \ldots, \sigma_n$ the embeddings of K in $\mathbb{C}$. We define

$$\Delta\{b_1, \ldots, b_n\} = \left(\det\begin{pmatrix} \sigma_1(b_1) & \cdots & \sigma_n(b_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(b_1) & \cdots & \sigma_n(b_n) \end{pmatrix}\right)^2$$

and call this the discriminant of $\{b_1, \ldots, b_n\}$.

Definition 5.8. If $\mathcal{O}$ is an order in a number field K and $\mathcal{O} = b_1\mathbb{Z} + \cdots + b_n\mathbb{Z}$ then we define the discriminant of $\mathcal{O}$ to be $\Delta(\mathcal{O}) = \Delta\{b_1, \ldots, b_n\}$. We write $\Delta(\mathcal{O}_K) = \Delta_K$.

By the change of basis formula, we can see that the discriminant of an order is invariant under the basis chosen. By Example 5.1, we deduce that, for $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ square-free and $d \neq 0, 1$,

$$\Delta_K = \begin{cases} d, & d \equiv 1 \mod 4 \\ 4d, & \text{otherwise.} \end{cases}$$

More generally, we know if $\mathcal{O}$ is an order in a quadratic field K then $\mathcal{O} = \mathbb{Z} + fw_K\mathbb{Z}$ so

$$\Delta(\mathcal{O}) = f^2\Delta_K.$$

As we can recover $\mathcal{O}$ from $\pm f$ we see that the discriminant of an order in a quadratic number field identifies it uniquely.

Since the only quadratic residues mod 4 are 0 and 1, we observe the following theorem:

Theorem 5.9. *Let $\mathcal{O}$ be an order in a quadratic field. Then $\Delta(\mathcal{O}) \equiv 0, 1 \mod 4$.*

Note that, if $\mathcal{O}$ is an order in a quadratic field $\mathbb{Q}(\sqrt{d})$ and $\Delta(\mathcal{O}) \equiv 0 \mod 4$ then either the conductor f is even or $d \not\equiv 1 \mod 4$. In the second case, we know

$$\mathcal{O} = \mathbb{Z} + f\sqrt{d}\mathbb{Z} = \mathbb{Z} = \sqrt{f^2 d}\mathbb{Z}.$$

If $d \equiv 1 \mod 4$ then f must be even so $f/2$ is an integer, and we can write

$$\mathcal{O} = \mathbb{Z} + f\frac{1+\sqrt{d}}{2}\mathbb{Z} = \mathbb{Z} + (f/2)(1+\sqrt{d})\mathbb{Z} = \mathbb{Z} + \sqrt{(f^2/4)d}\mathbb{Z}.$$

We therefore have the following result:

Proposition 5.10. *Let $\mathcal{O}$ be an order in quadratic field. If $\Delta(\mathcal{O}) \equiv 0 \mod 4$ then there exists some $n \in \mathbb{Z}$ such that*

$$\mathcal{O} = \mathbb{Z} + \sqrt{n}\mathbb{Z}.$$

One of the powerful facts about the ring of algebraic integers in a number field is that it is a Dedekind domain and hence its ideals factorise uniquely into a product of prime ideals. There are two important notions that are vital to the proof of this fact. The first is a way of 'cancelling' prime ideals which we do by constructing multiplicative inverses. In a Dedekind domain, this construction works for any prime ideal, however, in an order, only certain ideals have this property.

Definition 5.11. A fractional ideal of an order $\mathcal{O}$ is a subset $\mathfrak{a} \subseteq K$ such that $\beta\mathfrak{a}$ is an ideal of $\mathcal{O}$ for some non-zero $\beta \in \mathcal{O}$. Equivalently, $\mathfrak{a}$ is a non-zero, finitely generated $\mathcal{O}$-module. If $\mathfrak{a}$ and $\mathfrak{b}$ are fractional ideals of $\mathcal{O}$ then define

$$\mathfrak{ab} = \left\{ \sum_{i=1}^{n} \alpha_i\beta_i : \alpha_i \in \mathfrak{a},\, \beta_i \in \mathfrak{b},\, n \in \mathbb{Z}_{\geq 1} \right\}.$$

We say $\mathfrak{a}$ is invertible if there exists a fractional ideal $\mathfrak{a}^{-1}$ of $\mathcal{O}$ such that $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$.

Definition 5.12. We say a fractional ideal $\mathfrak{a}$ of an order $\mathcal{O}$ in K is proper if

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

For instance, note that any principal ideal is proper.

Proposition 5.13. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. A fractional ideal of $\mathcal{O}$ is proper if and only if it is invertible.*

Proof. If $\mathfrak{a}$ is invertible then $\mathfrak{ab} = \mathcal{O}$ for some fractional ideal $\mathfrak{b}$. Let $\beta \in K$ such that $\beta\mathfrak{a} \subseteq \mathfrak{a}$. Then

$$\beta\mathcal{O} = \beta(\mathfrak{ab}) \subseteq \mathfrak{ab} = \mathcal{O}$$

so $\beta \in \mathcal{O}$, and it follows that $\mathfrak{a}$ is proper.

For the other direction, see [Cox, 2013] Proposition 7.4 and Lemma 7.5. □

In the case of the maximal order $\mathcal{O}_K$, every ideal is proper and, using this, we can show that all ideals uniquely factorise into a product of prime ideals. This is not, in general, true for arbitrary orders, however there is a slight generalisation we can make. A useful tool in proving these facts is the idea of a norm which assigns a 'size' to ideals.

To motivate this definition, consider the following lemma.

Lemma 5.14. *Let K be an algebraic number field, $\mathcal{O}$ an order in K and $\mathfrak{a}$ a non-zero ideal of $\mathcal{O}$. Then*

$$\frac{\mathcal{O}}{\mathfrak{a}}$$

is finite.

Proof. Let $\alpha \in \mathfrak{a}$. Note then that there exist integers $\lambda_0, \dots, \lambda_{r-1}$ such that

$$\alpha^r + \lambda_{r-1}\alpha^{r-1} + \cdots + \lambda_0 = 0.$$

We deduce that $\lambda_0 \in (\alpha) \subseteq \mathfrak{a}$. There is hence a surjection

$$\frac{\mathcal{O}}{(\lambda_0)} \to \frac{\mathcal{O}}{\mathfrak{a}}.$$

However, $\frac{\mathcal{O}}{(\lambda_0)}$ is a finitely generated abelian group annihilated by $\lambda_0 \in \mathbb{Z}$, it thus must be finite and so the result follows. □

Definition 5.15. Let K be a number field and $\mathcal{O}$ an order of K. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$. We then define the norm of $\mathfrak{a}$ to be

$$N(\mathfrak{a}) = \left|\frac{\mathcal{O}}{\mathfrak{a}}\right|.$$

Note that as all finite integral domains are fields, the above shows that prime ideals of an order are maximal.

The norm of an ideal has many properties we may expect.

Definition 5.16. Let $\mathcal{O}$ be an order in an imaginary quadratic field K and $\mathfrak{a}$ a proper fractional ideal of $\mathcal{O}$. The conjugate of $\mathfrak{a}$, denoted $\overline{\mathfrak{a}}$, is the image of $\mathfrak{a}$ of the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$.

Proposition 5.17. *Let $\mathcal{O}$ be an order in an imaginary quadratic field and $\mathfrak{a}$ a proper fractional ideal of $\mathcal{O}$. Then*

$$\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O}.$$

Proof. See, for instance, [Cox, 2013] Lemma 7.14. □

Corollary 5.18. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K. Let $\mathfrak{a}$ and $\mathfrak{b}$ be proper fractional ideals of $\mathcal{O}$. Then*

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

Proof.

$$N(\mathfrak{ab})\mathcal{O} = \mathfrak{ab}\overline{\mathfrak{a}}\overline{\mathfrak{b}} = N(\mathfrak{a})N(\mathfrak{b})\mathcal{O}.$$

□

With these results at hand, it is straightforward to see that fractional ideals of an order $\mathcal{O}$ in an imaginary quadratic field K, denoted $I(\mathcal{O})$, is a group under multiplication. As principal ideals are always proper, let $P(\mathcal{O})$ be the subset of principal ideals of $\mathcal{O}$.

Definition 5.19. The class group of an order $\mathcal{O}$ in an imaginary quadratic field is the group

$$\mathrm{Cl}(\mathcal{O}) = \frac{I(\mathcal{O})}{P(\mathcal{O})}.$$

The class group measures the failure of all proper ideals being principal as, when this is the case, the class group is trivial. Since all ideals are proper in the maximal order $\mathcal{O}_K$, in this case we can think of the class group as measuring the failure of $\mathcal{O}_K$ being a UFD.

While we can't say exactly the same thing about arbitrary orders in an imaginary quadratic field, we are able to uniquely factorise a certain class of ideals.

Definition 5.20. Let $\mathcal{O}$ be an order in an imaginary quadratic field with conductor $f\mathcal{O}$. An ideal $\mathfrak{a}$ of $\mathcal{O}$ is coprime to the conductor if $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$.

If $\mathcal{O}$ is then an order in the imaginary quadratic field K and $\mathfrak{a}$ an $\mathcal{O}$-ideal coprime to the conductor, one can show that $\mathfrak{a}$ is proper. Furthermore, $\mathfrak{a}$ is prime if and only if $\mathfrak{a}\mathcal{O}_K$ is prime. This allows us to uniquely factorise $\mathcal{O}$-ideals coprime to the conductor into prime $\mathcal{O}$-ideals (which are necessarily also coprime to the conductor) using the factorisation in $\mathcal{O}_K$. If we let $I(\mathcal{O}, f)$ and $P(\mathcal{O}, f)$ be the subgroups of $I(\mathcal{O})$ and $P(\mathcal{O})$ respectively generated by ideals coprime to the conductor, one can show that

$$\mathrm{Cl}(\mathcal{O}) \cong \frac{I(\mathcal{O}, f)}{P(\mathcal{O}, f)}$$

and hence $\mathrm{Cl}(\mathcal{O})$, in some sense, measures the failure of $\mathcal{O}$ 'being a UFD' when we only consider $\alpha \in \mathcal{O}$ where (α) is coprime to the conductor. For a more detailed account of these facts, we suggest the reader consult [Cox, 2013], Chapter 7.

5.3 Splitting and Ramification of Primes

In this section, we study how primes in a number field K behave inside a finite field extension L of K. The main source for this section is [Marcus, 2018], Chapter 3 and 4. In an abuse of language, we say prime of a number field to mean a non-zero prime ideal of the respective ring of algebraic integers.

In this section, fix algebraic number fields K and L with $K \subseteq L$. Let $\mathfrak{p}$ be a prime of K. We mentioned in the previous section that ideals in rings of algebraic integers factorise uniquely into a product of prime ideals. The question we want to answer is what factorisations of $\mathfrak{p}\mathcal{O}_L$ are possible.

First, observe that if $\mathfrak{q}$ is a prime of L then $\mathfrak{q} \cap \mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$. Since

$$\frac{\mathcal{O}_K}{\mathfrak{q} \cap \mathcal{O}_K} \cong \frac{\mathcal{O}_K + \mathfrak{q}}{\mathfrak{q}} \subseteq \frac{\mathcal{O}_L}{\mathfrak{q}}$$

is finite, it must be that $\mathfrak{q} \cap K$ is non-zero and so a prime of K.

Also see that, if $\mathfrak{p}$ is a prime of K then $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$. It is not too hard to show that $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$, so we know there exist some distinct primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ of L such that

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_n^{e_n} \tag{$*$}$$

for some $e_1, \ldots, e_n \in \mathbb{Z}_{\geq 1}$. We hence deduce that $\mathfrak{p} \subseteq \mathfrak{q}_1$. It follows that $\mathfrak{q}_1 \cap \mathcal{O}_K$ contains $\mathfrak{p}$ but $\mathfrak{p}$ is maximal and $1 \notin \mathfrak{q}_1$ so $\mathfrak{q}_1 \cap \mathcal{O}_K \neq \mathcal{O}_K$. Therefore, $\mathfrak{q}_1 \cap \mathcal{O}_K = \mathfrak{p}$.

Definition 5.21. Let $\mathfrak{p}$ be a prime of K and $\mathfrak{q}$ a prime of L. We say $\mathfrak{p}$ lies below $\mathfrak{q}$ and $\mathfrak{q}$ lies above $\mathfrak{p}$ whenever $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$.

Our preceding discussion therefore shows that every prime of L lies above exactly one prime of K and every prime of K has at least one prime lying above it. The primes lying above the prime $\mathfrak{p}$ of K are precisely those in the prime decomposition $(*)$. We aim to study what these primes are and how they appear in the prime decomposition.

Definition 5.22. Let $\mathfrak{p}$ be a prime of K and

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_n^{e_n}$$

the prime decomposition of $\mathfrak{p}\mathcal{O}_L$. We call e_i the ramification index of $\mathfrak{q}_i$ over $\mathfrak{p}$ and denote it by $e(\mathfrak{q}_i|\mathfrak{p})$. If any of the ramification indices are greater than 1, we say $\mathfrak{p}$ ramifies in L. Otherwise, we say it splits.

Another natural quantity to consider is the inertial degree.

Definition 5.23. Let $\mathfrak{p}$ be a prime of K and $\mathfrak{q}$ a prime of L lying above $\mathfrak{p}$. The inertial degree of $\mathfrak{q}$ over $\mathfrak{p}$ is the degree of the field extension

$$\frac{\mathcal{O}_L}{\mathfrak{q}} \Big/ \frac{\mathcal{O}_K}{\mathfrak{p}}$$

and is denoted $f(\mathfrak{q}|\mathfrak{p})$.

The field extension in the above definition does indeed make sense. We have an inclusion $\mathcal{O}_K \to \mathcal{O}_L$ which induces a map $\mathcal{O}_K \to \frac{\mathcal{O}_L}{\mathfrak{q}}$ with kernel $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$, making $\frac{\mathcal{O}_K}{\mathfrak{p}} \to \frac{\mathcal{O}_L}{\mathfrak{q}}$ an injection. Further, both rings are fields as prime ideals in rings of algebraic integers are maximal.

Example 5.3. In $K = \mathbb{Q}(\sqrt{3})$ we have that $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$. One can verify that

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

is a prime decomposition so the ramification index of $(2, 1 + \sqrt{3})$ over (2) is 2. Moreover,

$$\frac{\mathbb{Z}[\sqrt{3}]}{(2, 1 + \sqrt{3})} \cong \frac{\mathbb{F}_2[x]}{(x + 1, x^2 + 1)} \cong \frac{\mathbb{F}_2[x]}{(x + 1)} \cong \mathbb{F}_2$$

is a degree 1 extension of

$$\frac{\mathbb{Z}}{(2)} \cong \mathbb{F}_2$$

so the inertial degree of $(2, 1 + \sqrt{3})$ over (2) is 1.

There is a strong relationship between ramification indices and inertial degrees.

Theorem 5.24. *Let $\mathfrak{p}$ be a prime in K and suppose*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_n^{e_n}$$

where the $\mathfrak{q}_i$ are distinct primes and $e_i \in \mathbb{Z}_{\geq 1}$. Let f_i be the inertial degree of $\mathfrak{q}_i$ over $\mathfrak{p}$. Then

$$\sum_{i=1}^{n} e_i f_i = [L : K].$$

Proof. See, for instance, [Marcus, 2018], Theorem 21. □

It is not too hard to see that ramification indices have a kind of tower law. That is, if M is a number field containing L and $\mathfrak{r}$ is a prime of M lying above a prime $\mathfrak{q}$ of L which lies above the prime $\mathfrak{p}$ of K, then

$$e(\mathfrak{r}|\mathfrak{p}) = e(\mathfrak{r}|\mathfrak{q})e(\mathfrak{q}|\mathfrak{p})$$
$$f(\mathfrak{r}|\mathfrak{p}) = f(\mathfrak{r}|\mathfrak{q})f(\mathfrak{q}|\mathfrak{p}).$$

In particular if $\mathfrak{p}$ ramifies in $\mathcal{O}_L$ then $\mathfrak{p} \cap \mathbb{Z} = (p)$ (for some prime $p \in \mathbb{Z}$) must ramify in L. It is a standard result of algebraic number theory that a prime of $\mathbb{Z}$ only ramifies in a number field K if it divides Δ_K and so this is an easy way to see that only finitely many prime of K can ramify in L.

Of special interest to us is when the extension L/K is Galois. If this is the case, let $\mathfrak{p}$ be a prime of K and $\mathfrak{q}$ a prime of L lying above $\mathfrak{p}$. For all $\sigma \in \mathrm{Gal}(L/K)$, notice that

$$\sigma(\mathfrak{q}) \cap \mathcal{O}_K = \sigma(\mathfrak{q} \cap \mathcal{O}_K) = \sigma(\mathfrak{p}) = \mathfrak{p}$$

so $\sigma(\mathfrak{q})$ is also a prime lying above $\mathfrak{p}$. In fact, one can show a stronger result.

Proposition 5.25. *If L/K is Galois and $\mathfrak{q}_1, \mathfrak{q}_2$ are two primes of L lying above the prime $\mathfrak{p}$ of K, then there exists some $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$.*

Proof. See, for instance, [Marcus, 2018], Theorem 23. □

Suppose then that $\mathfrak{p}$ is a prime of K and

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_n^{e_n}$$

is a prime decomposition. Applying $\sigma \in \mathrm{Gal}(L/K)$, we see

$$\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{q}_1)^{e_1} \cdots \sigma(\mathfrak{q}_n)^{e_n}.$$

Hence, by Proposition 5.25, we can deduce that $e_1 = \cdots = e_n$. Denote this value by e. Similarly, as $\sigma(\mathcal{O}_L) = \mathcal{O}_L$, we have

$$\frac{\mathcal{O}_L}{\mathfrak{q}_i} \cong \frac{\mathcal{O}_L}{\sigma(\mathfrak{q}_i)}$$

so, again by Proposition 5.25, the inertial degrees of all the $\mathfrak{q}_i$ must be equal. Denote this value by f. By Theorem 5.24, we see

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

In particular, if $e = f = 1$ then $\mathfrak{p}$ splits into precisely $[K : L]$ primes. This is the case we are particular interested in and so it gets a name.

Definition 5.26. We say that the prime $\mathfrak{p}$ of K splits completely in L if it is unramified and the inertial degrees of each prime above $\mathfrak{p}$ is 1.

We should mention the following helpful tool in determining how primes split or ramify.

Theorem 5.27. *Let L/K be a Galois extension of number fields where $L = K(\alpha)$ for some $\alpha \in \mathcal{O}_L$. Let $m \in \mathcal{O}_K[X]$ be the minimal polynomial of α over K. For a prime $\mathfrak{p}$ of K, if we can write*

$$m(X) \equiv m_1(X) \cdots m_n(X) \mod \mathfrak{p}$$

where the m_i are pairwise distinct and irreducible mod $\mathfrak{p}$. Then

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_n$$

where $\mathfrak{q}_i = \mathfrak{p} + m_i(\alpha)\mathcal{O}_L$ is a prime of L and the $\mathfrak{q}_i$ are pairwise distinct.

Proof. This follows from [Marcus, 2018], Theorem 27. □

5.4 Results of Class Field Theory

To thoroughly study elliptic curves with complex multiplication, at least some class field theory is required. In what we aim to achieve, the amount needed is relatively little, but any further study in the subject will require even more. Thus, in this section, we hope to outline the main aims of class field theory as well as the results we need to use without spending too much time on the details. The main result we will need is the existence of a field extension of an imaginary quadratic field associated to each order. This extension then has a lot of useful properties relating to how primes ramify and/or split.

The key result is as follows.

Theorem 5.28. *Let K be an imaginary quadratic field and $\mathcal{O}$ an order of K with conductor f. There exists a finite Galois extension L/K such that all primes of K which ramify in L divide $f\mathcal{O}_K$ and*

$$\mathrm{Cl}(\mathcal{O}) \cong \mathrm{Gal}(L/K).$$

Proof. This follows from the Artin reciprocity theorem. We recommend the reader consult [Cox, 2013], Chapter 8 for more details. □

Definition 5.29. Using the notation of Theorem 5.28, we call L the ring class field of $\mathcal{O}$. If $\mathcal{O} = \mathcal{O}_K$ then we call L the Hilbert class field.

The Hilbert class field has the following additional property.

Theorem 5.30. *Let K be an imaginary quadratic field and L the Hilbert class field of K. If M is an extension of K such that $\mathrm{Gal}(M/K)$ is abelian and every prime of K is unramified in M then $M \subseteq L$.*

Proof. See, for instance, [Cox, 2013], Theorem 8.10. □

In the next section, we will aim to prove that, given an order $\mathcal{O}$ and $\mathfrak{a}$ a proper fractional ideal of $\mathcal{O}$, $j(\mathfrak{a})$ is an algebraic integer (when $\mathfrak{a}$ is interpreted as a lattice). We can make the proof of this much easier by showing there exists an element $\alpha \in \mathcal{O}$ such that $N(\alpha)$ is prime. Luckily, we can do this using class field theory. Before we can state these results, we introduce some notation.

Definition 5.31. Let A and B be sets. We write $A \dot{\subseteq} B$ if there is some finite set C such that $A \subseteq B \cup C$. If $A \dot{\subseteq} B$ and $B \dot{\subseteq} A$ then we write $A \doteq B$.

One can think of $A \doteq B$ as saying A and B are the same up to some finite number of elements.

Theorem 5.32. *Let K be an imaginary quadratic field and $\mathcal{O}$ an order of K. Let L be the ring class field of $\mathcal{O}$ and S the set of primes of $\mathbb{Q}$ which split completely in L. Then*

$$S \doteq \{p \in \mathbb{Z} \text{ prime} : \ N(\alpha) = p \text{ for some } \alpha \in \mathcal{O}\}.$$

Proof. This is essentially Theorem 9.4 of [Cox, 2013]. □

By this result, if we can show the there are infinitely many primes of $\mathbb{Q}$ which split completely in the class field of an order, then the corollary we need will follow. Thankfully, this is another standard result of class field theory.

Theorem 5.33. *Let K be a number field and L a Galois extension of K. There are infinitely many primes of K which split completely in L.*

Proof. This is a direct consequence of the Čebotarev Density theorem. See [Cox, 2013], Chapter 8 for more details. □

Corollary 5.34. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. Then $\mathcal{O}$ contains an element of prime norm.*

6 Complex Multiplication

In this section, we will study the endomorphism ring $\mathrm{End}(E)$ of an elliptic curve E, that is the ring of isogenies from an elliptic curve to itself. Using the results in the previous section, we will see that this ring is either $\mathbb{Z}$ or an order in an imaginary quadratic field. We will then see that, if we fix an order $\mathcal{O}$ in an imaginary quadratic field, then we can identify isomorphism classes of elliptic curves E such that $\mathrm{End}(E) = \mathcal{O}$ with the elements of the ideal class group of $\mathcal{O}$. We will then see that proper fractional ideals $\mathfrak{a}$ of $\mathcal{O}$ give us lattices with $\mathcal{O}$ as the CM ring and then show that $j(\mathfrak{a})$ is an algebraic integer.

6.1 Curves with CM

Let us look at isogenies from an elliptic curve to itself.

Definition 6.1. For an elliptic curve E, let $\mathrm{End}(E)$ denote the ring of isogenies from E to itself, that is, endomorphisms of E.

We know that an elliptic curve E is isomorphic to some torus $\mathbb{C}/\Lambda$ where Λ is a lattice in $\mathbb{C}$. By the results of Section 4, we can then identify

$$\mathrm{End}(E) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}.$$

It is this clear that $\mathbb{Z} \subseteq \mathrm{End}(E)$ for all elliptic curves. To see what the rest of $\mathrm{End}(E)$ looks like, recall that we can replace Λ by a homothetic lattice, and so we may assume $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ for some $\tau \in \mathbb{H}$. Thus, $\alpha \in \mathrm{End}(E)$ if and only if we have

$$\alpha = a + b\tau \text{ and } \alpha\tau = c + d\tau$$

for some $a, b, c, d \in \mathbb{Z}$. We see then that $\mathrm{End}(E) \subseteq \mathbb{Q}(\tau)$. Assuming $\mathbb{Z} \neq \mathrm{End}(E)$, suppose $b \neq 0$, we then derive the relation

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

So τ is not real and is the root of a quadratic polynomial, meaning $\mathbb{Q}(\tau)$ is an imaginary quadratic field. Also note that

$$\frac{\alpha - a}{b} = \tau = \frac{c}{\alpha - d}$$

so

$$(\alpha - a)(\alpha - d) - bc = 0.$$

This shows us that $\mathrm{End}(E)$ is integral over $\mathbb{Z}$ and hence a finitely generated $\mathbb{Z}$-module. However, we can also see that $\mathrm{End}(E)$ contains $\{1, \tau\}$ so generates $\mathbb{Q}(\tau)$ over $\mathbb{Q}$. All of this put together implies that $\mathrm{End}(E)$ is an order in $\mathbb{Q}(\tau)$. We summarise these results in the following proposition.

Proposition 6.2. *Let E be an elliptic curve. Then, either $\mathrm{End}(E) = \mathbb{Z}$ or $\mathrm{End}(E)$ is an order in an imaginary quadratic field.*

Definition 6.3. We say an elliptic curve E has complex multiplication (CM) if $\mathrm{End}(E) \neq \mathbb{Z}$. If this is the case, we call $\mathrm{End}(E)$ the CM ring of E. In a slight abuse of language, we also often refer to the CM ring of a lattice by which we mean the CM ring of an associated elliptic curve.

Example 6.1. Let $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ which is a lattice in $\mathbb{C}$. It follows that the elliptic curve

$$E\colon\ Y^2 = 4X^3 - g_2(\sqrt{-5})X - g_3(\sqrt{-5})$$

is isomorphic to $\mathbb{C}/\mathcal{O}_K$ and hence

$$\mathrm{End}(E) = \{\alpha \in \mathbb{C} : \alpha\mathcal{O}_K \subseteq \mathcal{O}_K\}$$

so $\mathcal{O}_K \subseteq \mathrm{End}(E)$. However, we know $\mathrm{End}(E)$ is an order in K and $\mathcal{O}_K$ is the maximal order so $\mathrm{End}(E) = \mathcal{O}_K$.

Suppose now we start with an imaginary quadratic field K and an order $\mathcal{O}$. If Λ is a lattice with CM ring $\mathcal{O}$ then

$$\mathcal{O} = \{\alpha \in K : \alpha\Lambda \subseteq \Lambda\},$$

and so we see that Λ is a proper fractional ideal. Conversely, suppose $\mathfrak{a}$ is a proper fractional ideal of $\mathcal{O}$. Then $\mathfrak{a}$ is a finitely generated $\mathcal{O}$-module and hence a finitely generated $\mathbb{Z}$-module of rank 2. It follows that $\mathfrak{a}$ is a lattice in K. The CM ring of this lattice is $\mathcal{O}$ as $\mathfrak{a}$ is proper. Furthermore, if $\mathfrak{b}$ is another proper fractional ideal of $\mathcal{O}$ and $\mathfrak{a} = \lambda\mathfrak{b}$ for some $\lambda \in \mathbb{C}$ with $\lambda \neq 0$ then $\mathfrak{a}\mathfrak{b} = \lambda\mathcal{O}$ so $\mathfrak{a} = \mathfrak{b}$ in $\mathrm{Cl}(\mathcal{O})$.

The above discussion allows us to identify $\mathrm{Cl}(\mathcal{O})$ with the homothety classes of lattices with $\mathcal{O}$ as their CM ring. Since we can uniquely identify the homothety classes (and hence isomorphism classes of elliptic curves) with the j-invariant, we define

$$\mathcal{E}(\mathcal{O}) = \{j(E) : E \text{ is an elliptic curve with } \mathrm{End}(E) = \mathcal{O}\},$$

and thus we identify $\mathrm{Cl}(\mathcal{O})$ and $\mathcal{E}(\mathcal{O})$.

6.2 Modular Functions for Subgroups

So far, we know if $\mathfrak{a}$ is a proper fractional ideal of an order $\mathcal{O}$ in an imaginary quadratic field then $\mathfrak{a}$ is a lattice with CM ring $\mathcal{O}$. Our next goal is to find a polynomial satisfied by $j(\mathfrak{a})$, and we will show that this polynomial has coefficients in $\mathbb{Z}$. To do this, we must return to our study of modular functions.

Definition 6.4. For $N \in \mathbb{Z}_{\geq 1}$,

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

We want to define modular functions for $\Gamma_0(N)$, that is meromorphic functions of $\mathbb{H}$ that satisfy the modularity condition with weight 0 when we consider only the action of $\Gamma_0(N)$ on $\mathbb{H}$. However, we need to be careful with how we consider the behaviour of these functions at infinity. When we were considering the action of all of $\mathrm{SL}_2(\mathbb{Z})$, this was easy to take care of, but now we must deal with the issue more precisely.

Recall, we defined the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ by linear fractional transformations. The space $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is not compact, so we add a point at infinity to compactify it. However, since

$$\frac{a\tau + b}{c\tau + d} \to \frac{a}{c} \text{ as } \mathrm{Im}\tau \to \infty,$$

if we add a point at infinity we must also add in $\mathbb{Q}$. We thus consider $\mathrm{SL}_2(\mathbb{Z})$ acting on

$$\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$$

where we define

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{x}{y} = \frac{ax + by}{cx + dy}$$

and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \begin{cases} \frac{a}{c}, & c \neq 0 \\ \infty, & c = 0. \end{cases}$$

We can then consider the space $\Gamma_0(N)\backslash\mathbb{H}^*$, which is now compact. The additional points $\mathbb{Q} \cup \{\infty\}$ are called the cusps. Modular functions for $\Gamma_0(N)$ should thus be the meromorphic functions on this space.

They must satisfy the modularity condition for $\Gamma_0(N)$ and have nice behaviour at the cusps. Luckily, it is straightforward to calculate that all points of $\mathbb{Q} \cup \{\infty\}$ are equivalent modulo the action of $\mathrm{SL}_2(\mathbb{Z})$, thus if we want $f(\tau)$ to behave well at all the cusps, it is enough to ensure that $f(\gamma\tau)$ behaves well at infinity for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. This motivates the following definition.

Definition 6.5. A modular function of weight $k \in \mathbb{Z}_{\geq 0}$ for $\Gamma_0(N)$ is a meromorphic function $f\colon \mathbb{H} \to \mathbb{C}$ such that

(i) the map f satisfies the modularity condition with weight k for $\Gamma_0(N)$;

(ii) for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the function $f(\gamma\tau)$ is meromorphic at ∞, that is f is meromorphic at the cusps.

We define the field of modular functions of weight 0 for $\Gamma_0(N)$ to be $\mathcal{M}(N)$.

We saw that the space of modular functions for $\mathrm{SL}_2(\mathbb{Z})$ of weight 0 is $\mathbb{C}(j)$, we want to prove something similar for modular functions for $\Gamma_0(N)$ of weight 0.

Definition 6.6. For $N \in \mathbb{Z}_{>1}$, define $j_N(\tau) = j(N\tau)$.

Proposition 6.7. *For $N \in \mathbb{Z}_{>1}$, the function j_N is a modular function of weight 0 for $\Gamma_0(N)$.*

Proof. As j is holomorphic on $\mathbb{H}$, so is j_N. Note τ is a cusp if and only if $N\tau$ is, so j_N is meromorphic at the cusps as j is. Let

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

Then

$$\begin{aligned} j_N(\gamma\tau) &= j(N\gamma\tau) \\ &= j\left(\frac{aN\tau + bN}{c\tau + d}\right) \\ &= j\left(\begin{pmatrix} a & bN \\ c/N & d \end{pmatrix} N\tau\right) \\ &= j(N\tau) \\ &= j_N(\tau). \end{aligned}$$

□

We aim to show that $\mathcal{M}(N) = \mathbb{C}(j, j_N)$. Observe that $\mathcal{M}(N)$ is an extension of $\mathbb{C}(j)$.

Lemma 6.8. *The extension $\mathcal{M}(N)$ over $\mathbb{C}(j)$ is algebraic.*

Proof. Let $\{\gamma_1, \ldots, \gamma_n\} \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a set of right coset representatives for $\Gamma_0(N)$ so

$$\mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(N)\gamma_1 \sqcup \cdots \sqcup \Gamma_0(N)\gamma_n.$$

We may assume γ_1 is the identity.

Let f be a modular function of weight 0 for $\Gamma_0(N)$ and define $f_i(\tau) = f(\gamma_i\tau)$. Note that, for any $\rho \in \Gamma_0(N)\gamma_i$, we have $f(\rho\tau) = f_i(\tau)$. Hence, for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, we have

$$\{f_i(\gamma\tau) : i \in \{1, \ldots, n\}\} = \{f_i(\tau) : i \in \{1, \ldots, n\}\}$$

since multiplication on the left by γ simply permutes the cosets of $\Gamma_0(N)$. From this, we conclude that any symmetric polynomial in the f_i is a modular function for $\mathrm{SL}_2(\mathbb{Z})$ and, therefore, must be in $\mathbb{C}(j)$.

Now, define the polynomial

$$P(Y) = \prod_{i=1}^{n} (Y - f_i)$$

and, by the previous remark, note that $P \in \mathbb{C}(j)[Y]$. Observe that $P(f_1) = P(f) = 0$. Therefore, every modular function of weight 0 for $\Gamma_0(N)$ is a root of a polynomial over $\mathbb{C}(j)$, hence $\mathcal{M}(N)$ is an algebraic extension. □

Lemma 6.9. *The extension $\mathcal{M}(N)$ is finite over $\mathbb{C}(j)$ and has degree at most $n = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$.*

Proof. We first show $\mathcal{M}(N)$ is finitely generated. Aiming for a contradiction, assume $\mathcal{M}(N)$ is not finitely generated over $\mathbb{C}(j)$. We can then take some $g_1, \ldots, g_{n+1} \in \mathcal{M}(N)$ such that

$$\mathbb{C}(j) \subsetneq \mathbb{C}(j)(g_1) \subsetneq \cdots \subsetneq \mathbb{C}(j)(g_1, \ldots, g_{n+1}) \subsetneq \mathcal{M}(N).$$

Let $\mathbb{F} = \mathbb{C}(j)(g_1, \ldots, g_{n+1})$. By Lemma 6.8, $\mathbb{F}$ is a finitely generated, algebraic extension on $\mathbb{C}(j)$ so is finite of degree at least $n + 1$. By the primitive element theorem, there is some $g \in \mathbb{F}$ such that $\mathbb{F} = \mathbb{C}(j)(g)$. The minimal polynomial of g must therefore be of degree at least $n + 1$. However, in the proof of Lemma 6.8, we saw that g is the root of a polynomial of degree n. A contradiction.

Hence, $\mathcal{M}(N)$ is finitely generated over $\mathbb{C}(j)$. Again, by Lemma 6.8, this means $\mathcal{M}(N)$ is finite over $\mathbb{C}(j)$ and, by the above, the degree of $\mathcal{M}(N)$ over $\mathbb{C}(j)$ is at most n. □

Lemma 6.10. *The minimal polynomial of j_N has degree at least $n = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$.*

Proof. Let $m \in \mathbb{C}(j)[Y]$ be the minimal polynomial of j_N. Then $m(j(\tau), j_N(\tau)) = f(\tau)$ is the zero function. Hence,

$$0 = f(\gamma\tau) = m(j(\gamma\tau), j_N(\gamma\tau)) = m(j(\tau), j_N(\gamma\tau))$$

for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Hence, $j_N(\gamma\tau)$ is also a root of m. In particular, let $\{\gamma_1, \ldots, \gamma_n\} \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a set of right coset representatives for $\Gamma_0(N)$, assuming γ_1 is the identity. Then $j_N(\gamma_i\tau)$ is a root of m for each $i \in \{1, \ldots, n\}$. It is therefore enough to show that the $j_N(\gamma_i\tau)$ are distinct.

Aiming for a contradiction, assume we take some $i, k \in \{1, \ldots, n\}$ with $i \neq k$ such that $j_N(\gamma_i\tau) = j_N(\gamma_k\tau)$ for some $\tau \notin \{i, e^{2\pi i/3}, -e^{-2\pi i/3}\}$. We recall the fact that there is a domain $\mathcal{F}$ in $\mathbb{H}$ containing precisely one point from each coset of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. For a proof of this fact, see [Serre, 1973], Theorem VII.1. Using this, we can take $\alpha, \beta \in \mathrm{SL}_2(\mathbb{Z})$ such that $\alpha N\gamma_i\tau$ and $\beta N\gamma_k\tau$ both lie in $\mathcal{F}$. As j is injective on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$, and hence on $\mathcal{F}$, the fact that

$$j(\alpha N\gamma_i\tau) = j(N\gamma_i\tau) = j_N(\gamma_i\tau) = j_N(\gamma_k\tau) = j(\beta N\gamma_k\tau)$$

implies that $\alpha N\gamma_i = \beta N\gamma_k$.

We write the derived equality as

$$\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \gamma_i = \alpha^{-1}\beta \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \gamma_k.$$

Let

$$\alpha^{-1}\beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We then see that

$$\begin{aligned}\gamma_i\gamma_k^{-1} &= \begin{pmatrix} 1/N & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} a & b/N \\ cN & d \end{pmatrix}.\end{aligned}$$

Since $\gamma_i\gamma_k^{-1} \in \mathrm{SL}_2(\mathbb{Z})$, b/N is an integer and, as $cN \equiv 0 \mod N$, we see that $\gamma_i\gamma_k^{-1} \in \Gamma_0(N)$. However, this means γ_i and γ_k are in the same right coset of $\Gamma_0(N)$, a contradiction. □

Theorem 6.11. *We have that $\mathcal{M}(N) = \mathbb{C}(j, j_N)$.*

Proof. This follows immediately from Lemma 6.8, Lemma 6.9, and Lemma 6.10. □

6.3 The Modular Polynomial

We use what we have studied in the previous section to define the minimal polynomial of j_N over $\mathbb{C}(j)$. A small generalisation of this polynomial will give us an element of $\mathbb{Z}[X, Y]$. This polynomial will have the pair $(j(\mathfrak{a}), j(\mathfrak{a}))$ as a root where $\mathfrak{a}$ is a proper fractional ideal of an order in an imaginary quadratic field. It is then easy to show that $j(\mathfrak{a})$ is an algebraic integer.

By Lemma 6.10, the minimal polynomial of j_N has degree at least $n = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$. Also, in the proof of Lemma 6.8, we constructed a polynomial of degree n which a given modular form is the root of. We use this to define the minimal polynomial of j_N.

Definition 6.12. Let $\{\gamma_1, \ldots, \gamma_n\} \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a set of right coset representatives for $\Gamma_0(N)$. Set $j_{N,i}(\tau) = j_N(\gamma_i\tau)$. The modular polynomial of level N is

$$\Phi_N(Y) = \prod_{i=1}^{n}(Y - j_{N,i}) \in \mathbb{C}(j)[Y].$$

By the preceding discussion, $\Phi_N(Y)$ is the minimal polynomial of j_N over $\mathbb{C}(j)$. Let us study this polynomial more closely. We will first show that it's coefficients are, in fact, polynomials in j but, before this, we need an auxiliary result.

Lemma 6.13. *Let f be a modular function for $\mathrm{SL}_2(\mathbb{Z})$ of weight 0. Then $f \in \mathbb{C}(j)$ so, if f is holomorphic on $\mathbb{H}$, $f = P(j)$ for some $P \in \mathbb{C}[X]$. We claim that the degree of P is the order of the pole of f at ∞ and the coefficients of P are $\mathbb{Z}$-linear combinations of the coefficients in the q-series of f.*

Proof. Let R be the order of the pole of f at ∞. We induct on R. If $R = 0$, f is a modular form of weight 0 so constant and the result is immediate.

Suppose the claim holds for all modular functions with a pole of order $R - 1$ at ∞. We can write

$$f = \sum_{n=-R}^{\infty} a_n q^n$$

for some $a_n \in \mathbb{C}$. Observe that $f - a_{-R}j^R$ then has a pole of order $R - 1$ at ∞ so, by the inductive hypothesis

$$f - a_{-R}j^R = \sum_{i=0}^{R-1} c_i j^i.$$

As the coefficients of j in its q-series are integers, the result follows by induction. □

Lemma 6.14. *The coefficients in $\Phi_N(Y)$ are holomorphic on $\mathbb{H}$ and hence are polynomials in j.*

Proof. Let $f(\tau)$ be a coefficient. We already know it is a modular function of weight 0 for $\mathrm{SL}_2(\mathbb{Z})$ since, by the proof of Lemma 6.8, $f(\tau)$ is a symmetric polynomial in $j_N(\gamma_i\tau)$ where $\{\gamma_1, \ldots, \gamma_n\} \subseteq \mathrm{SL}_2(\mathbb{Z})$ are a set of right coset representatives for $\Gamma_0(N)$. Note, however, that the $j_N(\gamma_i\tau)$ are holomorphic on $\mathbb{H}$ and hence so is $f(\tau)$. The fact that f is a polynomial in j follows from Lemma 6.13. □

By writing out every coefficient in $\Phi_N(Y)$ as a polynomial in j and replacing each instance of j with an indeterminant X, we define a new polynomial $\Phi(X, Y) \in \mathbb{C}[X, Y]$. In an abuse of language, we also call this the modular polynomial of level N.

We aim to show that $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$. Our idea is to show that the coefficients of $\Phi_N(Y)$ are modular functions for $\mathrm{SL}_2(\mathbb{Z})$ of weight 0 which are holomorphic on $\mathbb{H}$ and, hence, are polynomials in j. We will then show that these modular functions have integer coefficients in their q-series. Combining this with the following lemma will imply the result.

Theorem 6.15. *We have that $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$.*

Proof. This is a fact that holds true in general, but we will only prove it for the case where N is prime. The reason for this is that, in this instance, the coset representatives are very nice. Furthermore, this is the only case we will actually need for proving our main results.

It is not too hard to show that, if N is prime, then

$$\mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(N) \sqcup \Gamma_0(N)S \sqcup \Gamma_0(N)ST \sqcup \cdots \sqcup \Gamma_0(N)ST^{N-1}$$

where

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Observe that

$$\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} S = \begin{pmatrix} 0 & -N \\ 1 & 0 \end{pmatrix} = S \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}.$$

Hence,

$$\begin{aligned} j_N(ST^k\tau) &= j\left(\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} ST^k\tau\right) \\ &= j\left(S\begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\tau\right) \\ &= j\left(\begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\tau\right) \\ &= j\left(\frac{\tau + k}{N}\right). \end{aligned}$$

Writing

$$e^{2\pi i\left(\frac{\tau+k}{N}\right)} = \zeta_N^k q^{1/N},$$

where ζ_N is the Nth root of unity and $q = e^{2\pi i\tau}$, using the q-series for j, we find

$$j_N(ST^k\tau) = \zeta_N^{-k} q^{-1/N} + \sum_{r=0}^{\infty} a_r \zeta_N^{kr} q^{r/N}$$

for some $a_r \in \mathbb{Z}$.

We thus see that $j_N(ST^k\tau) \in \mathbb{Q}(\zeta_N)((q^{1/N}))$. Observe that the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ permutes the set $\left\{j_N(ST^k\tau) : k \in \{0,\dots,N-1\}\right\}$ and fixes $j_N(\tau)$. Thus, any symmetric polynomial in $j_N(\tau)$ and the $j_N(ST^k\tau)$ must lie in $\mathbb{Q}((q^{1/N}))$. In particular, any coefficient f of $\Phi_N(Y)$ lies in $\mathbb{Q}((q^{1/N}))$. However, f is a modular function for $\mathrm{SL}_2(\mathbb{Z})$ so $f \in \mathbb{Q}((q))$.

Finally, observe that the coefficients in the q-series of $j_N(\tau)$ and the $j_N(ST^k\tau)$ are algebraic integers, so must the coefficients of the q-series of f. These coefficients lie in $\mathbb{Q}$ by the above, so they must be integers. By Lemma 6.13, f is a polynomial in j with coefficients in $\mathbb{Z}$, that is $f \in \mathbb{Z}[j]$. Hence, $\Phi_N(X,Y) \in \mathbb{Z}[X,Y]$. □

We aim to show that certain values of the j-invariant are roots of the modular polynomial in order to show that these values are algebraic integers. For this, we will show that the leading coefficient of $\Phi_N(X,X)$ is -1.

Proposition 6.16. *If $N \in \mathbb{Z}_{>1}$ is prime then the leading coefficient of $\Phi_N(X,X)$ is -1.*

Proof. Recall that

$$\Phi_N(j(\tau),Y) = (Y - j(N\tau)) \prod_{k=0}^{N-1} (Y - j(NST^k\tau)).$$

Hence,

$$\Phi_N(j(\tau),j(\tau)) = (j(\tau) - j(N\tau)) \prod_{k=0}^{N-1} (j(\tau) - j(NST^k\tau)).$$

In the proof of Theorem 6.15, we found that

$$\begin{aligned} j(N\tau) &= q^{-N} + \cdots \\ j(NST^k\tau) &= \zeta_N^{-k} q^{-1/N} + \cdots . \end{aligned}$$

Meaning,

$$\begin{aligned} j(\tau) - j(N\tau) &= -q^{-N} + q^{-1} + \cdots \\ j(\tau) - j(NST^k\tau) &= q^{-1} + \zeta_N^{-k} q^{-1/N} + \cdots . \end{aligned}$$

We thus deduce that the q-series of $\Phi_N(j(\tau),j(\tau))$ begins with

$$-q^{-2N} + \cdots .$$

Therefore, the leading term of $\Phi_N(X,X)$ must be $-X^{2N}$. □

6.4 Roots of the Modular Polynomial

We will begin to study the roots of $\Phi_N(X,Y)$ and begin to relate this back to lattices and elliptic curves with CM. It turns out that $\Phi_N(u,v) = 0$ if and only if $u = j(\Lambda_1)$ and $v = j(\Lambda_2)$ where Λ_2 is homothetic to a sublattice of Λ_1 with the property that Λ_1/Λ_2 is a cyclic group of order N.

Proposition 6.17. *Sublattices of $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ of index $m \in \mathbb{Z}_{\geq 1}$ are in bijection with the set*

$$S_m = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_{2\times 2}(\mathbb{Z}) : \ ad = m,\ a \geq 1,\ 0 \leq b < d \right\}$$

under the map

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto (a\omega_1 + b\omega_2)\mathbb{Z} + (d\omega_1)\mathbb{Z}.$$

Proof. See, for instance, [Serre, 1973], Lemma VII.2. □

From this result, we see that, if $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$, then sublattices of Λ of index n have the form

$$d\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\tau\mathbb{Z} + \mathbb{Z}\right)$$

where $ad = m$, $a \geq 1$ and $0 \leq b < d$. In particular, if m is prime, the sublattices of index n are

$$\mathbb{Z} + m\tau\mathbb{Z} \text{ and } m\mathbb{Z} + (k + \tau)\mathbb{Z}$$

where $0 \leq k < m$.

Theorem 6.18. *Let $N \in \mathbb{Z}_{\geq 1}$ be prime. For $u, v \in \mathbb{C}$, $\Phi_N(u, v) = 0$ if and only if $u = j(\Lambda_1)$ and $v = j(\Lambda_2)$ where Λ_1 is a lattice and Λ_2 is homothetic to a sublattice of Λ_1 of index N.*

Proof. Recall, for each $u \in \mathbb{C}$, there is a lattice

$$\Lambda_1 = \mathbb{Z} + \tau\mathbb{Z}$$

such that $j(\Lambda_1) = j(\tau) = u$. Also recall that

$$\Phi_N(j(\tau), Y) = (Y - j(N\tau)) \prod_{k=0}^{N-1} (Y - j(NST^k\tau))$$

and that

$$j(NST^k\tau) = j\left(\frac{\tau + k}{N}\right)$$

by the proof of Theorem 6.15. So $v \in \mathbb{C}$ such that $\Phi_N(u, v) = 0$ if and only if

$$v = j\left(\frac{\tau + k}{N}\right) \text{ or } v = j(N\tau).$$

Equivalently,

$$v = j\left(\mathbb{Z} + \frac{k + \tau}{N}\mathbb{Z}\right) \text{ or } v = j\left(\mathbb{Z} + N\tau\mathbb{Z}\right).$$

From this and the preceding discussion, the result follows. □

As mentioned, an analogous result holds for arbitrary N with the extra condition that Λ_1/Λ_2 is cyclic (which of course is always the case if N is prime). For a full proof of this, we recommend the reader consult [Sutherland, 2022a]. For our purposes, we will only need to consider the case where N is prime.

We now want to focus on the case where we have a lattice $\mathfrak{a}$ which is a proper fractional ideal of an order $\mathcal{O}$ in an imaginary quadratic field K. We assume $\mathfrak{a} \subseteq \mathcal{O}$, as we will only be concerned with $j(\mathfrak{a})$ and we are free to replace $\mathfrak{a}$ by a homothetic lattice. Let $\mathfrak{b}$ be a proper $\mathcal{O}$-ideal so $\mathfrak{ab}$ is a sublattice of $\mathfrak{a}$. Considering the exact sequence

$$0 \to \frac{\mathfrak{a}}{\mathfrak{ab}} \to \frac{\mathcal{O}}{\mathfrak{ab}} \to \frac{\mathcal{O}}{\mathfrak{a}} \to 0$$

we observe that

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

so $\mathfrak{ab}$ is a sublattice of $\mathfrak{a}$ of index $N(\mathfrak{b})$. In particular, if $\mathfrak{b} = \beta\mathcal{O}$ then $\beta\mathfrak{a}$ is a sublattice of index $N(\beta)$. By Corollary 5.34, we can choose a β with norm a prime p, so applying Theorem 6.18 shows us that

$$\Phi_p(j(\beta\mathfrak{a}), j(\mathfrak{a})) = 0.$$

However, $\beta\mathfrak{a}$ is homothetic to $\mathfrak{a}$ so

$$\Phi_p(j(\mathfrak{a}), j(\mathfrak{a})) = 0$$

and therefore $j(\mathfrak{a})$ is an algebraic integer. We summarise this with the following theorem.

Theorem 6.19. *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. If $\mathfrak{a}$ is a proper fractional ideal of $\mathcal{O}$ then $j(\mathfrak{a})$ is an algebraic integer.*

Corollary 6.20. *Let $d \in \mathbb{Z}$ be square-free with $d \neq 0, 1$. Then $j(\sqrt{d})$ is an algebraic integer.*

Using more class field theory, one can also prove the following, extremely powerful statement:

Theorem 6.21. *Let K be an imaginary quadratic field and $\mathcal{O}$ an order of K. For any proper fractional ideal $\mathfrak{a}$ of $\mathcal{O}$, the field $K(j(\mathfrak{a}))$ is the ring class field of $\mathcal{O}$. Furthermore, for a proper fractional ideal $\mathfrak{b}$ of $\mathcal{O}$, let the map $\sigma_{\mathfrak{b}}$ be defined by $\sigma_{\mathfrak{b}}(j(\mathfrak{a})) = j(\overline{\mathfrak{b}}\mathfrak{a})$. Then, the map*

$$\mathrm{Cl}(\mathcal{O}) \to \mathrm{Gal}(K(j(\mathfrak{a}))/K)$$

defined by

$$\mathfrak{b} \mapsto \sigma_{\mathfrak{b}}$$

is well-defined and is an isomorphism.

Proof. For the first part, see, for instance, [Cox, 2013], Theorem 11.1. For the explicit isomorphism, see Corollary 11.37. □

Corollary 6.22. *Let K be an imaginary quadratic field, $\mathcal{O}$ an order of K and $\mathfrak{a}$ a proper fractional ideal of $\mathcal{O}$. Then the degree of $j(\mathfrak{a})$ is $|\mathrm{Cl}(\mathcal{O})|$.*

Proof. By Theorem 6.21, we know $L = K(j(\mathfrak{a}))$ is the ring class field of $\mathcal{O}$. Thus,

$$\mathrm{Gal}(L/K) \cong \mathrm{Cl}(\mathcal{O}).$$

By the fundamental theorem of Galois theory, the degree of L/K is therefore $|\mathrm{Cl}(\mathcal{O})|$ and hence the degree of the minimal polynomial of $j(\mathfrak{a})$ is $|\mathrm{Cl}(\mathcal{O})|$ as required. □

7 Calculating Examples

7.1 Class Number 1

We know that if K is an imaginary quadratic field and $\mathcal{O}$ an order in K then, for any proper fractional $\mathcal{O}$-ideal $\mathfrak{a}$, $j(\mathfrak{a})$ is an algebraic integer of degree $|\mathrm{Cl}(\mathcal{O})|$. In particular, if $|\mathrm{Cl}(\mathcal{O})| = 1$ then $j(\mathfrak{a})$ is an integer. To look at a few cases of this, consider the following classical theorem of Stark-Heegner.

Theorem 7.1. *Let $d \in \mathbb{Z}$ be square-free and $K = \mathbb{Q}(\sqrt{d})$. If $d < 0$ then $\mathcal{O}_K$ is a PID if and only if*

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Proof. The first generally accepted proof is by Stark in [Stark, 1967]. □

Thus, if we let $K = \mathbb{Q}(\sqrt{d})$ with d one of the above then $j(\mathcal{O}_K)$ is an integer. We can verify this computationally and find

τ	$j(\tau)$
$\sqrt{-1}$	1728
$\sqrt{-2}$	8000
$\frac{1+\sqrt{-3}}{2}$	0
$\frac{1+\sqrt{-7}}{2}$	-3375
$\frac{1+\sqrt{-11}}{2}$	-32768
$\frac{1+\sqrt{-19}}{2}$	-884736
$\frac{1+\sqrt{-43}}{2}$	-884736000
$\frac{1+\sqrt{-67}}{2}$	-147197952000
$\frac{1+\sqrt{-163}}{2}$	$-262537412640768000.$

These calculations were done using the Sage software package, [Stein et al., 2024], specifically the calculation is done using the `elliptic_j()` function, written by John Cremona, which also relies on the GMP library, [Granlund et al., 2023], and the MPFR library, [Hanrot et al., 2023].

As you would expect, computing these values is not done exactly, and we always end up with some kind of error. Luckily, for a small enough error, the fact that these values are integers allows us to very easily find the exact values. This can only work in the case where $|\mathrm{Cl}(\mathcal{O})| = 1$, otherwise this method won't be able to give us an exact value. We will, therefore, have to calculate them in another way.

7.2 Weber Functions

We will use the approach given in [Cox, 2013] to calculate $j(\sqrt{-14})$ and then adapt this methodology to compute $j(\sqrt{-46})$ and $j(\sqrt{-142})$. This is originally based on calculations by Weber where the key idea is to consider 'simpler' functions, known as Weber functions, which also generate the class field and using these to find values of the j-function. We will briefly describe some of the theory of these Weber functions.

Recall that

$$j = \frac{E_4^3}{\Delta}$$

and so a natural, 'simpler' function to consider may be the cube root of j, removing the cuber from the numerator. For this, we need to be able to take the cube root of Δ. This is no problem as Δ is non-vanishing and holomorphic on $\mathbb{H}$. The question then becomes, which cube root to take? The definition of Δ is ultimately derived from the lattice functions G_4 and G_6 where

$$G_k(\Lambda) = \sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{w^k}.$$

If we let $\overline{\Lambda}$ be the lattice with points the conjugate of points in Λ then we can easily see from the definition that

$$G_k(\overline{\Lambda}) = \overline{G_k(\Lambda)}.$$

Hence, if $\Lambda = \mathbb{Z} + ix\mathbb{Z}$ for some $x \in \mathbb{R}$, then $\Lambda = \overline{\Lambda}$ and it must be that $G_k(\Lambda)$ is real. From this, it follows that $\Delta(ix) \in \mathbb{R}$. We will therefore choose $\sqrt[3]{\Delta}$ to also be real when evaluated on the imaginary axis.

Definition 7.2. Let

$$\gamma_2 = \frac{E_4}{\sqrt[3]{\Delta}}$$

where we take the cube root of Δ to be real on $i\mathbb{R}_{>0}$.

We want to show that γ_2 can also be used to generate ring class fields. However, one can check that $\gamma_2(\tau+1) = \zeta_3^{-1}\gamma_2(\tau)$ (where $\zeta_3 = e^{2\pi i/3}$) so we need to take care with where we evaluate γ_2.

Theorem 7.3. *Let K be an imaginary quadratic field and $\mathcal{O}$ an order of K with discriminant D. If 3 does not divide D write $\mathcal{O} = \mathbb{Z} + \tau_0\mathbb{Z}$ where*

$$\tau_0 = \begin{cases} \sqrt{D/4}, & D \equiv 0 \mod 4 \\ \frac{3+\sqrt{D}}{2}, & D \equiv 1 \mod 4. \end{cases}$$

Then $\gamma_2(\tau_0)$ is an algebraic integer; $K(\gamma_2(\tau_0)) = K(j(\tau_0))$ (and hence is the ring class field of $\mathcal{O}$); and $\mathbb{Q}(\gamma_2(\tau_0)) = \mathbb{Q}(j(\tau_0))$.

Proof. See, for instance, [Cox, 2013], Theorem 12.2. □

We are not done with simplifications yet as we will now rewrite γ_2 in terms of functions which we can more easily evaluate. To slightly motivate where these functions come from, we first introduce the Dedekind eta function.

Definition 7.4. Define $\eta\colon \mathbb{H} \to \mathbb{C}$ by

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

where $q = e^{2\pi i\tau}$.

Note that the infinite product in this definition does indeed converge and, in fact, converges absolutely and uniformly on compact subsets of $\mathbb{H}$ since $|q| < 1$ if $\tau \in \mathbb{H}$. Hence, η is holomorphic on $\mathbb{H}$.

Proposition 7.5. *We have that*

(i) $\eta(\tau+1) = e^{\pi i/12}\eta(\tau)$;

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

where the square root is chosen such that $\sqrt{-i\tau} = 1$ for $\tau = i$.

Proof. For the first part, note

$$\eta(\tau+1) = e^{\pi i\tau/12}e^{\pi i/12}\prod_{n=1}^{\infty}(1-e^{2n\pi i\tau}e^{2n\pi i}) = e^{\pi i/12}\eta(\tau)$$

since $e^{2n\pi i} = 1$ for $n \in \mathbb{Z}$.

For a proof of the second identity see [Apostol, 1990], Theorem 3.1. □

You will notice that these identities are very similar to those satisfied by a modular form. The following theorem confirms why this is the case.

Theorem 7.6. *We have*

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

Proof. See, for instance, [Apostol, 1990], Theorem 3.3. □

The function η is known as the Dedekind eta function, and we will use it to define three functions known as the Weber functions. Due to the close link between η and Δ, we will be able to use the Weber functions to calculate $\gamma_2(\tau)$, and hence $j(\tau)$, for some nice values of τ.

Definition 7.7. We define the Weber functions $\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2 \colon \mathbb{H} \to \mathbb{C}$ by

$$\begin{aligned}\mathfrak{f}(\tau) &= \zeta_{48}^{-1} \frac{\eta\left(\frac{\tau+1}{2}\right)}{\eta(\tau)} \\ \mathfrak{f}_1(\tau) &= \frac{\eta\left(\frac{\tau}{2}\right)}{\eta(\tau)} \\ \mathfrak{f}_2(\tau) &= \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)},\end{aligned}$$

where $\zeta_{48} = e^{2\pi i/48}$. Equivalently,

$$\begin{aligned}\mathfrak{f}(\tau) &= q^{-1/48} \prod_{n=1}^{\infty} (1 + q^{n-1/2}) \\ \mathfrak{f}_1(\tau) &= q^{-1/48} \prod_{n=1}^{\infty} (1 - q^{n-1/2}) \\ \mathfrak{f}_2(\tau) &= \sqrt{2} q^{1/24} \prod_{n=1}^{\infty} (1 + q^n).\end{aligned}$$

These functions may seem to come out of nowhere, so we will spend a brief bit of time trying to make them appear less arbitrary. We want to find some function $\mathfrak{g} \colon \mathbb{H} \to \mathbb{C}$ so that, for some $F \in \mathbb{C}(X)$, we have

$$j(\tau) = F(\mathfrak{g}(\tau))$$

for all $\tau \in \mathbb{H}$ and so that $\mathfrak{g}(\tau)$ is easier to compute than $j(\tau)$. Now, it is likely that $\mathfrak{g}$ is not unique, so let S be the set of all functions $\mathfrak{g}' \colon \mathbb{H} \to \mathbb{C}$ where we have

$$j(\tau) = F(\mathfrak{g}'(\tau))$$

for all $\tau \in \mathbb{H}$. Since for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, we have $j(\gamma\tau) = j(\tau)$, it follows that $F(\mathfrak{g}'(\gamma\tau)) = j(\tau)$. That is, the function $\tau \mapsto \mathfrak{g}'(\gamma\tau)$ must be in S. Hence, S is closed under the action of $\mathrm{SL}_2(\mathbb{Z})$ defined by taking a function $h \colon \mathbb{H} \to \mathbb{C}$ to the function $\tau \mapsto h(\gamma\tau)$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. If we can find an S satisfying this requirement with something more relating it to j then perhaps we can recover j from S.

One of the more obvious places to start is with some expressions involving η; we already know this links to j and, since it is very 'close' to being a modular form, it should be very easy to see how these expressions change under the action of $\mathrm{SL}_2(\mathbb{Z})$, moreover, it is defined in terms of quite a simple infinite product, so we should be able to get some relatively 'simple' functions out of it. Since $\eta(\tau + 1) = e^{\pi i/12}\eta(\tau)$ and $\eta(-1/\tau) = \sqrt{-i\tau}\eta(\tau)$, we might want to take some quotients involving η to deal with these multiplication factors. Clearly, $\eta(\tau)/\eta(\tau)$ won't do us much good, but maybe something like $\eta(2\tau)/\eta(\tau)$ would help. It is this line of thinking that might lead us to consider the set $S = \{-\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2\}$. Indeed, one can verify that

$$-\mathfrak{f}(-1/\tau) = -\mathfrak{f}(\tau),\ \mathfrak{f}_1(-1/\tau) = \mathfrak{f}_2(\tau),\ \text{and}\ \mathfrak{f}_2(-1/\tau) = \mathfrak{f}_1(\tau).$$

However, we find

$$-\mathfrak{f}(\tau + 1) = \zeta_{48}^{-1}\mathfrak{f}_1(\tau),\ \mathfrak{f}_1(\tau + 1) = \zeta_{48}^{-1}\mathfrak{f}_1(\tau),\ \text{and}\ \mathfrak{f}_2(\tau + 1) = \zeta_{24}\mathfrak{f}_2(\tau)$$

where $\zeta_k = e^{2\pi i/k}$. If we instead set $S = \{-\mathfrak{f}^{24}, \mathfrak{f}_1^{24}, \mathfrak{f}_2^{24}\}$ then we see that S is closed under the action of $\mathrm{SL}_2(\mathbb{Z})$. Thankfully, we can also derive a relation between elements of S that yields j, which we give in the following theorem alongside a summary of the identities satisfied by the Weber functions.

Theorem 7.8. *We have*

(i) $\mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) = \sqrt{2}$;

(ii) $\mathfrak{f}_1(2\tau)\mathfrak{f}_2(\tau) = \sqrt{2}$;

(iii) $\mathfrak{f}(\tau+1) = \zeta_{48}^{-1}\mathfrak{f}_1(\tau)$;

(iv) $\mathfrak{f}_1(\tau+1) = \zeta_{48}^{-1}\mathfrak{f}(\tau)$;

(v) $\mathfrak{f}_2(\tau+1) = \zeta_{24}\mathfrak{f}_2(\tau)$;

(vi) $\mathfrak{f}(-1/\tau) = \mathfrak{f}(\tau)$;

(vii) $\mathfrak{f}_1(-1/\tau) = \mathfrak{f}_2(\tau)$;

(viii) $\mathfrak{f}_2(-1/\tau) = \mathfrak{f}_1(\tau)$;

(ix)

$$\gamma_2(\tau) = \frac{\mathfrak{f}(\tau)^{24} - 16}{\mathfrak{f}(\tau)^8} = \frac{\mathfrak{f}_1(\tau)^{24} + 16}{\mathfrak{f}_1(\tau)^8} = \frac{\mathfrak{f}_2(\tau)^{24} + 16}{\mathfrak{f}_2(\tau)^8},$$

where $\zeta_k = e^{2\pi i/k}$.

Proof. See, for instance, [Cox, 2013], Theorem 12.17 and Corollary 12.19. □

The Weber functions are also very useful for calculations as their q-series converge rather rapidly. This makes calculating approximations for them much simpler, especially by hand as Weber would have been doing.

In some cases, Weber functions are enough to generate the ring class field.

Theorem 7.9. *Let $m \in \mathbb{Z}_{>0}$ be such that 3 does not divide m and $m \equiv 6 \mod 8$. Set $K = \mathbb{Q}(\sqrt{-m})$ and let $\mathcal{O} = \mathbb{Z}[\sqrt{-m}]$. Then $\mathfrak{f}_1(\sqrt{-m})^2$ is an algebraic integer and $K(\mathfrak{f}_1(\sqrt{-m})^2)$ is the ring class field of $\mathcal{O}$.*

Proof. See, for instance, [Cox, 2013], Theorem 12.24. □

7.3 Calculating $j(\sqrt{-14})$

We will now go through the steps for calculating $j(\sqrt{-14})$ as given in [Cox, 2013], using techniques originally developed by Weber. In later sections, we will adapt these techniques to calculate a couple more examples.

For this section, fix $K = \mathbb{Q}(\sqrt{-14})$ and $L = K(j(\sqrt{-14})$, the Hilbert class field of $\mathcal{O}_K$.

The idea for the calculation is to first find $\alpha = \mathfrak{f}_1(\sqrt{-14})^2$ and then, using Theorem 7.8, we can find $\gamma_2(\sqrt{-14})$ and hence $j(\sqrt{-14})$. To find α, we will show that $K(\sqrt{2})$ is an intermediate field of L/K and that $\alpha + \frac{2}{\alpha}$ lies in this field. The fact that α is real and an algebraic integer (from Theorem 7.9) allows us to deduce that $\alpha + \frac{2}{\alpha} = a + b\sqrt{2}$ for some $a, b \in \mathbb{Z}$. We will then argue that a and b must both be positive. As the set $S = \left\{a + b\sqrt{2} : \ a, b \in \mathbb{Z}_{>0}\right\}$ is discrete in $\mathbb{R}$, if we can approximate $\alpha + \frac{2}{\alpha}$ to sufficient accuracy, only one element of S will be within this error range and this will give us an explicit value for α.

A key preliminary step is to find $\mathrm{Gal}(L/K) \cong \mathrm{Cl}(\mathcal{O}_K)$. This is a simple exercise but requires more algebraic number theory than we have developed. We therefore simply assert that $\mathrm{Cl}(\mathcal{O}_K) \cong C_4$, the cyclic group of order 4.

The first step in the calculation is to show that

$$K \subsetneq K(\sqrt{2}) \subsetneq L$$

as claimed. It is straightforward to check that $\sqrt{2} \notin K = \mathbb{Q}(\sqrt{-14})$ so $K \subsetneq K(\sqrt{2})$. Furthermore, as $[K(\sqrt{2}) : K] = 2$, we know $K(\sqrt{2})/K$ is an abelian extension and that $K(\sqrt{2}) \neq L$ (as L/K is a degree 4 extension). Thus, by Theorem 5.30, to show $K(\sqrt{2}) \subsetneq L$, we need only show that all primes of K are unramified in $K(\sqrt{2})$. Let $\mathfrak{p}$ be a prime of K. We consider two cases.

First, consider when $2 \notin \mathfrak{p}$. We will use Theorem 5.27. Note, $\sqrt{2}$ is a root of $m(X) = X^2 - 2$ and, as $\sqrt{2} \notin K$, it can not be a root of a linear polynomial over K so m is the minimal polynomial of $\sqrt{2}$ over K. The discriminant of m is 8 and, as $2 \notin \mathfrak{p}$, neither is 8. It follows that m is separable mod $\mathfrak{p}$ and hence we can apply Theorem 5.27 to show us that $\mathfrak{p}$ is unramified.

Now, consider when $2 \in \mathfrak{p}$. Note then that $-7 \notin \mathfrak{p}$ as otherwise $\mathfrak{p} = \mathcal{O}_K$, a contradiction. Also note that

$$K(\sqrt{2}) = \mathbb{Q}(\sqrt{-14}, \sqrt{2}) = K(\sqrt{-7}) = K\left(\frac{-1+\sqrt{-7}}{2}\right).$$

See that $\frac{-1+\sqrt{-7}}{2}$ is a root of $r(X) = X^2 + X + 2$ and, for similar reasoning as before, r must thus be the minimal polynomial of $\frac{-1+\sqrt{-7}}{2}$. See that r has discriminant $-7 \notin \mathfrak{p}$ and hence r is separable mod $\mathfrak{p}$. As with the previous case, we therefore conclude that $\mathfrak{p}$ is unramified in $K(\sqrt{2})$.

We therefore have

$$K \subsetneq K(\sqrt{2}) \subsetneq L$$

as desired.

For the next step, let $\sigma \in \mathrm{Gal}(L/K)$ be the unique element of order 2. It follows that $\alpha + \sigma(\alpha)$ is fixed by the subgroup generated by σ. This is the only proper, non-trivial subgroup of $\mathrm{Gal}(L/K)$ and so the field fixed by σ must be $K(\sqrt{2})$ by the fundamental theorem of Galois theory. Hence, $\alpha+\sigma(\alpha) \in K(\sqrt{2})$. If we can write $\sigma(\alpha)$ in terms of α, then, hopefully, as α is a real algebraic integer (by Theorem 7.9 and the product formula for $\mathfrak{f}_1$), we should be able to show that $\alpha + \sigma(\alpha) \in \mathbb{Z}[\sqrt{2}]$. We will thus aim to show that $\sigma(\alpha) = \frac{2}{\alpha}$. The first thing we will prove is that $\sigma(\alpha) = \mathfrak{f}_2\left(\frac{\sqrt{-14}}{2}\right)^2$. In order to do this, we will need the following fact.

Proposition 7.10. *The function $\mathfrak{f}_1(8\tau)^6$ is a modular function of weight 0 for $\Gamma_0(32)$ which is holomorphic and the coefficients of its q-series are integers. Hence, for some $R \in \mathbb{Q}(X, Y)$, we have*

$$\mathfrak{f}_1(8\tau)^6 = R(j(\tau), j(32\tau)).$$

Proof. See, for instance, [Cox, 2013] Proposition 12.25. Notice how the last part of the statement is a refinement of Theorem 6.11. □

Using the above, we see that

$$\mathfrak{f}_1(\sqrt{-14})^6 = R(j(\mathfrak{b}), j(\mathcal{O}'))$$

where $\mathcal{O}' = \mathbb{Z} + 4\sqrt{-14}\mathbb{Z}$ is an order in K and $\mathfrak{b} = 8\mathbb{Z} + \sqrt{-14}\mathbb{Z}$ is a fractional ideal of $\mathcal{O}'$. One can check that $\mathfrak{b}$ is in fact a proper fractional ideal. Hence, if we let L' be the ring class field of $\mathcal{O}'$, $\mathfrak{b}$ determines an element of $\mathrm{Cl}(\mathcal{O}')$ and hence an element $\sigma_{\mathfrak{b}}$ of $\mathrm{Gal}(L'/K)$, as described in Theorem 6.21. Observe that, as $\overline{\mathfrak{b}} = \mathfrak{b}$,

$$\sigma_{\mathfrak{b}}(j(\mathfrak{b})) = j(\overline{\mathfrak{b}}\mathfrak{b}) = j(\mathfrak{b}^2) = j(2\mathcal{O}') = j(\mathcal{O}')$$

and hence

$$\sigma_{\mathfrak{b}}(\mathfrak{f}_1(\sqrt{-14})^6) = R(j(\mathcal{O}'), j(\mathfrak{b})).$$

Recall from Theorem 7.8 that $\mathfrak{f}_2(\tau) = \mathfrak{f}_1\left(-\frac{1}{\tau}\right)$. Writing

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

this relation becomes $\mathfrak{f}_2(\tau) = \mathfrak{f}_1(S\tau)$ and so

$$\mathfrak{f}_2(\tau)^6 = \mathfrak{f}_1(S\tau)^6 = R\left(j\left(\frac{S\tau}{8}\right), j(4S\tau)\right) = R(j(\mathbb{Z} + 8\tau\mathbb{Z}), j(4\mathbb{Z} + \tau\mathbb{Z})).$$

In particular,

$$\mathfrak{f}_2\left(\frac{\sqrt{-14}}{2}\right)^6 = R(j(\mathbb{Z} + 4\sqrt{-14}\mathbb{Z}), j(8\mathbb{Z} + \sqrt{-14}\mathbb{Z})) + R(j(\mathcal{O}'), j(\mathfrak{b})) = \sigma_{\mathfrak{b}}(\mathfrak{f}_1(\sqrt{-14})^6).$$

Now, as $\mathfrak{b}^2 = 2\mathcal{O}'$, we note that $\sigma_{\mathfrak{b}}$ must restrict to σ on L. Therefore,

$$\sigma(\alpha)^3 = \mathfrak{f}_2\left(\frac{\sqrt{-14}}{2}\right)^6.$$

Taking cube roots,

$$\sigma(\alpha) = \zeta_3^r \mathfrak{f}_2\left(\frac{\sqrt{-14}}{2}\right)^2$$

for some $r \in \{0, 1, 2\}$ where $\zeta_3 = e^{2\pi i/3}$. However,

$$\alpha\sigma(\alpha) = \zeta_3^r \mathfrak{f}_1(\sqrt{-14})^2 \mathfrak{f}_2\left(\frac{\sqrt{-14}}{2}\right) = 2\zeta_3^r$$

by Theorem 7.8 and $\alpha\sigma(\alpha)$ is fixed by σ so lies in $K(\sqrt{2})$, meaning that $\zeta_3^r \in K(\sqrt{2})$, so it must be that $r = 0$ and

$$\sigma(\alpha) = \mathfrak{f}_2\left(\frac{\sqrt{-14}}{2}\right)^2.$$

Now, as $\alpha\sigma(\alpha) = 2$, we find that $\sigma(\alpha) = \frac{2}{\alpha}$. Therefore, if we let

$$\beta = \alpha + \frac{2}{\alpha},$$

we see that β is fixed by σ and so lies in $K(\sqrt{2})$. By looking at the product formula for $\mathfrak{f}_1$, we note that $\alpha \in \mathbb{R}$ so $\beta \in \mathbb{Q}(\sqrt{2})$. Moreover, by Theorem 7.9, α is an algebraic integer. As $\sigma(\alpha)$ is a root of the minimal polynomial of α, it must be an algebraic integer too. We therefore find that $\beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}]$, and hence

$$\beta = a + b\sqrt{2}$$

for some $a, b \in \mathbb{Z}$.

The next step in our calculation is to show that a and b must be positive. Multiplying both sides of

$$\alpha + \frac{2}{\alpha} = a + b\sqrt{2}$$

by α shows that α is a real root of

$$X^2 - (a + b\sqrt{2})X + 2$$

which means that the discriminant $(a + b\sqrt{2})^2 - 8$ is non-negative. Thus,

$$(a + b\sqrt{2})^2 \geq 8.$$

Now, let ρ be a generator for $\mathrm{Gal}(L/K)$ so $\rho^2 = \sigma$. It follows that $\rho(\sqrt{2}) = -\sqrt{2}$ so

$$\rho(\beta) = \rho(\alpha) + \frac{2}{\rho(\alpha)} = a - b\sqrt{2}.$$

We claim that $\rho(\alpha) \notin \mathbb{R}$ and hence the polynomial

$$X^2 - (a - b\sqrt{2})X + 2$$

has negative discriminant, that is

$$(a - b\sqrt{2})^2 < 8.$$

Combining the two inequalities yields

$$4ab\sqrt{2} > 0.$$

From the product formula for $\mathfrak{f}_1$, $\alpha > 0$ and therefore this implies $a, b > 0$.

How do we know $\rho(\alpha)$ is not real? This would imply $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois extension and this can't happen due to [Cox, 2013], Lemma 9.3.

We can now consider the set

$$S = \left\{ a + b\sqrt{2} : \ a, b \in \mathbb{Z}_{>0} \right\}$$

to which $\alpha + \frac{2}{\alpha}$ belongs. Unlike $\mathbb{Z}[\sqrt{2}]$, S is discrete in $\mathbb{R}$. Thus, if we find an estimate E for $\alpha + \frac{2}{\alpha}$ where

$$\left| E - \alpha - \frac{2}{\alpha} \right| < \varepsilon$$

for a small enough $\varepsilon \in \mathbb{R}_{\geq 0}$ such that there is a unique $\omega \in S$ with $|E - \omega| < \varepsilon$, we can deduce that

$$\omega = \alpha + \frac{2}{\alpha},$$

allowing us to get an explicit formula for α.

To find such an estimate, we turn back to the product formulae. For instance, we know that

$$\frac{2}{\alpha} = \mathfrak{f}_2 \left(\frac{\sqrt{-14}}{2} \right)^2 = 2q^{1/12} \prod_{n=1}^{\infty} (1 + q^n)^2$$

when $q = e^{-\pi\sqrt{14}}$. To approximate this, we use the fact that, for $x \in \mathbb{R}_{>0}$, we have $1 + x < e^x$ so

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

However,

$$\log \prod_{n=1}^{\infty} e^{q^n} = \sum_{n=1}^{\infty} q^n = \frac{q}{1 - q}$$

since $q < 1$. Hence,

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

Moreover, as $q < e^{-2\pi}$, we note that

$$\frac{q}{1 - q} < \frac{q}{1 - e^{-2\pi}} < 1.002q.$$

We therefore get that

$$2q^{1/12} < \frac{2}{\alpha} < 2q^{1/12} e^{2.004q},$$

and hence

$$q^{-1/12} e^{-2.004q} < \alpha < q^{-1/12}.$$

So $q^{-1/12}$ should be a good approximation for α. How good? Well, if we let

$$\varepsilon = q^{-1/12} - q^{-1/12}e^{-2.004q} = q^{-1/12}(1 - e^{-2.004q})$$

then we know $\left|\alpha - q^{-1/12}\right| < \varepsilon$. If we approximate q numerically, this should be able to tell us if we are close enough to α.

To find a numerical approximation for $q^{-1/12}$, we return to using Sage, [Stein et al., 2024], and the `RealField()` class by [Schalm et al., 2024] which itself utilises the MPFR library [Hanrot et al., 2023]. With these tools, we approximate

$$q^{-1/12} \approx 2.66329376209099 = Q.$$

The calculation is done to 53-bit precision and hence the error between Q and $q^{-1/12}$ is less than 10^{-15}. Similarly, we find

$$\varepsilon \approx 0.0000419068009806803 = E$$

with an error less than 10^{-15}. Therefore,

$$|\alpha - Q| < E + 2 \cdot 10^{-15}.$$

It is thus safe to say that

$$\alpha + \frac{2}{\alpha} \approx q^{-1/12} + 2q^{-1/12} \approx 2.6633 + 0.7509 = 3.4142$$

with an error of at most 10^{-4}. Since $2 + \sqrt{2} \approx 3.4142$ is within this error range, we can determine that

$$\alpha + \frac{2}{\alpha} = 2 + \sqrt{2}.$$

Hence, α is a root of $X^2 - (2 + \sqrt{2})X + 2$, so

$$\alpha = \frac{\sqrt{2} + 1 + \sqrt{2\sqrt{2} - 1}}{\sqrt{2}} = \mathfrak{f}_1(\sqrt{-14})^2,$$

where we take the larger root as the other root, $\frac{2}{\alpha}$, is smaller than α. By Theorem 7.8, we have

$$\begin{aligned}
\gamma_2(\sqrt{-14}) &= \mathfrak{f}_1(\sqrt{-14})^{16} + \frac{16}{\mathfrak{f}_1(\sqrt{-14})^8} \\
&= \alpha^8 + \frac{16}{\alpha^4} \\
&= \alpha^8 + \left(\frac{2}{\alpha}\right)^4 \\
&= \left(\frac{\sqrt{2} + 1 + \sqrt{2\sqrt{2} - 1}}{\sqrt{2}}\right)^8 + \left(\frac{\sqrt{2} + 1 - \sqrt{2\sqrt{2} - 1}}{\sqrt{2}}\right)^4 \\
&= 2\left(323 + 228\sqrt{2} + (231 + 161\sqrt{2})\sqrt{2\sqrt{2} - 1}\right).
\end{aligned}$$

Then, as $j = \gamma_2^3$, we finally find

$$j(\sqrt{-14}) = 2^3\left(323 + 228\sqrt{2} + (231 + 161\sqrt{2})\sqrt{2\sqrt{2} - 1}\right)^3.$$

7.4 Further Examples

Our calculation of $j(\sqrt{-14})$ relied on a few key facts: that $14 \equiv 6 \mod 8$, 3 does not divide 14 and $\mathrm{Cl}(\mathbb{Z}(\sqrt{-14}))$ is cyclic of order 4. So if we can find a square-free $m \in \mathbb{Z}_{>0}$ such that $m \equiv 6 \mod 8$, 3 does not divide m and $\mathrm{Cl}(\mathbb{Z}(\sqrt{-14}))$ is cyclic of order 4, then we should be able to use the same method as above to find $j(\sqrt{-m})$. However, this leaves us with very few choices for m, the main hurdle being the fact that there are only finitely many imaginary quadratic fields of a given class number. The reason for this is that the class number of $\mathbb{Q}(\sqrt{-m})$ tends to ∞ as m does, this was a conjecture made by Gauss and was proven by Heilbronn in [Heilbronn, 1934]. For our particular case, there are only 54 imaginary quadratic fields of class number 4, with a complete list and proof provided by [Arno, 1992]. Using this list and either software such as Sage or manual computation, one can check that the only m satisfying our conditions are 14, 46, and 142.

It is straightforward to check that the steps of the calculation remain the same when swapping $m = 14$ for $m = 46$ or $m = 142$. We still end up with

$$\alpha + \frac{2}{\alpha} = a + b\sqrt{2}$$

for some $a, b \in \mathbb{Z}_{>0}$ where $\alpha = \mathfrak{f}_1(\sqrt{-m})^2$. We also have the approximation

$$\alpha + \frac{2}{\alpha} \approx q^{-1/12} + 2q^{-1/12}$$

where $q = e^{-\pi\sqrt{m}}$. Thus, using the same methods as in the case $m = 14$, we find

$$\alpha + \frac{2}{\alpha} \approx 6.2426, \text{ when } m = 46$$
$$\alpha + \frac{2}{\alpha} \approx 22.7279, \text{ when } m = 142$$

with an error of at most 10^{-4}. As $2 + 3\sqrt{2} \approx 6.2426$ and $10 + 9\sqrt{2} \approx 22.7279$, we find

$$\mathfrak{f}_1(\sqrt{-46})^2 = \frac{\sqrt{2} + 3 + \sqrt{6\sqrt{2} + 7}}{\sqrt{2}}$$
$$\mathfrak{f}_1(\sqrt{-142})^2 = \frac{5\sqrt{2} + 9 + \sqrt{90\sqrt{2} + 127}}{\sqrt{2}}.$$

Hence,

$$j(\sqrt{-46}) = 6^3 \left(61553 + 43524\sqrt{2} + (15615 + 11043\sqrt{2})\sqrt{6\sqrt{2} + 7}\right)^3,$$
$$j(\sqrt{-142}) = 30^3 \left(575131981 + 406679724\sqrt{2} + (36066897 + 25503147\sqrt{2})\sqrt{90\sqrt{2} + 127}\right)^3.$$

References

[Apostol, 1990] Apostol, T. M. (1990). *Modular Functions and Dirichlet Series in Number Theory*. Springer, 2nd edition.

[Arno, 1992] Arno, S. (1992). The imaginary quadratic fields of class number 4. *Acta Arithmetica*, 60(4):321–334.

[Cox, 2013] Cox, D. (2013). *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication*. Wiley, 2nd edition.

[Granlund et al., 2023] Granlund, T. et al. (2023). *GNU MP: The GNU Multiple Precision Arithmetic Library*, 6.3.0 edition. `https://www.gmplib.org`.

[Hanrot et al., 2023] Hanrot, G., Lefèvre, V., Pélissier, P., Théveny, P., Zimmerman, P., et al. (2023). *GNU MPFR: The GNU Multiple Precision Floating-Point Reliable Library*, 4.2.1 edition. `https://www.mpfr.org`.

[Heilbronn, 1934] Heilbronn, H. (1934). On the Class-Number in Imaginary Quadratic Fields. *The Quarterly Journal of Mathematics*, os-5(1):150–160.

[Janusz, 1996] Janusz, G. J. (1996). *Algebraic Number Fields*. American Mathematical Society, 2nd edition.

[Marcus, 2018] Marcus, D. A. (2018). *Number Fields*. Springer, 2nd edition.

[Schalm et al., 2024] Schalm, K., Stein, W., Deshommes, D., Harvey, D., Zimmerman, P., Witty, C., Bradshaw, R., Demeyer, J., Scrimshaw, T., Bach, E., and Klein, V. (2024). *RealField() Class*, 10.4 edition. `https://doc.sagemath.org/html/en/reference/rings_numerical/sage/rings/real_mpfr.html`.

[Serre, 1973] Serre, J.-P. (1973). *A Course in Arithmetic*. Springer.

[Silverman, 2009] Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves*, chapter VI. Springer, 2nd edition.

[Silverman and Tate, 2015] Silverman, J. H. and Tate, J. T. (2015). *Rational Points on Elliptic Curves*. Springer, 2nd edition.

[Stark, 1967] Stark, H. M. (1967). A complete determination of the complex quadratic fields of class-number one. *Michigan Mathematical Journal*, 14(1):1–27.

[Stein et al., 2024] Stein, W. et al. (2024). *Sage Mathematics Software (Version 10.3)*. The Sage Development Team. `https://www.sagemath.org/`.

[Sutherland, 2022a] Sutherland, A. (2022a). Elliptic curves: Lecture #20. `https://math.mit.edu/classes/18.783/2022/LectureNotes20.pdf`.

[Sutherland, 2022b] Sutherland, A. (2022b). Elliptic curves: Lecture #4. `https://math.mit.edu/classes/18.783/2022/LectureNotes4.pdf`.