CM Elliptic Curves and Class Field Theory

Jack Petok

Contents

1 Introduction

One of the most useful objects in the study of elliptic curves is the j-invariant. The j-invariant determines elliptic curves over K up to $\overline{K}$-isomorphism. Given a curve E in Weierstrass form $y^2 = x^3 + ax + b$ (which can always be done in characteristic $\neq 2, 3$), the j-invariant $j(E)$ is a simply a rational function of the coefficients. Given a model for a complex elliptic curve $E \simeq \mathbf{C}/\Lambda$ where $\Lambda \subset \mathbf{C}$ is a lattice, the j-invariant is a transcendental function on the generators of the lattice.

We say an elliptic curve has *complex multiplication* whenever $\mathrm{End}(E) \otimes_{\mathbf{Z}} \mathbf{Q}$ is an imaginary quadratic field $\mathbf{Q}(\sqrt{-D})/\mathbf{Q}$. Given the transcendental nature of j, it is remarkable that for E an elliptic curve with complex multiplication, $j(E)$ is an *algebraic integer*. Even more remarkably, $K(j(E))$ is the Hilbert class field of K, the maximal unramified abelian extension of K. There will be a natural simply transitive action of the ideal class group of $\mathcal{O}_K$ on the set of elliptic curves with $\mathrm{End}(E) \cong \mathcal{O}_K$ up to $\mathbf{C}$-isomorphism. We will obtain a beautiful set of results connecting elliptic curves, which are geometric objects, and class fields, which are number theoretic objects, via the j-invariant, which is an analytic object. We will assume the reader has some passing familiarity with the geometry and arithmetic of elliptic curves over $\mathbf{C}$, local fields, global fields, and finite fields, although the reader without previous knowledge in these areas can simply accept some facts on faith. We also assume comfort with material covered in a first course in algebraic number theory, including Dedekind domains, ideal class groups, valuations, completions, and decomposition and inertia groups.

2 Basic background and definitions

I will not review the entire theory of elliptic curves and elliptic functions, but will remind the reader of a few concepts. Good references include Silverman [SilvAEC] for an algebro-geometric viewpoint, and Lang [LangEF] for a more analytic perspective. Unless otherwise stated, we take our elliptic curves to be defined over $\mathbf{C}$.

2.1 Elliptic curves, lattices, and isogenies

Recall that an *elliptic curve* (E, O) is a smooth projective algebraic curve of genus 1, and $O \in E$. Elliptic curves are *group varieties*, with identity element O, often called the "point at infinity", and the group law is written additively. Every elliptic curve E over $\mathbf{C}$ is isomorphic to $\mathbf{C}/\Lambda$, where

$\Lambda \in \mathbf{C}$ is a lattice; that is, there exist $\omega_1, \omega_2 \in \mathbf{C}$ with $\Lambda = \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2$ and $\Lambda \otimes \mathbf{R} = \mathbf{C}$. We will always choose the order of the basis to be such that $\mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0$. This isomorphism of complex analytic manifolds $E \simeq \mathbf{C}/\Lambda$ is not only a diffeomorphism between an algebraic curve and a torus, but also is a group isomorphism (where $\mathbf{C}/\Lambda$ is a group under addition mod Λ). When an elliptic curve E is defined over K, we write E/K. $E(K)$ is the set of K-rational points of E/K.

If E_1 and E_2 are two elliptic curves over a field K, then by a *morphism* of elliptic curves $\varphi\colon E_1 \to E_2$ we mean a morphism of curves such that $\phi(O) = O$ (a rational map regular at every point). We remark that a morphism of elliptic curves always has finite degree. We will also need that these are in fact morphisms of *group* varieties (they are also group homomorphisms). Finally, we will use that a nontrivial morphism (called an *isogeny*) is surjective.

Proposition 1. *If $E_1 \cong \mathbf{C}/\Lambda_1$, $E_2 \cong \mathbf{C}/\Lambda$, then a nontrivial isogeny is a surjective map of complex Lie groups $\mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$ induced by the "multiplication by λ" map $\mathbf{C} \to \mathbf{C}$ given by $z \mapsto \lambda z$ such that $\lambda\Lambda_1 \subseteq \Lambda_2$*

Proof. Given a holomorphic map $\varphi\colon \mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$, there is a holomorphic lift $\tilde{\varphi}\colon \mathbf{C} \to \mathbf{C}$ since the universal cover of the complex torus is the complex plane, giving the diagram:

$$\begin{array}{ccc} \mathbf{C} & \xrightarrow{\tilde{\varphi}} & \mathbf{C} \\ \downarrow & & \downarrow \\ \mathbf{C}/\Lambda_1 & \xrightarrow{\varphi} & \mathbf{C}/\Lambda_2. \end{array}$$

Then $\tilde{\varphi}(z) \equiv \tilde{\varphi}(z') \mod \Lambda_2$ for all $z \equiv z' \mod \Lambda_1$. Thus, $\tilde{\varphi}(z) - \tilde{\varphi}(z') \in \Lambda_2$. Fixing a lattice element $\omega \in \Lambda_1$, this leads to

$$\tilde{\varphi}(z) - \tilde{\varphi}(z + \omega) \in \Lambda_2.$$

But

$$f(z) \colon = \tilde{\varphi}(z) - \tilde{\varphi}(z + \omega)$$

is a holomorphic function on $\mathbf{C}$ mapping to a discrete set, so f must be a constant map. Thus,

$$\tilde{\varphi}'(z) - \tilde{\varphi}'(z + \omega) = 0.$$

Since the above actually holds for all $\omega \in \Lambda_1$, $\tilde{\varphi}'$ is an elliptic function that is holomorphic in all of $\mathbf{C}$. Such an elliptic function must be constant, so $\tilde{\varphi}$ must be linear. This together with $\varphi(0) = 0$ proves that $\tilde{\varphi}(z) = \lambda z$. □

Proposition 1 gives the immediate corollary:

Corollary 1. *A* $\mathbf{C}$*-isomorphism of elliptic curves* $\mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$ *is induced by multiplication by some* $\lambda \in \mathbf{C}^*$ *such that* $\lambda\Lambda_1 = \Lambda_2$.

Two lattices satisfying $\lambda\Lambda_1 = \Lambda_2$ as in Corollary 1 are said to be *homothetic*. It is often convenient to view an elliptic curve as $\mathbf{C}/[\tau, 1]$ for $\tau \in \mathbf{C}$, which may always be arranged by homothety.

2.2 Endomorphisms and complex multiplication

The endomorphism ring $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ for an elliptic curve E will be of great importance to us. Given a model for E as a lattice $E \cong \mathbf{C}/\Lambda$, we see that

$$\mathrm{End}(E) \cong \{\lambda \in \mathbf{C} \colon \lambda\Lambda \subset \Lambda\} \subset \mathbf{C}.$$

We can actually fully classify $\mathrm{End}(E)$ for elliptic curves $E/\mathbf{C}$, as captured in the following theorem:

Theorem 1. *Let* $E/\mathbf{C}$ *be an elliptic curve. Then exactly one of the following is true:*

(i) $\mathrm{End}(E) \cong \mathbf{Z}$.

(ii) $\mathrm{End}(E) \cong \mathcal{O}$, *where* $\mathcal{O}$ *is isomorphic to an order in some imaginary quadratic field* $\mathbf{Q}(\sqrt{-D})/\mathbf{Q}$.

Recall that an *order* $\mathcal{O}$ of a degree n number field $K/\mathbf{Q}$ is a finitely generated free $\mathbf{Z}$-subalgebra of $\mathcal{O}_k$ of rank n. So in the setting of the theorem above, these are subrings $\mathcal{O} \subseteq \mathcal{O}_K$ with $\mathcal{O} \otimes_{\mathbf{Z}} \mathbf{Q} = K$.

Proof. Write $E \cong \mathbf{C}/\Lambda$, $\Lambda = [\omega_1, \omega_2]$. Then we may view $\mathrm{End}(E) \subseteq \mathbf{C}$. Clearly $\mathrm{End}(E) \supseteq \mathbf{Z}$ because for an integer n we have $n\Lambda \subseteq \Lambda$. Suppose then that $\mathrm{End}(E) \supsetneq \mathbf{Z}$. For any $\alpha \in \mathrm{End}(E)$, $\alpha \neq \mathbf{Z}$, we have

$$\alpha\omega_1 = m\omega_1 + n\omega_2$$

$$\alpha\omega_2 = q\omega_1 + r\omega_2$$

where $m, n, q, r \in \mathbf{Z}$. Letting $\tau = \omega_1/\omega_2$, we get

$$\alpha\tau = m\tau + n$$

$$\alpha = q\tau + r$$

which gives the equation

$$(q\tau + r)\tau = m\tau + n$$

$$\implies q\tau^2 + (r - m)\tau - n = 0$$

So τ is integral over $\mathbf{Z}$, and thus every α is integral over $\mathbf{Z}$. If $\alpha \notin \mathbf{Z}$, it follows that $q \neq 0$ and that $\alpha \in \mathbf{Q}(\tau) = K$, which is an imaginary quadratic extension of $\mathbf{Q}$. Since $\alpha\Lambda \subset \Lambda$ for all $\alpha \in \mathrm{End}(E)$, we have $\alpha \in \mathcal{O}_K$, by one of the equivalent definitions of algebraic integer. Thus, $\mathrm{End}(E)$ is an order of $\mathbf{Q}(\tau)$. □

We have a special name for elliptic curves satisfying (ii) in Theorem 1.

Definition 1. An elliptic curve $E/\mathbf{C}$ is said to have *complex multiplication* if

$$\mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{End}(E) \cong \mathbf{Q}(\sqrt{d})$$

for some discriminant d of an imaginary quadratic field (in other words, $\mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{End}(E)$ is isomorphic to an imaginary quadratic field when embedded into $\mathbf{C}$).

Often, we abbreviate this by writing *E a CM elliptic curve*.

To be clear, for $\alpha \in \mathrm{End}(E)$ with $E \simeq \mathbf{C}/\Lambda$, α acts as map $\mathbf{C}/\Lambda \to \mathbf{C}/\Lambda$ via $z \mapsto \alpha z$. The endomorphism α acts on the smooth projective curve E, with the image of a point P written as αP, such that the following diagram commutes

$$\begin{array}{ccc} \mathbf{C}/\Lambda & \xrightarrow{z \mapsto \alpha z} & \mathbf{C}/\Lambda \\ \downarrow \simeq & & \downarrow \simeq \\ E & \xrightarrow{P \mapsto \alpha P} & E \end{array}$$

3 The j-invariant and integrality

Before proving the main theorem of complex multiplication, we prove that the j-invariant of a CM-elliptic curve is an algebraic integer.

3.1 The j-invariant and modular functions

Recall that the j-invariant of an elliptic curve E (in characteristic $\neq 2, 3$) with Weierstrass equation $y^2 = 4x^3 - g_2 x - g_3$ is defined as

$$j(E) = 1728 \frac{g_2^3}{g_2^3 - 27 g_3^2} \tag{1}$$

For a lattice $\Lambda = [\omega_1, \omega_2] \subset \mathbf{C}$, we have Eisenstein series of weight $2k$ for $k \geq 2$

$$G_{2k}(\Lambda) = \sum_{\substack{(m,n) \in \mathbf{Z} \times \mathbf{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m\omega_1 + n\omega_2)^{2k}}$$

In our setting over $\mathbf{C}$, using the lattice model for $E \cong \mathbf{C}/\Lambda$, we have the *uniformization theorem* that lets us translate from the Weierstrass model to the lattice model; namely, for any g_2, g_3 with $g_2^3 - 27g_3^2 \neq 0$ (which says the Weierstrass equation is nonsingular), there is a lattice Λ

$$g_2 = g_2(\Lambda) = 60G_4(\Lambda), g_3 = g_3(\Lambda) = 140G_6(\Lambda). \tag{2}$$

Basic module theory tells us if $\{\omega_1, \omega_2\}$ is a $\mathbf{Z}$-basis for lattice with $\mathrm{Im}\left(\frac{\omega_1}{\omega_2}\right) > 0$, the only linear transformations that preserve this lattice are elements of $GL_2(\mathbf{Z})$ with determinant ± 1. In fact, since we would like our lattices to satisfy $\mathrm{Im}\left(\frac{\omega_1}{\omega_2}\right) > 0$, we consider only the group of matrices which preserve the lattice *and* the orientation the lattice. This group is $\Gamma = SL_2(\mathbf{Z})$. Γ is called the *modular group*

The functions $G_{2k}(\Lambda)$ may be viewed as functions of τ. A computation shows, for $\tau = \omega_1/\omega_2$, that

$$G_{2k}([\tau, 1]) = (\omega_2)^{-2k} G_{2k}([\omega_1, \omega_2])$$

From the above, it is clear that the j-invariant is independent of homothety: for $\tau = \omega_1/\omega_2$ we have

$$j([\tau, 1]) = j([\omega_1, \omega_2])$$

Thus, j may be viewed as a meromorphic function $j\colon \mathbf{H} \to \mathbf{C}$ given by

$$j(\tau) = j([\tau, 1]).$$

Since homothety of lattices and change of basis do not change the value of j, it follows that

$$j(\tau) = j(\gamma\tau). \tag{3}$$

for all $\gamma \in SL_2(\mathbf{Z})$, where γ acts on τ via the standard linear fractional transformation. Holomorphic functions on the upper half plane that are $SL_2(\mathbf{Z})$ and that are meromorphic at ∞ and satisfy a functional equation as in (3) are known as *modular functions of weight 0*. Classical results give that $j\colon \mathbf{H}\backslash\Gamma \to \mathbf{C}$ is an isomorphism, and that j is holomorphic on the upper half plane with a simple pole at ∞

The j-invariant has Fourier expansion

$$j(\tau) = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n \tag{4}$$

where $q = e^{2\pi i\tau}$ and the c_n are the Fourier coefficients. Carrying out the derivation for the Fourier expansion via the Fourier expansions for the Eisenstein series shows that $c_n \in \mathbf{Z}$. The first few coefficients are $c_0 = 744, c_1 = 196884, c_2 = 21493760$. Further study of this Fourier expansion, often called the q-expansion, will be central to proving our integrality result.

3.2 Integrality and j

We get some matrix theory out of the way first, since we will need to understand some subsets of the modular group $\Gamma = SL_2(\mathbf{Z})$ to work with the modular function j.

For $n \in \mathbf{Z}^+$, let $\mathcal{D}_n \subset M_2(\mathbf{Z})$ be defined as

$$\mathcal{D}_n = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc = n \}.$$

and we also define $\mathcal{S}_n \subset M_2(\mathbf{Z})$ by

$$\mathcal{S}_n = \{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = n, d > 0, 0 \leq b < d \}$$

We have the following proposition:

Proposition 2. *The cosets $\Gamma \backslash \mathcal{D}_n$ are in bijection with $\mathcal{S}_n$, so we may write*

$$\mathcal{S}_n = \Gamma \backslash \mathcal{D}_n$$

Proof. Since $\mathcal{S}_n \subset \mathcal{D}_n$, there is an obvious mapping $\mathcal{S}_n \to \Gamma \backslash \mathcal{D}_n$ induced by inclusion. First we show that for every $\alpha \in \mathcal{D}_n$, there is some $\gamma \in \Gamma$ such that $\gamma\alpha \in \mathcal{S}_n$. This will prove that $\mathcal{S}_n$ surjects onto the right Γ-cosets of $\mathcal{D}_n$. Say

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We want to multiply on the left by some $\gamma \in \Gamma$ which will kill c.

If $c \neq 0$, then write $-\frac{a}{c} = \frac{q}{p}$, where $(p, q) = 1$. Then there exist integers r, s such that $ps + qr = 1$, and we have the relation $ap + cq = 0$. Then taking $\gamma = \begin{pmatrix} r & -s \\ p & q \end{pmatrix}$ gives

$$\gamma\alpha = \begin{pmatrix} ra - sc & rb - sd \\ 0 & pb + qd \end{pmatrix}.$$

Now we may assume that, after multiplying on the left by suitable $\gamma \in \Gamma$ we have $\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. If $d < 0$, multiply by $\gamma' = -\mathrm{id}$ on the left. So now we are reduced to the case where $\alpha \in \mathcal{D}_n$ has $d > 0$, $c = 0$, $ad = n$. For any integer m, $\gamma_m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \in \Gamma$, and we have

$$\gamma_m\alpha = \begin{pmatrix} a & b + dm \\ 0 & d \end{pmatrix}.$$

Choosing the unique integer m' that gives the least nonnegative integer value of $b + dm$ yields $0 \leq b + dm' < d$, so $\gamma_{m'}\alpha \in \mathcal{S}_n$, which is what we wanted.

Next, we show that map $\mathcal{S}_n \to \Gamma\backslash\mathcal{D}_n$ induced by inclusion is injective. If $\alpha, \beta \in \mathcal{S}_n$ have the same image in $\Gamma\backslash\mathcal{D}_n$ under our map, then $\alpha = \gamma\beta$ for some $\gamma \in \Gamma$. Writing this out:

$$\alpha = \gamma\beta$$

$$\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} w & x \\ y & z \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} wa' & wb' + xd' \\ ya' & yb' + zd' \end{pmatrix}$$

We must have $ya' = 0$, so $y = 0$. Now looking at determinants, we must have $wz = 1$, so $w = z = 1$, which gives $d' = d$ and $a' = a$, as well as $b' + xd' = b$. Thus, $b \equiv b' \mod d$. Since b, b' are least nonnegative integers representing residue classes $\mod d$, they must represent the same residue class $\mod d$, giving $b = b'$. Thus, $\alpha = \beta$, completing the injectivity part of the proof. □

We will use Proposition 2 to construct a polynomial of degree $|\mathcal{S}_n|$ for every n, called the *modular polynomial*. Studying this polynomial will give the integrality of j.

Lemma 1. *If f is a modular function with q-expansion $f = \sum_{n=-N}^{\infty} c_n q^n$, then $f \in \mathbf{Z}[c_{-N}, c_{-N+1}, \ldots][j]$.*

Proof. The function $g(\tau) = f(\tau) - \sum_{n=0}^{N} c_{-n} j^n(\tau)$ is holomorphic on the upper half plane, and vanishes as $\tau \to i\infty$ since $e^{2\pi i\tau} \to 0$ as $\tau \to i\infty$. Viewing j as a function on the Riemann surface $\mathbf{H}\backslash\Gamma \cup \{\infty\}$, we see that $j = 0$ since it is a holomorphic function on a compact Riemann surface. □

We are now ready to define the modular polynomials. The *modular polynomial of order n* is defined to be

$$\Phi_n(X) = \prod_{\alpha \in \mathcal{S}_n} (X - j \circ \alpha).$$

Writing $s_m(\tau)$, $m = 1, \ldots |\mathcal{S}_n|$ to denote the m-th elementary symmetric function of the $j \circ \alpha$, we have:

Lemma 2. *$s_m(\tau) = s_m(\gamma\tau)$ for all $\gamma \in \Gamma$.*

Proof. Since the s_m are symmetric, it suffices to show that $\{j \circ (\alpha\gamma) \colon \alpha \in \mathcal{S}_n\} = \{j \circ \alpha \colon \alpha \in \mathcal{S}_n\}$. Since $\alpha\gamma \in \mathcal{D}_n$, Proposition 2 tells s there exists some $\alpha' \in \Gamma$ such that $\alpha'\alpha\gamma \in \mathcal{S}_n$. Since the map of sets $\mathcal{S}_n \to \Gamma\backslash\mathcal{D}_n$ induced by the inclusion $\mathcal{S}_n \subset \mathcal{D}_n$ is a bijection, α' is uniquely determined by α, γ, i.e. if there is some $\alpha'' \in \Gamma$ with $\alpha''\alpha\gamma \in \mathcal{S}_n$, then $\alpha'' = \alpha'$. Now if there is $\beta \in \mathcal{S}_n$, $\beta' \in \Gamma$ with $\beta'\beta\gamma = \alpha'\alpha\gamma$, then $\alpha = \alpha'^{-1}\beta'\beta$, which by Proposition 2 means $\alpha = \beta$, so that $\alpha' = \beta'$. Now

the map of sets $\mathcal{S}_n \to \mathcal{S}_n$ given by $\alpha \mapsto \alpha'\alpha\gamma$ is injective, so is a bijection (since $\mathcal{S}_n$ is finite). Note that for any $\alpha \in \mathcal{S}_n$ we have $j \circ (\alpha'\alpha\gamma) = j \circ (\alpha\gamma)$ since $\alpha' \in \Gamma$. Thus, using the self-bijection of $\mathcal{S}_n$ we just constructed,

$$\{j \circ (\alpha\gamma) \colon \alpha \in \mathcal{S}_n\} = \{j \circ (\alpha'\alpha\gamma) \colon \alpha \in \mathcal{S}_n\} = \{j \circ \alpha \colon \alpha \in \mathcal{S}_n\}.$$

□

Recall the following proposition:

Proposition 3. *If f is modular function of weight zero that is holomorphic in $\mathbf{H}$, then $f \in \mathbf{C}[j]$.*

Proof. (sketch) j gives a complex analytic isomorphism $j \colon X(1) \to P^1(\mathbf{C})$, where $X(1)$ is the modular curve. Modular functions of weight 0 are meromorphic functions on $X(1)$. Then $f \circ j^{-1}$ is a meromorphic $P^1(\mathbf{C}) \to P^1(\mathbf{C})$, so it must be that $f \circ j^{-1}$ is a rational function. It follows that $f \in \mathbf{C}(j)$. Furthermore, f must be be a polynomial as follows: if f is not a polynomial, then there is $z_0 \in P^1(\mathbf{C})$, giving rise to a pole for f in $\mathbf{H}$. This is not compatible with f being holomorphic, so f must be a polynomial.

□

Lemma 3. *For the $s_m, m = 1, \ldots, |\mathcal{S}_n|$ defined above, $s_m(\tau) \in \mathbf{C}[j]$, $m = 1, \ldots, |\mathcal{S}_n|$.*

Proof. Clearly $s_m(\tau)$ is Γ-invariant, since each $j \circ \alpha$ is Γ invariant by . Thus, s_m is 1-periodic, so has a Fourier expansion in $q = e^{2\pi i\tau}$. Each $j \circ \alpha(\tau)$ is meromorphic at ∞, which follows from q-expansion of each $j \circ \alpha$ together with $\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ and $ad = n$. Thus there is some l such that $q^l(j \circ \alpha)$ is holomorphic at ∞, i.e. as $q \to 0$. Then there is some N such that $q^N s_m(\tau) \to 0$, as $q \to 0$, which is the same as $\tau \to i\infty$. Proposition then yields that $s_m \in \mathbf{C}[j]$. □

Now we look at the Fourier expansion of s_m:

Lemma 4. *The Fourier coefficients c_k in the q-expansion of $s_m(\tau)$*

$$s_m(\tau) = \sum_{k=-N}^{\infty} a_k q^k$$

are integers.

Proof. Let $\zeta_n = e^{2\pi i/n}$. For $\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathcal{S}_n$ (so that $ad = n$), we rewrite

$$q \circ \alpha(\tau) = e^{2\pi i \frac{a\tau + b}{d}} = e^{2\pi i a^2 \tau/n} e^{2\pi i ab/n} = \zeta_n^{ab} q^{a^2/n}$$

so that

$$\begin{aligned} j \circ \alpha(\tau) &= \frac{1}{q \circ \alpha} + \sum_{k=0}^{\infty} c_k (q \circ \alpha)^k \\ &= \zeta_n^{-ab} q^{-ka^2/n} + \sum_{k=0}^{\infty} c_k \zeta_n^{kab} q^{ka^2/n} \end{aligned}$$

Thus, the $q^{1/n}$-Fourier expansion for $j \circ \alpha(\tau)$ has all of its coefficients in $\mathbf{Z}[\zeta_n]$, so it follows that the $s_m(\tau)$ have all of their $q^{1/n}$-Fourier coefficients in $\mathbf{Z}[\zeta_n]$ as well. Now for any $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$, we act σ naturally on the $q^{1/n}$-expansion of $j \circ \alpha$ to get

$$(j \circ \alpha)^\sigma = \sigma(\zeta_n^{-ab}) q^{-ka^2/n} + \sum_{k=0}^{\infty} c_k \sigma(\zeta_n^{kab}) q^{ka^2/n}.$$

Via the natural isomorphism $G\colon \mathrm{Gal}(\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})) \to (\mathbf{Z}/n/\mathbf{Z})^\times$, one has

$$(j \circ \alpha)^\sigma = \zeta_n^{-G(\sigma)ab} q^{-ka^2/n} + \sum_{k=0}^{\infty} c_k \zeta_n^{G(\sigma)kab} q^{ka^2/n} = j \circ \beta_\sigma$$

where

$$\beta_\sigma \coloneqq \begin{pmatrix} a & G(\sigma)b \\ 0 & d \end{pmatrix}.$$

Since j is modular, $j \circ \alpha$ depends on b only up to $b \mod d$. Because $G(\sigma)$ is relatively prime to d (recall that $ad = n$ and $G(\sigma) \in (\mathbf{Z}/n\mathbf{Z})^\times$), $G(\sigma)(\mathbf{Z}/d\mathbf{Z}) = \mathbf{Z}/d\mathbf{Z}$. Thus, we have an equality of sets

$$\left\{ j \circ \alpha\colon \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathcal{S}_n \right\} = \left\{ j \circ \begin{pmatrix} a & G(\sigma)b \\ 0 & d \end{pmatrix} : \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathcal{S}_n \right\},$$

or in other words,

$$\{ j \circ \alpha\colon \alpha \in \mathcal{S}_n \} = \{ (j \circ \alpha)^\sigma\colon \alpha \in \mathcal{S}_n \}.$$

Since each $s_m(\tau)$ is a symmetric polynomial in $j \circ \alpha$, it follows from the above equality of sets that σ fixes the $q^{1/n}$-Fourier coefficients of $s_m(\tau)$. Thus, the $q^{1/n}$ Fourier coefficients lie in $\mathbf{Q}$ and in $\mathbf{Z}[\zeta_n]$, so lie in $\mathbf{Z} = \mathbf{Z}[\zeta_n] \cap \mathbf{Q}$. Since $s_m(\tau)$ is 1-periodic, we see that the only nonvanishing terms can be the coefficients of q. □

We need one more lemma before we prove the key theorem for integrality of $j(E)$.

Lemma 5. $s_m \in \mathbf{Z}[j]$.

Lemma 4 and Lemma 3 give us that $s_m \in \mathbf{C}[j]$ and $s_m \in \mathbf{Z}[q, q^{-1}]$.

Proof. We show that $s_m = a_d j^d + \ldots + a_0$ has $a_0, a_1, \ldots a_d \in \mathbf{Z}$. Using the q-expansion for j gives

$$s_m = \frac{a_d}{q^d} + \frac{a_1 + 744 d a_0}{q^{d-1}} + \ldots$$

Since $s_m \in \mathbf{Z}[[q, q^{-1}]]$, we must have $a_d \in \mathbf{Z}$. Repeating the argument by replacing s_m with $s_m - a_d j^d$ gives $a_{d-1} \in \mathbf{Z}$, and inductively we can reapply this argument until we get all $a_i \in \mathbf{Z}$. □

These lemmas let us harvest some big theorems.

Theorem 2. $\Phi_n(X) = \prod_{\alpha \in \mathcal{S}_n} (X - j \circ \alpha) \in \mathbf{Z}[j, X]$

Proof. By definition of the s_m, $\Phi_n(X) = \sum_{m=1}^{|\mathcal{S}_n|} s_m X^m \in \mathbf{Z}[j, X]$ by Lemma 5. □

We are interested in the polynomial $F_n(X, Y) \in \mathbf{Z}[X, Y]$ which is defined to be polynomial such that $F_n(j, X) = \Phi_n(X)$

Theorem 3. *For $\beta \in M_2(\mathbf{Z})$ with $\det \beta \in \mathbf{Z}^+$, $j \circ \beta$ is integral over $\mathbf{Z}[j]$*

Proof. Letting $n = \det \beta$, there $\gamma \in \Gamma$ such that $\gamma\beta = \alpha \in \mathcal{S}_n$. Since j is a modular of weight 0, $j \circ \beta = j \circ \alpha$, so $j \circ \alpha$ is a root of $F_n(j, X)$..

□

Theorem 4. *For n not a perfect square, $F_n(X, X) \in \mathbf{Z}[X]$ is a non-constant polynomial with leading coefficient -1 or 1.*

Proof. Writing $\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, the hypothesis that $n = ad$ is not a square implies that $a \neq d$. Thus, in the expansion

$$j - j \circ \alpha = \frac{1}{q} + \sum_{k=0}^{\infty} c_k q^k - \frac{1}{\zeta_n a b q^{a^2/n}} - \sum_{k=0}^{\infty} c_k \zeta^{kab} q^{ka^2/n}$$

there is not cancellation of polar terms. So the leading coefficient is a root of unity, either 1 or ζ_n^{-ab}. By Theorem 2, we have that $F_n(j, j) \in \mathbf{Z}[j]$, so that $F_n(j, j) = b_M j^M + \ldots + b_0$, where $M = |\mathcal{S}_n|$. Since b_M is the product of the leading coefficients of each term $j - j \circ \alpha$, it follows that b_M is a root of unity. Since b_M is also an integer, it follows that $b_M = \pm 1$. □

We are ready to prove the integrality of $j(E)$ for E with complex multiplication.

Theorem 5. *Let $E/\mathbf{C}$ have complex multiplication. Then $j(E)$ is an algebraic integer*

Proof. We have $\mathrm{End}(E) \otimes \mathbf{Q} \cong \mathbf{Q}(\sqrt{-D}) = K$ for some $D \in \mathbf{Z}^+$, $D > 1$ and square-free. We will first consider $\mathrm{End}(E) \cong \mathcal{O}_K$, and then we will consider the case where $\mathrm{End}(E)$ is a more general order.

Suppose first that $\mathrm{End}(E) \cong \mathcal{O}_K$. Of course, $j(E) = j(\tau)$ for the lattice $\Lambda = [\tau, 1]$ that models E, where τ is an imaginary quadratic integer. Pick some $\alpha \in \mathcal{O}_K$ such that $n = |\mathrm{Nm}_{K/\mathbf{Q}}(\alpha)|$ is not a perfect square, which can always be done as follows: if $K = \mathbf{Q}(i)$, pick $\alpha = i + 1$, while if $K = \mathbf{Q}(\sqrt{-D})$ for $D > 1$ and square-free, choose $\alpha = \sqrt{-D}$. Since α acts as an endomorphism of E, multiplication by α gives an endomorphism of Λ, so that for some $a, b, c, d \in \mathbf{Z}$ we have

$$\alpha \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \gamma \begin{pmatrix} \tau \\ 1 \end{pmatrix}, \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{5}$$

Since $\{\tau, 1\}$ is $\mathbf{Q}$-basis for K, equation 5 tells us that $|\mathrm{Nm}_{K/\mathbf{Q}}(\alpha)| = ad - bc = n$. The above matrix equation also yields that $\tau = \frac{a\tau + b}{c\tau + d} = \gamma\tau$. Thus, $(j \circ \gamma)(\tau) = j(\tau)$. By Theorem 2, $X = j \circ \gamma$ is a solution of $F_n(j, X) = 0$. Since $(j \circ \gamma)(\tau) = j(\tau)$, we have $F_n(j(\tau), j(\tau)) = F_n(j(E), j(E)) = 0$. By Theorem 4, $j(E)$ is an algebraic integer.

Now we turn to the case where $\mathrm{End}(E) \cong \mathcal{O}$ where $\mathcal{O}$ is any order in K. Suppose the lattice that models E is given by $\Lambda = [\omega_1, \omega_2]$, with $\Lambda \subseteq \mathcal{O}_K$ (this may always be arranged via some homothety of the lattice Λ, by "clearing denominators" of $\mathbf{Z}$-basis for Λ). For this E, then, $j(E) = j(\omega_1/\omega_2)$. $\mathcal{O}_K$ may also be written as a lattice $[\tau, 1]$ as in the first case we analyzed above. Since we have arranged that $\omega_1, \omega_2 \in \mathcal{O}_K$, there are integers a, b, c, d such that

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \beta \begin{pmatrix} \tau \\ 1 \end{pmatrix}, \beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{6}$$

By our convention for the orienting a basis of a lattice, $ad - bc = \det \beta \in \mathbf{Z}^+$. By Equation 6, $j(E) = j(\omega_1/\omega_2) = j(\frac{a\tau + b}{c\tau + d}) = (j \circ \beta)(\tau)$. By Theorem 3, $(j \circ \beta)(\tau)$ is integral over $j(\tau)$. But $j(\tau)$ is the j-invariant of a CM elliptic curve E' modeled on the lattice $\mathcal{O}_K$, so has endomorphism ring $\mathrm{End}(E') \cong \mathcal{O}_K$ (since $\mathcal{O}_K$ is the *unique* maximal order of K). Thus, from the first case above, $j(\tau)$ is an algebraic integer. By the transitivity of integrality, $(j \circ \beta)(\tau) = j(E)$ is also an algebraic integer. □

4 Class Field Theory

While the integrality of j for CM curves is an nice result, the most important theorems in the theory concern the relationship between elliptic curves and various class fields. Here, we review

some of the basic results of class field theory before moving on to the Main Theorem of the theory of complex multiplication.

Let K be a number field (or more generally a global field). Recall that a *modulus* $\mathfrak{m}$ of K is given by $\prod_{\mathfrak{p}} \mathfrak{p}^{m(p)}$ where the product is taken over all the real and finite places of $\mathfrak{p}$, $m(\mathfrak{p}) \geq 0$ for all $\mathfrak{p}$ with all but finitely many $m(\mathfrak{p}) = 0$, with $m(\mathfrak{p}) \geq 1$ for only finitely many places, and $m(\mathfrak{p}) < 2$ if $\mathfrak{p}$ is a real place.

Definition 2. $K_{\mathfrak{m},1}$ denotes the set of all $a \in K^\times$ such that $\mathrm{ord}_{\mathfrak{p}}(a-1) \geq m(\mathfrak{p})$ for all finite $\mathfrak{p} \mid \mathfrak{m}$, and $\sigma(a) > 1$ for all real $\mathfrak{p} \mid \mathfrak{m}$ (where σ is the real embedding given by the real place $\mathfrak{p}$).

For a finite set S of finite primes dividing $\mathfrak{m}$, we write I^S for the group of fractional ideals of K which are relatively prime to S. Let $S(\mathfrak{m})$ be the set of primes dividing $\mathfrak{m}$. Consider the map $i\colon K_{\mathfrak{m},1} \to I^{S(\mathfrak{m})}$ given by $a \mapsto (a)$. Then $i(K_{\mathfrak{m},1})$ is a subgroup of $I^{S(\mathfrak{m})}$. We have the following definition:

Definition 3. The **ray class group modulo** $\mathfrak{m}$ is defined to be

$$C_{\mathfrak{m}} = I^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1}).$$

For example, if $\mathfrak{m} = 1$, then $C_{\mathfrak{m}} = \mathrm{Cl}(K)$, the usual ideal class group, since then $I^{S(\mathfrak{m})}$ is just the free abelian group on all finite primes of K and $K_{1,1} = K^\times$, meaning $i(K_{1,1})$ is the group of principal fractional ideals.

An important result that we will use in the proof of the Main Theorem is the following generalization of Dirichlet's Theorem on primes in arithmetic progressions.

Theorem 6. *Let K be a number field with modulus $\mathfrak{m}$. Then each class of $C_{\mathfrak{m}}$ has infinitely many representatives that are primes of K.*

Now we recall the global reciprocity map. Let L/K be a finite abelian extension of global fields, and let G be its abelian Galois group. Recall that only finitely many primes of K ramify in L, namely those primes that divide the discriminant ideal $\mathfrak{d}_{L/K} = (\mathrm{disc}(L/K))$. Let S be the set of primes dividing $\mathfrak{d}_{L/K}$. Then we have the *Artin reciprocity map* $\omega_{L/K}\colon I^S \to \mathrm{Gal}(L/K)$ which associates to each prime $\mathfrak{p} \in I^S$ the unique element of $D(\mathfrak{p})$, —the decomposition group of $\mathfrak{p}$—, that acts as the Frobenius on the tower of residue fields, $\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$ where $\mathfrak{P}$ is any prime of K that lies above $\mathfrak{p}$, and is then extended by linearity, so that

$$\omega_{L/K}(\prod \mathfrak{p}_i^{n_i}) = \prod_i (\omega_{L/K}(\mathfrak{p}_i))^{n_i}.$$

Analogous to its role in local class field theory, the norm map $\mathrm{Nm}_{L/K}$ is one of the key players in the global theory.

Theorem 7. *Let L/K be a finite abelian extension of global fields, and let S be a finite set of primes of L. Then $\ker \omega_{L/K}$ contains $\mathrm{Nm}_{L/K}(I_L^S)$. Here I_L^S is the set of fractional ideals of L relatively prime to S.*

In general, for a homomorphism $\omega\colon I^S \to G$, S a finite set of primes of K, we can ask whether there exists a modulus $\mathfrak{m}$ such that $S(\mathfrak{m}) \supseteq S$ and $\omega(i(K_{\mathfrak{m},1})) = 0$. This means ω factors through $C_{\mathfrak{m}}$. If such a modulus $\mathfrak{m}$ exists, we say that *ω admits a modulus.* This brings us to the Artin global reciprocity law:

Theorem 8. *Let L/K be a finite abelian extension of global fields, and let S be precisely the set of primes of K that ramify in L (precisely those that divide that discriminant ideal). Then $\omega_{L/K}$ admits a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) = S$ and there is an isomorphism*

$$I^S/(i(K_{\mathfrak{m},1})\mathrm{Nm}_{L/K}(I_L^S)) \xrightarrow{\simeq} \mathrm{Gal}(L/K).$$

Any admissible modulus satisfying these conditions is called a defining modulus for L.

A *congruence subgroup modulo* $\mathfrak{m}$ is a group H with $I^{S(\mathfrak{m})} \supseteq H \supseteq i(K_{\mathfrak{m},1})$. Then we have the existence theorem:

Theorem 9. *If H is a congruence subgroup for a modulus $\mathfrak{m}$, then there exists a finite abelian extension L/K such that $H = i(K_{m,1})\mathrm{Nm}_{L/K} I_L^{S(\mathfrak{m})}$.*

For Theorem 8 to be of any use, we would like the existence of various abelian extensions L/K. Theorem 9 gives us just that. In particular, let $H = i(K_{\mathfrak{m},1})$. Then we get a finite abelian extension L/K such that $i(K_{\mathfrak{m},1}) = i(K_{m,1})\mathrm{Nm}_{L/K} I_L^{S(\mathfrak{m})}$, so Artin reciprocity (Theorem 8) gives an isomorphism

$$I^S/i(K_{\mathfrak{m},1}) = C_{\mathfrak{m}} \xrightarrow{\simeq} \mathrm{Gal}(L/K).$$

Definition 4. The **ray class field modulo** $\mathfrak{m}$ is the finite abelian extension $L_{\mathfrak{m}}/K$ such that $C_{\mathfrak{m}} \simeq \mathrm{Gal}(L_{\mathfrak{m}}/K)$.

The existence of ray class fields is guaranteed by our theorems, and it is unique.

Definition 5. The Hilbert class field of K is the ray class field of K modulo $\mathfrak{m} = 1$.

The Hilbert class field H/K is the unique abelian extension of K with $\mathrm{Gal}(H/K) = C_1 = \mathrm{Cl}(K)$. It is the maximal unramified abelian extension of K.

One more useful object from class field theory that we will need is the *conductor* of an abelian extension L/K.

Definition 6. Let $\mathfrak{m}_1, \mathfrak{m}_2$ be two moduli of L. We say that $\mathfrak{m}_1$ is *smaller* than $\mathfrak{m}_2$ if $\mathfrak{m}_1 | \mathfrak{m}_2$. The *conductor* of L/K is the smallest defining modulus $\mathfrak{c}$ for L/K.

We will make use of the following fact about conductors:

Proposition 4. *Let L/K be an abelian extension. A prime $\mathfrak{p} \subset \mathcal{O}_K$ ramifies in L if and only if $\mathfrak{p} | \mathfrak{c}_{L/K}$.*

5 The Main Theorem

Throughout the rest of this paper $\mathrm{Cl}(K)$ for a number field K denotes the ideal class group of K, and ideal classes will be denoted by $[\mathfrak{a}]$. We now come to the main theorem for CM elliptic curves connecting an arithmetic object associated to a curve with an analytic one- namely, the Hilbert class field (arithmetic) and the j-invariant (analytic). We shall work with CM curves which have $\mathrm{End}(E) \cong \mathcal{O}_K$, since the results are a bit easier to state and prove.

First, a notational convention. We define

$$\mathcal{E}(K) = \{\text{elliptic curves } E \text{ over } K \text{ with } \mathrm{End}(E) = \mathcal{O}_K\} \ / \ \overline{K}\text{-isomorphism.}$$

Note that $\mathcal{E}(K)$ is in natural bijection with

$$\mathcal{L}(K) = \{\text{lattices } \Lambda \subset \mathbf{C} \text{ with } \alpha\Lambda \subset \Lambda \text{ for all } \alpha \in \mathcal{O}_K\} \ / \text{ homothety of } \Lambda.$$

The bijection is given by $\Lambda \mapsto E_\Lambda$, where E_Λ is a model for $\mathbf{C}/\Lambda$.

5.1 Ideal classes and lattices

Let $\mathfrak{a}_1, \ldots \mathfrak{a}_h$ be a choice of representatives for the ideal class group $\mathrm{Cl}(K)$, where $h = h_K$, the class number of K. Recall that for an imaginary quadratic field K, $\mathcal{O}_K$ is a free rank 2 $\mathbf{Z}$-module. Clearly each $\mathfrak{a}_i \subset K$ is a lattice in $\mathbf{C}$, since for some $d \in K$ we have $d\mathfrak{a}_i \subset K$, a free rank 2 $\mathbf{Z}$-submodule of the free rank 2 $\mathbf{Z}$-module $\mathcal{O}_K$.

The class represented by $E_{\mathfrak{a}_i} \in \mathcal{E}(K)$ is independent of choice of representative for the ideal class $[\mathfrak{a}_i]$ for every i. To see this, take a different representative for $[\mathfrak{a}_i]$, say $(c)\mathfrak{a}_i$ for some $c \in \mathcal{O}_K$.

Then $(c)\mathfrak{a}_i = c\mathfrak{a}_i \mapsto E_{(c)\mathfrak{a}_i}$ under our bijection. Since $(c)\mathfrak{a}_i$ is a homothety of the lattice $\mathfrak{a}_i$ by c, we have $E_{\mathfrak{a}_i} \cong E_{(c)\mathfrak{a}_i}$. This discussion hints at a connection between $\mathcal{E}(K)$ and $\mathrm{Cl}(K)$, which we now state (Silverman ATAEC II.1.2(a)).

Theorem 10. *Let $\Lambda \subset \mathbf{C}$ be a lattice with $\mathrm{End}(E_\Lambda) = \mathcal{O}_K$ for some imaginary quadratic $K/\mathbf{Q}$, and let $\mathfrak{a}, \mathfrak{b}$ be (nonzero) fractional ideals of K, and let $[\mathfrak{a}], [\mathfrak{b}]$ represent their ideal classes. Then*

(i) *$\mathfrak{a}\Lambda$ is a lattice with $\mathfrak{a}\Lambda \in \mathcal{L}(K)$.*

(ii) *$E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ if and only if $[\mathfrak{a}] = [\mathfrak{b}]$.*

(iii) *$\mathrm{Cl}(K)$ acts on $\mathcal{E}(K)$ by $\mathfrak{a} \cdot E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$, and this action is simply transitive.*

Proof. To prove that $\mathfrak{a}\Lambda$ is a lattice, it suffices to show that $\mathfrak{a}\Lambda$ is a discrete subgroup of $\mathbf{C}$ with $\mathfrak{a}\Lambda \otimes \mathbf{R} = \mathbf{C}$. Since $\mathfrak{a}$ is a fractional ideal, there is some $f \in \mathcal{O}_K$ such that $f\mathfrak{a} \subseteq \mathcal{O}_K$. Then $f\mathfrak{a}\Lambda \subseteq \Lambda$ because Λ has complex multiplication by $\mathcal{O}_K$. Thus, $\mathfrak{a}\Lambda \subset f^{-1}\Lambda$, so $\mathfrak{a}\Lambda$ is discrete, being a subgroup of the discrete group $f^{-1}\Lambda$. By observing that there is some $g \in K$ such that $g\mathcal{O}_K \subset \mathfrak{a}$, we have that $g\mathcal{O}_K\Lambda = g\Lambda \subset \mathfrak{a}\Lambda$. But $g\Lambda \otimes \mathbf{R} = \mathbf{C}$, so that $\mathfrak{a}\Lambda \otimes \mathbf{R} = \mathbf{C}$ as well. To show that $\mathfrak{a}\Lambda \in \mathcal{L}(K)$, take any $\alpha \in \mathcal{O}_K$. Then $\alpha\mathfrak{a} \subseteq \mathfrak{a}$, so $\alpha\mathfrak{a}\Lambda \subseteq \mathfrak{a}\Lambda$. Then $\alpha \in \mathrm{End}(\mathfrak{a}\Lambda)$. Conversely, if $\alpha \in \mathrm{End}(\mathfrak{a}\Lambda)$, we have $\alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda$. Then multiplying by the ideal $\mathfrak{a}^{-1}$ gives

$$\alpha\Lambda \subset \Lambda,$$

giving $\alpha \in \mathcal{O}_K$. Thus, $\mathrm{End}(\mathfrak{a}\Lambda) = \mathcal{O}_K$, so $\mathfrak{a}\Lambda \in \mathcal{L}(K)$. This completes the proof of (i).

We already proved the "only if" direction of (ii) in our discussion above. For the other direction, suppose we have fractional ideals $\mathfrak{a}, \mathfrak{b} \subset K$ with $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$. Then

$$\mathfrak{a}\Lambda = c\mathfrak{b}\Lambda \tag{7}$$

for some $c \in \mathbf{C}^\times$. Multiplying both sides of (7) by the ideal $\mathfrak{a}^{-1}$ gives

$$\Lambda = c\mathfrak{a}^{-1}\mathfrak{b}\Lambda.$$

Thus, $c\mathfrak{a}^{-1}\mathfrak{b} \subset \mathcal{O}_K$. If we instead multiply both sides of (7) by $c^{-1}\mathfrak{b}^{-1}$, we get

$$\Lambda = c^{-1}\mathfrak{b}^{-1}\mathfrak{a}\Lambda$$

which means $c^{-1}\mathfrak{b}^{-1}\mathfrak{a} \subset \mathcal{O}_K$. Since $c\mathfrak{a}^{-1}\mathfrak{b}$ and its inverse ideal are both contained in $\mathcal{O}_K$, it follows that $c\mathfrak{a}^{-1}\mathfrak{b} = c^{-1}\mathfrak{a}\mathfrak{b}^{-1} = \mathcal{O}_K$. This yields that $\mathfrak{a} = c\mathfrak{b}$, so $c \in K$ and $[\mathfrak{a}] = [\mathfrak{b}]$. This concludes the proof of (ii).

To prove (iii), first we must show that the proposed action really is a group action. In the discussion immediately preceding the statement of the theorem, we showed that $\mathfrak{a} \cdot E_\Lambda$ only depends on the ideal class of $\mathfrak{a}$. Then it is easy to see that

$$(\mathfrak{a}\mathfrak{b}) \cdot E_\Lambda = E_{\mathfrak{a}^{-1}\mathfrak{b}^{-1}\Lambda} = \mathfrak{a} \cdot E_{\mathfrak{b}^{-1}\Lambda} = \mathfrak{a} \cdot (\mathfrak{b} \cdot E_\Lambda).$$

Also, the identity acts trivially, since $\mathcal{O}_K$ is represents the identity and $\mathcal{O}_K^{-1}\Lambda = \mathcal{O}_K\Lambda = \Lambda$, finishing the proof that $[\cdot]$ is a group action. It remains to show that the action is simply transitive. Given two lattices $\Lambda, \Lambda' \in \mathcal{L}(K)$, we want to give a fractional ideal $\mathfrak{a}$ such that $\mathfrak{a} \cdot E_\Lambda = E_{\Lambda'}$. In other words, we need to find $\mathfrak{a}$ so that $\mathfrak{a}^{-1}\Lambda$ is homothetic to Λ'. We know that, after some homothety, $c\Lambda = [\tau, 1]$ where $c = \frac{1}{\omega_2}$ and $\tau = \frac{\omega_1}{\omega_2}$ for ω_1, ω_2 a $\mathbf{Z}$-basis for Λ. Then $c\Lambda$ is in fact a fractional ideal of $\mathcal{O}_K$— that is, a finitely generated $\mathcal{O}_K$-submodule of K. Similarly, some homothety of Λ_2 gives $d\Lambda'$ is a fractional ideal of $\mathcal{O}_K$ for some $d \in \mathbf{C}^\times$. Writing $c\Lambda = \mathfrak{b}_1$ and $d\Lambda' = \mathfrak{b}_2$, we observe that

$$\mathfrak{b}_1^{-1}\mathfrak{b}_2\Lambda = c^{-1}d\Lambda'$$

so letting $\mathfrak{a} = \mathfrak{b}_1\mathfrak{b}_2^{-1}$ gives us $\mathfrak{a} \cdot E_\Lambda = E_{\Lambda'}$. The action is thus transitive Now if $\mathfrak{a}_1 \cdot E_\Lambda = \mathfrak{a}_2 \cdot E_\Lambda$, we know from (ii) that $[\mathfrak{a}_1] = [\mathfrak{a}_2]$. The action is thus simply transitive, completing the proof of (iii). □

Theorem 10, part (iii) yields the corollary:

Corollary 2. *$\mathcal{E}(K)$ is finite and has $|\mathcal{E}(K)| = |\mathrm{Cl}(K)|$.*

5.2 CM curves and the Hilbert class field

As discussed in the introduction, our main theorem states, in part, that $H = K(j(E))$ is the Hilbert class field of K. The the theory of complex multiplication tells us that this action given by Theorem 10 is the same as the action of $\mathrm{Gal}(H/K)$ on $j(E)$.

Theorem 11. (Main Theorem) *Let $E/\mathbf{C}$ be an elliptic curve with $\mathrm{End}(E) \cong \mathcal{O}_K$ for some imaginary quadratic field K. Then*

(i) *$H = K(j(E))$ is the Hilbert class field of K.*

(ii) *$K(j(E)) = K(j(\mathfrak{a} \cdot E))$ for all nonzero fractional ideals $\mathfrak{a} \subset K$.*

(iii) *The Galois conjugates of $j(E)$ are $j(E)^{\omega_{H/K}(\mathfrak{a}_i)} = j(\mathfrak{a}_i \cdot E)$, where the $\mathfrak{a}_i$ form a complete set of representatives for $\mathrm{Cl}(K)$. For for any nonzero fractional ideal of K,*

$$j(E)^{\omega_{H/K}(\mathfrak{a}_i)} = j(\mathfrak{a} \cdot E).$$

The proof of the Main Theorem will rely on two technical lemmas. One of these lemmas is about the existence of a certain homomorphism $\varphi\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Cl}(K)$, and the other concerns a key property of this homomorphism on Frobenius elements for certain primes of K.

Recall that any elliptic curve E/K with $j(E) \in \overline{K}$ is isomorphic to an elliptic curve defined over $K(j(E))$. For a CM curve $E \in \mathcal{E}(K)$, the j invariant is an algebraic integer, so E is isomorphic over $\mathbf{C}$ to an elliptic curve defined over $K(j(E))$, i.e. we may take E to be an elliptic curve where the coefficients of its Weierstrass form lie in $K(j(E))$. For $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and a CM curve E, E^σ is a CM curve as well, with

$$\mathrm{End}(E^\sigma) = \mathrm{End}(E)^\sigma = \mathrm{End}(E) = \mathcal{O}_K$$

so $E^\sigma \in \mathcal{E}(K)$. Since $\mathrm{Cl}(K)$ acts simply transitively on $\mathcal{E}$, $E^\sigma = [\mathfrak{a}] \cdot E$ for some ideal class $\mathfrak{a} \in \mathrm{Cl}(K)$. We will eventually show that this defines a homomorphism

$$\varphi\colon \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Cl}(K)$$

$$\sigma \longmapsto \mathfrak{a}$$

as stated in the lemma below. And even more importantly, the map φ is independent of our choice of elliptic curve E. This is quite difficult to show. The proof of this will be given after the proof of our Main Theorem.

Lemma 6. (The First Lemma) *For an imaginary quadratic field, $\varphi\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Cl}(K)$ is defined independently of E, is well-defined, and is a group homomorphism.*

In other words, the homomorphism φ is essentially defined by

$$\varphi(\sigma) \cdot E = E^\sigma.$$

Since $\mathrm{Cl}(K)$ is abelian, the maximal abelian extension of K, K^{ab}, with abelian Galois group $\mathrm{Gal}(K^{ab}/K)$, satisfies the property that φ factors uniquely through $\mathrm{Gal}(K^{ab}/K)$, giving a homomorphism of abelian groups

$$\varphi\colon \mathrm{Gal}(K^{ab}/K) \longrightarrow \mathrm{Cl}(K).$$

The next lemma we will state concerns an important arithmetic feature of φ, and will also be proved after we prove the Main Theorem. First, we need to review some facts about ramification

groups. Let L/K be a finite Galois extension of number fields. Recall that for a prime $\mathfrak{P}$ of L, the *decomposition group* $D_{\mathfrak{P}}$ is defined to be

$$D_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) \colon \sigma\mathfrak{P} = \mathfrak{P}\}.$$

Let $\mathfrak{p} = \mathfrak{P} \cap K$, which is a prime $\mathfrak{p} \subset \mathcal{O}_K$. Any $\sigma \in D_{\mathfrak{P}}$ naturally induces an automorphism $\overline{\sigma} \in \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$. A result from algebraic number theory says that this map $D_{\mathfrak{P}} \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$ is surjective. The kernel of this map is the *inertia group* $I_{\mathfrak{P}}$. Thus, there is a unique coset of $I_{\mathfrak{P}}$ in $D_{\mathfrak{P}}$, $\sigma I_{\mathfrak{P}}$, such that, for any representative σ' of this coset,

$$\sigma' x = x^{\mathrm{Nm}_{F/\mathbf{Q}}\mathfrak{p}} \mod \mathfrak{P}$$

for all $x \in \mathcal{O}_L/\mathfrak{P}$. A representative of this coset is called a Frobenius element of L/K, since it acts as the Frobenius automorphism on the residue fields.

Recall that for a prime $\mathfrak{p}$ of K, we have that $D_{\sigma\mathfrak{P}} = \sigma D_{\mathfrak{P}} \sigma^{-1}$ for any $\sigma \in \mathrm{Gal}(L/K)$. Thus, the decomposition groups $D_{\mathfrak{P}}$ for all $\mathfrak{P}|\mathfrak{p}$ are $\mathrm{Gal}(L/K)$-conjugates of each other. It follows that if L/K is finite abelian, $D_{\mathfrak{P}} = D_{\mathfrak{P}'}$ for any $\mathfrak{P}, \mathfrak{P}'$ lying above $\mathfrak{p}$. Thus,there is only one decomposition associated to the abelian extension L/K for each prime $\mathfrak{p}$, and we denote it by $D_{\mathfrak{p}}$; similarly, there is the inertia group $I_{\mathfrak{p}} \subset D_{\mathfrak{p}}$ For L/K abelian, we will denote a representative of the Frobenius coset for a prime $\mathfrak{p}$ of K by $\sigma_{\mathfrak{p}}$. By Zorn's lemma, the above works for infinite extensions. Thus, if we consider the maximal abelian extension K^{ab}/K, then for every prime $\mathfrak{p}$ we have a unique Frobenius coset of $I_{\mathfrak{p}}$ in $\mathrm{Gal}(K^{ab}/K)$. We will denote a representative of this coset by $\sigma_{\mathfrak{p}}$. We are now ready to state the second key lemma.

Lemma 7. (The Second Lemma) *Let K be an imaginary quadratic field. There exists a finite set S of primes of $\mathbf{Z}$ such that for $p \notin S$ and p unramified in K with $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p}$ and $\mathfrak{p}'$ are distinct primes of K, we have*

$$\varphi(\sigma_{\mathfrak{p}}) = [\mathfrak{p}].$$

Accepting these lemmas for now, we may proceed to the proof the Main Theorem.

Proof of Main Theorem. First, we show that L/K is an abelian extension. Let φ be the homomorphism from Lemma 6. Since E has Weierstrass coefficients in $K(j(E))$, the elements $\sigma \in \mathrm{Gal}(\overline{K}/K)$ fixing the coefficients of E represent a finite index subgroup of F, namely $\mathrm{Gal}(\overline{K}/L)$ where L is the Galois closure of $K(j(E))$ over K. In other words, L is the fixed field of $\ker\varphi = \mathrm{Gal}(\overline{K}/L)$. We first claim that in fact $L = K(j(E))$— equivalently, that $\mathrm{Gal}(\overline{K}/L) = \mathrm{Gal}(\overline{K}/K(j(E)))$.

We already have $\mathrm{Gal}(\overline{K}/L) \subseteq \mathrm{Gal}(\overline{K}/K(j(E)))$. Now take any $\sigma \in \mathrm{Gal}(\overline{K}/K(j(E)))$. Then $j(E) = \sigma(j(E)) = j(E^\sigma)$, so $E \cong E^\sigma$ because j distinguishes between isomorphism classes of elliptic curves. But then $\varphi(\sigma) = 1$ since the action of $\mathrm{Cl}(K)$ on $\mathcal{E}(K)$ is faithful. It follows that $\sigma \in \ker\varphi = \mathrm{Gal}(\overline{K}/K(j(E)))$, and thus we have shown $L = K(j(E))$. In particular, $K(j(E))/K$ is a Galois extension. It also follows $\varphi\colon \mathrm{Gal}(K(j(E))/K) \hookrightarrow \mathrm{Cl}(K)$, so $\mathrm{Gal}(L/K)$ is abelian, proving that $K(j(E))/K$ is an abelian extension.

Next, we show that L/K is unramified. Let $\mathfrak{c}_{L/K}$ be the conductor of L/K, and consider an ideal $\mathfrak{a} \in I^{\mathfrak{c}_{L/K}}$. By Theorem 6, there exist infinitely many primes $\mathfrak{p} \in I^{\mathfrak{c}_{L/K}}$ which represent the same $i(K_{\mathfrak{c}_{L/K},1})$-coset in $C_{\mathfrak{c}_{L/K}}$ as $\mathfrak{a}$. Thus, there exists a prime $\mathfrak{p} \in I^{\mathfrak{c}_{L/K}}$ not lying above one of the primes in the finite set S from Lemma 7 which represents the same $i(K_{\mathfrak{c}_{L/K},1})$-coset as $\mathfrak{a}$. So there is some $a \in K^\times$ with $\mathrm{ord}_{\mathfrak{p}}(a-1) \geq 1$ such that $\mathfrak{a} = a\mathfrak{p}$. We now compute $\varphi(\omega_{L/K}(\mathfrak{a}))$. We get

$$\begin{aligned}\varphi(\omega_{L/K}(\mathfrak{a})) &= \varphi(\omega_{L/K}(a\mathfrak{p})) \\ &= \varphi(\omega_{L/K}(a)\omega_{L/K}(\mathfrak{p})) = \varphi(\omega_{L/K}(\mathfrak{p}))\end{aligned}$$

where we used $\omega_{L/K}((a)) = 1$ by Theorem 7. Then by Lemma 7, $\varphi(\omega_{L/K}(\mathfrak{p})) = [\mathfrak{p}] = [\mathfrak{a}]$. Thus, we have shown for all $\mathfrak{a} \in I^{\mathfrak{c}_{L/K}}$ that

$$\varphi(\omega_{L/K}(\mathfrak{a})) = [\mathfrak{a}]. \tag{8}$$

Setting $\mathfrak{a} = (a)$ in (8) for any a such that $(a) \in I^{\mathfrak{c}_{L/K}}$, we see that $\varphi(\omega_{L/K}((a))) = [(a)] = 1$, the identity element of $\mathrm{Cl}(K)$. Since $\varphi\colon \mathrm{Gal}(L/K) \to \mathrm{Cl}(K)$ is injective, we must have that $\omega_{L/K}((a)) = 1$ for all $(a) \in I^{\mathfrak{c}_{L/K}}$. The conductor $\mathfrak{c}_{L/K}$ is the smallest modulus (largest ideal) that $\omega_{L/K}$ admits, which is to say that $\mathfrak{c}_{L/K}$ is the smallest modulus such that for all $a \in K^\times$ with $\mathrm{ord}_{\mathfrak{p}}(a-1) \geq 1$ for all $\mathfrak{p}|\mathfrak{c}_{L/K}$, it holds that $\omega_{L/K}((a)) = 1$. Since $\omega_{L/K}((a)) = 1$ for all $(a) \in I^{\mathfrak{c}_{L/K}}$, we must have that $\mathfrak{c}_{L/K} = 1$. Thus, L/K is unramified since no primes divide 1.

So far, we have shown that L is contained in the Hilbert class field H of K, since L/K is unramified and abelian. Since the conductor $\mathfrak{c}_{L/K} = 1$,

$$\varphi(\omega_{L/K}(\mathfrak{a})) = [\mathfrak{a}]$$

for all fractional ideals of K. This proves that $\varphi\colon \mathrm{Gal}(L/K) \to \mathrm{Cl}(K)$ is surjective. We also know that φ is injective, so in fact

$$\varphi\colon \mathrm{Gal}(L/K) \xrightarrow{\simeq} \mathrm{Cl}(K).$$

Since $|\mathrm{Gal}(H/K)| = |\mathrm{Cl}(K)|$ and $L \subseteq H$, this isomorphism yields that $L = H$, proving (i).

By part (iii) of Theorem 10, a complete set of representative of $\mathcal{E}(K)$ is given by $\{\mathfrak{a} * E\}$ for any fixed $E \in \mathcal{E}(K)$ as $\mathfrak{a}$ runs over the fractional ideals of K. The above analysis holds for any elliptic curve in $\mathcal{E}(K)$, giving $K(j(\mathfrak{a} * E)) = H = K(j(E))$ for any $\mathfrak{a} \subset K$.

To prove (iii), first recall that for $\sigma \in \mathrm{Gal}(H/K)$ we have $E^\sigma = \varphi(\sigma) \cdot E$, which is well-defined because $\ker \varphi = \mathrm{Gal}(\overline{K}/H)$. Since $\varphi(\omega_{L/K}(\mathfrak{a})) = [\mathfrak{a}]$ for all fractional ideals $\mathfrak{a}$ (recall that $\mathfrak{c}_{L/K} = 1$), it follows that, in $\mathcal{E}(K)$

$$E^{\omega_{L/K}(\mathfrak{a})} = \mathfrak{a} \cdot E$$

so that, upon taking j of each side,

$$j(E^{\omega_{L/K}(\mathfrak{a})}) = j(E)^{\omega_{L/K}(\mathfrak{a})} = j(\mathfrak{a} \cdot E) \tag{9}$$

proving the second claim of (iii). The first claim of part (iii) follows immediately from (9) and the fact that φ is an isomorphism. □

5.3 The First Lemma

Let us now take up the task of proving the first technical lemma, Lemma 6.

Proof of Lemma 6. Fix an elliptic curve $E \in \mathcal{E}(K)$, and consider the map $\varphi_E \colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Cl}(K)$, defined by

$$\varphi_E(\sigma) \cdot E = E^\sigma.$$

Theorem 10 ensures that φ is well-defined, provided that E is fixed. Furthermore, φ is a group homomorphism, since

$$\begin{aligned} \varphi(\sigma_1\sigma_2) \cdot E &= E^{\sigma_1\sigma_2} = (E^{\sigma_2})^{\sigma_1} \\ &= (\varphi(\sigma_2) \cdot E)_1^\sigma = (\varphi(\sigma_1)\varphi(\sigma_2)) \cdot E. \end{aligned}$$

To show that φ is independent of E, suppose we have $E_1, E_2 \in \mathcal{E}$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$. We have

$$E_1^\sigma = [\mathfrak{a}_1] \cdot E_1$$

$$E_2^\sigma = [\mathfrak{a}_2] \cdot E_2$$

and we want to show that $[\mathfrak{a}_1] = [\mathfrak{a}_2]$. By Theorem 10, there exists a unique $[\mathfrak{b}] \in \mathrm{Cl}(K)$ with $[\mathfrak{b}] \cdot E_1 = E_2$, so

$$([\mathfrak{b}] \cdot E_1)^\sigma = E_2^\sigma = [\mathfrak{a}_2] \cdot ([\mathfrak{b}] \cdot E_1) = [\mathfrak{a}_2\mathfrak{b}\mathfrak{a}_1^{-1}] \cdot E_1^\sigma$$

and if we can show that $([\mathfrak{b}] \cdot E_1)^\sigma = [\mathfrak{b}] \cdot E_1^\sigma$, we will have that

$$[\mathfrak{b}] \cdot E_1^\sigma = [\mathfrak{b}\mathfrak{a}_1\mathfrak{a}_2^{-1}] \cdot E_1^\sigma$$

so that $[a_1] = [a_2]$, proving that φ is independent of E_1, E_2.

So to complete the proof, we are going to show that for $E \in \mathcal{E}(K)$, $[\mathfrak{a}] \in \mathrm{Cl}(K)$, and $\sigma \in \mathrm{Gal}(\overline{K}/K)$, we have $([\mathfrak{a}] \cdot E)^\sigma = [\mathfrak{a}] \cdot E^\sigma$. Choose a representative $\mathfrak{a} \subset \mathcal{O}_K$ for $[\mathfrak{a}]$, which can always be done by multiplying by some principal ideal. Consider the lattice Λ so that $E \simeq \mathbf{C}/\Lambda$. We have the following free resolution of $\mathfrak{a}$ (as a $\mathcal{O}_K$-module)

$$\mathcal{O}_K^n \xrightarrow{A} \mathcal{O}_K^m \longrightarrow \mathfrak{a} \longrightarrow 0$$

and the following exact sequence

$$0 \longrightarrow \mathbf{C} \longrightarrow \Lambda \longrightarrow E \longrightarrow 0 \tag{10}$$

We get the following commutative diagram, which is exact in its rows and columns by the left exactness of the functors $\mathrm{Hom}_{\mathcal{O}_K}(M, -)$ and $\mathrm{Hom}_{\mathcal{O}_K}(-, M)$ for $\mathcal{O}_K$-modules M:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{a}, \Lambda) & \longrightarrow & \mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{a}, \mathbf{C}) & \longrightarrow & \mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{a}, E) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_K^m, \Lambda) & \longrightarrow & \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_K^m, \mathbf{C}) & \longrightarrow & \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_K^m, E) \\
 & & \downarrow{\scriptstyle A} & & \downarrow{\scriptstyle A} & & \downarrow{\scriptstyle A} \\
0 & \longrightarrow & \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_K^n, \Lambda) & \longrightarrow & \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_K^n, \mathbf{C}) & \longrightarrow & \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_K^n, E)
\end{array}$$

where A acts through precomposition.

For M a torsion-free $\mathcal{O}_K$ module, we have an isomorphism

$$\eta\colon \mathfrak{a}^{-1}M \xrightarrow{\simeq} \mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{a}, M) \tag{11}$$

$$m \longmapsto \phi_m$$

where $\phi_m(a) = am$. To see this, suppose we have $\phi \in \mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{a}, M)$. ϕ extends to a homomorphism $\Phi = \mathrm{id} \otimes \phi\colon \mathfrak{a}^{-1} \otimes_{\mathcal{O}_K} \mathfrak{a} \to \mathfrak{a}^{-1} \otimes_{\mathcal{O}_K} M$. For any N a torsion-free module over a Dedekind domain, N is flat. As N is flat, $I \otimes_{\mathcal{O}_K} N \simeq IN$ for any fractional ideal $I \subset \mathcal{O}_K$. We have then that M is

flat, so $\mathfrak{a}^{-1} \otimes_{\mathcal{O}_K} \mathfrak{a} \simeq \mathcal{O}_K$ via the obvious isomorphism $x \otimes y \mapsto xy$, and so we may choose to view Φ as a map

$$\Phi \colon \mathcal{O}_K \longrightarrow \mathfrak{a}^{-1}M.$$

Let $\Phi(1) = m$. Using $\mathfrak{a}^{-1} \supset \mathcal{O}_K$ and $\mathcal{O}_K$-linearity of Φ, we have

$$\phi(a) = \Phi(1 \otimes a) = \Phi(a) = am.$$

This proves η is surjective. Injectivity of η follows from M being torsion free.

The above analysis shows that when $M = \mathbf{C}$ in (11),

$$\mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{a}, \mathbf{C}) \simeq \mathfrak{a}^{-1}\mathbf{C} = \mathbf{C},$$

and when $M = \Lambda$,

$$\mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{a}, \Lambda) \simeq \mathfrak{a}^{-1}\Lambda.$$

For the maps $\mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_K^m, M) \xrightarrow{A} \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_K^n, M)$, we may identify $\mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_K^n, M) \simeq M^n$, and we get $M^m \xrightarrow{A^T} M^n$, where A^T is the transpose of the linear operator A, induced by functoriality. Putting all this together, we get the commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathfrak{a}^{-1}\Lambda & \longrightarrow & \mathbf{C} & \longrightarrow & \mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{a}, E) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \Lambda^m & \longrightarrow & \mathbf{C}^m & \longrightarrow & \mathbf{E}^m & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle A_1^T} & & \downarrow{\scriptstyle A_2^T} & & \downarrow{\scriptstyle A_3^T} & & \\
0 & \longrightarrow & \Lambda^n & \longrightarrow & \mathbf{C}^n & \longrightarrow & E^n & \longrightarrow & 0
\end{array} \tag{12}$$

where the last two rows are exact again because (10) is exact, and the labeling on the A^T's is just for convenience in what follows. Since the bottom two rows of the diagram are exact, the snake lemma tells us that

$$0 \longrightarrow \ker A_1^T \longrightarrow \ker A_2^T \longrightarrow \ker A_3^T \longrightarrow \mathrm{coker} A_1^T \longrightarrow \mathrm{coker} A_2^T \longrightarrow \mathrm{coker} A_3^T \longrightarrow 0$$

is exact. Using exactness of the columns of (12), we get the exact sequence

$$0 \longrightarrow \mathfrak{a}^{-1}\Lambda \longrightarrow \mathbf{C} \longrightarrow \ker A_3^T \longrightarrow \Lambda^n / A^T\Lambda^m \longrightarrow \mathrm{coker} A_2^T \longrightarrow \mathrm{coker} A_3^T \longrightarrow 0$$

which gives an exact sequence

$$\mathbf{C}/\mathfrak{a}^{-1}\Lambda \xhookrightarrow{f} \ker A_3^T \longrightarrow g\Lambda^n / A^T\Lambda^m \tag{13}$$

Since A_3^T is an algebraic map of algebraic group varieties (it is a matrix with entries in $\mathcal{O}_K$), $\ker A_3^T$ is an algebraic group subvariety of E^m. Note that $\mathbf{C}/\mathfrak{a}^{-1}\Lambda \simeq \ker g$ is connected, while $\Lambda^n/A^T\Lambda^m$ is discrete. Thus, the entire connected component of the identity of $\ker A_3^T$ must map to 0 under g. Thus,

$$\mathfrak{a} \cdot E \simeq \mathbf{C}/\mathfrak{a}^{-1} \simeq \ker g = \text{connected component of 0 of } \ker A_3^T.$$

Now we have, for $\sigma \in \mathrm{Gal}(\overline{K}/K)$, a natural action

$$\mathfrak{a} \cdot E^\sigma = \mathfrak{a}^\sigma \cdot E^\sigma \simeq \text{connected component of 0 of } \ker((A_3^T)^\sigma \colon (E^\sigma)^m \longrightarrow (E^\sigma)^n)$$

$$= (\text{connected component of 0 of } \ker A_3^T)^\sigma = (\mathfrak{a} \cdot E)^\sigma$$

which completes our proof. □

6 Reduction of elliptic curves and the Second Lemma

To prove the second technical lemma, Lemma 7, we will need a few facts about reduction of elliptic curves over local fields at good and bad primes. Before proceeding to the proof, let us review a few more notions from the basic geometry and arithmetic of elliptic curves.

6.1 The invariant differential, the Tate module, and the Weil pairing

Recall that we associate to every elliptic curve E/K, for any field K, the *invariant differential*. In any characteristic, E has Weierstrass form

$$E \colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{14}$$

with $a_i \in K$ and discriminant $\Delta = -16(4a_4^3 + 27a_6^2)$. The invariant differential is the 1-form on E associated to a Weierstrass equation for E is given by

$$\omega_E = \frac{dx}{2y + a_1x + a_3}.$$

ω_E deserves its name *invariant* it is invariant under pullback by the translation map; namely, for the map $\tau_Q \colon E \to E$ given by $\tau_Q(P) = P + Q$ for points $P, Q \in E$, a straightforward computation shows that

$$\tau_Q^* \omega_E = \omega_E.$$

The only coordinate changes preserving both the Weierstrass form and the point at infinity are of the form

$$x \longmapsto u^2x + r,\ y \longmapsto u^3y + u^2sx + t \tag{15}$$

for $u \in K^\times, r, s, t \in K$.

For E an elliptic curve and $m \in \mathbf{Z}$, there is a map $[m] \in \mathrm{Hom}(E, E)$ given by

$$[m](P) = \underbrace{P + \cdots + P}_{m \text{ times}}.$$

By $E[m]$, we mean the group of m-torsion points of E; that is,

$$E[m] = \{P \in E \colon [m]P = 0\}.$$

Given two elliptic curves E_1, E_2 defined over the same field K and an isogeny $\phi \in \mathrm{Hom}(E_1, E_2)$ of degree d, there exists a *unique* isogeny $\hat{\phi} \in \mathrm{Hom}(E_2, E_1)$ such that $\hat{\phi}\phi = [d]$ on E_1 and $\phi\hat{\phi} = [d]$ on E_2. This is proved in [SilvAEC, III.6]. $\hat{\phi}$ is called the *isogeny dual to* ϕ.

A useful characteristic 0 object which captures data about the positive characteristic torsion groups is the Tate module of an elliptic curve. Given a prime $\ell \in \mathbf{Z}$ and an elliptic curve E. There is a directed system of maps $E[\ell^{n+1}] \to E[\ell^n]$ for all positive integers n given by $P \mapsto [\ell]P$. The *Tate module* $T_\ell(E)$ is defined by

$$T_\ell(E) = \varprojlim_n E[\ell^n]$$

where the limit is over the directed system just described. As shown in [SilvAEC, III.6], $E[m] \simeq \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$. Therefore, as abstract groups, we have an isomorphism

$$T_\ell(E) \simeq \mathbf{Z}_\ell \times \mathbf{Z}_\ell$$

where $\mathbf{Z}_\ell$ is the additive group of ℓ-adic integers. The multiplicative group of roots of unity $\mu \subset K^\times$ also has a Tate module given by the directed system induced by the natural maps $\mu_{\ell^{n+1}} \to \mu_{\ell^n}$ given by $\zeta_{\ell^{n+1}} \mapsto \zeta_{\ell^{n+1}}^{\ell}$. Then the Tate module is given by the limit over this directed system

$$T_\ell(\mu) = \varprojlim_n \mu_{\ell^n}$$

and we have an abstract isomorphism of groups

$$T_\ell(\mu) \simeq \mathbf{Z}_\ell.$$

The *Weil pairing* is a fundamental tool in the study of elliptic curves. Rather then present the definition of the Weil pairing, which would require us to wade through a substantial amount of

algebro-geometric background, we present some properties of the Weil pairing, which the reader can treat like axioms, and accept on faith that the Weil pairing exists. The reader interested in a complete treatment of the Weil pairing should refer to [SilvAEC, III.8]. For an integer $m \geq 2$ and an elliptic curve E/K, the *Weil pairing*

$$e_m \colon E[m] \times E[m] \longrightarrow \mu_m$$

is a certain nondegenerate bilinear form satisfying the following properties. Let $S, S', T, T' \in E[m]$:

(i) e_m is bilinear:

$$e_m(S, T + T') = e_m(S, T)e_m(S, T')$$

$$e_m(S + S', T) = e_m(S, T)e_m(S', T).$$

(ii) e_m is nondegenerate. If

$$e_m(S, T) = 0$$

for all $S \in E$, then $T = 0$.

(iii) e_m is alternating:

$$e_m(S, T) = e_m(T, S)^{-1}. =$$

(iv) e_m is Galois-invariant. For $\sigma \in \mathrm{Gal}(\overline{K}/K)$,

$$e_m(S^\sigma, T^\sigma) = e_m(S, T)^\sigma.$$

(v) e_m is compatible. For any integer $m' \geq 2$,

$$e_{mm'}(Q, T) = e_m([m']Q, T)$$

for all $Q \in E[mm']$.

Proposition 5. *dual Let $\phi \in \mathrm{Hom}(E_1, E_2)$, m be an integer ≥ 2, and let $S \in E_1[m], T \in E_2[m]$. Then*

$$e_m(S, \hat{\phi}(T)) = e_m(\phi(S), T)$$

In other words, ϕ left adjoint to $\hat{\phi}$ in the Weil pairing.

Proof. See [SilvAEC, III.8.2]. □

For a prime $\ell \in \mathbf{Z}$, recall from our discussion of the Tate module the maps

$$E[\ell^{n+1}] \longrightarrow E[\ell^n]$$

$$P \longmapsto [\ell]P$$

and

$$\mu_{\ell^{n+1}} \longrightarrow \mu_{\ell^n}$$

$$\zeta_{\ell^{n+1}} \longmapsto \zeta_{\ell^{n+1}}^{\ell}.$$

For $S, T \in E[\ell^{n+1}]$, we have, using the properties of the Weil pairing described above,

$$\begin{aligned} e_{\ell^{n+1}}(S,T)^{\ell} &= e_{\ell^{n+1}}(S,[\ell]T) \\ &= e_{\ell^n}([\ell]S,\ell[T]). \end{aligned}$$

Thus, the directed system for the limit giving the Tate module $T_\ell(E)$ is compatible with the Weil pairing, and so we get a well-defined map

$$e_E \colon T_\ell(E) \times T_\ell(E) \longrightarrow T_\ell(\mu).$$

This construction is known as the *Weil pairing on the Tate module.*. It naturally inherits the properties of the Weil pairing on elliptic curves.

6.2 Reduction of elliptic curves

We will come across elliptic curves over non-archimedean local fields of characteristic zero. In our setting, these fields will arise from completions of number fields with respect to primes. Let K be a local non-archimedean field of characteristic zero, complete with respect to valuation v normalized so that $v(\pi) = 1$ for a uniformizer $\pi \in \mathcal{O}_K$. Let $\mathfrak{m}$ be the unique maximal ideal $\pi\mathcal{O}_K$, and let k be the residue field $k = \mathcal{O}_K/\mathfrak{m}$. Let E be an elliptic curve defined over K and let E have Weierstrass form as in (14), with $a_i \in K$. Pick m large enough so that $\pi^m a_i \in \mathcal{O}_K$ for all i. Then the coordinate change $(x, y) \mapsto (\pi^{-2m}x, \pi^{-3m}y)$ gives gives E Weierstrass form

$$E \colon y^2 + \pi^m a_1 xy + \pi^{3m} a_3 y = x^3 + \pi^{2m} a_2 x^2 + \pi^{4m} a_4 x + \pi^{6m} a_6$$

which gives a Weierstrass equation with coefficients in $\mathcal{O}_K$. Thus, any elliptic curve E/K can be taken with Weierstrass coefficients in the local ring $\mathcal{O}_K$. We say that a Weierstrass equation for E with coefficients in $\mathcal{O}_K$ is a *minimal Weierstrass equation* for E if, for any Weierstrass equation for E with coefficients in $\mathcal{O}_K$ and discriminant Δ', we have$v(\Delta) \leq v(\Delta')$. Clearly, minimal Weierstrass equations exist. The following result will be useful.

Proposition 6. *Let E be an elliptic curve defined over K, a non-archimedean local field of characteristic zero.*

(i) *There is a unique minimal Weierstrass equation for E, up to coordinate changes as given in (15) with $u \in \mathcal{O}_K^\times$, $r, s, t \in \mathcal{O}_K$.*

(ii) *The invariant differential for E associated to a minimal Weierstrass equation for E is unique up to multiplication by $u \in \mathcal{O}_k^\times$.*

Proof. See [SilvAEC, VII.1.3]. □

Given E/K, one is interested in the reduction of E modulo π; that is, given a minimal Weierstrass form for E/K, we consider the reduced curve $\overline{E}/k$, where $\overline{E}$ has the Weierstrass coefficients of E reduced modulo π. By Proposition 6, any other minimal Weierstrass form for E will give a curve isomorphic to $\overline{E}$. Note that $\overline{E}$ may be a *singular* curve; it may not be smooth at a point. When $\overline{E}$ is *nonsingular*, we say that E has *good reduction.* when $\overline{E}$ is *singular*, we say that E has *bad reduction.*

Proposition 7. *Let K be a local non-archimedean field with char $K = 0$, and let E/K have good reduction. Let $m \geq 2$ be such that char $k \nmid m$. Then the natural map induced by reduction mod π*

$$E(K)[m] \longrightarrow \overline{E}(k)$$

is injective. It follows that $E(K)[m] \simeq \overline{E}(k)[m]$.

Proof. See [SilvAEC, VII.3.1]. □

Now let L be a *number field*, $L/\mathbf{Q}$, and let E be an elliptic curve defined over L. Given a prime $\mathfrak{p} \subset \mathcal{O}_L$, we may take $L_\mathfrak{p}$, the completion of L with respect to the $\mathfrak{p}$-adic valuation, and then we may take the residue field $l_\mathfrak{p} = \mathcal{O}_{L_\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L_\mathfrak{p}}$. Then there is the elliptic curve $E_\mathfrak{p}/l_\mathfrak{p}$ given by viewing the Weierstrass equation for E as in equation over $L_\mathfrak{p}$. We say that E has *good reduction at* $\mathfrak{p}$ whenever the elliptic curve $E_\mathfrak{p}$ has good reduction, and we denote the reduced elliptic curve by $\overline{E}_\mathfrak{p}$. Of course, when $\overline{E_\mathfrak{p}}$ is singular, we say that E has *bad reduction* at $\mathfrak{p}$. Fortunately, few primes give bad reduction:

Proposition 8. *Let L be a number field and E be defined over L. Then E has good reduction at all but finitely many primes of L.*

Proof. See [SilvAEC, VIII.1]. □

Given two elliptic curves $E_1/L, E_2/L$ and an isogeny $\phi \in \mathrm{Hom}(E_1, E_2)$, there is an induced isogeny $\overline{\phi}_{\mathfrak{p}} \in \mathrm{Hom}(\overline{E_1}_{\mathfrak{p}}, \overline{E_2}_{\mathfrak{p}})$. The following proposition says that this map $\mathrm{Hom}(E_1, E_2) \longrightarrow \mathrm{Hom}(\overline{E_1}_{\mathfrak{p}}, \overline{E_2}_{\mathfrak{p}})$ is injective whenever E_1, E_2 have good reduction at $\mathfrak{p}$.

Proposition 9. *Let L be a number field, $\mathfrak{P}$ a prime of L, and E_1, E_2 elliptic curves defined over L with good reduction at $\mathfrak{P}$. Then the natural map*

$$\mathrm{Hom}(E_1, E_2) \longrightarrow \mathrm{Hom}(\overline{E_1}_{\mathfrak{P}}, \overline{E_2}_{\mathfrak{P}})$$

$$\phi \longmapsto \overline{\phi}_{\mathfrak{P}}$$

is injective and

$$\deg(\phi) = \deg(\overline{\phi}_{\mathfrak{P}}).$$

Proof. Let $\ell \in \mathbf{Z}$ be a prime such that $\mathfrak{P} \nmid p$. Proposition 7 tells us that for $i = 1, 2$ and any nonnegative integer n

$$E_i[\ell^n] \simeq \overline{E_i}_{\mathfrak{P}}[\ell^n]$$

which means that $T_\ell(E_i) \simeq T_\ell(\overline{E_i}_{\mathfrak{P}})$. Furthermore, by examining the construction of the Weil pairing on the Tate module, this implies for $s, t \in T_\ell(E_i)$

$$\overline{e_{E_i}(s,t)} = e_{\overline{E_i}_{\mathfrak{p}}}(\overline{s}, \overline{t}) \tag{16}$$

where $\overline{e_{E_i}(s,t)}$ is determined by viewing the maps $E_i[\ell^{n+1}] \to E_i[\ell^n]$ as maps $E_i(L_{\mathfrak{P}})[\ell^{n+1}] \to E_i(L_{\mathfrak{P}})[\ell^n]$ and then reducing modulo $\mathfrak{P}$, and where $\overline{s}, \overline{t}$ are the images of s, t respectively under the the isomorphism $T_\ell(E_i) \to T_\ell(\overline{E_i}_{\mathfrak{P}})$.

For $s, t \in T_\ell(E_i)$, we use the properties of the Weil pairing to compute

$$\begin{aligned} e_{E_1}(s,t)^{\deg(\phi)} &= e_{E_1}(s, [\deg(\phi)]t) && \text{by bilinearity of the Weil pairing} \\ &= e_{E_1}(s, \hat{\phi}\phi(t)) \\ &= e_{E_2}(\phi(s), \phi(t)) && \text{since } \phi \text{ is dual to } \hat{\phi} \text{ in the Weil pairing.} \end{aligned}$$

giving the equation

$$e_{E_1}(s,t)^{\deg(\phi)} = e_{E_2}(\phi(s), \phi(t)). \tag{17}$$

For $\overline{s}, \overline{t} \in T_\ell(\overline{E_1}_{\mathfrak{P}})$, we also then get

$$e_{\overline{E_1}_{\mathfrak{P}}}(\overline{s}, \overline{t})^{\deg(\overline{\phi}_{\mathfrak{P}})} = e_{\overline{E_2}_{\mathfrak{P}}}(\overline{\phi}_{\mathfrak{P}}(\overline{s}), \overline{\phi}_{\mathfrak{P}}(\overline{t})). \tag{18}$$

Putting these small results together, we show, for $s, t \in T_\ell(E_1)$, that

$$e_{\overline{E_1\mathfrak{P}}}(\overline{s}, \overline{t})^{\deg(\phi)} = e_{\overline{E_1\mathfrak{P}}}(\overline{s}, \overline{t})^{\deg(\overline{\phi}_\mathfrak{P})}$$

which will implies $\deg(\phi) = \deg(\overline{\phi}_\mathfrak{P})$ by the nondegeneracy of the Weil pairing:

$$\begin{aligned}
e_{\overline{E_1\mathfrak{P}}}(\overline{s}, \overline{t})^{\deg(\phi)} &= \overline{e_{E_1}(s,t)}^{\deg(\phi)} && \text{by (16)} \\
&= \overline{e_{E_1}(s,t)^{\deg(\phi)}} = \overline{e_{E_2}(\phi(s), \phi(t))} && \text{by (17)} \\
&= e_{\overline{E_2\mathfrak{P}}}(\overline{\phi(s)}, \overline{\phi(t)}) && \text{by (16)} \\
&= e_{\overline{E_2\mathfrak{P}}}(\overline{\phi}_\mathfrak{P}(s), \overline{\phi}_\mathfrak{P}(t)) = e_{\overline{E_1\mathfrak{P}}}(\overline{s}, \overline{t})^{\deg(\overline{\phi}_\mathfrak{P})} && \text{by (18).}
\end{aligned}$$

This proves that $\deg(\phi) = \deg(\overline{\phi}_\mathfrak{P})$. An isogeny is the zero map if and only if its degree is zero. Thus, the equality of degrees proves that the map $\phi \mapsto \overline{\phi}_\mathfrak{P}$ is injective. □

6.3 Proof of the Second Lemma

Proof. (**The Second Lemma)** By the algebraicity of the j-invariants for the finite set elliptic curves in $E_1, \ldots E_n \in \mathcal{E}(K)$, then $E_1, \ldots E_n$ may be defined simultaneously over a field $L = K(j(E_1), \ldots j(E_n))$. Since $\mathrm{Hom}(E_i, E_j)$ is finitely generated (see [SilvAEC III.7]), all isogenies in $\{\mathrm{Hom}(E_i, E_j) \colon 1 \le i, j \le n\}$ may be defined over some finite extension of L, so we replace L with this finite extension of L. Our set S of finite primes will be

$$S = A \cup B \cup C$$

where

$$A = \{\text{primes } p \in \mathbf{Z} \colon p \text{ ramifies in } L\}$$

$$B = \{\text{primes } p \in \mathbf{Z} \colon E_i \text{ has bad reduction for some prime of } L \text{ lying above } p \text{ for some } 1 \le i \le n\}$$

$$C = \{\text{primes } p \in \mathbf{Z} \colon p | \mathrm{Nm}_{L/\mathbf{Q}}(j(E_k) - j(E_l)) \text{for some } k \ne l\}.$$

A is finite because the only primes that ramify are those dividing the discriminant $\mathrm{disc}(L/\mathbf{Q})$. B is finite by Proposition 8. C is obviously finite, and makes sense because each $j(E_i)$ is integral.

Choose a model $E \simeq \mathbf{C}/\Lambda$, and a prime $p \notin S$. By hypothesis, p is unramified in K, so $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ for some primes $\mathfrak{p} \ne \mathfrak{p}'$ of K. Let $c \in \mathcal{O}_K$ be such that $c\mathfrak{p}^{-1}$ is an integral ideal of K and $c\mathfrak{p}^{-1}$ is relatively prime to p. Then $c\mathfrak{p}^{-1}\mathfrak{p} = (c)$, and we have a sequence of holomorphisms of elliptic curves

$$\mathbf{C}/\Lambda \longrightarrow \mathbf{C}/\mathfrak{p}^{-1}\Lambda \longrightarrow \mathbf{C}/(c^{-1}\mathfrak{p}\mathfrak{p}^{-1}\Lambda) \xrightarrow{z \mapsto cz} \mathbf{C}/\Lambda \quad (*)$$

where the first two maps are the maps lifting to $z \mapsto z$ as maps $\mathbf{C} \to \mathbf{C}$ (see Proposition 1). Note that the last arrow is an isomorphism (see Corollary 1). The above analytic maps of tori give algebraic isogenies of algebraic curves under the equivalence of categories for elliptic curves viewed as complex tori and elliptic curves viewed as complex algebraic curves:

$$E \xrightarrow{\phi} \mathfrak{p} \cdot E \xrightarrow{\psi} (c\mathfrak{p}^{-1}) \cdot \mathfrak{p} \cdot E \xrightarrow{\lambda} E$$

where λ is the isomorphism from the diagram (*). These fit together into a commutative diagram

$$\begin{array}{ccccccc} \mathbf{C}/\Lambda & \longrightarrow & \mathbf{C}/\mathfrak{p}^{-1}\Lambda & \longrightarrow & \mathbf{C}/(c^{-1}\mathfrak{p}\mathfrak{p}^{-1}\Lambda) & \xrightarrow{z \mapsto cz} & \mathbf{C}/\Lambda \\ \downarrow{\scriptstyle \eta_1} & & \downarrow{\scriptstyle \eta_2} & & \downarrow{\scriptstyle \eta_3} & & \downarrow{\scriptstyle \eta_4} \\ E & \xrightarrow{\phi} & \mathfrak{p} \cdot E & \xrightarrow{\psi} & (c\mathfrak{p}^{-1}) \cdot \mathfrak{p} \cdot E & \xrightarrow{\lambda} & E \end{array} \qquad (**)$$

where η_i are the isomorphisms between the curves as complex tori and the curves as complex projective curves.

Let $\mathfrak{P}$ be a prime of L lying over p, and let

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

be a Weierstrass equation for E which is minimal over $L_{\mathfrak{P}}$ (so that $a_1, a_3, a_4, a_6 \in \mathcal{O}_{K_{\mathfrak{P}}}$). The associated invariant differential for this Weierstrass equation is

$$\omega = \frac{dx}{2y + a_1x + a_3},$$

both as a 1-form on $E(L)$ and on $E(L_{\mathfrak{P}})$. Under the pullback by the isomorphism η_1, ω pulls back to an invariant 1-form $\eta_1^*\omega \in \Omega_{\mathbf{C}/\Lambda}$, so $\eta_1^*\omega = \alpha dz$ for some $\alpha \in \mathbf{C}$. Since the composition of maps along the top row is just $z \mapsto cz$, we see that dz pulls back along the top row to $c\ dz$, so we get that $(\lambda \circ \psi \circ \phi)^*\omega = c\ dz$.

$\overline{E}_{\mathfrak{P}}$ is a nonsingular elliptic curve because E has good reduction at $\mathfrak{P}$. Thus, when $2, a_1$ and a_3 are viewed modulo $\mathfrak{P}$, we get an nonzero invariant differential on $\overline{E_{\mathfrak{P}}}$:

$$\overline{\omega_{\mathfrak{P}}} = \frac{dx}{2y + \overline{a_1}x + \overline{a_3}}.$$

and using our pullback computation from above, we see that

$$(\overline{\lambda_{\mathfrak{P}}} \circ \overline{\psi_{\mathfrak{P}}} \circ \overline{\phi_{\mathfrak{P}}})^*\overline{\omega_{\mathfrak{P}}} = \overline{((\lambda \circ \psi \circ \phi)^*\omega)_{\mathfrak{P}}} = \overline{c\omega_{\mathfrak{P}}}$$

Since $\mathfrak{P}$ divides c, it follows that $(\overline{\lambda_{\mathfrak{P}}} \circ \overline{\psi_{\mathfrak{P}}} \circ \overline{\phi_{\mathfrak{P}}})^*\overline{\omega_{\mathfrak{P}}} = 0$.

From the theory of algebraic curves (see [SilvAEC, II.2]), a map $f\colon C_1 \to C_2$ of algebraic curves is *inseparable* if $f^*\colon \Omega_{C_2} \to \Omega_{C_1}$ is the zero map. Since the invariant differential $\overline{\omega_{\mathfrak{P}}}$ spans $\Omega_{\overline{E_{\mathfrak{P}}}}$, it follows that $\overline{\lambda_{\mathfrak{P}}} \circ \overline{\psi_{\mathfrak{P}}} \circ \overline{\phi_{\mathfrak{P}}}$ is inseparable; that is, if we let $f = \overline{\lambda_{\mathfrak{P}}} \circ \overline{\psi_{\mathfrak{P}}} \circ \overline{\phi_{\mathfrak{P}}}$ and $l_{\mathfrak{P}}(\overline{E_{\mathfrak{P}}})$ denote the field of functions of $\overline{E_{\mathfrak{P}}}$, then $l_{\mathfrak{P}}(\overline{E_{\mathfrak{P}}})/f^* l_{\mathfrak{P}}(\overline{E_{\mathfrak{P}}})$ is an inseparable extension. Thus, the map f factors into an inseparable part and a separable part, corresponding to the separable and inseparable parts of the extension $l_{\mathfrak{P}}(\overline{E_{\mathfrak{P}}})/f^* l_{\mathfrak{P}}(\overline{E_{\mathfrak{P}}})$, and the inseparable part of the map is some Frobenius homomorphism. This Frobenius map will allow us to extract information about the map φ. To determine these separable and inseparable factors, it suffices to study the degrees of the $\overline{\lambda_{\mathfrak{P}}}$, $\overline{\psi_{\mathfrak{P}}}$, and $\overline{\phi_{\mathfrak{P}}}$, which are the same as the degrees of the corresponding extensions of function fields. By Proposition 9,

$$\deg(\overline{\lambda_{\mathfrak{P}}}) = \deg(\lambda)$$

$$\deg(\overline{\psi_{\mathfrak{P}}}) = \deg(\psi)$$

$$\deg(\overline{\phi_{\mathfrak{P}}}) = \deg(\phi).$$

Since λ is an isomorphism, $\deg(\lambda) = 1$. For the degrees of ψ and ϕ, we need the following lemma. For an integral ideal $\mathfrak{a} \subseteq \mathcal{O}_K$, and an elliptic curve $E \simeq \mathbf{C}/\Lambda \in \mathcal{E}(K)$, we define the *$\mathfrak{a}$-torsion points of E* to be the subgroup

$$E[\mathfrak{a}] = \{z \in \mathbf{C}/\Lambda\colon az = 0 \text{ for all } a \in \mathfrak{a}\}.$$

Lemma 8. *Let $E \simeq \mathbf{C}/\Lambda \in \mathcal{E}(K)$ and $\mathfrak{a}$ be an integral ideal.*

(i) $\ker(\mathbf{C}/\Lambda \xrightarrow{z\mapsto z} \mathbf{C}/\mathfrak{a}^{-1}\Lambda) = E[\mathfrak{a}] = \mathfrak{a}^{-1}\Lambda/\Lambda$.

(ii) *$E[\mathfrak{a}] \simeq \mathcal{O}_K/\mathfrak{a}$ as $\mathcal{O}_K/\mathfrak{a}$-modules.*

(iii) $\deg(\mathbf{C}/\Lambda \xrightarrow{z\mapsto z} \mathbf{C}/\mathfrak{a}^{-1}\Lambda) = \mathrm{Nm}_{K/\mathbf{Q}}\mathfrak{a} = |\mathcal{O}_K/\mathfrak{a}|$.

Proof. We have

$$\begin{aligned}
\ker(\mathbf{C}/\Lambda \to \mathbf{C}/\mathfrak{a}^{-1}\Lambda) &= \{z \in \mathbf{C}\colon z \in \mathfrak{a}^{-1}\Lambda\}/\Lambda = \mathfrak{a}^{-1}\Lambda/\Lambda \\
&= \{z \in \mathbf{C}\colon \mathfrak{a}z \subset \Lambda\}/\Lambda \\
&= \{z \in \mathbf{C}\colon az \in \Lambda \text{ for all } a \in \mathfrak{a}\}/\Lambda \\
&= \{z \in \mathbf{C}/\Lambda\colon az = 0f = \text{ for all } a \in \mathfrak{a}\} = E[\mathfrak{a}]
\end{aligned}$$

which proves (i).

To prove (ii), note that, up to homothety, we may write $\Lambda = [\tau, 1]$ where τ is an imaginary quadratic integer, so that $\Lambda \subset \mathcal{O}_K$. Since $\alpha\Lambda \subset \Lambda$ for all $\alpha \in \mathcal{O}_K$, this allows us to take Λ to be an integral ideal of $\mathcal{O}_K$. Since $\mathfrak{a}^{-1}\Lambda/\Lambda \simeq E[\mathfrak{a}]$ as $\mathcal{O}_K/\mathfrak{a}$ -modules, we have

$$(\mathfrak{a}^{-1}\Lambda/\Lambda) \otimes_{\mathcal{O}_K} \mathcal{O}_K/\mathfrak{a} \simeq E[\mathfrak{a}]$$

By the Chinese Remainder theorem, if $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$, then

$$\mathcal{O}_K/\mathfrak{a} \simeq \bigoplus_{i=1}^{n} \mathcal{O}_K/\mathfrak{p}_i^{e_i}$$

and so we may write

$$\begin{aligned}(\mathfrak{a}^{-1}\Lambda/\Lambda) \otimes_{\mathcal{O}_K} \mathcal{O}_K/\mathfrak{a} &\simeq \bigoplus_{i=1}^{n} \left((\mathfrak{a}^{-1}\Lambda/\Lambda) \otimes_{\mathcal{O}_K} \mathcal{O}_K/\mathfrak{p}_i^{e_i}\right) \\ &\simeq \bigoplus_{i=1}^{n} \left(\mathfrak{a}^{-1}\Lambda/(\Lambda + \mathfrak{a}^{-1}\mathfrak{p}_i^{e_i})\Lambda\right) \simeq \bigoplus_{i=1}^{n} \left(\mathfrak{a}^{-1}\Lambda/(\mathfrak{a}^{-1}\mathfrak{p}_i^{e_i}\Lambda)\right).\end{aligned}$$

Note that $A_i = \mathcal{O}_K/\mathfrak{p}_i^{e_i}$ is a local ring with unique maximal ideal $\mathfrak{p}_i$ (in a Dedekind domain all prime ideals are maximal). Now letting $M_i = \mathfrak{a}^{-1}\Lambda/(\mathfrak{a}^{-1}\mathfrak{p}_i^{e_i}\Lambda)$, and $\mathfrak{p}_i' = \mathfrak{p}_i/\mathfrak{p}_i^{e_i}$, we see that $M_i/\mathfrak{p}_i'M_i$ is a vector space over $A_i/\mathfrak{p}_i \simeq \mathcal{O}_K/\mathfrak{p}_i$. If we can show that $M_i/\mathfrak{p}_iM_i$ is a 1-dimensional $A_i/\mathfrak{p}_i$-vector space, it will follow by Nakayama's lemma that M_i is generated over $\mathcal{O}_K/\mathfrak{p}_i^{e_I}$ by a single element, and thus is a free $\mathcal{O}_K/\mathfrak{p}_i^{e_i}$ module of rank 1.

To prove that $M_i/\mathfrak{p}_i'M_i$ is 1-dimensional, note that $M_i/\mathfrak{p}_i'M_i \simeq \mathfrak{a}^{-1}\Lambda/(\mathfrak{a}^{-1}\mathfrak{p}_i\Lambda)$ as $\mathcal{O}_K/\mathfrak{p}_i$-vector spaces. Since $\mathfrak{a}^{-1}\Lambda$ is a fractional ideal of $\mathcal{O}_K$, a maximally $\mathcal{O}_K$-linearly independent set has at most 1 element, which means that $\mathfrak{a}^{-1}\Lambda/(\mathfrak{a}^{-1}\mathfrak{p}_i\Lambda)$ is at most 1-dimensional as a $\mathcal{O}_K/\mathfrak{p}_i$ vector space. Clearly the dimension is at least one, since $\mathfrak{a}^{-1}\mathfrak{p}\Lambda$ is strictly contained in $\mathfrak{a}^{-1}\Lambda$. This proves that the dimension is 1.

Since $E[\mathfrak{a}]$ is now the direct sum of rank 1 $\mathcal{O}_K/\mathfrak{p}_i^{e_I}$ modules, it follows that $E[\mathfrak{a}]$ is a free rank 1 $\mathcal{O}_K/\mathfrak{a}$-module.

(iii) follows easily, because

$$\deg(\mathbf{C}/\Lambda \xrightarrow{z\mapsto z} \mathbf{C}/\mathfrak{a}^{-1}\Lambda) = |\ker(\mathbf{C}/\Lambda \xrightarrow{z\mapsto z} \mathbf{C}/\mathfrak{a}^{-1}\Lambda)| = |\mathcal{O}_K/\mathfrak{a}|$$

□

Retruning to the proof of Lemma 7, we have from what we just proved that

$$\deg(\psi) = \mathrm{Nm}_{K/\mathbf{Q}}(c\mathfrak{p}^{-1}) = \frac{c}{p}$$

$$\deg(\phi) = \mathrm{Nm}_{K/\mathbf{Q}}\mathfrak{p} = p$$

and that $\frac{c}{p}$ is an integer relatively prime to p because $c\mathfrak{p}^{-1}$ is an integral ideal relatively prime to p. Summarizing our work, we have shown

$$\deg(\overline{\lambda_{\mathfrak{P}}}) = 1$$

$$\deg(\overline{\psi_{\mathfrak{P}}}) = \frac{c}{p}$$

$$\deg(\overline{\phi_{\mathfrak{P}}}) = p$$

It follows that $\overline{\lambda_{\mathfrak{P}}}, \overline{\psi_{\mathfrak{P}}}$ must be separable factors of f, forcing that $\overline{\phi_{\mathfrak{P}}}$ must factor through the p-th power map $\mathrm{Frob}_p \colon \overline{E_{\mathfrak{P}}} \to \overline{E_{\mathfrak{P}}}^p$, which act in projective coordinates by $[x_0, x_1] \mapsto [x_0^p, x_1^p]$. Thus,

$$\overline{\phi_{\mathfrak{P}}} = g \circ \mathrm{Frob}$$

where g is some degree 1 map $g \colon \overline{E_{\mathfrak{P}}}^p \xrightarrow{\simeq} \overline{\mathfrak{p} \cdot E}$. Thus, in the field $l_{\mathfrak{P}}$, we have $j(\overline{(\mathfrak{p} \cdot E)_{\mathfrak{P}}}) = j(\overline{E_{\mathfrak{P}}}^p) = j(\overline{E_{\mathfrak{P}}})^p$. Thus, *still working over the residue field*, we recall that $\sigma_{\mathfrak{p}}$ is the p-th power Frobenius map, so

$$j([\mathfrak{p}] \cdot E) = j(E)^p = j(E)_{\mathfrak{p}}^{\sigma} = j(E_{\mathfrak{p}}^{\sigma}) = j(\varphi(\sigma_{\mathfrak{p}}) \cdot E).$$

Lifting back to L,

$$p \mid (j([\mathfrak{p}] \cdot E) - j(\varphi(\sigma_{\mathfrak{p}}) \cdot E)).$$

Since $p \notin C$, this means

$$[\mathfrak{p}] \cdot E = \varphi(\sigma_{\mathfrak{p}}) \cdot E.$$

□

7 A fun application

It is no coincidence that

$$e^{\pi\sqrt{163}} = 262537412640768743.9999999999992\ldots$$

is almost an integer. This fact was remarked upon in Ramanujan's notebook, and Martin Gardner once published a famous April Fool's Day column claiming $e^{\pi\sqrt{163}}$ was, in fact, an integer.

The explanation is simple with the theory of complex multiplication. Consider the elliptic curve $E \simeq \mathbf{C}/[\tau 1]$, where $\tau = \frac{\sqrt{-163}+1}{2}$. The lattice associated to E is the ring of integers of $K = \mathbf{Q}(\sqrt{-163})$, with $\mathcal{O}_K = \mathbf{Z}[\frac{\sqrt{-163}+1}{2}]$, so E has complex multiplication. Since K has class

number 1, class field theory tells us that the Hilbert class field H of K is a degree 1 extension of K, so $H = K$. By the main theorem, $H = K(j(\tau))$,so $j(\tau) =\in K$. Since $j(\tau)$ is also an algebraic integer, as we showed earlier, $j(\tau) \in \mathcal{O}_K$.

Recall the Fourier expansion for j:

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

where $q = e^{2\pi i \tau} = e^{-\sqrt{163}\pi}$. This shows that $j(\tau)$ is real, so $j(\tau) \in \mathcal{O}_K \cap \mathbf{R} = \mathbf{Z}$. It is a result of Petersson, using the well-known "circle method" of analytic number theory, that

$$c_n \sim \frac{e^{4\pi\sqrt{n}}}{\sqrt{2}n^{3/4}}$$

as $n \to \infty$, and that this convergence is rapid enough such that only the first two terms of $j(\tau)$ dominate the other terms. This leads to the almost-equality

$$e^{\pi\sqrt{163}} \approx 262537412640768744.$$

References:

[ChildressCFT]: N. Childress, Class Field Theory.

[LangEF]: S. Lang, Elliptic Functions.

[LangANT]: S. Lang, Algebraic Number Theory

[MilneANT]: J Milne, Algebraic Number Theory.

[MilneCFG]: J. Milne, Class Field Theory.

[SerreCM]: J.P. Serre et al, Seminar on Complex Multiplication.

[SilvAEC]: J. Silverman, Arithmetic of Elliptic Curves.

[SilvATAEC]: J. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves.