COMPLEX MULTIPLICATION AND CLASS FIELD THEORY

TOAN Q. PHAM

Contents

1. Motivation: Explicit class field theory

For a global/local field K, the main theorem of class field theory (see Theorem 4 for instance) does not give an explicit description (for example, in terms of generators) for the maximal abelian extension K^{ab}. This is the Hilbert's twelfth problem, or Kronecker's Jugendtraum ("dream of youth"). Such question has been explored for certain global/local fields, and from my first glance, give strangely similar methods. Here is a brief summary of what I understand of the general picture (the following statements may not be completely correct)

(1) Cyclotomic theory: When $K = \mathbb{Q}$, the Kronecker-Weber theorem says that $\mathbb{Q}^{ab}$ is the union of all torsion points of the multiplicative group $\mathbb{G}_m$, which carries an action of $\mathbb{Z} \xrightarrow{\sim} \mathrm{End}(\mathbb{G}_m)$.
(2) Complex multiplication theory: When K is imaginary quadratic, E is an elliptic curve with an action $\mathcal{O}_K \xrightarrow{\sim} \mathrm{End}(E)$ of $\mathcal{O}_K$, then K^{ab} is generated by torsion points of E (see [Sil, Thm.II.5.6] for the precise statement).
(3) Lubin-Tate theory: When F is a nonarchimedean local field, there is a formal group scheme $\mathcal{G}$ over $\mathcal{O}_F$ with an action $\mathcal{O}_F \to \mathrm{End}(\mathcal{G})$, and F^{ab} is generated by taking torsion points of $\mathcal{G}$ (see [Jar] for the precise statement).

Date: May 21, 2023.

(4) Drinfeld-modules theory: Let K be a global function field defined from a curve X over $\mathbb{F}_q$. Fix a closed point $\infty \in X$, a Drinfeld module is roughly a group scheme L over X with an action $\mathcal{O}(X-\infty) \to \mathrm{End}(L)$. (Somehow) taking torsion points of L gives all maximal abelian extension of K unramified away from ∞. We refer [Poo] for the precise statement.

In this notes, we will mainly focus on the case where K where K is an imaginary quadratic field. Our goal is to understand the proofs of Theorem 23 and 33, giving generators for ray class fields of K created from any elliptic curve with complex multiplication by $\mathcal{O}_K$. We will spend the next two sections giving the required knowledge, the next section to talk about Theorem 23, and the last section to discuss Theorem 33.

2. Global class field theory

In this section, we let K be a global field. We wish to state ideal-theoretic global class field theory in this section. We follow [LiCFT].

Definition 1. *A* modulus *of K is a formal product $\mathfrak{m} = \prod_v \mathfrak{p}_v^{e_v}$ over all places v of K, where $\mathfrak{p}_v$ is a prime ideal for finite place v, such that*

(1) $e_v \geq 0$ and $e_v = 0$ for almost all v,
(2) for a real place v, $e_v = 0, 1$,
(3) for a complex place, $e_v = 0$.

We write $v \mid \mathfrak{m}$ or $\mathfrak{p}_v \mid \mathfrak{m}$ if $e_v > 0$.

One think of modulus as a way to encode ramification for a field extension of K. To make this more precise, we introduce a few more definitions,

Definition 2. *Let $x_v \in K_v^\times$, we write $x_v \equiv 1 \pmod{\mathfrak{m}_v}$ if*

- *v is non-archimedean and $e_v > 0$, then $x_v \in 1 + \mathfrak{p}_v^{e_v}$,*
- *v is non-archimedean and $e_v = 0$, then $x_v \in \mathcal{O}_{K_v}^\times$,*
- *v is archimedean, and $e_v = 1$, then $x_v > 0$,*
- *no requirement for v archimedean and $e_v = 0$.*

Definition 3 (Ray class group)**.** *For a modulus $\mathfrak{m}$ of K, we define*

- *$I_\mathfrak{m}$ the free abelian group of fractional ideals of K generated by $\{\mathfrak{p}_v : v \nmid \mathfrak{m}\}$,*
- *$P_\mathfrak{m}$ is the subgroup of $I_\mathfrak{m}$, whose elements are principal fractional ideal (x) where $x \in K^\times, x \equiv 1 \mod \mathfrak{p}_v$ for all $v \mid \mathfrak{m}$.*
- *We denote $Cl_\mathfrak{m}(K) = I_\mathfrak{m}/P_\mathfrak{m}$, called* the ray class group *of $\mathfrak{m}$.*

When $\mathfrak{m} = 1$ then $\mathrm{Cl}_\mathfrak{m} = \mathrm{Cl}(K)$ is the ideal class group of K.

Theorem 4 (Ideal-theoretic class field theory)**.** *There is a one-to-one correspondence between abelian extensions of K and a pair $(\mathfrak{m}, U)$ where $\mathfrak{m}$ is a modulus and U is a subgroup lying between $P_\mathfrak{m} \subset U \subset I_\mathfrak{m}$. The correspondence can be described as follows:*

Let L/K be an abelian extension, and $\mathfrak{m}$ be a modulus of K which is divisible by all the ramified places, we can define the Artin map, which is a surjective map

$$\Psi_{L/K} : I_\mathfrak{m} \to \mathrm{Gal}(L/K),$$

by sending $\pi_v \mapsto Frob_\mathfrak{p}$, where $\pi_v \in \mathfrak{p}_v$ is a uniformiser. In fact, there exists a modulus $\mathfrak{m}$ containing ramified primes of L/K such that $P_\mathfrak{m} \subset \ker \Psi_{L/K}$. The greatest common divisor of all such $\mathfrak{m}$ is called the conductor *of L/K.*

Conversely, given a modulus $\mathfrak{m}$, there exists a unique finite abelian extension $K_\mathfrak{m}/K$ such that $\ker \Psi_{L/K} = P_\mathfrak{m}$. We call $K_\mathfrak{m}$ the ray class field of modulus $\mathfrak{m}$*. In particular, the conductor of $K_\mathfrak{m}$ divides $\mathfrak{m}$, and if L/K is an abelian extension whose conductor divides $\mathfrak{m}$ then $L \subset K_\mathfrak{m}$.*

The theorem implies that K^{ab} is the union of ray class fields. When $\mathfrak{m} = 1$, $H := K_{\mathfrak{m}}$ is the maximal abelian unramified extension of K, called the *Hilbert class field* of K. The Artin map induces an isomorphism between the ideal class group $\mathrm{Cl}(K)$ of K and $\mathrm{Gal}(H/K)$.

We will state a corollary from CFT (in fact, from Chebotarev density theorem) that will be used for later.

Corollary 5. *Let K be a number field.*

(1) For any fractional ideal $\mathfrak{a}$ any modulus $\mathfrak{m}$ of K, there exists infinitely many prime ideals $\mathfrak{p}$ of prime norm $N\mathfrak{p} = p$ so that $[\mathfrak{a}] = [\mathfrak{p}]$ in the ray class group $Cl_{\mathfrak{m}}$.

(2) Let L, L' be finite extension of K with L Galois over K. For any finite set T of primes of K. If any prime $\mathfrak{p} \notin T$ of K that is unramified in L' and has a prime $\mathfrak{q}$ of L' lying above $\mathfrak{p}$ with inertia degree 1 in L', splits completely in L. Then $L \subset L'$.

Note that, if furthermore, L' is Galois over K, the set of all unramified primes of K in L' with inertia degree 1 are precisely primes that splits completely in L.

Proof. For (ii), we refer to [Cox, Prop.II.8.20]. Part (i) is stated in [Sil, Thm.II.3.4] but with no proof ... □

Corollary 6. *A Galois extension L/K satisfies $(\mathfrak{p}, L/K) = 1 \iff \mathfrak{p} \in P_{\mathfrak{m}}$ for almost all $\mathfrak{p}$ then $L = K_{\mathfrak{m}}$.*

3. Elliptic curves with complex multiplication

In this section, following [Sil, Sun] we define elliptic curves with complex multiplication and study their properties.

3.1. Elliptic curves and isogenies.

Let k be a field.

Definition 7. *An elliptic curve E over k is a nonsingular projective curve of genus 1 with a distinguished k-rational point $O \in E(k)$.*

Remark 8. When the field k is of characteristic different from 2 and 3, one can show that (see [Mil, Chapter II]) an elliptic curve E over k is a plane projective curve over k of the (Weierstrass) form

$$y^2z = x^3 + axz^2 + bz^3,$$

where $a, b \in k, 4a^3 + 27b^2 \neq 0$, and the distinguished point is $(0 : 1 : 0)$. For a field K/k, we denote $E(K)$ to be the set of K-rational points of E, i.e. the set of points $(x : y : z) \in \mathbb{P}^2(K)$ satisfying the above equation.

An elliptic curve E over k is in fact an abelian variety with the distinguished point $O \in E(k)$ as the identity element. In other words, $E(K)$ is an abelian group for any field extension K/k. We refer to [Sun, Lecture 2] for the defining group structure on E. We are interested in morphisms between elliptic curves that preserve this group structure.

Definition 9. *An isogeny $\phi : E_1 \to E_2$ of elliptic curves defined over k is a non-constant rational map that sends the distinguished point of E_1 to the distinguished point of E_2.*

An endomorphism of an elliptic curve E is a morphism from E to itself that fixes the distinguished element. Thus, an endomorphism on E is either a zero morphism (which sends every point on E to the distinguished point) or an isogeny. We denote $End(E)$ to be the ring of all endomorphisms of E, with multiplication given by composition and addition given by the group structure on E.

Remark 10. Equivalently, an isogeny $\phi : E_1 \to E_2$ between elliptic curves over k is a (regular) morphism such that it induces a surjective group homomorphism $E_1(\overline{k}) \to E_2(\overline{k})$ (see [Sun, Lecture 4]). This is because

(1) Any morphism of abelian varieties that preserves the identity element induces a group homomorphism.
(2) Any rational map from a smooth projective curve C_1 to a projective curve C_2 is a (regular) morphism.
(3) A morphism of projective curves is either surjective or constant.

Below are some examples of isogenies that we will need in later sections.

Example 11 (Multiplication by n map). For an elliptic curve E over k and $n \in \mathbb{Z} \setminus \{0\}$, the map $[n] : E \to E$ defined by sending $P \mapsto nP$ for all $P \in E(k)$ is an isogeny.

Example 12 (Frobenius map). Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic p. Then the Frobenius map on E, defined by $(x : y : z) \mapsto (x^q : y^q : z^q)$ is an isogeny.

Definition 13 (Degree of an isogeny)**.** *Let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves defined over k, which induces an injective map of function fields $\phi^* : k(E_2) \to k(E_1)$. The* degree *of ϕ is the degree of the finite field extension $k(E_1)/k(E_2)$. The isogeny ϕ is said to be* separable *if this field extension is separable.*

Example 14 (Frobenius map). Let E be an elliptic curve over a field k of characteristic $p > 0$. Suppose E has Weierstrass form $y^2z = x^3+axz^2+bz^3$. We can define $E^{(p)}$ by $y^2z = x^3+a^pxz^2+b^pz^3$, and a p-power Frobenius map $\pi : E \to E^{(p)}$ by $(x : y : z) \mapsto (x^p : y^p : z^p)$. This map is an isogeny of degree p.

Example 15 (Multiplication-by-n-map). Let E be an elliptic curve over field k. The multiplication-by-n map $[n] : E \to E$ has degree n^2. It is separable if and only if n is not divisible by the characteristic of k. We refer to [Sun, Lecture 5] for the proof of this.

Proposition 16. *Let ϕ be an isogeny of elliptic curves over a field k of characteristic $p > 0$. Then $\phi = \phi_{sep} \circ \pi^n$ for some separable isogeny ϕ_{sep} and integer $n \geq 0$, where π is the p-power Frobenius morphism $(x : y : z) \mapsto (x^p : y^p : z^p)$. We then have $\deg \phi = p^n \deg \phi_{sep}$.*

We refer to [Sun, Lecture 5] for the proof of this proposition.

3.2. **Elliptic curves over $\mathbb{C}$.** Here is our main theorem for this subsection.

Theorem 17 (Uniformization theorem)**.** *The following categories are equivalent:*
(1) Category of lattices in $\mathbb{C}$ (i.e. $\mathbb{Z}$-submodule of rank 2 of $\mathbb{C}$). A morphism $\Lambda \to \Lambda'$ between two lattices is given by $\alpha\Lambda \subset \Lambda'$ for some $\alpha \in \mathbb{C}$.
(2) Category of complex tori, i.e. compact connected complex Lie group, of (complex) dimension 1.
(3) Category of elliptic curves over $\mathbb{C}$, where morphisms are (regular) morphisms of varieties that send one's distinguished point to the other.

Sketch. Given a lattice Λ in $\mathbb{C}$, we can get a complex torus $\mathbb{C}/\Lambda$ and an elliptic curve

$$E_\Lambda : y^2z = 4x^3 - g_2(\Lambda)xz^2 - g_3(\Lambda)z^3,$$

where

$$g_2(\Lambda) := 60 \sum_{\Lambda\setminus\{0\}} \omega^{-4}, g_3(\Lambda) := 140 \sum_{\Lambda\setminus\{0\}} \omega^{-6}.$$

Furthermore, the map

$$\Phi : \mathbb{C}/\Lambda \to E_\Lambda(\mathbb{C}),$$
$$z \mapsto \begin{cases} (\wp(z), \wp'(z)) & z \notin \Lambda \\ 0 & z \in \Lambda \end{cases}$$

where

$$\wp(z) = z^{-2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right), \wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3},$$

is an isomorphism of complex Lie groups. □

3.3. **Elliptic curves with complex multiplication.** Given an elliptic curve E over a field k, one can classify the endomorphism algebra $\mathrm{End}^0(E) := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ as follows (see [Sun, Lecture 12] for the proof)

Theorem 18. *The $\mathbb{Q}$-algebra is $\mathrm{End}^0(E)$ is isomorphic to either $\mathbb{Q}$, an imaginary quadratic field or a quaternion algebra over $\mathbb{Q}$.*

Thus, from this theorem, we can subdivide the class of elliptic curves according to their endomorphism algebra. An elliptic curve E over k is said to have *complex multiplication (CM)* if $\mathrm{End}(E) \ncong \mathbb{Z}$, meaning $\mathrm{End}^0(E)$ is either an imaginary quadratic field or a quaternion $\mathbb{Q}$-algebra, and $\mathrm{End}(E)$ is an *order* of the $\mathbb{Q}$-algebra $\mathrm{End}^0(E)$.

When E is an elliptic curve over $\mathbb{C}$, there is an easier way to make sense of the previous theorem. Indeed, by the uniformization theorem 17, one can associate a lattice $\Lambda \subset \mathbb{C}$ so $E \cong E_\Lambda$, and the endomorphism ring can be described as

$$\mathrm{End}(E_\Lambda) \cong \mathrm{End}(\mathbb{C}/\Lambda) \cong \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}, \tag{1}$$

which serves as motivation for the name 'complex multiplication'.

Given an imaginary quadratic field K, we are interested in elliptic curves over $\mathbb{C}$ so that $\mathrm{End}(E) \cong \mathcal{O}_K$. In this case, we will say E has *CM by $\mathcal{O}_K$*. Note that the previous argument implies $\mathrm{End}^0(E) \cong K$, and we can always choose an embedding of $\mathrm{End}^0(E)$ into $\mathbb{C}$ so that one can identify $\mathcal{O}_K$ with $\mathrm{End}(E_\Lambda)$ via the commutative diagram where $\alpha \in \mathcal{O}_K$

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{\sim} & E_\Lambda \\ \downarrow{\scriptstyle z \mapsto \alpha z} & & \downarrow{\scriptstyle [\alpha]} \\ \mathbb{C}/\Lambda & \xrightarrow{\sim} & E_\Lambda \end{array}$$

This is known as the *normalized identification* of $\mathrm{End}(E)$ with $\mathcal{O}_K$. This identification is compatible with maps between elliptic curves with CM by $\mathcal{O}_K$ [1].

Theorem 19 (Classification of CM elliptic curves)**.** *Let K be an imaginary quadratic field. There is a bijection between the ideal class group $Cl(K)$ of K and the set $\mathcal{E}_{\mathbb{C}}(K)$ of isomorphic classes of elliptic curves over $\mathbb{C}$ that has CM by $\mathcal{O}_K$, given by*

$$Cl(K) \to \mathcal{E}_{\mathbb{C}}(K) : [\mathfrak{a}] \mapsto \mathbb{C}/\mathfrak{a}.$$

Sketch. A fractional ideal $\mathfrak{a} \in \mathrm{Cl}(K)$ is a lattice in $\mathbb{C}$. Since for every $\lambda \in \mathcal{O}_K$, one has $\lambda\mathfrak{a} \subset \mathfrak{a}$, so $\mathcal{O}_K \subset \mathrm{End}(\mathbb{C}/\mathfrak{a})$. Since $\mathcal{O}_K$ is of maximal order of K, and $\mathrm{End}(\mathbb{C}/\mathfrak{a})$ is also an order of K, we find $\mathrm{End}(\mathbb{C}/\mathfrak{a}) = \mathcal{O}_K$. Conversely, given a lattice Λ in $\mathbb{C}$ so $\mathrm{End}(E) = \mathcal{O}_K$, by (1), Λ is a fractional ideal of K. □

In particular, since the class group $\mathrm{Cl}(K)$ is finite, up to isomorphism, there are finitely many elliptic curves with CM by $\mathcal{O}_K$.

[1] Another way to describe this identification $[\cdot] : \mathcal{O}_K \to \mathrm{End}(E)$: For any invariant differential ω on E, $[\alpha]^*\omega = \alpha\omega$ for all $\alpha \in \mathcal{O}_K$. We refer to [Sil, Prop.II.1.1] for more details.

3.4. **The j-invariant and rationality of elliptic curves with CM.** Let E be an elliptic curve over a field k (for convenience, suppose char $k \neq 2, 3$), then E has Weierstrass form $y^2z = x^3 + Axz^2 + Bz^3$.

Definition 20. *The j-invariant of the elliptic curve E is defined to be $j(E) = 1728\frac{4A^3}{4A^3+27B^2}$.*

Proposition 21. *(a) For every $j_0 \in k$, there is an elliptic curve over k with j-invariant $j(E) = j_0$.*

(b) Let E and E' be elliptic curves over k, then E and E' are isomorphic over $\overline{k}$ if and only if $j(E) = j(E')$. If $j(E) = j(E')$ and char $k \neq 2, 3$, then there exists a field extension K/k of degree at most 6 such that E and E' are isomorphic over K.

We refer to [Sun, Lecture 13] for the proof of this proposition. The following result says that elliptic curves over $\mathbb{C}$ with CM by $\mathcal{O}_K$ are defined over algebraic extension over $\mathbb{Q}$.

Proposition 22. *Let K be an imaginary quadratic field. Let $\mathcal{E}_{\overline{\mathbb{Q}}}(K)$ be the category of isomorphism classes of elliptic curves over $\overline{\mathbb{Q}}$ that have CM by $\mathcal{O}_K$. Then the natural map $\mathcal{E}_{\overline{\mathbb{Q}}}(K) \xrightarrow{\sim} \mathcal{E}_{\mathbb{C}}(K)$ is an isomorphism of categories.*

Sketch. There are a few steps:

(1) For $E \in \mathcal{E}_{\mathbb{C}}(K)$ then $j(E)$ is an algebraic number. Indeed, let $\sigma \in \mathrm{Aut}(\mathbb{C}$, let E^σ denote the elliptic curve defined by $y^2z = x^3 + \sigma(A)xz^2 + \sigma(B)z^3$. Since $\mathrm{End}(E) \xrightarrow{\sim} \mathrm{End}(E^\sigma)$ so $E^\sigma \in \mathcal{E}_{\mathbb{C}}(K)$. By Theorem 19, E^σ is one of finitely many isomorphism classes of elliptic curves, implying $j(E^\sigma) = j(E)^\sigma$ attains at most $h = |\mathrm{Cl}(K)|$ values from Proposition 21. Thus, $j(E)$ is algebraic.

(2) Given $E \in \mathcal{E}_{\mathbb{C}}(K)$, as $j(E) \in \overline{\mathbb{Q}}$, from Proposition 21(a), there exists an elliptic curve E' over $\mathbb{Q}(j(E))$ with j-invariant $j(E') = j(E)$, implying $E \cong E'$ over $\overline{\mathbb{Q}}$. Thus, the map $\mathcal{E}_{\overline{\mathbb{Q}}}(K) \xrightarrow{\sim} \mathcal{E}_{\mathbb{C}}(K)$ is surjective at the level of objects.

(3) To show the map is injective at the level of objects, suppose $E, E' \in \mathcal{E}_{\overline{\mathbb{Q}}}(K)$ so that $E \cong E'$ over $\mathbb{C}$. By Proposition 21, we know $j(E) = j(E') \in \overline{\mathbb{Q}}$ and by using this proposition again, we find $E \cong E'$ over $\overline{\mathbb{Q}}$.

(4) To show surjection at the level of morphisms for the map $\mathcal{E}_{\overline{\mathbb{Q}}}(K) \xrightarrow{\sim} \mathcal{E}_{\mathbb{C}}(K)$, we show that for every elliptic curves E_1, E_2 defined over some field $L \subset \mathbb{C}$, then there is a finite extension L'/L so that every isogeny from E_1 to E_2 is defined over L'. We refer to [Sil, Theo.II.2.2] for this argument.

□

Thus, from now on, we will denote $\mathcal{E}(K)$ to mean both $\mathcal{E}_{\overline{\mathbb{Q}}}(K)$ and $\mathcal{E}_{\mathbb{C}}(K)$, or even $\{j(E) : E \in \mathcal{E}(K)\} \subset \overline{\mathbb{Q}}$.

3.5. **Reduction theory of elliptic curves with CM.** Let E be an elliptic curve over $\mathbb{C}$ with CM by $\mathcal{O}_K$. From proposition 22, E can be defined over a finite extension $M \supset \mathbb{Q}(j(E))$ that has Weierstrass equation $y^2z = x^3 + Axz^2 + Bz^3$ with $A, B \in \mathcal{O}_M$. For each prime $\mathfrak{q}$ of M, as long as $\Delta(E) := 4A^3 + 27B^2$ is nonzero under taking modulo $\mathfrak{q}$, we can obtain an elliptic curve $\tilde{E}$ over $\mathbb{F}_\mathfrak{q} = \mathcal{O}_L/\mathfrak{q}$ defined by $y^2z = x^3 + \overline{A}xz^2 + \overline{B}z^3$. We then say E has *good reduction modulo* $\mathfrak{q}$. This holds for all but finitely many primes $\mathfrak{q}$ of M as there are only finitely many primes $\mathfrak{q}$ dividing $\Delta(E)\mathcal{O}_M$.

4. Hilbert class field of imaginary quadratic field

We state the main theorem for this notes.

Theorem 23. *Let K be an imaginary quadratic field, E be an elliptic curve with CM by $\mathcal{O}_K$. Then $H = K(j(E))$ is the maximal unramified abelian extension of K.*

We will spend this whole section outlining the proof of this theorem. We learned this proof from [Sun, Lecture 21], [Sil, Theorem II.4.1], [LiCM] and [Cox, Chap.III].

4.1. **Action of $\mathbf{Cl}(K)$ and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathcal{E}(K)$.** There is an action of the class group $\mathrm{Cl}(K)$ on $\mathcal{E}(K)$, the set isomorphism classes of elliptic curves over $\mathbb{C}$ with CM by $\mathcal{O}_K$, given by

$$[\mathfrak{a}] \cdot (\mathbb{C}/\mathfrak{b}) := \mathbb{C}/(\mathfrak{a}^{-1}\mathfrak{b}),$$

where $[\mathfrak{a}] \in \mathrm{Cl}(K), \mathbb{C}/\mathfrak{b} \in \mathcal{E}_{\mathbb{C}}(K)$. From Theorem 19, this action is transitive and free.

Because from Proposition 22, $E \in \mathcal{E}(K)$ is defined over an algebraic extension of $\mathbb{Q}$, i.e. E has Weierstrass form $y^2z = x^3 + Axz^2 + Bz^3$ where $A, B \in \overline{\mathbb{Q}}$. For $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we can define E^σ by $y^2z = x^3 + \sigma(A)xz^2 + \sigma(B)z^3$. Note that σ also induces an isomorphism $\mathrm{End}(E) \xrightarrow{\sim} \mathrm{End}(E^\sigma)$ so $E^\sigma \in \mathcal{E}(K)$. Thus, we have defined an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathcal{E}(K)$.

Proposition 24. *There is a well-defined group homomorphism*

$$F : \mathrm{Gal}(\overline{K}/K) \to Cl(K),$$

characterized by the property

$$E^\sigma = F(\sigma) \cdot E \qquad \text{for all } \sigma \in \mathrm{Gal}(\overline{K}/K), E \in \mathcal{E}(K).$$

The map F induces an injective group homomorphism

$$F : \mathrm{Gal}(K(j(E_1), \cdots, j(E_h))/K) \to Cl(K),$$

where h is the class number, E_i's are representatives of elements in $\mathcal{E}(K)$.

Sketch. For $E \in \mathcal{E}(K)$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$, since the action of $\mathrm{Cl}(K)$ on $\mathcal{E}(K)$ is transitive, there is $[\mathfrak{a}] \in \mathrm{Cl}(K)$ so $E^\sigma \cong [\mathfrak{a}] \cdot E$. We define $F(\sigma) := [\mathfrak{a}]$.

There is a nontrivial result that for any $E \in \mathcal{E}(K), [\mathfrak{a}] \in \mathrm{Cl}(K)$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then

$$([\mathfrak{a}] \cdot E)^\sigma = [\mathfrak{a}^\sigma] \cdot E^\sigma.$$

We refer to [Sil, Prop.II.2.5] for the proof. This result would imply that the definition of F is independent of the choice of elliptic curve. It is then not difficult to show that F is a group homomorphism.

Let L be the fixed field of $\ker F$, then

$$\begin{aligned}
\mathrm{Gal}(\overline{K}/L) &:= \ker F, \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : E^\sigma = E \ \forall E \in \mathcal{E}(K)\}, \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : j(E^\sigma) = j(E) \ \forall E \in \mathcal{E}(K)\}, \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : j(E)^\sigma = j(E) \ \forall E \in \mathcal{E}(K)\}, \\
&= \mathrm{Gal}(\overline{K}/K(j(E_1), \cdots, j(E_h))).
\end{aligned}$$

Thus, $L = K(j(E_1), \cdots, j(E_h))$.

F induces an injection (since L is Galois)

$$F : \mathrm{Gal}(K(j(E_1), \cdots, j(E_h))/K) \to \mathrm{Cl}(K),$$

implying that $K(j(E_1), \cdots, j(E_h))$ is an abelian extension. □

4.2. **Using reduction theory of elliptic curves.** We wish to prove that $K(j(E_1),\dots,j(E_h))$ is the Hilbert class field of K, and furthermore, the map

$$F : \mathrm{Gal}(K(j(E_1),\cdots,j(E_h))/K) \to \mathrm{Cl}(K)$$

is precisely the inverse of the Artin map, as defined in Theorem 4 of class field theory.

Let S be a set of primes of K satisfying

(i) $\mathfrak{p}$ is lying above a prime p of $\mathbb{Q}$ that splits completely in K,
(ii) $\mathfrak{p}$ is unramified in $K(j(E_1),\cdots,j(E_h))$,
(iii) Each $j(E) \in \mathcal{E}(K)$ is the j-invariant of an elliptic curve E defined over $M \supset K(j(E_1),\cdots,j(E_h))$ that has good reduction modulo every prime $\mathfrak{q} \mid \mathfrak{p}$.
(iv) All the j-invariants $j(E) \in \mathcal{O}_M$ are distinct modulo every prime $\mathfrak{q} \mid \mathfrak{p}$.

Note that conditions (ii)-(iv) remove only finite number of primes from condition (i).

Lemma 25. *If for all $\mathfrak{p} \in S$, we have $F(Frob_{\mathfrak{p}}) = [\mathfrak{p}]$, then $K(j(E_1),\cdots,j(E_h))$ is the Hilbert class field of K, and F is the inverse of the Artin map.*

Proof. Let H be the Hilbert class field of K. We first show that $H \subset K(j(E_1),\cdots,j(E_h))$ using corollary 5. Indeed, let p be a prime of $\mathbb{Q}$ so that p is unramified in $K(j(E_1),\cdots,j(E_h))$ and there is a prime ideal $\mathfrak{q}$ of $K(j(E_1),\cdots,j(E_h))$ lying above p so that the inertia degree $f_{\mathfrak{q}|p} = 1$. We want to show that almost all such prime p splits completely in H.

The existence of $\mathfrak{q}$ implies that p must split completely as $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ in K. Hence, except finitely many such prime p, there is a prime $\mathfrak{p}$ of K lying above p so $\mathfrak{p} \in S$.

We have $F(\mathrm{Frob}_{\mathfrak{p}}) = [\mathfrak{p}]$, which implies $E^{\mathrm{Frob}_{\mathfrak{p}}} \cong [\mathfrak{p}]\cdot E$, implying $j(E)^{\mathrm{Frob}_{\mathfrak{p}}} = j(E^{\mathrm{Frob}_{\mathfrak{p}}}) = j([\mathfrak{p}]\cdot E)$ because of Proposition 21. By the definition of Frobenius map over $K(j(E_1),\cdots,j(E_h))/K$, we find $j(\mathfrak{p}\cdot E)^{N\mathfrak{p}} \equiv j(E) \pmod{\mathfrak{q}}$ for any prime $\mathfrak{q}$ of $K(j(E_1),\cdots,j(E_h))$ lying above $\mathfrak{p}$. Note $N\mathfrak{p} = p$ because of condition (i), and $j(\mathfrak{p}\cdot E)^p \equiv j(\mathfrak{p}\cdot E) \pmod{\mathfrak{q}}$ since $f_{\mathfrak{q}|\mathfrak{p}} = 1$ for certain $\mathfrak{q}$. Thus, we find $j(\mathfrak{p}\cdot E) \equiv j(E) \pmod{\mathfrak{q}}$. Because of (iv), we find $j(\mathfrak{p}\cdot E) = j(E)$, hence $[\mathfrak{p}]\cdot E \cong E$. Since the action of $\mathrm{Cl}(K)$ on $\mathcal{E}(K)$ is free, we find $\mathfrak{p}$ to be a principal ideal of $\mathcal{O}_K$, giving trivial Artin map $\mathrm{Frob}_{\mathfrak{p}} = 1$ for the Hilbert class group H. Therefore, p splits completely in H. Hence, we have shown $H \subset K(j(E_1),\cdots,j(E_h))$.

Next, we will show the map F is an isomorphism. We already know F is injective. To show F is surjective, let $\alpha \in \mathrm{Cl}(K)$, then by corollary 5, we know there are infinitely many prime ideal $\mathfrak{p}$ of prime norm so $[\mathfrak{p}] = \alpha$ in $\mathrm{Cl}(K)$. As almost all such prime satisfies condition (i), hence there exists $\mathfrak{p} \in S$ so $[\mathfrak{p}] = \alpha$, giving $F(\mathrm{Frob}_{\mathfrak{p}}) = [\mathfrak{p}] = \alpha$. Thus, F is surjective.

By class field theory Theorem 4, we then know

$$\begin{aligned}[K(j(E_1),\cdots,j(E_h)) : K] &= |\,\mathrm{Gal}(K(j(E_1),\cdots,j(E_h))/K)|,\\ &= |\mathrm{Cl}(K)| = |\,\mathrm{Gal}(H/K)| = [H : K],\end{aligned}$$

giving $H = K(j(E_1),\cdots,j(E_h))$, as desired. □

Lemma 26. *For $\mathfrak{p} \in S$, we have $F(Frob_{\mathfrak{p}}) = [\mathfrak{p}]$.*

Proof. We wish to show $E^{\mathrm{Frob}_{\mathfrak{p}}} \cong [\mathfrak{p}]\cdot E$ for $E \in \mathcal{E}(K)$. As $\mathfrak{p} \in S$, let $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$. By corollary 5, there are prime $\mathfrak{a}$ of $\mathcal{O}_K$ not lying above p so $[\mathfrak{a}] = [\overline{\mathfrak{p}}]$. It means $[\mathfrak{a}\mathfrak{p}] = 1$ in $\mathrm{Cl}(K)$, hence $\mathfrak{p}\mathfrak{a} = \alpha\mathcal{O}_K$ for some $\alpha \in \mathfrak{p}$.

Suppose $E \cong \mathbb{C}/\mathfrak{b}$ over $\mathbb{C}$, we consider isogenies $\lambda : E \to [\mathfrak{p}]\cdot E$ and $\mu : [\mathfrak{p}]\cdot E \to E$, defined as follows

$$\begin{array}{ccccccc}
\mathbb{C}/\mathfrak{b} & \xrightarrow{z\mapsto z} & \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{b} & \xrightarrow{z\mapsto z} & \mathbb{C}/(\mathfrak{a}^{-1}\mathfrak{p}^{-1}\mathfrak{b}) & \xrightarrow{z\mapsto \alpha z} & \mathbb{C}/\mathfrak{b} \\
\downarrow\sim & & \downarrow\sim & & \downarrow\sim & & \downarrow\sim \\
E & \xrightarrow{\lambda} & [\mathfrak{p}]\cdot E & \xrightarrow{\mu} & [\mathfrak{a}\mathfrak{p}]\cdot E & \xrightarrow{\sim} & E
\end{array}$$

Via the normalized identification of $\mathcal{O}_K$ and $\mathrm{End}(E)$, we know that $\mu \circ \lambda = [\alpha]$. We compute that $\deg \lambda = \#(\mathfrak{p}^{-1}\mathfrak{b})/\mathfrak{b} = N\mathfrak{p} = p$ and $\deg \mu = \#(\alpha\mathfrak{b})/(\mathfrak{p}^{-1}\mathfrak{b}) = N(\mathfrak{a})$, which is coprime to p by our choice of $\mathfrak{a}$ [2].

From condition (iii), we can suppose that E has good reduction modulo prime $\mathfrak{q}$ lying above $\mathfrak{p}$ of some finite extension $M \supset K(j(E_1), \cdots, j(E_h))$. Note that by Proposition 22, we can choose M so every isogeny between $E \in \mathcal{E}(K)$ is defined over M. Hence, we can reduction modulo $\mathfrak{q}$ to obtain isogeny $\tilde{\lambda} \circ \tilde{\mu} = \widetilde{[\alpha]} \in \mathrm{End}(\tilde{E})$. Since $\alpha \in \mathfrak{p} \subset \mathfrak{q}$, we find $\widetilde{[\alpha]}$ is inseparable [3]. Because good reduction preserves degree (see [Sil, Prop.II.4.4]), we find that $\deg \tilde{\mu} = N\mathfrak{a}$ is prime to p, hence is separable by Proposition 16. It follows then $\tilde{\lambda}$ is inseparable of degree p. By Proposition 16, $\tilde{\lambda}$ is the composition of the p-power Frobenius $\tilde{E} \to \tilde{E}^{(p)} = \widetilde{E^{\mathrm{Frob}_\mathfrak{p}}}$ and an isomorphism $\widetilde{E^{\mathrm{Frob}_\mathfrak{p}}} \to \widetilde{[\mathfrak{p}] \cdot E}$. This isomorphism implies $j(E^{\mathrm{Frob}_\mathfrak{p}}) \equiv j(\mathfrak{p} \cdot E) \pmod{\mathfrak{q}}$. According to (iv), we find $E^{\mathrm{Frob}_\mathfrak{p}} = [\mathfrak{p}] \cdot E$ in $\mathcal{E}(K)$, as desired. □

Lemma 27. *Given any $E \in \mathcal{E}(K)$, the set $j(E_1), \ldots, j(E_h)$ are all the $\mathrm{Gal}(\overline{K}/K)$ conjugates for $j(E)$. This gives $K(j(E)) = K(j(E_1), \ldots, j(E_h))$.*

Proof. From Lemma 25, we know $F : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Cl}(K)$ is surjective. By the definition of F, and the fact that $\mathrm{Cl}(K)$ acts on $\mathcal{E}(K)$ transitively, we know $\mathrm{Gal}(\overline{K}/K)$ also acts on $\mathcal{E}(K)$ transitively. As $j(E^\sigma) = j(E)^\sigma$, we are done. □

These three lemmas completes the proof of our main theorem 23.

[2] Here is a brief explanation on why we can compute the degree like this: Over field k of characteristic 0, any isogeny $\phi : E_1 \to E_2$ is separable and its degree equals $\#\ker\phi = \#\{x \in E_1(\overline{k}), \phi(x) = 0\}$ (see [Sun, Lecture 5]), which is finite. We then apply this for $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ where $\Lambda \subset \Lambda'$ lattices in $\mathbb{C}$, giving $\deg\phi = \#\Lambda'/\Lambda$. See [Sun, Lecture 17.5] for more details

[3] the argument here is that an isogeny $\phi : E_1 \to E_2$ is separable iff the induced map ϕ^* on the differentials is nonzero. We know α^* is a linear map over $\mathbb{F}_\mathfrak{q}$ given by $\tilde{\omega} \mapsto \tilde{\alpha}\tilde{\omega}$. As $\alpha \in \mathfrak{q}$, so $\tilde{\alpha}^* = 0$, implying $\tilde{\alpha}$ is inseparable

5. Ray class field of imaginary quadratic field

5.1. **Motivation for the construction of explicit ray class fields.** We recall, from previous section, in order to look for generators of the Hilbert class field H of an imaginary quadratic field K, we let $\mathrm{Gal}(H/K)$ acts on this set of generators, which, in this case, is $\mathcal{E}(K)$, the set of isomorphism classes of elliptic curves with CM by $\mathcal{O}_K$. Magically, the class group $\mathrm{Cl}(K)$ also acts on this set and the two actions are compatible with the Artin map, i.e. one get one action from the other via the Artin map $\mathrm{Cl}(K) \cong \mathrm{Gal}(H/K)$. This compatibility allows us to verify that the set really consists of generators of H using class field theory. Furthermore, because the action of $\mathrm{Cl}(K)$ on $\mathcal{E}(K)$ is quite explicit, we obtain an explicit description of the Galois group $\mathrm{Gal}(H/K)$.

For the ray class field $K_{\mathfrak{m}}$ of K where $\mathfrak{m}$ is a modulus of K (which in this case, $\mathfrak{m}$ is just an ideal of $\mathcal{O}_K$ as K is imaginary quadratic), from the analogy with Kronecker-Weber theorem for $\mathbb{Q}$, we wish that the generators of $K_{\mathfrak{m}}$ can be constructed from elements in the $\mathfrak{m}$-torsion subgroup $E[\mathfrak{m}]$ of $E \in \mathcal{E}(K)$. We first give a definition of this set.

Definition 28. *Let E be an elliptic curve with CM by $\mathcal{O}_K$, and let $\mathfrak{m}$ be an ideal of $\mathcal{O}_K$. The* $\mathfrak{m}$-torsion subgroup *of E is defined by*

$$E[\mathfrak{m}] := \{P \in E(\overline{\mathbb{Q}}) : [\alpha] \cdot P = 0 \ \forall \alpha \in \mathfrak{m}\}$$

Remark 29. Under normalized identification, if E corresponds to the torus $\mathbb{C}/\mathfrak{a}$ for some fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$, then $E[\mathfrak{m}] = \mathfrak{m}^{-1}\mathfrak{a}/\mathfrak{a}$.

Now, we want to analyze at the actions of $\mathrm{Gal}(K_{\mathfrak{m}}/K)$ and the ray class group $\mathrm{Cl}_{\mathfrak{m}} = I_{\mathfrak{m}}/P_{\mathfrak{m}}$ on the $\mathfrak{m}$-torsion points of $\mathcal{E}(K)$:

For an ideal class $\mathfrak{a} \in \mathrm{Cl}_{\mathfrak{m}}$, we have an isogeny $[\mathfrak{a}] : E \to [\mathfrak{a}] \cdot E = E^{(H/K,\mathfrak{a})}$ which induces a map on the $\mathfrak{m}$-torsion subgroups. On the other hand, as E is defined over $H \subset K_{\mathfrak{m}}$, the image $(K_{\mathfrak{m}}/K, \mathfrak{a})$ of $\mathfrak{a}$ under the Artin map also induces a map $(K_{\mathfrak{m}}/K, \mathfrak{a}) : E \to E^{(K_{\mathfrak{m}}/K,\mathfrak{a})} = E^{(H/K,\mathfrak{a})}$ given by $(x, y) \mapsto (x^{(K_{\mathfrak{m}}/K,\mathfrak{a})}, y^{(K_{\mathfrak{m}}/K,\mathfrak{a})})$, which also descends to a map on the $\mathfrak{m}$-torsion subgroups. Even though the map $(K_{\mathfrak{m}}/K, \mathfrak{a})$ is not necessarily an isogeny, we shall show later that there exists $\epsilon \in \mathrm{Aut}(E^{(K_{\mathfrak{m}}/K,\mathfrak{a})})$ so $\epsilon \circ [\mathfrak{a}] = (K_{\mathfrak{m}}/K, \mathfrak{a})$ on $E[\mathfrak{m}]$. This means that the actions of $\mathrm{Gal}(K_{\mathfrak{m}}/K)$ and $\mathrm{Cl}_{\mathfrak{m}}$ on the $\mathfrak{m}$-torsion points of elliptic curves in $\mathcal{E}(K)$ are compatible up to automorphisms of elements in $\mathcal{E}(K)$ (see Lemma 34). Suppose now that $\mathfrak{a} \in P_{\mathfrak{m}}$, i.e. $\mathfrak{a} = (\alpha)$ for $\alpha \in \mathcal{O}_K$ and $\alpha \equiv 1 \pmod{\mathfrak{m}}$ then $(K_{\mathfrak{m}}/K, \mathfrak{a}) = 1$, meaning it acts trivially on $E[\mathfrak{m}]$. On the other hand, we cannot tell much about how $\epsilon \circ [\mathfrak{a}] \in \mathrm{Aut}(E) = \mathcal{O}_K^\times$ acts on $E[\mathfrak{m}]$. This suggests that the $\mathfrak{m}$-torsion points of $\mathcal{E}(K)$ are not the generators of $K_{\mathfrak{m}}$. However, if instead we act these groups on $E[\mathfrak{m}]/\mathrm{Aut}(E)$ then the two actions are compatible (at least so far, we see it for $\mathfrak{a} \in P_{\mathfrak{m}}$). This motivates the definition of the Weber function, which is a finite map $h : E \to E/\mathrm{Aut}(E) \cong \mathbb{P}^1$.

Definition 30. *For $E \in \mathcal{E}(K)$, which is defined over H, a* Weber function for E *is a map $h : E \to E/\mathrm{Aut}(E) \cong \mathbb{P}^1$ defined over H.*

Remark 31. For example, if E has Weierstrass equation of the form $y^2 = x^3 + Ax + B$ with $A, B \in H$, then we can define

$$h(x, y) = \begin{cases} x & AB \neq 0 \\ x^2 & B = 0 \\ x^3 & A = 0. \end{cases}$$

We can also define h analytically (see [Sil, Example 5.5.2]).

Here is the main take-away property of this Weber function

Proposition 32. *Let E be an elliptic curve defined over $\mathbb{C}$. Then*

(1) For $P, P' \in E$ then $h(P) = h(P')$ iff $P = \epsilon P'$ for some $\epsilon \in \mathrm{Aut}(E)$;

(2) If $\phi : E \to E'$ is an isomorphism of elliptic curves then $h_E = h'_E \circ \phi$, where h_E denotes the Weber function of E.

We are now comfortable enough to state the main theorem for explicit ray class fields.

Theorem 33. *Let E be an elliptic curve over H with CM by $\mathcal{O}_K$* [4] *with its Weber function h, then for any modulus $\mathfrak{m}$ of K (as K is imaginary quadratic, a modulus $\mathfrak{m}$ is simply an ideal of $\mathcal{O}_K$), $K(j(E)h(E[\mathfrak{m}])) = H(h(E[\mathfrak{m}]))$ is the ray class field of K of modulus $\mathfrak{m}$.*

5.2. **Actions of Galois groups and ray class on $\mathfrak{m}$-torsion points.** Following our theme in the motivation section, we will investigate two actions on the $\mathfrak{m}$-torsion points of $\mathcal{E}(K)$: one of $\mathfrak{a} \in \mathrm{Cl}_{\mathfrak{m}}$ via the isogeny $[\mathfrak{a}] : E \to [\mathfrak{a}] \cdot E = E^{(H/K,\mathfrak{a})}$; second of $(H/K, \mathfrak{a}) \in \mathrm{Gal}(H/K)$ via the map $E \to E^{(H/K,\mathfrak{a})}$ sending $(x, y) \mapsto (x^{(H/K,\mathfrak{a})}, y^{(H/K,\mathfrak{a})})$. Because of corollary 5, one can replace $\mathfrak{a}$ with prime ideals $\mathfrak{p}$ of prime norm $N\mathfrak{p} = p$ that belongs to the same ray class in $\mathrm{Cl}_{\mathfrak{m}}$.

In fact, from now on, we will consider the following set $T \subset S$ of prime ideals of K (the set S is defined in our proof of explicit Hilbert class field by four conditions (i)-(iv)):

(v) There exists a finite extension $M \supset H$ so that every element of $\mathrm{Hom}(E, E')$ for $E, E' \in \mathcal{E}(K)$ is defined over M. Because each $E \in \mathcal{E}(K)$ has good reduction modulo all but finitely many primes in M, we can remove a finite set of primes in S to get set $T \subset S$, so every element of $\mathrm{Hom}(E, E')$ for $E, E' \in \mathcal{E}(K)$ decends to $\mathcal{O}_M/\mathfrak{q}$- isogeny for every prime $\mathfrak{q}$ of M lying above $\mathfrak{p} \in T$.

(vi) The $\mathfrak{p}$ lying above p satisfies $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ (from condition (i)) where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are coprime to $\mathfrak{m}$. This guarantees that the reduction map $E[\mathfrak{m}] \to \widetilde{E}[\mathfrak{m}]$ is injective (see [Sil1, VII.3. Proposition 3.1.]).

Note that these conditions also remove only finite number of primes from condition (i) (which asserts that prime $\mathfrak{p}$ has prime norm).

Lemma 34. *Let $\mathfrak{p} \in T$ and let E be an elliptic curve with CM by $\mathcal{O}_K$. Then there exists $\epsilon \in \mathrm{Aut}(E^{Frob_{\mathfrak{p}}})$ so that the two maps $\epsilon \circ [\mathfrak{p}]$ and $Frob_{\mathfrak{p}} = (H/K, \mathfrak{p})$ from E to $E^{Frob_{\mathfrak{p}}}$ agree with each other on $E[\mathfrak{m}]$.*

Sketch. We consider the number field M as in conditions (iii)-(v) so that taking reduction of E modulo prime $\mathfrak{q}$ of M lying above $\mathfrak{p}$ is nice. In particular, the reduction map $\mathrm{End}_M(E) \to \mathrm{End}_{\mathcal{O}_M/\mathfrak{q}}(\widetilde{E})$ makes sense. In fact, it is injective, see [Sil, II.4 Proposition 4.4.].

From Proposition 16 and that $N\mathfrak{p} = p$, we know that the isogeny $[\mathfrak{p}] : E \to [\mathfrak{p}] \cdot E = E^{\mathrm{Frob}_{\mathfrak{p}}}$ of degree p factors under reduction any modulo prime $\mathfrak{q} \mid \mathfrak{p}$ of M as

$$\widetilde{[\mathfrak{p}]} : \widetilde{E} \xrightarrow{\pi} \widetilde{E}^{(p)} = \widetilde{E^{\mathrm{Frob}_{\mathfrak{p}}}} \xrightarrow{\widetilde{\epsilon}} \widetilde{E}^{(p)}$$

where $\widetilde{\epsilon} \in \mathrm{Aut}_{\mathcal{O}_M/\mathfrak{q}}(\widetilde{E}^{(p)})$ and π is the p-power Frobenius map $(x, y) \mapsto (x^p, y^p)$.

Next, we show that there exists a lift $\epsilon \in \mathrm{Aut}(E^{\mathrm{Frob}_{\mathfrak{p}}})$ of $\widetilde{\epsilon}$. Indeed, if $\widetilde{\epsilon}$ is a multiplication-by-n map then it is clear, so we suppose $\widetilde{\epsilon} \notin \mathbb{Z}$. As $\widetilde{\epsilon}$ commutes with every endomorphism of $\widetilde{E}^{(p)}$ (see [Sil, Proposition 5.3]), we find $\mathrm{End}(\widetilde{E}^{(p)})$ can only be an order of an imaginary quadratic field (as we know the classification of endomorphism rings of elliptic curves, being discussed before). As the reduction map $\mathrm{End}_M(E) \to \mathrm{End}_{\mathcal{O}_M/\mathfrak{q}}(\widetilde{E})$ is injective, so its image $\mathrm{End}(E) = \mathcal{O}_K$, which is a maximal order of K, must be all of $\mathrm{End}_{\mathcal{O}_M/\mathfrak{q}}(\widetilde{E})$. This means there exists a lift $\epsilon \in \mathrm{Aut}(E^{\mathrm{Frob}_{\mathfrak{p}}})$ of $\widetilde{\epsilon}$.

[4] such elliptic curve exists: indeed, as $H = K(j(E'))$ for any elliptic curve with CM by $\mathcal{O}_K$, by Proposition 21, there exists elliptic curve E over $H = K(j(E'))$ with j-invariant $j(E) = j(E')$, implying $E \equiv E'$ over $\overline{\mathbb{Q}}$

Then $\phi = \epsilon^{-1} \circ [\mathfrak{p}]$ satisfies $\widetilde{\phi} = \widetilde{\text{Frob}_\mathfrak{p}}$ where $\text{Frob}_\mathfrak{p} : E \to E^{\text{Frob}_\mathfrak{p}}$ is defined by $(x, y) \mapsto (x^{\text{Frob}_\mathfrak{p}}, x^{\text{Frob}_\mathfrak{p}})$. Because the reduction map $E^{\text{Frob}_\mathfrak{p}}[\mathfrak{m}] \to \widetilde{E^{\text{Frob}_\mathfrak{p}}}[\mathfrak{m}]$ is injective from condition (vi), we find $\phi = \epsilon^{-1} \circ [\mathfrak{p}] = \text{Frob}_\mathfrak{p}$ on $E[\mathfrak{m}]$. □

Corollary 35. *$K(j(E), h(E[\mathfrak{m}]))$ is Galois over K.*

Proof. It suffices to show $K(j(E), h(E[\mathfrak{m}]))/K$ is a normal extension. Let $\tau \in \text{Gal}(\overline{K}/K(j(E), h(E[\mathfrak{m}])))$ and $\sigma \in \text{Gal}(\overline{K}/K)$, we want to show $\sigma\tau\sigma^{-1}$ fixes $j(E)$ and $h(P)$ for all $P \in E[\mathfrak{m}]$. As H/K is normal, we know $\sigma\tau\sigma^{-1}$ fixes $H = K(j(E))$ and that $E = E^{\sigma\tau\sigma^{-1}}$. Hence, $\sigma\tau\sigma^{-1}(h(P)) = h(P^{\sigma\tau\sigma^{-1}})$.

On the other hand, by class field theory, there exists $\mathfrak{a} \in \text{Cl}(K)$ so $\sigma\tau\sigma^{-1}|_H = (H/K, \mathfrak{a})$. By corollary 5, one can choose $\mathfrak{p} \in T$ so $(H/K, \mathfrak{a}) = (H/K, \mathfrak{p}) = \text{Frob}_\mathfrak{p}$. As we know $\text{Frob}_\mathfrak{p}|_H = 1$ so using Lemma 34, we find that $\sigma\tau\sigma^{-1} : E[\mathfrak{m}] \to E[\mathfrak{m}]$ comes from an element in $\text{Aut}(E) = \mathcal{O}_K^\times$, i.e. there is $\epsilon \in \text{Aut}(E)$ so $\epsilon(P) = P^{\sigma\tau\sigma^{-1}}$ for all $P \in E[\mathfrak{m}]$. This means $h(P) = h(P^{\sigma\tau\sigma^{-1}})$, as desired. □

5.3. **Proof of Theorem 33 for explicit ray class fields.** As we know that $K(j(E), h(E[\mathfrak{m}]))$ is Galois, from Chebotarev's density theorem corollary 5, it suffices to show that for all primes $\mathfrak{p}$ of K except those in a finite set, $\mathfrak{p}$ splits completely in $K(j(E), h(E[\mathfrak{m}]))$ iff it splits completely in $K_\mathfrak{m}$, the ray class field of modulus $\mathfrak{m}$ of K. The former is equivalent to saying $\text{Frob}_\mathfrak{p} = 1$ on $K(j(E), h(E[\mathfrak{m}]))$, while the latter is equivalent to saying $\mathfrak{p} \in P_\mathfrak{m}$, i.e. $\mathfrak{p} = (\alpha)$ for $\alpha \in \mathcal{O}_K$ and $\alpha \equiv 1 \pmod{\mathfrak{m}}$ (see corollary 6). To prove this, it suffices to consider $\mathfrak{p} \in T$ (as being split in either $K_\mathfrak{m}$ or $K(j(E), h(E[\mathfrak{m}]))$ would imply splitting in $H = K(j(E))$, which encompasses condition (i) that defines the set T).

(1) If $\text{Frob}_\mathfrak{p} = 1$ in $K(j(E), h(E[\mathfrak{m}]))$ then $\text{Frob}_\mathfrak{p}|_H = 1$, hence $\mathfrak{p} = \alpha_\mathfrak{p}\mathcal{O}_K$ for some $\alpha_\mathfrak{p} \in \mathcal{O}_K$ (again, from corollary 6). For $E(\mathbb{C}) = \mathbb{C}/\mathfrak{a}$ for $\mathfrak{a} \in \text{Cl}(K)$, we can consider map $\alpha : [\mathfrak{p}] \cdot E = E^{\text{Frob}_\mathfrak{p}} \to E$ that comes from $\mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} \xrightarrow{z \mapsto \alpha_\mathfrak{p} z} \mathbb{C}/\mathfrak{a}$. Then $\alpha \circ [\mathfrak{p}] : E \to E$ is simply $[\alpha_\mathfrak{p}]$ according to normalized identification. Note that as $E^{\text{Frob}_\mathfrak{p}} = E$ so $\alpha \in \text{Aut}(E)$ (its inverse is given by multiplication-by-$\alpha_\mathfrak{p}^{-1}$).

On the other hand, from the previous paragraph, we know $\epsilon^{-1} \circ [\mathfrak{p}] = \text{Frob}_\mathfrak{p} = 1$ on $E[\mathfrak{m}]$ for some $\epsilon \in \text{Aut}(E^{\text{Frob}_\mathfrak{p}}) = \text{Aut}(E)$, so for $P \in E[\mathfrak{m}]$, as the Weber function does not distinguish automorphisms between elliptic curves, we find

$$h(P) = h(\text{Frob}_\mathfrak{p}(P)) = h([\mathfrak{p}] \cdot P) = h([\alpha_\mathfrak{p}] \cdot P).$$

This implies there exists $[\xi] \in \mathcal{O}_K^\times = \text{Aut}(E)$ so $P = [\xi\alpha_\mathfrak{p}] \cdot P$. As we may assume that P is the generator of the free rank one $\mathcal{O}_K/\mathfrak{m}$-module $E[\mathfrak{m}]$, we find that $[\xi\alpha_\mathfrak{p}] = 1$ on $E[\mathfrak{m}]$. Under normalized identification, if $E(\mathbb{C}) = \mathbb{C}/\mathfrak{a}$, then $E[\mathfrak{m}] = \mathfrak{m}^{-1}\mathfrak{a}/\mathfrak{a}$. The condition $[\xi\alpha_\mathfrak{p}] = 1$ on $E[\mathfrak{m}]$ then says $\xi\alpha_\mathfrak{p} \equiv 1 \pmod{\mathfrak{m}}$. Thus, as $\mathfrak{p} = (\xi\alpha_\mathfrak{p})$, we are done.

(2) If $\mathfrak{p} = (\alpha_\mathfrak{p})$ for some $\alpha_\mathfrak{p} \in \mathcal{O}_K$ so $\alpha_\mathfrak{p} \equiv 1 \pmod{\mathfrak{m}}$. As $\mathfrak{p}$ is principal so $\mathfrak{p}$ splits in $H = K(j(E))$, implying $\text{Frob}_\mathfrak{p}|_H = 1$, hence $E = E^{\text{Frob}_\mathfrak{p}}$ (as E is defined over H). With completely same argument, for $P \in E[\mathfrak{m}]$, we find $h(\text{Frob}_\mathfrak{p}(P)) = h([\alpha_\mathfrak{p}] \cdot P) = h(P)$ as $\alpha_\mathfrak{p} \equiv 1 \pmod{\mathfrak{m}}$. On the other hand, note that $\text{Frob}_\mathfrak{p}(h(P)) = h(\text{Frob}_\mathfrak{p}(P))$ (h is the Weber function for $E = E^{\text{Frob}_\mathfrak{p}}$). This implies $\text{Frob}_\mathfrak{p}$ fixes $j(E)$ and $h(P)$ for all $P \in E[\mathfrak{m}]$, i.e. $\text{Frob}_\mathfrak{p} = 1$ on $K(j(E), h(E[\mathfrak{m}])$, as desired.

6. More to learn

I just want to give a list of things I have not gotten the chance to read more of.

(1) Adelic formulation of complex multiplication. Its relation with modular curves, Heegner points: https://mathoverflow.net/q/96314/89665 https://math.stanford.edu/~conrad/vigregroup/vigre04/mainthm.pdf.

Consequences of complex multiplication in terms of L-functions.

Generalization of complex multiplication theory for abelian varieties: https://math.berkeley.edu/~dcorwin/files/jp12.pdf.

(2) Because the endomorphism ring of elliptic curves can only be $\mathbb{Z}$, imaginary quadratic field or quaternion algebra over $\mathbb{Q}$, one cannot hope to use elliptic curves to construct explicit class field theory for other number fields.

One could ask if there is an analogue object of elliptic curves that could allow us to construct explicit class field theory for other number fields? The failure to find such object lies at the uniformization theorem for elliptic curves (see Weinstein [Wein]): as $\dim_{\mathbb{R}} \mathbb{C} = 2$, meaning one cannot hope to find discrete $\mathbb{Z}$-submodule of $\mathbb{C}$ of rank ≥ 3, as a result, there is no analogue for the moduli space of elliptic curves for number field K of degree > 2.

However, the situation is very different in the function field case, as one does not meet the obstacle of infinite places. More details on this are discussed at [Wein], [Poo] and [UM]. The analogue of elliptic curves in function fields are Drinfeld modules.

Somehow Drinfeld modules and Shtukas are related: https://people.math.harvard.edu/~sli/notes/shtukas_intro.pdf.

(3) How similar is Lubin-Tate theory in explicit local class field theory compared to these global explicit class field theory?

References

[LiCFT] Chao Li. Class field theory lecture notes. https://www.math.columbia.edu/~chaoli/docs/ClassFieldTheory.html

[Sun] Andrew Sunderland. Elliptic curves MIT course. https://math.mit.edu/classes/18.783/2022/lectures.html

[Mil] Milne. Elliptic curves.

[Sil] Silverman. Advanced topics in the theory of elliptic curves.

[Sil1] Silverman. The Arithmetic of Elliptic Curves.

[Cox] Cox. Primes of the form $x^2 + ny^2$.

[Jar] Weinstein. The Geometry of Lubin-Tate spaces lecture notes. http://math.bu.edu/people/jsweinst/FRGLecture.pdf.

[Poo] Poonen. An introduction to Drinfeld modules. https://math.mit.edu/~poonen/papers/drinfeld.pdf.

[LiCM] Chao Li. Minor thesis III: Complex multiplication and singular moduli. https://www.math.columbia.edu/~chaoli/docs/MinorThesis3.html

[UM] http://www-personal.umich.edu/~asnowden/seminar/2017/drinfeld/

[Wein] Jared Weinstein. Drinfeld modules notes. http://math.bu.edu/people/jsweinst/Teaching/MA841Fall17/DrinfeldModules.pdf