THE j-FUNCTION AND COMPLEX MULTIPLICATION

KISHAN JANI

Abstract. The j-function is an elliptic modular function of weight zero defined on the upper half-plane $\mathbb{H}$. The subsequent $\mathrm{SL}_2(\mathbb{Z})$ invariance, along with other special features, allow the function several compelling properties. Studying these will be a central theme of this paper. In particular, we will focus on the ability of the j-function to classify elliptic curves $E/\mathbb{C}$ upto isomorphism, which correspond to lattices modulo homothety.
That will serve as a starting point for our number theoretic exposition, developed via the beautiful theory of complex multiplication. As we will see, the j-function and complex multiplication enable a straightforward characterization of abelian extensions of imaginary quadratic fields, resolving part of a central problem in class field theory. Finally, we will look at some other consequences of complex multiplication, studying its applications to primality proving, characterization of primes of the form $x^2 + ny^2$, and the theory of binary quadratic forms. A background in complex analysis and algebraic number theory is recommended.

1. Modular Forms and Functions

1.1. **Introductory Theory.** Many of the analytic properties of the j-function emerge from the fact that it is defined to be a modular function of weight zero, which is a rare but particularly consequential property. Modular forms and functions have many uses in number theory and complex analysis; however, their definition is rather specific and may seem odd to a first-time beholder. Consequently, we begin by motivating some key ideas that compel number theorists to study modular forms and functions.
The *uniformization theorem of complex analysis* states that every simply connected Riemann surface is conformally equivalent to one of the following:

(1) The unit disk $\mathbb{D}$
(2) The complex plane $\mathbb{C}$
(3) The Riemann sphere $\widehat{\mathbb{C}}$

Modular forms emerge from the very natural study of Riemann surfaces with universal cover $\mathbb{H}$ generated by the action $\Gamma \setminus \mathbb{H}$ for a discrete group Γ. Note that this is the same as talking about universal cover $\mathbb{D}$ due to the conformal map $f(z) = \frac{i-z}{i+z}$.
The *projective special linear group* $\mathrm{PSL}_2(\mathbb{R}) \cong \mathrm{SL}_2(\mathbb{R})/\{\pm I\}$ is rather important. $\mathrm{PSL}_2(\mathbb{R})$ has a well-defined action on $\mathbb{H}$ via fractional linear transformations and is isomorphic to the automorphisms of $\mathbb{H}$. That is, $\mathrm{SL}_2(\mathbb{R})/\{\pm I\} \cong \mathrm{Aut}(\mathbb{H})$. This motivates the study of discrete subgroups Γ of $\mathrm{SL}_2(\mathbb{R})/\{\pm I\}$. The ones of number theoretic interest are

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\} \text{ for } N \geq 0,$$

each called a principle congruence subgroup of level N. It is natural to study meromorphic functions on any Riemann surface. Modular forms and functions are simply their richer variant on surfaces $X(N) = \Gamma(N) \setminus \mathbb{H}^*$ due to their invariance-based transformation property. We require the extended upper half plane $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ as a means of compactification. Our study of modular forms will mostly be restricted to those of level 1.

Definition 1.1.1. Naturally, $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ is the most fundamental of these subgroups, and is called the *modular group*

$$\Gamma(1) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc = 1 \text{ for } a, b, c, d \in \mathbb{Z} \right\} \Big/ \{\pm I\},$$

which acts on the upper half plane $\mathbb{H}$ via fractional linear transformations $z \to \frac{az+b}{cz+d}$.

Definition 1.1.2. For $k \in \mathbb{Z}$, a function $f : \mathbb{H} \to \mathbb{C}$ is a *modular form* of weight k (and level 1) if it satisfies the following:

(1) f is holomorphic on $\mathbb{H}$, and is holomorphic as $z \to i\infty$.

(2) For all $\tau \in \mathbb{H}$ and any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$, we have that

$$f(\gamma\tau) = f\Big(\frac{a\tau + b}{c\tau + d}\Big) = (c\tau + d)^k f(\tau)$$

Remark. Since the modular group is generated by the matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, instead of condition (2), it is sufficient to say that $f(\frac{-1}{\tau}) = \tau^k f(\tau)$ and $f(\tau + 1) = f(\tau)$ for all $\tau \in \mathbb{H}$. The latter implies $f(z)$ has period 1, and thus a convergent Fourier series of the form $\sum_{n=0}^{\infty} a_n q^n$, where $q = e^{2\pi i \tau}$.

Modular functions are characterized by relaxed conditions for holomorphicity so that we can actually have non-trivial functions with the modular property.

Definition 1.1.3. A meromorphic function $f : \mathbb{H} \to \mathbb{C}$ is a *modular function* of weight k if and only if the following conditions are satisfied:

(1) $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ for $\tau \in \mathbb{H}$ and $\gamma \in \Gamma(1)$

(2) The function f has a Fourier series of the form

$$f(\tau) = \sum_{n=-n_0}^{\infty} a_n q^n \text{ for } q = e^{2\pi i \tau} \text{ and } n_0 > 0.$$

Example 1.1. The kth *Eisenstein Series* $G_k(\tau)$ for $k \geq 2$ over a lattice Λ is defined as

$$G_k(\tau) = \sum_{\omega \in \Lambda \setminus 0} \frac{1}{\omega^k} = \sum_{(m,n) \in \mathbb{Z}^2 \setminus (0,0)} \frac{1}{(m + n\tau)^k},$$

where the lattice $\Lambda = [\omega_1, \omega_2]$ has been adjusted to be $[1, \tau]$ to convert it into a function in τ, where $\tau = \omega_2/\omega_1$.

Each Eisenstein series G_k is a modular form of that weight for even k, while for odd k we have $G_k = 0$. In a certain sense, it is the simplest modular form of a given weight. This becomes much more apparent when we consider some analytic properties of modular forms.

1.2. **Properties.** Various properties of modular forms and functions make them incredibly fascinating in their own right. Firstly, the modular forms of weight k form a vector space $\mathbb{M}_k$. This space has several properties

(1) The dimension of $\mathbb{M}_k$ satisfies the relation

$$\dim \mathbb{M}_k = \begin{cases} 0 & \text{for odd } k \\ \lfloor \frac{k}{12} \rfloor + 1 & \text{for } k \not\equiv 2 \pmod{12} \\ \lfloor \frac{k}{12} \rfloor & \text{for } k \equiv 2 \pmod{12} \end{cases}$$

(2) The set $\{G_4^a G_6^b : a, b \geq 0, 4a + 6b = k\}$ is a basis for $\mathbb{M}_k$. That is, the Eisenstein series G_4 and G_6 generate all modular forms.

A proof for these properties, along with many other interesting ones, can be found in any reasonable book on modular forms. Here, we provide reference to Chapters 1 and 3 of [DS05].
The j-function is the weight zero modular function with respect to $\Gamma(1)$, referred to as a *hauptmodul*, a property that makes it a crucial map in the theory of modular forms. In fact, the related hauptmodul $\lambda(\tau)$ for $\Gamma(2)$ is famously used in a proof of Picard's Little theorem as the holomorphic covering map $\mathbb{H} \to \mathbb{C}\backslash\{0,1\}$. See Chapters 7 and 8 of [Ahl66]. In this case, $j : X(1) \to \widehat{\mathbb{C}}$ gives an isomorphism between Riemann surfaces, and every modular function of weight zero is a rational function of $j(\tau)$.
There is a lot more to be said about modular curves emergent from $\Gamma(N)$ and their function fields. For genus zero modular curves, their respective hauptmoduls generate the entire function field of $X(N)$. However, it can be shown using the Riemann-Hurwitz formula that there are only finitely many curves $X(N)$ with genus zero. In particular $g = 0$ only for $1 \leq N \leq 5$, as demonstrated in Chapter 5 of [RS11].

2. The Elliptic Curve Correspondence

For the purpose of this paper, we concern ourselves with one profound application of modular forms to number theory, specifically, to the theory of elliptic curves. In essence, we can view modular forms and functions as functions on isomorphism classes of elliptic curves. Consequently, it so happens that by studying these, one can often infer properties of elliptic curves. See Chapter 1 of [Sil94] for great detail on the subject.

2.1. **Differential Equation.**

The main link between modular forms and elliptic curves comes from a curious differential equation satisfied by $\wp(z)$, with coefficients in terms of the aforementioned Eisenstein series.

Definition 2.1.1. The Weierstrass $\wp$ function $\wp(z;\Lambda)$ is defined as the meromorphic function

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda\backslash\{0\}} \left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \right) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2k+1) G_{2k+2} z^{2k}.$$

With the Laurent series expansion, the following differential equation that takes the form of an elliptic curve is readily obtained.

Theorem 1. *For a lattice Λ, $\wp(z)$ satisfies*

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

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

This differential equation suggests a direct correspondence between lattices Λ, which can be interpreted as complex tori, and elliptic curves E over $\mathbb{C}$. Before we present this, we first develop the elliptic curve side of things, which is important not only for setting up the j-function, but also for exploring Complex Multiplication later.

2.2. **Elliptic Curves.**

Definition 2.2.1. The natural setting for Elliptic Curves is the Complex Projective Space $\mathbb{CP}^2 = \{(z_1, z_2, z_3) : z_1, z_2, z_3 \in \mathbb{C}\}/\sim$, where the equivalence relation λ is such that $(z_1, z_2, z_3) \sim (w_1, w_2, w_3)$ if $(w_1, w_2, w_3) = \lambda(z_1, z_2, z_3)$ for $\lambda \in \mathbb{C}_{\neq 0}$.

Definition 2.2.2. An elliptic curve E/k is a smooth, projective, non-singular curve defined over a field k with $\mathrm{char}(k) \neq 2, 3$ by

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where $\Delta = 4a^3 + 27b^2$ is the discriminant that is required to be non-zero. The condition $\Delta \neq 0$ is necessary for ensuring the uniqueness of the j-invariant and for avoiding singularity through repeated roots.

Elliptic curves are primarily studied over the following fields:

(1) Over $\mathbb{C}$: As part of the uniformization theorem, elliptic curves $E/\mathbb{C}$ are equivalent to lattices in $\mathbb{C}$, and equivalently tori. This relationship is made explicit by the $\wp$ function.

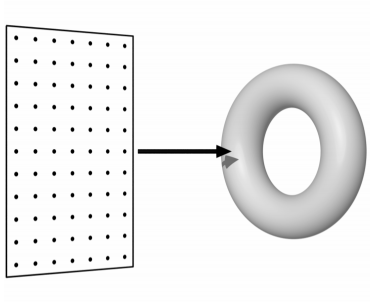

FIGURE 1. $E/\mathbb{C}$ as a torus (Figure 6 from [dSG16])

(2) Over $\mathbb{Q}$: There is much to be said about the theory of elliptic curves over $\mathbb{Q}$. One of the primary applications is in finding integral solutions to Diophantine equations. The group structure of $E/\mathbb{Q}$ has been of interest for a long time. The Mordell-Weil theorem provides an extremely useful characterization of $E/\mathbb{Q}$:

Theorem 2 (Mordell-Weil)**.** *The group of rational points on an elliptic curve is finitely generated.*

By the classification of finitely generated abelian groups, this equivalently is

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r.$$

$E(\mathbb{Q})_{\text{tors}}$ is well understood by virtue of Mazur's torsion theorem. The mysterious part is the $\mathbb{Z}^r$, where r is called the rank of an elliptic curve. The Birch and Swinnerton-Dyer conjecture provides a very simple interpretation of this rank. See [Mil20] for more on the subject.

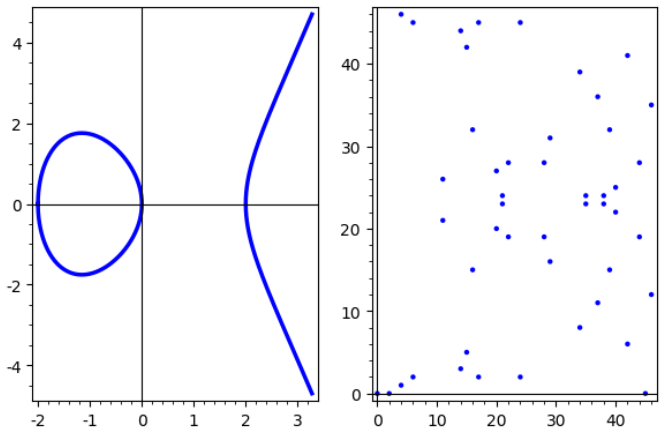

FIGURE 2. The elliptic curve $E : y^2 = x^3 - 4x$ over $\mathbb{Q}$ (left) and $\mathbb{F}_{47}$ (right)

(3) Over $\mathbb{F}_p$: Elliptic curves over finite fields have tremendous applications in cryptography and primality proving. We will explore the latter in detail, especially in the context of elliptic curves with complex multiplication.

Elliptic curves are particularly important because they form an abelian variety, that is we have an abelian group defined on the points of an elliptic curve.
For two points P, Q on E, we define the group operation addition as follows: there is a unique line through P and Q that passes through a third point R on the elliptic curve. The vertical line through the infinity point O and R intersects the elliptic curve at R' which is the result of $P+Q$. The identity of this operation is the point at infinity $O = (0:1:0)$.
Adding a point P to itself is defined as follows: the tangent at point P intersects E at another point R. The vertical line through O and R passes through a third point, which is $P+P$. In general, $\underbrace{P+P+\cdots+P}_{n \text{ times}} := [n]P$.

Theorem 3 (Elliptic Curve Group Law)**.** *The points on an elliptic curve form an Abelian Group under the aforementioned operation with the following:*

(1) The point $O = (0:1:0)$, which is the point at infinity, acts as the identity.
(2) The inverse of a point $P = (x:y:z)$ is the point $-P = (x:-y:z)$.
(3) Commutativity is $P+Q = Q+P$ and associativity is given by $P+(Q+R) = (P+Q)+R$.

Proof. A proof of this theorem can be found in any reasonable book on elliptic curves, take for example [Sil09].

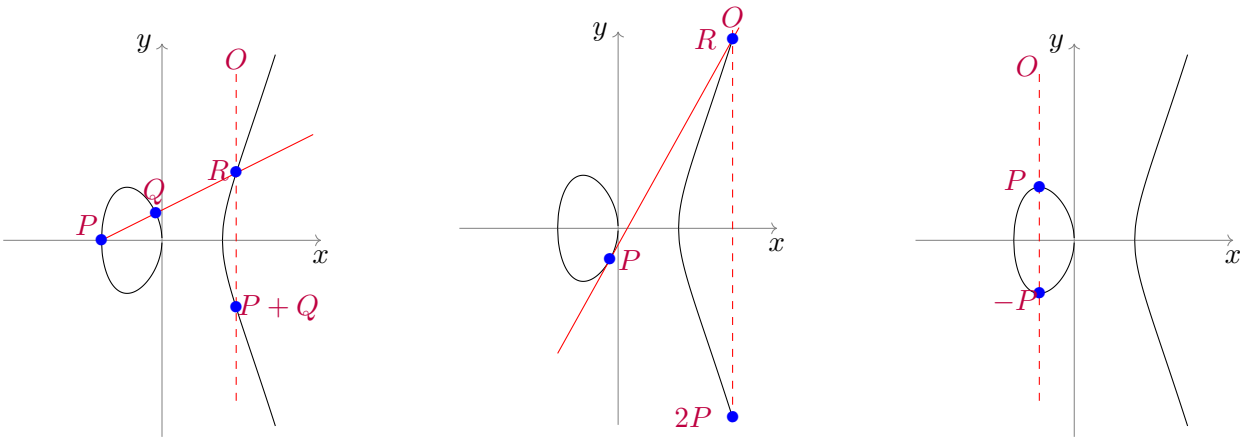

FIGURE 3. The elliptic curve group law (associativity not shown).

□

To see why the existence of an abelian group is significant, consider elliptic curves in analogy to the unit circle. Points on the unit circle $\mathbb{T}$ have a very natural group law with a simple parametrization $(\cos\theta, \sin\theta)$. Addition is defined as $(\cos\theta_1, \sin\theta_1) + (\cos\theta_2, \sin\theta_2) = (\cos(\theta_1+\theta_2), \sin(\theta_1+\theta_2))$, or $(a,b)+(c,d) = (ac-bd, ad+bc)$.
We are familiar with the many exciting properties and symmetries the unit circle has. With their group law, elliptic curves mirror many of these properties, which is what makes them particularly interesting to study. Similar to the unit circle, we can make several geometric and algebraic constructions on an elliptic curve that describe different features.

Definition 2.2.3 (Torsion Subgroup)**.** The torsion subroup E_{tors} of an elliptic curve is the set of all points with finite order. That is,

$$E_{\text{tors}} = \{P \in E : [n]P = O \text{ for } n \in \mathbb{N}\}.$$

Additionally, let $E[N] = \{P \in E : [N]P = O\}$ denote the N-torsion points of E for fixed N.

Continuing our analogy to the unit circle, the torsion points take the role of the roots of unity. This connection will become much more apparent when we encounter the construction of ray class fields via complex multiplication.
The torsion subgroup has a surprising connection back to the theory of modular forms. Consider the family of modular curves $X_1(N) = \Gamma_1(N) \setminus \mathbb{H}^*$, where $\Gamma_1(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \bmod N\}$. The genus zero modular curves are once again finitely many: $g = 0$ for $1 \leq N \leq 10$ and $N = 12$. However, quite remarkably these genus zero curves correspond to the possibilities of torsion subgroups for elliptic curves over $\mathbb{Q}$. This is the content of the statement and proof of Mazur's torsion theorem:

Theorem 4 (Mazur, [Maz77])**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following:*

(1) $\mathbb{Z}/N\mathbb{Z}$, where $1 \leq N \leq 10$ or $N = 12$,
(2) $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2N\mathbb{Z})$ for $N = 1, 2, 3, 4$.

Furthermore, all fifteen groups are the torsion subgroups to infinitely many elliptic curves $E/\mathbb{Q}$.

As mentioned before, this resolves part of our understanding of $E(\mathbb{Q})$, and what remains is the considerably more difficult $\mathbb{Z}^r$ portion.
The next useful tool to study elliptic curves is the j-invariant. Historically, the j-invariant was defined as a way to parametrize elliptic curves. Here, we have defined and observed the properties of the modular variant $j(\tau)$ first, but it will be immediate how this is an invariant of $E/\mathbb{C}$.

Definition 2.2.4 (The j-invariant)**.** Finally, we define the star of this expository paper. The j-invariant of a lattice Λ is given by

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

Proposition 5. *Two lattices Λ_1 and Λ_2 are homothetic iff $j(\Lambda_1) = j(\Lambda_2)$.*

Proof. Suppose we have homothetic lattices $\Lambda_1 = \alpha\Lambda_2$. Then for the weight 4 Eisenstein series coefficient, we have

$$g_2(\Lambda_1) = 60 \sum_{\omega \in \alpha\Lambda_2 0} \frac{1}{\omega^k} = 60 \sum_{\omega \in \Lambda_2} \frac{1}{(\alpha\omega)^k} = \frac{1}{\alpha^4} g_2(\Lambda_2).$$

Similarly, we also have $g_3(\Lambda_1) = \frac{1}{\alpha^6} g_3(\Lambda_2)$. Then for the j-invariant,

$$j(\Lambda_1) = 1728 \cdot \frac{\frac{1}{\alpha^{12}} g_2(\Lambda_2)^3}{\frac{1}{\alpha^{12}}(g_2(\Lambda_2)^3 - 27g_3(\Lambda_2)^2)} = j(\Lambda_2).$$

For the other direction, suppose we have $j(\Lambda_1) = j(\Lambda_2)$.

$$\frac{g_2(\Lambda_1)^3}{(g_2(\Lambda_1)^3 - 27g_3(\Lambda_1)^2)} = \frac{g_2(\Lambda_2)^3}{(g_2(\Lambda_2)^3 - 27g_3(\Lambda_2)^2)}$$

Upon cross multiplying, we get

$$g_2(\Lambda_1)^3 g_3(\Lambda_2)^2 = g_2(\Lambda_2)^3 g_3(\Lambda_1)^2$$

Let $\mu \in \mathbb{C}^\times$ be such that $g_2(\Lambda_2) = \mu^4 g_2(\Lambda_1)$. Then $g_3(\Lambda_2) = \mu^6 g_3(\Lambda_1)$. By the scaling property of $g_2(\Lambda)$ and $g_3(\Lambda)$ seen in the forward direction, we then have that $g_2(\Lambda_2) = g_2(\mu\Lambda_1)$ and $g_3(\Lambda_2) = g_3(\mu\Lambda_1)$. In terms of the original Eisenstein series, this is equivalent to saying $G_4(\Lambda_2) = G_4(\mu\Lambda_1)$ and $G_6(\Lambda_2) = G_6(\mu\Lambda_1)$. To show that this indeed implies homothety of lattices, recall the Laurent series of the $\wp$ function

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

The coefficients of this series are exclusively dependent on the Eisenstein series $G_k(\tau)$. Since all modular forms can be generated by $G_4(\tau)$ and $G_6(\tau)$, it follows that these two series uniquely determine $\wp(z)$. Then since we have $G_4(\Lambda_2) = G_4(\mu\Lambda_1)$ and $G_6(\Lambda_2) = G_6(\mu\Lambda_1)$, it follows that $\wp(z;\Lambda_2) = \wp(z;\mu\Lambda_1)$ as well. However, since the poles of the $\wp$-function are exactly on the lattice, $\wp(z, L)$ uniquely determines a lattice L. Then $\Lambda_2 = \mu\Lambda_1$ as desired. □

By the homothety property, we can construct the j-function as a natural extension of the j-invariant beyond lattices.

Definition 2.2.5. The j-function is a modular function of weight 0 defined as follows: let $j(\tau) = j([1,\tau])$, where $\tau = \frac{\omega_1}{\omega_2}$ for some lattice $\Lambda = [\omega_1, \omega_2]$. In particular, we have for $f : \mathbb{H} \to \mathbb{C}$ that

$$j(\tau) = 1728 \cdot \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2},$$

which is still equal to $j([\omega_1, \omega_2])$. 1728 is the smallest number chosen so that the q expansion of the j-invariant has integer coefficients, a very important property.

2.3. **Uniformization Theorem.** The j-function will be used in our proof of the uniformization theorem for elliptic curves, mainly because it induces an isomorphism between Riemann surfaces

$$j : X(1) \to \mathbb{P}^1(\mathbb{C}),$$

which affirms the existence of a unique $j(\tau)$ for all elliptic curves over $\mathbb{C}$. We omit a proof of this result, which can be found in Chapter 1 of [Sil94], since it requires a formal description of modular functions in terms of k-differential forms. Instead, we use a weaker but sufficient lemma defined over a fundamental domain for $j(\tau)$.

Proposition 6. *The set $\mathcal{F}$, defined as*

$$\mathcal{F} = \{\tau \in \mathbb{H} : |\Re\tau| \leq 1/2 \text{ and } |\tau| \geq 1\},$$

is a fundamental domain for $\mathbb{H}/SL_2(\mathbb{Z})$.

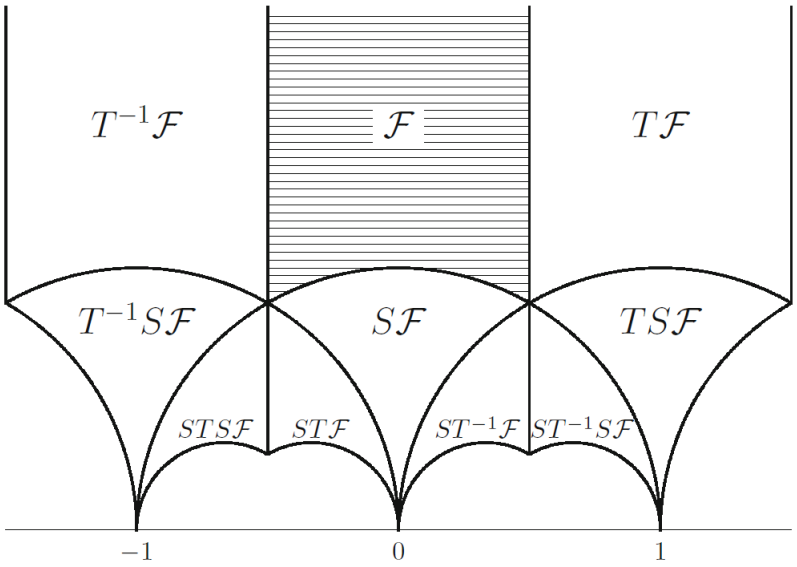

FIGURE 4. The fundamental domain $\mathcal{F}$ and some of its $\mathrm{PSL}_2(\mathbb{Z})$ translates (Figure 3.1 in [Sil09]).

Proof. This amounts to proving two different things:
(1) **Existence:** For every $\tau \in \mathbb{H}$, there exists $\tau' \in \mathcal{F}$ such that $\tau' = \gamma\tau$ for some $\gamma \in \Gamma(1)$.
Set $\tau \in \mathbb{H}$. First note that for action by $\gamma \in \Gamma(1)$, we have

$$\mathfrak{I}(\gamma\tau) = \frac{\mathfrak{I}[(a\tau+b)(c\overline{\tau}+d)]}{|c\tau+d|^2} = \frac{\mathfrak{I}\tau}{|c\tau+d|^2}.$$

Let $c\tau+d$ be the shortest vector in the lattice $\Lambda = [1,\tau]$ so that $|c\tau+d|$ is maximized. It is also true that c, d are then relatively prime, so there exist $a, b \in \mathbb{Z}$ such that $a_0 d - b_0 c = 1$. Subsequently, the matrix $\gamma_0 = \left(\begin{smallmatrix} a_0 & b_0 \\ c & d \end{smallmatrix}\right)$ maximizes $\mathfrak{I}(\gamma\tau)$ over $\Gamma(1)$. Now, we adjust the image of the transformation of τ under γ_0. To do this, use the clever transform $\gamma = T^k\gamma_0$, where $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Notice that $\mathfrak{I}(\gamma\tau)$ is still maximal because $T^k = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ just affects the real part. Thus, set $\gamma = T^k\gamma_0$, where we choose k so that $|\mathfrak{R}(\gamma\tau)| \leq 1/2$. Observe that we also must have $|\gamma\tau| \geq 1$, since otherwise it might be that $\mathfrak{I}(S\gamma\tau) > \mathfrak{I}(\gamma\tau)$ by comparison of real and imaginary parts of $\gamma\tau$, contradicting the maximality of $\mathfrak{I}(\gamma\tau)$. The final case is that $\gamma\tau \notin \mathcal{F}$ because $|\gamma\tau| = 1$ and $\mathfrak{R}\tau > 0$. Here, we simply make the adjustment $\tau' = S\gamma\tau$ to get τ' in $\mathcal{F}$.
(2) **Uniqueness:** Points in $\mathcal{F}$ are unique; consequently, if $\tau' = \gamma\tau$ for $\tau, \tau' \in \mathcal{F}$ and $\gamma \in \Gamma(1)$, then it must be that $\gamma = \pm I$.
Set $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$. If $c \neq 0$ and $\tau \in \mathcal{F}$, we have $|c\tau+d|^2 > 1$. This is easy to see: first observe that

$$|c\tau+d|^2 = c^2|\tau|^2 + 2cd\,\mathfrak{R}\tau + d^2 > c^2 - |cd| + d^2 \text{ since } \tau \in \mathcal{F}.$$

If $d = 0$, then $|c\tau+d|^2 > c^2 > 1$. If $d \neq 0$, then

$$c^2 - |cd| + d^2 \geq (|c| - |d|)^2 + |cd| \geq |cd| \geq 1,$$

giving once again that $|c\tau+d|^2 > 1$. Consequently, $\mathfrak{I}(\gamma\tau) < \mathfrak{I}(\tau)$ for any $\gamma \in \Gamma(1)$.
Now suppose we have $\tau', \tau \in \mathcal{F}$ and $\gamma \in \Gamma(1)$ such that $\tau' = \gamma\tau$. Then by the above result, $\mathfrak{I}\tau' < \mathfrak{I}\tau$. But then we also have $\tau = \gamma^{-1}\tau'$, so $\mathfrak{I}\tau > \mathfrak{I}\tau'$. Since both cannot be true together, we must have $c = 0$. Then $\det\gamma = ad = 1$, so $a, d = \pm 1$. This leaves

$$\gamma = \begin{pmatrix} \pm 1 & b \\ 0 & \pm 1 \end{pmatrix}, \text{ so } \tau' = \tau \pm b.$$

But since both points are in the fundamental domain, $|\mathfrak{R}\tau' - \mathfrak{R}\tau| < 1$, so $|b| < 1$ or $b = 0$. Thus $\gamma = \pm I$ □
Finally, we can state and prove the weaker j-function correspondence.

Theorem 7. *The restriction of $j(\tau)$ to $\mathcal{F}$ creates a one-to-one correspondence between $\mathcal{F}$ and $\mathbb{C}$.*

Proof. Injectivity of $j : \mathcal{F} \to \mathbb{C}$ follows directly from Propositions 5 and 6. We will prove surjectivity by first showing that the $j(\mathbb{H}) \subseteq \mathbb{C}$ is both closed and open, and since $\mathbb{C}$ is connected, it must be that $j(\mathbb{H}) = \mathbb{C}$. The surjectivity of $j : \mathbb{H} \to \mathbb{C}$ will then be naturally extended to that of $j : \mathcal{F} \to \mathbb{C}$.
$j(\mathbb{H})$ is open: We examine $j(\tau)$ in the limit $\mathfrak{I}\tau \to \infty$. Note that we have

$$\lim_{\mathfrak{I}\tau\to\infty} g_2(\tau) = \lim_{\mathfrak{I}\tau\to\infty} 60G_4(\tau) = \lim_{\mathfrak{I}\tau\to\infty} 60\left(\sum_{m=1}^{\infty}\frac{1}{m^4} + \sum_{n\neq 0}\frac{1}{(m+n\tau)^4}\right) = 60\sum_{m=1}^{\infty}\frac{1}{m^4} = \frac{4\pi^4}{3}.$$

Similarly, $g_3(\tau) = 140\zeta(6) = \frac{8\pi^6}{27}$. Then

$$\lim_{\mathfrak{I}\tau\to\infty} \Delta(\tau) = \left(\frac{4}{3}\pi^4\right)^3 - 27\left(\frac{8}{27}\pi^6\right)^2 = 0$$

Thus, $j(\tau)$ is unbounded as $\mathfrak{I}\tau \to \infty$ and subsequently non-constant. As a non-constant and holomorphic function on $\mathbb{H}$, by the open-mapping theorem, the image $j(\mathbb{H})$ must be open as well.
$j(\mathbb{H})$ is closed: Consider a convergent sequence $j(\tau_1), j(\tau_2), \ldots$ in $j(\mathbb{H})$ converging to $w \in \mathbb{C}$. By $\mathrm{SL}_2(\mathbb{Z})$ invariance of $j(\tau)$, we can assume WLOG that $\tau_1, \tau_2, \ldots$ is in $\mathcal{F}$. Since $j(\tau) \to \infty$ as

$\Im\tau \to \infty$, the imaginary parts $\Im\tau_1, \Im\tau_2, \dots$ must be bounded (say by M) for convergence of the above sequence. Thus all τ_n lie in the compact set

$$\mathcal{F}_M = \{\tau \in \mathbb{H} : |\Re\tau| \leq 1/2, \Im\tau \in [1/2, M]\}$$

Consequently, a subsequence $\{\tau_{n_k}\}$ converges to some $\tau \in \mathcal{F}_M$. Since $j(\tau)$ is continuous, it must be that $j(\tau) = \omega$. Thus all limit points ω are contained in $j(\mathbb{H})$, making the set closed.
Thus $j(\mathbb{H})$ is clopen and equal to $\mathbb{C}$. Now, recall that all points $\tau \in \mathbb{H}$ are $\mathrm{SL}_2(\mathbb{Z})$ equivalent to some point $\tau' \in \mathcal{F}$. However, $j(\tau)$ is $\mathrm{SL}_2(\mathbb{Z})$ invariant, so then it must be that $j(\mathcal{F}) = \mathbb{C}$ as well. □
Equipped with a background in Elliptic curves and the j-function, we can now solidify the correspondence between lattices modulo homothety and isomorphism classes of elliptic curves, which we denote by $\mathcal{ELL}_{\mathbb{C}}$, with the following two theorems. Here, we define E_Λ to be the elliptic curve associated with the lattice Λ, taking its coefficients as $g_2(\Lambda)$ and $g_3(\Lambda)$ in accordance to the Weierstrass differential equation.

Theorem 8 (Uniformization theorem for elliptic curves)**.** *For an elliptic curve $E/\mathbb{C}$, there exists a lattice $\Lambda \subset \mathbb{C}$, unique up to homothety, such that $E \cong E_\Lambda$.*

Proof. An equivalent statement is that for any two $A, B \in \mathbb{C}$ such that $A^3 - 27B^2 \neq 0$ for the elliptic curve $E : y^2 = 4x^3 - Ax - B$, we can find a lattice Λ such that $g_2(\Lambda) = A$ and $g_3(\Lambda) = B$. This will be the result that we prove.
Theorem 7 is crucial here, since it allows us to take $\tau \in \mathbb{H}$ such that

$$j(\tau) = 1728 \cdot \frac{A^3}{A^3 - 27B^2}, \text{ and so } 1 - \frac{1}{j(\tau)} = \frac{27B^2}{A^3} \tag{1}$$

since $j(\tau) \neq 0$. Define the base lattice Λ to be $\alpha[1, \tau]$, where

$$\alpha^2 = \frac{A}{B} \cdot \frac{g_3(\tau)}{g_2(\tau)}.$$

Then we have

$$\frac{g_2(\alpha[1,\tau])}{g_3(\alpha[1,\tau])} = \frac{\alpha^{-4} g_2(\tau)}{\alpha^{-6} g_3(\tau)} = \alpha^2 \frac{g_2(\tau)}{g_3(\tau)} = \frac{A}{B} \tag{2}$$

This makes the constant α particularly crucial, since by the regular definition of the j-invariant we now have

$$1 - \frac{1}{j(\tau)} = 1 - \frac{1}{j(\alpha[1,\tau])} = \frac{27 g_3(\alpha[1,\tau])^3}{g_2(\alpha[1,\tau])^2} = \frac{27B^2}{A^2 g_2(\alpha[1,\tau])}$$

by (2), where we initially used the fact that homothetic lattices have equal j-invariants as seen with Proposition 5. Equating this to (1), we get that

$$g_2(\alpha[1,\tau]) = A, \text{ and by (2), } g_3(\alpha[1,\tau]) = B$$

as desired. If either A or B is equal to zero, we can analogously take

$$\alpha^6 := \frac{g_3(\tau)}{B} \text{ and } \alpha^4 := \frac{g_2(\tau)}{A}$$

respectively. Uniqueness follows from the fact that if we have $g_2(\Lambda_1) = g_2(\Lambda_2)$ and $g_3(\Lambda_1) = g_3(\Lambda_2)$, it must be that $\Lambda_1 = \Lambda_2$. This was shown in the proof of Proposition 5 by using the Weierstrass $\wp$ function. □
While theorem 8 suffices for our purposes, in reality, we can say something much more powerful about the relationship between lattices and elliptic curves.

Theorem 9. *For an elliptic curve $E/\mathbb{C}$, as well as a map $\varphi : C/\Lambda \to E(\mathbb{C})$ defined by*

$$\varphi(z) = (\wp(z;\Lambda) : \wp'(z;\Lambda)) : 1),$$

which is both an isomorphism between Riemann surfaces, and a group homomorphism.

Proof. A detailed proof can be found in Chapter VI of [Sil09]. □

Observe that this result fits very naturally within the framework of the uniformization theorem. A corollary of uniformization is that every compact Riemann surfaces of genus 1 can be represented as a torus. An elliptic curve over $\mathbb{C}$ is exactly that, and so it can also be interpreted as a torus, or equivalently a lattice in $\mathbb{C}$.

Corollary 9.1. *Elliptic curves $E/\mathbb{C}$ are topologically equivalent to a torus.*

However, as we will see, it is also very useful to look at the specifics of the aforementioned correspondence.

Corollary 9.2. *The following addition and duplication formulas are satisfied by the $\wp$ function:*

$$\wp(w+z) + \wp(w) + \wp(z) = \frac{1}{4}\Big(\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)}\Big)^2, \quad \wp(2z) = \frac{1}{16}\Big(\frac{12\wp(z)^2 - g_2}{2\wp'(z)}\Big)^2 - 2\wp(z)$$

Proof. By the Group law of the Elliptic Curve $E : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$, it can readily be derived that for points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on E, the line L passing through both points necessarily intersects E at a third point $P_3 = (x_3, y_3)$. The reflection of this point is $P_1 + P_2$. Let $y = mx + b$ be the equation of L. Substituting this into the elliptic curve, we have $(mx+b)^2 = 4x^3 - g_2x - g_3$. The roots of this equation are x_1, x_2, x_3 by assumption, so by Vieta's formula it follows that $x_1 + x_2 + x_3 = \frac{m^2}{4}$.
Next, by the theorem above, we can set $(x_1, y_1) = (\wp(w), \wp'(w))$ and $(x_2, y_2) = (\wp(z), \wp'(z))$ so that P_3 as the reflection of $P_1 + P_2$ is $(\wp(z+w), -\wp'(z+w))$. It then follows that

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

For the duplication identity, set $x_1 = x_2$. We now have a tangent at P_1 intersecting the curve at P_3, whose slope m is found by $2ydy = 12x^2 - g_2,$ so $m = \frac{12x_1^2 - g_2}{2y_1}$ Repeating the process above gives $2x_1 + x_2 = \frac{m^2}{4}$, so we have

$$\wp(2z) = \frac{1}{16}\Big(\frac{12\wp(z)^2 - g_2}{2\wp'(z)}\Big)^2 - 2\wp(z).$$

□

Another way to derive these identities would be to simplify the Laurent series expansions; however, the intractability of that approach is apparent.
One of the other remarkable consequences of Theorems 8 and 9 is that we have a nice analytic representation of the points on $E(\mathbb{C})$. In terms of our unit circle analogy, just like $(\cos\theta, \sin\theta)$ for $\theta \in [0, 2\pi]$ represents the unit circle, $(\wp(z), \wp'(z))$ corresponds to points on the elliptic curve. Addition using this version of points is also easy, since $P_1 + P_2 \Longrightarrow (\wp(w+z), -\wp'(w+z))$ as seen above.

3. CM Part I: The Algebraic Number Theory Connection

There is a significant conceptual difference between the analytic theory of modular forms and the algebraic theory of class fields which complex multiplication (abbreviated CM) elegantly connects. Consequently, we first discuss the bigger picture by motivating the purpose of CM and proving some introductory results. This will direct us towards the algebraic number theory lurking beneath.

3.1. **Motivation.** As the connection between modular forms and elliptic curves, lattices certainly bear a great deal of importance. Interesting properties of elliptic and modular functions come from the lattice over which they are defined, and in the other direction, lattices (modulo homothety) correspond to isomorphism classes of elliptic curves via $j([1,\tau])$.
The analytic motivation behind CM is to add extra symmetry to a lattice in the form of scaling-based endomorphisms and look at the consequences. It seems natural that this will lead to interesting properties of elliptic functions and curves; we have seen a glimpse of this, where the group law readily proved two identities for $\wp(z)$. As a matter of fact, we will be able to show something even more remarkable:

Property 1. If $\alpha \in \mathbb{C}/\mathbb{Z}$ is a complex number that allows complex multiplication, then $\wp(\alpha z)$ is a rational function in $\wp(z)$

With this small glimpse into what CM holds, we finally provide a definition.

Definition 3.1.1. We say an elliptic curve $E/\mathbb{C}$ has *complex multiplication* it has an endomorphism ring $\mathrm{End}(E) \supsetneq \mathbb{Z}$ larger than the integers.

In the language of lattices, we can interpret the endomorphism ring of an elliptic curve E over $\mathbb{C}$ as $\mathrm{End}_{\mathbb{C}}(E) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$, which will be a helpful equivalent definition. In essence, we want the endomorphism ring to be

$$\mathrm{End}_{\mathbb{C}}(E) \cong \mathbb{Z} \cup \{\text{more symmetry}\}.$$

The quadratic imaginary constraint on our extra symmetry comes from the following theorem:

Theorem 10. *If $E/\mathbb{C}$ is an elliptic curve with CM with corresponding lattice $\Lambda = \mathbb{Z} + \mathbb{Z}\alpha$, then $\mathbb{Q}(\alpha)$ is an imaginary quadratic extension of $\mathbb{Q}$ and $End_{\mathbb{C}}(E) \cong \mathcal{O}$ for an order $\mathcal{O} \subset \mathbb{Q}(\alpha)$.*

Proof. The proof is straightforward from the lattice of interpretation of CM: we examine $\lambda \in \mathbb{C}^\times$ such that

$$\mathrm{End}_{\mathbb{C}}(E) = \{\lambda \in \mathbb{C}^\times : \lambda\Lambda \subset \Lambda\}, \text{ where } \Lambda = [1,\alpha],$$

is an endomorphism ring is larger than $\mathbb{Z}$. Subseqently, there must be $a,b,c,d \in \mathbb{Z}$ such that for $\lambda \in \Lambda$,

$$\lambda = a + b\alpha, \quad \alpha\lambda = c + d\alpha.$$

Eliminating α, we get $\lambda^2 - (a+d)\lambda + ad - bc = 0$, and so $\mathrm{End}_{\mathbb{C}}(E)$ is an integral extension of $\mathbb{Z}$. Then upon eliminating λ, we have $b\alpha^2 - (a-d)\alpha - c = 0$, and for $b \neq 0$, it must be that α is an imaginary quadratic. □

Definition 3.1.2. We say that an elliptic curve $E/\mathbb{C}$ has complex multiplication by $\mathcal{O}$ if Λ is homothetic to $\mathbb{Z}+\omega\mathbb{Z}$, where $\mathbb{Q}(\omega)$ is an imaginary quadratic field and $\mathcal{O} \subset \mathbb{Q}(\omega)$ an order. Usually the order is just taken to be $\mathcal{O}_K$.

The setup for CM will now allow us to come across some interesting results due to the Elliptic Curve correspondence.

Example 3.1. To see this, let us deal with the problem of finding an elliptic curve with CM by $\mathcal{O}_K$ for some quadratic imaginary field $K/\mathbb{Q}$. Let $\mathfrak{a}$ be a non-zero fractional ideal of K. As an ideal in a quadratic imaginary field, it is a rank 2 $\mathbb{Z}$-module. Then by the embedding $\mathfrak{a} \subset K \subset \mathbb{C}$, it must be that $\mathfrak{a}$ can be interpreted as a lattice in $\mathbb{C}$. Subsequently, we can form an elliptic curve $E_{\mathfrak{a}}$ with $\mathrm{End}_{\mathbb{C}}(E_{\mathfrak{a}}) \cong \{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subset \mathfrak{a}\}$. This in turn is the same as $\{\alpha \in K : \alpha\mathfrak{a} \subset \mathfrak{a}\}$, since $\mathfrak{a}$ itself is a subset of K. By definition, this gives the ring of integers since $\mathfrak{a}$ is fractional, and so $\mathrm{End}_{\mathbb{C}}(E_{\mathfrak{a}}) \cong \mathcal{O}_K$ as desired.

The fractional ideals of K thus generate elliptic curves with CM by O_K. However, since homothetic lattices give isomorphic elliptic curves, ideals $\mathfrak{a}$ and $c\mathfrak{a}$ give the same curve in the set of isomorphism class

$$\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K) = \{E/\mathbb{C} \text{ with } \mathrm{End}_{\mathbb{C}}(E) \cong \mathcal{O}_K\}/\cong$$

This suggests a direct correspondence between isomorphism classes of elliptic curves with CM by $\mathcal{O}_K$ and fractional ideals modulo principal ideals. The latter is exactly the definition of the class group.

4. A Class Field Theoretic interlude

The final result of the previous section establishes a connection to algebraic number theory: in a sense, the ideals of the number field K measure the number of elliptic curves that some particular CM can allow. It so happens that this connection goes much deeper into class groups and class fields, which we introduce here.

4.1. **Class Groups.**

In generalizing number theory from $\mathbb{Z}$ to arbitrary number fields, the first question one asks is which fundamental properties are preserved, and which ones are not. Unfortunately, unique factorization into prime numbers as part of the fundamental theorem of arithmetic, perhaps the most important property, is usually not true.

Example 4.1. Consider the number field $\mathbb{Q}(\sqrt{-5})$. Then

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

and factorization is not unique.

Class groups and fields can be seen as a way to analyze this. Recall that typically, we are able to fix unique factorization problems by dealing instead with prime ideals instead of elements.

Theorem 11. *The ring of integers has unique factorization over prime ideals. In particular,*

(1) Let $\mathfrak{a}$ be a non-zero proper ideal in a Dedekind domain R. Then $\mathfrak{a}$ can be unique factored into a finite product of non-zero prime ideals $\mathfrak{p}_i$ as

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_n^{e_n}$$

(2) $\mathcal{O}_K$ is a Dedekind domain.

Definition 4.1.1. Two ideals $\mathfrak{a}, \mathfrak{b}$ of an order $\mathcal{O}$ are equivalent if they carry lattice homothety so that $\mathfrak{a} = \alpha\mathfrak{b}$ for $\alpha \in \mathcal{O}$. The set of equivalence classes of ideals forms a multiplicative group called the class croup, denoted by $\mathrm{Cl}(\mathcal{O})$. The class group of $\mathcal{O}_K$ (or K) is called the *ideal class group*, and is alternatively and more prominently defined as the quotient I_K/P_k of fractional ideals over principal ideals.

Definition 4.1.2. The order of the ideal class group $|\mathrm{Cl}(K)|$ is called the class number $h(\mathcal{O}_K)$ of the field. Intuitively, the class number measures the extent to which unique factorization fails in the ring of integers of a number field.

(1) First note that the identity of $\mathrm{Cl}(\mathcal{O}_K)$ is the class of principal ideals. Then $h(\mathcal{O}_K) = 1$ means that the class group is trivial, so in essence all ideals are principal, and so unique factorization of elements follows from that of ideals (the ring $\mathcal{O}_K$ is a principal ideal domain).
(2) Roughly, the class number $h(K)$ is defined as the *ratio* of ideals of $\mathcal{O}_K$ to elements of $\mathcal{O}_K$. So in a sense for higher ratio of ideals, we require much more than simply the elements to have unique factorization in $\mathcal{O}_K$, and so we are considerably far from unique factorization for elements themselves.

A classic theorem related to this area is the finiteness of the class groups, which plays a significant role in determining algebraicity of $j(\tau)$.

Theorem 12 (Minkowski Bound)**.** *Let K be a number field with discriminant D and degree n over $\mathbb{Q}$. Then each ideal class of $Cl(K)$ contains an integral ideal $\mathfrak{o}$ such that*

$$\mathrm{Norm}(\mathfrak{o}) \leq \sqrt{|D|} \cdot \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n},$$

where $2t$ is the number of complex embeddings of K.

Then since there are only finitely many integral ideals of a given norm, there are finitely many classes, and so the result follows.

Corollary 12.1. *The class number is finite.*

The Minkowski bound may seem oddly geometrical for algebraic number theory, but this connection is precisely the point of the field called Geometry of Numbers that originated from Minkowski's work. For an introduction, see [Cas12].

4.2. **Class Field Theory and Abelian extensions.** There is a clear applicability of Galois theory in algebraic number theory, since the idea of a field extension is fundamental to studying number fields $K/\mathbb{Q}$ and their extensions that may permit some algebraic number α. However, a proper explicit resolution of this idea has proven to be difficult, which was one of the motivations behind class field theory.
Class field theory is a rich and deep part of number theory; consequently, we end up citing many famous theorems in our exposition. However, since this is not the main subject of our paper, we leave many out many of these proofs. Any reasonable text on class field theory will have these results, take for example [Cox11].

Question 4.1. Given a number field $K/\mathbb{Q}$, what do the abelian extensions of K look like?

The simplest case of $\mathbb{Q}$ was resolved by the work of Kronecker, Weber, and Hilbert in the second half of the 19th century.

Theorem 13 (Kronecker-Weber)**.** *Every finite abelian extension of $\mathbb{Q}$ is contained within some cyclotomic extension $\mathbb{Q}(\zeta_n)$.*

Originating from this result is the study of *maximum abelian extensions* of K. If the abelian extension is unramified, it is called the Hilbert class field H, which is at the center of class field theory. We are typically interested in $\mathrm{Gal}(H/K)$ and other abelian extensions of K.
To motivate this definition, we are first required to introduce essential concepts to understanding the Hilbert class field.
Much of algebraic number theory deals with prime ideals, so we often use primes in K to say non-zero prime ideals in $\mathcal{O}_K$ for simplicity. To develop a more complete picture of class field theory, we introduce the important notion of residue fields.

Definition 4.2.1. The quotient ring $\mathcal{O}_K/\mathfrak{p}$ is actually a finite field called the *residue field* of $\mathfrak{p}$.

Definition 4.2.2. A non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is said to be *ramified* in L/K if the prime ideal factorization

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_n^{e_n}$$

is such that $e_i > 1$ for some $\mathfrak{P}_i$, where $\mathfrak{P}_1, \ldots \mathfrak{P}_n$ are prime ideals in $\mathcal{O}_L$. If $e_i = 1$ for all $\mathfrak{P}_i$, then the prime is said to be *unramified*.

(1) If $n = 1$ for an unramified prime, then observe that the prime stays prime in $\mathcal{O}_L$ as well, and is appropriately labelled *inert*.
(2) If $n > 1$, then the unramified prime is said to be *split*.

Here, $e_i = e_{\mathfrak{P}_i|\mathfrak{p}}$ is called the *ramification index*. Additionally, the residue field $(\mathcal{O}_L/\mathfrak{P}_i)/(\mathcal{O}_K/\mathfrak{p})$ is a field extension, whose degree is $f_i = f_{\mathfrak{P}_i|\mathfrak{p}}$ is called the *intertial degree*.

There is a very natural relationship between e_i and f_i; as one might expect,

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

The utility of Galois theory becomes much more apparent when we consider the following theorem about the action of $\mathrm{Gal}(L/K)$ on primes.

Theorem 14. *Let L/K be a Galois extension, and let $\mathfrak{p}$ be a prime in K.*

(1) The action of $Gal(L/K)$ on primes of L containing $\mathfrak{p}$ is transitive. In other words, if $\mathfrak{P}_1$ and $\mathfrak{P}_2$ of L contain $\mathfrak{p}$, then there is a permutation $\sigma \in Gal(L/K)$ such that $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$.

(2) All primes $\mathfrak{P}_1, \ldots \mathfrak{P}_g$ containing $\mathfrak{p}$ have the same ramification index and degree, and so $efg = [L : K]$.

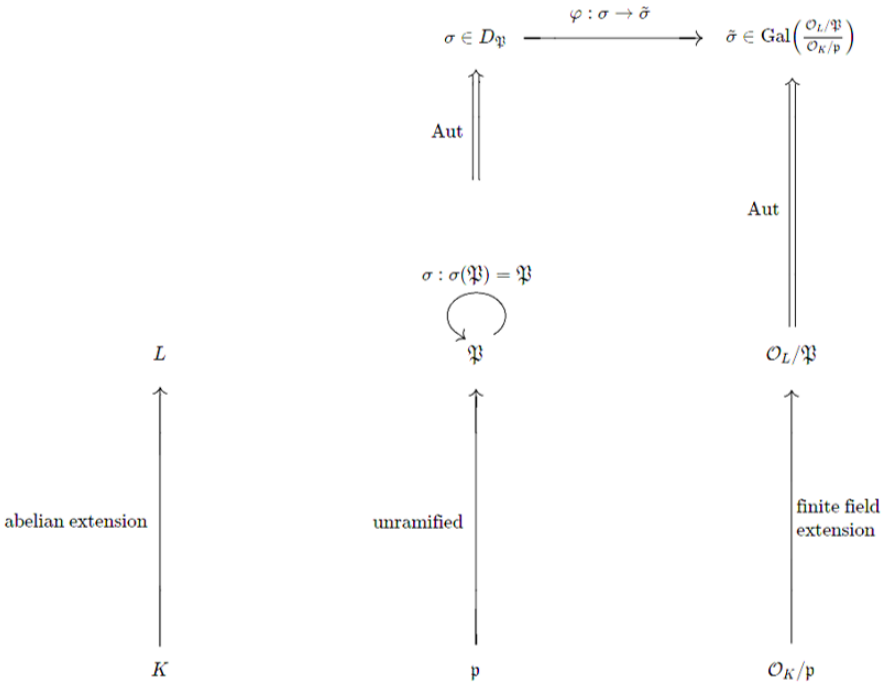

FIGURE 5. The general setting of class field theory leading up to the Artin symbol

An *unramified extension* is one that is unramified at all primes, both finite and infinite. We have encountered the finite case with prime ideals. Infinite primes are essentially the real and complex embeddings $K \to \mathbb{C}$, and we say an infinite prime ramifies if a real embedding $K \to \mathbb{C}$ extends to a complex one $L \to \mathbb{C}$. Finally, this brings us to the Hilbert class field.

Definition 4.2.3. The Hilbert Class Field H is the maximum unramified abelian extension of K.

The reason the Hilbert Class field is a particularly useful extension is that it carries many important properties that are particularly relevant in analyzing abelian extensions

Theorem 15 (Hilbert Class Field)**.** *Let H/K be the Hilbert Class Field as defined above. Then H exists and has the following interesting properties:*

(1) H is a finite Galois extension with $[H : K] = h_K$

(2) H/K is Galois with $Gal(H/K) \cong Cl(K)$.
(3) Every ideal in K becomes principal in H.
(4) Any unramified extension of K is a sub-field of H.

Not only does the above theorem resolve partly Question 3.1, it says that all information about unramified abelian extensions is contained within K itself because of the isomorphism $\mathrm{Gal}(H/K) \cong \mathrm{Cl}(K)$. We will go into more detail for this.
To introduce the truly remarkable aspects of CM, we go a little further into class field theory all the way to Artin reciprocity, one of the defining results of this field. There is a very interesting relationship between the automorphisms of primes $\mathfrak{P}$ and residue fields $\mathcal{O}_L/\mathfrak{P}$.

Definition 4.2.4. For a prime $\mathfrak{P}$ lying above $\mathfrak{p}$, we define the decomposition group to be

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

What is really interesting is that such an automorphism $\sigma \in D_{\mathfrak{P}}$ induces an automorphism $\widetilde{\sigma}$ of $\mathcal{O}_L/\mathfrak{P}$. This gives us a crucial homomorphism

$$\varphi : D_{\mathfrak{P}} \longrightarrow \mathrm{Gal}\Big(\frac{\mathcal{O}_L/\mathfrak{P}}{\mathcal{O}_K/\mathfrak{p}}\Big), \text{ where } \varphi(\sigma) = \widetilde{\sigma}.$$

One might wonder if this translates to some isomorphism. Indeed, by the first isomorphism theorem, we have the following:

Theorem 16. *For $D_{\mathbb{P}}$ and $Gal(\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p})$ as above, the homomorphism is surjective, and so*

$$D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong Gal\Big(\frac{\mathcal{O}_L/\mathfrak{P}}{\mathcal{O}_K/\mathfrak{p}}\Big),$$

where the kernel $I_{\mathfrak{P}}$ is $\ker(\phi) = \{\sigma \in D_{\mathfrak{P}} : \sigma(a) \equiv a \bmod \mathfrak{p}$ for all $a \in \mathcal{O}_L\}$. Furthemore, we have $|I_{\mathbb{P}}| = e_{\mathfrak{P}|\mathfrak{p}}$ and $|D_{\mathfrak{P}}| = e_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}}$.

Much of the interesting mathematics here comes from the right hand side: $\mathrm{Gal}(\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p})$ is a cyclic group with q elements. The canonical generator of this cyclic group is the Frobenius automorphism $x \mapsto x^q$, where $q = N(\mathfrak{p})$ is the norm of $\mathfrak{p}$ by definition. This sets up the following theorem:

Theorem 17. *Let L/K be a Galois extension, and let $\mathfrak{p}$ be a prime unramified in L. If $\mathfrak{P}$ is a prime above $\mathfrak{p}$, then there is a unique element $\sigma \in Gal(L/K)$ such that for all $\alpha \in \mathcal{O}_L$,*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}},$$

where $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ is the norm of $\mathfrak{p}$. This unique element σ is called the Artin symbol, *denoted $\left(\frac{L/K}{\mathfrak{P}}\right)$. Thus for all $\alpha \in \mathcal{O}_L$, we have*

$$\Big(\frac{L/K}{\mathfrak{P}}\Big)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}$$

Proof. We have already provided a partial proof of this in setting up the theorem. For an unramified prime $\mathfrak{p}$, $e_{\mathfrak{P}|\mathfrak{p}} = |I_{\mathfrak{P}}| = 1$, so the isomorphism is directly $D_{\mathfrak{P}} \cong \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p})$. Since $\mathrm{Gal}(\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p})$ is cyclic, there exists a unique $\sigma \in D_{\mathfrak{P}}$ that maps to the Frobenius element. Then since $q = N(\mathfrak{p})$, we have that for all $\alpha \in \mathcal{O}_L$, σ uniquely satisfies $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}$. □

Note that a really important component to the definition of the Artin symbol is that the prime $\mathfrak{p}$ is unramified. Subsequently, exciting things happen if we consider an unramified abelian extension L/Kl; in this case, all primes are unramified.

Definition 4.2.5. Every fractional ideal $\mathfrak{a} \in I_K$ has factorization $\mathfrak{a} = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\cdots\mathfrak{p}_n^{r_n}$. By virtue of this, we can define a generalized Artin symbol $\left(\frac{L/K}{\mathfrak{a}}\right)$ as

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{j=1}^{n}\left(\frac{L/K}{\mathfrak{p}_j}\right)^{r_j},$$

which defines a homomorphism

$$\left(\frac{L/K}{\cdot}\right) : I_K \longrightarrow \mathrm{Gal}(L/K) \text{ called the } \textit{Artin map.}$$

This brings us to one of the defining results of class field theory: Artin reciprocity.

Theorem 18 (Artin Reciprocity for Hilbert Class Fields)**.** *If H is the Hilbert class field, then the Artin map*

$$\left(\frac{H/K}{\cdot}\right) : I_K \longrightarrow \mathrm{Gal}(H/K)$$

induces a surjective homomorphism with kernel as P_K, the group of principal ideals. Thus the Artin map produces an isomorphism

$$\mathrm{Cl}(K) \cong \mathrm{Gal}(H/K).$$

This reciprocity law leads to a rather interesting correspondence stated in Theorem 15: if H is the Hilbert class field and $\mathfrak{p}$ is a prime ideal,

$$\mathfrak{p} \text{ is a principal ideal} \iff \mathfrak{p} \text{ splits completely in } H$$

Ramification for certain field extensions makes a general Artin reciprocity statement somewhat difficult to articulate. Instead, we provide next a weaker, but more generalized variant that will suit our purposes.
Here is the general scenario: let $\mathfrak{c}$ be an integral ideal that is divisible by all primes that ramify in L/K. The generalized group of fractional and principal ideals (modulo $\mathfrak{c}$) is defined to be

$$I(\mathfrak{c}) = \{\mathfrak{a} \in I_K : \mathfrak{a} \text{ is relatively prime to } \mathfrak{c}\}$$
$$P(\mathfrak{c}) = \{(\alpha) \in P_K : \alpha \equiv 1 \bmod \mathfrak{c}\}$$

Then the new Artin map is given by

$$\left(\frac{L/K}{\cdot}\right) : I(\mathfrak{c}) \longrightarrow \mathrm{Gal}(L/K)$$

Theorem 19 (Weak Artin Recpiprocity)**.** *Let L/K be a finite abelian extension. Then there exists an integral ideal $\mathfrak{c} \in \mathcal{O}_K$ that divides the ramifying primes of K such that for the Artin map, we have*

$$\left(\frac{L/K}{(\alpha)}\right) = 1 \textit{ for all } (\alpha) \in P(\mathfrak{c})$$

The important thing to note here is that we have circumvented the ramification condition. One might wonder how to generate the isomorphism that is characteristic of Artin reciprocity. This is done by considering the maximal $\mathfrak{c}$.

Definition 4.2.6. The largest ideal for which Theorem 19 is true is called the conductor of L/K, denoted $\mathfrak{c}_{L/K}$.

With this, we can indeed state a result for something more general than the Hilbert class field, called the ray class field of K modulo $\mathfrak{c}$.

Definition 4.2.7. The *ray class field* $M_\mathfrak{c}$ of K modulo $\mathfrak{c}$ is the largest field with a specific conductor $\mathfrak{c}_{L/K}$. That is, $\mathfrak{c}_{L/K} \mid \mathfrak{c}$ implies $L \subset M_\mathfrak{c}$.

Now, we have the following:

Theorem 20 (Ray Class Field Theory)**.** *Let L/K be a finite abelian extension.*

(1) The Artin map

$$\left(\frac{L/K}{\cdot}\right) : I(\mathfrak{c}_{L/K}) \longrightarrow Gal(L/K)$$

is a surjective homomorphism, with a corresponding isomorphism enabled by the first isomorphism theorem.

(2) The ray class field $M_{\mathfrak{c}}$ exists and has the defining property

$$\{\text{primes of } K \text{ splitting completely in } M_{\mathfrak{c}}\} \Longleftrightarrow \{\text{prime ideals in } P(\mathfrak{c})\}.$$

4.3. **Explicit Class Field Theory.** Our detour into Artin reciprocity relates back to our study of abelian extensions by Theorem 18. As a consequence, we have a one-to-one correspondence between unramified abelian extensions L of K and subgroups S of the $\mathrm{Cl}(K)$. Not only that, within each correspondence, the Artin map induces an isomorphism $\mathrm{Cl}(K)/S \cong \mathrm{Gal}(L/K)$. In essence then, all the information about abelian extensions is contained within K itself.

As noteworthy as these theorems are, they do not shed light on an *explicit computation* of these abelian extensions. The Kronecker-Weber theorem can be restated to that end as follows:

Theorem 21 (Explicit Kronecker-Weber theorem)**.** *For the field $\mathbb{Q}$, the function $f(x) = e^{2\pi ix}$ evaluated at elements $x \in \mathbb{Q}$ generates all abelian extensions of $\mathbb{Q}$. Specifically, the ray class fields are generated by rational values of the complex exponential as above.*

The above theorem is particularly elegant in the ease with which we can generate abelian extensions. Hilbert's 12th problem seeks a generalization to arbitrary number fields.

Conjecture 22 (Hilbert's 12th Problem)**.** *Let K be a number field. Then there exists a function F such that we can find points $x_1, x_2, \ldots \in K$ so that $K\Big(F(x_1), F(x_2), \ldots, \{r_i\}\Big)$ as a field extension allows the generation of all abelian extensions of K, where the functions r_i are other relevant objects.*

The theory of CM originated as a particularly beautiful resolution of this conjecture for imaginary quadratic fields $K/\mathbb{Q}$, with the elliptic modular function $j(\tau)$ playing the role of the complex exponential.

Theorem 23. *Let K be an imaginary quadratic field and $E/\mathbb{C}$ an elliptic curve with CM by $\mathcal{O}_K$. Additionally, let $w : E \to \mathbb{CP}^1$ denote the Weber function of an elliptic curve that isolates the x-coordinate for the curve. Then for an integral ideal $\mathfrak{o}$, the ray class field M of modulus $\mathfrak{o}$ is given by*

$$M_{\mathfrak{o}} \cong K(j(E), E[\mathfrak{o}]),$$

where $E[\mathfrak{o}] = \{P \in E : [\alpha]P = 0 \text{ for all } \alpha \in \mathfrak{o}\}$ represents the $\mathfrak{o}$-torsion points of the curve.

Beyond this case, Hilbert's 12th problem remains mostly unsolved. Very recently, great progress has been made in the case of totally real fields F. Here, the abelian extensions are constructed by Brumer-Stark units and some other elements of the field F. The paper proving this remarkable theorem, in preprint at the time of this exposition, is [DK21].
Once again, it is useful to observe parallels between the two results that we have, especially since it contextualizes the relevance of the elliptic curves with the unit circle. The rational points of $e^{2\pi iz}$ are essentially the torsion points of the multiplicative group on the unit circle $\mathbb{T} \cong \mathrm{SO}(2)$. So then in regards to theorem 12, the quadratic imaginary case replaces the unit circle's nice symmetry with that of an elliptic curve.

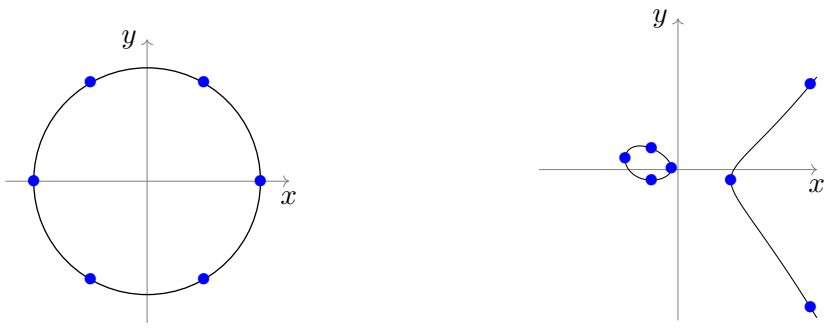

FIGURE 6. Left: The 6-torsion points $\{z \in \mathbb{T} : z^6 = 1\}$ of the unit circle
Right: The 8-torsion points $\{P \in E : 8P = O\}$ of the elliptic curve
$E/\mathbb{Q} : y^2 + xy = x^3 - 4x - 1$ (along with the one at infinity).

5. CM Part II: The beauty of Complex Multiplication

5.1. **Algebraicity conditions.** In this section, with an adequate background in class groups and class fields, we finally begin to discuss some of the very exciting consequences of the extra symmetries of CM curves. First recall that we suggested a strong relationship between isomorphism classes in $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$ and ideal classes of K. We start by developing this correspondence with the following theorem:

Theorem 24. *Let Λ be a CM lattice such that $E_\Lambda \in \mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$. Further, let $\mathfrak{a}$ be a non-zero fractional ideal of K which is $\widetilde{\mathfrak{a}}$ in $Cl(K)$.*

(1) There exists a well-defined action of $Cl(K)$ on $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$ defined by

$$\widetilde{\mathfrak{a}} \circ E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda},$$

with the product $\mathfrak{a}\Lambda$ defined as $\mathfrak{a}\Lambda = \{a_1\lambda_1 + \cdots a_n\lambda_n : a_i \in \mathfrak{a}, _i \in \Lambda\}$. That is, the action

$$\circ : \mathrm{Cl}(K) \times \mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K) \to \mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$$

is an injective homomorphism.

(2) The action above is simply transitive.

Proof. The group action part is readily seen by noting that

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

(1) **Closure.** This is verified by first proving that $\mathfrak{a}\Lambda$ is indeed a lattice, and then that $E_{\mathfrak{a}\Lambda} \in \mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$. By assumption, since $\mathrm{End}_{\mathbb{C}}(E_\Lambda) = \mathcal{O}_K$, it follows that $\mathcal{O}_K\Lambda = \Lambda$. Choose $d \in \mathbb{Z}$ such that $d\mathfrak{a} \subset \mathcal{O}_K$ for a fractional ideal $\mathfrak{a}$, so that $d\mathfrak{a}\Lambda \subseteq \mathcal{O}_K\Lambda = \Lambda$. This makes $\mathfrak{a}\Lambda$ a discrete subset of $\mathbb{C}$. But we can also choose d such that $d\mathcal{O}_K \subseteq \mathfrak{a}$, which gives $d\Lambda \subseteq \mathfrak{a}\Lambda$. Thus, $\mathfrak{a}\Lambda$ must span $\mathbb{C}$ as well, making it a lattice.
Next, for $\alpha \in \mathbb{C}^*$ we have $\mathrm{End}_{\mathbb{C}}(E_{\mathfrak{a}\Lambda}) = \{\alpha : \alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda\}$. But then by multiplying the inverse ideal $\mathfrak{a}^{-1}$, this set is equivalent to $\{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$, which is precisely $\mathrm{End}_{\mathbb{C}}(E_\Lambda) = \mathcal{O}_K$. The action thus gives an element that is in $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$ again.

(2) **Injectivity.** By the elliptic curve and lattice correspondence, we have $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ if and only if the lattices are homothetic, if and only if there exists $c \in \mathbb{C}^*$ such that $\mathfrak{a}\Lambda = c\mathfrak{b}\Lambda$. Multiplying both sides by $\mathfrak{a}^{-1}$, we get on the left that $\mathfrak{a}^{-1}\mathfrak{a}\Lambda = (1)\Lambda = \mathcal{O}_K\Lambda = \Lambda$. Then $\Lambda = c\mathfrak{a}^{-1}\mathfrak{b}\Lambda$. Similarly, by multiplying $c^{-1}\mathfrak{b}^{-1}$, we also get $\Lambda = c^{-1}\mathfrak{a}\mathfrak{b}^{-1}\Lambda$. Since both take the lattice exactly back to itself, they are each contained in $\mathcal{O}_K$.
Thus $\mathfrak{p} = c\mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathcal{O}_K$, but since $\mathfrak{p}^{-1} = c^{-1}\mathfrak{a}\mathfrak{b}^{-1}\Lambda = \{x \in K : x(\mathfrak{p}) \subseteq A\}$, we must have 1 in $\mathfrak{p}^{-1}$. Since it is a fractional ideal, $\mathfrak{p}^{-1} = \mathcal{O}_K$ and so $\mathfrak{p} = \mathcal{O}_K$ as well. Then $c\mathfrak{a}^{-1}\mathfrak{b} = (1)$,

and so $\mathfrak{a} = c\mathfrak{b}$. This means that they are equal in the class group. Thus $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ implies $\widetilde{a} = \widetilde{b}$ as part of injectivity. This completes the well-defined portion.

(3) **Transitivity.** Let Λ_1 and Λ_2 be two lattices such that $E_{\Lambda_1}, E_{\Lambda_2} \in \mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$. To show transitivity, we simply need to find $\mathfrak{a}$ such that $\widetilde{\mathfrak{a}}\Lambda_1 = \Lambda_2$. For nonzero λ_1 and λ_2 in Λ_1 and Λ_2 respectively, we define fractional ideals $\mathfrak{a}_1 = \frac{1}{\lambda_1}\Lambda_1$ and $\mathfrak{a}_2 = \frac{1}{\lambda_2}\Lambda_2$. We can use this to construct our desire ideal, since $\frac{\lambda_2}{\lambda_1}\mathfrak{a}_2\mathfrak{a}_1^{-1}\Lambda_1 = \Lambda_2$. With $\mathfrak{a} = \mathfrak{a}_2^{-1}\mathfrak{a}_1$, we have homothety of lattices $\mathfrak{a}^{-1}\Lambda_1$ and Λ_2, which then gives transitivity because

$$\widetilde{\mathfrak{a}} \circ E_{\Lambda_1} = E_{\mathfrak{a}^{-1}\Lambda_1} = E_{\Lambda_2} \text{ as desired.}$$

The action is simply transitive due to injectivity, which finishes the proof.

□

Corollary 24.1. *There are only finitely many isomorphism classes of elliptic curves with complex multiplication by K.*

Proof. Thus there is a unique fractional ideal $\mathfrak{a}$ for every two elliptic curves $E_\Lambda, E_{\Lambda'}$ such that $\widetilde{\mathfrak{a}} \circ E_\Lambda = E_{\Lambda'}$ by the above theorem. Then the $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$ is equal to that of the class group. Consequently,

$$|\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)| = h_K.$$

By Corollary 12.1, the class number is finite, so the number of isomorphism classes must be finite as well. □

This tells us that CM is sadly a rare phenomenon, occurring only for finitely many elliptic curves for each imaginary quadratic field K. However, as we will see, these curves are extremely special and can be exploited for a great deal of applications.

Theorem 25. *For an elliptic curve $E/\mathbb{C}$ with CM by $\mathcal{O}_K$, the j-invariant $j(E)$ is an algebraic number.*

Proof. We show this result by proving that for all automorphisms of $\mathbb{C}$, $j(E)$ is only able to take finitely many values, and so it must have finitely many Galois Conjugates and thus is algebraic. Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ and $E/\mathbb{C}$ be an elliptic curve with CM by $\mathcal{O}_K$. First note that if $\mathrm{End}_{\mathbb{C}}(E) \cong \mathrm{End}_{\mathbb{C}}(E^\sigma)$ because if $\phi : E \to E$ is an endomorphism, so must be $\phi^\sigma : E^\sigma \to E^\sigma$. Then $\mathrm{End}_{\mathbb{C}}(E^\sigma) = \mathcal{O}_K$ as well, and since $|\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)| = h_K$, E^σ belongs to one of the finitely many h_K isomorphism classes. On the other side, $j(E)$ is a rational combination of the coefficients of $E/\mathbb{C}$ in the Weierstrass form. Now with σ acting on these coefficients, it follows that $j(E^\sigma) = j(E)^\sigma$.
As we have seen before, as σ ranges over $\mathrm{Aut}(\mathbb{C})$ elliptic curves E^σ can be in one of only h_K many isomorphism classes. Since $j(E^\sigma) = j(E)^\sigma$ determines these classes through its values, it must be that $j(E)^\sigma$ takes less than h_K total values for all $\sigma \in \mathrm{Aut}(\mathbb{C})$. Thus $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$ is finite, making $j(E)$ algebraic. □
This result already is quite powerful, but as we will see, CM strengthens this to say that the degree of $j(E)$ is exactly equal to h_K.

Remark (Transcendence beyond degree 2)**.** The above theorem amounts to saying that in the case of quadratic imaginary fields K, the j-function $j(E_\Lambda)$ is algebraic, where Λ is the lattice associated with the field K. An extension that can be found in [WBS87] is that for a lattice $\Lambda = [1, \alpha]$ such that the degree $[\mathbb{Q}(\alpha) : \mathbb{Q}] > 2$, $j(E_\Lambda)$ is transcendental.

This says that imaginary quadratic fields are very special not only in that they always admit algebraic values of $j(E)$ with degree h_K, but that all fields of a greater degree give only transcendental values.

5.2. **Integrality of $j(\tau)$ and Heegner Numbers.** Now, we strengthen the previous result, since we can actually say that $j(\tau)$ is an algebraic integer of degree h_K.

Theorem 26. *Let $E/\mathbb{C}$ have CM by an order $\mathcal{O}$. Then $j(E)$ is an algebraic integer of degree h_K.*

This is a really exciting result, especially when we consider what it really means for $j(\tau)$ to be algebraic at some points. It is defined as a rational function of Eisenstein series, which are already quite difficult to evaluate. In spite of this, we have a lot of specific information about transcendentality and algebraicity as seen in the Remark above.
Furthermore, we prove this theorem in a way that seamlessly connects the analytic properties of modular forms and modular curves with elliptic curves.

We have seen the use of modular groups $\Gamma(N), \Gamma_1(N)$ and their corresponding modular curves, especially in the context of elliptic curves. There is another commonly used modular group that has number theoretic meaning:

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

The modular curve $X_0(N) = \Gamma_0(N) \backslash \mathbb{H}^*$ will be particularly useful to us, and will serve as the main link between the analytic and algebraic properties of $j(\tau)$ that gives Theorem 26. The Modularity theorem, one of the most famous theorems for $E(\mathbb{Q})$, can be stated to say that every elliptic curve $E(\mathbb{Q})$ admits a morphism $X_0(N) \to E$ for some $N \in \mathbb{N}$. More properties of modular curves in the context of elliptic curves can be found in [DS05] and [RS11].

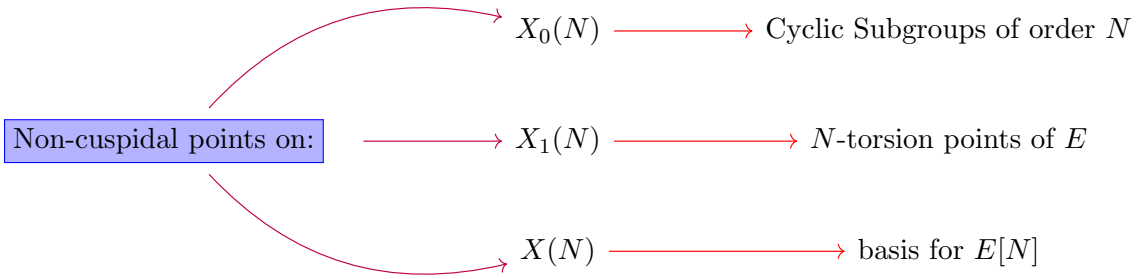

FIGURE 7. Correspondence between modular curves and the extra structure of elliptic curves (Theorem 5.2.5 in [RS11]).

In our case, $X_0(N)$ accomplishes the following:

(1) $X_0(N)$ can be interpreted as a curve over any field, including finite fields, which helps in developing relationships to elliptic curves.
(2) The family of modular curves $X_0(N)$ parametrizes isogenies between elliptic curves. That is, for a given j-invariant of an elliptic curve and $N \in \mathbb{N}$, we can use $X_0(N)$ to find j-invariants of all curves related to E by an isogeny with kernel a cyclic group of order N.

The applicability of the second one will be much more apparent through our study of the modular polynomial Φ_N. For reference, the first one alludes to the fact that $X_0(N)$ can be interpreted as a *moduli space* for cyclic N-isogenies, but we do not go into that here.

Definition 5.2.1. We define the modular polynomial to be

$$\Phi_N(X, j(\tau)) = \prod_{\gamma \in \mathcal{S}(N)} (X - j(N\gamma\tau)),$$

where $\mathcal{S}(N)$ is the set of matrices

$$\mathcal{S}(N) = \Big\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = N, 0 \le b < d \Big\}.$$

The reason this matrix is important is that it is a set of the right cosets of the modular curve $X_0(N)$. We will first show that $\Phi_N(X, j(\tau))$ has coefficients in $\mathbb{Z}[X, j]$. Using the correspondence between $X_0(N)$ and cyclic N-isogenies of elliptic curves, we will then be able to prove that a related Hilbert class polynomial H has coefficients in $\mathbb{Z}$.

Definition 5.2.2. The Hilbert Class Polynomial $H_D(X)$ is defined as

$$H_D(X) = \prod_{j(E) \in j(\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}))} (X - j(E)).$$

The theorem evidently follows from the fact that $H_D(X) \in \mathbb{Z}[X]$.
We begin with an examination of the modular polynomial $\Phi_N(X, j(\tau))$. Naturally, the matrices $\mathcal{S}(N)$ admit a representation in terms of the elementary matrices S and T. In particular, we have

$$\mathcal{S}(N) = \{\Gamma_0(N)\} \cup \{\Gamma_0(N) S T^K \text{ for } 0 \le k \le N-1\}, \text{ so}$$

$$\Phi_N(X, j(\tau)) = (X - j(N\tau)) \prod_{k=0}^{n-1} (X - j(N\gamma_k \tau)) \text{ where } \gamma_k = ST^k.$$

Lemma 27. *The modular polynomial has integral coefficients. That is, $\Phi_N(X, j(\tau)) \in \mathbb{Z}[X, j]$.*

Proof. An arbitrary coefficient $C(\tau)$ of $\Phi_N(X, j)$, as a polynomial in $j(N\tau)$ and $j(N\gamma_k\tau)$, has some noteworthy features. Since $j(\tau)$ is holomorphic on $\mathbb{H}$, so is $C(\tau)$. By the same logic $C(\tau)$ is also $\Gamma(1)$ invariant. Then as a modular function holomorphic on $\mathbb{H}$, it must be a polynomial in $j(\tau)$. This is incredibly useful, because if we can show that the q-expansion of $C(\tau)$ has integer coefficients, then it must be an integer polynomial in $j(\tau)$. This would make $\Phi_N(X, j(\tau))$ automatically an integer polynomial as well.
Our approach will be to first show that $C(\tau)$ has rational coefficients. Since q-expansions of $j(N\tau)$ and $j(N\gamma_k\tau)$ have coefficients as algebraic integers, we already know that $C(\tau)$ must have algebraic integer coefficients. If would the follow that $C(\tau)$ must have coefficients in $\mathbb{Q} \cap \{\text{number ring}\} = \mathbb{Z}$.
By the q-expansion of the j function,

$$j(N\tau) = \frac{1}{q^N} + 744 + \sum_{n=1}^{\infty} c_n q^{nN}, \text{ and}$$

$$\begin{aligned} j(N\gamma_k\tau) &= j\Big(\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} S T^K \tau \Big) = j\Big(S \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix} T^k \tau \Big) \\ &= j\Big(\begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \tau \Big) \qquad \text{(By } SL_2(\mathbb{Z}) \text{ invariance of } j) \\ &= j\Big(\frac{\tau + k}{N} \Big). \end{aligned}$$

Now observe that we can transform the powers of $j(N\gamma_k\tau)$ as

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

Subsequently, the individual expansions, with c_n as integer coefficients, look like

$$j(N\tau) = \frac{1}{q^N} + 744 + \sum_{n=1}^{\infty} c_n q^{nN}, \; j(N\gamma_k\tau) = \frac{1}{\zeta_N^k q^{1/N}} + 744 + \sum_{n=1}^{\infty} c_n \zeta_N^{kn} q^{n/N}.$$

As a result, $j(N\gamma_k\tau) \in \mathbb{Q}(\zeta_n)((q^{1/N}))$, where $K((x))$ denotes a the formal power series ring of K. $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ just permutes the $j(N\gamma_k\tau)$, and so the coefficients of $f(\tau)$ are fixed by the group and so must lie in $\mathbb{Q}$. This proves rationality of coefficients, and also integrality by the previously mentioned reasoning. So $\Phi_N(X, j(\tau)) \in \mathbb{Z}[X, j]$. □

With this, we can finally prove the theorem.

Proof of Theorem 26. We relate the Hilbert Class Polynomial to $\Phi_N(X, Y)$. Let $\mathcal{O}$ be an order of an imaginary quadratic field $K/\mathbb{Q}$ with discriminant D and let $E/\mathbb{C}$ be an elliptic curve with CM by $\mathcal{O}$. Next, let (p) be a principal ideal of prime norm p in $\mathcal{O}$. Since it is principal, it is the identity of $\mathrm{Cl}(\mathcal{O})$,. By the group action defined in Theorem 13, it acts trivially on $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O})$ so that $\widetilde{(p)}E \cong E$. The ideal can thus be interpreted as a degree p endomorphism of E, and since the degree of the kernel is prime, this isogeny is cyclic. This is precisely the condition under which $j(E)$ would be a root of $\Phi_P(X, j)$, and so we have $\Phi_p(j(E), j(E)) = 0$.
It is easy to verify that $\Phi_n(X, X)$ has leading coefficient one by examining the q-expansion. Since it also has integer coefficients by the above lemma, $j(E)$ is an algebraic integer. Since the roots $j(\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}))$ are algebraic integers, the coefficients of $H_D(X)$ must be so as well.

For rationality, first observe that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the set $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O})$ through the coefficients A and B of the Weierstrass equation of an elliptic curve. For $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have shown in Theorem 25 that E^σ has CM by $\mathcal{O}$, so even under this automorphism, $j(E^\sigma) \in j(\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}))$. Thus it follows that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $j(\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}))$; i.e, all the roots of $H_D(X)$. However, when expanded, the polynomial $H_D(X)$ has coefficients as symmetric polynomials in these roots. Thus $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ends up fixing the coefficients and so they all lie in $\mathbb{Q}$.
However, we know that the coefficients are already algebraic integers. Combining both, the coefficients lie in $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$.
This proves our result: since we have h_K distinct isomorphism classes of elliptic curves over which the $H_D(X)$ is defined with integral coefficients, the polynomial has degree h_K. So $j(E)$ is an algebraic integer of degree h_K. □

If $h(\mathcal{O}_K) = 1$ for $E/\mathbb{C}$ with CM, something very unique happens. By theorem 26, $j(\tau)$ is actually an integer.
Consider the imaginary quadratic field $K = Q[\sqrt{-163}]$ which has class number one. The Fourier series of $j(\tau)$ is given by

$$j(\tau) = \frac{1}{q} + 744 + O(q), \text{ where } q = e^{2\pi i\tau}.$$

We substitute the basis for the lattice $\Lambda = [1, \tau]$, which is $\tau = \frac{1+\sqrt{-163}}{2}$ since $-163 \equiv 1 \bmod 4$. That gives

$$j(\tau) = e^{-2\pi i\frac{1+\sqrt{-163}}{2}} + 744 + O(q), \text{ or } e^{\pi\sqrt{163}} = -j(\tau) + 744 + O(e^{-\pi\sqrt{163}})$$

Now since $j(\tau) \in \mathbb{Z}$, $e^{\pi\sqrt{163}}$ is really close to an integer, with an error of only about 3.8×10^{-18}. In general, however, class number one and consequent near integrality of $e^{\pi\sqrt{d}}$ is a very rare situation.

Theorem 28 (Stark-Heegner Theorem)**.** *For $d < 0$, then the class number of $\mathbb{Q}(\sqrt{d})$ is equal to 1 only when*

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

5.3. **Class Field Theory.** Notice that one of the rather peculiar aspects of our proof is that we used the polynomial $H_D(X)$, whose roots are actually being acted upon by two different groups. First we naturally have the class group $\mathrm{Cl}(K)$, whose action on $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O})$ was defined in Theorem

13. But then we also have the action of $\mathrm{Gal}(L/\mathbb{Q})$, where $L \subseteq \overline{\mathbb{Q}}$ is the splitting field of $H_D(X)$. It is reasonable to suspect some form of compatibility between the two, because otherwise the world would implode. Such a relationship, albeit a little different, indeed is true.

Theorem 29. *Let $E/\mathbb{C}$ have CM by $\mathcal{O}$. Then $K(j(E))$, which is also the splitting field of $H_D(X)$, forms the Hilbert class field of the order $\mathcal{O}_K$.*

This makes the explicit class field theory problem remarkably easy. We prove the thoerem using the method of Artin reciprocity and other class field theory developed in Section 4.

Proof. Let L/K be the finite field extensions that is the fixed field of $\ker(\phi)$ for the homomorphism $\phi : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Cl}(K)$. Then

$$\begin{aligned}
\mathrm{Gal}(\overline{K}/L) &= \ker(\phi) \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : \phi(\sigma) = 1\} && \text{(definition of } \ker(\phi)) \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : \phi(\sigma) * E = E\} && \text{(action of } \mathrm{Cl}(K), \text{ Theorem 24)} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : E^\sigma = E\} && \text{(image of } \phi) \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : j(E^\sigma) = j(E)\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : j(E)^\sigma = j(E)\} \\
&= \mathrm{Gal}(\overline{K}/K(j(E))),
\end{aligned}$$

so $L = K(j(E))$. Since the map ϕ is injective, it is evident that $L/K = K(j(E))/K$ is an abelian extension. This, along with the map, already hint at L being the Hilbert Class field, since it is resonant what we had for Artin reciprocity of Hilbert class fields. We wish to solidify our reasoning: Let $\mathfrak{c}_{L/K}$ be the conductor of L/K. We study the composition of ϕ with the Artin map.

Claim 29.1. *The composition of maps*

$$I(\mathfrak{c}_{L/K}) \xrightarrow{\left(\frac{L/K}{\cdot}\right)} Gal(L/K) \xrightarrow{\quad\phi\quad} Cl(K)$$

yields just the natural projection of $I(\mathfrak{c}_{L/K})$ onto $Cl(K)$. That is, $\phi \circ \left(\frac{L/K}{\cdot}\right)$ acts as an identity in that $\phi(\left(\frac{L/K}{\mathfrak{a}}\right)) = \widetilde{\mathfrak{a}}$ for all $\mathfrak{a} \in I(\mathfrak{c}_{L/K})$.

The significance of this claim is that we use a special prime $\mathfrak{p}$ to carry out the Artin map of $\mathfrak{a}$, which will make the extension L unramified.
To prove this claim, we need the existence of a splitting prime $\mathfrak{p}$ that is the preimage of its Frobenius element. This uses powerful results such as a generalized Dirichlet theorem for prime ideals and curves with good reduction, so we omit a proof of existence, which can be found in [Sil94]. For our purposes, we have the existence of a degree 1 prime $\mathfrak{p} \in I(\mathfrak{c}_{L/K})$ that is in the same ideal class as $\mathfrak{a}$. This corresponds to the condition that $\alpha \equiv 1 \pmod{\mathfrak{c}}_{L/K}$ for $\mathfrak{a} = (\alpha)\mathfrak{p}$. Now we have

$$\begin{aligned}
\phi(\left(\frac{L/K}{\mathfrak{a}}\right)) &= \phi(\left(\frac{L/K}{(\alpha)\mathfrak{p}}\right)) && \mathfrak{a} = (\alpha)\mathfrak{p} \\
&= \phi(\left(\frac{L/K}{\mathfrak{p}}\right)) && \alpha \equiv 1 \pmod{\mathfrak{c}}_{L/K} \\
&= \widetilde{\mathfrak{p}} && \text{by construction} \\
&= \widetilde{\mathfrak{a}}.
\end{aligned}$$

This proves the claim.
Next, by the claim, since principal ideals are trivial in the class group, $\phi(\left(\frac{L/K}{(\alpha)}\right)) = 1$ for all principal

ideals $(\alpha) \in I(\mathfrak{c}_{L/K})$. Since ϕ is injective, it must be that $(\left(\frac{L/K}{(\alpha)}\right)) = 1$ for the Artin symbol, for all principal ideals. But recall that the conductor is defined to have the property

$$\alpha \equiv 1 \mod \mathfrak{c}_{L/K} \text{ implies } (\left(\frac{L/K}{(\alpha)}\right)) = 1.$$

Then it must be that the conductor is trivially (1). The conductor is thus divisible by every ramifying prime, making L/K everywhere unramified. As an abelian unramified extension, $L = K(j(E))$ must be contained within the Hilbert class field.

To show that it is exactly equal, first note that the natural map induced by the Artin symbol $I(\mathfrak{c}_{L/K}) = I((1)) \to \mathrm{Cl}(K)$ is surjective trivially, which implies that ϕ is surjective. Since ϕ is both surjective and injective, it is an isomorphism. Thus

$$[L : K] = |\mathrm{Gal}(L/K)| = |\mathrm{Cl}(K)| = \mathrm{Gal}(H/K) = [H : K].$$

Coupled with the fact that $L \subset H$, this proves that L must be equal to H. Consequently, $H = K(j(E))$. □

This gives us an extremely simple interpretation of the Hilbert Class Field that can be used to explicitly construct unramified abelian extensions in a straightforward manner. For abelian extensions, we require Theorem 23, a proof of which can be found in Chapter 2 of [Sil94] using similar, albeit more complex, methods.

6. Applications of CM

6.1. **Primes of the form $x^2 + ny^2$.** The representation of prime numbers in the form $x^2 + ny^2$ is a problem that has oddly established its significance over centuries of mathematics, appearing in different fields in a variety of contexts. The study of this problem leads to striking connections between preliminary number theory, Class Field Theory, and complex multiplication. See [Cox11] for an entire book on this subject.

Complex Multiplication plays a particularly valuable role in this problem by allowing an explicit calculation of one of the main conditions behind the representation.

Theorem 30. *Let $n > 0$ be an integer. Then there exists a monic irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ of degree $h(\mathcal{O})$ with the following property: if $p \nmid n$ and $p \nmid Disc(f_n)$, then*

$$p \text{ is of the form } x^2 + ny^2 \iff (\frac{-n}{p}) = 1 \text{ and } f_n(x) \equiv 0 \bmod p.$$

Additionally, $f_n(x)$ can be taken as the minimal polynomial of an algebraic integer α that is such that $L = K(\alpha)$ is the ring class field of $\mathbb{Z}[\sqrt{-n}]$ for an imaginary quadratic field $K = Q(\sqrt{-n})$. Such an $f_n(x)$ is also the minimal polynomial of a primitive element of the ring class field L/K.

Note that even though the above theorem is a very powerful and precise result, it does not say anything about what $f_n(x)$ really is, neither does it allow an explicit computation. We will show an algorithmic method to calculate $H_D(X)$, but its efficiency is somewhat dubious.

First note by Theorem 15 that $H_{-4n}(X)$ is the minimal polynomial of degree $h(\mathcal{O})$ of $j(\sqrt{-n})$ for $K = \mathbb{Q}(\sqrt{-n})$ as above. Furthermore, we also know that $j(\sqrt{-n})$ is primitive in a primitive element of the ring class field of $\mathcal{O}$, and so we can simply take $f_n(X) = H_{-4n}(X)$. Thus our problem now becomes to calculate the Hilbert Class polynomial, which we have just seen in the proof of Theorem 26 has a very convenient form. In particular, since $H_D(X)$ is simply

$$H_D(X) = \prod_{j(E) \in j(\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}))} (X - j(E)),$$

one can prove the following:

Theorem 31. *Let $\mathcal{O} \subset K$ be an order of an imaginary quadratic field with discriminant d and class number $h(\mathcal{O})$. Then for each reduced positive primitive definite quadratic form $a_k x^2 + b_k xy + c_k y^2$ of discriminant d, let r_k denote the root $\tau_k = \frac{-b_k+d}{2a_k}$ of the quadratic equation $a_k z^2 + b_k z + c_k = 0$, which belongs to the fundamental domain for all $1 \leq k \leq h$. Then the class equation is alternatively*

$$H_d(X) = \prod_{k=1}^{h} (X - j(\tau_k)).$$

This remarkable theorem, which can be found in [KY91], allows an algorithmic construction of the Hilbert Class polynomial partly using the theory of binary quadratic forms. See the same source for more on the subject.

7. And Beyond...

We conclude this expository paper by discussing some other places where the j-function and complex multiplication appear.

7.1. **Monstrous Moonshine Conjecture.** It was observed by McKay in a 1978 paper that the coefficients of the q-expansion of $j(\tau)$ were linear combinations in the dimensions of irreducible representations of the Fisher-Griess sporadic monster group. This mysterious relationship and its conjectured extensions to all Hauptmoduls is called the Monstrous Moonshine conjecture. Richard Borcherds proved the conjecture for $j(\tau)$ (See [Bor92]), although the generalized version and a reasonable understanding of the conjecture are not yet resolved.

7.2. **Elliptic Curve Primality Proving.** One of the striking applications of complex multiplication is in Elliptic curve primality proving. A famous algorithm by Goldwasser and Killian provided a method for proving primality of elliptic curves using Hasse's bound for elliptic curves

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

A significant source of time complexity is finding an elliptic curve with a suitable number of points. The CM method employed by Atkin and Morain allows us to circumvent this step by guaranteeing a CM curve with a suitable number of points. This significantly reduces the complexity involved. A great source for these methods is [AM93].

Atkin-Morain primality proving has proven to be one of the most practical methods of proving the primality of large primes. In fact, most of the top 20 primes on the list `https://primes.utm.edu/top20/page.php?id=27` use ECPP and Atkin and Morain's method.

References

[Ahl66] Lars Valerian Ahlfors. *Complex analysis: an introduction to the theory of analytic functions of one complex variable*, volume 2. McGraw-Hill New York, 1966.

[AM93] A Oliver L Atkin and François Morain. Elliptic curves and primality proving. *Mathematics of computation*, 61(203):29–68, 1993.

[Bor92] Richard E Borcherds. Monstrous moonshine and monstrous lie superalgebras. In *Invent. math.* Citeseer, 1992.

[Cas12] John William Scott Cassels. *An introduction to the geometry of numbers*. Springer Science & Business Media, 2012.

[Cox11] David A Cox. *Primes of the form x2+ ny2: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011.

[DK21] Samit Dasgupta and Mahesh Kakde. Brumer-stark units and hilbert's 12th problem. *arXiv preprint arXiv:2103.02516*, 2021.

[DS05] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*, volume 228. Springer, 2005.

[dSG16] Henri Paul de Saint-Gervais. *Uniformization of Riemann surfaces*. 2016.

[KY91] Erich Kaltofen and Noriko Yui. Explicit construction of the hilbert class fields of imaginary quadratic fields by integer lattice reduction. In *Number theory*, pages 149–202. Springer, 1991.

[Maz77] Barry Mazur. Modular curves and the eisenstein ideal. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 47(1):33–186, 1977.

[Mil20] James S Milne. *Elliptic curves*. World Scientific, 2020.

[RS11] Kenneth A Ribet and William A Stein. Lectures on modular forms and hecke operators. *Available on the web: http://wstein. org/books/ribet-stein/main. pdf*, 2011.

[Sil94] Joseph H Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer Science & Business Media, 1994.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[WBS87] Michel Waldschmidt, Daniel Bertrand, and J-P SERRE. Nombres transcendants et groupes algébriques: seconde édition. *Astérisque*, (69-70), 1987.