MATH UN3901.001 Supervised Readings in Mathematics Fall 2023

Elliptic Curves with Complex Multiplication

Prof. Nathan Chen *Scribe: Ekene Ezeunala*

Contents

1 Lecture 01—Elliptic Curves and their Endomorphism Rings **2**
1.1 Elliptic curve as a pointed algebraic curve . . . 2
1.2 Elliptic curve as an algebraic group . . . 3
1.3 Morphisms between elliptic curves—isogenies . . . 3
1.4 The structure of the endomorphism ring $\mathrm{End}(E_{\overline{K}})$ . . . 4

2 Lecture 02—Elliptic Curves over $\mathbb{C}$ and Complex Multiplication **6**
2.1 Elliptic curves over $\mathbb{C}$ and lattices . . . 6
2.1.1 Functions on $\mathbb{C}/\Lambda$ . . . 7
2.1.2 Associating an elliptic curve to a lattice Λ . . . 7
2.1.3 Associate a lattice to an elliptic curve . . . 8
2.2 CM elliptic curves over $\mathbb{C}$ . . . 8
2.2.1 From a proper fractional ideal to a CM elliptic curve . . . 8
2.2.2 From a CM elliptic curve to a proper fractional ideal . . . 9

3 Lecture 03—Modular Curve $X(1)$ and the j-invariant **11**
3.1 Modular functions and uniformisation . . . 11
3.2 The j-invariant of an elliptic curve . . . 13
3.3 The j-invariant of a CM elliptic curve . . . 13

4 Lecture 04—Modular Curves and the CM points on Modular Curves **16**
4.1 Rational points on algebraic curves . . . 16
4.2 Congruence subgroups and modular curves . . . 17
4.3 Rational points on modular curves and CM elliptic curves . . . 18
4.4 Heegner points . . . 19

5 Lecture 05—Arithmetic of CM Elliptic Curves **20**
5.1 Galois action on elliptic curves . . . 20
5.2 Field of definition for $\mathrm{End}(E)$ . . . 20
5.3 Field of definition for CM elliptic curves . . . 21
5.4 Torsion fields of CM elliptic curves . . . 22

6 Lecture 06—Reductions of CM Elliptic Curves **23**
6.1 Endomorphism rings of elliptic curves over finite fields . . . 23
6.2 Density of supersingular primes . . . 24
6.3 Elkies's theorem . . . 24

7 Problems and solutions **27**

§1 Lecture 01—Elliptic Curves and their Endomorphism Rings

Welcome to the first lecture of the Preliminary Arizona Winter School 2023. We start by giving some aspects to an object of our study, the *elliptic curve*.

§1.1 Elliptic curve as a pointed algebraic curve

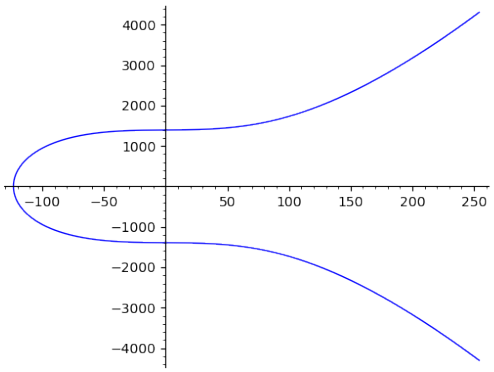

Figure 1.1: An elliptic curve

The blue curve in this picture contains points (x, y), $x, y \in \mathbb{R}$ satisfying the equation $y^2 = x^3 + 504x + 1942452$. This is an example of an elliptic curve (this one in particular is taken from the L-functions and modular forms database).

By an elliptic curve we mean a smooth genus 1 algebraic curve with a marked point. Every equation $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{C}$ and $4A^3 + 27B^2 \neq 0$ defines an elliptic curve. Namely, there is a a smooth projective model corresponding to this affine curve with the marked point being the point at ∞.

Definition 1.1. *An* elliptic curve *defined over a field K is a pair (E, O) where E is a smooth projective curve of genus* 1 *defined over K and $O \in E(K)$ is a marked point.*

When the characteristic of the field K is not 2 or 3, then any elliptic curve (E, O) satisfies an affine defining equation of the form $y^2 = x^3 + Ax + B$, $A, B \in K$, with O placed at ∞. A defining equation of the form $y^2 = f(x)$ with $\deg(f) = 3$ is called a *Weierstrass equation* for the associated elliptic curve.

Since an elliptic curve E/K is an algebraic curve of genus 1, the set of holomorphic differentials $\Omega_{E/K}$ on E is a 1-dimensional K vector space which we simply denote by V. If E is given by the affine equation $y^2 = x^3 + Ax + B$, then the differential $\omega = dx/y$ is a basis for V and is both holomorphic and non-vanishing. Thus the vector space V is $V = \{\alpha\omega : \alpha \in K\}$.

§1.2 Elliptic curve as an algebraic group

For an algebraic group C/K, let $\mathrm{Pic}^0(C)$ denote its divisor class group, defined as the set of degree 0 divisors over $\overline{K}$ modulo its subset of principal divisors. The Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on $\mathrm{Pic}^0(C)$ via its action on $C(\overline{K})$ by translation.

Definition 1.2. *The map $\phi : E(\overline{K}) \to \mathrm{Pic}^0(E) : P \mapsto (P) - (O)$ from the curve to its divisor class group is a bijection. The group law*

$$E \times E \mapsto E : (P_1, P_2) \mapsto \phi^{-1}\left(\phi(P_1) + \phi(P_2)\right)$$

and $E \to E : P \mapsto \phi^{-1}\left(-\phi(P)\right)$ induced on E is an algebraic morphism defined over K.

This group law makes elliptic curves projective group schemes of dimension 1. Higher dimensional projective varieties with an algebraic group structure are called *abelian varieties*. This is beyond the scope of this course, but we will see it in AWS 2024.

Remark 1.3. *For any field L/K and an elliptic curve E/K, the group law makes the set $E(L)$ into an abelian group. Thus it is natural to ask whether $E(L)$ is a finitely generated abelian group. The* Mordell-Weil theorem *states that when L is a number field, then $E(L)$ is a finitely generated abelian group, and on the other hand, when $L = \overline{\mathbb{Q}}$, even the torsion part of $E(L)$ is not finitely generated. This is a deep theorem and we will not prove it here. But the implications are that given an elliptic curve E/K, for which L/K is $E(L)$ finitely generated? This problem is a matter of current study in the realm of Diophantine stability.*

§1.3 Morphisms between elliptic curves—isogenies

After introducing the objects we call elliptic curves, our next goal is to study the morphisms between them. These morphisms will be regular maps between algebraic curves which are also group homomorphisms. Such maps are called *isogenies*.

Definition 1.4. *An* isogeny *between elliptic curves (E_1, O_1) and (E_2, O_2) over a field K is a non-constant algebraic map $E_1 \to E_2$ which maps O_1 to O_2. The map $\phi : E_1 \to O_2$ is called the trivial isogeny. Any nontrivial isogeny is a group homomorphism with finite kernel.*

Since isogenies are regular maps between algebraic curves, they induce maps between their divisor class groups Pic^0 and their sets of holomorphic differentials V. Both of the induced maps are very important tools in our study of isogenies.

Definition 1.5. *Let $\phi : E_1 \to E_2$ be a nontrivial isogeny. Then it induces a map $\phi^* : \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1)$. By composing isomorphisms $E_i \simeq \mathrm{Pic}^0(E_i)$, we obtain an isogeny $\hat{\phi} : E_2 \to E_1$ called the dual isogeny of ϕ.*

The veracity of the next lemma is immediate from the definition of the group law on elliptic curves and the dual isogeny. It will play an important role in the study of the structure of the endomorphism ring $\mathrm{End}(E)$.

Lemma 1.6. *Let $\phi : E_1 \to E_2$ be an isogeny. Then $\hat{\phi} \circ \phi = [\deg(\phi)]$.*

§1.4 The structure of the endomorphism ring $\mathrm{End}(E_{\overline{K}})$

We write $\mathrm{Hom}(E_1, E_2)$ for the set of isogenies from E_1 to E_2—this is a group under composition of maps—and $\mathrm{End}(E)$ for the set of isogenies from E to itself over K. We will denote by $\mathrm{End}(E_{\overline{K}})$ the set of endomorphisms from E to itself base changed to the algebraic closure $\overline{K}$. Next we discuss some properties of the set of isogenies between two elliptic curves E_1 and E_2.

Lemma 1.7. *The set of isogenies* $\mathrm{Hom}(E_1, E_2)$ *is a free abelian group under the addition law* $(\phi_1 + \phi_2)(P) = \phi_1(P) + \phi_2(P)$ *and the identity element being the trivial isogeny.*

Proof. The multiplication by m map (denoted as ϕ_m) is an isogeny and $m\phi = \phi_m \circ \phi$ for any isogeny ϕ. The composition of two dominant maps is dominnt, and this $\phi_m \circ \phi_n = \phi_{mn}$. Thus $\mathrm{Hom}(E_1, E_2)$ is a subgroup of the group of all dominant maps from E_1 to E_2. Since E_1 is a smooth projective curve, the Riemann-Roch theorem implies that the dimension of the vector space of regular maps from E_1 to E_2 is $\deg(E_2)$. Thus $\mathrm{Hom}(E_1, E_2)$ is a finitely generated abelian group. Since it is a subgroup of a free abelian group, it is itself free abelian. □

Lemma 1.8. *The endomorphism ring* $\mathrm{End}(E)$ *with multiplication being composition is an integral domain.*

Proof. Let $\phi \in \mathrm{End}(E)$ be a nontrivial endomorphism. Then ϕ is an isogeny and $\deg(\phi) \neq 0$. If $\psi \in \mathrm{End}(E)$ is such that $\phi \circ \psi = 0$, then $\deg(\phi)\deg(\psi) = 0$. Since $\deg(\phi) \neq 0$, we have $\deg(\psi) = 0$ and hence $\psi = 0$. Thus $\mathrm{End}(E)$ is an integral domain. □

Now let E_1, E_2 be elliptic curves given by Weierstrass equations. Let ω_1, ω_2 be the holomorphic differentials given by dx/y on E_1, E_2 respectively, and let V_i be the K-vector space of holomorphic differentials on E_i. For an isogeny $\phi : E_1 \to E_2$, we consider the induced map $\phi^* : V_2 \to V_1$.

Proposition 1.9. *Let E be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + Ax + B$ and let $\omega = dx/y$. Then the differential ω is invariant under the action of* $\mathrm{End}(E)$ *on V.*

Theorem 1.1. *Let $\phi_1, \phi_2 : E_1 \to E_2$ be two isogenies and $\phi_1^*, \phi_2^* : V_2 \to V_1$ be the induced maps on the spaces of holomorphic differentials. Then*

$$(\phi_1 + \phi_2)^*\omega = \phi_1^*\omega + \phi_2^*\omega.$$

Moreover, the map $\mathrm{End}(E) \to \mathrm{End}(V) \simeq K : \phi \mapsto \phi^*$ *is a ring homomorphism with kernel being the inseparable morphisms (morphisms whose induced map on the function fields is an inseparable field extension).*

Corollary 1.10. *If K is a field of characteristic 0, then* $\mathrm{End}(E_{\overline{K}})$ *is a commutative subring of* $\overline{K}$.

Recall that following the set of isomorphism theorems for groups, every group homomorphism $\phi : G \to H$ is determined by its kernel $\mathrm{Ker}(\phi)$ which is a normal subgroup of G (up to an isomorphism of H). To study $\mathrm{End}(E_{\overline{K}})$, we next look at the finite subgroups of $E(\overline{K})$.

Lemma 1.11. *When m is coprime to the characteristic of the field K, we have $E(\overline{K})[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$ where $E(\overline{K})[m]$ denotes the kernel of the multiplication by m map $\phi_m : E \to E, P \mapsto mP$.*

Proof. First note that the dual isogeny to the multiplication by m map is itself, $\widehat{\phi}_m = \phi_m$. Since ϕ_m is separable by assumption, we conclude that $|E/mE| = \deg(\phi_m) = m^2$. Since $E[m]$ is a subgroup of $E(\overline{K})$ of order m^2, it is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^2$. □

Any isogeny $\phi : E_1 \to E_2$ induces a map $E_1[m] \to E_2[m]$ for any $m \in \mathbb{Z}_{>0}$. For any prime ℓ coprime to the characteristic of the field K, there is an injection

$$\mathrm{Hom}(E_1, E_2) \hookrightarrow \mathrm{Hom}(E_1[\ell^\infty], E_2[\ell^\infty]).$$

Moreover, the following map is also injective.

$$\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \hookrightarrow \mathrm{Hom}(E_1[\ell^\infty], E_2[\ell^\infty]).$$

We now see a lemma.

Lemma 1.12. $\mathrm{End}(E_{\overline{K}})$ *is a free $\mathbb{Z}$-module of rank at most 4.*

Proof. Using the injectivity of the above map, we have

$$\mathrm{rank}_{\mathbb{Z}}\mathrm{End}(E_{\overline{K}}) = \mathrm{rank}_{\mathbb{Z}_\ell}\mathrm{End}(E_{\overline{K}}) \otimes \mathbb{Z}_\ell \leq \mathrm{rank}_{\mathbb{Z}_\ell}\mathrm{Hom}(E[\ell^\infty], E[\ell^\infty]) = 4,$$

and so the proof is done. □

Theorem 1.2. *For an elliptic curve E defined over a field K, the endomorphism ring* $\mathrm{End}(E_{\overline{K}})$ *is either isomorphic to $\mathbb{Z}$, an order of a quadratic imaginary field, or an order of a quaternion algebra over $\mathbb{Q}$.*

- *If K is of characteristic 0, then* $\mathrm{End}(E_{\overline{K}})$ *is commutative.*
- *If K is a finite field, then* $\mathrm{End}(E_{\overline{K}})$ *strictly contains $\mathbb{Z}$.*

Proof. The endomorphism ring $\mathrm{End}(E_{\overline{K}})$ satisfies the following statements:

- $\mathrm{End}(E_{\overline{K}})$ is a free $\mathbb{Z}$-module of rank at most 4, and an integral domain;
- there is an involution $\mathrm{End}(E_{\overline{K}}) \to \mathrm{End}(E_{\overline{K}}) : \phi \mapsto \hat{\phi}$;
- for any isogeny $\phi \in \mathrm{End}(E_{\overline{K}})$, the product $\phi\hat{\phi}$ is a non-negative integer, and $\phi\hat{\phi} = 0$ if and only if $\phi = 0$;

A ring satisfying these three conditions can only be one of the three types stated above. When K is of characteristic 0, then $\mathrm{End}(E_{\overline{K}})$ is commutative. When K is a finite field $\mathbb{F}_q$, then the Frobenius morphism is purely inseparable of degree q and it is different from the multiplication by $\sqrt{q}$ map even when q is a square. Thus $\mathrm{End}(E_{\overline{K}})$ strictly contains $\mathbb{Z}$. □

For the elliptic curve E/K where K has the characteristic 0, if $\mathrm{End}(E_{\overline{K}})$ strictly contains $\mathbb{Z}$, we say E has *complex multiplication.*

§2 Lecture 02—Elliptic Curves over $\mathbb{C}$ and Complex Multiplication

In last week's lecture we introduced elliptic curves from an abstract algebraic perspective. In this lecture we give a more geometric description of elliptic curves defined over the complex numbers $\mathbb{C}$. This description will allow us to think more concretely about points on a elliptic curve, visualise the set of torsion points, and more importantly provide an avenue by which we can parameterise all elliptic cuves over $\mathbb{C}$ and observe the ones with complex multiplication.

§2.1 Elliptic curves over $\mathbb{C}$ and lattices

Recall from the last lecture that an elliptic curve E is a smooth, projective, genus 1 algebraic curve with a marked point O. The set of complex points on a genus 1 curve over $\mathbb{C}$ is topologically a torus with complex analytic topology.

The universal cover of a torus is a 2-dimensional plane and the covering map is given by $\mathbb{R}^2$ moding out all translations $(x, y) \mapsto (x+m, y+n)$ where $m, n \in \mathbb{Z}$. The set of $\mathbb{C}$-points on an elliptic curve

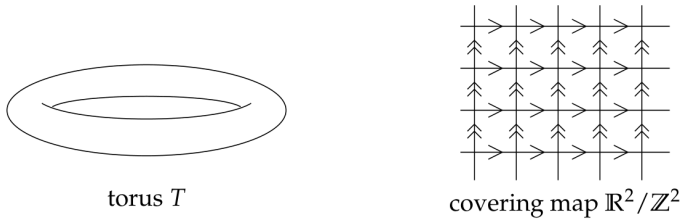

Figure 2.1: The universal cover of a torus

$E/\mathbb{C}$ can also be described in this way.

Definition 2.1. *A lattice $\Lambda \subset \mathbb{C}$ is a discrete subgroup of $\mathbb{C}$ which contains an $\mathbb{R}$-basis for $\mathbb{C}$.*

Question: Why is such a Λ isomorphic to $\mathbb{Z}^2$?

Let $\{\omega_1, \omega_2\}$ be a set of generators of Λ, i.e. $\Lambda = \{n_1\omega_1 + n_2\omega_2 : n_1, n_2 \in \mathbb{Z}\}$. The quotient C/Λ is a

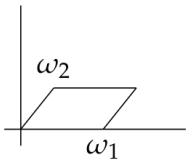

Figure 2.2: A lattice Λ

complex Lie group with the addition on $\mathbb{C}$. Given two lattices Λ_1, Λ_2, any maps between quotients $C/\Lambda_1 \to C/\Lambda_2$ are given by complex numbers $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 \subset \Lambda_2$ by

$$\phi_\alpha(z) \coloneqq \alpha z \mod \Lambda_2.$$

Two lattices Λ_1, Λ_2 are called homothetic if there is $\alpha \in \mathbb{C}^\times$ such that $\alpha\Lambda_2 = \Lambda_1$. This is an equivalence relation between lattices in $\mathbb{C}$. We will show that the complex points of an elliptic curve

$E(\mathbb{C})$ are isomorphic to $\mathbb{C}/\Lambda$ for some lattice Λ as complex Lie groups. Moreover, the following categories are equivalent:

Objects: elliptic curves over $\mathbb{C}$, up to isomorphism Maps: isogenies	$\Longleftrightarrow$	Objects: lattices $\Lambda \subset \mathbb{C}$, up to homothety Maps: $\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\}$

§2.1.1 Functions on $\mathbb{C}/\Lambda$

Recall points on an elliptic curve E defined over $\mathbb{C}$ satisfies a Weierstrass equation $y^2 = x^3 + Ax + B$. Thus to identify the set of points $E(\mathbb{C})$ and points in $\mathbb{C}/\Lambda$, where Λ is a lattice, we need to construct the functions f, g on C/Λ such that the values of $f(z), g(z)$ satisfy $f(z)^2 = g(z)^3 + Ag(z) + B$ for $z \in \mathbb{C}/\Lambda$.

Definition 2.2. *Let $\Lambda \subset \mathbb{C}$ be a lattice. The Weierstrass $\wp$-function relative to Λ is defined by the series*

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

The seriews in the definition of $\wp(z)$ converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$. The Weierstrass $\wp$-function is a meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at every lattice point and no other poles. It satisfies conditions

$$\wp(z + \omega) = \wp(z) \quad \text{for all } \omega \in \Lambda, z \in \mathbb{C}.$$

Meromorphic functions on $\mathbb{C}$ satisfying this condition are called *elliptic functions* on $C \setminus \Lambda$. The set of elliptic functions on $\mathbb{C}$ is a field which we denote by $\mathbb{C}(\Lambda)$. The derivative $\wp'(z)$ of the Weierstrass $\wp$-function is also an elliptic function. Moreover, the field $\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp')$ is generated by $\wp$ and $\wp'$ over $\mathbb{C}$. Every elliptic function is a rational combination of $\wp$ and $\wp'$.

§2.1.2 Associating an elliptic curve to a lattice Λ

Next we show that $\wp(z)$ and $\wp'(z)$ satisfies an equation of the form $\wp'(z)^2 = 4\wp(z)^3 + A\wp(z) + B$.

Definition 2.3. *Let $\Lambda \in \mathbb{C}$ be a lattice. The* Eisenstein series *of weight $2k$ is the series*

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^{2k}}.$$

The Eisenstein series is absolutely convergent for all $k > 1$. Thus for a fixed lattice Λ and $k > 1$, the values $G_{2k}(\Lambda)$ are constants associated to Λ which we simply denote by G_{2k}. The Laurent series for $\wp(z)$ around $z = 0$ is given by

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

The only holomorphic elliptic functions are constant functions. Thus, using the Laurent series of $\wp(z)$ and $\wp'(z)$, we could compare the order of the pole at $z = 0$ to conclude the following

statement. For a fixed lattice Λ, the Weierstrass $\wp$-function and the Eisenstein series G_4, G_6 satisfy the following differential equation:

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6, \text{ for all } z \in \mathbb{C}/\Lambda.$$

Now we can associate to a lattice $\Lambda \subset \mathbb{C}$ an elliptic curve $E/\mathbb{C}$.

Theorem 2.1. *Given a lattice $\Lambda \subset \mathbb{C}$, let $E/\mathbb{C}$ be the curve*

$$E : y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda).$$

Then E is an elliptic curve and the map

$$\begin{aligned} \phi : \mathbb{C}/\Lambda &\to E(\mathbb{C}) \\ z &\mapsto (\wp(z), \wp'(z)) \end{aligned}$$

is a complex analytic isomorphism of complex Lie groups.

§2.1.3 Associate a lattice to an elliptic curve

By using Weierstrass $\wp$-function, we could associate a lattice $\Lambda \subset \mathbb{C}$ with an elliptic curve $E/\mathbb{C}$. Moreover, the points $E(\mathbb{C})$ are identified with $\mathbb{C}/\Lambda$ with addition being the group law induced from $\mathbb{C}$. Next we will show every elliptic curve $E/\mathbb{C}$ arises from this way. Thus, this identification gives us a way to concretely visualise the torsion points on E.

Let $E/\mathbb{C}$ be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + Ax + B$. From the last lecture, we see that dx/y is a holomorphic differential on E which is invariant under translation. Let α, β be closed paths on $E(\mathbb{C})$ giving a basis for the singular homology group $H_1(E(\mathbb{C}), \mathbb{Z})$. Then the periods

$$\omega := \int_\alpha \frac{dx}{y}, \quad \omega' := \int_\beta \frac{dx}{y}$$

are $\mathbb{R}$-linearly independent and generate a lattice $\Lambda \subset \mathbb{C}$. Moreover, the map

$$F : E(\mathbb{C}) \to \mathbb{C}/\Lambda, \quad F(P) = \int_O^P \frac{dx}{y} \mod A$$

is a complex analytic isomorphism of complex Lie groups.

§2.2 CM elliptic curves over $\mathbb{C}$

§2.2.1 From a proper fractional ideal to a CM elliptic curve

Recall from the previous lecture that for an elliptic curve $E/\mathbb{C}$, the endomorphism ring $\mathrm{End}(E)$ is either isomorphic to $\mathbb{Z}$ or an order in an imaginary quadratic field K. We will now discuss the structure of orders in imaginary quadratic fields and their proper fractional ideals. This will allow us to construct CM elliptic curves by constructing their corresponding lattices.

Definition 2.4. *An order $\mathcal{O}$ of an imaginary quadratic field K is a subring of K such that $\mathcal{O}$ is a rank 2 free $\mathbb{Z}$-module.*

Let $\mathcal{O}_K$ be the ring of integers of K. For any order $\mathcal{O} \subset K$, we have $\mathcal{O} \subset \mathcal{O}_K$ with finite index and K is the field of fractions of $\mathcal{O}$. The ring $\mathcal{O}_K$ is referred to as the maximal order of K.

A *fractional* ideal of $\mathcal{O}$ is a subset of K which is a nonzero finitely generated $\mathcal{O}$-module. It is of the form αa for some $\alpha \in K^\times$ and a an $\mathcal{O}$-ideal. Moreover, a nonzero fractional Q-ideal is a free $\mathbb{Z}$-module of rank 2.

Thus under an embedding $K \hookrightarrow \mathbb{C}$, the image of a fractional $\mathcal{O}$-ideal α is a lattice $\Lambda_\alpha \in \mathbb{C}$ such that $\alpha\Lambda_\alpha \subset \Lambda_\alpha$ for any $\alpha \in \mathcal{O}$. From the previous discussion, it corresponds to an elliptic curve E with $\mathcal{O} \subset \mathrm{End}(E)$. Next we discuss for which fractional $\mathcal{O}$-ideals we exactly have $\mathcal{O} = \mathrm{End}(E)$.

Definition 2.5. *1. A fractional $\mathcal{O}$-ideal a is called* proper *if $\mathcal{O} = \{\alpha \in K : \alpha a \subset a\}$.*

2. A fractional $\mathcal{O}$-ideal a is called invertible *if there exists a fractional $\mathcal{O}$-ideal b such that $ab = \mathcal{O}$.*

Let $\mathcal{O}$ be an order of an imaginary quadratic field K. Then a fractional $\mathcal{O}$-ideal a is proper if and only if a is invertible. Moreover, for the maximal order of an imaginary quadratic field K, every fractional $\mathcal{O}_K$-ideal is proper. The set of all proper fractional $\mathcal{O}$-ideals which we denote by $I(\mathcal{O})$ forms a group under multiplication.

By definition, the lattice of a proper fractional $\mathcal{O}$-ideal in $\mathbb{C}$ gives rise to an elliptic curve E such that $\mathcal{O} = \mathrm{End}(E)$. We will discuss later that every elliptic curve arises from this way. As we want to classify all elliptic curves up to isomorphism, lattices up to homothety, we discuss this equivalence relation among proper fractional $\mathcal{O}$-ideals.

A fractional $\mathcal{O}$-ideal a is called *principal* if it is of the form $\alpha\mathcal{O}$ for some $\alpha \in K^\times$. Principal fractional ideals are proper and invertible. They form a subgroup of $I(\mathcal{O})$ which we denote by $P(\mathcal{O})$. Let a, b be proper fractional $\mathcal{O}$-ideals, under an embedding $K \hookrightarrow \mathbb{C}$, the lattices Λ_a, Λ_b are homothetic if and only if ab^{-1} is a principal fractional $\mathcal{O}$-ideal. So naturally, we consider the quotient group $C(\mathcal{O}) \coloneqq I(\mathcal{O})/P(\mathcal{O})$ which is a finite group called the *ideal class group* of $\mathcal{O}$ and its order $h(\mathcal{O})$ is referred to as the class number of $\mathcal{O}$. We will see that the ideal class group $C(\mathcal{O})$ parameterises isomorphism classes of elliptic curves with endomorphism ring $\mathcal{O}$.

§2.2.2 From a CM elliptic curve to a proper fractional ideal

We have seen that a proper fractional ideal of an order in an imaginary quadratic gives rise to a CM elliptic curve. Now we will show that every CM elliptic curve arises from this way. Given a lattice $\Lambda \subset \mathbb{C}$, the endomorphisms of $\mathbb{C}/\Lambda$ is the set $\{\phi_a : a \in \mathbb{C}, a\Lambda \subset \Lambda\}$. A lattice Λ corresponds to a CM elliptic curve if there exists $\alpha \in \mathbb{C} \setminus \mathbb{Z}$, such that $\alpha\Lambda \subset \Lambda$. We say that such a lattice has complex multiplication (CM).

Theorem 2.2. *A lattice Λ has CM if and only if it is homothetic to a lattice of a proper fractional ideal of an order $\mathcal{O}$ in an imaginary quadratic field K.*

Proof. By definition, the lattice of a proper fractional $\mathcal{O}$-ideal under an embedding $\mathcal{O} \hookrightarrow \mathbb{C}$ has its endomorphism ring being $\mathcal{O}$, thus it has CM. So we focus on proving the converse. For any lattice $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, we can find a homothetic lattice $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ for some $\tau \in \mathbb{C}$. So for an $\alpha \in \mathrm{End}(\Lambda)$, we have $\alpha = a + b\tau$ and $\alpha\tau = c + d\tau$ for some $a, b, c, d \in \mathbb{Z}$. Thus τ safisfies a quadratic equation

$$(a + b\tau)\tau = c + d\tau.$$

Since $\{1, \tau\}$ generates a lattice, we know that τ is not real. Thus the field $K = \mathbb{Q}(\tau)$ is imaginary quadratic. Moreover

$$\mathcal{O} \coloneqq \{\beta \in K : \beta\Lambda \subset \Lambda\}$$

is an order of K for which Λ is the lattice of a proper fractional $\mathcal{O}$-ideal. $\square$

§3 Lecture 03—Modular Curve $X(1)$ and the j-invariant

§3.1 Modular functions and uniformisation

In the last lecture, we discussed that isomorphism classes of elliptic curves defined over the complex numbers correspond to lattices $\Lambda \subset \mathbb{C}$ up to homothety. Thus, we can parameterise isomorphism classes of elliptic curves over $\mathbb{C}$ by parameterising lattices up to homothety. For any lattice $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, we can find a homothetic lattice $\Lambda_r = \mathbb{Z} + \mathbb{Z}\tau$ for some $\tau \in \mathbb{C}$ satisfying $\tau > 0$. Thus there is a surjective map from the upper half plane

$$\mathbb{H} = \{\tau \in \mathbb{C} : \mathrm{Im}\tau > 0\}$$

to the set of homothety classes of lattices given by $\tau \mapsto \Lambda_\tau \coloneqq \mathbb{Z} + \mathbb{Z}\tau$. But the choice from Λ to such a τ is not unique.

The modular group

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ s.t. } a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

acts on $\mathbb{H}$ by linear fractional transformations

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \quad \gamma(\tau) = \frac{a\tau + b}{c\tau + d} \text{ for all } \tau \in \mathbb{H}.$$

For any $\tau_1, \tau_2 \in \mathbb{H}$, the lattices Λ_{τ_1} and Λ_{τ_2} are homothetic if and only if there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma(\tau_1) = \tau_2$. Thus lattices up to homothety are parameterised by the upper half plane $\mathbb{H}$ modulo the action of $\mathrm{SL}_2(\mathbb{Z})$. And this set $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H}$ is in bijection to the region

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

This region is called the *fundamental domain* for $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H}$ and every lattice $\Lambda \subset \mathbb{C}$ is homothetic to a unique lattice Λ_τ for some $\tau \in \mathcal{F}$. The quotient $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H}$ (denoted by $Y(1)$) has a natural

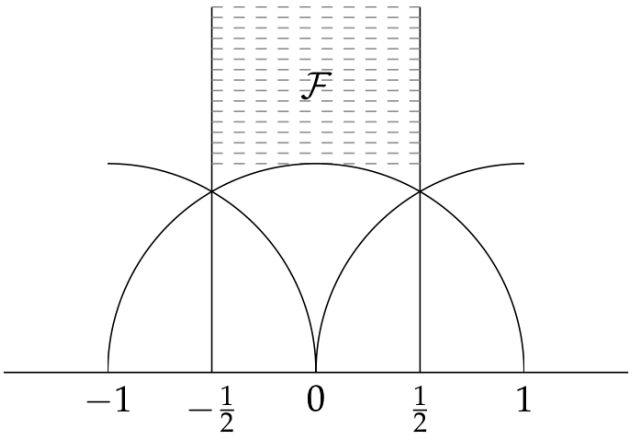

Figure 3.1: The fundamental domain $\mathcal{F}$

structure of a genus 0 Riemann surface puncture, a 2-sphere with one point missing. Then it is

natural to want to compactify this topological space. To add this missing point and give it a moduli interpretation, we define the extended upper half plane

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

Then $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}^*$ by linear fractional transformations and the quotient group $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H}^*$ (denoted as $X(1)$) is a compact Riemann surface of genus 0 with 3 punctures. There is one point in the complement of $Y(1) \subset X(1)$ and this point is called the *cusp* of $X(1)$.

Next, we introduce a function j on homothety classes of lattices which is a complex analytic isomorphism of (open) Riemann surfaces $j : Y(1) \to \mathbb{C}$ extending to $j : X(1) \simeq \mathbb{P}^1(\mathbb{C})$. Recall from Lecture 2 that given a lattice Λ and $k \in \mathbb{Z}_{>1}$, the Eisenstein series of weight $2k$ is given by

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^{2k}}.$$

Given $\tau \in \mathbb{H}$, it is naturally associated to the lattice $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$, and thus we can consider the Eisenstein series $G_{2k}(\tau)$ as a meromorphic function defined on the upper half plane $\mathbb{H}$. Moreover, note that for any

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

we have

$$G_{2k}(\gamma\tau) = (c\tau + d)^{2k} G_{2k}(\tau).$$

Meromorphic functions on $\mathbb{H}$ satisfying this condition are called weakly modular of weight $2k$. The Eisenstein series G_{2k}, $k > 1$ is not only weakly modular, but also holomorphic on $\mathbb{H}$ and at ∞. It is an example of a modular form of weight $2k$.

More to the point, the function G_{2k} is defined on the set of lattices but it is not a function on homothety classes of lattices. However, we can construct a function on homothety classes of lattices using G_{2k}.

Definition 3.1. *Let $\mathbb{Z} + \mathbb{Z}\tau$ be a lattice in $\mathbb{C}$. The j-invariant is defined to be the complex number*

$$j(\tau) \coloneqq 1728 \cdot \frac{(60G_4(\tau))^3}{(60G_4(\tau))^3 - 27\,(140G_6(\tau))^2}.$$

For any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, we have that $j(\gamma\tau) = j(\tau)$.

Theorem 3.1. *If $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ are two lattices, then they are homothetic if and only if $j(\Lambda_1) = j(\Lambda_2)$.*

Since

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

the function $j : \mathbb{H} \to \mathbb{C}$ satisfies $j(\tau + 1) = j(\tau)$. Thus, let $q = e^{2\pi i \tau}$, then $j(\tau)$ has a Laurent expansion in the variable q. Explicitly, we have

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots = \sum_{n=0}^{\infty} c_n q^n,$$

where the coefficients c_n are integers for all $n \geq 0$.

§3.2 The j-invariant of an elliptic curve

From the discussion in Lecture 2, a lattice $\Lambda \subset \mathbb{C}$ corresponds to an elliptic curve E defined by a Weierstrass equation

$$y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda).$$

Following the definition of the j-invariant for a lattice Λ, given an elliptic curve E over some field K with Weierstrass equation $y^2 = x^3 + Ax + B$, we define the j-invariant of E to be

$$j(E) \coloneqq 1728 \cdot \frac{(4A)^3}{16(4A^3 + 27B^2)}.$$

When K is a subfield of $\mathbb{C}$, our discussion implies that the j-invariant determines the isomorphism class of E over $\mathbb{C}$. Although we will not prove this, it is true that the j-invariant determines the isomorphism class of E over $\overline{K}$ for any field K.

From the definition, we can see that for E defined over any field K (thus $A, B \in K$), its j-invariant takes value in K. Conversely, given a j-invariant $j_0 \in K$, for some field K, the elliptic curve

$$y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

has its j-invariant equal to j_0 unless $j_0 = 0, 1728$. Values 0 and 1728 are j-invariants of singular elliptic curves $y^2 + y = x^3$ and $y^2 = x^3 + x$ respectively. Thus, over an algebraic closed field $\overline{K}$, the set of isomorphism classes of elliptic curves in bijection to the set of all j values in $\overline{K}$.

Note that the cusp of $X(1)$ corresponds to the j-invariant $j = \infty$. Thus, let p be a prime of a field K and E/K an elliptic curve, if the valuatuion of the j-invariant is negative at p ("having a power of p in the denominator of $j(E)$"), then the reduction of E modulo p is singular. and we call this reduction a bad reduction. If the valuation of the j-invariant is non-negative at p, then E has potential good reduction at p, meaning that there is a finite extension L/K such that $E \otimes \mathrm{Spec}(L)$ has good reduction at a prime above p.

Moreover, let E_1, E_2 be two elliptic curves defined over a number field K and let p be a prime of K at which E_1, E_2 admit good reduction. For each E_i there exists a Weierstrass equation $y^2 = x^3 + A_i x + B_i$ such that $y^2 = x^3 + \overline{A_i}x + \overline{B_i}$ with $\overline{A_i}, \overline{B_i} \in \mathbb{F}_p$ the reduction of A, B in the residue field of p and defines an elliptic curve $\mathscr{E}_i$ over $\mathbb{F}_p$. Then the j-invariants $j(E_1) \equiv j(E_2)$ mod p if and only if $\mathscr{E}_1$ and $\mathscr{E}_2$ are isomorphic over $\overline{\mathbb{F}_p}$.

§3.3 The j-invariant of a CM elliptic curve

Recall from Lecture 2, a lattice $\Lambda = \mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{C}$ corresponds to a CM elliptic curve when τ is an imaginary quadratic number. Now we discuss the j-invariant of a CM elliptic curve, which is often called a singular modulus.

Proposition 3.2. *The j-invariant of a CM elliptic curve E is an algebraic number*

Proof. Let $E/\mathbb{C} : y^2 = x^3 + Ax + B$ be an elliptic curve and $\phi \in \mathrm{End}(E)$ be a non-zero endomorphism. For any $\sigma \in \mathrm{Aut}(\mathbb{C})$, let E^σ be the elliptic curve with Weierstrass equation $y^2 =$

$x^3+\sigma(A)x+\sigma(B)$. Then $\sigma\circ\phi\circ\sigma^{-1}\in\mathrm{End}(E^\sigma)$ and therefore if E has CM by an order $\mathcal{O}$, so does E^σ.

The isomorphism classes of E and E^σ are determined by their j-invariants and $j(E^\sigma)=\sigma(j(E))$ following the definition of the j-invariant. Recall from Lecture 2 that the isomorphism classes of elliptic curves with CM by $\mathcal{O}$ are parameterised by the class group of $\mathcal{O}$ which is a finite group. We conclude that $j(E)$ is algebraic. □

Let h be the class number of an order $\mathcal{O}$ of an imaginary quadratic field K. From the above proof, we can see that $\mathbb{Q}(j(E))$ is a number field of degree at most h where E is an elliptic curve with CM by $\mathcal{O}$. In fact, $|\mathbb{Q}(j(E))|:\mathbb{Q}|=h$.

Theorem 3.2. *The j-invariant of a CM elliptic curve E is an algebraic integer. Thus, a CM elliptic curve has potentially good reduction at all primes.*

Proof sketch. First recall the degree of the multiplication by m isogeny is m^2 for any positive integer m. Let $\alpha\in\mathcal{O}\subset\mathbb{C}$ be an endomorphism of an elliptic curve E. Then the degree of $\alpha:E\to E$ is its norm, or simply $\overline{\alpha}\alpha$ where $\overline{\alpha}$ is the complex conjugate of α. Thus, an elliptic curve having CM by an order $\mathcal{O}\subset\mathbb{Q}(\sqrt{-d})$ can be characterised by the existence of an endomorphism whose degree m is not a perfect square.

Consider a lattice $\Lambda_\tau=\mathbb{Z}+\mathbb{Z}\tau$, the elliptic curve $\mathbb{C}/\Lambda_\tau$ admits a degree m isogeny to $\mathbb{C}/\Lambda_{m\tau}$ by $z\mapsto mz$. Using the existence of dual isogeny, admitting a degree m isogeny to or from $\mathbb{C}/\Lambda_\tau$ are equivalent. In fact, all lattices Λ for which $\mathbb{C}/\Lambda$ admits a degree m isogeny to $\mathbb{C}/\Lambda_\tau$ takes the form $\mathbb{Z}+\mathbb{Z}(m\gamma\tau)$ for some $\gamma\in\mathrm{SL}_2(\mathbb{Z})$. Up to homothety, there are finitely many homothety classes of such lattices Λ for which $\mathbb{C}/\Lambda$ admits a degree m isogeny to $\mathbb{C}/\Lambda_\tau$ for a fixed Λ_τ. We list a representative of this set of $m\gamma\tau$ as $\tau_1,\tau_2,\ldots,\tau_r$.

Now we can define a polynomial in variable x in the following way:

$$\Phi_m(X,\tau)\coloneqq\prod_{i=1}^{n}(X-j(\tau_i)).$$

This theorem follows from the following facts about the polynomial $\Phi_m(X,\tau)$. The proof of these statements all base on the q-expansion of the j-function. If

$$j(\tau)=\frac{p}{q}+\sum_{n=0}^{\infty}c_nq^n,$$

then we have that

$$j(m\gamma\tau)=\frac{\zeta_m^{-ab}}{\left(q^{1/m}\right)^{a^2}}+\sum_{n=0}^{\infty}c_n\zeta_m^{abn}\left(q^{1/m}\right)^{a^2n},\ \text{in which we take } m\gamma=\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}.$$

Now, consider:

- If we vary τ, the coefficients of $\Phi_m(X,\tau)$ varies in the following way: $\Phi_m(X,\tau)\in\mathbb{C}(j(\tau))[X]$. This follows from the coefficients of Φ_m as symmetric polynomials of $j(m\gamma\tau)$ are holomorphic Functions on $\tau\in\mathcal{H}$ and invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$. These coefficients are meromorphic at the cusps, thus are modular functions (weakly modular and meromorphic at ∞). All holomorphic modular functions of $\mathrm{SL}_2(\mathbb{Z})$ are polynomials of $j(\tau)$.

- Consider $\Phi_m(X, \tau)$ as a polynomial with two variables $\Phi_m(X, Y) \in \mathbb{C}[X, Y]$ by setting $Y = j(\tau)$. Then, in fact $\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$.
  Using the explicit Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $j(m\gamma\tau)$ using the q-expansion, we can conclude that $\Phi_m(X, Y) \in \mathbb{Q}[X, Y]$. Since the coefficients of the q-expansions of $j(m\gamma\tau)$ are algebraic integers, we conclude that $\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$.
- When m is not a perfect square, $\Phi_m(X, X)$ is an integral polynomial of X with leading coefficients ± 1.
  This again follows from the explicit q-expansion of $j(m\gamma\tau)$, where $m\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. Note that we need $m = ad$ to not be a perfect square in this argument.

The proof is then completed by noting that $\Phi_m(X, X)$ is a polynomial of X with leading coefficient ± 1 and $j(E)$ is a root of $\Phi_m(X, X)$ for any elliptic curve E with CM by $\mathcal{O}$. $\square$

§4 Lecture 04—Modular Curves and the CM points on Modular Curves

In our last three lectures, we introduced the notion of a CM elliptic curve, an explicit description of a CM elliptic curve defined over the complex numbers (lattice $\mathbb{Z}+\mathbb{Z}\tau \in \mathbb{C}$, where τ is an imaginary quadratic number), and some properties of CM elliptic curves (they are defined over number fields and they have everywhere potentially good reduction).

In this lecture, we introduce some central problems in modern arithmetic geometry where CM elliptic curves played a critical role in the study of.

§4.1 Rational points on algebraic curves

One origin of number theory and arithmetic geometry is the study of Diophantine problems, namely the study of integral solutions to polynomial equations. Integral roots of polynomials correspond to rational points on an algebraic variety, and the starting point of this problem is to study the set of K-points on an algebraic curve defined over some non-algebraically closed field K.

The most famous example of this problem is the Fermat's last theorem, in which it states that the only integral solutions to $x^n + y^n = z^n$ for $n \geq 3$ are the trivial solutions satisfying $xyz = 0$. The proof of this theorem relies on the study of elliptic curves and modular curves which we will define today. To talk about rational points on algebraic curves, we start with the set of rational points on an elliptic curve defined over $\mathbb{Q}$.

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over $\mathbb{Q}$ and we want to study the set of points $(x, y) \in E(\mathbb{Q})$. From the group law on E, we know that the set of rational points $E(\mathbb{Q})$ is a finitely generated abelian group.

Theorem 4.1 (Mordell-Weil theorem)**.** *Let $E \setminus \mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is a finitely generated abelian group.*

By the fundamental theorem of finitely generated abelian groups, the group $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E_{\text{tors}}(\mathbb{Q})$ where r is a non-negative integer called the rank of E and $E_{\text{tors}}(\mathbb{Q})$ is a finite abelian group called the torsion subgroup of E. We have a relatively good understanding of the group $E_{\text{tors}}(\mathbb{Q})$ thanks to the following theorem of Mazur.

Theorem 4.2 (Mazur)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ of $E(\mathbb{Q})$ is isomorphic to one of the following fifteen groups:*

$$\mathbb{Z}/n\mathbb{Z}, \quad n = 1, 2, \ldots, 10, 12.$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, \quad n = 1, 2, 3, 4.$$

Further, each of these groups occurs as $E_{\text{tors}}(\mathbb{Q})$ for some elliptic curve $E/\mathbb{Q}$.

But the rank of an elliptic curve is much more mysterious. We don't know whether the rank for the set of elliptic curves defined over $\mathbb{Q}$ is bounded and we don't have an algorithm which guarantees to compute the rank of an arbitrary elliptic curve $E/\mathbb{Q}$.

The most important conjecture regarding the rank of an elliptic curve is the Birch and Swinnerton-Dyer conjecture which predicts that the rank of $E(\mathbb{Q})$ is determined by the L-function of E which contains the information of the number of points on the reductions of E at all primes. This conjecture is wide open, especially for E without complex multiplication. One topic we will discuss today us a method to construct rational points (called *Heegner points*) on an elliptic curve using the theory of complex multiplication. These points were used in the work of Gross-Zagier and Kolyvagin to prove some cases of the BSD conjecture.

§4.2 Congruence subgroups and modular curves

Let N be a positive integer. Consider the reduction homomorphism

$$r_N : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

This map is in fact surjective with kernel the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of matrices congruent to the identity modulo N, referred to as the *principal congruence subgroup* of level N and denoted by $\Gamma(N)$:

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Definition 4.1. *A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a* congruence subgroup *if it contains $\Gamma(N)$ for some $N \in \mathbb{Z}_{>0}$, in which case Γ is called a congruence subgroup of level N.*

Besides the principal congruence subgroups, the most important congruence subgroups are

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

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Note that $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$.

Definition 4.2. *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. The modular curve $Y(\Gamma)$ is the quotient $\Gamma \backslash \mathbb{H}$ and the modular curve $X(\Gamma)$ is its compactification of $X(\Gamma) = \Gamma \backslash \mathbb{H}^*$. The orbits of the points $\mathbb{Q} \cup \{\infty\}$ under the Γ-action are called the cusps of $X(\Gamma)$.*

The modular curves $X(\Gamma)$ are compact Riemann surfaces. Moreover, for Γ being $\Gamma(N)$, $\Gamma_0(N)$ or $\Gamma_1(N)$, the modular curves $Y(\Gamma(N))$ (denoted as $Y(N)$), $Y(\Gamma_0(N))$ (denoted as $Y_0(N)$) and $Y(\Gamma_1(N))$ (denoted as $Y_1(N)$) all have modular interpretations. Here we discuss the case of $Y_0(N)$ as an example.

Consider the pair (E, C) where E is an elliptic curve over $\mathbb{C}$ and C is a cyclic subgroup of E of order N. The set of $\mathbb{C}$-points on $Y_0(N)$ are in bijection with the set of isomorphism classes of pairs (E, C) up to equivalence condition $(E_1, C_1) \sim (E_2, C_2)$ where there exists an isomorphism $\phi : E_1 \to E_2$ such that $\phi(C_1) = C_2$. Equivalently, a $\mathbb{C}$-point on $Y_0(N)$ corresponds to a pair of elliptic curves

(E, E') together with a degree N isogeny $\phi : E \to E'$. To each $\tau \in \mathbb{H}$, this pair of elliptic curves is $(\mathbb{C} \setminus (\mathbb{Z} + \mathbb{Z}\tau), \mathbb{C}/(\mathbb{Z} + \mathbb{Z}N\tau))$ and the isogeny is given by $z \mapsto Nz$.

The modular curve $X(1)$ has a model over $\mathbb{Q}$, i.e. $\mathbb{P}^1_{\mathbb{Q}}$ and its function field is $\mathbb{Q}(j)$. The curve $X_0(N)$ also has a model over $\mathbb{Q}$, meaning that there exists an irreducible polynomial $f(x) \in \mathbb{Q}(j)[x]$ such that the curve $X \setminus \mathbb{Q}$ whose function field is isomorphic to $\mathbb{Q}(j)[x]/(f(x))$ satisfies $X \otimes \mathrm{Spec}\mathbb{C} \simeq X_0(N)$. In fact, this polynomial $f(x)$ is exactly the polynomial $\Phi_N(x, \tau) \in \mathbb{Q}(j(\tau))[x]$ from Lecture 3.

Theorem 4.3 (Modularity theorem, Wiles, Taylor-Wiles, Breuil-Conrad-Diamond-Taylor)**.** *Let E be an elliptic curve with $j(E) \in \mathbb{Q}$. Then for some positive integer N there exists a surjective morphism over $\mathbb{Q}$ from the modular curve $X_0(N)/\mathbb{Q}$ to the elliptic curve E,*

$$X_0(N) \to E.$$

The modularity theorem was first conjectured by Shimura-Taniyama-Weil and it was the key ingredient in the proof of Fermat's last theorem by Wiles. The proof of the modularity theorem is a long story and we will not discuss it in this course.

§4.3 Rational points on modular curves and CM elliptic curves

Let E be an elliptic curve defined over a field K. For any positive integer m which is coprime to the characteristic of K, let $E[m]$ denote the group of m-torsion points on E,

$$E[m] = \{P \in E(\overline{K}) : mP = O\}, \qquad \text{and recall } E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2.$$

Then $E[m]$ is a scheme defined over K and the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on $E[m]$ by acting on the $\overline{K}$-points of E. This action gives a Galois representation

$$\phi_m : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

If an elliptic curve E/K has an order N cyclic subgroup $C \in E[N]$ fixed by the $\mathrm{Gal}(\overline{K}/K)$ action, then the pair (E, C) gives rise to a K-point on $X_0(N)$. If further the action of $\mathrm{Gal}(\overline{K}/K)$ restricts on C is the trivial action, then it gives rise to a K-point on $X_1(N)$. A $\mathbb{C}$-point on Y_1 corresponds to a pair (E, P) where $E/\mathbb{C}$ is an elliptic curve and $P \in E(\mathbb{C})$ is a point of order N on E. A major part of Mazur's theorem on the structure of the torsion subgroup $E_{\mathrm{tors}}(\mathbb{Q})$ is to prove the non-existence of $\mathbb{Q}$-points on $X_1(N)$ which are not cusps for $N \geq 13$.

We can use CM elliptic curves to construct points on modular curves whose defining field is of low degree over $\mathbb{Q}$. Let $\alpha : E \to E$ be an endomorphism of E defined over K. Then the map $\alpha : E[m] \to E[m]$ commutes with the $\mathrm{Gal}(\overline{K}/K)$ action. This forces the image of ϕ_m to be an abelian subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ when E is a CM elliptic curve with all of its endomorphisms defined over K. This image is much smaller tha the typical behaviour of a non-CM elliptic curve defined over a number field K.

Theorem 4.4 (Serre)**.** *Let K be a number field and let E/K be an elliptic curve without complex multiplication.*

1. *$\phi_{\ell^\infty}(\mathrm{Gal}(\overline{K}/K))$ is of finite index in $\mathrm{Aut}(E[\ell^\infty])$ for all primes ℓ;*

2. $\phi_{\ell^\infty}(\mathrm{Gal}(\overline{K}/K)) = \mathrm{Aut}(E[\ell^\infty])$ *for all but finitely many primes* ℓ.

Thus the m-torsion points of a CM elliptic curve E/K is defined over number field L with relatively low degree over K. Using this fact, we deduce that CM elliptic curves give rise to points on modular curves whose defining field is of relatively low degree. Moreover, we can use CM elliptic curves to construct explicit points on modular curves for which we can analyse their defining fields.

§4.4 Heegner points

The set of Heegner points on $Y_0(N)(\mathbb{C})$ are points corresponding to a pair of elliptic curves (E, E') such that $\mathrm{End}(E) \simeq \mathrm{End}(E') \simeq \mathcal{O}$ where $\mathcal{O}$ is an order in an imaginary quadratic field K.

Given an order $\mathcal{O} \subset \mathbb{Q}(\sqrt{-d})$ where d is the discriminant of the field $K = \mathbb{Q}(\sqrt{d})$. Let c be the index of $\mathcal{O}$ in $\mathcal{O}_K$ and then $D = dc^2$ is the discriminant of $\mathcal{O}$. The order $\mathcal{O}$ is determined by its discriminant. Given a positive integer N, if the equation $D = B^2 - 4NC$ has integer solutions $B, C \in \mathbb{Z}$ satisfying $\gcd(B, C, N) = 1$, then there exists proper fractional $\mathcal{O}$-ideals α, β such that under an embedding $K \hookrightarrow \mathbb{C}$, the images of α and β are lattices with a cyclic degree N isogeny between their corresponding elliptic curves.

For fixed $\mathcal{O}$ and N, the set of Heegner points is fixed under the action of $\mathrm{Aut}(\mathbb{C})$. They are algebraic points defined over some $K(j(\tau))$ where $j(\tau)$ is the j-invariant of an elliptic curve with CM by $\mathcal{O}$. Recall from the modularity theorem that given an elliptic curve $E/\mathbb{Q}$, there exists $X_0(N)$ which admits a surjective map $\pi : X_0(N) \to E$ over $\mathbb{Q}$. Thus, for an order $\mathcal{O}$ such that we can construct Heegner points $P_1, \ldots, P_{h(\mathcal{O})}$ on $X_0(N)$, we can consider the point $P = \pi(P_1) + \ldots + \pi\left(P_{h(\mathcal{O})}\right)$ on E which is defined over K. The work of Gross-Zagier related the height of P with the value of the L-function $L(E, 1)$, thus giving a method to construct a rational point of infinite order for elliptic curves whose L-function satisfies certain conditions.

§5 Lecture 05—Arithmetic of CM Elliptic Curves

I In Lecture 2, we explicitly constructed CM elliptic curves defined over the complex numbers. In Lecture 3, using the j-invariant, we showed CM elliptic curves are defined over number fields. Today, we will further discuss the fields over which CM elliptic curves are defined and where isogenies among them are defined.

§5.1 Galois action on elliptic curves

Let E be an elliptic curve defined over a number field K. Recall that this means that there exist $A, B \in K$ such that the elliptic curve E is defined by Weierstrass equation $y^2 = x^3 + Ax + B$. The absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on the set of $\overline{K}$-points of E by acting on the coordinates of the points. For any $\sigma \in \mathrm{Gal}(\overline{K}/K)$, $P = (x, y) \in E(\overline{K})$ is sent to $P^\sigma = (\sigma(x), \sigma(y)) \in E(\overline{K})$.

Let $\phi : E_1 \to E_2$ be an isogeny between elliptic curves E_1, E_2 defined over K. Recall a morphism ϕ is defined over K if for any $\sigma \in \mathrm{Gal}(\overline{K}/K)$, we have that $\phi(P^\sigma) = \phi(P)^\sigma$ for all $P \in E_1(\overline{K})$. Because an isogeny is determined by its kernel $\mathrm{Ker}(\phi) \subset E_1$, the field over which the isogeny is defined is the minimal field L such that for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$ and $P \in \mathrm{Ker}(\phi(\overline{\mathbb{Q}}))$, the point P^σ is also in $\mathrm{Ker}(\phi(\overline{\mathbb{Q}}))$. In particular, if $\mathrm{Ker}(\phi) = E_1[m]$ for some positive integer m, then the field over which ϕ is defined is $\mathbb{Q}(\zeta_m)$ where ζ_m is a primitive m-th root of unity.

Let $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then we can define an elliptic curve $E^\tau : y^2 = x^3 + \tau(A)x + \tau(B)$ and for any $P \in E(\overline{\mathbb{Q}})$, the point $P^\tau \in E^\tau(\overline{\mathbb{Q}})$. Another way to say an elliptic curve E is defined over K is that E is isomorphic to E^τ for any $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for some isomorphism defined over K. Note that the map $E \to E^\tau$ given by $P \mapsto P^\tau$ is not algebraic in most cases. In other words, in general, an elliptic curve defined over a number field is not isogenous to its Galois conjugates. But we saw in Problem Set 2 Problem 3 that CM elliptic curves are isogenous (over $\overline{\mathbb{Q}}$) to all of their Galois conjugates.

§5.2 Field of definition for $\mathrm{End}(E)$

Let E be an elliptic curve defined over a number field L. The endomorphism ring $\mathrm{End}_{\overline{L}}(E) \simeq \mathcal{O}$ where $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$ is an order in an imaginary quadratic field K. We want to know over which field these endomorphisms are defined.

Lemma 5.1. *Let F be the field over which the endomorphisms are defined. Then $K \subset F$.*

Proof. Recall the set of holomorphic differentials $H^0(E, \Omega)$ is a 1-dimensional vector space over $\mathbb{C}$. Let $\Lambda \in \mathbb{C}$ be a lattice such that $\mathbb{C}/\Lambda \simeq E(\mathbb{C})$ with $z \in \mathbb{C}$ corresponding to a point $P_z \in E(\mathbb{C})$ and let $\iota : L \hookrightarrow \mathbb{C}$ be the embedding such that $\iota(\alpha)z = \alpha(P_z)$. Then the induced action α^* on $H^0(E, \Omega)$ is multiplication by α. Thus, if the endomorphism α commutes with Galois actions in $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$, then $\alpha \in F$. □

The embedding $\iota : K \hookrightarrow \mathbb{C}$ in the proof of Lemma 5.1 is part of the CM data. To precisely describe the CM action, one must give $\mathcal{O}$ together with ι and this notion will be generalised to the notion CM type in the case of higher dimensional abelian varieties with complex multiplication.

Proposition 5.2. *Let E be an elliptic curve defined over a number field L. The endomorphism ring $\mathrm{End}_{\overline{L}}(E) \simeq \mathcal{O}$ where $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$ is an order in an imaginary quadratic field K. Then for any $\alpha \in \mathcal{O}$, the endomorphism α is defined over the composition LK.*

Proof. From the proof of Lemma 5.1, there is an embedding $\iota : K \hookrightarrow \mathbb{C}$ such that the action of $\alpha \in \mathcal{O}$ on $V = H^0(E, \Omega)$ is multiplication by $\iota(\alpha)$. Recall from Lecture 1, since our discussion is over fields of characteristic 0, the map $\mathrm{End}_{\overline{L}}(K) \to \mathrm{End}(V)$ is injective. For any $\sigma \in \mathrm{Gal}(\overline{Q}/LK)$, since it fixes α^*, it also fixes α. We conclude the statement. □

§5.3 Field of definition for CM elliptic curves

We will restrict our discussion to the case of elliptic curves with CM by a maximal order. Let E be an elliptic curve defined over a number field L such that $\mathrm{End}_{\overline{L}}(E) \simeq \mathcal{O}_K$ where $\mathcal{O}_K$ is the ring of integers of an imaginary quadratic field K. We will discuss the field $K(j(E))$. Let's first state the conclusion and instead of discussing the proof, we will discuss the statement and its implications.

Theorem 5.1. *The field $K(j(E))$ is the Hilbert class field of K.*

The *Hilbert class field* L of a number field K is the maximal unramified abelian extension of K. It is a Galois extension of K with Galois group $\mathrm{Gal}(L/K)$ isomorphic to the ideal class group $\mathrm{C}(K)$ (the group of fractional $\mathcal{O}_K$-ideals modulo the subgroup of principal fractional ideals) of K. The principal ideal theorem gives an interesting property of the Hilbert class field, namely for any ideal $I \subset \mathcal{O}_K$, its extension $I\mathcal{O}_L \subset \mathcal{O}_L$ is a principal ideal.

For a number field K, the set of field extensions L/K are determined by the set of primes of K which splits completely in the extension. The Hilbert class field L is exactly the field extension L/K over which the set of split primes are all the principal ideals of K.

Recall the isomorphism classes of elliptic curves with CM by $\mathcal{O}_K$ are in bijection to lattices in $\mathbb{C}$ which are obtained from embeddings of fractional $\mathcal{O}_K$-ideals into $\mathbb{C}$ up to homothety. Let $\alpha \subset K$ be a fractional $\mathcal{O}$-ideal and under an embedding $K \subset \mathcal{C}$ we make the following identification:

$$\boxed{\text{fractional } \mathcal{O}_K\text{-ideal } \mathfrak{a}} \iff \boxed{\text{lattice } \Lambda_{\mathfrak{a}}} \iff \boxed{\text{CM elliptic curve } E_{\mathfrak{a}}}.$$

This gives a bijection between the set of these isomorphism classes of elliptic curves $\mathcal{S}$ with $\mathcal{C}(K)$ and thus $\mathcal{C}(K)$ acts on $\mathcal{S}$. Let L be the Hilbert class field of K, then there is a canonical isomorphism $\phi : \mathrm{Gal}(L/K) \to \mathcal{C}(K)$. This gives a $\mathrm{Gal}(\overline{K}/K)$ action on $\mathcal{S}$ and the theorem was proved by showing that this action can be identified with the natural Galois action on $\mathcal{S}$ as we now describe.

Since $\overline{K}$-isomorphism classes of elliptic curves are determined by their j-invariants, we can describe the relationship between these two actions in the following way:

$$(\phi^{-1}(\mathfrak{a}))(j(E_{\mathfrak{a}})) = j\left(E_{\mathfrak{a}^{-1}\mathfrak{b}}\right)$$

where the left hand side action is the Galois action on the algebraic number $j(E_{\mathfrak{b}}) \in \overline{K}$.

Since the right hand side action $\mathcal{C}(K)$ acting on $\mathcal{S}$ by $\mathfrak{a} : E_{\mathfrak{b}} \mapsto E_{\mathfrak{a}^{-1}\mathfrak{b}}$ is transitive, we conclude that the extension $K(j(E_{\mathfrak{a}}))/K$ is Galois with Galois group isomorphic to $\mathcal{C}(K)$. And the left

hand Galois action shows that $\mathrm{Gal}(\overline{K}/L)$ acts trivially on $j(E_{\mathfrak{a}})$ identifying the field extensions $K(j(E_{\mathfrak{a}}))/L$ and L/K.

In general, if E is an elliptic curve with CM by an order $\mathcal{O}$ of K, not necessarily the maximal order, then the field $K(j(E))$ is the ring class field of the order $\mathcal{O}$. This result is sometimes referred to as the **first main theorem of complex multiplication**.

The field extension $K(j(E))/K$ is abelian with Galois group $\mathrm{Gal}(K(j(E))/K) \simeq \mathcal{C}(\mathcal{O})$. Moreover, the field extension $K(j(E))/\mathbb{Q}$ is Galois and $\mathrm{Gal}(K(j(E))/\mathbb{Q}) \simeq \mathcal{C}(\mathcal{O}) \rtimes (\mathbb{Z}/2\mathbb{Z})$, a generalised dihedral group. In fact, if L/K is a finite abelian extension, then $L/\mathbb{Q}$ is a generalised dihedral extension if and only if $L \subset K(j(\mathcal{O}))$ for some order $\mathcal{O} \subset K$. So the first main theorem of complex multiplication helps us to describe abelian extensions of an imaginary quadratic field K which are generalised dihedral extensions of $\mathbb{Q}$. Next we will use CM elliptic curves to describe all abelian extensions of K.

§5.4 Torsion fields of CM elliptic curves

Let K be an imaginary quadratic field. To describe all abelian extensions of K, we will use the torsion points of a CM elliptic curve.

Theorem 5.2. *Let E be an elliptic curve with CM by $\mathcal{O}_K$ defined over the Hilbert class field H of K. Consider the map $h : E \to E/\mathrm{Aut}(E) \simeq \mathbb{P}^1$ defined over H. By picking a parameter for $\mathbb{P}^1_H$, we get a function $h : E(\overline{H}) \setminus \{O\} \to \overline{H}$. Such a function is called a Weber function for E/H.*

Let L/K be a finite abelian extension, then there exists an ideal defined by $\mathfrak{a} \subset \mathcal{O}_K$ such that $L \subset K(j(E), h(E[\mathfrak{a}]))$ where $E[\mathfrak{a}] = \{P \in E(\overline{H}) : \alpha P = O \text{ for all } \alpha \in \mathfrak{a}\}$.

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over H with CM by $\mathcal{O}_K$. If $j(E)$ is not equal to 0 or 1728, then its only nontrivial automorphism is $(x, y) \mapsto (x, -y)$ and thus the function $(x, y) \mapsto x$ is a Weber functon defined over H.

The theorem states that the maximal abelian extension of K is generated by the x-coordinates of all the torsion points of E. This is an implication of the second theorem of complex multiplication.

§6 Lecture 06—Reductions of CM Elliptic Curves

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over $\mathbb{Q}$. As we discussed, the endomorphism ring $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ is either isomorphic to $\mathbb{Z}$ or isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field K which is a free $\mathbb{Z}$-module of rank 2.

For all but finitely many primes p, the reduction of E at p is an elliptic curve $\mathcal{E}_p$ defined over $\mathbb{F}_p$. The endomorphism ring $\mathrm{End}_{\overline{\mathbb{F}}_p}(\mathcal{E}_p)$ is either isomorphic to an order of an imaginary quadratic field or isomorphic to an order of a quaternion algebra which is a free $\mathbb{Z}$-module of rank 4. Given a fixed curve $E/\mathbb{Q}$, we want to discuss the set of primes at which the reduction of E has a larger endomorphism ring than $\mathbb{Z}$.

§6.1 Endomorphism rings of elliptic curves over finite fields

Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_q$ defined by $y^2 = x^3 + ax + b$, $a, b \in \mathbb{F}_q$. Let p be the characteristic of $\mathbb{F}_q$. The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \simeq \hat{\mathbb{Z}}$ is topologically generated by a single element σ, often referred to as the Frobenius element. For $\alpha \in \overline{F}_p$, $\sigma(\alpha) = \alpha^p$. Recall the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ acts on the set of elliptic curves defined over $\overline{\mathbb{F}}_p$ with σ maps $\mathcal{E}$ to $\mathcal{E}^\sigma : y^2 = x^3 + a^p x + b^p$. Note that the map $\mathcal{E} \to \mathcal{E}^\sigma : (x, y) \mapsto (x^p, y^p)$ is an algebraic map (different from a Galois element in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ case), thus an isogeny.

Since $\mathcal{E}$ is defined over $\mathbb{F}_q$, it admits an endomorphism $\phi : (x, y) \mapsto (x^q, y^q)$, the q-th power Frobenius map. The map ϕ is purely inseparable of degree q. For simplicity, we can consider $\mathcal{E}$ defined over a prime field $\mathbb{F}_p$ with $p \neq 2$. Since the Frobenius morphism has degree p, we can see that the ring $\mathrm{End}_{\overline{\mathbb{F}}_p}(\mathcal{E})$ has an element with norm p. If $\mathrm{End}_{\overline{\mathbb{F}}_p}(\mathcal{E})$ is isomorphic to an order $\mathcal{O}$ of an imaginary quadratic field K, then p has to split in $K/\mathbb{Q}$. In this case, we say $\mathcal{E}$ is ordinary.

Definition 6.1. *A definite quaternion algebra B over $\mathbb{Q}$ is the $\mathbb{Q}$-algebra defined by*

$$B = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

with multiplication defined by

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2, \beta^2 < 0, \quad \beta\alpha = -\alpha\beta.$$

For any prime p, the $\mathbb{Q}_p$ algebra $B \otimes \mathbb{Q}_p$ s either still a division algebra or is isomorphic to the matrix algebra $M_2(\mathbb{Q}_p)$. If $B \otimes \mathbb{Q}_p \simeq M_2(\mathbb{Q}_p)$, then we say p is split or unramified for B, and if $B \otimes \mathbb{Q}_p$ is a division algebra, then we call p ramified. Every quaternion algebra is ramified at finitely many primes and this set of primes determines B.

An order $O \subset B$ is a lattice (a finitely generated $\mathbb{Z}$-module satisfying $O \otimes \mathbb{Q} = B$) that is also a subring of B. An order is maximal if it is not properly contained in another order.

If $\mathrm{End}_{\overline{\mathbb{F}}_p}(\mathcal{E})$ is not isomorphic to an order of an imaginary quadratic field, then $B = \mathrm{End}_{\overline{\mathbb{F}}_p}(\mathcal{E}) \otimes \mathbb{Q}$ is a definite quaternion algebra over $\mathbb{Q}$ with the only ramified finite prime being p. The endomorphism ring $\mathrm{End}_{\overline{\mathbb{F}}_p}(\mathcal{E})$ is isomorphic to $O \subset B$ which is a maximal order of B. In this case we say that $\mathcal{E}$ is supersingular.

Note that from our defnition, the property for an elliptic curve $\mathcal{E}/\mathbb{F}_q$ being ordinary or supersingular does not change under base field extensions. Thus they are determined by the j-invariants.

When p is ramified in B, the division algebra $B \otimes \mathbb{Q}_p$ has a unique maximal order O_p which contains all elements with non-negative valuation with respect to the unique valuation on $B \otimes \mathbb{Q}_p$ extending the p-adic valuation of $\mathbb{Q}_p$. The ring O_p has a unique maximal ideal P_p whose residue field is isomorphic to $\mathbb{F}_{p^2}$. Moreover, $P_p = pO$ and the algebra $B \otimes \mathbb{Q}_{p^2} \simeq M_2(\mathbb{Q}_{p^2})$. The quadratic fields $K/\mathbb{Q}$ contained in B are the ones satisfying $B \otimes K \simeq M_2(K)$, and these are exactly the imaginary quadratic fields $K/\mathbb{Q}$ in which p is inert or ramified.

§6.2 Density of supersingular primes

Let $E/\mathbb{Q}$ be an elliptic curve. Let $p > 3$ be a prime of good reduction for E. The reduction of E at p is an elliptic curve $\mathcal{E}_p$ defined over $\mathbb{F}_p$. Let $a_p \in \mathbb{Z}$ be the trace of Frobenius action on $\mathcal{E}_p[\ell^\infty]$. Then $\mathcal{E}_p$ is supersingular if and only if $a_p = 0$. From the Hasse bound, we know that $|a_p| \leq 2\sqrt{p}$. Thus, if a_p is randomly distributed, then the probability of $a_p = 0$ is roughly $(4\sqrt{p})^{-1}$. If we sum over all primes p, the number of primes $p < X$ such that $\mathcal{E}_p$ is a supersingular elliptic curve is about $\sqrt{X}\,(\log X)^{-1}$. This is a special case of the Lang-Trotter conjecture predicting the expectation for the number of supersingular primes for a general elliptic curve. When an elliptic curve E has complex multiplication, the distribution of a_p is known to be not random.

Theorem 6.1 (Shimura-Taniyama)**.** *Let E/L be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K. Let $\mathfrak{p} \subset L$ be a prime lying above the rational prime p at which E admits good reduction. If p splits in $K/\mathbb{Q}$, then the reduction $\mathcal{E}_\mathfrak{p}$ is ordinary. If p is inert or ramified in $K/\mathbb{Q}$, then the reduction $\mathcal{E}_\mathfrak{p}$ is supersingular.*

Extending the field L as necesary such that $K \subset L$, this theorem follows from the fact that $\mathrm{End}_L(E) \to \mathrm{End}_{\overline{\mathbb{F}}_p}(\mathcal{E}_\mathfrak{p})$ is injective. As we discussed in the previous section, the endomorphism algebra $\mathrm{End}_{\overline{\mathbb{F}}_p}(\mathcal{E}_\mathfrak{p}) \otimes \mathbb{Q}$ contains an imaginary quadratic field $K/\mathbb{Q}$ in which p splits if and only if $\mathcal{E}_p$ is ordinary.

Theorem 6.2 (Serre)**.** *Let E be an elliptic curve without complex multiplication defined over $\mathbb{Q}$, the set of primes p at which the reduction of E is ordinary has density* 1*.*

§6.3 Elkies's theorem

Theorem 6.3 (Elkies)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$. Then there exist infinitely many primes p such that the reduction of E at p is supersingular.*

When E is a CM elliptic curve, the statement follows from the theorem of Shimura-Taniyama. So we assume E does not have CM.

Proof sketch. Assume E admits supersingular reduction at finitely many primes. Let the finite set S contain all supersingular primes and all primes at which E admits bad reduction. We would want to construct a prime $p \notin S$ such that $\mathcal{E}_p$ is supersingular.

To construct such a p, we will construct a CM elliptic curve E_0 such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E_0) \otimes \mathbb{Q} \simeq K$, $\mathcal{E}_p$ is isomorphic to the reduction of E_0 at a prime above p over $\overline{\mathbb{F}}_p$ and p does not split in $K/\mathbb{Q}$. In fact,

instead of constructing a E_0, in practice, we construct the field K which guarantees the existence of a desired E_0. We will now sketch the proof in a simplified case.

Goal: Given $E/\mathbb{Q}$ with $j_E < 1728$ and a finite set S of primes, construct a supersingular prime $p \notin S$.

1. Let D be a prime satisfying
   (a) $D \equiv 3 \pmod 4$;
   (b) for each $p \in S$ or $p \mid (j_E - 1728)$, we have p splits in $K = \mathbb{Q}(\sqrt{-D})/\mathbb{Q}$;
   (c) D is sufficiently large.

   Such a prime D exists by Dirichlet's theorem which states that there exist infinitely many primes in any congruence class $a \pmod b$ with $\gcd(a, b) = 1$.

   Note that $D \equiv 3 \pmod 4$ implies that $\left(\frac{-1}{D}\right) = -1$ which is of important use in the proof.

2. Consider elliptic curves $E_1, \ldots, E_n$ with complex multiplication by the maximal order $\mathcal{O}_K$ of K.

   Any p non-split in $K/\mathbb{Q}$ is a supersingular prime for $E_1, \ldots, E_n$.

3. Define the following monic irreducible polynomial
$$P_D(x) = \prod_{i=1}^{n}(x - j_i) \in \mathbb{Z}[x]$$
   whose roots are the j-invariants of $E_1, \ldots, E_n$.

   Recall that $P_D(x)$ has all coefficients in $\mathbb{Z}$ because $j_1, \ldots, j_n$ are Galois conjugates and they are all algebraic integers.

   Moreover, for any prime $p \mid P_D(j_E)$, the reduction $\mathcal{E}_p$ is isomorphic to the reduction of some E_i at a prime above p over $\overline{\mathbb{F}}_p$.

4. Show $(j_E - 1728)P_D(j_E) \equiv \square \pmod D$.

   This statement follows from Deuring's lifting lemma.

   This implies either $D \mid (j_E - 1728)P_D(j_E)$ (recall that $D \nmid j_E - 1728$ by our assumption) or the Legendre symbol
$$\left(\frac{(j_E - 1728)P_D(j_E)}{D}\right) = 1.$$

5. $P_D(x)$ has a unique real root and $(j_E - 1728)P_D(j_E) < 0$ as long as D is sufficiently large.

   To determine the sign of $P_D(j_E)$, we must analyse the real roots of $P_D(x)$. The real j-invariants correspond to lattices which are fixed by complx conjugation. These are the fractional ideal classes $\mathfrak{a} \in cl(\mathcal{O}_K)$ such that $\mathfrak{a} = \mathfrak{a}^{-1} = \overline{\mathfrak{a}}$, thus they are in $cl(O_K)[2]$. From genus theory, for imaginary quadratic field with prime discriminant, the group $cl(\mathcal{O}_K)[2]$ is trivial. Thus the only real CM j-invariant is $j\left(\frac{1+\sqrt{-D}}{2}\right)$.

   Recall that $j(\tau) = q^-1 + 744 + 196884q + \ldots$ where $q = e^{2\pi i\tau}$. Thus, $j\left(\frac{1+\sqrt{-D}}{2}\right) < 0$ for D sufficiently large. Combine this fact with our assumption that $j_E < 1728$.

If $D \nmid P_D(j_E)$, we deduce the Legendre symbol

$$\left(\frac{(j_E - 1728)P_D(j_E)}{D}\right) = \left((-1)\frac{|(j_E - 1728)P_D(j_E)|}{D}\right) = 1.$$

Combined with $\left(\frac{-1}{D}\right) = -1$, we deduce that

$$\left(\frac{|(j_E - 1728)P_D(j_E)|}{D}\right) = -1.$$

6. Recall that the Legendre symbol is multiplicative. Therefore there either exists a positive $p \mid P_D(j_E)$ such that (recall all $p \mid (j_E - 1728)$ splits in $\mathbb{Q}(-D)/\mathbb{Q}$)

$$\left(\frac{p}{D}\right) = \left(\frac{-D}{p}\right) = -1;$$

or $D \mid P_D(j_E)$. In either case, we obtain a non-split prime p for D which is a supersingular prime for E not contained in S.

The proof is then done. □

§7 Problems and solutions

Problem 1: Let $\Im(\tau)$ denote the imaginary parts. Show that $j(\tau) \to \infty$ as $\Im(\tau) \to \infty$.
Solution. One has that

$$\begin{aligned}\lim_{\Im\to\infty} g_2(\tau) &= 120 \cdot \zeta(4) + \lim_{\Im\to\infty} \sum_{(m,n)\neq(0,0)} \frac{1}{(m+n\tau)^4} \\ &= 120 \cdot \zeta(4) + \lim_{\Im\to\infty} \sum_{(m,n)\neq(0,0)} \frac{1}{(n+m\tau)^4} \\ &= 120 \cdot \zeta(4) + \lim_{\Im\to\infty} \sum_{(m,n)\neq(0,0)} \frac{1}{n^4} \\ &= 120 \cdot \zeta(4)\end{aligned}$$

and similarly that

$$\lim_{\Im\to\infty} g_3(\tau) = 280 \cdot \zeta(6),$$

where we have used the uniform convergence in $\mathcal{F}$ of the sums involved here. Recalling the classical evaluations $\zeta(4) = \pi^4/90$ and $\zeta(6) = \pi^6/945$, we conclude with the limits

$$\begin{aligned}\lim_{\Im\to\infty} g_2(\tau) &= \frac{4\pi^4}{3}, \\ \lim_{\Im\to\infty} g_3(\tau) &= \frac{8\pi^6}{27}, \\ \lim_{\Im\to\infty} \Delta(\tau) &= \left(\frac{4\pi^4}{3}\right)^3 - \left(\frac{8\pi^6}{27}\right)^2 = 0.\end{aligned}$$

Therefore, we have that

$$\lim_{\Im\to\infty} j(\tau) = \infty.$$

Problem 2: Show that if a curve E given by a Weierstrass equation is singular, then there exists a rational map $\phi : E \to \mathbb{P}^1$ of degree one, i.e. the curve E is birational to $\mathbb{P}^1$.
Solution. Given a Weierstrass function for the curve

$$E : f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,$$

we know that by making a linear change of variables we may assume that the singular point of E is $(0,0)$. Then, checking the value of the function and of the partial derivatives

$$f(0,0) = a_6 = 0, \quad \frac{\partial f}{\partial x}(0,0) = -a_4, \quad \frac{\partial f}{\partial y}(0,0) = a_3 = 0,$$

we may simplify the equation of E to

$$E : y^2 + a_1xy = x^3 + a_2x^2.$$

Then the rational map $E \to \mathbb{P}^1$, $(x,y) \mapsto [x,y]$ has degree 1, since it has an inverse given by $\mathbb{P}^1 \to E$, $[1,t] \mapsto (t^2 + a_1t - a_2, t^3 + a_1t^2 - a_2t)$. To derive this formula, let $t = y/x$ and note that $f(x,y)/x^2$ yields to $t^2 + a_1t = x + a_2$, so both x and $y = tx$ are determined by t and in $\overline{K}(t)$.

Problem 3: Show that a holomorphic elliptic function, i.e. an elliptic function with no poles, is constant. Similarly, an elliptic function with no zeros is constant.
Solution. Let $f(z) \in \mathbb{C}(\Lambda)$ is holomorphic. Let D be a fundamental parallelogram for Λ. The periodicity of f implies that

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

where $\overline{D}$ denotes the closure of D in $\mathbb{C}$. Since f is a continuous function on the compact set $\overline{D}$, then f attains its maximum on $\overline{D}$ at some point $z_0 \in \overline{D}$. Hence f is bounded on all of $\mathbb{C}$, so Liouville's theorem implies that f is constant, proving the first statement. The second statment follows: if f has no zeros, then $1/f$ has no poles, so $1/f$ is holomorphic, hence constant.

Problem 4: Let R be an order in the imaginary quadratic field K. Then there exists a unique positive integer c such that $R = \mathbb{Z} + cR_k = [1, c\tau]$. In particular, the integer c is the index of R in R_K as an abelian group.
Solution. We first note that R is a sublattice of $R_K = [1, \tau]$, so it has a finite index. Let $c > 0$ be the unique positive integer such that $R \cap \mathbb{Z}\tau = c\mathbb{Z}\tau$. We want to show that this integer satisfies the statement. Let $\lambda \in R$, then surely there exust some integers m, n such that $\lambda = m + n\tau$, but it means that $n\tau = \lambda - m$, and since $n\tau = \mathbb{Z}\tau$, $\lambda - m \in R$, then this quantity belongs to their intersection, but by construction $R \cap \mathbb{Z}\tau = c\mathbb{Z}\tau$, so $c \mid n$ and then $\lambda = m + n\tau \in \mathbb{Z} + c\mathbb{Z}\tau$.

Problem 5: Suppose that $E = \mathbb{C}/\Lambda$ is an elliptic curve with complex multiplication. Then there exists $\beta \in \mathbb{C}$ such that $\beta\Lambda$ is a lattice in some imaginary quadratic field K.
Solution. Consider the result we already saw with $\Lambda_1 = \Lambda_2 = \Lambda$, which tells us that $\mathrm{End}(E)$ is in bijective correspondence with the set $S = \{a \in \mathbb{C} : a\Lambda \subset \Lambda\}$. Since E has complex multiplication, we immediately know that $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$, so it also contains nontrivial endomorphisms, so that S also contains elements of $\mathbb{C}$ which are not in $\mathbb{Z}$. In general, let $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, and let $\alpha \in S$, so that $\alpha\Lambda \subset \Lambda$. Then there exist integers a, b, m, n such that

$$\begin{cases} \alpha\omega_1 = a\omega_1 + b\omega_2, \\ \alpha\omega_2 = m\omega_1 + n\omega_2, \end{cases}$$

so that α is a root of the polynomial

$$\det \begin{bmatrix} x-a & -b \\ -m & x-n \end{bmatrix} = 0 \iff (x-a)(x-n) - bm = 0$$

so that α is a quadratic irrational over $\mathbb{Q}$ and integral over $\mathbb{Z}$. Dividing $\alpha\omega_2$ by ω_2 we get

$$\alpha = \frac{m\omega_1 + n\omega_2}{\omega_2} = m\frac{\omega_1}{\omega_2} + n, \quad \text{where } \tau = \frac{\omega_1}{\omega_2}.$$

Since ω_1, ω_2 span a lattice, their ratio cannot be real, so $\tau \notin \mathbb{R}$.

Moreover, suppose that α induces a nontrivial endomorphism, i.e., $\alpha \notin \mathbb{Z}$. This implies that $c \neq 0$ (otherwise $\alpha = n \in \mathbb{Z}$), and then $\mathbb{Q}(\tau) = \mathbb{Q}(\alpha)$, so that $\alpha \notin \mathbb{R}$ i.e., α is quadratic imaginary. Thus the ring R of elements $\alpha \in \mathbb{Q}(\tau)$ such that $\alpha\Lambda \subset \Lambda$ is a subring of the quadratic field $K = \mathbb{Q}(\tau)$, and in fact, a subring of R_K.

Problem 6: Compute the isogeny on the elliptic curve E with Weierstrass equation $y^2 = x^3 + x$.
Solution. We have that

$$\frac{\partial f}{\partial x} = -3x^2 - 1, \quad \frac{\partial f}{\partial y} = 2y,$$

and thus the tangent line through an arbitrary point $P = (x_1, y_1)$ on E is the line $(2y_1, 3x_1^2+1)\lambda + (x_1, y_1)$. Plugging this into the equation for E we obtain the equation

$$((3x_1^2 + 1)\lambda + y_1)^2 = (2y_1\lambda + x_1)^3 + (2y_1\lambda + x_1).$$

In order to find the third intersection point, we must solve for λ, but expanding out the equation we find that we end up solving

$$\lambda^3 8y_1^3 + (12y_1^2 - 9x_1^4 - 6x_1^4 - 1)\lambda^2 = 0.$$

Dividing out by λ^2 we obtain that

$$\lambda = \frac{12y_1^2 - 9x_1^4 - 6x_1^2 - 1}{8y_1^2}.$$

Therefore the third intersection point is given by

$$\left(x_1 + \frac{12y_1^2 - 9x_1^4 - 6x_1^2 - 1}{8y_1^2}, y_1 + \frac{(3x_1^2 + 1)(12y_1^2 - 9x_1^4 - 6x_1^2 - 1)}{8y_1^2}\right)$$

and hence $2P$ is the point

$$\left(x_1 + \frac{12y_1^2 - 9x_1^4 - 6x_1^2 - 1}{8y_1^2}, -y_1 - \frac{(3x_1^2 + 1)(12y_1^2 - 9x_1^4 - 6x_1^2 - 1)}{8y_1^2}\right)$$

Problem 7: Let $\phi : C_1 \to V$ be a rational map where $V \subset \mathbb{P}^n$ is a projective variety. Show that for any point $P \in C_1$, f is regular at P and hence f is a regular map.
Solution. By definition, f is a typle $(g_0, \ldots, g_n)$ where the $g_i \in \overline{K}(C)$. Let $P \in C$ and let t be a local parameter at P. Then let

$$m = \min_i \left(\mathrm{ord}_P(g_i)\right).$$

Then ϕ is also given by $(t^{-m}g_0, \ldots, t^{-m}g_n)$, so that f is regular at P.

Problem 8: Let $f : X \to \mathbb{C}$ be a holomorphic map where X is a compact Riemann surface. Show that f is constant.
Solution. By the open mapping theorem $f(X)$ is open, but $f(X)$ is also compact and hence closed. Since $\mathbb{C}$ is connected, $f(X) = \mathbb{C}$, contradicting $f(X)$ compact. Thus f is constant.

Problem 9: Let $f : E_{\Lambda_1} \to E_{\Lambda_2}$ be a holomorphic map of complex tori which maps 0 to 0. Show that f is the map $[\alpha]$ for some $\alpha \in \mathbb{C}$ for which $\alpha\Lambda_1 \subset \Lambda_2$.
Solution. Since $\mathbb{C}$ is simply connected, the map $\mathbb{C} \to E_{\Lambda_1} \to E_{\Lambda_2}$ lifts to a continuous map F

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

where the vertical maps are just the natural projections and we can assume F maps 0 to 0. Since the projections $\pi_i : \mathbb{C} \to E_{\Lambda_i}$ are local isomorphisms, the map F is holomorphic. Let $\omega \in \Lambda_1$,

then $G(z) = F(z+\omega) - F(z)$ takes values in Λ_2 which is discrete, hence $G(z)$ is constant. Thus $F'(z+\omega) = F'(z)$ and since this is true for all $\omega \in \Lambda_1$, by considering F' on a fundamental parallelogram we conclude that F' is bounded. It follows from Liouville's theorem that F is constant, i.e. $F(z) = \alpha z + \beta$. As f maps 0 to 0, we have that $\beta \in \Lambda_2$, and we conclude that f is the map $[\alpha]$.

Problem 10: Show that two lattices Λ_{τ_1} and Λ_{τ_2} are homothetic if and only if $\tau_2 = \gamma\tau_1$ for some $\gamma \in \Gamma$.
Solution. Let γ be as above. Then $\Lambda_{\gamma\tau}$ is homothetic to the lattice $\langle a\tau + b, c\tau + d\rangle$ but since $ad - bc = 1$, this lattice is just Λ_τ. Conversely, let us suppose Λ_{τ_1} and Λ_{τ_2} are homothetic, so that $\exists\, \alpha \in \mathbb{C}^\times$ such that $\langle \alpha, \alpha\tau_2\rangle = \langle 1, \tau_1\rangle$. Thus $\alpha = c\tau_1 + d$ for some $c, d \in \mathbb{Z}$ and $\alpha\tau_2 = a\tau_1 + b$ for some $a, b \in \mathbb{Z}$. Similarly there are $w, x, y, z \in \mathbb{Z}$ such that

$$\begin{aligned} \tau_1 &= w(a\tau_1 + b) + x(c\tau_1 + d) \\ 1 &= y(a\tau_1 + b) + z(c\tau_1 + d). \end{aligned}$$

Since τ_1 and 1 are linearly independent over $\mathbb{Z}$, this condition is equivalent to

$$\begin{bmatrix} w & x \\ y & z \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Therefore $\det(\gamma) = \pm 1$, but at the same time we can see that

$$\Im\tau_2 = \Im\frac{a\tau_1 + b}{c\tau_1 + d} = \frac{\det(\gamma)}{|c\tau_1 + d|^2}\Im\tau_1.$$

Then since $\Im\tau_1, \Im\tau_2 > 0$, we have that $\det(\gamma) > 0$, and hence $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, from which the statement follows.

Problem 11: If f is a meromorphic function on $\mathbb{C}$, let $v_z(f)$ denote the order of vanishing of f at z, and suppose that f is elliptic with respect to the lattice Λ. Show that

$$\sum_{z \in \mathbb{C}\setminus\Lambda} v_z(f) = 0.$$

Solution. Since $\mathbb{C}/\Lambda$ is compact, it follows by the isolation of zeros and poles theorem that f has only finitely many zeros or poles in $\mathbb{C}/\Lambda$ and hence the sum is well defined. Taking any fundamental parallelogram whose edges do not contain any pole of zero of f, we have that since f is elliptic

$$\int_\gamma \frac{f'}{f} dz = \int_\gamma \frac{d}{dz}\log(f) dz = \log(f(z_2)) - \log(f(z_1)) = 0,$$

where γ is the boundary of the parallelogram. By the argument principle, this integral is precisely the sum in the problem.

Problem 12: Show that for all $a \in \mathbb{C}$, there exists a $w \in \mathbb{C}$ such that $\wp(w) = a$, and in particular, the set of such solutions are $\{w, -w\}$ if $w \notin \left\{\frac{\omega}{2} : \omega \in \Lambda\right\}$. *Solution.* Consider $\wp(z) - a$. This is an elliptic function with a double pole at 0, and hence by the previous problem we have that the sum of the zeros of this function is 2 up to the multiplicities. Let w be a zero, so that if $w \notin \left\{\frac{\omega}{2} : \omega \in \Lambda\right\}$,

then $-w$ is another zero and hence these are all the zeros of $\wp(z) - a$. Suppose $w \in \{\frac{\omega}{2} : \omega \in \Lambda\}$. Since $\wp(z)$ is even, we have that $\wp'$ is odd so that $\wp'(z) = -\wp'(z+\omega)$ for all $\omega \in \Lambda$. It follows that $\wp'(w) = 0$, and hence $\wp$ has a double root at w and hence w is the only zero.

Problem 13: Show that $N(\alpha) = |N\alpha|$, where α is a nonzero element of an order $\mathcal{O}$ in a number field K and (α) denotes the principal $\mathcal{O}$-ideal generated by α.
Solution. We know that the determinant of $M_\alpha \in \mathrm{GL}(K) \simeq \mathrm{GL}_n(\mathbb{Z})$ can be interpreted as the signed volume of the fundamental parallelpiped of the lattice (α) in the $\mathbb{Q}$-vector space $K \simeq \mathbb{Q}^n$, where $n = [K : \mathbb{Q}]$ is the degree of K. Notice that $N(\alpha) = [\mathcal{O} : (\alpha)] = [\mathcal{O}_K : \alpha\mathcal{O}_K]$ depends only on α and K, not the order $\mathcal{O}$. The statement in the problem follows.

Problem 14: Show that the ideal class group $\mathsf{cl}(\mathcal{O})$ is the group of invertible fractional $\mathcal{O}$-ideals modulo its subgroup of principal fractional ideals.
Solution. Recall from the problem-solving session that $\mathsf{cl}(\mathcal{O}) = \{\text{proper } \mathcal{O}\text{-ideals}\}/\sim$, where $\sim$ denotes homothety. Let G be the group of invertible fractional $\mathcal{O}$-ideals and H its subgroup of principal fractional $\mathcal{O}$-ideals. Every invertible fractional $\mathcal{O}$-ideal $\mathfrak{b} = \frac{1}{b}\mathfrak{a}$ is the product of is the product of an invertible principal fractional $\mathcal{O}$-ideal $\left(\frac{1}{b}\right)$ and an invertible $\mathcal{O}$-ideal $\mathfrak{a}$. It then follows that G/H contains all the cosets $\mathfrak{a}H$, where $\mathfrak{a}$ is any invertible (equivalently, proper) $\mathcal{O}$-ideal. Every nonzero principal fractional $\mathcal{O}$-ideal is invertible (since $(\alpha)^{-1} = (\alpha^{-1})$), and so H contains every nonzero principal fractional $\mathcal{O}$-ideal and for any two proper/invertible $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$, we have that $\mathfrak{a}H = \mathfrak{b}H$ if and only if $\mathfrak{a} \sim \mathfrak{b}$. Thu $\mathsf{cl}(\mathcal{O}) = G/H$.

Problem 15: Let D be an imaginary quadratic discriminant. Show that there exists a unique imaginary quadratic order $\mathcal{O}$ with $\mathrm{disc}(\mathcal{O}) = \mathcal{D} = u^2 D_K$, where D_K is the fundamental discriminant of the maximal order $\mathcal{O}_K$ in $K = \mathbb{Q}(\sqrt{D_K})$ and $u = [\mathcal{O}_K : \mathcal{O}]$.
Solution. Write $D = \mathrm{disc}(\mathcal{O})$ as $D = u^2 D_K$, with $u \in \mathbb{Z}_{>0}$ and D_K is the fundamental discriminant. Let $K = \mathbb{Q}(\sqrt{D_K})$ and $\mathcal{O}_K$ be the maximal order in K. Then $\mathcal{O}_K$ is the ring of integers of K. Now define

$$\tau := \begin{cases} \frac{\sqrt{D_K}}{2} & \text{if } D_K \equiv 0 \pmod 4, \\ \frac{1+\sqrt{D_K}}{2} & \text{if } D_K \equiv 1 \pmod 4. \end{cases}$$

Then $\mathrm{disc}([1,\tau]) = (\tau - \overline{\tau})^2 = D_K$, and $\tau + \overline{\tau}$ and $\tau\overline{\tau}$ are integers, so $\tau \in \mathcal{O}_K$ and $[1,\tau]$ is a suborder of $\mathcal{O}_K$. But $\mathcal{O}_K$ is the maximal order of K, so $\mathcal{O}_K = [1,\tau]$ and $\mathrm{disc}(\mathcal{O}_K) = D_K$. The order $\mathcal{O} = [1, u\tau]$ has discriminant $D = u^2 D_K$.

Conversely, if $|O = [1,\omega]$ is any imaginary quadratic order of discriminant D, then ω is the root of a quadratic equation of discriminant D and therefore an algebraic integer in the field $K = \mathbb{Q}(\sqrt{D_K})$. We must then have $\mathcal{O}_K \supseteq O$, since $\mathcal{O}_K$ is the unique maximal order.The ratio of the squares of the areas of the fundamental parallelograms of $\mathcal{O}_K$ and $\mathcal{O}$ must be $D/D_K = u^2$ which implies $[\mathcal{O}_K : \mathcal{O}] = u$. Let $\mathcal{O}_K = [1,\tau]$, where τ is defined as above. Then $u\mathcal{O}_K \subseteq \mathcal{O}$, so that $u\tau \in \mathcal{O}$, and the lattice $[1, u\tau]$ is a suborder of $\mathcal{O}$ with index $u \in \mathcal{O}_K$ and thus equal to $\mathcal{O}$. It follows then that $[1, u\tau]$ is the unique imaginary quadratic order of discriminant D.

Problem 16: Suppose that the elliptic curve E is given by a Weierstrass equation $y^2 = x^3 + ax + b$. Show that if $\mathrm{Aut}(E)$ contains an element of order 4 (resp. 6), then $a = 0$ (resp. $b = 0$).
Solution. We know that the only automorphisms of such a Weierstrass elliptic curve are of the form $(x, y) \mapsto (u^2 x, u^3 y)$. The order of such an automorphism is the order of u in $F^\times$, and when u has order 3 or 4, this change of variables preserves the Weierstrass equation if and only if $a = 0$ or

$b = 0$ respectively.

Problem 17: Suppose that E is defined by a minimal Weierstrass equation and

$$E_1(F) = \{(x, y) \in E(F) : v(x) < 0\} = \{(x, y) \in E(F) : v(y) < 0\}.$$

Show that if $(x, y) \in E_1(F)$, then $3v(x) = 2v(y) < 0$.
Solution. We can immediately see by the definition of the reduction map that $(x, y, 1)$ reduces to $(0, 1, 0)$ if and only if $v(y) < 0$ and $v(y) < v(x)$. If $(x, y) \in E(F)$ then, since x and y satisfy a Weierstrass equation, with coeffients in $\mathcal{O}$, it follows that $v(x) < 0$ if and only if $v(y) < 0$. In that case, $v(y) = \frac{3}{2}v(x) < v(x)$, and we conclude that $3v(x) = 2v(y) < 0$.

Problem 18: Suppose that $\mathfrak{p}$ is a prime of K lying above a rational prime $\mathfrak{p} > 3$, and $n \geq 0$. Let C be a subgroup of $(\mathcal{O}/\mathfrak{p}^n)^\times$ acting on $\mathcal{O}/\mathfrak{p}^n$ by multiplication. Show that if C is not a p-group, then for every $i > 0$, $H^i(C, \mathcal{O}/\mathfrak{p}^n) = 0$.
Solution. If C'. the prime-to-p-part of C, is nontrivial, then $(\mathcal{O}/\mathfrak{p}^n)^{C'} = 0$ and since $H^i(C', \mathcal{O}/\mathfrak{p}^n) = 0$ for every i, the inflation-restriction exact sequence

$$0 \to H^i(C/C', (\mathcal{O}/\mathfrak{p}^n)^{\mathbb{C}'}) \to H^i(C, \mathcal{O}/\mathfrak{p}^n) \to H^i(C', \mathcal{O}/\mathfrak{p}^n)$$

shows that $H^i(C, \mathcal{O}/\mathfrak{p}^n) = 0$ for every $i > 0$.

Problem 19: Let $\phi : \mathbb{C}/L_1 \to \mathbb{C}/L_2$ be a holomorphic map with $\phi(0) = 0$. Show then that there is a unique $\alpha \in \mathbb{C}$ for which $\phi = \phi_\alpha$.
Solution. Let $\phi_i : \mathbb{C} \to \mathbb{C}/L_i$ be quotient maps and let $f : \mathbb{C} \to \mathbb{C}$ be a holomorphic function for which $\phi(\pi_1(z)) = \pi_2(f(z))$. Then for all $z \in \mathbb{C}$ and $\omega \in L_1$, we have that

$$\pi_2(f(z + \omega)) = \phi(\pi_1(z + \omega)) = \phi(\pi_1(z)) = \pi_2(f(z)),$$

and thus $f(z + \omega) - f(z) \in \ker \pi_2 = L_2$. For each $\omega \in L$, the function $g_\omega(z) = f(z + \omega) - f(z)$ is a continuous map from the connected set $\mathbb{C}$ to a discrete set L_2; its image must be connected and therefore consists of a single point. It follows then that $g_\omega(z)$ is constant and $g'_\omega(z) = 0$, which implies that $f'(z + \omega) = f'(z)$ for all $z \in \mathbb{C}$ and $\omega \in L_1$. This implies that $f'(z)$ is periodic with respect to L_1, and is therefore a holomorphic function on the compact Riemann surface $\mathbb{C}/L_1$, and hence constant. Thus $f(z) = \alpha z + \beta$ for some $\alpha, \beta \in \mathbb{C}$. Since $\phi(0) = 0$, we he have that for all $\omega \in L_1$, we have

$$\pi_2(f(\omega)) = \phi(\pi_1(\omega)) = \phi(0) = 0.$$

Taking $\omega = 0$ suggests that $\beta = f(0) \in L_2$, and therefore we have that $\alpha L_1 \subseteq L_2$. For all $z \in \mathbb{C}$ we have hat $\phi(\pi_2(z)) = \pi_2(f(z)) = \pi_2(\alpha z)$, thus $\phi = \phi_\alpha$. The value of α is unique: if $\phi = \phi_\gamma$ for some $\gamma \in \mathbb{C}$, then $(\alpha - \gamma)z \in L_2$ for all $z \in \mathbb{C}$, and therefore $\alpha - \gamma = ((\alpha - \gamma) \cdot z)' = 0$ as argued above, so that $\alpha = \gamma$.

Problem 20: Let K be an imaginary quadratic field, and let E be an elliptic curve representing an isomorphism class in $\mathcal{E}(\mathcal{O}_K)$. Show that $K(j(E))$ is an abelian extension of K.
Solution. Let L be the fixed field of the kernel of the homomorphism $\mathfrak{F} : \mathrm{Gal}(\overline{K}/K) \to \mathsf{cl}(\mathcal{O}_K)$, i.e.

$\mathrm{Gal}(\overline{K}/L) = \ker \mathfrak{F}$. Then

$$\begin{aligned}
\mathrm{Gal}(\overline{K}/L) &= \ker \mathfrak{F} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : \mathfrak{F}(\sigma) = 1\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : \mathfrak{F}(\sigma) * E = E\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : E^{\sigma} = E\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : j(E^{\sigma}) = j(E)\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K(j(E)))\},
\end{aligned}$$

and hence $L = K(j(E))$. Furthermore, since

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/L) = \mathrm{Gal}(\overline{K}/K)/\ker \mathfrak{F},$$

it follows that $\mathfrak{F}$ maps $\mathrm{Gal}(L/K)$ injectively into $\mathsf{cl}(\mathcal{O}_K)$. Hence $\mathsf{cl}(\mathcal{O}_K)$ is an abelian group, and hence $\mathrm{Gal}(L/K)$ is abelian.