MODULAR CURVES

SARAH FUJIMORI

1. Introduction

Modular curves are important to number theory because they parameterize isomorphism classes of elliptic curves, along with some additional structure. In this paper, we define the modular groups and congruence subgroups and the compactified modular curves $X_0(N), X_1(N)$, and $X(N)$. We then prove some results about parameterization of elliptic curves and briefly discuss modular curves when viewed as algebraic curves. This paper assumes knowledge of abstract algebra and basic ring theory and algebraic geometry.

2. The Modular Group and Congruence Subgroups

We begin by defining the modular group:

Definition 2.1. The *modular group* is the group of 2-by-2 matrices with integer entries and determinant 1:

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

The group operation is matrix multiplication. These transformations have natural group properties: having an identity transformation, having inverse transformations, and being associative. Any element in the modular group represents a transformation of the half plane, and the product of two matrices in the modular group represents the transformation that is obtained by consecutively applying the transformations represented by the two matrices.

We say that the modular group *acts* on the half plane $\mathcal{H}$. Each element in the modular group is a linear fractional transformation on the upper half plane $\mathcal{H} = \{\tau \in \mathbb{C} : \Im(\tau) > 0\}$. That is, for an element $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, we define the map

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}(\tau) = \frac{a\tau + b}{c\tau + d}, \quad \tau \in \mathcal{H}\,.$$

The following proposition shows that for an element $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $\gamma\tau$ is actually in the upper half plane:

Proposition 2.2. *Let* $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *be an element of* $\mathrm{SL}_2(\mathbb{Z})$*. Then, for any* $\tau \in \mathcal{H}$*, we have*

$$\Im(\gamma\tau) = \frac{\Im(\tau)}{|c\tau + d|^2}.$$

Proof. By the definition of the group action of $\mathrm{SL}_2(\mathbb{Z})$, we have

$$\Im(\gamma z) = \Im\left(\frac{a\tau + b}{c\tau + d}\right).$$

Multiplying numerator and denominator by $\overline{c\tau + d}$ to rationalize this quantity, this is equal to

$$\Im\left(\frac{(a\tau+b)(\overline{c\tau+d})}{(c\tau+d)(\overline{c\tau+d})}\right) = \frac{\Im(a\tau+b)(\overline{c\tau+d})}{|c\tau+d|^2}.$$

Let $\tau = x + yi$. Since $ad - bc = 1$, the imaginary part of $(a\tau + b)(\overline{c\tau + d})$ is

$$\Im\left((ax + ayi + b)(cx + d - cyi)\right) = -acxy + acxy + ady - bcy = (ad - bc)y = y,$$

so our expression simplifies to

$$\frac{\Im(\tau)}{|c\tau+d|^2}$$

as desired. □

We now introduce some key subgroups of the modular group:

Definition 2.3. Let N be a positive integer. The **principal congruence subgroup of level** N is the group

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \underset{2}{\mathrm{SL}}(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod N \right\}.$$

Then, we can define a general congruence subgroup as follows:

Definition 2.4. A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a **congruence subgroup** of **level** N if there exists an integer N such that $\Gamma(N) \subset \Gamma$.

There are two important types of congruence subgroups called $\Gamma_0(N)$ and $\Gamma_1(N)$ that we also want to introduce:

Definition 2.5. The subgroup $\Gamma_0(N)$ is defined by

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

Definition 2.6. The subgroup $\Gamma_1(N)$ is defined by

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

The relationship between these subgroups can be described with the following proposition:

Proposition 2.7. *$\Gamma(N) \triangleleft \Gamma_1(N)$ and $\Gamma_1(N) \triangleleft \Gamma_0(N)$.*

Proof. Recall that H is a normal subgroup of G if it is the kernel of some group homomorphism with domain G. Consider the homomorphism

$$\phi : \Gamma_1(N) \to \mathbb{Z}/N\mathbb{Z}, \phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = b \pmod N$$

Clearly, $\Gamma(N)$ is the kernel of this homomorphism, so $\Gamma(N) \triangleleft \Gamma_1(N)$.

We can use a similar technique to show that $\Gamma_1(N) \triangleleft \Gamma_0(N)$. Consider the homomorphism

$$\phi : \Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^*, \phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = d \pmod N$$

Clearly, $\Gamma_1(N)$ is the kernel of this homomorphism, so $\Gamma_1(N) \triangleleft \Gamma_0(N)$. □

We can now define modular curves:

Definition 2.8. For any congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$, the **modular curve** $Y(\Gamma)$ is defined as the space of orbits under Γ:

$$Y(\Gamma) = \Gamma \setminus \mathcal{H} = \{\Gamma\tau : \tau \in H\}$$

Recall that we defined three important types of congruence subgroups: $\Gamma(N)$, $\Gamma_0(N)$, and $\Gamma_1(N)$. The modular curves for $\Gamma_0(N)$, $\Gamma_1(N)$, and $\Gamma(N)$ are denoted

$$Y_0(N) = \Gamma_0(N) \setminus \mathcal{H}, Y_1(N) = \Gamma_1(N) \setminus \mathcal{H}, Y(N) = \Gamma(N) \setminus \mathcal{H}\,.$$

3. Compactification of Modular Curves

Although the parametrization of elliptic curves that we are focusing on is about the points on the modular curves $Y_0(N)$, $Y_1(N)$, and $Y(N)$, it is often useful to compactify the modular curves to give them useful topological properties. This definition involves extending the upper half plane as follows:

Definition 3.1. The **extended complex upper half plane** is $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$.

We want to introduce a topology on $\mathcal{H}^*$ that will then give us a topology for a modular curve. For real $M > 0$, define

$$\mathcal{N}_M = \{\tau \in \mathcal{H} : \Im(\tau) > M\}$$

We then define the topology with the following basis for open sets: we take open sets in $\mathcal{H}$, and sets of the form

$$\alpha(\mathcal{N}_M \cup \{\infty\}) : \alpha \in \mathrm{SL}_2(\mathbb{Z}), M > 0.$$

This allows us to define a topology on modular curves; see [DS, Section 2.1] for more details.

Definition 3.2. The compactification of the modular curves $Y_0(N)$, $Y_1(N)$, and $Y(N)$ is defined as

$$X_0(N) = \Gamma_0(N)\setminus \mathcal{H}^*, X_1(N) = \Gamma_1(N) \setminus \mathcal{H}^*, X(N) = \Gamma(N) \setminus \mathcal{H}^*$$

Notice that this definition is equivalent to defining $X(\Gamma)$ as $Y(\Gamma) \cup \Gamma \setminus \{\mathbb{Q} \cup \infty\}$ for some congruence subgroup Γ. This means $X(\Gamma)$ is $Y(\Gamma)$ with a few extra orbits.

Definition 3.3. The orbits in $\Gamma \setminus \{\mathbb{Q} \cup \infty\}$ are the **cusps** of $X(\Gamma)$.

It turns out that the compactified modular curves $X_0(N)$, $X_1(N)$, and $X(N)$ are compact Riemann surfaces; see [DS, Chapter 2] for a discussion of this.

4. Lattices and Elliptic Curves

In this section, we introduce lattices and describe the maps between them, which will be important for our discussion of the Weierstrass $\wp$-function in section 5. We begin by defining a lattice:

Definition 4.1. A **lattice** is a free abelian group, $\mathbb{Z}\,\omega_1 + \mathbb{Z}\,\omega_2$, where $\omega_1, \omega_2 \in \mathbb{C}$ and satisfy $\mathbb{R}\,\omega_1 + \mathbb{R}\,\omega_2 = \mathbb{C}$.

We can think of a lattice as "tiling" the complex plane into parallelograms.

Example. We can take $\omega_1 = 1$ and $\omega_2 = i$ for an example of the lattice.

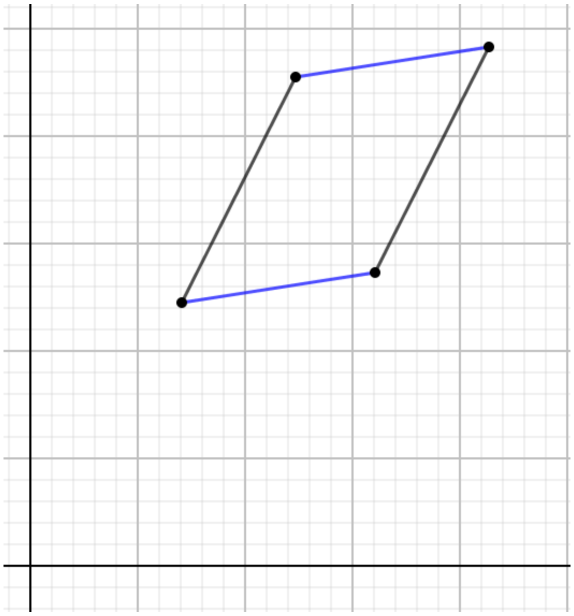

Figure 1. Taking the quotient of the complex plane by a lattice.

Nonexample. $\mathbb{Z}(i+1)+\mathbb{Z}(3i+3)$ would not be an example of a lattice, since $i+1$ and $3i+3$ clearly do not span the complex plane.

Since a lattice is a subgroup of the complex numbers, we can take the quotient group:

Definition 4.2. The quotient group $\mathbb{C}/\Lambda = \{z+\Lambda : z \in \mathbb{C}\}$, where Λ is a lattice, is a **complex torus**.

Remark 4.3. The term "complex torus" comes from the fact that when we take the quotient of the complex plane by the lattice, we consider two points to be the same if their difference is a multiple of ω_1 and ω_2. We can think of a lattice as a tiling of the complex plane into parallelograms, so taking this quotient reduces the complex plane into one of these parallelograms (See Figure 1). We then "fold" the blue edges onto each other and the black edges onto each other, which forms a donut shape or torus.

Since a lattice is a group, we can consider homomorphisms between them. In particular, we have isogenies:

Definition 4.4. A nonzero holomorphic (i.e., complex differentiable) homomorphism of complex tori is called an **isogeny**.

Example. The multiplication by N map,

$$[N] : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda, z+\Lambda \to Nz+\Lambda$$

is an important example of an isogeny. We call the kernel of this map the **group of N-torsion points**.

We can actually characterize all homomorphisms of complex tori with the following proposition:

Proposition 4.5. *Any homomorphism between complex tori $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ is determined by a $\mathbb{C}$-linear map $T : \mathbb{C} \to \mathbb{C}$ that sends $\Lambda \to \Lambda'$.*

Proof. We will sketch the proof; see [DS, Proposition 1.3.2] for more details.

The idea is to lift φ to a map $\widetilde{\varphi} : \mathbb{C} \to \mathbb{C}$ using topology and show that $\widetilde{\varphi}'$ is holomorphic and Λ-periodic, i.e. $\widetilde{\varphi}'(z + \lambda) = \widetilde{\varphi}'(z)$ for any $\lambda \in \Lambda$. This also means that $\widetilde{\varphi}'$ is a bounded function. Liouville's Theorem in complex analysis says that a bounded holomorphic function is constant, so $\widetilde{\varphi}$ must be a linear map $\widetilde{\varphi}(z + \Lambda) = mz + b + \Lambda'$. Using the properties of $\widetilde{\varphi}$, we can also show that $m\Lambda \subseteq \Lambda'$ (which means that the linear map sends $\Lambda \to \Lambda'$). We know that a homomorphism must send the identity to the identity, so $b = 0$, and we are done. □

We can easily conclude the following corollary about isomorphisms of lattices, which are just bijective homomorphisms:

Corollary 4.6. $\mathbb{C}/\Lambda_1 \cong \mathbb{C}/\Lambda_2$ *if and only if there exists* $\alpha \in \mathbb{C}$ *such that* $\alpha\Lambda_1 = \Lambda_2$*.*

Example. The lattice $\mathbb{Z}(i+1)+\mathbb{Z}(i-1)$ is isomorphic to $\mathbb{Z}(-i-3)+\mathbb{Z}(-3i+1)$ by multiplication by $i-2$. On the other hand, the lattice $\mathbb{Z}+\mathbb{Z}(2i)$ is not isomorphic to the lattice $\mathbb{Z}+\mathbb{Z}(i)$.

Proposition 4.7. *For any nontrivial homomorphism between complex tori* $\varphi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$*, we have* $\ker(\varphi) \cong \Lambda_2/T(\Lambda_2)$*, where* T *is the linear map corresponding to* φ*.*

Proof. Let $T(z) = cz$. Then, φ sends $a + \Lambda_1 \mapsto ca + \Lambda_2$. Note that if $a \in \ker(\varphi)$, then $\phi(a + \Lambda_1) = \Lambda_2$, so $ca \in \Lambda_2$. Thus, we can construct a map

$$\phi : \ker(\varphi) \to \Lambda_2/T(\Lambda_1),\ \phi(a + \Lambda_1) = ca + T(\Lambda_1),\ a \in \mathbb{C}$$

and an inverse

$$\psi : \Lambda_2/T(\Lambda_1) \to \ker(\varphi),\ \psi(b + T(\Lambda_1)) = \frac{b}{c} + \Lambda_1,\ b \in \Lambda_2$$

Each of these maps are homomorphisms, and $\psi \circ \phi$ and $\phi \circ \psi$ are clearly the identity maps, so we conclude that $\ker(\varphi) \cong \Lambda_2/T(\Lambda_2)$. □

Taking $\Lambda_1 = \Lambda_2$ and φ to be the multiplication by N map yields the following:

Corollary 4.8. *The* N *torsion group is isomorphic to* $(\frac{1}{N}\Lambda)/\Lambda \cong (\mathbb{Z}/N\mathbb{Z})^2$*, so the set* $\{\frac{\tau}{N}, \frac{1}{N}\}$ *is a basis for this group.*

For a lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, let $\omega = \omega_1/\omega_2$. Then, the lattice defined by $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$ is isomorphic to Λ. This means that we can represent lattices in terms of a single complex number.

5. The Weierstrass $\wp$-function

The key to describing the correspondence between lattices and elliptic curves is the following function:

Definition 5.1. The **Weierstrass $\wp$-function** is defined by

$$\wp(z) = \frac{1}{z} + \sum_{\omega \in \Lambda}{}' \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right), z \in \mathbb{C}, z \notin \Lambda$$

where the primed summation means that we omit 0 in the sum.

It is not immediately obvious that this series actually converges for $z \in \mathbb{C} \setminus \Lambda$. To see this, we can bound the summand:

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{z^2 - 2z\omega}{\omega^2 (z-\omega)^2} \right| < \frac{C_z}{|\omega|^3}$$

for some constant C_z. Since the sum

$$\sum_{\omega \in \Lambda}{}' \frac{1}{\omega^3}$$

does actually converge, this shows that the Weierstrass $\wp$-function converges for $z \in \mathbb{C} \setminus \Lambda$. On the other hand, as $z \to \lambda$ for $\lambda \in \Lambda$, the quantity $|\wp(z)|$ approaches infinity, which is why we sum over $\mathbb{C} \setminus \Lambda$ instead of just $\mathbb{C}$. The points in Λ are called **poles** of the function $\wp(z)$.

We also define the Eisenstein series and other important functions:

Definition 5.2. The **Eisenstein series of weight** k for lattices is the function

$$G_k(\Lambda) = \sum_{\omega \in \Lambda}{}' \frac{1}{\omega^k}, \ k > 2 \text{ even.}$$

Remark 5.3. We specify that k is even because $G_k(\Lambda) = 0$ when k is odd.

Definition 5.4. We define the functions $g_2(\Lambda), g_3(\Lambda)$ by

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

Since isomorphisms of lattices and elliptic curves are equivalence relations, we can consider the equivalence classes of these objects, which we call isomorphism classes. Our goal is to use the Weierstrass $\wp$ function to show that there is a bijection between isomorphism classes of lattices and isomorphisms classes of elliptic curves. We first show the following lemma:

Lemma 5.5. *The Weierstrass $\wp$ function satisfies the following:*

(1) *For $0 < |z| < \inf\{|\omega| : \omega \in \Lambda \setminus \{0\}\}$, we have*

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{n=2 \\ n \equiv 0 \pmod 2}}^{\infty} (n+1) G_{n+2}(\Lambda) z^n$$

(2) *The derivative of $\wp$ satisfies*

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

Proof. (1) When $|z| < |\omega|$, we have

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2} \left(\frac{1}{\left(1 - \frac{z}{\omega}\right)^2} - 1 \right)$$

Notice that the if we differentiate both sides of the geometric series $\frac{1}{1-r} = \sum_{n=0}^{\infty} r^n$, we get the identity $\frac{1}{(1-r)^2} = \sum_{n=0}^{\infty} (n+1) r^n$. Expanding $\left(1 - \frac{z}{\omega}\right)^2$ using this yields:

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2} \left(\sum_{n=0}^{\infty} \frac{(n+1)z^n}{\omega^n} - 1 \right) = \sum_{n=1}^{\infty} \frac{(n+1)z^n}{\omega^{n+2}}$$

We substitute this into the Weirstrass $\wp$-function and switch the double sums:

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda}{}' \sum_{n=1}^{\infty} \frac{(n+1)z^n}{\omega^{n+2}} = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)z^n \sum_{\omega\in\Lambda}{}' \frac{1}{\omega^{n+2}}$$

Since $G_k(\Lambda) = 0$ for odd k, this is equal to

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{n=2 \\ n\equiv 0 \pmod 2}}^{\infty} (n+1)G_{n+2}(\Lambda)z^n$$

as desired.

□

This means that we can construct an elliptic curve with points $(\wp(z), \wp'(z))$, so that it has the equation

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda).$$

It turns out that we can go the other way as well and construct a lattice from an elliptic curve. We first introduce the j-function:

Definition 5.6. Let $G_k(\tau)$ be the Eisenstein series of weight k,

$$G_k(\tau) = \sum_{(c,d)\in\mathbb{Z}^2}{}' \frac{1}{(c\tau+d)^k}.$$

for an even integer k. We define the functions

$$g_2(\tau) = 60G_4(\tau), g_3(\tau) = 140G_6(\tau)$$

The **j-function** is the function

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

Lemma 5.7. *Let $y^2 = 4x^3 - a_2x - a_3$ be an elliptic curve. Then, there is a lattice Λ such that $a_2 = g_2(\Lambda)$ and $a_3 = g_3(\Lambda)$.*

Proof. We will provide a sketch of the proof; see [DS, Proposition 1.4.3] for more details.

The main idea is that the j-function is surjective on the complex plane, so there is some $\tau \in \mathbb{C}$ such that

$$j(\tau) = 1728\frac{a_2^3}{a_2^3 - a_3^2}$$

This means that

$$\frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2} = \frac{a_2^3}{a_2^3 - 27a_3^2}$$

Clearing denominators, we have

$$a_2^3g_2^3(\tau) - 27a_2^3g_3^2(\tau) = a_2^3g_2^3(\tau) - 27a_3^2g_2^3(\tau)$$

Simplifying yields

$$\frac{a_2^3(\tau)}{g_2^3(\tau)} = \frac{a_3^2(\tau)}{g_3^2(\tau)} \tag{1}$$

For any $\omega_2 \in \mathbb{C}$, let $\omega_1 = \tau\omega_2$ and $\Lambda = \omega_1 \mathbb{Z} + \omega_2 \mathbb{Z}$. We can show that

$$g_2(\Lambda) = \omega_2^{-4} g_2(\tau), g_3(\Lambda) = \omega_2^{-6} g_3(\tau)$$

We want to find ω_1 and ω_2 satisfying

$$\omega_2^{-4} = \frac{a_2}{g_2(\tau)}, \omega_2^{-6} = \frac{a_3}{g_3(\tau)}$$

By 1, we have

$$\omega_2^{-12} = \frac{a_2^3}{g_2^3(\tau)} = \frac{a_3^2}{g_3^2(\tau)}$$

This means that $\omega_2^{-6} = \pm\frac{a_3}{g_3(\tau)}$, so we can choose either ω_2 or $i\omega_2$. Thus, we have constructed a lattice Λ such that $a_2 = g_2(\Lambda)$ and $a_3 = g_3(\Lambda)$.

□

Theorem 5.8. *There is a bijection between isomorphism classes of lattices and isomorphism classes of elliptic curves of the form $y^2 = 4x^3 - a_2x - a_3$, where $a_2^3 - 27a_3^2 \neq 0$. The correspondence is given by $a_2 = g_2(\Lambda), a_3 = g_3(\Lambda)$.*

Proof. This result follows from Lemmas 5.5 and 5.7. □

6. Parameterization of Elliptic Curves

In this section, we show that the curves $X_0(N)$, $X_1(N)$, and $X(N)$ parameterize isomorphism classes of elliptic curves along with additional data about cyclic subgroups with order N, points of order N, and bases of the N-torsion subgroup, respectively. We start with defining a bijection between elliptic curves and orbits of $\mathrm{SL}_2(\mathbb{Z})/\mathcal{H}$:

Proposition 6.1. *Let E_τ denote the elliptic curve associated to Λ_τ. Then, $E_{\tau_1} \cong E_{\tau_2}$ if and only if there exists $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau_1 = g(\tau_2)$. This yields a natural bijection between isomorphism classes of elliptic curves and orbits $\mathrm{SL}_2(\mathbb{Z})/\mathcal{H}$.*

Proof. Suppose $E_{\tau_1} \cong E_{\tau_2}$; we want to show that there is some $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau_1 = g(\tau_2)$. By Corollary 4.6, we know that there is some $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_{\tau_1} = \Lambda_{\tau_2}$. This means that $\alpha \cdot \tau_1 = a\tau_2 + b$ and $\alpha \cdot 1 = c\tau_2 + d$ for some $a, b, c, d \in \mathbb{Z}$.

Now suppose there is some $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau_1 = g(\tau_2)$; we want to show that $E_{\tau_1} \cong E_{\tau_1}$. □

We now begin to describe the relationship between points on modular curves and isomorphism classes of elliptic curves. For an elliptic curve E_τ corresponding to the lattice $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, define P_τ and Q_τ as the points corresponding to $\frac{1}{N}$ and $\frac{\tau}{N}$, respectively. Additionally, let C_τ be the cyclic subgroup of order N generated by P_τ. Then we have the following lemma:

Lemma 6.2. *Let E be an elliptic curve over $\mathbb{C}$. If P is a point on E with order N, then there exists $\tau \in \mathcal{H}$ such that $(E, P) \cong (E_\tau, P_\tau)$. Furthermore, if C is a cyclic subgroup of E with order N, then there exists $\tau \in \mathcal{H}$ such that $(E, C) \cong (E_\tau, C_\tau)$.*

Proof. We present the proof from [Ste03, Proposition 1.4.5].

We write $E = \mathbb{C}/\Lambda$, where the lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, and $\frac{\omega_1}{\omega_2} \in \mathcal{H}$. Let $P = \frac{a\omega_1}{N} + \frac{b\omega_2}{N}$ be a point of order N. Then, we claim that $\gcd(a, b, N) = 1$: otherwise, we would be able to write $P = \frac{a'\omega_1}{N'} + \frac{b'\omega_2}{N'}$ for some $N' < N$, so P would not have order N. Notice that we can also assume WLOG that $\gcd(a, b) = 1$, since we can add multiples of N to a and b until they satisfy this condition.

Since a and b are relatively prime, we can find some $c, d \in \mathbb{Z}$ such that $ad - bc = 1$. This means that the complex numbers

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

form a basis for Λ. Let $\tau = \frac{\omega_2'}{\omega_1'}$ (we can replace ω_2 with $-\omega_2$ if necessary to ensure that $\tau \in \mathcal{H}$). Thus, we have an isomorphism from $\Lambda \to \Lambda_\tau$ defined by

$$\omega_1' = a\omega_1 + b\omega_2 \mapsto 1, \omega_2' = c\omega_1 + d\omega_2 \mapsto \tau = \frac{c\omega_1 + d\omega_2}{a\omega_1 + b\omega_2}$$

We can see that this isomorphism is division by ω_1', so it sends $\frac{a\omega_1}{N} + \frac{b\omega_2}{N}$ to $\frac{1}{N}$. This means that $P \mapsto P_\tau$, so $(E, P) \cong (E_\tau, P_\tau)$ as desired.

We can deduce the second part of the lemma from the first part of the lemma. If the cyclic subgroup C is generated by a point P of order P, we can find $\tau \in \mathcal{H}$ such that $(E, P) \cong (E_\tau, P_\tau)$. Since C_τ is generated by the point $\frac{1}{N}$, this isomorphism also maps C to C_τ, so we are done. □

Now that we know that every pair (E, C) is isomorphic to a pair (E_τ, C_τ) with the extra condition that C_τ is generated by $P_\tau = \frac{1}{N}$ (and vice versa for points P of order N), we can characterize the correspondence between points on modular curves and isomorphism classes of elliptic curves in terms of the specific group C_τ and the specific point P_τ.

Lemma 6.3. *A pair (E_τ, C_τ) is isomorphic to a pair $(E_{\tau'}, C_{\tau'})$ iff there exists $g \in \Gamma_0(N)$ such that $g(\tau) = \tau'$. Analogously, a pair (E_τ, P_τ) is isomorphic to a pair $(E_{\tau'}, P_{\tau'})$ iff there exists $g \in \Gamma_1(N)$ such that $g(\tau) = \tau'$.*

Proof. We prove the first statement; the proof of the second statement is analogous.

Suppose $(E_\tau, C_\tau) \cong (E_{\tau'}, C_{\tau'})$. Then, there exists some $\lambda \in \mathbb{C}$ satisfying $\lambda\Lambda_\tau = \Lambda_{\tau'}$. We can thus write

$$\lambda\tau = a\tau' + b, \lambda \cdot 1 = c\tau' + d \tag{2}$$

for some $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. We want to show that $\gamma \in \Gamma_0(N)$, i.e. $c \equiv 0 \pmod{N}$.

If we divide the second equation of 2 by N, we get $\frac{\lambda \cdot 1}{N} = \frac{c}{N}\tau' + \frac{d}{N}$. We assumed that $(E_\tau, C_\tau) \cong (E_{\tau'}, C_{\tau'})$, so $\frac{c}{N}\tau' + \frac{d}{N}$ must be an element of $\Lambda_\tau = \mathbb{Z}\tau' + \frac{1}{N}\mathbb{Z}$. We conclude that $c \equiv 0 \pmod{N}$, and $\gamma \in \Gamma_0(N)$.

Now suppose that there exists some $g \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$ such that $g(\tau) = \tau'$. Then, if $c \equiv 0 \pmod{N}$, then $\frac{c}{N}\tau' + \frac{d}{N} \in \Lambda_{\tau'}$. Let $\alpha = c\tau' + d$; then, $\tau'\alpha = a\tau' + b$. Then, the complex number α defines an isomorphism between E_τ and $E_{\tau'}$ that sends C to C', as desired. □

It turns out that the modular curves $X_0(N)$, $X_1(N)$, and $X(N)$ will give us three ways to parameterize elliptic curves. We have already shown a correspondence between points on $X_0(N)$ and pairs (E, C), where C is a cyclic subgroup of E with order N; and a correspondence between points on $X_1(N)$ for pairs (E, P) where P is a point on E with order N. The parametrization of elliptic curves using points on $X(N)$ will use the following map known as the Weil pairing.

Definition 6.4. Let E be an elliptic curve corresponding to the lattice $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$. The **Weil pairing** is a map $e : E[N] \times E[N] \to \mathbb{Z}/N\mathbb{Z}$ defined by $e(P, Q) = ad - bc$, where $P = a\tau/N + b \cdot 1/N$ and $Q = c\tau/N + d \cdot 1/N$.

Remark 6.5. The Weil pairing is very important in number theory and algebraic geometry, and also has practical applications to elliptic curve cryptography and identity-based encryption.

Example. Let P_τ and Q_τ be the points on E corresponding to $\frac{1}{N}$ and $\frac{\tau}{N}$, respectively. Then, $e(P_\tau, Q_\tau) = -1$.

We can prove an analog of Lemmas 6.2 and 6.3 for the Weil pairing:

Lemma 6.6. *If P and Q form a basis for $E[N]$ with $e(P, Q) = -1$, then there exists $\tau \in \mathcal{H}$ such that $(E, P, Q) \cong (E_\tau, P_\tau, Q_\tau)$. Furthermore, $(E_\tau, P_\tau, Q_\tau) \cong (E_{\tau'}, P_{\tau'}, Q_{\tau'})$ iff there is some $g \in \Gamma(N)$such that $\gamma(\tau) = \tau'$.*

Proof. The proof is analogous to that of Lemmas 6.2 and 6.3, so we skip it. □

Combining Lemmas 6.2, 6.3, and 6.6, we have the following summary of these results:

Theorem 6.7.
(1) *The non-cuspidal points of $X_0(N)$ correspond to isomorphism classes of pairs (E, C), where E is an elliptic curve and C is a cyclic subgroup of E with order N. Two pairs (E, C) and (E, C') are isomorphic if there is an isomorphism $\varphi : E \to E'$ such that $\varphi(C) = C'$.*
(2) *The non-cuspidal points of $X_1(N)$ correspond to pairs (E, P), where E is an elliptic curve and P is a point of E with order N. Two pairs (E, P) and (E, P') are isomorphic if there is an isomorphism $\varphi : E \to E'$ such that $\varphi(P) = P'$.*
(3) *The non-cuspidal points of X_N correspond to triples (E, P, Q), where E is an elliptic curve and P, Q form a basis of $E[N]$ such that $e(P, Q) = -1 \in \mathbb{Z}/N\mathbb{Z}$. Two triples (E, P, Q) and (E, P', Q') are isomorphic if there is an isomorphism $\varphi : E \to E'$ such that $\varphi(P) = P'$ and $\varphi(Q) = Q'$.*

This theorem is useful in number theory because we can analyze modular curves in order to prove statements about elliptic curves. One of the most famous examples of this is a theorem due to Mazur and Tate:

Theorem 6.8 (Mazur–Tate)**.** *No elliptic curve over $\mathbb{Q}$ has a rational point of order 13.*

Proof. Note that this statement is equivalent to saying that there are no rational points on the modular curve $X_1(13)$ besides the cusps. We refer the reader to [MT73] for the proof. □

7. Modular Curves as Algebraic Curves

It turns out that we can also define modular curves as algebraic curves (so as solutions to systems of polynomials in multiple variables). In this section, we will briefly outline some of the properties of modular curves when viewed this way. See [DS, Chapter 7] for a more detailed and advanced discussion of this theory.

We start by discussing the cusps of the modular curve.

Proposition 7.1. *The modular curve $X(1) = \mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H}^*$ has one cusp. For any congruence subgroup $\Gamma \in \mathrm{SL}_2(\mathbb{Z})$, $X(\Gamma)$ has finitely many cusps.*

Proof. See [DS, Lemma 2.4.1] for a proof. □

Recall that we can also construct rings and fields from curves:

Definition 7.2. The **coordinate ring** of an algebraic set C over a field k is the ring

$$\overline{k}[C] = \overline{k}[x_1, x_2, \ldots, x_n]/I(C)$$

where $\overline{k}$ is the algebraic closure of k, and $I(C)$ is the ideal

$$\{p \in \overline{k}[x_1, x_2, \ldots, x_n] : p(a_1, a_2, \ldots, a_n) = 0 \; \forall (a_1, a_2, \ldots, a_n) \in C\}$$

We will sometimes denote this ring $\mathcal{O}(C)$. An element of this ring is called a **polynomial function on** C.

Definition 7.3. The **function field** of an algebraic set C is the fraction field of the coordinate ring,

$$\overline{k}(C) = \left\{ \frac{f}{g} : f, g \in \overline{k}[C], g \neq 0 \right\}$$

An element of this field is called a **rational function on** C.

We can actually describe the function field of $X(1) = X(\mathrm{SL}_2(\mathbb{Z})$ explicitly in terms of the modular invariant:

Proposition 7.4. *The function field* $\mathbb{C}(X(1))$ *is generated by the modular invariant, i.e.* $\mathbb{C}(X(1)) = \mathbb{C}(j)$.

We also have the following interesting result:

Theorem 7.5. *The field extension* $\mathbb{C}(X(N))/\,\mathbb{C}(X(1))$ *is Galois with Galois group* $\mathrm{SL}_2(\mathbb{Z}\,/N\,\mathbb{Z})/\{\pm I\}$, *where* I *is the identity matrix.*

We refer the reader to Section 7.5 of [DS] for the proofs of these results.

References

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

[MT73] Barry Mazur and John Tate. Points of order 13 on elliptic curves. *Inventiones mathematicae*, 22(1):41–49, 1973.

[Ste03] William Stein. Points on modular curves parameterize elliptic curves with extra structure, 2003.