MODULAR CURVES

CHRISTIAN ZHOU-ZHENG

1. Introduction

The study of modular curves lies at the intersection of complex analysis, algebraic geometry, and number theory. These mathematical objects arise naturally when investigating the relationship between lattices and elliptic functions, as in Chapter 13 of the textbook [2]. This paper aims to explain the basics of modular curves and their interpretation as *moduli spaces*, spaces where each point represents a class of mathematical objects.

2. Preliminaries

2.1. **Riemann spaces.** Recall that a Riemann surface is a one-dimensional complex manifold: a surface that locally resembles the complex plane and where transition maps between local coordinates are holomorphic. Prototypical examples include the complex plane $\mathbb{C}$, the upper half-plane $\mathbb{H}$, and the Riemann sphere $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$.

2.2. **Elliptic curves.** You may recall an aside from Chapter 13 of the textbook [2] that mentioned complex tori as being elliptic curves. We will explore that aside in more depth later, but first it stands to define what an elliptic curve even is. We restrict our definition to $\mathbb{C}$ for simplicity, which fortunately also works over $\mathbb{R}$ for purposes of visualization.

Definition 1. An *elliptic curve* is a smooth curve defined by the zero set of the equation

$$y^2 = x^3 + bx + c \tag{1}$$

equipped with a distinguished ”point at infinity” $\mathcal{O}$ and a group structure.

This is a very informal definition of an elliptic curve; see [3] for the formal version, as the algebraic geometry perspective on elliptic curves is also rather fascinating. Unfortunately we do not have the space here to do it justice.

It is easy to visualize an elliptic curve over $\mathbb{R}$: simply plug it into your preferred graphing software. It is not very different over $\mathbb{C}$. The group structure and ”point at infinity” are harder to comprehend, but they are as follows:

Construction. The point at infinity $\mathcal{O}$ is such that any two parallel lines intersect at it, so that in particular any two lines in the plane intersect at exactly one point.

Let $\oplus$ denote the group operation, with $\mathcal{O}$ the identity element. To add points p, q on an elliptic curve E over $\mathbb{C}$, find the line running through p and q if $p \neq q$ or the tangent line to E at p if $p = q$. It can be shown that this line intersects E at exactly one other point (possibly $\mathcal{O}$). The negation of this third intersection point is then $p \oplus q$, where $(x, -y)$ is the negation of (x, y), since the curve is symmetric about the x-axis (note that this definition of negation is consistent with the identity $p - p = p + (-p) = \mathcal{O}$). See Figure 1.

Date: June 8, 2025.

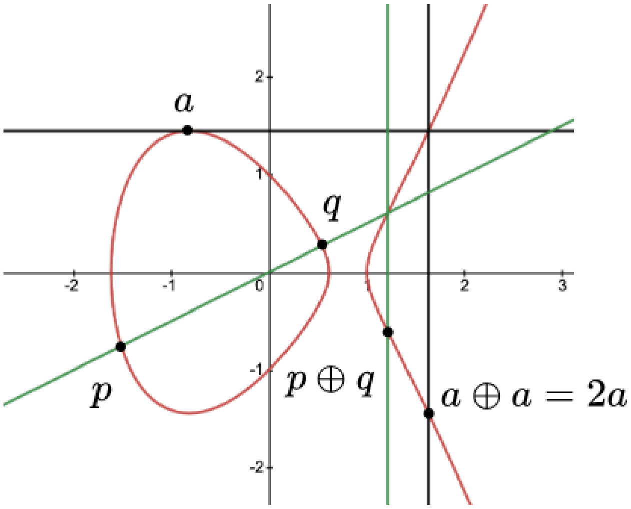

Figure 1. The group operation on an elliptic curve over $\mathbb{R}$.

Exercise 1. Verify that the above construction defines a group. You may take the fact that a line intersects E at exactly three points to be given; it is a corollary of Bézout's theorem and requires the full projective-geometry definition of an elliptic curve to be applied.

We finally care about ways to classify elliptic curves up to their structure, though in a weaker way than strict isomorphisms. Elliptic curves admit a notion called an *isogeny* for this:

Definition 2. Let E_1, E_2 be elliptic curves over $\mathbb{C}$. A nonconstant rational group homomorphism $\phi : E_1 \to E_2$ is called an *isogeny*, and E_1 and E_2 are *isogenous.*

Crucially, isogenies can have nontrivial kernels, so that they need not be injective. Despite this, isogeny defines an equivalence relation on the class of elliptic curves:

Proposition 3. *If there exists an isogeny $\phi : E_1 \to E_2$, then there exists an isogeny $\widehat{\phi} : E_2 \to E_1$ called the* dual isogeny*.*

Proof. See [3]. ■

Corollary 4. *Isogeny defines an equivalence relation on elliptic curves.*

Elliptic curves can in fact be defined over any field, including finite fields $\mathbb{F}_q$ and the rationals $\mathbb{Q}$. Their existence combines algebraic geometry, number theory, and complex analysis in surprising ways—you may vaguely know them as complex tori, or being related somehow to Wiles's proof of Fermat's Last Theorem, or from the elliptic-curve cryptographic protocols that protect apps like WhatsApp Messenger. Elliptic curves are a fascinating topic of study in their own right, but the point of this discussion is merely to motivate what elliptic curves are and why we will care about them shortly.

3. Lattices

To motivate our discussion, recall complex lattices:

Definition 5. A lattice Λ in $\mathbb{C}$ is a discrete subgroup of the form $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, where ω_1 and ω_2 are $\mathbb{R}$-linearly independent complex numbers.

Definition 6. We say that lattices Λ and Λ' are *homothetic* if there exists a complex number m such that $\Lambda = m\Lambda'$, i.e. they are equivalent up to scaling and rotation.

Clearly the above defines an equivalence relation on lattices. Up to homothety, we can thus rotate and scale any lattice to the normalized form $\Lambda_\tau = \{m + n\tau : m, n \in \mathbb{Z}\}$, where $\tau \in \mathbb{H}$, by setting $\tau = \omega_2/\omega_1$. Hence we can associate lattices with points $\tau \in \mathbb{H}$. However, this association is not unique: different values of τ can generate homothetic lattices. In particular, the lattices Λ_τ, $\Lambda_{\tau+1}$, and $\Lambda_{-1/\tau}$ are homothetic. Indeed:

- $\Lambda_{\tau+1} = \{m + n(\tau + 1) : m, n \in \mathbb{Z}\} = \{(m + n) + n\tau : m, n \in \mathbb{Z}\} = \Lambda_\tau$.
- $\Lambda_{-1/\tau} = \{m + n(-1/\tau) : m, n \in \mathbb{Z}\}$. Setting $m' = -n$ and $n' = m$, we get $\Lambda_{-1/\tau} = \{-n' + m'(-1/\tau) : m', n' \in \mathbb{Z}\} = \{-n' - m'/\tau : m', n' \in \mathbb{Z}\} = -\frac{1}{\tau}\{n'\tau + m' : m', n' \in \mathbb{Z}\} = -\frac{1}{\tau}\Lambda_\tau$. Thus, $\Lambda_{-1/\tau}$ is a scalar multiple of Λ_τ.

Consider then the transformations $\tau \mapsto \tau + 1$ and $\tau \mapsto -1/\tau$. We can associate transformations on the complex plane with 2×2 matrices, such that $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ acts on τ by the Möbius transformation:

$$\tau' = \gamma \cdot \tau = \frac{a\tau + b}{c\tau + d}. \tag{2}$$

We can then characterize the matrices that correspond to certain transformations on lattices.

Definition 7. The *modular group* consists of all 2×2 matrices with integer entries and determinant 1:

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ab - cd = 1 \right\}$$

By the notation of Equation 2, $\tau \mapsto \tau + 1$ and $\tau \mapsto -1/\tau$ are respectively $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. In fact, they generate $\mathrm{SL}_2(\mathbb{Z})$, which was the point of the motivation.

Exercise 2. Show that $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ generate $\mathrm{SL}_2(\mathbb{Z})$.

Exercise 3. Show that two lattices Λ_τ and $\Lambda_{\tau'}$ are homothetic if and only if $\tau' = \gamma \cdot \tau$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. (This is basically Problem 8, Chapter 13 of [2].)

Recall the earlier discussion of associating lattices to points $\tau \in \mathbb{H}$; now we can identify those τ with points τ' satisfying Equation 2 to form a space that can be thought of as classifying lattices up to homothety. By Exercise 3, this is in fact the quotient group $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$. Keep this in mind; we will return to this structure shortly.

3.1. Complex tori.

Before we go any deeper, we ought to take a brief detour to discuss how else lattices are topical. Naturally, the quotient $\mathbb{C}/\Lambda$ is a torus, formed by gluing together opposite edges of the fundamental parallelogram. However, every torus formed by a quotient of $\mathbb{C}$ by some lattice is isomorphic; the group structure does not in fact depend on the underlying lattice.

Exercise 4. Prove that $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$ with the obvious group operations for lattices Λ, Λ'.

Since the groups on any two complex tori (which we can now identify with lattices) are isomorphic, the classification of lattices we were doing in the previous section was certainly not up to group isomorphism of the corresponding tori. So what was it? It turns out that homothety of lattices is an equivalent condition to *holomorphic* group isomorphism, i.e. the group isomorphism between the tori is holomorphic:

Theorem 8. *Let Λ, Λ' be lattices. There exists a holomorphic group homomorphism between the complex tori $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ if and only if Λ and Λ' are homothetic.*

Proof.

$\Longrightarrow$: Suppose $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ is a holomorphic group homomorphism. By the lifting property of covering maps, there exists a holomorphic map $F : \mathbb{C} \to \mathbb{C}$ such that $F(0) = 0$ and $f(z + \Lambda) = F(z) + \Lambda'$ for all $z \in \mathbb{C}$. Since f is a group homomorphism, $F(z + w) + \Lambda' = F(z) + F(w) + \Lambda'$. This implies $F(z + w) - F(z) - F(w) \in \Lambda'$ for all $z, w \in \mathbb{C}$. Since F is continuous and Λ' is discrete, we must have $F(z + w) = F(z) + F(w)$ for all $z, w \in \mathbb{C}$. Thus since $F : \mathbb{C} \to \mathbb{C}$ is holomorphic, additive, and $F(0) = 0$, it is linear: $F(z) = \alpha z$ for some $\alpha \in \mathbb{C}$.

For f to be well-defined, we need $F(\omega) \in \Lambda'$ for all $\omega \in \Lambda$. This gives us $\alpha\omega \in \Lambda'$ for all $\omega \in \Lambda$, so $\alpha\Lambda \subseteq \Lambda'$. Since f is a homomorphism between tori of the same dimension and is holomorphic (hence continuous), and both quotient spaces are compact, f is surjective. This means $F(\mathbb{C}) + \Lambda' = \mathbb{C} + \Lambda' = \mathbb{C}/\Lambda'$, which implies that $\alpha\Lambda + \Lambda' = \Lambda'$. Combined with $\alpha\Lambda \subseteq \Lambda'$, we get $\alpha\Lambda = \Lambda'$ (since both are lattices of the same rank). Therefore Λ' and Λ are homothetic.

$\Longleftarrow$: Suppose $\Lambda' = \alpha\Lambda$ for some $\alpha \in \mathbb{C} \setminus \{0\}$. Define $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ by $f(z + \Lambda) = \alpha z + \Lambda'$. Since this is induced by multiplication, it is holomorphic, and it is easily checked that it is a homomorphism and well-defined. The inverse is given by multiplication by α^{-1}. ■

You may also remember that lattices correspond to a particular elliptic function, the Weierstraß $\wp$-function:

Definition 9. Given a lattice Λ, the Weierstraß $\wp$-function is defined as

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

As it's elliptic, it's doubly periodic:

Theorem 10 (Theorem 3.3, Chapter 13, [2])**.** *The $\wp$ function and its derivative are doubly periodic with periods ω_1, ω_2 of the lattice.*

Hence we may define a map $\varphi : z \mapsto (\wp(z), \wp'(z))$ from the torus $\mathbb{C}/\Lambda$ to $\mathbb{C}^2$. This map turns out to be a bijection that maps the torus to an elliptic curve over $\mathbb{C}$, thanks to the differential equation satisfied by the $\wp$ function:

Theorem 11 (Theorem 3.5, Chapter 13, [2])**.** *There exist $b, c \in \mathbb{C}$ such that*

$$\wp'(z)^2 = 4\wp(z)^3 + b\wp(z) + c \tag{4}$$

for any $z \in \mathbb{C}/\Lambda$.

Hence every complex torus corresponds to an elliptic curve. Furthermore, it can be shown that the converse holds, i.e. every elliptic curve corresponds to a complex torus that gives the curve as its image [1]. Thus the map φ is a bijection between the class of complex tori and the class of complex elliptic curves. Wouldn't it be nice if, in the spirit of Theorem 8, this preserved holomorphic group homomorphism on those complex tori? Indeed it does:

Theorem 12. *Let $E_\Lambda, E_{\Lambda'}$ be elliptic curves corresponding to the tori $\mathbb{C}/\Lambda, \mathbb{C}/\Lambda'$. E_Λ and $E_{\Lambda'}$ are isogenous if and only if there exists a holomorphic group homomorphism from $\mathbb{C}/\Lambda$ to $\mathbb{C}/\Lambda'$, or equivalently, Λ and Λ' are homothetic.*

Proof.

$\Longleftarrow$: Suppose there exists a holomorphic group homomorphism $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$. By Theorem 8, this occurs if and only if Λ and Λ' are homothetic. The holomorphic group homomorphism ϕ induces a rational map between the elliptic curves that preserves the group structure. Specifically, if ϕ lifts to the map $F(z) = \alpha z$ on $\mathbb{C}$, then the induced map on elliptic curves is given by $(x, y) \mapsto (\alpha^{-4}x, \alpha^{-6}y)$ using the transformation properties of the Weierstrass function under scaling [2]. This gives an isogeny between E_Λ and $E_{\Lambda'}$.

$\Longrightarrow$: Suppose E_Λ and $E_{\Lambda'}$ are isogenous via an isogeny $\psi : E_\Lambda \to E_{\Lambda'}$. Since isogeny is an equivalence relation, there exists a dual isogeny $\hat{\psi} : E_{\Lambda'} \to E_\Lambda$. The isogeny ψ corresponds to a holomorphic map between the Riemann surfaces, and since both curves are parametrized by their respective tori via the Weierstrass function, this induces a holomorphic map $\tilde{\psi} : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$. To see that $\tilde{\psi}$ is a group homomorphism, note that the group law on the elliptic curve corresponds exactly to the addition law on the torus $\mathbb{C}/\Lambda$, and isogenies preserve the group structure by definition. Therefore $\tilde{\psi}$ is a holomorphic group homomorphism between tori. ■

4. Congruence subgroups

In the last section, we came up with a way of classifying lattices up to homothety via points in $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$. However, homothety is a pretty blunt tool, so it is of greater interest to classify lattices up to more nuanced relations. Fortunately, we can apply most of the same logic by taking the quotient of $\mathbb{H}$ by *subgroups* of $\mathrm{SL}_2(\mathbb{Z})$, where the choice of subgroup determines the structure of the quotient group. Naturally, some quotients are more interesting than others, and some simpler than others. We will examine some of the more interesting but also more elementary quotients, so we must first define the subgroups of interest:

Definition 13. For an integer $N \geq 1$, the *principal congruence subgroup of level* N is defined as

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\} \tag{5}$$

where congruence is performed entry-wise.

Definition 14. For an integer $N \geq 1$, a *congruence subgroup of level* N is a subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ that contain the principal congruence subgroup of level N, i.e. $\Gamma(N) \subset \Gamma$. Important examples include:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\} \tag{6}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\} \tag{7}$$

where the asterisk indicates no restriction.

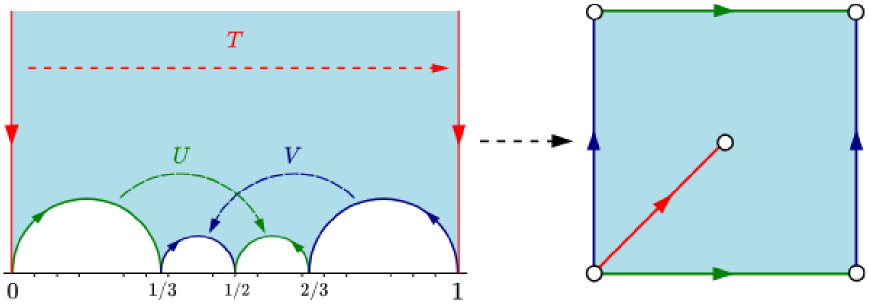

Figure 2. A fundamental domain for $\mathbb{H}/\Gamma_0(11)$ and the quotient space as a flattened torus. T, U, V correspond to the actions of the generators of $\Gamma_0(11)$.

The quotient $\mathbb{H}/\Gamma(N)$ is defined in the same way as $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$; the reader should verify that pretty much everything works the same as modulo $\mathrm{SL}_2(\mathbb{Z})$.

Example. This example is adapted from [4]. $\Gamma_0(11)$ is generated by the set of matrices

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad U = \begin{pmatrix} 7 & -2 \\ 11 & -3 \end{pmatrix} \quad V = \begin{pmatrix} 8 & -3 \\ 11 & -4 \end{pmatrix}.$$

Figure 2 shows a fundamental domain for $\mathbb{H}/\Gamma_0(11)$ in blue, and we see that (after identifying edges) it forms a torus with two punctured holes. If we added those holes, we would get a compact Riemann surface. We don't have the machinery to do so here, but the reader may see [1] or [4].

Definition 15. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The group $\mathbb{H}/\Gamma$ is a *modular curve.*

We established previously that lattices are complex tori are elliptic curves. What classes of elliptic curves do $\Gamma_0(N)$ and $\Gamma_1(N)$ parametrize? The following is adapted from [1] due to the unwieldy lengths of the proofs, and proofs can be found therein.

Definition 16. An *enhanced curve* for $\Gamma_0(N)$ is a pair (E, C) where E is a complex elliptic curve and C is a cyclic subgroup of E (recall the group structure on E) of order N. Two such pairs (E, C) and (E', C') are said to be *isomorphic* if there exists an isomorphism $\phi : E \to E'$ such that $\phi(C) = C'$. This defines an equivalence relation on enhanced elliptic curves for $\Gamma_0(N)$. Let $S_0(N)$ denote the quotient set of enhanced elliptic curves for $\Gamma_0(N)$ under this relation.

Proposition 17. *Every point in $\mathbb{H}/\Gamma_0(N)$ represents a unique element of $S_0(N)$.*

So the modular curve that arises from $\Gamma_0(N)$ parametrizes pairs (E, C) of elliptic curves and order-N cyclic subgroups. What about $\Gamma_1(N)$? It turns out it's the same, but order-N *points* instead of cyclic subgroups:

Definition 18. An *enhanced curve* for $\Gamma_1(N)$ is a pair (E, p) where E is a complex elliptic curve and $p \in E$ is a point of order N. Two such pairs (E, p) and (E', p') are said to be *isomorphic* if there exists an isomorphism $\phi : E \to E'$ such that $\phi(p) = p'$. This defines an equivalence relation on enhanced elliptic curves for $\Gamma_1(N)$. Let $S_1(N)$ denote the quotient set of enhanced elliptic curves for $\Gamma_1(N)$ under this relation.

Proposition 19. *Every point in $\mathbb{H}/\Gamma_1(N)$ represents a unique element of $S_1(N)$.*

References

[1] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Graduate Texts in Mathematics. Springer, New York, NY, 1st edition, 2010.

[2] S. Rubinstein-Salzedo. *Complex Analysis*. Euler Circle, Palo Alto, CA, 2024.

[3] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 2009.

[4] T. Weston. The modular curves $X_0(11)$ and $X_1(11)$. Arizona Winter School 2001, 2001.