A BEGINNER'S GUIDE TO MODULAR CURVES

ALY SOLIMAN

Abstract. In this expository paper, we introduce modular curves to a reader with no prior exposure to the topic. The aim is to motivate the basic concepts and give some concrete examples.

Contents

1. Introduction 1
2. Algebraic Plane Curves 2
2.1. Basic definitions 2
2.2. Elliptic curves 4
3. Riemann Surfaces 6
4. Quotient Spaces 8
5. Complex Tori 9
5.1. Construction of Complex tori 9
5.2. Elliptic Curves as Complex Tori 11
6. Quotients of $\mathbb{H}$ 12
6.1. The modular group 12
6.2. Congruence subgroups 15
7. Modular Curves 17
7.1. The extended upper half plane 17
7.2. The topology on $X(\Gamma)$ 19
7.3. Elliptic points 21
Acknowledgments 25
References 25

1. Introduction

A moduli space is a space where each point represents a class of algebraic or geometric objects — this is a fundamental concept in algebraic geometry. Our aim is to introduce the analytic definition of modular curves, which are surfaces where points represent classes of elliptic curves up to some notion of isomorphism. This is an important example of a moduli space.

In section 2, we briefly introduce algebraic plane curves and define elliptic curves. In section 3, we review some definitions about manifolds and define Riemann surfaces. In section 5, we define complex tori, which are Riemann surfaces that can be

identified with elliptic curves. In sections 6 and 7, we define modular curves as compact Riemann surfaces where points represent isomorphism classes of elliptic curves.

The reader is assumed to have some background in analysis and point-set topology but very little knowledge in algebra is assumed.

2. Algebraic Plane Curves

2.1. **Basic definitions.** Throughout this section, k will denote an arbitrary field — usually taken to be $\mathbb{R}$ or $\mathbb{C}$.

Definition 2.1. In algebraic geometry, the n-Cartesian product of k is referred to as the *n-affine space* over k and is denoted as $\mathbb{A}_k^n$.

Definition 2.2. Let P be a polynomial of degree n in two variables over k. An *affine plane curve C of degree n* is the zero set

$$C = \{(x, y) \in \mathbb{A}_k^2 \mid P(x, y) = 0\}. \tag{2.3}$$

It is a curve that lives in the *affine plane* $\mathbb{A}_k^2$.

Definition 2.4. We can define polynomial differentiation over any field by following the usual differentiation rules from calculus over the reals. In particular, we set

$$\frac{\partial}{\partial x}[x^n] = nx^{n-1}, \tag{2.5}$$

for integers $n \geq 1$, and extend the definition of $\partial/\partial x$ to any polynomial by linearity.

Definition 2.6. Let an affine plane curve C be the zero set of a polynomial P. Then a point $p = (x, y)$ on C is said to be *singular* if

$$\frac{\partial P}{\partial x} = \frac{\partial P}{\partial y} = 0. \tag{2.7}$$

If none of the points on a curve are singular then it is said to be *smooth*.

Example 2.8. Figures 1 and 2 display the smooth real curves $2x^3 + 7y^2 + 1 = 0$ and $2x^2 + 2y^2 = 1$ respectively.

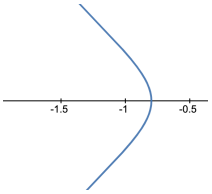


Figure 1

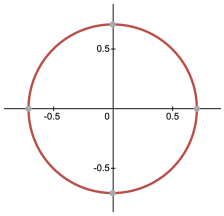


Figure 2

Non-Example 2.9. Figures 3 and 4 display the non-smooth real curves $y^3 = x^2$ and $x^2 = y^2 + x^3$ respectively. Both curves are singular at $(0, 0)$.

Definition 2.10. We can identify points $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{A}_k^n$ if there's some nonzero $\lambda \in k$ such that $x_i = \lambda y_i$ for all $i = 1, \ldots, n$. This defines

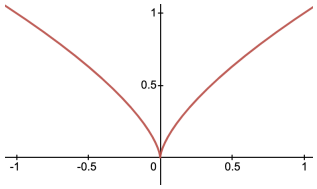


FIGURE 3

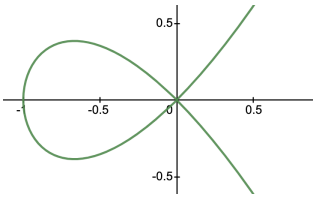


FIGURE 4

an equivalence relation. Let $(x) = (x_1 : \ldots : x_n)$ denote the equivalence class of a point $x = (x_1, \ldots, x_n)$ under this relation. The *n-projective space* is defined as

$$\mathbb{P}_k^n = \{(x) \mid \text{nonzero points } x \in \mathbb{A}_k^{n+1}\}. \tag{2.11}$$

If we fix some nonzero $z \in k$ then the set $\{(x : y : z) \mid x \in \mathbb{A}_k^3\}$ can be identified with an affine plane by the embedding $(x : y : z) \mapsto (x/z, y/z)$. The complement of such a set is $\{(x : y : 0) \mid (x, y) \mid \mathbb{A}_l^2\}$ which can be identified with $\mathbb{P}_k^1$ by the embedding $(x : y : 0) \mapsto (x : y)$. Put loosely, the complement of a plane in $\mathbb{P}_k^2$ is $\mathbb{P}_k^1$. Hence, we may identify $\mathbb{P}_k^2$ with an affine plane unioned with $\mathbb{P}_k^1$ — the points in $\mathbb{P}_k^1$ are called points at infinity.

To define projective plane curves, we need polynomials with zeros that are well defined in the projective plane.

Definition 2.12. A polynomial P of degree d is said to be *homogeneous* if

$$P(\lambda x_1, \ldots, \lambda x_n) = \lambda^d P(x_1, \ldots, x_n), \tag{2.13}$$

for any $x_1, \ldots, x_n \in k$. Thus, if $x \in \mathbb{A}_k^n$ is such that $P(x) = 0$ then $P(\lambda x) = 0$ for any nonzero $\lambda \in k$. Hence, the zero set of P is well defined over points in $\mathbb{P}_k^{n-1}$.

Definition 2.14. Let P be a homogeneous polynomial of degree n in three variables. A *projective plane curve C of degree n* is the zero set

$$C = \{(x) \in \mathbb{P}_k^2 \mid P(x) = 0\}. \tag{2.15}$$

It is a curve that lives in the *projective plane* $\mathbb{P}_k^2$.

Example 2.16. Let C be the zero set $\{(x : y : z) \mid P(x, y, z) = 0\}$ of the homogeneous polynomial $P(x, y, z) = zy^2 - x^3 - zx^2$ over the reals. If $z \neq 0$ then $(x : y : z) = (x/z, y/z : 1)$, and so we can write C as the union

$$C = \{(x : y : 1) \mid P(x, y, 1) = 0\} \cup \{(x : y : 0) \mid P(x, y, 0) = 0\}.$$

If $z = 0$ and $P(x, y, z) = 0$ then $x = 0$. Thus, the only possible zero with $z = 0$ is $(0 : 1 : 0)$. Indeed, $P(0, 1, 0) = 0$, and so

$$C = \{(x : y : 1) \mid P(x, y, 1) = 0\} \cup \{(0 : 1 : 0)\}.$$

By the natural embedding $(x : y : 1) \mapsto (x, y)$, we can identify C with the affine curve shown in figure 5 in addition to the extra point $(0 : 1 : 0)$ at infinity.

Definition 2.17. Let a projective curve C be the zero set of a homogeneous polynomial P. A point $p = (x : y : z)$ on C is said to be singular if

$$\frac{\partial P}{\partial x} = \frac{\partial P}{\partial y} = \frac{\partial P}{\partial z} = 0.$$

If none of the points on C are singular then C is said to be smooth.

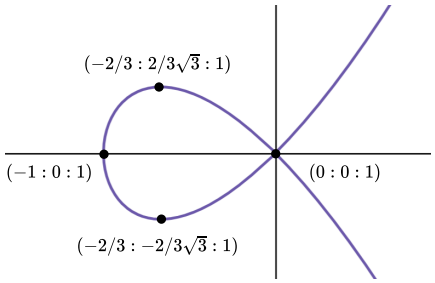


FIGURE 5

The curve in example 2.16 is *not* smooth since it has a singular point at $(0 : 0 : 1)$. The reader is encouraged to find a homogeneous polynomial that gives a smooth projective plane curve.

2.2. **Elliptic curves.** A lot is known about plane curves of degrees 1 and 2. Degree 3 curves, however, are much harder and much more interesting to study.

Definition 2.18. An *elliptic curve* E over a field k is a smooth projective plane curve obtained as the zero set of the degree 3 homogeneous polynomial

$$F(x, y, z) = y^2z - (ax^3 + bx^2z + cxz^2 + dz^3), \tag{2.19}$$

for $a, b, c, d \in k$. If the characteristic of k is not 2 then, for reasons to be seen later, we may restrict our attention to elliptic curves of the form

$$F(x, y, z) = y^2z - (x^3 + bxz^2 + cz^3), \tag{2.20}$$

for $b, c \in k$. We will always assume that k has characteristic not equal to 2. Solutions for (2.20) of the form $(x, y, 1)$ give us the affine plane curve

$$y^2 = x^3 + bx + c. \tag{2.21}$$

We can quickly check that $F(0, 1, 0) = 0$ and that $F(x, 0, 0)$ only if $x = 0$. Hence, we can identify the elliptic curve E with the affine curve (2.21) in addition to the point $(0 : 1 : 0)$ at infinity. Since the only point not on the affine curve is $(0 : 1 : 0)$, the elliptic curve is uniquely determined by the affine curve.

Example 2.22. Let $k = \mathbb{R}$. Figure 6 shows the affine curve $y^2 = x^3 - 2x + 1$ and figure 7 shows the affine curve $y^2 = x^3 - x + 1$. An elliptic curve E can be identified with the affine curve in figure 6 unioned with the point $(0 : 1 : 0)$ at infinity — the same goes for figure 7.

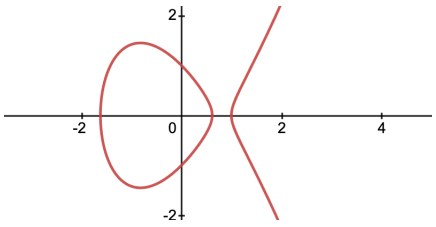


FIGURE 6

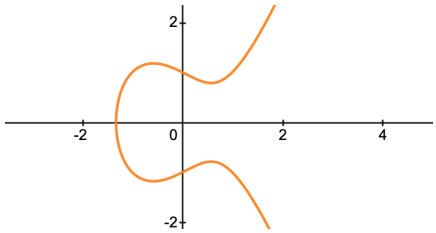


FIGURE 7

Construction 2.23. We can define a group structure over elliptic curves. Let E be an elliptic curve. Let $\oplus$ denote the group operation and take $\mathcal{O} = (0:1:0)$ to be the identity element. A line going through points $x, y \in E$ is the set of points of the form $\lambda x + (1-\lambda)y$, where λ runs over k. It is a line in the projective space but it can be identified with a line in the affine space or a line in the affine space in addition to the point $\mathcal{O}$. The curve E, as an affine curve, is symmetric about the x axis — if (x, y) is on the affine curve then so is $(x, -y)$. If $p = (x, y)$ lies on E then we take the inverse of p to be $-p = (x, -y)$. Let p_1 and p_2 be distinct points on E. It can be shown that the line going through p_1 and p_2 will intersect E at exactly one third point — denoted it as p_3. Define $p_1 \oplus p_2 = -p_3$. If $p_1 = p_2$ then define $p_1 \oplus p_2 = -p_3$ where p_3 is where the line tangent to p_1 on E intersects E again. See figure 8 where $k = \mathbb{R}$.

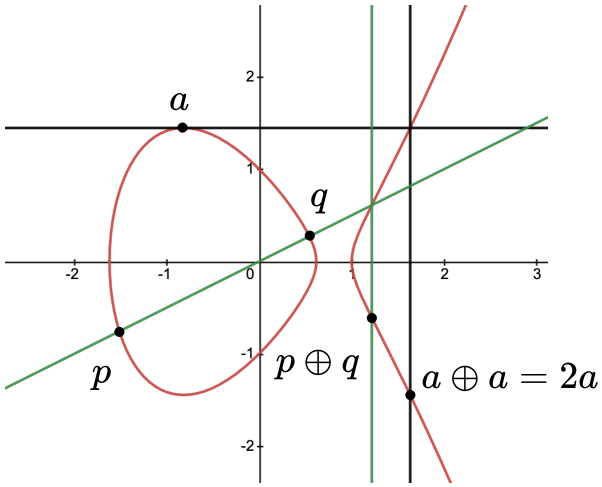


FIGURE 8. Group structure

Theorem 2.24. *The above construction defines a group.*

Proof. A reader is encouraged to check the group conditions. Otherwise a proof can be found at [4]. The fact that a line intersects an elliptic curve at exactly 3 points is a corollary of Bezout's theorem [5]. □

From now on, we will take $k = \mathbb{C}$.

Definition 2.25. Let E_1 and E_2 be two complex elliptic curves. A non-constant map $\phi : E_1 \to E_2$ defined as $\phi(x, y) = (R_1(x, y), R_2(x, y))$ for rational functions R_1 and R_2 is said to be an isogeny if it is also a group homomorphism.

Example 2.26. Consider the complex elliptic curves $E_1 : y^2 = x^3 + x$ and $E_2 : y^2 = x^3 - 4x$. Then the map

$$\phi(x, y) = \left(\frac{x^2 + 1}{x}, \frac{yx^2 - y}{x^2} \right)$$

is an isogeny from E_1 to E_2.

Remark 2.27. When the characteristic of the field is not 2, any elliptic curve of the form (2.19) is isogenous to some elliptic curve of the form (2.20). Hence, we're usually interested in curves of the form (2.20).

If an isogeny is a group isomorphism then it is said to be an isomorphism. This defines an equivalence relation between elliptic curves. However, although it's not obvious, an isogeny is already an equivalence relation.

Proposition 2.28. *If there's an isogeny ϕ from E_1 to E_2 then there's an isogeny $\widehat{\phi} : E_2 \to E_1$ called the dual isogeny, and we say that E_1 and E_2 are isogenuous. This defines an equivalence relation.*

This concludes our brief discussion of elliptic curves.

3. Riemann Surfaces

Before defining Riemann surfaces, we will review some notions about manifolds. A manifold is a space that locally looks like an Euclidean space.

Definition 3.1. In a topological space, an open set U that's homeomorphic to an open set in $\mathbb{R}^n$ is called an n-Euclidean neighborhood.

Definition 3.2. A topological space is called an n-manifold if it's Hausdorff and for any point in it, there's an n-Euclidean neighborhood containing that point.

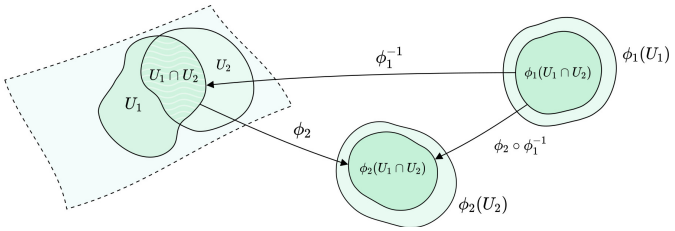
The Hausdorff condition ensures that this very bare-bone notion of a locally Euclidean space is still nice to work with. However, we're still interested in defining some more structure on manifolds. To do so, we look at charts and transition maps.

Definition 3.3. For an n-Euclidean neighborhood U, a homeomorphism ϕ from U to an open set in $\mathbb{R}^n$ is called a chart — we will slightly abuse terminology and also refer to the pair (U, ϕ) as a chart.

Definition 3.4. In a topological space, a collection $\mathcal{A} = \{(U_i, \phi_i)\}_{i \in I}$ of charts is called an atlas. An atlas $\mathcal{A} = \{(U_i, \phi_i)\}_{i \in I}$ is said to cover the space if the collection $\{U_i\}_{i \in I}$ of n-Euclidean neighborhoods covers the space. It's assumed that there's a fixed n such that each U_i in the collection is homeomorphic to an open set in $\mathbb{R}^n$.

To show that a Hausdorff space is a manifold, it suffices to find an atlas that covers it. How we choose the charts in an atlas can add more structure to the manifold. Specifically, we want to choose the charts so that transition maps are differentiable.

Definition 3.5. Given two charts (U_1, ϕ_1) and (U_2, ϕ_2) on an n-manifold such that U_1 and U_2 overlap, the map $\phi_2 \circ \phi_1^{-1} : \phi_1(U_1 \cap U_2) \to \phi_2(U_1 \cap U_2)$ is called a transition map — see the figure below.



Transition maps are continuous. Further requiring them to be of class C^k defines C^k manifolds. Requiring them to be smooth defines smooth manifolds. What other restrictions can we impose? For 2-manifolds, a transition map is a map from an open set in $\mathbb{R}^2$ to another open set in $\mathbb{R}^2$. Treating $\mathbb{R}^2$ as the complex plane leads us to a natural restriction — requiring transition maps to be holomorphic. Holomorphic maps on the complex plane are smooth maps on $\mathbb{R}^2$ that satisfy the Cauchy equations — a much more rigid condition than smoothness. Requiring transition maps over 2-manifolds to be holomorphic defines *Riemann surfaces*.

Definition 3.6. Let M be a connected 2-manifold. If M is covered by an atlas $\mathcal{A} = \{(U_i, \phi_i)\}_{i \in I}$ and charts $\phi_i : U_i \to \mathbb{C}$ that give holomorphic transition maps then M is called a Riemann surface. This definition makes sense since any map from $\mathbb{R}^2$ to $\mathbb{R}^2$ can be defined as a map from $\mathbb{C}$ to $\mathbb{C}$. We call $\mathcal{A}$ a complex atlas.

Remark 3.7. Other than being Hausdorff, a commonly imposed condition on manifolds is second-countability. It can be shown that if the transition maps are holomorphic then a 2-manifold is second-countable, making this requirement redundant for Riemann surfaces [6]. It can also be shown that any Riemann surface is orientable [7].

Non-Example 3.8. The Möbius strip, shown in figure 9, is a non-orientable smooth connected 2-manifold, and so it's a good example of a 2-manifold that's *not* a Riemann surface.

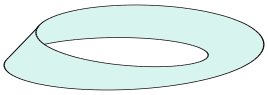


FIGURE 9. Möbius strip

Examples 3.9. The following are examples of Riemann surfaces.

(1) The upper half-plane $\mathbb{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$ is an example of a Riemann surface. The reader is encouraged to find a complex atlas for this surface.
(2) The Riemann sphere $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ is the one point compactification of $\mathbb{C}$ — it is a connected compact space. A set U is open in $\widehat{\mathbb{C}}$ if U is an open subset of $\mathbb{C}$ or if $\infty \in U$ and $\widehat{\mathbb{C}} \setminus U$ is a compact subset of $\mathbb{C}$.
(3) Any complex plane curve (affine or projective) is a Riemann surface.

Proposition 3.10. *The Riemann sphere is a Riemann surface.*

Proof. The open sets $\mathbb{C}$ and $\widehat{\mathbb{C}} \setminus \{0\}$ cover $\widehat{\mathbb{C}}$. Define the maps $\varphi : \mathbb{C} \to \mathbb{C}$ and $\psi : \widehat{\mathbb{C}} \setminus \{0\} \to \mathbb{C}$ as $\varphi(z) = z$ and

$$\psi(z) = \begin{cases} 1/z, & z \neq \infty \\ 0, & z = \infty \end{cases}.$$

We want to show that the collection $\{(\mathbb{C}, \phi), (\widehat{\mathbb{C}} \setminus \{0\}, \psi)\}$ is a complex atlas for $\widehat{\mathbb{C}}$. Note that φ is a homeomorphism. We want to show that ψ is also a homeomorphism. We can quickly check that ψ is invertible with inverse

$$\psi^{-1}(z) = \begin{cases} 1/z & z \neq 0 \\ \infty & z = 0 \end{cases}.$$

If an open set $U \subset \mathbb{C}$ doesn't contain 0 then $\psi^{-1}(U)$ is an open subset of $\mathbb{C}$. Otherwise, if U contains 0 then there's some $r > 0$ such that the punctured disk $D = \{z \in \mathbb{C} \mid 0 < |z| < r\}$ is contained in the open set $U' = U \setminus \{0\}$. This means that $\psi^{-1}(D)$ is contained in the open set $\psi^{-1}(U')$. One can quickly check that

$$\psi^{-1}(D) = \{z \in \mathbb{C} \mid |z| > 1/r\},$$

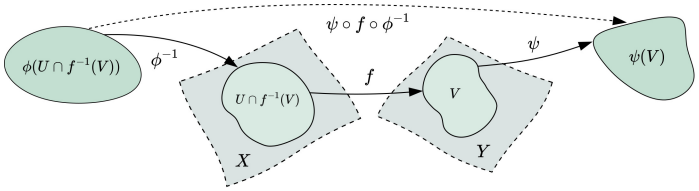
and so the closed set $\mathbb{C} \setminus \psi^{-1}(U')$ is bounded by the disk $\{z \in \mathbb{C} \mid |z| \leq 1/r\}$. Thus, $\mathbb{C} \setminus \psi^{-1}(U')$ is compact. Note that $\widehat{\mathbb{C}} \setminus \psi^{-1}(U) = \mathbb{C} \setminus \psi^{-1}(U')$, and so $\psi^{-1}(U)$ is open in $\widehat{\mathbb{C}}$. Hence, ψ is continuous. We'll now show that it's also an open map. Let $U \subset \widehat{\mathbb{C}} \setminus \{0\}$ be an open set. We know from complex analysis that if U is an open subset of $\mathbb{C}$ then $\psi(U)$ is also open in $\mathbb{C}$. Otherwise, if $\infty \in U$ then $\widehat{\mathbb{C}} \setminus U$ is a compact subset of $\mathbb{C}$, and so $\psi(\widehat{C} \setminus U)$ is compact and, hence, closed. Observe that $\psi(\widehat{\mathbb{C}} \setminus U) = \mathbb{C} \setminus \psi(U)$, and so $\psi(U)$ is open. Therefore, ψ is an open map and a homeomorphism. To finish the proof, we need to show that φ and ψ give holomorphic transition maps. The only two transition maps that can be formed from φ and ψ are

$$\varphi \circ \psi^{-1} : \mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\} \text{ and } \psi \circ \varphi^{-1} : \mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\}.$$

Over $\mathbb{C} \setminus \{0\}$, these maps are equal and are given by $\varphi \circ \psi^{-1}(z) = \psi \circ \varphi^{-1}(z) = 1/z$. From complex analysis, we know that the map $z \mapsto 1/z$ is holomorphic over $\mathbb{C} \setminus \{0\}$. Thus, we've found a complex atlas for the Riemann sphere. □

Now that we've defined Riemann surfaces, we can define holomorphic maps between them.

Definition 3.11. Let X and Y be Riemann surfaces. A map $f : X \to Y$ is said to be holomorphic if for any two charts $\phi : U \to \phi(U)$ and $\psi : V \to \psi(V)$ defined on X and Y respectively, the complex valued function $\psi \circ f \circ \phi^{-1}$ is holomorphic over the neighborhood $\phi(U \cap f^{-1}(V))$ — see the figure below.



We conclude our discussion of Riemann surfaces with the following theorem.

Theorem 3.12. *Any compact Riemann surface is a sphere with g handles, for some integer $g \geq 0$ called the genus of the surface.*

The Riemann sphere is a Riemann surface with genus 0. A Riemann surface with genus 1 is called a torus. Tori are the focus of section 5.

4. Quotient Spaces

In this section, we quickly review what a quotient space is and bring the reader's attention to a simple but important result that will consistently come up in the following sections.

Definition 4.1. Let X be a topological space and let $\sim$ be an equivalence relation defined on X. Let $X/\sim$ denote the set of equivalence classes under $\sim$. Consider the natural projection $\pi : X \to X/\sim$ that sends a point to its equivalence class. The quotient topology over $X/\sim$ is the finest topology (the topology with most open sets) under which π is continuous. In particular, a set U is open in $X/\sim$ under the quotient topology, if $\pi^{-1}(U)$ is open in X. Under the quotient topology, the set $X/\sim$ is called the *quotient space* of X under $\sim$.

Definition 4.2. Let X be a topological space and let $\sim$ be an equivalence relation defined on X. A *fundamental domain* of X under $\sim$ is a subspace D (we're inducing the subspace topology) such that for any $x \in X$ there's a unique point $y \in D$ for which $x \sim y$. This definition differs slightly from the standard definition of a fundamental domain [8], but it is good enough for the purpose of this paper.

Theorem 4.3. *Let D be a fundamental domain of X under a relation $\sim$. If $D/\sim$ is compact and $X/\sim$ is Hausdorff then $D/\sim$ and $X/\sim$ are homeomorphic.*

Proof. Any equivalence class A in $D/\sim$ can be written as $A = A_X \cap D$ for some equivalence class A_X in $X/\sim$. By the condition imposed on D, any equivalence class A in $X/\sim$ gives us an equivalence class $A \cap D$ in $D/\sim$. Hence, the map

$$\phi : A_X \cap D \mapsto A_X$$

from $D/\sim$ to $X/\sim$ is a bijection with inverse $\phi^{-1} : A \mapsto A \cap D$. We will now show that ϕ is a homeomorphism. Let $\pi_X : X \to X/\sim$ and $\pi_D : D \to D/\sim$ denote projection maps that send a point to its equivalence class. Let $U \subset X/\sim$ be an open set. Then $\pi_X^{-1}(U)$ is open in X, and so the set

$$\begin{aligned}\pi_D^{-1}(\phi^{-1}(U)) &= \pi_D^{-1}(\{A \cap D \mid A \in U\}) \\ &= \pi_X^{-1}(U) \cap D\end{aligned}$$

is open in D. Thus, $\phi^{-1}(U)$ is open in $D/\sim$. Therefore, ϕ is a continuous bijection from a compact space to a Hausdorff space, and so ϕ is a homeomorphism. □

When D is picked carefully, the quotient space $D/\sim$ is usually easier to visualize than $X/\sim$, and so $D/\sim$ is taken as a "model" for $X/\sim$. Sometimes, a point in X is not identified with a unique point in D but with more than one point. This doesn't affect theorem 4.3 but one has to be careful when allowing such exceptions in order make sure that $D/\sim$ is still a good representation of $X/\sim$. We will see an example of this in the next section.

5. Complex Tori

Complex tori are compact Riemann surfaces of genus 1 that are constructed as quotient spaces of $\mathbb{C}$. Through this construction, we will see that every complex elliptic curve can be identified with a complex torus.

5.1. Construction of Complex tori.

Definition 5.1. For complex numbers ω_1 and ω_2 that are linearly independent over the reals, the *lattice* generated by the pair (ω_1, ω_2) is the set

$$\Lambda = \langle \omega_1, \omega_2 \rangle := \{n\omega_1 + m\omega_2 \mid n, m \in \mathbb{Z}\}. \tag{5.2}$$

Examples 5.3. Figure 10 shows lattice $\langle 1, i \rangle$ and figure 11 shows lattice $\langle 2, 1+2i \rangle$.

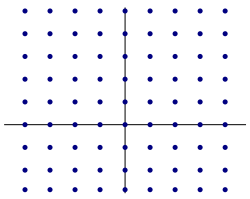


FIGURE 10

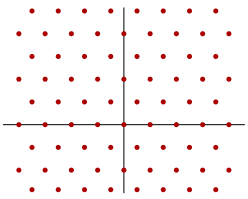


FIGURE 11

Definition 5.4. If complex numbers x and y are such that $x - y \in \Lambda$ then we say that x and y are Λ-equivalent. This defines an equivalence relation on $\mathbb{C}$. Let $\mathbb{C}/\Lambda$ denote the quotient space of $\mathbb{C}$ under this relation.

Proposition 5.5. *The quotient space $\mathbb{C}/\Lambda$ is a compact Riemann surface.*

Definition 5.6. Consider a lattice $\Lambda = \langle \omega_1, \omega_2 \rangle$. Taken as vectors on the plane, ω_1 and ω_2 form the sides of a parallelogram region — see figure 12. This region is called the **fundamental parallelogram** of Λ and is denoted as Π. More precisely,

$$\Pi = \{\lambda_1\omega_1 + \lambda_2\omega_2 \mid 0 \leq \lambda_1 \leq 1 \text{ and } 0 \leq \lambda_2 \leq 1\}.$$

Theorem 5.7. *Any complex number is Λ-equivalent to a point in Π. If distinct points $\tau_1, \tau_2 \in \Pi$ are Λ-equivalent then $\tau_1 - \tau_2 \in \{-\omega_1, -\omega_2, \omega_1, \omega_2\}$.*

Proof. The reader is encouraged to prove this theorem. Otherwise, a proof can be found at [4] □

Theorem 5.7 shows that Π is an example of a fundamental domain — the spaces Π/Λ and $\mathbb{C}/\Lambda$ are homeomorphic. Figure 12 shows the sides of Π that are identified together by the conditions in theorem 5.7 — we see that the quotient space Π/Λ is a torus. Hence, $\mathbb{C}/\Lambda$ is a complex torus. We can define a group structure on

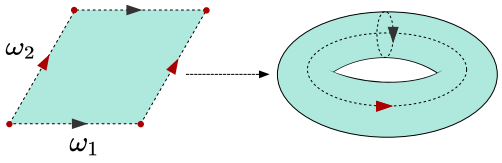


FIGURE 12

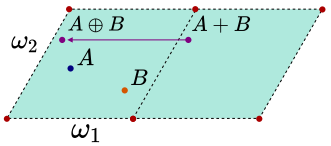


FIGURE 13

the torus $\mathbb{C}/\Lambda$ by taking it to be the quotient group of $\mathbb{C}$ by Λ. If the reader is not familiar with quotient groups then the following is a concrete description of the group structure. Let $\oplus_\Lambda$ denote the group operation defined on $\mathbb{C}/\Lambda$. Then we can define the group operation $\oplus$ on Π/Λ by taking a homeomorphism $h : \Pi/\Lambda \to \mathbb{C}/\Lambda$ and setting $x \oplus y = h^{-1}(h(x) \oplus h(y))$ for any $x, y \in \Pi/\Lambda$. Hence, Π/Λ inherits the group structure from $\mathbb{C}/\Lambda$ — the groups $(\mathbb{C}/\Lambda, \oplus_\Lambda)$ and $(\Pi/\Lambda, \oplus)$ are isomorphic. Points in Π/Λ can be identified with points in Π by unwrapping the torus back to the parallelogram in figure 12. Figure 13 then allows us to visualize the group structure on Π/Λ. In particular, for any two complex numbers A and B in Π, the point in Π that's Λ-equivalent to $A + B$ is taken to be $A \oplus B$. This description may provide some intuition to the fact that the group $(\mathbb{C}/\Lambda, \oplus_\Lambda)$ doesn't depend on Λ. In particular, the group $(\mathbb{C}/\Lambda, \oplus_\Lambda)$ is isomorphic to $(\mathbb{C}/\Lambda', \oplus_{\Lambda'})$ for any two

lattices Λ and Λ'. The reader is encouraged to prove this fact.

Since the groups on any two complex tori are isomorphic, trying to identify complex tori up to group isomorphism is not a great idea. Perhaps a better approach is to identify them up *holomorphic* group isomorphism. In particular, we identify two tori whenever there's a holomorphic map from one to the other that is a group isomorphism.

Definition 5.8. We say that lattices Λ and Λ' are *homothetic* if there's a complex number m such that $\Lambda = m\Lambda'$. This defines an equivalence relation on lattices.

Theorem 5.9. *Let Λ and Λ' be lattices. There's a holomorphic group homorphism between the complex tori $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ if, and only if, there's some complex number m such that $m\Lambda \subset \Lambda'$. There's a holomorphic group isomorphism between the tori if, and only, Λ and Λ' are homothetic.*

Proof. A proof can be found at [1]. □

5.2. **Elliptic Curves as Complex Tori.**

Definition 5.10. Given a lattice Λ, the Weierstrass $\wp$-function is defined as

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right), \tag{5.11}$$

where $z \notin \Lambda$.

Theorem 5.12. *For any lattice Λ, the Weierstrass $\wp$-function converges absolutely and uniformly over compact subsets disjoint from Λ.*

Proof. This theorem is given as a sequence of hinted exercises at [1]. □

Proposition 5.13. *Given a lattice $\Lambda = \langle\omega_1, \omega_2\rangle$, the function $\wp(z;\Lambda)$ and its derivative $\wp'(z;\Lambda)$ are well defined over $\mathbb{C}/\Lambda$. In particular, we have $\wp(z+\omega_1;\Lambda) = \wp(z,\Lambda)$ and $\wp(z+\omega_2;\Lambda) = \wp(z,\Lambda)$ for any $z \in \mathbb{C}$, and the same holds for $\wp'$.*

Proof. The reader is encouraged to come up with a proof. Otherwise, see [1]. □

Hence, we can define the map $z \mapsto (\wp(z;\Lambda), \wp'(z;\Lambda))$ from the complex torus $\mathbb{C}/\Lambda$ to the affine plane $\mathbb{A}^2_{\mathbb{C}}$. This map is a bijection and the image of the torus under this map is a complex elliptic curve.

Proposition 5.14. *There exist complex numbers b and c such that*

$$\wp'(z;\Lambda)^2 = 4\wp(z;\Lambda)^3 + a\wp(z;\lambda) + c$$

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

Proof. See [1] and [4]. □

Hence, we can associate an elliptic curve with every complex tori. Furthermore, it can be shown that for every elliptic curve, we can find a complex tori giving the curve as its image. Thus, we found a bijection between the class of complex tori and the class of complex elliptic curves. What structure does this bijection preserve? Let E_Λ denote the elliptic curve associated with the torus $\mathbb{C}/\Lambda$. The first thing to note is that the group structure $(E_\Lambda, \oplus)$ is isomorphic to $(\mathbb{C}/\Lambda, \oplus)$. Hence, the group structure on any complex elliptic curve doesn't depend on the curve.

Theorem 5.15. *Elliptic curves E_Λ and $E_{\Lambda'}$ are isogenous if, and only if, there's a holomorphic homomorphism from $\mathbb{C}/\Lambda$ to $\mathbb{C}/\Lambda'$. Furthermore, the curves are isomorphic if, and only if Λ and Λ' are homothetic.*

Proof. See [1] □

Remark 5.16. In category theory terms, the map $z \mapsto (\wp, \wp')$ defines a functor and an "inverse" functor from the category of complex tori to the category of complex elliptic curves. Hence, the two categories are equivalent. It should also be noted that a complex elliptic curve as a subset of the complex projective plane is a compact Riemann surface of genus 1 — it is a torus. However, the map $z \mapsto (\wp, \wp')$ provides a nice equivalence between the category of elliptic curves as algebraic objects and the category of tori as Riemann surfaces.

One can see that the task of parameterizing complex elliptic curves up to isomorphism reduces to parameterizing complex lattices up to homothety. Let $\mathcal{L}$ denote the quotient set of lattices by homothety. In the section, we construct a Riemann surface that is in bijection with $\mathcal{L}$.

6. Quotients of $\mathbb{H}$

6.1. The modular group.

Definition 6.1. The modular group, denoted as $\mathrm{SL}_2(\mathbb{Z})$, is the group of 2×2 matrices with integer entries and determinant 1. It is a group under standard matrix multiplication.

Definition 6.2. A group G is said to be generated by a subset $S \subset G$ if any element in G can be written as a composition of elements in S or their inverses.

Proposition 6.3. *The modular group is generated by the set of matrices*

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{6.4}$$

Proof. The reader is encouraged to come up with a proof. It is given as a hinted exercise at [1]. A full proof can be found at [4]. □

Definition 6.5. Recall that $\mathbb{H}$ denotes the upper half-plane. A pair (ω_1, ω_2) is said to have positive orientation if $\omega_1/\omega_2 \in \mathbb{H}$. We can express ω_1 and ω_2 as

$$\omega_1 = |\omega_1| e^{i\theta_1} \quad \text{and} \quad \omega_2 = |\omega_2| e^{i\theta_2},$$

where θ_1 and θ_2 are the angles ω_1 and ω_2 respectively make with the real line on $\mathbb{C}$. Having positive orientation means that $0 < \theta_1 - \theta_2 < \pi$. Visually, this means that the angle from ω_2 to ω_1 is strictly between 0 and π (like in figures 5 and 13).

Remark 6.6. If a pair (ω_1, ω_2) is not positively oriented then the pair (ω_2, ω_1) is. Since $\langle \omega_1, \omega_2 \rangle = \langle \omega_2, \omega_1 \rangle$, any lattice has a positively oriented generating pair.

Lemma 6.7. *If pairs (ω_1, ω_2) and (ω_1', ω_2') have positive orientation then they generate the same lattice if, and only if, there's some matrix*

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

in the modular group such that

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a\omega_1 + b\omega_2 \\ c\omega_1 + d\omega_2 \end{pmatrix}.$$

Proof. We omit the proof for this lemma to save space. The reader is encouraged to come up with a proof. Otherwise, it can be found at [1]. □

Proposition 6.8. *Any lattice is homothetic to some lattice $\langle \tau, 1\rangle$ where τ lies in the upper half-plane. Furthermore, if τ_1 and τ_2 are points in the upper half-plane then lattices $\langle \tau_1, 1\rangle$ and $\langle \tau_2, 1\rangle$ are homothetic if, and only if, there's some matrix*

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{6.9}$$

in the modular group such that

$$\tau_2 = \frac{a\tau_1 + b}{c\tau_1 + d}. \tag{6.10}$$

Proof. Any lattice is generated by some positively oriented pair (ω_1, ω_2) and is homothetic to $\langle \omega_1/\omega_2, 1\rangle$. Hence, any lattice is homothetic to some lattice $\langle \tau, 1\rangle$ where $\tau \in \mathbb{H}$. Suppose that the pairs $(\tau_1, 1)$ and $(\tau_2, 1)$ generate homoethic lattices. Then there's a complex number m such that $\langle \tau_1, 1\rangle = \langle m\tau_2, m\rangle$. By lemma 6.7, there's a matrix like (6.9) such that $m\tau_2 = a\tau_1 + b$ and $m = c\tau_1 + d$. Dividing $m\tau_2$ by m gives us (6.10). Now suppose that (6.10) holds. Then $\langle \tau_2, 1\rangle$ is homothetic to $\langle a\tau_1 + b, c\tau_1 + d\rangle$. Lemma 6.7 tells us that $\langle a\tau_1 + b, c\tau_1 + d\rangle = \langle \tau_1, 1\rangle$, and so (6.10) is a necessary and sufficient condition for $\langle \tau_1, 1\rangle$ and $\langle \tau_2, 1\rangle$ to be homothetic. □

Proposition 6.8 motivates a surjection from $\mathbb{H}$ to $\mathcal{L}$ that sends a point $\tau \in \mathbb{H}$ to the equivalence class containing $\langle \tau, 1\rangle$. We can turn this surjection into a bijection by identifying points in $\mathbb{H}$ that satisfy (6.10). The quotient space of $\mathbb{H}$ under this relation can then be thought of as a space that classifies lattices up to homothety. We will soon see that this quotient space can be compactified to form a Riemann sphere. In order to properly define this quotient space, we first need to review some group theory.

Definition 6.11. If G is a group with identity element e and X is some set then a (left) group action of G on X is a map $\cdot : G \times X \to X$ such that the $e \cdot x = x$ for any $x \in X$ and $g \cdot (h \cdot x) = (g \cdot h) \cdot x$ for any $g, h \in G$ and $x \in X$. For any $x \in X$, the orbit of x under the action of G is the set

$$G \cdot x = \{g \cdot x \mid g \in G\}.$$

One can quickly show that for elements $x, y \in X$, we have $G \cdot x = G \cdot y$ if, and only if, there exists some $g \in G$ such that $y = g \cdot x$. Furthermore, we can define an equivalence relation on X by identifying any two elements with the same orbit. The stabilizing group of an element $x \in X$ is the set

$$G_x = \{g \in G \mid g \cdot x = x\}.$$

One can quickly check that this set is a subgroup of G — it always contains e.

Definition 6.12. Let us define the group action $\cdot : \mathrm{SL}_2(\mathbb{Z}) \times \mathbb{H} \to \mathbb{H}$ as

$$\gamma \cdot \tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}, \tag{6.13}$$

for any γ in the modular group. In order to verify that $\gamma \cdot \tau \in \mathbb{H}$ for any $\tau \in \mathbb{H}$, the reader is encouraged to check that

$$\mathrm{Im}(\gamma \cdot \tau) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2}. \tag{6.14}$$

The reader is also encouraged to check that this map indeed defines a group action. The actions of the matrices from proposition (6.3) are $T \cdot \tau = \tau + 1$ and $S \cdot \tau = -1/\tau$.

Remark 6.15. Any two points in $\mathbb{H}$ are in the same orbit under group action (6.13) if, and only if, they satisfy (6.10). Hence, the orbits partition $\mathbb{H}$ into our desired quotient space.

Definition 6.16. If points x and y in $\mathbb{H}$ belong to the same orbit under group action (6.13) then we say x and y are $\mathrm{SL}_2(\mathbb{Z})$-equivalent. Let $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H}$ denote the quotient space under this equivalence relation. Proposition 6.8 gives us a bijection from $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H}$ to $\mathcal{L}$.

We want to visualize $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H}$. Let $L = \{\tau \in \mathbb{C} \mid \mathrm{Re}(\tau) = 1/2\}$. Then the blue lines in figure 14 are subsets of the set

$$\mathrm{SL}_2(\mathbb{Z}) \cdot L = \{\mathrm{SL}_2(\mathbb{Z}) \cdot \tau \mid \tau \in L\}.$$

Highlighted points of the same color are in the same orbit.

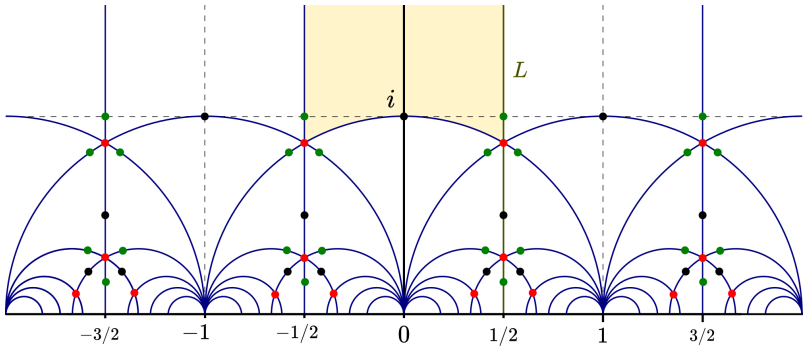


FIGURE 14. Orbits in $\mathrm{SL}_2(\mathbb{Z}) \cdot L$

Note that, by the action of T, highlighted points τ_1 and τ_2 such that $\tau_2 - \tau_1 = 1$ are in the same orbit.

Definition 6.17. The yellow region in figure 14 is called the **fundamental domain** of $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H}$. It can be described as

$$\mathcal{D} = \{\tau \in \mathbb{H} \mid |\tau| \geq 1 \text{ and } |\mathrm{Re}(\tau)| \leq 1/2\}.$$

Theorem 6.18. *Every complex number is $SL_2(\mathbb{Z})$-equivalent to some point in $\mathcal{D}$. Furthermore, if distinct points $\tau_1, \tau_2 \in \mathcal{D}$ are $SL_2(\mathbb{Z})$-equivalent then one of the following holds.*

(1) $Re(\tau_1) \in \{-1/2, 1/2\}$ and $|\tau_2 - \tau_1| = 1$.
(2) $|\tau_1| = 1$ and $\tau_2 = -1/\tau_1$.

Thus, $\mathcal{D}$ is an example of a fundamental domain from section 4 - the quotient spaces $SL_2(\mathbb{Z}) \setminus \mathcal{D}$ and $SL_2(\mathbb{Z}) \setminus \mathbb{H}$ are homeomorphic.

Proof. A proof can be found at [4]. □

Figure 15 shows the sides of $\mathcal{D}$ that are identified together by the conditions in 6.18 — we see that the quotient space $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{D}$ is a punctured sphere. One might therefore want to add a single point to $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{D}$ and turn it into a compact sphere — this will be discussed in more detail in section 7.

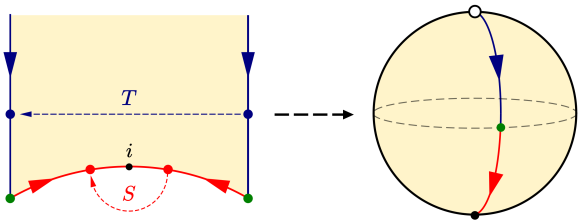


FIGURE 15. The fundamental domain

6.2. **Congruence subgroups.** Every point on our punctured sphere represents a class of homothetic lattices. However, it is usually of greater interest to parametrize lattices up to relations that are more nuanced than homothety. One way of doing so is to mod $\mathbb{H}$ by group actions of subgroups of $\mathrm{SL}_2(\mathbb{Z})$ instead of $\mathrm{SL}_2(\mathbb{Z})$ itself. Our choice of the subgroup can yield interesting and applicable results.

Definition 6.19. For an integer $N \geq 1$, the *principal congruence subgroup of level* N is defined as

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}, \tag{6.20}$$

where congruence comparison of matrices is done entry wise. Hence, $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$.

Definition 6.21. For integer $N \geq 1$, a *congruence subgroup of level* N is a subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ such that $\Gamma(N) \subset \Gamma$. The following are important examples.

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\} \tag{6.22}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\} \tag{6.23}$$

The reader should check that $\Gamma_0(N)$ and $\Gamma_1(N)$ are indeed congruence subgroups.

Definition 6.24. Given a congruence subgroup Γ, we can restrict the $\mathrm{SL}_2(\mathbb{Z})$-group action to Γ and consider the group action of Γ on $\mathbb{H}$. Any two points $x, y \in \mathbb{H}$ are said to be Γ-equivalent if they're in the same Γ-orbit or, equivalently, if there exists some $\gamma \in \Gamma$ such that $x = \gamma \cdot y$. Let $Y(\Gamma)$ denote the quotient space of $\mathbb{H}$ under this equivalence relation. We adopt the notation $Y(N) = Y(\Gamma(N))$, $Y_0(N) = Y(\Gamma_0(N))$, and $Y_1(N) = Y(\Gamma_1(N))$. Thus, $Y(1) = \mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H}$.

Example 6.25. This example is from [2]. It can be shown that $\Gamma_0(11)$ is generated by the set of matrices

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

It can also be shown that the blue region $\mathcal{B}$ in figure 16 is a fundamental domain for the quotient space $Y_0(11)$. Figure 16 shows the edges of $\mathcal{B}$ identified under $\Gamma_0(11)$-equivalence — we see that $Y_0(11)$ is a torus with two punctures holes. Naturally, we would want to add those two points to get a compact torus.

Let us now look at the classes of elliptic curves $\Gamma_0(N)$ and $\Gamma_1(N)$ parameterize. Proofs for the following results can be found at [1].

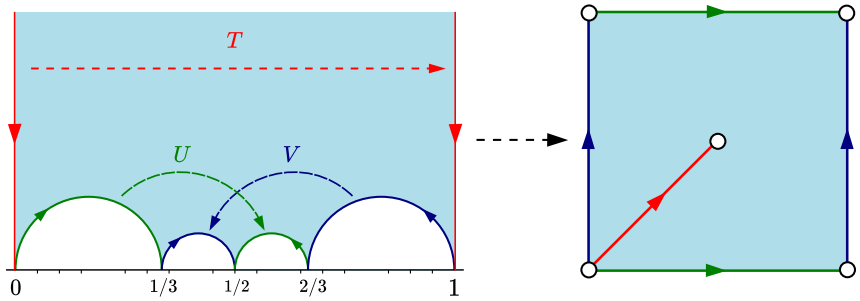


FIGURE 16

Definition 6.26. Let G be a group with identity e. The least integer $k \geq 1$ such that $g^k = e$ is called the order of g. If no such k exists then the order is said to be infinite. Furthermore, the set $\langle g \rangle = \{g^k \mid k \geq 0\}$ is a subgroup of G. If $G = \langle g \rangle$ for some $g \in G$ then G is said to be a cyclic group of order k where k is the order of g.

Definition 6.27. 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 of order N. Two such pairs (E, C) and (E', C') are said to be isomorphic if there's 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 6.28. *Every point in the quotient space $Y_0(N)$ represents a unique element of $S_0(N)$.*

Definition 6.29. 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's 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 6.30. *Every point in the quotient space $Y_1(N)$ represents a unique element of $S_1(N)$.*

In general, for any congruence subgroup Γ, the quotient space $Y(\Gamma)$ will be a surface with g handles that's missing finitely many points. Adding those points will give us a compact Riemann surface that we call a modular curve. However, those added points don't correspond to classes of lattices. Hence, compactifying $Y(\Gamma)$ by adding those missing points will give us a compact Riemann surface where all but finitely many points represent isomorphism classes of complex elliptic curves. Could we have constructed compact Riemann surfaces such that *every* point corresponds to an isomorphism class of elliptic curves? This is a good example of a problem in algebraic geometry called the *moduli problem* — put very loosely, can we find a nice geometric space, without having to add "extra" points, with a nice bijection with isomorphism classes of other geometric objects? A more precise formulation of the problem is beyond the scope of this paper — see the discussion in section 7 at [2]. Such geometric objects have not been found in many cases — we usually need to fill in "holes" and allow for a small set of points to not represent isomorphism classes.

In our case, filling in the holes in $Y(\Gamma)$ will give us a modular curve. Section 7 will discuss this in more detail. We now discuss an important fact about congruence subgroups.

Definition 6.31. Let $H \subset G$ be a subgroup of a group G. Given an element $g \in G$, the set $Hg = \{hg \mid h \in H\}$ is called a (right) coset of H in G. The the number of cosets is called the index of H and is denoted as $[G : H] := |\{Hg \mid g \in G\}|$

Remark 6.32. One can quickly check that each coset is in bijection with H and that the cosets partition G. Hence, if G is finite then $|G| = [G : H]|H|$.

Theorem 6.33. *The index $[SL_2(\mathbb{Z}) : \Gamma]$ of any congruence subgroup Γ is finite. For $N \geq 1$, we have*

$$[SL_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right), \tag{6.34}$$

where the product is taken over the prime divisors of N.

Proof. This is a sketch of the proof. If the reader is not familiar with group theory then they can jump to section 7. The general idea is that $\Gamma(N)$ is the kernel of the natural homeomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, and so it's a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and we have a natural injection $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. The reader is encouraged to check that the injection $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is actually a surjection and, hence, an isomorphism. By a counting argument, we can show that $|\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})|$ is given by (6.34). □

7. Modular Curves

Throughout this section, $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ will denote a congruence subgroup. The aim of this section is to compactify $Y(\Gamma)$ to get a compact Riemann surface. We start by adding points to the upper half-plane.

7.1. The extended upper half plane.

Definition 7.1. Let $\mathbb{P}^1_{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$ denote the rational projective line. Then the *extended upper half plane* is defined as the union

$$\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1_{\mathbb{Q}}. \tag{7.2}$$

Points in $\mathbb{P}^1_{\mathbb{Q}}$ are called *cusp points*.

Construction 7.3. Let us define an appropriate topology on $\mathbb{H}^*$. If a set $U \subset \mathbb{H}^*$ doesn't contain any points from $\mathbb{P}^1_{\mathbb{Q}}$ then U is open in $\mathbb{H}^*$ if, and only if, it's open in the standard topology on $\mathbb{H}$. If $\infty \in U$ then U is open if $U = \mathbb{H} \cup \{\infty\}$ or

$$U = \{\tau \in \mathbb{H} \mid \mathrm{Im}(\tau) > r\} \cup \{\infty\} \text{ for some } r > 0. \tag{7.4}$$

If U contains a rational point q then U is open if $U = \mathbb{H} \cup \{q\}$ or U is the interior of a circle in $\mathbb{H}$ that's tangent to the real line at point q. The subspace topology induced on $\mathbb{H}$ under this topology is the same as the standard topology on $\mathbb{H}$. Figure 7.3 shows some examples of open neighborhoods in $\mathbb{H}^*$.

Remark 7.5. If U is an open neighborhood of ∞ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ is such that $\gamma \cdot \infty = \tau \in \mathbb{Q}$ then $\gamma \cdot U$ is an open neighborhood of τ.

Proposition 7.6. *The extended plane $\mathbb{H}^*$ is connected.*

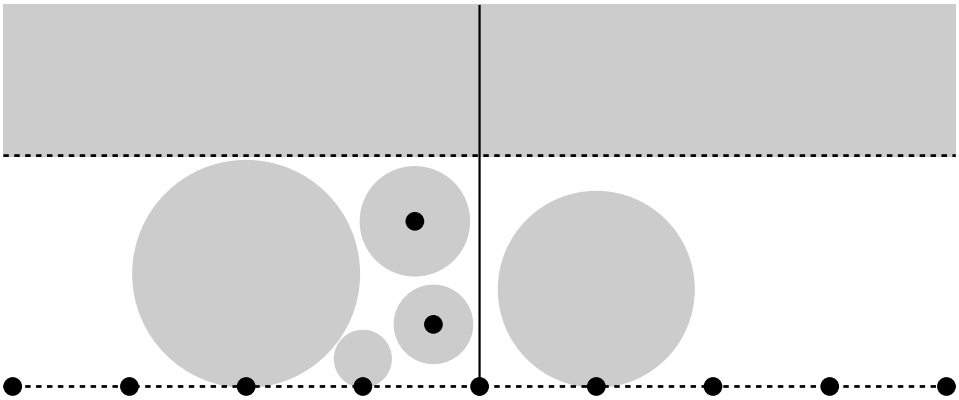


FIGURE 17. Open neighborhoods in $\mathbb{H}^*$

Proof. Suppose that $\mathbb{H}^* = O_1 \cup O_2$ for open sets O_1 and O_2. Then $O_1 \cap \mathbb{H}$ and $O_2 \cap \mathbb{H}$ are open in $\mathbb{H}$ and $\mathbb{H} = (O_1 \cap \mathbb{H}) \cup (O_2 \cap \mathbb{H})$. However, $\mathbb{H}$ is connected, and so we can assume, without loss of generality, that $O_2 \cap \mathbb{H}$ is empty. Therefore, any point in O_2 must be from $\mathbb{P}^1_{\mathbb{Q}}$. The topology defined on $\mathbb{H}^*$ tells us that any open neighborhood of a point in $\mathbb{P}^1_{\mathbb{Q}}$ must intersect $\mathbb{H}$, and so O_2 must be empty. □

Now that we have a topology on $\mathbb{H}^*$, we can look at quotient spaces of $\mathbb{H}^*$.

Definition 7.7. The group action of $\mathrm{SL}_2(\mathbb{Z})$ can be extended to $\mathbb{H}^*$ by defining a new (left) action $\cdot : \mathrm{SL}_2(\mathbb{Z}) \times \mathbb{H}^* \to \mathbb{H}^*$ as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \begin{cases} (a\tau + b)/(c\tau + d) & , \tau \in \mathbb{H}^* \setminus \{-c/d\} \\ a/c & , \tau = \infty \\ \infty & , \tau = -c/d \end{cases} . \tag{7.8}$$

The reader is encouraged to check that this is a group action.

Definition 7.9. Points in $\mathbb{H}^*$ are said to be Γ-equivalent if they're in the same Γ-orbit under action 7.7. This defines an equivalence relation on $\mathbb{H}^*$. The quotient space of $\mathbb{H}^*$ under this relation is called a *modular curve* and is denoted as $X(\Gamma)$. Let $X(N) = X(\Gamma(N))$, $X_0(N) = X(\Gamma_0(N))$, and $X_1(N) = X(\Gamma_1(N))$. Equivalence classes of points in $\mathbb{P}^1_{\mathbb{Q}}$ are called cusp points.

Proposition 7.10. *The modular curve $X(1)$ has one cusp point.*

Proof. We can write a rational point τ as $\tau = a/c$ for relatively prime integers a and c. There exist integers b and d such that $ad - bc = \gcd(a, c) = 1$. The matrix

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

is such $\gamma \cdot \infty = \tau$. Thus, any rational is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to ∞, and so we have one cusp point in $X(1)$. □

Our aim is to show that $X(\Gamma)$ is a compact Riemann surface. The modular curve $X(1)$ is the Riemann sphere obtained by adding the missing cusp point to $Y(1)$. In general, we add missing cusp points to $Y(\Gamma)$ and turn it into the modular curve $X(\Gamma)$.

Theorem 7.11. *Any modular curve $X(\Gamma)$ has finitely many cusp points.*

Proof. The reader is encouraged to prove the theorem. Hint: the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ is finite. □

7.2. **The topology on $X(\Gamma)$.** A good start to showing that $X(\Gamma)$ is a compact Riemann surface is to show that it is connected, compact, and Hausdorff. Recall that $\mathbb{H}^*$ is connected. The projection $\pi : \mathbb{H}^* \to X(\Gamma)$ is continuous, and so $X(\Gamma)$ is also connected. We will now show that $X(\Gamma)$ is compact.

Lemma 7.12. *The set $\mathcal{D}^* = \mathcal{D} \cup \{\infty\}$ is compact in $\mathbb{H}^*$*

Proof. Let $\mathcal{G} = \{G_i\}_{i\in I}$ be an open cover of $\mathcal{D}^*$. Then $\mathcal{G}$ contains an open neighborhood O of ∞. If $O = \mathbb{H} \cup \{\infty\}$ then O already covers $\mathcal{D}$. Otherwise, we have $O = \{\tau \in \mathbb{H} \mid \mathrm{Im}(\tau) > r\} \cup \{\infty\}$ for some $r > 0$. Then the collection $\mathcal{G}$ admits a finite subcover $\mathcal{G}'$ of the compact set $\mathcal{D} \cap \{\tau \in \mathcal{D} \mid \mathrm{Im}(\tau) \leq r\}$ and the collection $\mathcal{G}' \cup \{O\}$ is a finite subcover of $\mathcal{G}$ of $\mathcal{D}$. □

Theorem 7.13. *The modular curve $X(\Gamma)$ is compact.*

Proof. Recall that $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ is finite, and so there's a finite collection of matrices $\{\gamma_i\}_{i\in I}$ such that

$$\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{i\in I} (\Gamma\gamma_i),$$

where each $\Gamma\gamma_i$ represents a coset. Note that

$$\mathbb{H}^* = \mathrm{SL}_2(\mathbb{Z}) \cdot \mathcal{D}^* = \bigcup_{i\in I} \Gamma \cdot \gamma_i \cdot \mathcal{D}^*,$$

where $\Gamma \cdot \gamma_i \cdot \mathcal{D}^* = \{\gamma \cdot \gamma_i \cdot x \mid \gamma \in \Gamma \text{ and } x \in \mathcal{D}^*\}$. Let $\pi : \mathbb{H}^* \to X(\Gamma)$ denote the natural projection sending each point to its orbit. Then

$$X(\Gamma) = \pi(\mathbb{H}^*) = \bigcup_{i\in I} \pi(\gamma_i \cdot \mathcal{D}^*).$$

Note that each map $\tau \mapsto \gamma_i \cdot \tau$ is continuous, and so, since π is also continuous, lemma 7.12 tells us that each $\pi(\gamma_i \cdot \mathcal{D}^*)$ is compact. Hence, $X(\Gamma)$ is he finite union of compact sets. □

Now we need to show that $X(\Gamma)$ is Hausdorff — we first show that the quotient $Y(\Gamma)$ is Hausdorff. To do so, we need to talk about some more group theory.

Definition 7.14. Let G be a group acting on a topological space X by (left) group action $\cdot : G \times X \to X$. Then the group action is said to be *properly discontinuous* if for any points $x, y \in X$, there exist open neighborhoods U_1 and U_2 of x and y respectively such that if $g \cdot x \neq y$ then $g \cdot U_1 \cap U_2 = \emptyset$. Put loosely, there are small enough neighborhoods around x and y such that if g takes x away from y then it also takes their neighborhoods away from each other.

Theorem 7.15. *The $SL_2(\mathbb{Z})$ group action on $\mathbb{H}$ is properly discontinuous.*

Proof. Let $\tau_1, \tau_2 \in \mathbb{H}$. There are open sets $V_1, V_2 \subset \mathbb{H}$ with compact closures containing τ_1 and τ_2, respectively. For $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with lower row (c, d), let

$$s(\gamma) := \sup\{\mathrm{Im}(\gamma \cdot \tau) \mid \tau \in V_1\}. \tag{7.16}$$

Since V_1 is bounded, there's a constant $C > 0$ such that $\mathrm{Im}(\tau) < C$ for all $\tau \in V_1$. By (6.14), we get the bound

$$s(\gamma) < \sup\left\{\frac{C}{|c\tau + d|^2} \mid \tau \in V_1\right\} = \frac{C}{\inf\{|c\tau + d|^2 \mid \tau \in V_1\}}.$$

We can make $\inf\{|c\tau + d|^2 \mid \tau \in V_1\}$ arbitrarily large for sufficiently large values of $|c|$ and $|d|$. Hence, we can make $s(\gamma)$ arbitrarily small for sufficiently large $|c|$ and $|d|$, and so, given some real $r > 0$, we have $s(\gamma) \geq r$ for only finitely many integers c and d. Visually, the $\mathrm{SL}_2(\mathbb{Z})$ action "squeezes" the imaginary part of V_1 down.

Let $r = \inf\{\mathrm{Im}(\tau) \mid \tau \in V_2\}$ (we have $r > 0$ since V_2 has compact closure). Note that $\gamma(V_1)$ and V_2 cannot share any points when $s(\gamma) < r$ since that implies $\mathrm{Im}(z_1) < \mathrm{Im}(z_2)$ for any points z_1 and z_2 from $\gamma(V_1)$ and V_2 respectively. Hence, $\gamma(V_1)$ and V_2 can share points for only finitely many integers c and d. Pick any two such integers c and d and let Q be some matrix in $\mathrm{SL}_2(\mathbb{Z})$ with lower row (c, d). Verify that the set of matrices in $\mathrm{SL}_2(\mathbb{Z})$ with lower row (c, d) is exactly the set

$$\left\{\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} Q \mid k \in \mathbb{Z}\right\}.$$

Therefore, for any $\tau \in V_1$ and γ with lower row (c, d), we have

$$\gamma \cdot \tau = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \cdot (Q \cdot \tau) = \frac{Q \cdot \tau + k}{0 + 1} = Q \cdot \tau + k.$$

Let $r = \inf\{|\mathrm{Re}(\tau)| \mid \tau \in V_2\}$. There are finitely many integers k such that

$$\sup\{|\mathrm{Re}(Q \cdot \tau + k)| \mid \tau \in V_1\} \geq r,$$

and so there are finitely many matrices γ with lower row (c, d) for which $\gamma(V_1)$ intersects V_2. In conclusion, there are only finitely many integers c and d for which a matrix γ with lower row (c, d) can give $\gamma \cdot V_1 \cap V_2 \neq \emptyset$ and, for any such integers (c, d), there are only finitely many γ such that $\gamma \cdot V_1 \cap V_2 \neq \emptyset$. Therefore, there are finitely many matrices $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma(V_1)$ intersects V_2 — let F denote the set of such matrices. It follows that the set

$$E = \{\gamma \in F \mid \gamma \cdot \tau_1 \neq \tau_2\} \subset F$$

is finite. For any $\gamma \in E$, there are disjoint neighborhoods A_γ and B_γ containing $\gamma \cdot \tau_1$ and τ_2 respectively. Define the open neighborhoods

$$U_1 = V_1 \cap \left(\bigcap_{\gamma \in E} \gamma^{-1}(A_\gamma)\right) \text{ and } U_2 = V_2 \cap \left(\bigcap_{\gamma \in E} B_\gamma\right).$$

If $\gamma \cdot \tau_1 = \tau_2$ then $\gamma \in E$, and so $\gamma \cdot U_1 \cap U_2 = \emptyset$. □

Lemma 7.17. *The projection $\pi : \mathbb{H} \to Y(\Gamma)$ is an open map.*

Proof. Any matrix $\gamma \in \Gamma$ can be written as a composition of S and T, and so the action of γ is an open map over $\mathbb{H}$ if the actions $T \cdot z = z + 1$ and $S \cdot z = -1/z$ are themselves open. These two maps are non-constant and holomorphic over $\mathbb{H}$ and so they're indeed open by the open mapping theorem. Therefore, the set

$$\pi^{-1}(\pi(U)) = \bigcup_{\gamma \in \Gamma} \gamma(U)$$

is open in $\mathbb{H}$ for any open $U \subset \mathbb{H}$, and so $\pi(U)$ is open in the quotient topology. □

Theorem 7.18. *The quotient $Y(\Gamma)$ is Hausdorff.*

Proof. Let $\pi(\tau_1)$ and $\pi(\tau_2)$ be distinct points in $Y(\Gamma)$. Then $\gamma \cdot \tau_1 \neq \tau_2$ for all $\gamma \in \Gamma$, and so theorem 7.15 gives us two open neighborhoods U_1 and U_2 containing τ_1 and τ_2 respectively such that $\Gamma \cdot U_1 \cap U_2 = \emptyset$. One can quickly check that $\pi(U_1) \cap \pi(U_2) = \emptyset$. Since π is an open map, $\pi(U_1)$ and $\pi(U_2)$ are disjoint open neighborhoods in $Y(\Gamma)$ containing $\pi(\tau_1)$ and $\pi(\tau_2)$ respectively. □

We are now ready to show that $X(\Gamma)$ is Hausdorff.

Theorem 7.19. *The modular curve $X(\Gamma)$ is Hausdorff.*

Proof. Let π denote the natural projection from $\mathbb{H}^*$ to $X(\Gamma)$. We can show that π is open by an argument similar to the proof for lemma 7.17. Let $\pi(\tau_1)$ and $\pi(\tau_2)$ be two distinct points in $X(\Gamma)$. If $\tau_1, \tau_2 \in \mathbb{H}$ then we're done by theorem 7.18. Suppose $\tau_1 \in \mathbb{P}^1_{\mathbb{Q}}$ and $\tau_2 \in \mathbb{H}$. Let $V \subset \mathbb{H}$ be an open neighborhood of τ_2 with compact closure $K \subset V$. We can quickly check that

$$\mathrm{Im}(\gamma \cdot \tau) \leq \max\{\mathrm{Im}(\tau), 1/\mathrm{Im}(\tau)\},$$

for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in K$. Thus, if $r = 1 + \sup\{\max\{\mathrm{Im}(\tau), 1/\mathrm{Im}(\tau)\} \mid \tau \in K\}$ then $\{\tau \in \mathbb{H} \mid \mathrm{Im}(\tau) > r\} \cap (\mathrm{SL}_2(\mathbb{Z}) \cdot K) = \emptyset$. Consider the open neighborhood $U = \{\tau \in \mathbb{H} \mid \mathrm{Im}(\tau) > r\} \cup \{\infty\}$ of ∞. There exists some $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau_1 = \alpha \cdot \infty$. The image $\alpha \cdot U$ is an open neighborhood of τ_1. It follows that $(\alpha \cdot U) \cap (\mathrm{SL}_2(\mathbb{Z}) \cdot V) = \emptyset$, and so $\pi(\alpha \cdot U)$ and $\pi(V)$ are disjoint open neighborhoods of $\pi(\tau_1)$ and $\pi(\tau_2)$ respectively.

The last case to consider is if $\tau_1, \tau_2 \in \mathbb{P}^1_{\mathbb{Q}}$. The are matrices $\alpha_1, \alpha_2 \in \mathrm{SL}_2(\mathbb{Z})$ such that $\alpha_1 \cdot \infty = \tau_1$ and $\alpha_2 \cdot \infty = \tau_2$. Consider the set $V = \{\tau \mid \mathrm{Im}(\tau) > 2\} \cup \{\infty\}$, an open neighborhood of ∞. Let $U_1 = \alpha_1 \cdot V$ and $U_2 = \alpha_2 \cdot V$. If $\pi(U_1) \cap \pi(U_2) \neq \emptyset$ then there's some $\gamma \in \Gamma$ such that $\gamma \cdot (\alpha_1 \cdot x_1) = \alpha_2 \cdot x_2$ where $x_1, x_2 \in V$. This means that $(\alpha_2^{-1} \gamma \alpha_1) \cdot x_1 = x_2$. We will see later that if $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$ is such that $\gamma' \cdot x_1 = x_2$ and $\mathrm{Im}(x_1), \mathrm{Im}(x_1) > 2$ then

$$\gamma' = \pm \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix},$$

for some integer m. Hence, $\alpha_2^{-1} \gamma \alpha_2$ sends ∞ to ∞, and so $\gamma \cdot \tau_1 = \tau_2$. This is a contradiction since $\pi(\tau_1)$ and $\pi(\tau_2)$ are distinct, and so $\pi(U_1) \cap \pi(U_2) = \emptyset$. Thus, $\pi(U_1)$ and $\pi(U_2) = \emptyset$ are disjoint open neighborhoods of $\pi(\tau_1)$ and $\pi(\tau_2)$ respectively. □

We've shown that $X(\Gamma)$ is compact, connected, and Hausdorff. This concludes our investigations of the topology on $X(\Gamma)$.

7.3. **Elliptic points.** Next, we want to put a complex atlas on $X(\Gamma)$. Doing so requires some care with certain points in $\mathbb{H}^*$. We start by finding charts for points in $\mathbb{H}$. Recall from definition 6.11 that the *stabilizer* subgroup of a point $\tau \in \mathbb{H}$ is

$$\Gamma_\tau = \{\gamma \in \Gamma \mid \gamma \cdot \tau = \tau\}.$$

Since the Γ-group action is properly discontinuous, there's a neighborhood U of τ such that if $\gamma \in \Gamma$ and $\gamma \cdot \tau \neq \tau$ then $\gamma \cdot U \cap U = \emptyset$ — we're taking the two points in the definition of proper discontinuity to both be τ. If there are distinct points $x, y \in U$ such that $x = \gamma \cdot y$ for some $\gamma \in \Gamma$ then $\gamma \cdot U \cap U \neq \emptyset$, and so $\gamma \in \Gamma_\tau$. This

is an important observation — for any point $\tau \in \mathbb{H}$, there's a neighborhood U of τ so that any transformation that takes one point in U to another is a transformation that fixes τ.

If I is the identity matrix then I and $-I$ fix τ. Therefore, the set $\Gamma \cap \{-I, I\}$ is contained in Γ_τ — we say that Γ_τ is trivial if $\Gamma_\tau = \Gamma \cap \{-I, I\}$. There's a very natural choice for a chart around τ if its stabilizer group is trivial.

Proposition 7.20. *Let π to be the natural projection from $\mathbb{H}$ to $Y(\Gamma)$. If $\tau \in \mathbb{H}$ has a trivial stabilizer group then there exists some open neighborhood $U \subset \mathbb{H}$ of τ such that $\pi : U \to \pi(U)$ is a homeomorphism, and so $\pi^{-1}(U)$ is a 2-Euclidean neighborhood.*

Proof. Let U be the neighborhood containing τ from the discussion above. Suppose that $\pi(x) = \pi(y)$ for some $x, y \in U$. This means that there's some $\gamma \in \Gamma$ such that $x = \gamma \cdot y$, and so $\gamma = \pm I$ since Γ_τ is trivial. Hence, γ fixes y, and so $x = y$. In other words, the map $\pi : U \to \pi(U)$ is an injection and, thus, a bijection. It is open and continuous, and so it's a homeomorphism. □

However, it's not obvious what we should do if the stabilizer group is not trivial. A point in $\mathbb{H}$ is called an *elliptic point* if its stabilizer group is not trivial. Let us now investigate those points.

Proposition 7.21. *If $\gamma \in SL_2(\mathbb{Z})$ is such that $\gamma \cdot \tau = \tau$ for some $\tau \in \mathbb{H}$ then γ has order $1, 2, 3, 4,$ or 6 as a matrix in $SL_2(\mathbb{Z})$.*

Proof. Assume that the matrix

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

is such that $\gamma \cdot \tau = \tau$. Then $a\tau + b = c\tau^2 + d\tau$. If $c = 0$ then $a = d = \pm 1$, and so we'd have $b = 0$ and $\gamma = \pm I$. If $c \neq 0$ then we get the quadratic solutions

$$\tau = \frac{(a-d) \pm \sqrt{(a-d)^2 + 4bc}}{2c}.$$

Since $\mathrm{Im}(\tau) \neq 0$, we must have $(a-d)^2 + 4bc < 0$. Hence, we have

$$\begin{aligned} (a-d)^2 + 4 - 4ad &< 0, \\ a^2 + 2ad + d^2 &< 8ad - 4, \\ (a+d)^2 &< 4(2ad - 1). \end{aligned}$$

Note that $4bc \leq (a-d)^2 + 4bc < 0$, and so $bc < 0$. This means that $ad < 1$, and so $2ad - 1 < 1$. In particular, we have $(a+d)^2 < 4$, and so $|a+d| < 2$. Thus, $a + d \in \{-1, 0, 1\}$. The characteristic polynomial of γ is

$$(a-\lambda)(d-\lambda) - bc = \lambda^2 - \lambda(a+d) + 1,$$

and so it must equal $\lambda^2 + 1$, $\lambda^2 + \lambda + 1$, or $\lambda^2 - \lambda + 1$. The Cayley–Hamilton theorem tells us that γ must satisfy its characteristic polynomial in $\mathrm{SL}_2(\mathbb{Z})$. Thus, we must have

$$\gamma^2 + I = 0, \ \gamma^2 + \gamma + I = 0, \ \text{or } \gamma^2 - \gamma + 1 = 0.$$

The polynomial $x^2 + 1$ is a factor of $x^4 - 1$ and the polynomials $x^2 + x + 1$ and $x^2 - x + 1$ are factors of $x^6 - 1$. Hence, the possible orders of γ are $1, 2, 3, 4$ or 6. □

Remark 7.22. If $\gamma^2 = I$ then $a^2 + bc = 1$ and $ab + bd = 0$. If $b \neq 0$ then $a = -d$, and so $ad - bc = 1 = -a^2 - bc$. This gives us the contradiction $1 = a^2 + bc = -1$, and so we must have $b = 0$. This implies $ad = 1$, and so $a = d = \pm 1$ and $\gamma = \pm I$. Thus, if γ has order 1 or 2 then $\gamma = \pm I$.

The next theorem classifies the matrices in $\mathrm{SL}_2(\mathbb{Z})$ with orders $3, 4$ and 6.

Theorem 7.23. *Consider the following matrices*

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \; B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \text{ and } C = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}. \tag{7.24}$$

The following holds.

1. *If γ has order 3 then γ is conjugate to A in $SL_2(\mathbb{Z})$.*
2. *If γ has order 4 then γ is conjugate to B in $SL_2(\mathbb{Z})$.*
3. *If γ has order 6 then γ is conjugate to C in $SL_2(\mathbb{Z})$.*

Proof. Can be found at [1] □

Corollary 7.25. *The only elliptic points in $\mathcal{D}$ are i and $\rho = e^{2\pi i/3}$. The stabilizer of i is a cyclic subgroup of order 2 and the stabilizer of ρ is a cyclic subgroup of order 3.*

If $x \in \mathbb{H}$ is an elliptic point then $\Gamma \cdot x \in X(\Gamma)$ is also called an elliptic point.

Corollary 7.26. *The stabilizer group of every elliptic point in $\mathbb{H}$ is finite-cyclic and every modular curve $X(\Gamma)$ has finitely many elliptic points.*

Remark 7.27. If x and y have imaginary parts greater than 2 then they are not elliptic points since the only elliptic points in $\mathcal{D}$ are i and ρ. Thus, if $\gamma \cdot x = y$ for some γ then we must have $\gamma = T^m$ for some integer m.

This concludes our investigation of elliptic points and we can now define charts around them. Suppose $\tau \in \mathbb{H}$ is an elliptic point.

Definition 7.28. For every $\tau \in \mathbb{H}$, since Γ_τ is finite cyclic, we can associate an integer called the *period* of τ and is defined as

$$h_\tau = \begin{cases} |\Gamma_\tau|/2 & , -I \in \Gamma \\ |\Gamma_\tau| & , -I \notin \Gamma \end{cases}. \tag{7.29}$$

Note that if $-I \in \Gamma_\tau$ then $-\gamma$ and γ both represent the same transformation on τ. Hence, h_τ correctly counts the number of τ fixing transformations.

Proposition 7.30. *We have $h_\tau = h_{\gamma\cdot\tau}$ for any $\gamma \in \Gamma$. Hence, the period is well defined over points in $X(\Gamma)$.*

Proof. Let $\gamma \in \Gamma$. Observe that for any $\gamma' \in \Gamma$, we have $(\gamma\gamma'\gamma^{-1}) \cdot (\gamma \cdot \tau) = \gamma \cdot \tau$ if, and only if, $\gamma \cdot \tau = \tau$. Hence, we can define the bijection $\eta : \gamma' \mapsto \gamma\gamma'\gamma^{-1}$ from Γ_τ to $\Gamma_{\gamma\cdot\tau}$. This means that $|\Gamma_\tau| = |\Gamma_{\gamma\cdot\tau}|$. Furthermore, since $-I = \gamma(-I)\gamma^{-1}$, we have $-I \in \Gamma_\tau$ if, and only if, $-I \in \Gamma_{\gamma\cdot\tau}$. Thus, $h_\tau = h_{\gamma\cdot\tau}$. □

Observe that $h_\tau > 1$ for $\tau \in \mathbb{H}$ if, and only if, τ is an elliptic point.

Definition 7.31. For any $\tau \in \mathbb{H}$, consider the matrix

$$A_\tau = \begin{pmatrix} 1 & -\tau \\ 1 & -\overline{\tau} \end{pmatrix}. \tag{7.32}$$

This matrix is not in $\mathrm{SL}_2(\mathbb{Z})$, but we can extend our group action to it as

$$A_\tau \cdot \omega = \frac{\omega - \tau}{\omega - \overline{\tau}}. \tag{7.33}$$

In particular, note that $A_\tau \cdot \tau = 0$ and $A_\tau \cdot \overline{\tau} = \infty$.

Proposition 7.34. *We have*

$$\left(A_\tau \Gamma A_\tau^{-1}\right)_0 = A_\tau \Gamma_\tau A_\tau^{-1} \tag{7.35}$$

where $\left(A_\tau \Gamma A_\tau^{-1}\right)_0$ *is the stabilizer of* 0 *under the group action of* $A_\tau \Gamma A_\tau^{-1}$.

Hence, $\left(A_\tau \Gamma A_\tau^{-1}\right)_0$ is a cyclic group that fixes 0 and ∞, and so if $\gamma \in \left(A_\tau \Gamma A_\tau^{-1}\right)_0$ then $\gamma \cdot z = az$ for $a = e^{2\pi i/h_\tau}$. Each $\tau \in \mathbb{H}$ has neighborhood U in $\mathbb{H}$ such that if $\gamma \cdot U \cap U \neq \emptyset$ then $\gamma \in \Gamma_\tau$. No elliptic points other than τ are in U. The image $A_\tau(U)$ is a neighborhood of 0 and the map A_τ separates Γ-equivalent points in U to points separated by constant angle $2\pi/h_\tau$ — see figure 18 where $\tau = i$ and $h_i = 2$. Hence, applying the map $q : z \to z^{h_\tau}$ to the image $A_i(U)$, we see that $q \circ A_i$ is an injection from U to $q \circ A_i(U)$.

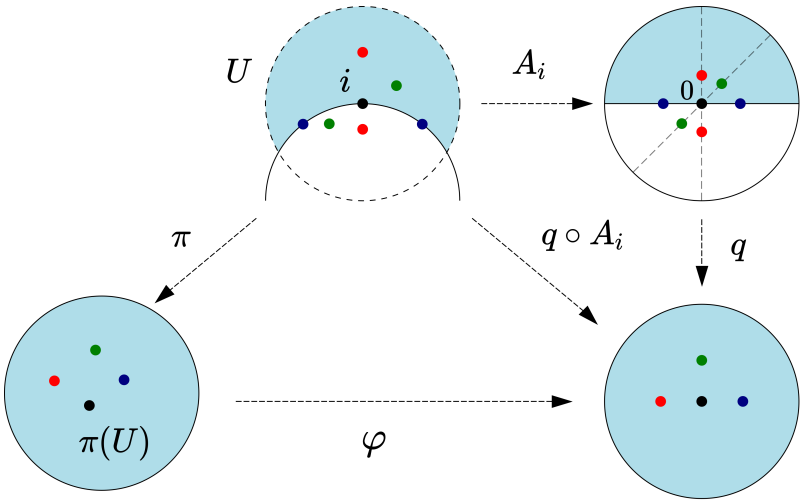


FIGURE 18

Proposition 7.36. *Let* $\psi = q \circ A_i$. *Then* $\psi(\tau_1) = \psi(\tau_2)$ *if, and only if,* $\pi(\tau_1) = \pi(\tau_2)$.

Proof. The reader is encouraged to come up with a proof. Otherwise it can be found at [1]. □

Hence, we can induce an injection $\varphi : \pi(U) \to \psi(U)$ such that $\varphi \circ \pi = \psi$. Note that π and ψ are both surjective open maps, and so φ is a homeomorphism. Defining charts around cusp points follows a similar approach to elliptic points although it might require some more familiarity with group theory than this paper assumes. A discussion of this can be found at [1] in details. Furthermore, [1] contains a tedious verification that the transition maps are indeed homolomorphic for the defined charts. This concludes our discussion of compactifying $Y(\Gamma)$.

Acknowledgments

I would like to thank my mentor, Yulia Kotelnikova, for her incredible help and patience throughout the program, and for introducing me to interesting material. I would also like to thank Peter May for organizing the REU and allowing me to participate.

References

[1] Diamond, Fred, and Jerry Shurman. A First Course in Modular Forms. 1st ed. Graduate Texts in Mathematics. New York, NY: Springer, 2010.
[2] Tom Weston. The Modular Curves $X_0(11)$ and $X_1(11)$. Arizona Winter School 2001. https://www.math.arizona.edu/ swc/aws/2001/01Weston1.pdf
[3] Bruinier, Jan Hendrik, Gerard Van Der Geer, Gunter Harder, and Don Zagier. "The 1-2-3 of Modular Forms SpringerLink." Accessed September 10, 2021. https://link.springer.com/book/10.1007/978-3-540-74119-0.
[4] Silverman, Joseph H. The Arithmetic of Elliptic Curves. New York: Springer-Verlag, 2009.
[5] https://www.win.tue.nl/ aeb/2WF02/bezout.pdf
[6] https://willierushrush.github.io/posts/2020/05/second-countability/
[7] https://math.stackexchange.com/questions/174322/orientability-of-riemann-surface/174365
[8] https://en.wikipedia.org/wiki/Fundamental domain