CALIFORNIA STATE UNIVERSITY SAN MARCOS

THESIS SIGNATURE PAGE

THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE

MASTER OF SCIENCE

IN

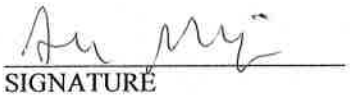
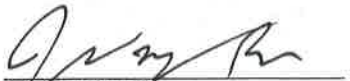
MATHEMATICS

THESIS TITLE: Data of Modular Curves

AUTHOR: Steven Newberg

DATE OF SUCCESSFUL DEFENSE: 11/28/17

THE THESIS HAS BEEN ACCEPTED BY THE THESIS COMMITTEE IN
PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF
SCIENCE IN MATHEMATICS.

Professor Shahed Sharif THESIS COMMITTEE CHAIR	 SIGNATURE	12/14/17 DATE
Professor Wayne Aitken THESIS COMMITTEE MEMBER	 SIGNATURE	12/14/17 DATE
Professor Badal Joshi THESIS COMMITTEE MEMBER	 SIGNATURE	12/13/17 DATE

CALIFORNIA STATE UNIVERSITY SAN MARCOS

MASTER'S THESIS

Data of Modular Curves

Author:
Steven NEWBERG

Supervisor:
Dr. Shahed SHARIF

A thesis submitted in fulfillment of the requirements for the degree of Master of Science

in the

Department of Mathematics
California State University San Marcos

December 14, 2017

Acknowledgements

I would like to begin by thanking my thesis advisor, Dr. Shahed Sharif, for his oft needed mathematical insight and enduring support. He holds significant responsibility for making the writing of this thesis such an enjoyable and fulfilling process.

I would also like to thank my committee members, Dr. Wayne Aitken and Dr. Badal Joshi, for their contribution to this thesis as well as my mathematical education.

I am grateful to my parents, Nick and Bella, for supporting my decision to pursue a graduate degree and for their unwavering encouragement at every step of the way. To my sister, Nicole, for assisting with my thesis submission and listening to my explanations of problems that I was working on.

Lastly, I would like to thank my best friend and wife, Heidi, for her unconditional love and encouragement. She allowed me to spend countless days and nights buried in a book or huddled over my keyboard. She has kept me grounded during the writing of this thesis.

Data of Modular Curves

Steven NEWBERG

Abstract

A moduli problem seeks to find a bijection between a class of objects and a topological space that describes the parameters of the class of objects. We will present the moduli problem for a type of curve used in cryptography, elliptic curves.

The topological space describing elliptic curves is the quotient of the complex plane by the action of matrices in $\mathrm{SL}_2(\mathbb{Z})$, which we call a *modular curve*. Taking a quotient of the upper half of the complex plane by subgroups of $\mathrm{SL}_2(\mathbb{Z})$ also give moduli spaces of elliptic curves but include some extra structure. There are special points on modular curves, which we will discuss and give methods for finding.

Contents

Chapter 1

Introduction

1.1 Moduli problem

We first present the idea of a *moduli problem*. A moduli problem seeks to find a bijection between a class of objects and a topological space that describes the parameters of the class of objects.

The key steps in solving a moduli problem are (1) defining the class of objects that we hope to describe; (2) determining the parameters, or what distinguishes one object from another; and (3) defining an equivalence relation for our parameter space. For clarity, we will show a few examples of moduli problems.

Example 1.1. We want to describe all the circles in $\mathbb{R}^2$.

We know that given any three distinct points we can define a circle. Unfortunately there are infinitely many points on any circle in the plane, so there are infinite triples of points that describe the same circle. This means 3 points do not uniquely define a circle, but we require uniqueness for our moduli space.

Instead we can describe distinct circles by their center and their radius. Since the center and radius can be represented by a triple (a, b, r) for $a, b, r \in \mathbb{R}$ and $r > 0$, the moduli space of circles is

$$M = \{(a, b, r) \in \mathbb{R}^3 | r > 0\}.$$

The map f which takes M to circles in $\mathbb{R}^2$ is clearly bijective. So the topological space M is a moduli space for the set of circles in $\mathbb{R}^2$.

Example 1.2. We want to describe all the triangles in the real plane.

We first observe that a triangle depends on the coordinates of its vertices a_1, a_2 and a_3, with each $a_i \in \mathbb{R}^2$. The question we need to ask is when do these points not specify a triangle. The only condition we need for our three points is that they are not collinear. We define the space C to be

$$C = \{(a_1, a_2, a_3) | a_i\text{'s are collinear}\}.$$

We see that any triangle can be represented by at least one point in $(\mathbb{R}^2)^3 - C$, but it is possible that one triangle corresponds to multiple points in this topological space. Notice that (a_1, a_2, a_3) and (a_2, a_1, a_3) both give the same triangle in the plane. It does not matter what order we list the vertices of the triangle, so all such permutations of the points a_1, a_2 and a_3 give the same triangle.

Recall that S_3 is the set of permutations on a set of size 3. We will define a group action on the set $(\mathbb{R}^2)^3 - C$. For $\sigma \in S_3$, define $\sigma(a_1, a_2, a_3) = (a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)})$. We would now like to prove the following proposition:

Proposition 1.3. Two triples (a_1, a_2, a_3) and (b_1, b_2, b_3) in $(\mathbb{R}^2)^3 - C$ give the same triangle if and only if there exists $\sigma \in S_3$ such that $\sigma((a_1, a_2, a_3)) = (b_1, b_2, b_3)$.

Proof. To prove the forward direction let (a_1, a_2, a_3) and (b_1, b_2, b_3) give the same triangle in $(\mathbb{R}^2)^3 - C$. Since a triangle has exactly 3 vertices then (a_1, a_2, a_3) and (b_1, b_2, b_3) contain the same points but permuted in some manner. Therefore for some $\sigma \in S_3$ we have that $\sigma((a_1, a_2, a_3)) = (b_1, b_2, b_3)$.

For the reverse direction let $\sigma((a_1, a_2, a_3)) = (b_1, b_2, b_3)$ for some $\sigma \in S_3$. Then (a_1, a_2, a_3) and (b_1, b_2, b_3) contain the same points a_i and b_j in $\mathbb{R}^2$. In the plane these sets of vertices are identical and hence give the same triangle. □

We have shown that different points give the same triangle if and only if they are permutations of each other. In our moduli space we require that distinct points give distinct objects so points that differ by a permutation are equivalent. We achieve this equivalence by modding out by the group action on $((\mathbb{R}^2)^3 - C)$:

$$S_3 \backslash ((\mathbb{R}^2)^3 - C) = \{\{\sigma(\alpha) : \sigma \in S_3\} : \alpha \in ((\mathbb{R}^2)^3 - C)\}.$$

Since we have shown triples give the same triangle only when permuted then this gives us a moduli space for all triangles in $\mathbb{R}^2$.

In our second example we saw the importance of finding all possible equivalences in our topological space and how to translate such an equivalence to our moduli space. The goal of this chapter will be to find the moduli space for elliptic curves.

1.2 Elliptic curves

To begin discussing the moduli problem for elliptic curves we first need to explore the types of objects that we would like to describe. We must first define the notion of a *lattice*.

Definition 1.4. A *lattice* $\Lambda \subset \mathbb{C}$ is a set of the form

$$\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z} = \{\omega_1\alpha + \omega_2\beta : \alpha, \beta \in \mathbb{Z}\}$$

where ω_1, ω_2 are $\mathbb{R}$-independent elements of $\mathbb{C}$ and are called a *basis* of Λ. Note that a basis of a lattice is not unique.

Definition 1.5. Fix a lattice Λ with basis ω_1 and ω_2. An *elliptic curve*, $E(\Lambda)$, is the quotient space $\mathbb{C}/\Lambda$. Two points $z, z' \in \mathbb{C}$ are equivalent if and only if there exist $m, n \in \mathbb{Z}$ such that

$$z = z' + m\omega_1 + n\omega_2.$$

Definition 1.6. Given a topological space X under a group action G, we define a *fundamental domain* to be a set of representatives for orbits in X.

Notice that the elliptic curve $E(\Lambda)$ contains infinitely many orbits and each orbit contains infinitely many points. Given an elliptic curve $E(\Lambda)$ and lattice Λ with basis ω_1 and ω_2 we define the *fundamental parallelogram* to be the set

$$\mathcal{P} = \{a\omega_1 + b\omega_2 : 0 \leq a < 1, 0 \leq b < 1\}.$$

Topologically this gives a parallelogram in the complex plane with opposite sides "glued" together. One can show that this is a fundamental domain.

From our discussion of moduli spaces, the first step in finding a moduli space is determining when two elliptic curves are isomorphic.

Definition 1.7. Two elliptic curves are *isomorphic* if there exists a holomorphic group isomorphism between them; that is, they are isomorphic as groups with the extra condition that the isomorphism between them is holomorphic.

Let $\Lambda(\omega_1, \omega_2)$ be the lattice formed by the basis ω_1 and ω_2. Let $\Lambda_1 = \Lambda(1, i)$ and $\Lambda_2 = \Lambda(2, 2i)$. By observation we can see that one lattice can be mapped to the other by stretching the smaller lattice using the function $\phi : \Lambda_1 \to \Lambda_2$ given by $z \mapsto 2z$. Notice that Λ_1 and Λ_2 are in fact different lattices since $(0, i) \in \Lambda_1$ but $(0, i) \notin \Lambda_2$.

Definition 1.8. Two lattices Λ_1 and Λ_2 are *homothetic* if and only if $\Lambda_1 = \alpha\Lambda_2$ for some $\alpha \in \mathbb{C}$. We will denote two homothetic lattices by $\Lambda_1 \sim \Lambda_2$.

Homothety of lattices is actually the property that defines isomorphic elliptic curves.

Theorem 1.9. *The elliptic curves $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are isomorphic if and only if there exists $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 = \Lambda_2$; that is, Λ_1 and Λ_2 are homothetic.*

Proof. [DS05, Corollary 1.3.3] □

1.3 Complex upper half-plane

From the previous section we saw that two elliptic curves are isomorphic if the associated lattices are homothetic. The goal of this section will be to give a map from the upper half-plane under a group action to the set of elliptic curves.

Consider the elliptic curve $E(\Lambda)$ where Λ is a lattice with basis elements ω_1 and ω_2. Both basis elements are nonzero since they are $\mathbb{R}$-linearly independent. Therefore we get the following homothety:

$$\Lambda(\omega_1, \omega_2) \sim \left(\frac{1}{\omega_1}\right)(\Lambda(\omega_1, \omega_2)) = \Lambda\left(1, \frac{\omega_2}{\omega_1}\right).$$

We can see that any lattice is homothetic to a lattice of the form $\Lambda(1, \tau)$. Since ω_1 and ω_2 are linearly independent over $\mathbb{R}$ then $\tau = \frac{\omega_2}{\omega_1}$ must have a nonzero imaginary part. The next lemma will show that, in fact, we can choose τ in the upper half-plane.

Lemma 1.10. Given a lattice $\Lambda(\omega_1, \omega_2)$ there is a lattice of the form $\Lambda(1, \tau)$ with $\text{Im}(\tau) > 0$ such that $\Lambda(\omega_1, \omega_2) \sim \Lambda(1, \tau)$.

Proof. Consider the lattice $\Lambda(\omega_1, \omega_2)$. Above we saw that $\Lambda(\omega_1, \omega_2) \sim \Lambda\left(1, \frac{\omega_2}{\omega_1}\right)$ and so $\Lambda(\omega_1, \omega_2) \sim \Lambda(1, \tau)$ where $\tau = \frac{\omega_2}{\omega_1}$.

If $\text{Im}(\tau) < 0$ then $\text{Im}(-\tau) > 0$. Therefore either τ or $-\tau$ is in the upper half-plane. Observe that for any complex number $\alpha \in \mathbb{C}$ with $\text{Im}(\alpha) \neq 0$, the lattices $\Lambda(1, \alpha)$ and $\Lambda(1, -\alpha)$ are equal since negating a basis element does not change the lattice. Therefore $\Lambda(\omega_1, \omega_2) \sim \Lambda(1, \tau)$ and $\Lambda(\omega_1, \omega_2) \sim \Lambda(1, -\tau)$ with either τ or $-\tau$ in the upper half-plane. □

The above lemma shows that every elliptic curve is isomorphic to an elliptic curve $E(\Lambda(1, \tau))$ where $\text{Im}(\tau) > 0$.

1.3.1 Action of $\text{SL}_2(\mathbb{Z})$ on $\mathbb{H}$

The basis of a lattice is not unique and so two different bases can represent the same lattice. Two bases give the same lattice if and only if they are $\mathbb{Z}$-linear combinations of each other. More explicitly two bases ω_1, ω_2 and ω_1', ω_2' give the same lattice if and only if

$$\begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} \tag{1.1}$$

for some matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \text{GL}_2(\mathbb{Z})$.

We denote the set of points in the upper half-plane as

$$\mathbb{H} = \{\tau \in \mathbb{C} : \text{Im}(\tau) > 0\}.$$

Given $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \text{SL}_2(\mathbb{Z})$ and $\tau \in \mathbb{H}$, define the action of $\text{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ by

$$A\tau = \frac{a\tau + b}{c\tau + d} \qquad \text{for } \tau \in \mathbb{H}. \tag{1.2}$$

One checks that this is a well-defined action.

We would like to verify that the action of $\text{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ is closed, that is, given a point $\tau \in \mathbb{H}$, $A\tau \in \mathbb{H}$ for every $A \in \text{SL}_2(\mathbb{Z})$.

Lemma 1.11. Let $z \in \mathbb{H}$ and $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \text{SL}_2(\mathbb{Z})$. If $Az = z'$ then $z' \in \mathbb{H}$.

Proof. Observe that

$$\begin{aligned}\mathrm{Im}(z') = \mathrm{Im}(Az) &= \mathrm{Im}\left(\frac{az+b}{cz+d}\right)\\ &= \mathrm{Im}\left(\frac{(az+b)(c\bar{z}+d)}{(cz+d)(c\bar{z}+d)}\right)\\ &= \frac{\mathrm{Im}(acz\bar{z}+azd+bc\bar{z}+bd)}{|cz+d|^2}\\ &= \frac{(ad-bc)\mathrm{Im}(z)}{|cz+d|^2}\\ &= \frac{\mathrm{Im}(z)}{|cz+d|}.\end{aligned}$$

By our assumption, $A \in \mathrm{SL}_2(\mathbb{Z})$, and so $ad - bc = 1$. Therefore $\mathrm{Im}(z') > 0$. □

Lemma 1.12. If $\Lambda(1,\tau) \sim \Lambda(1,\tau')$ for $\tau, \tau' \in \mathbb{H}$ then $A\tau' = \tau$ for some $A \in \mathrm{SL}_2(\mathbb{Z})$.

Proof. Let $\Lambda(1,\tau) \sim \Lambda(1,\tau')$. Therefore $\Lambda(1,\tau') = \Lambda(\alpha, \alpha\tau)$ for some $\alpha \in \mathbb{C}$ with $\alpha \neq 0$. This gives us that for some $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbb{Z})$

$$\begin{aligned}\begin{bmatrix}\alpha\tau \\ \alpha\end{bmatrix} &= \begin{bmatrix} a & b \\ c & d\end{bmatrix}\begin{bmatrix}\tau' \\ 1\end{bmatrix}\\ &= \begin{bmatrix} a\tau'+b \\ c\tau'+d\end{bmatrix}.\end{aligned}$$

Hence $\left[\begin{smallmatrix}\alpha\tau \\ \alpha\end{smallmatrix}\right] = \left[\begin{smallmatrix} a\tau'+b \\ c\tau'+d\end{smallmatrix}\right]$ and this implies that

$$a\tau' + b = \alpha\tau \tag{1.3}$$
$$c\tau' + d = \alpha. \tag{1.4}$$

Let $A = \left[\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right]$. Since $\alpha \neq 0$, we may divide (1.3) by (1.4) which gives

$$A\tau' = \tau.$$

Using the formula $\mathrm{Im}(\tau') = \frac{\mathrm{Im}(\tau)}{|c\tau+d|}$, we conclude that $ad - bc > 0$ since $\tau, \tau' \in \mathbb{H}$. Therefore $A \in \mathrm{SL}_2(\mathbb{Z})$, which proves the lemma. □

We would like to give a map between the set of isomorphism classes of elliptic curves to the quotient of the upper half-plane by $\mathrm{SL}_2(\mathbb{Z})$. Let $\mathrm{SL}_2(\mathbb{Z})\tau$ denote the orbit of τ under the action of $\mathrm{SL}_2(\mathbb{Z})$. Consider the set

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} = \{\mathrm{SL}_2(\mathbb{Z})\tau : \tau \in \mathbb{H}\}.$$

We now define the function

$$f : \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \longrightarrow \{\text{elliptic curves}\}/\sim$$

by

$$f(\mathrm{SL}_2(\mathbb{Z})\tau) = E(\Lambda(1,\tau)).$$

Theorem 1.13. *The map f is well-defined.*

Proof. Let $\mathrm{SL}_2(\mathbb{Z})\tau = \mathrm{SL}_2(\mathbb{Z})\tau'$ and so $A\tau = \tau'$ for some $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$.

We have that

$$\begin{aligned} f(\mathrm{SL}_2(\mathbb{Z})\tau) &= E(\Lambda(1,\tau)) \quad \text{and} \\ f(\mathrm{SL}_2(\mathbb{Z})\tau') &= E(\Lambda(1,\tau')) = E(\Lambda(1,A\tau)). \end{aligned}$$

If $\Lambda(1,\tau) \sim \Lambda(1,A\tau)$ then $E(\Lambda(1,\tau))$ is isomorphic to $E(\Lambda(1,A\tau))$. Therefore it suffices to show the claim that $\Lambda(1,\tau) \sim \Lambda(1,A\tau)$. Notice that

$$\Lambda\left(1, \frac{a\tau+b}{c\tau+d}\right) \sim \Lambda(c\tau+d, a\tau+b). \tag{1.5}$$

We will show that $\Lambda(1,\tau) = \Lambda(c\tau+d, a\tau+b)$. First we have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \tau \\ 1 \end{bmatrix} = \begin{bmatrix} a\tau+b \\ c\tau+d \end{bmatrix}. \tag{1.6}$$

Observe that

$$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} a\tau+b \\ c\tau+d \end{bmatrix} = \begin{bmatrix} \tau \\ 1 \end{bmatrix}. \tag{1.7}$$

By (1.6) and (1.7), the bases $\tau, 1$ and $c\tau+d, a\tau+b$ are $\mathbb{Z}$-linear combinations of each other. Therefore $\Lambda(1,\tau) = \Lambda(c\tau+d, a\tau+b)$.

Combining (1.5) and $\Lambda(1,\tau) = \Lambda(c\tau+d, a\tau+b)$ we get that $\Lambda(1,\tau) \sim \Lambda(1,A\tau)$ which proves the theorem. □

To show that $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is a moduli space we need to show that f is a bijection.

Theorem 1.14. *The map f is a bijection.*

Proof. First we will show that the map is surjective. Let $E(\Lambda(\omega_1,\omega_2))$ be an elliptic curve. By Lemma 1.10 there is $\tau \in \mathbb{H}$ such that $\Lambda(\omega_1,\omega_2) \sim \Lambda(1,\tau)$. Therefore $f(\mathrm{SL}_2(\mathbb{Z})\tau) = E(\Lambda(1,\tau))$ and since $E(\Lambda(\omega_1,\omega_2))$ is isomorphic to $E(\Lambda(1,\tau))$, this proves surjectivity.

Now we will show injectivity. Let $f(\mathrm{SL}_2(\mathbb{Z})\tau) = f(\mathrm{SL}_2(\mathbb{Z})\tau')$ for $\tau, \tau' \in \mathbb{H}$. Therefore $E(\Lambda(1,\tau))$ and $E(\Lambda(1,\tau'))$ are in the same isomorphism class and so $\Lambda(1,\tau) \sim \Lambda(1,\tau')$. By Lemma 1.12, if $\Lambda(1,\tau) \sim \Lambda(1,\tau')$ then $\tau = A\tau'$ for some $A \in \mathrm{SL}_2(\mathbb{Z})$ and so $\mathrm{SL}_2(\mathbb{Z})\tau = \mathrm{SL}_2(\mathbb{Z})\tau'$ which proves injectivity. □

Since f is a bijection then $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is a moduli space for the set of elliptic curves.

1.4 Modular curves

The previous section showed that every elliptic curve is represented by a point in the moduli space $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. Although it will not be covered in this thesis, one can study the moduli space to find general properties of elliptic curves. Additionally, restricting the group action to certain subgroups of $\mathrm{SL}_2(\mathbb{Z})$ gives rise to moduli spaces for the set of elliptic curves with some additional information. This thesis will only discuss the moduli spaces that arise; the details regarding their relationship to elliptic curves can be found in [DS05, Section 1.4].

The following definitions will be used to define the different moduli spaces.

Definition 1.15. The *principal congruence subgroup of level N*, denoted $\Gamma(N)$, is given by

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

Definition 1.16. A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a *congruence subgroup* if $\Gamma(N) \subset \Gamma$ for some $N \in \mathbb{Z}^+$. The two such congruence subgroups that will be studied in this thesis are

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} \star & \star \\ 0 & \star \end{bmatrix} (\mathrm{mod}\ N) \right\} \quad \text{and}$$
$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & \star \\ 0 & 1 \end{bmatrix} (\mathrm{mod}\ N) \right\}$$

where $\star$ denotes an entry in the matrix that is not restricted.

Definition 1.17. Let Γ be a congruence subgroup. The corresponding *modular curve* is defined as

$$Y(\Gamma) = \Gamma\backslash\mathbb{H} = \{\Gamma\tau : \tau \in \mathbb{H}\};$$

that is, the orbits of elements in $\mathbb{H}$ under the action of Γ.

We will write

$$\pi : \mathbb{H} \to Y(\Gamma) \tag{1.8}$$

for the natural surjection given by $\tau \mapsto \Gamma\tau$.

For brevity we will denote $Y(\Gamma(N))$ as $Y(N)$ and we will define $Y(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. Similarly, we denote $Y(\Gamma_0(N))$ and $Y(\Gamma_1(N))$ as $Y_0(N)$ and $Y_1(N)$ respectively.

Since these topological spaces are abstract and hard to visualize, one can give a fundamental domain for each modular curve. The fundamental domain for $Y(1)$ is given by the following proposition.

Proposition 1.18. A fundamental domain of $Y(1)$ is the space

$$\mathcal{M} = \{z = x+iy : -1/2 \leq x < 1/2, |z| > 1\} \cup \{z \in \mathbb{H} : |z| = 1, -1/2 \leq \mathrm{Re}(z) \leq 0\}.$$

Proof. See [DS05] Lemma 2.3.1 and Lemma 2.3.2. □

1.5 Elliptic points

One of the goals of this thesis is to identify important points on modular curves. A type of point that we are interested in finding is called an *elliptic point*. These are defined as points in the upper half-plane with nontrivial stabilizers. Since $-I$ and I act trivially on the upper half-plane, we refer to $\{\pm I\}$ as the *trivial stabilizer*.

Definition 1.19. Given a congruence subgroup Γ, a point $z \in \mathbb{H}$ is an *elliptic point* of Γ if there exists $\gamma \in \Gamma, \gamma \neq \pm I$ such that $\gamma z = z$.

The following lemma will be used to find the cusps of $Y(1)$:

Lemma 1.20. Let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

(a) If γ has order 3 then γ is conjugate to $\left[\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right]$ in $\mathrm{SL}_2(\mathbb{Z})$.

(b) If γ has order 4 then γ is conjugate to $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ in $\mathrm{SL}_2(\mathbb{Z})$.

(c) If γ has order 6 then γ is conjugate to $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right]$ in $\mathrm{SL}_2(\mathbb{Z})$.

Proof. See [DS05] Proposition 2.3.3 □

For the first example we will find the elliptic points of $Y(1)$.

Theorem 1.21. *The modular curve $Y(1) = SL_2(\mathbb{Z})\backslash\mathbb{H}$ has two elliptic points, the orbits of i and $\rho = e^{2\pi i/3}$.*

Proof. We want to find points $\tau \in \mathbb{H}$ such that there exists $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z}), \gamma \neq \pm I$ for which $\gamma\tau = \tau$. We need to satisfy the condition

$$\frac{a\tau + b}{c\tau + d} = \tau.$$

Therefore we want to solve

$$c\tau^2 + (d - a)\tau - b = 0.$$

If $c = 0$ and $a = d$ then $b = 0$ which forces $a = d = \pm 1$. Therefore $\gamma = \pm I$. Recall that τ is an elliptic point when $\gamma\tau = \tau$ for some $\gamma \neq \pm I$.

If $c = 0$ and $a \neq d$, then $\tau = b/(d - a)$. We assumed that $b, d, a \in \mathbb{Z}$ which implies that $\tau \in \mathbb{Q}$. This contradicts that τ is in $\mathbb{H}$.

Therefore $c \neq 0$. The discriminant is

$$(a - d)^2 + 4bc.$$

Since $\tau \in \mathbb{H}$ then there is a nonzero imaginary part so the discriminant is negative and must satisfy $(a - d)^2 + 4bc < 0$. Rearranging these terms we get

$$\begin{aligned} (a - d)^2 + 4bc &= a^2 - 2ad + d^2 + 4bc \\ &= (a + d)^2 - 4ad + 4bc \\ &= (a + d)^2 - 4 \qquad \text{since } ad - bc = 1. \end{aligned}$$

Therefore $(a+d)^2 < 4$ and

$$|a+d| < 2.$$

The characteristic polynomial of γ is

$$(a-x)(d-x) - bc = x^2 - (a+d)x + 1.$$

Our condition for $a+d$ implies that the characteristic polynomial is either x^2+1, x^2+x+1, or x^2-x+1.

Notice that x^2+x+1 and x^2-x+1 are both factors of x^6-1 so γ must satisfy the equation $\gamma^6 - I = 0$ or $\gamma^6 = I$. Therefore in these cases γ has order 6, 3, or 2.

Similarly x^2+1 is a factor of x^4-1 and so by the same argument in this case γ satisfies $\gamma^4 = I$ and so γ has order 4 or 2. Therefore γ has order 2, 3, 4, or 6.

If $\gamma^2 = I$ then $\gamma^2 - I = 0$ and so the minimal polynomial $p(t)$ of γ is either $t+1$, $t-1$, or t^2-1. If the minimal polynomial is t^2-1 then the determinant of γ is -1, which is a contradiction. If the minimal polynomial of γ is $t+1$ then $\gamma = -I$ and if the minimal polynomial of γ is $t-1$ then $\gamma = I$. Hence if $\gamma^2 = I$ then $\gamma = \pm I$ and so γ must have order 3, 4 or 6.

By Lemma 1.20 we know that γ is conjugate to either $\left[\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ or $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right]$.

We can now compute the fixed elements of the above matrices. For $\left[\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right]$ we want to find $z \in \mathbb{H}$ such that $\left[\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right] z = z$ so we want to solve the equation

$$\begin{aligned} \frac{1}{-z-1} &= z \qquad \text{or} \\ z^2 + z + 1 &= 0. \end{aligned}$$

Solving this quadratic gives the solutions $z = (-1 \pm i\sqrt{3})/2$, and since we are finding points in the upper half-plane we get one solution, $z = (-1+i\sqrt{3})/2$.

Now we find the point fixed by the matrix $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$:

$$\begin{aligned} \frac{-1}{z} &= z \qquad \text{so} \\ z^2 + 1 &= 0. \end{aligned}$$

This gives $z = i$.

If γ has order 4 then it is conjugate to $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ and so it has the form $\alpha \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \alpha^{-1}$. If a point z is fixed by γ then

$$\begin{aligned} \alpha \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \alpha^{-1}(z) &= z \qquad \text{so} \\ \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \alpha^{-1}(z) &= \alpha^{-1}(z). \end{aligned}$$

We found that i is the fixed element of $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ and so $\alpha^{-1}(z) = i$. Therefore $z = \alpha(i)$ which shows that the fixed point of γ is $\alpha(i)$.

A similar argument can be used to show that if γ has order 3 then it fixes some point in the orbit of ρ.

For the case where γ has order six, notice that if γ is in the stabilizer of some point z, then so is γ^2. Since γ^2 has order three, then the set of points fixed by γ is a subset of the elements from the order three case, which we have already solved.

The points i and ρ are distinct since they both lie in our fundamental domain for $Y(1)$ and therefore we get the elliptic points of $Y(1)$ as the orbits of i and ρ. □

1.6 Modular curve as a Riemann surface

We will now introduce the concept of a *compact Riemann surface*. A Riemann surface looks like the complex plane locally but globally can have a different topology.

Definition 1.22. A *Riemann surface* is a topological surface X that satisfies the following properties:

1. X is *Hausdorff*: if $\tau_1, \tau_2 \in \mathbb{H}$, there exist respective neighborhoods U_1 and U_2 of τ_1 and τ_2 such that if $\tau_1 \neq \tau_2$ then $\pi(U_1) \cap \pi(U_2) = \emptyset$.

2. has a *complex structure*, which is a covering $X = \bigcup_{i \in I} U_\alpha$ by open subsets along with homeomorphisms $z_i : U_i \to V_i$ where V_i is a connected open subset of $\mathbb{C}$. Additionally we require that $U_i \cap U_j \neq \emptyset$ implies that $z_j \circ z_i^{-1} : z_i(U_i \cap U_j) \to z_j(U_i \cap U_j)$ is holomorphic. If U_i is a neighborhood of a point $x \in X$, we define a *chart* for x to be a pair (U_i, z_i).

The details of the proof that $Y(\Gamma)$ is a Riemann surface can be found in [DS05, Chapter 2].

1.7 Degree

1.7.1 Properties of maps between compact Riemann surfaces

We would like to define the notion of the *degree* of maps between Riemann surfaces. Specifically we will be looking at maps between modular curves. For the purposes of this thesis we will be using a topologically motivated definition of *degree* and *ramification degree*.

Theorem 1.23. *Let $g : X \to Y$ be an analytic, nonconstant function between connected compact Riemann surfaces X and Y. Given $x \in X$ with $y = g(x)$ there exists an integer m_x such that for every neighborhood V of x there is a neighborhood $U \subset V$ of x such that every point, except possibly y, in $g(U)$ has m_x preimages in U.*

Proof. See the Open-Mapping Theorem [Mir95, Proposition 3.8] and [Mir95, Proposition 4.1]. □

Definition 1.24. Given an analytic, nonconstant function $f : X \to Y$ between connected compact Riemann surfaces X and Y, the integer m_x from the above theorem is called the *ramification degree* of x.

Definition 1.25. Let $f : X \to Y$ be an analytic, nonconstant function between connected compact Riemann surfaces X and Y. Choose some $y \in Y$. Then the *degree* of f at y, denoted $\deg_y(f)$, is the number of preimages of a point y counting ramification degree. More explicitly we have

$$\deg_y(f) = \sum_{x \in f^{-1}(y)} m_x.$$

Proposition 1.26. The degree of f at y is independent of y.

Proof. [Mir95, Proposition 4.8] □

Due to Proposition 1.26, we can denote the degree $\deg(f)$.

Definition 1.27. Let $f : X \to Y$ be an analytic, nonconstant function between connected compact Riemann surfaces X and Y. A point $x \in X$ is a *ramification point* if $m_x \geq 2$.

Lemma 1.28. Let $f : X \to Y$ be an analytic, nonconstant function between connected compact Riemann surfaces X and Y. The number of ramification points is finite.

Proof. By [Mir95, Lemma 4.4] the number of ramifications points is discrete and since X is a compact the number of ramifications points is finite. □

The degree of the maps between modular curves can be found explicitly.

Theorem 1.29. *Let Γ_1 and Γ_2 be congruence subgroups of $SL_2(\mathbb{Z})$ with $\Gamma_1 \subset \Gamma_2$. We define the map $f : Y(\Gamma_1) \to Y(\Gamma_2)$ given by $\Gamma_1\tau \mapsto \Gamma_2\tau$. The degree of f is given by*

$$\deg(f) = \begin{cases} [\Gamma_2 : \Gamma_1]/2 & \text{if } -I \in \Gamma_2 \text{ and } -I \notin \Gamma_1 \\ [\Gamma_2 : \Gamma_1] & \text{otherwise.} \end{cases}$$

Proof. Let $\{\pm I\}\Gamma_2 = \bigcup_j \{\pm I\}\Gamma_1\gamma_j$ be a coset decomposition. Since Γ_1 and Γ_2 are finite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$ then $[\{\pm I\}\Gamma_2 : \{\pm I\}\Gamma_1]$ is finite. Observe that the number of cosets is $[\{\pm I\}\Gamma_2 : \{\pm I\}\Gamma_1]$ and that

$$[\{\pm I\}\Gamma_2 : \{\pm I\}\Gamma_1] = \begin{cases} [\Gamma_2 : \Gamma_1]/2 & \text{if } -I \in \Gamma_2 \text{ and } -I \notin \Gamma_1 \\ [\Gamma_2 : \Gamma_1] & \text{otherwise.} \end{cases}$$

Therefore it suffices to show that the number of preimages for most points in the codomain is $[\{\pm I\}\Gamma_2 : \{\pm I\}\Gamma_1]$.

Let $\Gamma_2\tau$ be an orbit in $Y(\Gamma_2)$. Then $f^{-1}(\Gamma_2\tau) = \{\Gamma_1\gamma_j\tau\}$ for all j.

We claim that if τ is not an elliptic point for Γ_2 then $\Gamma_1\gamma_i\tau \neq \Gamma_1\gamma_j\tau$ for all $i \neq j$. We prove the contrapositive, so assume that $\Gamma_1\gamma_i\tau = \Gamma_1\gamma_j\tau$. Then $\alpha\gamma_i\tau = \gamma_j\tau$ for some $\alpha \in \Gamma_1$. This implies that $\gamma_j^{-1}\alpha\gamma_i\tau = \tau$ with $\gamma_j^{-1}\alpha\gamma_i \in \Gamma_2$.

We show that $\gamma_j^{-1}\alpha\gamma_i \neq \pm I$. If $\gamma_j^{-1}\alpha\gamma_i = \pm I$ then $\alpha\gamma_i = \pm\gamma_j$ which is a contradiction since the cosets $\{\pm I\}\Gamma_1\gamma_j$ are disjoint. Therefore $\gamma_j^{-1}\alpha\gamma_i \neq \pm I$ and so τ is an elliptic point, which proves the claim.

We showed that if τ is not an elliptic point for Γ_2 then $\Gamma_1\gamma_i\tau \neq \Gamma_1\gamma_j\tau$ for all $i \neq j$. Therefore the number of preimages of $\Gamma_2\tau$ equals $[\{\pm I\}\Gamma_2 : \{\pm I\}\Gamma_1]$ which proves the theorem. □

1.8 Genus

Another important invariant of Riemann surfaces is the genus. In this thesis we will be using the topological definition of genus.

Proposition 1.30. Every compact and connected Riemann surface is homeomorphic to a sphere with g handles, where g is a nonnegative integer.

Proof. See [Mir95, Proposition 1.23]. □

Definition 1.31. The integer g from Proposition 1.30 is called the $genus$.

In order to compute the genus we will use the following formula

Theorem 1.32. *(Riemann-Hurwitz Formula) Let $f : X \to Y$ be a nonconstant map between connected, compact Riemann surfaces. Let g_X be the genus of X, g_Y the genus of Y, d the degree of f, and m_x be the ramification degree of $x \in X$. The following formula holds:*

$$2g_X - 2 = d(2g_Y - 2) + \sum_{x \in X}(m_x - 1).$$

Proof. [Mir95, Theorem 4.11] □

For Theorem 1.32 note that the sum $\sum_{x\in X}(m_x - 1)$ is finite since the number of ramifications points is finite.

The goal of this thesis is to tabulate important properties of various modular curves. These include elliptic points and cusps with their ramification degrees as well as the genera of different modular curves.

Chapter 2

Cusps

2.1 Definitions

In Section 1.6 we discussed the fact that $Y(\Gamma)$ is a Riemann surface, but many results pertaining to Riemann surfaces require that they be compact. Since $Y(\Gamma)$ is not compact then we will make the surface compact by adding a "point at infinity" as well as points in the orbit of infinity under the action of $\mathrm{SL}_2(\mathbb{Z})$.

Denote the set $\mathbb{Q}^\star = \mathbb{Q} \cup \{\infty\}$. We would like to define the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{Q}^\star$. For $\frac{m}{n} \in \mathbb{Q}$ and $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$, define the action by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \frac{m}{n} = \frac{am + bn}{cm + dn}.$$

If $cm + dn = 0$ then $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] (m/n)$ is the point ∞.
Define the action of $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$ on ∞ as

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \infty = \frac{a}{c}.$$

We can represent the point ∞ by $\frac{1}{0}$.

Definition 2.1. Given a congruence subgroup Γ, the *cusps* of Γ are the orbits of $\mathbb{Q}^\star$ under the action of Γ.

In general, we add cusps to the modular curve $Y(\Gamma)$ and the result will be a compact Riemann surface, which we will denote $X(\Gamma)$. Let $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q}^\star$. Then we define

$$X(\Gamma) = \Gamma \backslash \mathbb{H}^*.$$

We define $X(1)$ to be the modular curve $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*$. We will use similar notation to $Y(\Gamma)$ and denote $X(\Gamma(N))$ as $X(N)$, and $X(\Gamma_0(N))$ and $X(\Gamma_1(N))$ as $X_0(N)$ and $X_1(N)$ respectively.

The modular curve $X(\Gamma)$ is a Riemann surface; see [DS05, Chapter 2]. For any real number k define the set

$$V_k = \{z \in \mathbb{H}^\star : \mathrm{Im}(z) > k\}.$$

These sets will serve as a basis for the neighborhoods of ∞.

Theorem 2.2. *$X(1)$ is compact.*

Proof. Recall the fundamental domain for $Y(1)$ which is given by

$\mathcal{M} = \{z = x+iy : -1/2 \leq x < 1/2, |z| > 1\} \cup \{z \in \mathbb{H} : |z| = 1, -1/2 \leq \mathrm{Re}(z) \leq 0\}$.

Let $\overline{\mathcal{M}}$ denote the closure of $\mathcal{M}$. The topology of $X(1)$ is the quotient topology from $\mathbb{H}$ and so it is sufficient to show that $\mathcal{M}^\star = \overline{\mathcal{M}} \cup \{\infty\}$ is compact. Consider an open covering of $\{U_i\}$ of $\mathcal{M}^\star$. There is an element of the open cover that contains ∞, say U_0. Clearly $\mathcal{M}^\star - U_0$ is compact since it is closed and bounded and so there is a finite subcover $\{U_1, \ldots, U_n\}$ that covers this set. The set $\{U_0, U_1, \ldots, U_n\}$ is a finite covering of $\mathcal{M}^\star$ and so $\mathcal{M}^\star$ is compact. □

2.2 Computing cusps of $X(1)$

Recall that cusps are defined as the orbits of points in $\mathbb{Q}^\star$ under the action of a congruence subgroup Γ. Therefore we will refer to a cusp as an element of $\Gamma\backslash\mathbb{Q}^\star$.

We would like to give a system of representatives for the cusps of $X(N)$, $X_1(N)$, and $X_0(N)$.

In order to compute a system of representatives we need some conditions for when points in $\mathbb{Q}^\star$ represent the same cusp. The following theorem will be useful in giving explicit equivalence conditions.

Proposition 2.3. Let $s, s' \in \mathbb{Q}^\star$ be given by $s = (a/c)$ and $s' = (a'/c')$ with $\gcd(a, c) = \gcd(a', c') = 1$. Then

$$\mathrm{SL}_2(\mathbb{Z})s' = \mathrm{SL}_2(\mathbb{Z})s \iff \begin{bmatrix} a' \\ c' \end{bmatrix} = \pm\gamma \begin{bmatrix} a \\ c \end{bmatrix}$$

for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Proof. See [DS05, Lemma 3.8.1] □

Recall that cusps are elements of $\Gamma\backslash\mathbb{Q}^\star$. Denote the set

$$(\mathbb{Z}^2)^\star = \{\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \in \mathbb{Z}^2 : \gcd(a, c) = 1\}.$$

Define an equivalence relation $\sim$ on $(\mathbb{Z}^2)^\star$ where $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right]$ if and only if $\Gamma(a/c) = \Gamma(a'/c')$. Define the map

$$\varphi : (\mathbb{Z}^2)^\star / \sim \to \Gamma\backslash\mathbb{Q}^\star$$

by $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \mapsto \Gamma(a/c)$.

Proposition 2.4. The map φ is a bijection.

Proof. To show that φ is well-defined let $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right], \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \in (\mathbb{Z}^2)^\star$ with $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right]$. By our hypothesis, $\Gamma(a/c) = \Gamma(a'/c')$ and therefore $\varphi(\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]) = \varphi\left(\left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right]\right)$. So φ is well-defined.

To show that φ is surjective, first let $\Gamma(a/c) \in \Gamma\backslash\mathbb{Q}^\star$. Since $a/c \in \mathbb{Q}^\star$, we can assume that the fraction is reduced which implies that $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \in (\mathbb{Z}^2)^\star$. Therefore $\varphi(\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]) = \Gamma(a/c)$ which proves the map is surjective.

To show that φ is injective assume that $\varphi([\begin{smallmatrix}a\\c\end{smallmatrix}]) = \varphi([\begin{smallmatrix}a'\\c'\end{smallmatrix}])$, which implies that $\Gamma(a/c) = \Gamma(a'/c')$. By our hypothesis, if $\Gamma(a/c) = \Gamma(a'/c')$ then $[\begin{smallmatrix}a\\c\end{smallmatrix}] \sim [\begin{smallmatrix}a'\\c'\end{smallmatrix}]$, and so φ is injective.

□

Thus the map φ gives a correspondence between elements of $(\mathbb{Z}^2)^\star/\sim$ and cusps of $X(\Gamma)$. We will develop methods for computing a system of representatives for $(\mathbb{Z}^2)^\star/\sim$ which will then give representatives for the cusps of $X(\Gamma)$.

We will now determine the cusps of $X(1)$; that is, the elements of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{Q}^\star$.

Define an equivalence relation $\sim$ on $(\mathbb{Z}^2)^\star$ by $[\begin{smallmatrix}a\\c\end{smallmatrix}] \sim [\begin{smallmatrix}a'\\c'\end{smallmatrix}]$ if and only if $[\begin{smallmatrix}a\\c\end{smallmatrix}] = \pm\gamma [\begin{smallmatrix}a'\\c'\end{smallmatrix}]$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

So applying Proposition 2.4,

$$\varphi : (\mathbb{Z}^2)^\star/\sim \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{Q}^\star$$

is a bijection. The following proposition shows that there is one element of $(\mathbb{Z}^2)^\star/\sim$ and hence one cusp for $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{Q}^\star$.

Proposition 2.5. There is one cusp in $X(1)$.

Proof. We want to show that there is one element in $(\mathbb{Z}^2)^\star/\sim$. Let $[\begin{smallmatrix}a\\c\end{smallmatrix}] \in (\mathbb{Z}^2)^\star$, so a and c are relatively prime. There exist $x, y \in \mathbb{Z}$ such that $ax + cy = 1$. We compute

$$\begin{bmatrix} x & y \\ -c & a \end{bmatrix} \begin{bmatrix} a \\ c \end{bmatrix} = \begin{bmatrix} ax + cy \\ -ac + ac \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

We check that $ax - (c)(-y) = 1$ so $[\begin{smallmatrix}x & y\\ -c & a\end{smallmatrix}] \in \mathrm{SL}_2(\mathbb{Z})$.

Therefore $[\begin{smallmatrix}a\\c\end{smallmatrix}] \sim [\begin{smallmatrix}1\\0\end{smallmatrix}]$ for any $[\begin{smallmatrix}a\\c\end{smallmatrix}]$ so there is one cusp in $X(1)$. □

2.3 Computing cusps of $X(\Gamma)$

We have similar results for cusps of $X(N), X_1(N)$ and $X_0(N)$.

Proposition 2.6. Let $(a/c), (a'/c')$ be in $\mathbb{Q}^\star$ with $\gcd(a, c) = \gcd(a', c') = 1$. Then

$$\begin{bmatrix} a' \\ c' \end{bmatrix} = \gamma \begin{bmatrix} a \\ c \end{bmatrix} \text{ for some } \gamma \in \Gamma(N) \iff \begin{bmatrix} a' \\ c' \end{bmatrix} \equiv \begin{bmatrix} a \\ c \end{bmatrix} \pmod{N}.$$

Proof. The forward direction is obvious.

To show the reverse direction, we first assume $[\begin{smallmatrix}a\\c\end{smallmatrix}] = [\begin{smallmatrix}1\\0\end{smallmatrix}]$, which implies that $a' \equiv 1 \pmod{N}$ and $c' \equiv 0 \pmod{N}$. This implies that there exists an integer ℓ such that $\ell = (1 - a')/N$. Since $\gcd(a', c') = 1$ there exist $x, y \in \mathbb{Z}$ such that $a'x - c'y = 1$. Then

$$\begin{aligned} a'x\ell - c'y\ell &= \ell \\ &= (1 - a')/N. \end{aligned}$$

If we let $\delta = x\ell$ and $\beta = y\ell$ then $a'\delta - c'\beta = (1-a')/N$. Let $\gamma = \left[\begin{smallmatrix} a' & \beta N \\ c' & 1+\delta N \end{smallmatrix}\right]$. By assumption $a' \equiv 1 \pmod N$ and $c' \equiv 0 \pmod N$. Therefore $\gamma \in \Gamma(N)$ and $\left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] = \gamma \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$.

Consider the general case. Assume that $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \equiv \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \pmod N$ with $\gcd(a,c) = \gcd(a',c') = 1$. By the Euclidean algorithm we can choose b, d such that $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ is in $\mathrm{SL}_2(\mathbb{Z})$. Observe that $\gamma \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]$, so we get

$$\begin{aligned} \gamma^{-1} \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] &\equiv \gamma^{-1} \left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \pmod N \\ &= \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]. \end{aligned}$$

Hence $\gamma^{-1} \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \equiv \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] \pmod N$. By the first case, there exists $\alpha \in \Gamma(N)$ such that $\alpha\gamma^{-1} \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$. Multiplying by γ on both sides gives

$$\begin{aligned} \gamma\alpha\gamma^{-1} \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] &= \gamma \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] \\ &= \left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]. \end{aligned}$$

Therefore $\gamma\alpha\gamma^{-1} \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] = \left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]$.

Let $\varphi : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ be the homomorphism given by reduction mod N. The kernel is $\Gamma(N)$. Therefore $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Therefore $\gamma\alpha\gamma^{-1} \in \Gamma(N)$, which completes the proof. □

Theorem 2.7. *Let $s = (a/c), s' = (a'/c')$ be in $\mathbb{Q}^\star$ with $\gcd(a,c) = \gcd(a',c') = 1$. Then*

$$\Gamma(N)s = \Gamma(N)s' \iff \left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \equiv \pm \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \pmod N, \tag{2.1}$$

$$\Gamma_1(N)s = \Gamma_1(N)s' \iff \left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \equiv \pm \left[\begin{smallmatrix} a'+jc \\ c' \end{smallmatrix}\right] \pmod N, \tag{2.2}$$

$$\Gamma_0(N)s = \Gamma_0(N)s' \iff \left[\begin{smallmatrix} ya \\ c \end{smallmatrix}\right] \equiv \left[\begin{smallmatrix} a'+jc \\ yc' \end{smallmatrix}\right] \pmod N \tag{2.3}$$

for some $j, y \in \mathbb{Z}$ with $\gcd(y, N) = 1$.

Proof. [DS05, Proposition 3.8.3] □

The remainder of the chapter will give algorithms for computing cusps for the modular curves $X(N), X_1(N)$, and $X_0(N)$. Theorem 2.7 gives us a correspondence between cusps and equivalence classes of $(\mathbb{Z}^2)^\star$. The next section will make this correspondence more explicit.

We will need the following lemma in the next section.

Lemma 2.8. Let integers $a, c \in \{0, \ldots, N-1\}$ have images $\bar{a}, \bar{c}$ in $\mathbb{Z}/n\mathbb{Z}$. Then $\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]$ has a lift $\left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \in \mathbb{Z}^2$ with $\gcd(a',c') = 1$ if and only if $\gcd(a, c, N) = 1$.

Proof. [DS05, Lemma 3.8.4] □

2.3.1 Computing cusps of $X(N)$

Recall

$$(\mathbb{Z}^2)^\star = \{\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \in \mathbb{Z}^2 : \gcd(a,c) = 1\}.$$

Define an equivalence relation $\sim_1$ on $(\mathbb{Z}^2)^\star$ by

$$\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \sim_1 \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \iff \left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \equiv \pm \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \pmod{N}.$$

By equation (2.1)

$$\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \sim_1 \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \iff \Gamma(N)(a/c) = \Gamma(N)(a'/c')$$

and so Proposition 2.4 proves that

$$\varphi : (\mathbb{Z}^2)^\star / \sim_1 \longrightarrow \Gamma(N) \backslash \mathbb{Q}^\star$$

is a bijection. Therefore the elements of $(\mathbb{Z}^2)^\star / \sim_1$ correspond to cusps of $X(N)$. This section will give an algorithm for finding a system of representatives for the equivalence classes of $(\mathbb{Z}^2)^\star$.

For $\bar{a}, \bar{c} \in \mathbb{Z}/N\mathbb{Z}$, define $\gcd(\bar{a}, \bar{c}) = \gcd(x, y)$ where x, y are the smallest positive representatives of $\bar{a}, \bar{c}$ respectively.

We will use the following lemma.

Lemma 2.9. Fix an integer N and let a, c be integers with $\gcd(a, c) = 1$. Let a', c' be integers such that $a \equiv a' \pmod{N}$ and $c \equiv c' \pmod{N}$. Then $\gcd(a', c', N) = 1$.

Proof. The congruences $a \equiv a' \pmod{N}$ and $c \equiv c' \pmod{N}$ imply that $a = a' + Nk_1$ and $c = c' + Nk_2$ for some integers k_1, k_2. Therefore $\gcd(a, c) = 1$ implies that $\gcd(a' + Nk_1, c' + Nk_2) = 1$ and so $\gcd(a', c', N) = 1$. □

Let $\bar{a}, \bar{c}$ be elements of $\mathbb{Z}/N\mathbb{Z}$. Define the set

$$((\mathbb{Z}/N\mathbb{Z})^2)^\star = \{\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right] : \bar{a}, \bar{c} \in (\mathbb{Z}/N\mathbb{Z}), \gcd(\bar{a}, \bar{c}, N) = 1\}.$$

Now we define the map

$$\psi : ((\mathbb{Z}/N\mathbb{Z})^2)^\star \longrightarrow (\mathbb{Z}^2)^\star / \sim_1$$

by $\psi\left(\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]\right) = \left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]$ where $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]$ is a lift of $\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]$ to $(\mathbb{Z}^2)^\star$. This lift is guaranteed to exist by the condition $gcd(\bar{a}, \bar{c}, N) = 1$.

Theorem 2.10. *The map ψ is independent of the choice of lift and surjective.*

Proof. To show that ψ is independent of the choice of lift, let $\left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} a'' \\ c'' \end{smallmatrix}\right]$ be lifts of $\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]$ to $(\mathbb{Z}^2)^\star$. Since $a' \equiv a'' \pmod{N}$ and $c' \equiv c'' \pmod{N}$, we have that $\left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \sim_1 \left[\begin{smallmatrix} a'' \\ c'' \end{smallmatrix}\right]$. Therefore the map ψ is independent of the choice of lift from $((\mathbb{Z}/N\mathbb{Z})^2)^\star$ to $(\mathbb{Z}^2)^\star$.

Next we show ψ is surjective. Let $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \in (\mathbb{Z}^2)^\star$ and $\bar{a}, \bar{c}$ be the images of a, c in $\mathbb{Z}/N\mathbb{Z}$. Since $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]$ is a lift of $\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]$ and ψ is independent of the choice of lift, we have that $\psi\left(\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]\right) = \left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]$. By Lemma 2.9, $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \in (\mathbb{Z}^2)^\star$ implies that $\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right] \in ((\mathbb{Z}/N\mathbb{Z})^2)^\star$ and so ψ is surjective. □

The following lemma will be used to prove the algorithm.

Lemma 2.11. Let $\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} \bar{x} \\ \bar{y} \end{smallmatrix}\right]$ be elements of $((\mathbb{Z}/N\mathbb{Z})^2)^\star$ and $\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right] \neq \left[\begin{smallmatrix} \bar{x} \\ \bar{y} \end{smallmatrix}\right]$. Then $\psi\left(\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix} \bar{x} \\ \bar{y} \end{smallmatrix}\right]\right)$ if and only if $\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right] = -\left[\begin{smallmatrix} \bar{x} \\ \bar{y} \end{smallmatrix}\right]$.

Proof. We will first show the forward direction. Assume that $\psi\left(\left[\begin{smallmatrix}\bar{a}\\ \bar{c}\end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix}\bar{x}\\ \bar{y}\end{smallmatrix}\right]\right)$. Let $\psi\left(\left[\begin{smallmatrix}\bar{a}\\ \bar{c}\end{smallmatrix}\right]\right)$ and $\psi\left(\left[\begin{smallmatrix}\bar{x}\\ \bar{y}\end{smallmatrix}\right]\right)$ be the respective classes of $\left[\begin{smallmatrix}a\\ c\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}x\\ y\end{smallmatrix}\right]$.

By our assumptions, $\left[\begin{smallmatrix}a\\ c\end{smallmatrix}\right] \sim_1 \left[\begin{smallmatrix}x\\ y\end{smallmatrix}\right]$ and so $\left[\begin{smallmatrix}a\\ c\end{smallmatrix}\right] \equiv \pm\left[\begin{smallmatrix}x\\ y\end{smallmatrix}\right] \pmod N$. This implies that $\left[\begin{smallmatrix}\bar{a}\\ \bar{c}\end{smallmatrix}\right] = \pm\left[\begin{smallmatrix}\bar{x}\\ \bar{y}\end{smallmatrix}\right]$. We assumed that $\left[\begin{smallmatrix}\bar{a}\\ \bar{c}\end{smallmatrix}\right] \neq \left[\begin{smallmatrix}\bar{x}\\ \bar{y}\end{smallmatrix}\right]$, and hence $\left[\begin{smallmatrix}\bar{a}\\ \bar{c}\end{smallmatrix}\right] = -\left[\begin{smallmatrix}\bar{x}\\ \bar{y}\end{smallmatrix}\right]$.

To prove the reverse direction assume that $\left[\begin{smallmatrix}\bar{a}\\ \bar{c}\end{smallmatrix}\right] = -\left[\begin{smallmatrix}\bar{x}\\ \bar{y}\end{smallmatrix}\right]$. Let $\psi\left(\left[\begin{smallmatrix}\bar{a}\\ \bar{c}\end{smallmatrix}\right]\right)$ and $\psi\left(\left[\begin{smallmatrix}\bar{x}\\ \bar{y}\end{smallmatrix}\right]\right)$ be the respective classes of $\left[\begin{smallmatrix}a\\ c\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}x\\ y\end{smallmatrix}\right]$. If $\left[\begin{smallmatrix}\bar{a}\\ \bar{c}\end{smallmatrix}\right] = -\left[\begin{smallmatrix}\bar{x}\\ \bar{y}\end{smallmatrix}\right]$ then $\left[\begin{smallmatrix}a\\ c\end{smallmatrix}\right] \equiv -\left[\begin{smallmatrix}x\\ y\end{smallmatrix}\right] \pmod N$ and so $\psi\left(\left[\begin{smallmatrix}\bar{a}\\ \bar{c}\end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix}\bar{x}\\ \bar{y}\end{smallmatrix}\right]\right)$. This proves the lemma.

□

2.3.2 Algorithm for cusps of $X(N)$

The algorithm for computing cusps of $X(N)$ is as follows:

1. For integers $a, c \in \{0, \ldots, N-1\}$, list out all elements $\left[\begin{smallmatrix}a\\ c\end{smallmatrix}\right]$ such that $\gcd(a, c, N) = 1$.
2. Compute sets $\left\{\left[\begin{smallmatrix}a\\ c\end{smallmatrix}\right], \left[\begin{smallmatrix}x\\ y\end{smallmatrix}\right]\right\}$ where $\left[\begin{smallmatrix}a\\ c\end{smallmatrix}\right] \equiv -\left[\begin{smallmatrix}x\\ y\end{smallmatrix}\right] \pmod N$ from elements found in Step 1.
3. Choose one element from each set computed in Step 2 and output these elements as a list.

Theorem 2.12. *The above algorithm outputs a set of elements in $((\mathbb{Z}/N\mathbb{Z})^2)^\star$ that lift to a system of representatives for the equivalence classes of $(\mathbb{Z}^2)^\star$ with respect to $\sim_1$.*

Proof. By Lemma 2.11, $\left[\begin{smallmatrix}\bar{a}\\ \bar{c}\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}\bar{x}\\ \bar{y}\end{smallmatrix}\right]$ in $((\mathbb{Z}/N\mathbb{Z})^2)^\star$ lift to the same equivalence class in $(\mathbb{Z}^2)^\star$ if and only if $\left[\begin{smallmatrix}\bar{a}\\ \bar{c}\end{smallmatrix}\right] = \pm\left[\begin{smallmatrix}\bar{x}\\ \bar{y}\end{smallmatrix}\right]$.

Therefore choosing one element from each pair $\left[\begin{smallmatrix}\bar{a}\\ \bar{c}\end{smallmatrix}\right], \left[\begin{smallmatrix}\bar{x}\\ \bar{y}\end{smallmatrix}\right]$ with $\left[\begin{smallmatrix}\bar{a}\\ \bar{c}\end{smallmatrix}\right] = -\left[\begin{smallmatrix}\bar{x}\\ \bar{y}\end{smallmatrix}\right]$, gives a subset of $((\mathbb{Z}/N\mathbb{Z})^2)^\star$ that lifts to a system of representatives for the equivalence classes of $(\mathbb{Z}^2)^\star$ with respect to $\sim_1$.

□

Corollary 2.13. The algorithm outputs a set that is in bijection with the cusps of $X(N)$.

Proof. By Theorem 2.12 the algorithm outputs a set that is in bijection with $(\mathbb{Z}^2)^\star/\sim_1$. By Proposition 2.4, the map

$$\varphi : (\mathbb{Z}^2)^\star/\sim_1 \to \Gamma\backslash\mathbb{Q}^\star$$

where $\varphi\left(\left[\begin{smallmatrix}a\\ c\end{smallmatrix}\right]\right) = \Gamma(a/c)$, is a bijection. Hence the algorithm outputs a set in bijection with the cusps of $X(N)$. □

We will give an example of the implementation of the algorithm.

Example 2.14. Find the cusps of $X(4)$.

The list from Step 1 is given by:

$$\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}3\\0\end{bmatrix},$$
$$\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\1\end{bmatrix}, \begin{bmatrix}2\\1\end{bmatrix}, \begin{bmatrix}3\\1\end{bmatrix},$$
$$\begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}3\\2\end{bmatrix},$$
$$\begin{bmatrix}0\\3\end{bmatrix}, \begin{bmatrix}1\\3\end{bmatrix}, \begin{bmatrix}2\\3\end{bmatrix}, \begin{bmatrix}3\\3\end{bmatrix}.$$

Next we compute the sets for Step 2. This gives us the following sets:

$$\{\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right], \left[\begin{smallmatrix}0\\3\end{smallmatrix}\right]\}, \{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right], \left[\begin{smallmatrix}3\\0\end{smallmatrix}\right]\}, \{\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right], \left[\begin{smallmatrix}3\\3\end{smallmatrix}\right]\}, \{\left[\begin{smallmatrix}1\\3\end{smallmatrix}\right], \left[\begin{smallmatrix}3\\1\end{smallmatrix}\right]\}, \{\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right], \left[\begin{smallmatrix}3\\2\end{smallmatrix}\right]\}, \{\left[\begin{smallmatrix}2\\1\end{smallmatrix}\right], \left[\begin{smallmatrix}2\\3\end{smallmatrix}\right]\}.$$

Now we choose the first element from each set and this gives the system of representatives for the cusps of $X(4)$ as

$$\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}1\\1\end{bmatrix}, \begin{bmatrix}1\\3\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}2\\1\end{bmatrix}.$$

Lemma 2.15. Let N be a positive integer and d a divisor of N. Let $c \in \{1, \ldots, N-1\}$. There are $\phi(N/d)$ values of c such that $\gcd(c, N) = 1$.

Proof. Let $P(M) = \{x : 1 \leq x \leq M-1, \gcd(M, x) = 1\}$. It suffices to show that the map

$$P(N/d) \to \{c : \gcd(c, N) = d\}$$

defined by $x \mapsto xd$ is a bijection. If $\gcd(x, N/d) = 1$ then $\gcd(xd, N) = d$ and so the map is well-defined.

Consider the map

$$\{c : \gcd(c, N) = d\} \to P(N/d)$$

given by $y \mapsto y/d$. If $\gcd(y, N) = d$ then $\gcd(y/d, N/d) = 1$ and so this map is well-defined. Clearly these maps are inverses of each other and so they are bijections. The order of $P(N/d)$ is $\phi(N/d)$ and the claim follows. □

Theorem 2.16. *For $N > 2$, the modular curve $X(N)$ has*

$$\frac{1}{2}\sum_{d|N}(N/d)\phi(d)\phi(N/d)$$

cusps. Additionally $X(2)$ has 3 cusps.

Proof. We will count the number of representatives by counting at each step in the algorithm given in this section. Fix $c \in \{0, \ldots, N-1\}$ and define $\gcd(c, N) = d$. We want to find the number of elements $a \in \{0, \ldots, N-1\}$

such that $\gcd(a,d) = 1$. The number of such values of a is $(N/d)\phi(d)$. By Lemma 2.15 there are $\phi(N/d)$ values of c such that $\gcd(c,N) = d$. Hence there are $\sum_{d|N}(N/d)\phi(d)\phi(N/d)$ elements in the list after Step 1.

To count the possible system of representatives after Step 2 we observe that we pair possible representatives by equivalence by $-I$. The only elements that satisfy $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \equiv -\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \pmod N$ are $\left[\begin{smallmatrix} N/2 \\ N/2 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 \\ N/2 \end{smallmatrix}\right]$, and $\left[\begin{smallmatrix} N/2 \\ 0 \end{smallmatrix}\right]$. Clearly if N is odd there are no such elements. If $N > 2$ is even, then none of those elements satisfy the $\gcd$ condition and therefore do not appear in Step 1. Therefore for $N > 2$ we halve the number of representatives found in Step 1. In total $X(N)$ has

$$\frac{1}{2}\sum_{d|N}(N/d)\phi(d)\phi(N/d)$$

cusps for $N > 2$.

If $N = 2$ the system of representatives is

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

Clearly none of these are equivalent by $-I$ and so this gives a system of representatives of the cusps of $X(2)$ which proves the theorem.

□

2.3.3 Algorithm in Sage

Sage is an open source mathematical software package that is based on Python. The following program implements the algorithm from the previous section.

```
def cusplist(N):
    """List all [a,b] where gcd(a,b,N)=1."""
    l = []
    for b in range(N):
        d= gcd(b,N)
        for a in range(N):
            if gcd(d,a)==1:
                l.append([a,b])
    return l

def cusps(N):
    """Output cusps of X(N).

    Creates list of [a,b] from cusplist and remove [c,d]
    if [a,b]=[-c,-d]."""
    l = cusplist(N)
    k=[]
    while len(l)>0:
        a = l.pop(0)
        k.append(a)
```

```
        for i in range(0,len(l)):
            if (a[0]+l[i][0])%N==0 and (a[1]+l[i][1])%N
               ↪ ==0:
                l.pop(i)
                break
    return k
```

2.3.4 Computing cusps of $X_1(N)$

We will now give an algorithm for finding the cusps of $X_1(N)$. Define an equivalence relation $\sim_2$ on $(\mathbb{Z}^2)^\star$ by

$$\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \sim_2 \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \iff \left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \equiv \pm \left[\begin{smallmatrix} a'+jc \\ c' \end{smallmatrix}\right] \pmod{N}$$

for some $j \in \mathbb{Z}$. By equation (2.2)

$$\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \sim_2 \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \iff \Gamma_1(N)(a/c) = \Gamma_1(N)(a'/c')$$

and so Proposition 2.4 proves that the map

$$\varphi : (\mathbb{Z}^2)^\star/\sim_2 \longrightarrow \Gamma_1(N)\backslash\mathbb{Q}^\star.$$

is a bijection. Recall we define the set

$$((\mathbb{Z}/N\mathbb{Z})^2)^\star = \{\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right] : \bar{a}, \bar{c} \in (\mathbb{Z}/N\mathbb{Z}), \gcd(\bar{a}, \bar{c}, N) = 1\}.$$

Now define the map,

$$\psi : ((\mathbb{Z}/N\mathbb{Z})^2)^\star \longrightarrow (\mathbb{Z}^2)^\star/\sim_2$$

by $\psi\left(\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]\right) = \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right]$ where $\left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right]$ is a lift of $\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]$ to $(\mathbb{Z}^2)^\star$.

Theorem 2.17. *The map ψ is independent of the choice of lift and is well-defined and surjective.*

The proof of Theorem 2.17 is analogous to the proof of Theorem 2.10. Now define an equivalence relation $\simeq_2$ on $(\mathbb{Z}^2)^\star$ where two elements $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right], \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right]$ are equivalent if and only if $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \equiv \left[\begin{smallmatrix} a'+jc \\ c' \end{smallmatrix}\right] \pmod{N}$ for some $j \in \mathbb{Z}$. Observe that this is the equivalence $\sim_2$ without the negation.

For the following lemmas when $\bar{a}, \bar{c} \in \mathbb{Z}/N\mathbb{Z}$ take a, c to be the smallest nonnegative representative of $\bar{a}, \bar{c}$, which will be in the set $\{0, \ldots, N-1\}$.

Lemma 2.18. Fix $\bar{c} \in (\mathbb{Z}/N\mathbb{Z})$. Let $\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} \bar{x} \\ \bar{c} \end{smallmatrix}\right]$ be elements of $((\mathbb{Z}/N\mathbb{Z})^2)^\star$ with lifts $\left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} x' \\ c' \end{smallmatrix}\right]$ in $(\mathbb{Z}^2)^\star$. Let $d = \gcd(c, N)$. Then $a \equiv x \pmod{d}$ if and only if $\left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \simeq_2 \left[\begin{smallmatrix} x' \\ c' \end{smallmatrix}\right]$.

Proof. First we prove the forward direction. Let $\gcd(c, N) = d$ and $a \equiv x \pmod{d}$. There exist integers ℓ, k, and w such that

$$c\ell + Nk = d \tag{2.4}$$
$$x - a = dw. \tag{2.5}$$

If we multiply through equation (2.4) by w, then we get $c(\ell w) + N(kw) = dw$. Plugging into equation (2.5) and rearranging gives

$$\begin{aligned} c(w\ell) + N(wk) &= x - a \\ a + c(w\ell) &= x - N(wk) \\ &\equiv x \pmod{N}. \end{aligned}$$

Observe that $a' \equiv a \pmod{N}$, $x \equiv x' \pmod{N}$, and $c \equiv c' \pmod{N}$. Since $a + c(w\ell) \equiv x \pmod{N}$, we have that

$$\begin{bmatrix} a' + c'(w\ell) \\ c' \end{bmatrix} \equiv \begin{bmatrix} x' \\ c' \end{bmatrix} \pmod{N}.$$

Therefore $\left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \simeq_2 \left[\begin{smallmatrix} x' \\ c' \end{smallmatrix}\right]$ which proves the forward direction.
Now to prove the reverse direction assume that $\left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \simeq_2 \left[\begin{smallmatrix} x' \\ c' \end{smallmatrix}\right]$. Therefore

$$\begin{bmatrix} a' + c'j \\ c' \end{bmatrix} \equiv \begin{bmatrix} x' \\ c' \end{bmatrix} \pmod{N}$$

for some integer j. Thus $a' + c'j \equiv x' \pmod{N}$ and so $a + cj \equiv x \pmod{N}$. Hence $a + cj \equiv x \pmod{d}$ since $d \mid N$. Therefore $a \equiv x \pmod{N}$ since $d \mid c$. □

2.3.5 Algorithm for cusps of $X_1(N)$

We will now give an algorithm for finding a set of elements in $((\mathbb{Z}/N\mathbb{Z})^2)^\star$ that lift to a set of representatives for the equivalence classes of $(\mathbb{Z}^2)^\star/\sim_2$. Define $P(n) = \{x : 0 \leq x < n, \gcd(x, n) = 1\}$.

1. For each $c \in \{0, 1, \ldots, N-1\}$, define $d = \gcd(c, N)$. For each $a \in P(d)$, add $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]$ to the list.

2. Choose an element $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]$ from the list in Step 1 and let $d = \gcd(c, N)$. If possible, find a different element $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$ from the list in Step 1 such that $y \equiv -c \pmod{N}$ and $x \equiv -a \pmod{d}$. Create the set $\left\{\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right], \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]\right\}$ if there is such an element $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$, otherwise create the set $\left\{\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]\right\}$.

3. Create a list choosing one element from each set found in Step 2. Output this list.

Theorem 2.19. *The above algorithm gives a set of elements in $((\mathbb{Z}/N\mathbb{Z})^2)^\star$ that lift to a set of representatives for the equivalence classes of $(\mathbb{Z}^2)^\star$ with respect to $\sim_2$.*

Proof. We claim that Step 1 gives a set of $((\mathbb{Z}/N\mathbb{Z})^2)^\star$ that lifts to a system of representatives for equivalence classes of $(\mathbb{Z}^2)^\star$ with respect to $\simeq_2$. Recall that two elements $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right], \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \in (\mathbb{Z}^2)^\star/\simeq_2$ are equivalent if and only if $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \equiv \left[\begin{smallmatrix} a'+jc \\ c' \end{smallmatrix}\right] \pmod{N}$ for some $j \in \mathbb{Z}$. Observe that $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right]$ are equivalent if and only if $c \equiv c' \pmod{N}$. Therefore $\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} \bar{x} \\ \bar{y} \end{smallmatrix}\right]$ lift to different elements of $(\mathbb{Z}^2)^\star/\sim_2$ if and only if $\bar{c} \neq \bar{y}$.

Fix $c \in \{0, \ldots, N-1\}$ and define $d = \gcd(c, N)$. By Lemma 2.18, $\left[\frac{\bar{a}}{\bar{c}}\right]$ and $\left[\frac{\bar{x}}{\bar{c}}\right]$ lift to the same equivalence class in $(\mathbb{Z}^2)^\star$ if and only if $a \equiv x \pmod{d}$ for a and x relatively prime to d. Observe that if a is not relatively prime to d then $\left[\frac{\bar{a}}{\bar{c}}\right]$ does not have a lift to $(\mathbb{Z}^2)^\star$.

Therefore for each $c \in \{0, \ldots, N-1\}$ choosing all elements $\left[\frac{\bar{a}}{\bar{c}}\right]$ where $a \in \{0, \ldots, d-1\}$ and $\gcd(a, d) = 1$ gives a set that lifts to a system of representatives of equivalence classes of $(\mathbb{Z}^2)^\star$ with respect to $\simeq_2$. This set is given by Step 1 of the algorithm.

Observe that the equivalence $\simeq_2$ is a refinement of the equivalence $\sim_2$. If we take a system of representatives of equivalence classes of $(\mathbb{Z}^2)^\star$ with respect to $\simeq_2$ and apply the equivalence by $-I$ then this gives a system of representatives with respect to $\sim_2$.

Choose an element $\left[\frac{a}{c}\right]$ from Step 1 and let $d = \gcd(c, N)$. A different element $\left[\frac{x}{y}\right]$ from Step 1 is in the same orbit as $\left[\frac{-a}{-c}\right]$ if $x \equiv -a \pmod{d}$ and $y \equiv -c \pmod{N}$. The set $\{\left[\frac{a}{c}\right], \left[\frac{x}{y}\right]\}$ gives elements from Step 1 that are equivalent by $-I$. Choosing one such element from each set gives a set that reduces to a system of representatives of $(\mathbb{Z}^2)^\star / \sim_2$.

□

Corollary 2.20. The algorithm outputs a set that is in bijection with the cusps of $X_1(N)$.

Proof. By Theorem 2.17 the algorithm outputs a set that is in bijection with $(\mathbb{Z}^2)^\star / \sim_2$. By Proposition 2.4, the map

$$\varphi : (\mathbb{Z}^2)^\star / \sim_2 \to \Gamma \backslash \mathbb{Q}^\star,$$

where $\varphi\left(\left[\frac{a}{c}\right]\right) = \Gamma(a/c)$, is a bijection. Hence the algorithm outputs a set in bijection with the cusps of $X_1(N)$. □

Example 2.21. We will find the cusps of $X_1(10)$.

First choose all $c \in \{0, \ldots, N-1\}$ such that $\gcd(c, 10) = 1$. This is the set $\{1, 3, 7, 9\}$. Applying Step 1 of the algorithm, we add the following elements to our list:

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \begin{bmatrix} 0 \\ 7 \end{bmatrix}, \begin{bmatrix} 0 \\ 9 \end{bmatrix}.$$

Let $c = 0$. Then $\gcd(0, 10) = 10$. Observe that $P(10) = \{1, 3, 7, 9\}$. Applying Step 1, we add the following elements to our list:

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 3 \\ 0 \end{bmatrix} \begin{bmatrix} 7 \\ 0 \end{bmatrix} \begin{bmatrix} 9 \\ 0 \end{bmatrix}.$$

If $c = 2$, then $\gcd(2, 10) = 2$. Since $P(2) = \{1\}$, we add the following element to our list:

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix}.$$

If $c = 4$ then $\gcd(4, 10) = 2$. Since $P(2) = \{1\}$, we add the following element to our list:

$$\begin{bmatrix}1\\4\end{bmatrix}.$$

If $b = 5$ then $\gcd(5, 10) = 5$, and repeating the previous steps we add the following elements to our list:

$$\begin{bmatrix}1\\5\end{bmatrix}\begin{bmatrix}2\\5\end{bmatrix}\begin{bmatrix}3\\5\end{bmatrix}\begin{bmatrix}4\\5\end{bmatrix}.$$

For both $c = 6$ and $c = 8$, $\gcd(c, 10) = 2$, so we add the following element to our list:

$$\begin{bmatrix}1\\6\end{bmatrix}, \begin{bmatrix}1\\8\end{bmatrix}.$$

We have now completed the list of elements for Step 1. For Step 2, we directly compute the sets $\left\{\left[\begin{smallmatrix}a\\c\end{smallmatrix}\right], \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]\right\}$ with $y \equiv -c \pmod N$ and $x \equiv -a \pmod d$ where $d = \gcd(c, N)$:

$$\begin{array}{ccc}
\left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}9\\0\end{bmatrix}\right\} & \left\{\begin{bmatrix}3\\0\end{bmatrix}, \begin{bmatrix}7\\0\end{bmatrix}\right\} & \left\{\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}0\\9\end{bmatrix}\right\} \\
\left\{\begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}1\\8\end{bmatrix}\right\} & \left\{\begin{bmatrix}0\\3\end{bmatrix}, \begin{bmatrix}0\\7\end{bmatrix}\right\} & \left\{\begin{bmatrix}1\\4\end{bmatrix}, \begin{bmatrix}1\\6\end{bmatrix}\right\} \\
\left\{\begin{bmatrix}1\\5\end{bmatrix}, \begin{bmatrix}4\\5\end{bmatrix}\right\} & \left\{\begin{bmatrix}2\\5\end{bmatrix}, \begin{bmatrix}3\\5\end{bmatrix}\right\}.
\end{array}$$

We can now choose one representative from each of the sets above. Therefore the following list gives representatives of the cusps of $X_1(10)$:

$$\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}3\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}0\\3\end{bmatrix}, \begin{bmatrix}1\\4\end{bmatrix}, \begin{bmatrix}1\\5\end{bmatrix}, \begin{bmatrix}2\\5\end{bmatrix}.$$

Theorem 2.22. *For $N = 3, N \geq 5$, the number of cusps in $X_1(N)$ is*

$$\frac{1}{2}\sum_{d|N}\phi(d)\phi(N/d)$$

Proof. We will count the number of cusps that are found for each step in the algorithm. Given N, fix $c \in \{0, \ldots, N-1\}$ and let $d = \gcd(c, N)$. We would like to count the elements $\left[\begin{smallmatrix}a\\c\end{smallmatrix}\right] \in (\mathbb{Z}/N\mathbb{Z})^2$ from Step 1. For each c, there are $\phi(d)$ possible representatives.

For each divisor d of N we want to determine how many $0 \leq c < N$ there are for which $\gcd(c, N) = d$.

We claim that the appropriate number is $\phi(N/d)$. If c satisfies $\gcd(c, N) = d$ it must be of the form ℓd for some $\ell \in \{1, 2, \ldots, N/d\}$. Then $c = \ell d$ satisfies $\gcd(c, N) = d$ exactly when $\gcd(\ell, N/d) = 1$. The number of choices of ℓ that

satisfy $\gcd(\ell, N/d) = 1$ is $\phi(N/d)$. For each divisor d of N, there are $\phi(d)\phi(N/d)$ possible representatives from Step 1.

In Step 2 we create the set $\{\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right], \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]\}$ where $x \equiv -a \pmod{d}$ and $y \equiv -c \pmod{N}$. If this set is a singleton then c is equal to 0 or $N/2$. If $c = 0$ then $a = N/2$. Therefore if N is odd there are no singletons in Step 2. Assume that N is even.

Since $\left[\begin{smallmatrix} 0 \\ N/2 \end{smallmatrix}\right]$ is in $((\mathbb{Z}/N\mathbb{Z})^2)^\star$ only when $N = 2$ we cannot have that $c = 0$. If $c = N/2$ then $a \equiv -a \pmod{N/2}$ and so $a = 0$ or $N/4$. The element $\left[\begin{smallmatrix} 0 \\ N/2 \end{smallmatrix}\right]$ is in $((\mathbb{Z}/N\mathbb{Z})^2)^\star$ only when $N = 2$ and $\left[\begin{smallmatrix} N/4 \\ N/2 \end{smallmatrix}\right]$ is in $((\mathbb{Z}/N\mathbb{Z})^2)^\star$ only when $N = 4$. Therefore there are only singletons in Step 2 when $N = 2$ and $N = 4$.

Thus we can halve the number of elements found in Step 1 which gives the total number of cusps as

$$\frac{1}{2}\sum_{d|N} \phi(d)\phi(N/d).$$

□

2.3.6 Algorithm in Sage

The following program implements the algorithm from the previous section.

```
def cusps1(N):
    """List all cusps of X_1(N).

    Creates list of [a,b] with a coprime to gcd(b,N),
       ↪ then
    removes [c,d] from cusplist if there is
    a [a,b] with [a,b]=[-c,-d]."""
    l = []
    for b in range(N):
        d = gcd(b,N)
        for k in range(0,d):
            if gcd(k,d)==1:
                l.append([k,b])
    r=[]
    while len(l)>0:
        a = l.pop(0)
        r.append(a)
        d=gcd(a[1],N)
        for i in range(len(l)):
            if (a[0]+l[i][0])%d==0 and (a[1]+l[i][1])%N
               ↪ ==0:
                l.pop(i)
                break
    return r
```

Using the algorithm defined in this section we can compute the cusps of the modular curves $X_1(N)$ for $2 \leq N \leq 12$. The computations are given in Table 2.1.

N	Cusps of $X_1(N)$
1	$\begin{bmatrix}1\\0\end{bmatrix}$
2	$\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}$
3	$\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}$
4	$\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}$
5	$\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}2\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}0\\2\end{bmatrix}$
6	$\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}1\\3\end{bmatrix}$
7	$\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}0\\2\end{bmatrix}, \begin{bmatrix}0\\3\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}2\\0\end{bmatrix}, \begin{bmatrix}3\\0\end{bmatrix}$
8	$\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}0\\3\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}3\\0\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}1\\4\end{bmatrix}$
9	$\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}2\\0\end{bmatrix}, \begin{bmatrix}4\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}0\\2\end{bmatrix}, \begin{bmatrix}1\\3\end{bmatrix}, \begin{bmatrix}2\\3\end{bmatrix}, \begin{bmatrix}0\\4\end{bmatrix}$
10	$\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}3\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}0\\3\end{bmatrix}, \begin{bmatrix}1\\4\end{bmatrix}, \begin{bmatrix}1\\5\end{bmatrix}, \begin{bmatrix}2\\5\end{bmatrix}$
11	$\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}2\\0\end{bmatrix}, \begin{bmatrix}3\\0\end{bmatrix}, \begin{bmatrix}4\\0\end{bmatrix}, \begin{bmatrix}5\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}0\\2\end{bmatrix}, \begin{bmatrix}0\\3\end{bmatrix}, \begin{bmatrix}0\\4\end{bmatrix}, \begin{bmatrix}0\\5\end{bmatrix}$
12	$\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}5\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}1\\3\end{bmatrix}, \begin{bmatrix}2\\3\end{bmatrix}, \begin{bmatrix}1\\4\end{bmatrix}, \begin{bmatrix}3\\4\end{bmatrix}, \begin{bmatrix}0\\5\end{bmatrix}, \begin{bmatrix}1\\6\end{bmatrix}$

TABLE 2.1: Cusps of $X_1(N)$

2.3.7 Computing cusps of $X_0(N)$

We will proceed as in the previous sections. Define an equivalence relation $\sim_3$ on $(\mathbb{Z}^2)^\star$ by

$$\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \sim_3 \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \iff \left[\begin{smallmatrix} ya \\ c \end{smallmatrix}\right] \equiv \begin{bmatrix} a'+jc \\ yc' \end{bmatrix} \pmod{N}$$

for some integers j, y with $\gcd(y, N) = 1$. By equation (2.2) of Theorem 2.7,

$$\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \sim_3 \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \iff \Gamma_0(N)(a/c) = \Gamma_0(N)(a'/c')$$

and so Proposition 2.4 proves that the map

$$\varphi : (\mathbb{Z}^2)^\star/\sim_3 \longrightarrow \Gamma_0(N)\backslash\mathbb{Q}^\star$$

is a bijection. Recall that if $\bar{a}, \bar{c}$ are elements of $\mathbb{Z}/N\mathbb{Z}$ then we define the set

$$((\mathbb{Z}/N\mathbb{Z})^2)^\star = \{\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right] : \bar{a}, \bar{c} \in (\mathbb{Z}/N\mathbb{Z}), \gcd(\bar{a}, \bar{c}, N) = 1\}.$$

Now define the map

$$\psi : ((\mathbb{Z}/N\mathbb{Z})^2)^\star \longrightarrow (\mathbb{Z}^2)^\star/\sim_3$$

by $\psi\left(\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]\right) = \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right]$ where $\left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right]$ is a lift of $\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]$ to $(\mathbb{Z}^2)^\star$ with $\gcd(a', c') = 1$.

Theorem 2.23. *The map ψ is independent of the choice of lift and is well-defined and surjective.*

The proof of this Theorem is analogous to the proof of Theorem 2.10. As in the previous section when $\bar{a}, \bar{c}, \bar{d} \in \mathbb{Z}/N\mathbb{Z}$ take a, c, d to be the smallest non-negative representative of $\bar{a}, \bar{c}, \bar{d}$, which will be in the set $\{0, \ldots, N-1\}$.

Theorem 2.24. *There are two cusps in $X_0(p)$ for p prime.*

Proof. Let p be prime. We will show that there are two elements in $(\mathbb{Z}^2)^\star/\sim_3$. More specifically we will show that $\left[\begin{smallmatrix} \bar{0} \\ \bar{1} \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} \bar{1} \\ \bar{0} \end{smallmatrix}\right]$ lift to a system of representatives for equivalence classes of $(\mathbb{Z}^2)^\star$ with respect to $\sim_3$.

We will first show that for $\bar{a} \in \mathbb{Z}/N\mathbb{Z}$, if $\left[\begin{smallmatrix} \bar{a} \\ \bar{0} \end{smallmatrix}\right] \in ((\mathbb{Z}/N\mathbb{Z})^2)^\star$ and $\bar{a} \neq \bar{0}$ then $\psi\left(\left[\begin{smallmatrix} \bar{a} \\ \bar{0} \end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix} \bar{1} \\ \bar{0} \end{smallmatrix}\right]\right)$.

Since a is nonzero, then it has an inverse mod p. Choose an integer y such that $ya \equiv 1 \pmod{p}$. Observe that

$$\begin{bmatrix} ya \\ p \end{bmatrix} \equiv \begin{bmatrix} 1 + j(0) \\ y(0) \end{bmatrix} \pmod{p}.$$

Therefore $\left[\begin{smallmatrix} a \\ p \end{smallmatrix}\right] \sim_3 \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$. Recall that ψ is independent of the choice of lift. Since $\left[\begin{smallmatrix} a \\ p \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$ are respective lifts of $\left[\begin{smallmatrix} \bar{a} \\ \bar{0} \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} \bar{1} \\ \bar{0} \end{smallmatrix}\right]$ to $(\mathbb{Z}^2)^\star$, we have that $\psi\left(\left[\begin{smallmatrix} \bar{a} \\ \bar{0} \end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix} \bar{1} \\ \bar{0} \end{smallmatrix}\right]\right)$.

Now assume that $\bar{c} \neq \bar{0}$. We will show that for all $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$, $\psi\left(\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix} \bar{0} \\ \bar{1} \end{smallmatrix}\right]\right)$.

Since c is nonzero, $\gcd(c, p) = 1$. Choose an integer y such that $y \equiv c \pmod{p}$ and so $\gcd(y, p) = 1$. Choose an integer j such that $j \equiv a \pmod{p}$.

Then we have the congruence

$$\begin{bmatrix} ya \\ c \end{bmatrix} \equiv \begin{bmatrix} 0 + jc \\ y \cdot 1 \end{bmatrix} \pmod{p}.$$

Therefore $\left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] \sim_3 \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$ where $\left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right]$ is a lift of $\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]$. Recall that ψ is independent of the choice of lift. Since $\left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$ are respective lifts of $\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} \bar{0} \\ \bar{1} \end{smallmatrix}\right]$ to $(\mathbb{Z}^2)^\star$, we have that $\psi\left(\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix} \bar{0} \\ \bar{1} \end{smallmatrix}\right]\right)$.

Lastly we need to show that $\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] \not\sim_3 \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$. By Theorem 2.7, if $\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] \sim_3 \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$ then

$$\begin{bmatrix} y(1) \\ 0 \end{bmatrix} \equiv \begin{bmatrix} 0 + j(0) \\ y(1) \end{bmatrix} \pmod{p}$$

for integers y, j with $\gcd(y, p) = 1$. Since $\gcd(y, p) = 1$ then $y \not\equiv 0 \pmod{p}$ which contradicts that $y(1) \equiv 0 + j(0) \pmod{p}$. Therefore $\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] \not\sim_3 \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$. Since the map ψ is independent of lift, $\psi\left(\left[\begin{smallmatrix} \bar{1} \\ \bar{0} \end{smallmatrix}\right]\right) \neq \psi\left(\left[\begin{smallmatrix} \bar{0} \\ \bar{1} \end{smallmatrix}\right]\right)$.

Therefore $X_0(p)$ has two cusps and they are represented by $\left[\begin{smallmatrix} \bar{1} \\ \bar{0} \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} \bar{0} \\ \bar{1} \end{smallmatrix}\right]$. □

Lemma 2.25. Let $c \in \mathbb{Z}^+$ and d a divisor of a positive integer N. Then

$$\gcd(c, N) = d \qquad \iff \qquad cy \equiv d \pmod{N} \tag{2.6}$$

for some $y \in \mathbb{Z}$ with $\gcd(y, N) = 1$.

Proof. For the reverse direction let $cy \equiv d \pmod{N}$, so there exists an integer k such that $cy + Nk = d$. Therefore $\gcd(c, N) \mid d$. Since $\gcd(y, N) = 1$ there is y' such that $yy' \equiv 1 \pmod{N}$. Observe that $c \equiv dy' \pmod{N}$ and so $c = dy' + Nm$ for some integer m. Hence $\gcd(d, N) \mid c$. Recall that d is a divisor of N so $\gcd(d, N) = d$ and so $d \mid c$ and $d \mid N$. Therefore $d \mid \gcd(c, N)$ and so $\gcd(c, N) = d$.

To show the forward direction assume $\gcd(c, N) = d$. Hence $d \mid c$ and so $c = d\ell$ with $\gcd(\ell, N/d) = 1$. Since $\gcd(\ell, N/d) = 1$, ℓ has an inverse mod N/d, call it y. Observe that

$$\begin{aligned} cy &= d\ell y \\ &\equiv d \pmod{N}. \end{aligned}$$

This proves the forward direction.

□

Lemma 2.26. Let $\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right] \in ((\mathbb{Z}/N\mathbb{Z})^2)^\star$. There exist $\bar{d}, \bar{x} \in \mathbb{Z}/N\mathbb{Z}$ with d a divisor of N such that $\psi\left(\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix} \bar{x} \\ \bar{d} \end{smallmatrix}\right]\right)$.

Proof. To prove the lemma let $\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right] \in ((\mathbb{Z}/N\mathbb{Z})^2)^\star$ and $\psi\left(\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]\right)$ be the class of $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]$. Observe that $\gcd(a, c, N) = 1$ and define $d = \gcd(c, N)$. By Lemma 2.25, there is $y \in \mathbb{Z}$ with $\gcd(y, N) = 1$ such that

$$cy \equiv d \pmod{N}.$$

Choose x such that $yx \equiv a \pmod{N}$. Then we have that

$$\begin{bmatrix} a \\ yc \end{bmatrix} \equiv \begin{bmatrix} yx \\ d \end{bmatrix} \pmod{N}.$$

We need to check that $\left[\begin{smallmatrix} \bar{x} \\ \bar{d} \end{smallmatrix}\right] \in ((\mathbb{Z}/N\mathbb{Z})^2)^\star$. Since $yx \equiv a \pmod{N}$, we have that $\gcd(x, N) \mid a$. Recall that $\gcd(a, c, N) = 1$ and $\gcd(c, N) = d$, and so $\gcd(a, d) = 1$. Therefore $\gcd(x, d, N) \mid \gcd(a, d) = 1$ which implies that $\gcd(x, d, N) = 1$. Hence $\left[\begin{smallmatrix} \bar{x} \\ \bar{d} \end{smallmatrix}\right]$ is in $((\mathbb{Z}/N\mathbb{Z})^2)^\star$.

By Theorem 2.7, $\psi\left(\left[\begin{smallmatrix} \bar{a} \\ \bar{c} \end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix} \bar{x} \\ \bar{d} \end{smallmatrix}\right]\right)$.

□

Lemma 2.27. The divisor d in Lemma 2.26 is unique.

Proof. Given a positive integer N, let d_1 and d_2 be divisors of N. It suffices to show that $\psi\left(\left[\begin{smallmatrix} \bar{a}_1 \\ \bar{d}_1 \end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix} \bar{a}_2 \\ \bar{d}_2 \end{smallmatrix}\right]\right)$ implies that $d_1 = d_2$.

Observe that if $\gcd(a_1, d_1, N) = 1$ then $\gcd(a_1, d_1) = 1$. Therefore $\left[\begin{smallmatrix} a_1 \\ d_1 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} a_2 \\ d_2 \end{smallmatrix}\right]$ are lifts of $\left[\begin{smallmatrix} \bar{a}_1 \\ \bar{d}_1 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} \bar{a}_2 \\ \bar{d}_2 \end{smallmatrix}\right]$ to $(\mathbb{Z}^2)^\star$.

If $\psi\left(\left[\begin{smallmatrix} \bar{a}_1 \\ \bar{d}_1 \end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix} \bar{a}_2 \\ \bar{d}_2 \end{smallmatrix}\right]\right)$ then

$$\begin{bmatrix} ya_1 \\ d_1 \end{bmatrix} \equiv \begin{bmatrix} a_2 + jd_1 \\ yd_2 \end{bmatrix} \pmod{N}$$

for some integers j, y with $\gcd(y, N) = 1$.

By Lemma 2.25 if $d_1 \equiv yd_2 \pmod{N}$ then $\gcd(d_1, N) = d_2$. Clearly $\gcd(d_1, N) = d_1$ and so $d_1 = d_2$ which proves the lemma.

□

Given $d \mid N$, let $\ell = \gcd(d, N/d)$.

Lemma 2.28. Suppose $d \mid N$ and $\psi\left(\left[\begin{smallmatrix} \bar{a}_1 \\ \bar{d} \end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix} \bar{a}_2 \\ \bar{d} \end{smallmatrix}\right]\right)$. Then $a_1 \equiv a_2 \pmod{\ell}$.

Proof. If $\psi\left(\left[\begin{smallmatrix} \bar{a}_1 \\ \bar{d} \end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix} \bar{a}_2 \\ \bar{d} \end{smallmatrix}\right]\right)$ then

$$\begin{bmatrix} ya_1 \\ d \end{bmatrix} \equiv \begin{bmatrix} a_2 + jd \\ yd \end{bmatrix} \pmod{N}$$

for some integers j, y with $\gcd(y, N) = 1$. The bottom congruence $yd \equiv d \pmod{N}$ implies that $y \equiv 1 \pmod{N/d}$ and so $y = 1 + (N/d)z$ for some integer z. Plugging into the top congruence gives

$$(1 + (N/d)z)a_1 \equiv a_2 + jd \pmod{N}.$$

Simplifying we get

$$a_1 \equiv a_2 - (N/d)za_1 + jd \pmod{N}.$$

Hence $a_1 \equiv a_2 \pmod{\ell}$ since $\ell \mid N/d$ and $\ell \mid d$.

□

Lemma 2.29. Suppose $d \mid N$ and $a_1 \equiv a_2 \pmod{\ell}$. Also suppose $\gcd(a_2, d) = 1$. Then there exist integers y, j with $y \equiv 1 \pmod{N/d}$ such that $ya_2 + jd \equiv a_1 \pmod{N}$.

Proof. Since $\ell = \gcd(d, N/d)$, there exist integers u, v such that $\ell = ud + v(N/d)$. Also if $a_1 \equiv a_2 \pmod{\ell}$ then $a_1 = a_2 + w\ell$ for some integer w. Plugging in ℓ gives

$$\begin{aligned} a_1 &= w(ud + v(N/d)) + a_2 \\ &= (wu)d + (wv)(N/d) + a_2 \\ &= jd + (wv)(N/d) + a_2 \qquad \text{letting } j = wu. \end{aligned}$$

Therefore it suffices to find y so that

$$(wv)(N/d) + a_2 \equiv ya_2 \pmod{N}. \tag{2.7}$$

Let $y = 1 + z(N/d)$. Plugging this in to (2.7) gives

$$\begin{aligned} (wv)(N/d) + a_2 &\equiv (1 + z(N/d))a_2 \pmod{N} \\ &= a_2 + a_2 z(N/d). \end{aligned}$$

Canceling a_2 we get

$$(wv)(N/d) \equiv a_2 z(N/d) \pmod{N}.$$

This congruence holds if $(wv) \equiv a_2 z \pmod{d}$, and since $\gcd(a_2, d) = 1$ we can solve for z so that $z \equiv (wv)a_2^{-1} \pmod{d}$. Thus if we let $z \equiv (wv)a_2^{-1} \pmod{d}$ then $y = 1 + z(N/d)$ is an integer and congruence (2.7) holds. This proves the lemma.

□

Lemma 2.30. Suppose $d \mid N$ and $a_1 \equiv a_2 \pmod{\ell}$. Also suppose $\gcd(a_1, d) = \gcd(a_2, d) = 1$. There exist y, j with $\gcd(y, N) = 1$ such that $ya_2 + jd \equiv a_1 \pmod{N}$ and $y \equiv 1 \pmod{N/d}$.

Proof. By Lemma 2.29 there are integers y, j such that

$$ya_2 + jd \equiv a_1 \pmod{N}. \tag{2.8}$$

Therefore $ya_2 \equiv a_1 \pmod{d}$. Recall that a_1, a_2 are invertible $\pmod{d}$ so $\gcd(y, d) = 1$. Lemma 2.29 gives that $\gcd(y, N/d) = 1$. Therefore $\gcd(y, N) = 1$, and this proves the lemma. □

Lemma 2.31. Suppose $d \mid N$ and $\left[\begin{smallmatrix} \bar{a}_1 \\ \bar{d} \end{smallmatrix}\right], \left[\begin{smallmatrix} \bar{a}_2 \\ \bar{d} \end{smallmatrix}\right] \in ((\mathbb{Z}/N\mathbb{Z})^2)^\star$. If $a_1 \equiv a_2 \pmod{\ell}$ then $\psi\left(\left[\begin{smallmatrix} \bar{a}_1 \\ \bar{d} \end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix} \bar{a}_2 \\ \bar{d} \end{smallmatrix}\right]\right)$.

Proof. Let $\left[\begin{smallmatrix} a_1 \\ d \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} a_2 \\ d \end{smallmatrix}\right]$ be lifts of $\left[\begin{smallmatrix} \bar{a}_1 \\ \bar{d} \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} \bar{a}_2 \\ \bar{d} \end{smallmatrix}\right]$ in $(\mathbb{Z}^2)^\star$ respectively. If $a_1 \equiv a_2 \pmod{\ell}$ then by Lemma 2.30 there are integers y, j with $\gcd(y, N) = 1$ such that

$$ya_1 \equiv a_2 - jd \pmod{N}.$$

Additionally $y \equiv 1 \pmod{N/d}$ so $d \equiv yd \pmod{N}$. Thus we have that

$$\begin{bmatrix} ya_1 \\ d \end{bmatrix} \equiv \begin{bmatrix} a_2 - jd \\ yd \end{bmatrix} \pmod{N}.$$

Therefore $\left[\begin{smallmatrix} a_1 \\ d \end{smallmatrix}\right] \sim_3 \left[\begin{smallmatrix} a_2 \\ d \end{smallmatrix}\right]$ and so $\psi\left(\left[\begin{smallmatrix} \bar{a}_1 \\ \bar{d} \end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix} \bar{a}_2 \\ \bar{d} \end{smallmatrix}\right]\right)$.

□

Lemma 2.32. Suppose $\left[\begin{smallmatrix} \bar{a} \\ \bar{d} \end{smallmatrix}\right] \in ((\mathbb{Z}/N\mathbb{Z})^2)^\star$ with $d \mid N$. Then $\gcd(a, \ell) = 1$.

Proof. Notice that $\gcd(a, d, N) = 1$ since $\left[\begin{smallmatrix} \bar{a} \\ \bar{d} \end{smallmatrix}\right]$ is in $((\mathbb{Z}/N\mathbb{Z})^2)^\star$. Therefore $\gcd(a, d) = 1$ which implies that $\gcd(a, \ell) = 1$ since $\ell \mid d$. □

Lemma 2.33. Let $a, d, N \in \mathbb{Z}$ such that $\gcd(a, d) = 1$ and $N \neq 0$. Let

$$P = \{\text{primes } p : p \mid N \quad \text{and} \quad p \nmid a\}$$

and

$$n = \prod_{p \in P} p.$$

Then $\gcd(a + nd, N) = 1$.

Proof. Suppose p is a prime such that $p \mid a + nd$ and $p \mid N$.

Case 1: suppose $p \mid a$. Thus $p \mid nd$ and so p divides n or d. If $p \mid n$ then $p \in P$ and so $p \nmid a$ which is a contradiction. If $p \mid d$ then $p \mid \gcd(a, d)$ which is a contradiction since $\gcd(a, d) = 1$.

Case 2: suppose $p \nmid a$. Therefore $p \in P$ and so $p \mid nd$. This is a contradiction since $p \mid a + nd$.

Thus there are no such primes, which proves the lemma. □

Lemma 2.34. Suppose $d \mid N$. Given an integer a_1 with $\gcd(a_1, \ell) = 1$, there exists $a_2 \equiv a_1 \pmod{\ell}$ such that $\left[\begin{smallmatrix} \bar{a}_2 \\ \bar{d} \end{smallmatrix}\right] \in ((\mathbb{Z}/N\mathbb{Z})^2)^\star$.

Proof. Since $\gcd(a_1, \ell, N) = 1$, by Lemma 2.33 there is an integer n such that $a_1 + \ell n$ is relatively prime to N. Let $a_2 = a_1 + \ell n$. Therefore $\gcd(a_2, d, N) = 1$ and so $\left[\begin{smallmatrix} \bar{a}_2 \\ \bar{d} \end{smallmatrix}\right] \in ((\mathbb{Z}/N\mathbb{Z})^2)^\star$. □

2.3.8 Algorithm for cusps of $X_0(N)$

We will use the following algorithm to determine the system of representatives for the elements of $(\mathbb{Z}^2)^\star/\sim_3$. Define the set $P(n) = \{x : 0 \leq x < n, \gcd(x, n) = 1\}$.

1. For each divisor d of N, define $\ell = \gcd(d, N/d)$. For every $a \in P(\ell)$ add $\left[\begin{smallmatrix} a \\ d \end{smallmatrix}\right]$ to the list.
2. For each elements $\left[\begin{smallmatrix} a \\ d \end{smallmatrix}\right]$ from the list created in Step 1, if $\gcd(a, d, N) \neq 1$ then replace with $\left[\begin{smallmatrix} a+\ell \\ d \end{smallmatrix}\right]$. Repeat adding ℓ until the resulting $\left[\begin{smallmatrix} a \\ d \end{smallmatrix}\right]$ satisfies $\gcd(a, d, N) = 1$.

We will prove that the algorithm gives the cusps of $X_0(N)$.

Theorem 2.35. *The above algorithm gives a set of elements in $((\mathbb{Z}/N\mathbb{Z})^2)^\star$ that lift to a set of representatives for the equivalence classes of $(\mathbb{Z}^2)^\star$ with respect to $\sim_3$.*

Proof. By Lemma 2.26, for any element $\left[\begin{smallmatrix}\bar{a}\\ \bar{c}\end{smallmatrix}\right]$ in $((\mathbb{Z}/N\mathbb{Z})^2)^\star$, there is $\bar{x}, \bar{d} \in \mathbb{Z}/N\mathbb{Z}$ with d a divisor of N such that $\psi\left(\left[\begin{smallmatrix}\bar{a}\\ \bar{c}\end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix}\bar{x}\\ \bar{d}\end{smallmatrix}\right]\right)$. By Lemma 2.27 this divisor is unique. Thus to choose elements of $((\mathbb{Z}/N\mathbb{Z})^2)^\star$ that lift to a set of representatives it suffices to give a condition for $\bar{a}_1, \bar{a}_2 \in ((\mathbb{Z}/N\mathbb{Z})^2)^\star$ so that $\psi\left(\left[\begin{smallmatrix}\bar{a}_1\\ \bar{d}\end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix}\bar{a}_2\\ \bar{d}\end{smallmatrix}\right]\right)$.

Suppose $d \mid N$ and $\left[\begin{smallmatrix}\bar{a}_1\\ \bar{d}\end{smallmatrix}\right], \left[\begin{smallmatrix}\bar{a}_2\\ \bar{d}\end{smallmatrix}\right] \in ((\mathbb{Z}/N\mathbb{Z})^2)^\star$. By Lemma 2.28 and Lemma 2.31, $a_1 \equiv a_2 \pmod{\ell}$ if and only if $\psi\left(\left[\begin{smallmatrix}\bar{a}_1\\ \bar{d}\end{smallmatrix}\right]\right) = \psi\left(\left[\begin{smallmatrix}\bar{a}_2\\ \bar{d}\end{smallmatrix}\right]\right)$. By Lemma 2.32, a_1 and a_2 must be relatively prime to ℓ. Therefore for each divisor d of N, the elements of $((\mathbb{Z}/N\mathbb{Z})^2)^\star$ that lift to a set of representatives are given by $\left[\begin{smallmatrix}\bar{a}\\ \bar{d}\end{smallmatrix}\right]$ where $\gcd(a, \ell) = 1$.

To give a list of all such element that lift to a set of representatives, for each divisor d of N add to the list $\left[\begin{smallmatrix}\bar{a}\\ \bar{d}\end{smallmatrix}\right]$ for each $a \in P(\ell)$. If $\left[\begin{smallmatrix}\bar{a}\\ \bar{d}\end{smallmatrix}\right] \notin ((\mathbb{Z}/N\mathbb{Z})^2)^\star$, by Lemma 2.34 there is an integer n with $x = a + \ell n$ such that $\left[\begin{smallmatrix}\bar{x}\\ \bar{d}\end{smallmatrix}\right] \in ((\mathbb{Z}/N\mathbb{Z})^2)^\star$. Thus Step 2 of the algorithm terminates and this proves the theorem.

□

Corollary 2.36. The algorithm outputs a set that is in bijection with the cusps of $X_0(N)$.

Proof. By Theorem 2.23 the algorithm outputs a set that is in bijection with $(\mathbb{Z}^2)^\star/\sim_3$. By Proposition 2.4, the map

$$\varphi : (\mathbb{Z}^2)^\star/\sim_3 \to \Gamma_0\backslash\mathbb{Q}^\star$$

where $\varphi\left(\left[\begin{smallmatrix}a\\ c\end{smallmatrix}\right]\right) = \Gamma_0(a/c)$, is a bijection. Hence the algorithm outputs a set in bijection with the cusps of $X_0(N)$. □

Theorem 2.37. *The number of cusps of $X_0(N)$ is*

$$\sum_{d|N} \phi(\gcd(d, N/d)).$$

Proof. From our algorithm we can count the number of cusps. For each divisor d of N, we add an element for each $x \in P(\gcd(d, N/d))$. Since there are $\phi(\gcd(d, N/d))$ elements in $P(\gcd(d, N/d))$ the number of cusps of $X_0(N)$ is

$$\sum_{d|N} \phi(\gcd(d, N/d)).$$

□

We will now implement the algorithm to determine the cusps of $X_0(4)$

Example 2.38. Compute the cusps of $X_0(4)$.

The divisors of 4 are $1, 2, 4$. First let $d = 1$, then $\ell = \gcd(1, 4) = 1$. Therefore add $\left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right]$ to the list. Let $d = 2$, and so $\ell = \gcd(2, 2) = 2$. Hence we can add $\left[\begin{smallmatrix}1\\ 2\end{smallmatrix}\right]$. Lastly let $d = 4$, so $\ell = \gcd(4, 1) = 1$. Hence we can add $\left[\begin{smallmatrix}1\\ 4\end{smallmatrix}\right]$ to the list.

Our final list is

$$\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}1\\4\end{bmatrix}.$$

We check that $\gcd(0,1,4) = \gcd(1,2,4) = \gcd(1,4,4) = 1$ and so this list gives a system of representatives for the cusps of $X_0(4)$.

2.3.9 Algorithm in Sage

We will give the Sage code to implement the algorithm for cusps in $X_0(N)$.

```
def div(N):
    """Output list of positive integers that divide N."""
    l=[]
    for i in range(1,N+1):
        if N%i==0:
            l.append(i)
    return l

def tot(N):
    """Output list of integers less than N coprime to N.
    ↪ """
    l=[]
    for i in range(N):
        if gcd(i,N)==1:
            l.append(i)
    return l

def lift2(x,d1,d2,N):
    """Output x+d1 if gcd(x,d2,N)!=1."""
    while true:
        e=gcd(x,d2)
        if gcd(e,N)==1:
            return x
        else:
            x = x +d1

def cusps0(N):
    """Output cusps of X_0(N).

    Create a list of pairs [a,d] with d a divisor of N
    and a is relatively prime to gcd(d,N/d)."""
    l=[]
    k = div(N)
    for i in k:
        d=gcd(i,N/i)
        g =tot(d)
        for m in g:
```

```
            l.append([lift2(m,d,i,N),i])
    return l
```

Using the algorithm defined in this section we can compute the cusps of the modular curves $X_0(N)$ for $2 \leq N \leq 12$. The computations are given in Table 2.2.

N	Cusps of $X_0(N)$
1	$\begin{bmatrix}1\\0\end{bmatrix}$
2	$\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}$
3	$\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\3\end{bmatrix}$
4	$\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}1\\4\end{bmatrix}$
5	$\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\5\end{bmatrix}$
6	$\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}1\\3\end{bmatrix}, \begin{bmatrix}1\\6\end{bmatrix}$
7	$\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\7\end{bmatrix}$
8	$\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}1\\4\end{bmatrix}, \begin{bmatrix}1\\8\end{bmatrix}$
9	$\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\3\end{bmatrix}, \begin{bmatrix}2\\3\end{bmatrix}, \begin{bmatrix}1\\9\end{bmatrix}$
10	$\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}1\\5\end{bmatrix}, \begin{bmatrix}1\\10\end{bmatrix}$
11	$\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\11\end{bmatrix}$
12	$\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}1\\3\end{bmatrix}, \begin{bmatrix}1\\4\end{bmatrix}, \begin{bmatrix}1\\6\end{bmatrix}, \begin{bmatrix}1\\12\end{bmatrix}$

TABLE 2.2: Cusps of $X_0(N)$

Chapter 3

Elliptic Points

3.1 Definitions

Recall the definition of an elliptic point:

Definition 3.1. Given a congruence subgroup Γ, a point $z \in \mathbb{H}$ is an *elliptic point* of Γ if there exists $\gamma \in \Gamma, \gamma \neq \pm I$ such that $\gamma z = z$. Let π be as in (1.8). The corresponding $\pi(z) \in X(\Gamma)$ is similarly called an *elliptic point*.

We have shown that $X(1)$ has two elliptic points, the orbits of i and ρ. We would like to give a method for finding the elliptic points of $X(N), X_1(N)$ and $X_0(N)$. Recall that if z is an elliptic point of Γ then the order of the stabilizer is either order 3,4 or 6. The order of the quotient of the stabilizer by $\{\pm I\}$ we call the *period of* z. If $-I$ is not in Γ, we first multiply Γ by $\{\pm I\}$ and then take the quotient. Additionally define the period of $\pi(z) \in X(\Gamma)$ to be the period of z. The period of an elliptic point is either 2 or 3.

3.2 Elliptic points of $X(N)$

Theorem 3.2. *For $N > 1$ the elliptic curve $X(N)$ has no elliptic points.*

Proof. Observe that an elliptic point of $X(N)$ has period 2 or 3.

First assume $\tau \in \mathbb{H}$ is an elliptic point of $\Gamma(N)$ with period 2. Then there is some $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma(N)$ of order 4 such that $\gamma\tau = \tau$. By Lemma 1.20, γ is conjugate to $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$. Notice that $a \equiv d \equiv 1 \pmod{N}$ and $c \equiv d \equiv 0 \pmod{N}$ since $\gamma \in \Gamma(N)$.

Conjugate matrices have the same trace and so $a = -d$. Substituting into the congruence gives

$$1 \equiv -1 \pmod{N},$$

which implies that $N = 2$.

We have the condition that $-a^2 - bc = 1$ since $a = -d$ and $\det(\gamma) = 1$. Also a is odd since $a \equiv 1 \pmod{2}$ and so $a = 2\ell + 1$ for some $\ell \in \mathbb{Z}$. Therefore $-4\ell^2 - 4\ell - 1 - bc = 1$ which simplifies to

$$-4\ell^2 - 4\ell - bc = 2. \tag{3.1}$$

We know that $2 \mid b$ and $2 \mid c$ since $b \equiv 0 \pmod 2$ and $c \equiv 0 \pmod 2$, and therefore $4 \mid bc$. Hence 4 divides the left hand side of (3.1). Thus $4 \nmid 2$ which gives a contradiction and so there is no elliptic point of $\Gamma(N)$ with period 2.

We will now show that $X(N)$ has no elliptic points of period 3. Assume that $\tau \in \mathbb{H}$ is an elliptic point of $\Gamma(N)$ with period 3. Therefore there is $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma(N)$ such that $\gamma\tau = \tau$ where γ is conjugate to $\left[\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right]$ by Lemma 1.20.

Conjugate matrices have the same trace so $a + d = -1$ and so $(-a - 1)a - bc = 1$. Therefore $-a^2 - a - bc = 1$. Substituting $a \equiv 1 \pmod N, b \equiv 0 \pmod N$ and $c \equiv 0 \pmod N$ we get

$$-2 \equiv 1 \pmod N$$

and so $N = 3$. We had that $-a^2 - a - bc = 1$ and since $a \equiv 1 \pmod 3$ then $a = 3\ell + 1$ for some ℓ. By substituting we get

$$\begin{aligned} 1 &= -(3\ell + 1)^2 - (3\ell + 1) - bc \\ &= -(9\ell^2 + 6\ell + 1) - (3\ell + 1) - bc \\ &= -9\ell^2 - 9\ell - bc - 2. \end{aligned}$$

Therefore $1 = -9\ell^2 - 9\ell - bc - 2$ and adding 2 to both sides we get

$$3 = -9\ell^2 - 9\ell - bc.$$

Since $3 \mid b$ and $3 \mid c$, 9 divides the right hand side of the above equation, but clearly 9 does not divide the left hand side. This gives a contradiction and proves that $X(N)$ does not contain any elliptic points. □

3.3 Elliptic points of $X_1(N)$

We will now find the elliptic points for $X_1(N)$.

Theorem 3.3. *There are no elliptic points in $X_1(N)$ for $N > 3$.*

Proof. We will prove that if $X_1(N)$ has an elliptic point with period 2 then $N = 2$ and if $X_1(N)$ has an elliptic point of period 3, then $N = 3$. This implies that if $X_1(N)$ has elliptic points then $N \leq 3$, which proves the theorem.

Case 1: Assume $X_1(N)$ has an elliptic point of period 2. Let $\tau \in \mathbb{H}$ be an elliptic point of $\Gamma_1(N)$ with period 2, so there is $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma_1(N)$ such that $\gamma\tau = \tau$ where γ is conjugate to $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ by Lemma 1.20.

Since γ is conjugate to $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$, their traces are the same and therefore $a+d = 0$. Additionally, $a \equiv d \equiv 1 \pmod N$ since $\gamma \in \Gamma_1(N)$. Substituting gives

$$2 \equiv 0 \pmod N.$$

This implies that $N = 2$. Therefore if $X_1(N)$ has an elliptic point of period 2 then $N = 2$.

Case 2: Assume $X_1(N)$ has an elliptic point with period 3. Let $\tau \in \mathbb{H}$ be an elliptic point of $\Gamma_1(N)$ with period 3, so there is $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma_1(N)$ such that $\gamma\tau = \tau$ where γ is conjugate to $\left[\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right]$ by Lemma 1.20. Conjugate matrices

have the same trace so $a+d=-1$. Additionally, $a \equiv d \equiv 1 \pmod{N}$. Plugging in the congruences to $a+d=-1$ gives

$$2 \equiv -1 \pmod{N}.$$

This implies that $N=3$. Hence if $X_1(N)$ has an elliptic point of period 3 then $N=3$. □

Both $X_1(2)$ and $X_1(3)$ may contain elliptic points. We will now explicitly find the elliptic points for these modular curves.

We will use Γ to denote either $\Gamma_1(N)$ or $\Gamma_0(N)$. The set Γ is a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and we can represent the latter group as the union of disjoint right cosets

$$\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{j=1}^{d} \Gamma\gamma_j \tag{3.2}$$

where the γ_j are called the *coset representatives*. From elementary group theory we know that the cosets form a partition of the set $\mathrm{SL}_2(\mathbb{Z})$.

Lemma 3.4. Let $\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{j=1}^{d} \Gamma\gamma_j$ be a coset decomposition of $\mathrm{SL}_2(\mathbb{Z})$. Each elliptic point of Γ of period 2 is in the orbit of at least one of $\gamma_1(i), \gamma_2(i), \ldots, \gamma_d(i)$. Each elliptic point of Γ with period 3 is in the orbit of at least one of $\gamma_1(\rho), \gamma_2(\rho), \ldots, \gamma_d(\rho)$.

The stabilizer of $\gamma_j(i)$ in $\mathrm{SL}_2(\mathbb{Z})$ is the subgroup generated by $\gamma_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \gamma_j^{-1}$ and the stabilizer of $\gamma_j(\rho)$ in $\mathrm{SL}_2(\mathbb{Z})$ is the subgroup generated by $\gamma_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right] \gamma_j^{-1}$.

Proof. Let $\tau \in \mathbb{H}$ be an elliptic point of Γ. The period of τ is either 2 or 3. Assume that τ has period 2. Therefore τ is some point in the $\mathrm{SL}_2(\mathbb{Z})$-orbit of i and so $\tau = \gamma(i)$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

The element γ is only in one right coset of (3.2), say $\Gamma\gamma_k$. Therefore $\gamma = \alpha\gamma_k$ for some $\alpha \in \Gamma$. Hence

$$\alpha\gamma_k(i) = \gamma(i)$$

and so $\gamma_k(i)$ and $\tau = \gamma(i)$ are in the same Γ-orbit. Since τ was an arbitrary elliptic point with period 2, this holds for any elliptic point of Γ with period 2.

Repeating the above argument for an elliptic point $\tau \in \mathbb{H}$ of Γ with period 3 gives that $\tau = \gamma(\rho)$ is in the same Γ-orbit as one of $\gamma_1(\rho), \gamma_2(\rho), \ldots, \gamma_d(\rho)$ in $X_i(N)$. This proves the first statement.

Now we will give the stabilizers of $\gamma_j(i)$ and $\gamma_j(\rho)$.

Let β be in the stabilizer of $\gamma_j(i)$, so $\beta\gamma_j(i) = \gamma_j(i)$. Therefore

$$\gamma_j^{-1}\beta\gamma_j(i) = (i).$$

We have shown that the stabilizer of i is $\langle \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \rangle$ and so $\gamma_j^{-1}\beta\gamma_j = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]^n$ for some integer n. Therefore $\beta = \gamma_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]^n \gamma_j^{-1}$. This proves that the stabilizer of $\gamma_j(i)$ is a subset of the group generated by $\gamma_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \gamma_j^{-1}$.

To show the reverse inclusion let $\gamma_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]^n \gamma_j^{-1}$ be an element of the group generated by $\gamma_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \gamma_j^{-1}$. We can see that

$$\begin{aligned}\gamma_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]^n \gamma_j^{-1}(\gamma_j(i)) &= \gamma_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]^n (i) \\ &= \gamma_j(i).\end{aligned}$$

Therefore $\gamma_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]^n \gamma_j^{-1}$ is in the stabilizer of $\gamma_j(i)$. This proves that the stabilizer of $\gamma_j(i)$ is the subgroup generated by $\gamma_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \gamma_j^{-1}$.

Repeating the above argument gives that the stabilizer of $\gamma_j(\rho)$ is the subgroup generated by $\gamma_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right] \gamma_j^{-1}$. This proves the second statement. □

Corollary 3.5. Let $\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{j=1}^{d} \Gamma\gamma_j$ be a coset decomposition of $\mathrm{SL}_2(\mathbb{Z})$. $\gamma_k \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \gamma_k^{-1}$ is in Γ if and only if $\gamma_k(i)$ is an elliptic point of Γ and $\pm\gamma_k \left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right] \gamma_k^{-1}$ is in Γ if and only if $\gamma_k(\rho)$ is an elliptic point of Γ.

To give all elliptic points of Γ it suffices to check if $\gamma_k \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \gamma_k^{-1} \in \Gamma$ and $\gamma_k \left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right] \gamma_k^{-1} \in \Gamma$ for each coset representative γ_k.

Proof. By Lemma 3.4, the stabilizer of $\gamma_k(i)$ is generated by $\gamma_k \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \gamma_k^{-1}$ and so if $\gamma_k \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \gamma_k^{-1} \in \Gamma$ then $\gamma_k(i)$ is an elliptic point of Γ. Similarly $\gamma_k(\rho)$ is an elliptic point of Γ if $\pm\gamma_k \left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right] \gamma_k^{-1} \in \Gamma$.

□

We have shown that only $X_1(2)$ and $X_1(3)$ contain elliptic points. The following theorems will gives the respective elliptic points of these two modular curves.

Theorem 3.6. *The elliptic point of $X_1(2)$ is the orbit of $\tau = \frac{1}{2} + \frac{1}{2}i$.*

Proof. We showed that if $X_1(2)$ has an elliptic point τ, then the stabilizer of τ has order 2.

The coset representatives of $\Gamma_1(2)$ are given by

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Theorem 4.8 gives that the index is 3. It is easy to check that these give different cosets.

By Lemma 3.4, every elliptic point is in the orbit of one of $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] i, \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] i, \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right] i$. If we compute $\gamma_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \gamma_j^{-1}$ for each coset representative we get

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^{-1} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \text{ and}$$

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -1 \\ 2 & -1 \end{bmatrix}.$$

We see that $\left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right] \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]^{-1} = \left[\begin{smallmatrix} 1 & -1 \\ 2 & -1 \end{smallmatrix}\right] \in \Gamma_1(2)$ and $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ is not in $\Gamma_1(2)$. Therefore every elliptic point of $\Gamma_1(2)$ is in the orbit of $\left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right] i$.

We compute

$$\begin{aligned}\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix} i &= \frac{i}{i+1}\\ &= \frac{i^2-i}{i^2-1}\\ &= \frac{-1-i}{-2}\\ &= \frac{1}{2}+\frac{1}{2}i.\end{aligned}$$

Hence the elliptic point of $X_1(2)$ is the orbit of $\tau = \frac{1}{2}+\frac{1}{2}i$. □

Theorem 3.7. *The elliptic point of $X_1(3)$ is the orbit of $\tau = -\frac{1}{2}+\frac{\sqrt{3}}{6}i$.*

Proof. We have shown that if τ is an elliptic point of $\Gamma_1(3)$then τ has period 3. A set of coset representatives for $\Gamma_1(3)$ is given by

$$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}, \begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}, \begin{bmatrix}0 & -1\\ 1 & 2\end{bmatrix}.$$

Theorem 4.8 gives that the index $[\{\pm I\}\Gamma(1) : \{\pm I\}\Gamma_1(3)]$ is 4. It is easy to check that these give different cosets.

The elliptic points of $X_1(3)$ have period 3. Therefore the elliptic points are in the orbit of $\left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]\rho$, $\left[\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right]\rho$, $\left[\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right]\rho$, and $\left[\begin{smallmatrix}0 & -1\\ 1 & 2\end{smallmatrix}\right]\rho$.

As in the previous theorem we can compute $\gamma_j \left[\begin{smallmatrix}0 & -1\\ 1 & 1\end{smallmatrix}\right] \gamma_j^{-1}$ for all coset representatives:

$$\begin{aligned}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}0 & -1\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}^{-1} &= \begin{bmatrix}0 & -1\\ 1 & 1\end{bmatrix},\\ \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0 & -1\\ 1 & 1\end{bmatrix}\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}^{-1} &= \begin{bmatrix}1 & -1\\ 1 & 0\end{bmatrix},\\ \begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}\begin{bmatrix}0 & -1\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}^{-1} &= \begin{bmatrix}1 & -1\\ 1 & 0\end{bmatrix}, \text{and}\\ \begin{bmatrix}0 & -1\\ 1 & 2\end{bmatrix}\begin{bmatrix}0 & -1\\ 1 & 1\end{bmatrix}\begin{bmatrix}0 & -1\\ 1 & 2\end{bmatrix}^{-1} &= \begin{bmatrix}-1 & -1\\ 3 & 2\end{bmatrix}.\end{aligned}$$

We can see that only the matrix $-\left[\begin{smallmatrix}-1 & -1\\ 3 & 2\end{smallmatrix}\right]$ is in $\Gamma_1(3)$. Therefore all elliptic points are in the orbit of $\left[\begin{smallmatrix}0 & -1\\ 1 & 2\end{smallmatrix}\right]\rho$. We compute

$$\begin{bmatrix}0 & -1\\ 1 & 2\end{bmatrix}\rho = \frac{-1}{\rho+2}.$$

Recall that $\rho = \frac{-1+i\sqrt{3}}{2}$ and so we can explicitly find $\frac{-1}{\rho+2}$. We have that

$$\begin{aligned}\frac{-1}{\rho+2} &= \frac{-1}{\frac{-1+i\sqrt{3}}{2}+2} \\ &= \frac{-1}{\frac{3+i\sqrt{3}}{2}} \\ &= \frac{-2}{3+i\sqrt{3}} \\ &= \frac{-2}{3+i\sqrt{3}}\frac{3-i\sqrt{3}}{3-i\sqrt{3}} \\ &= \frac{-6+i2\sqrt{3}}{12} \\ &= -\frac{1}{2}+\frac{\sqrt{3}}{6}i\end{aligned}$$

Therefore the elliptic point of $X_1(3)$ is the orbit of $\tau = -\frac{1}{2}+\frac{\sqrt{3}}{6}i$. □

3.4 Elliptic points of $X_0(N)$

We have given the elliptic points for $X(N)$ and $X_1(N)$. We will now give an easy method for finding elliptic points of $X_0(p)$ when p is prime. We will use a similar method that was used for finding the elliptic points of $\Gamma_1(2)$ and $\Gamma_1(3)$.

Lemma 3.8. Let $\alpha_j = \left[\begin{smallmatrix} 1 & 0 \\ j & 1 \end{smallmatrix}\right]$ for $j = 0, \ldots, p-1$ and $\alpha_\infty = \left[\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right]$. Then

$$\mathrm{SL}_2(\mathbb{Z}) = \bigcup_j \Gamma_0(p)\alpha_j$$

is a disjoint union.

Proof. We first would like to show that the cosets are disjoint. That is, $\Gamma_0(p)\alpha_i \cap \Gamma_0(p)\alpha_j = \emptyset$ if $i \neq j$. It suffices to show that $\alpha_i\alpha_j^{-1} \notin \Gamma_0(p)$. Let $i, j \in \{0, \ldots, p-1\}$. We compute $\alpha_i\alpha_j^{-1}$

$$\begin{bmatrix} 1 & 0 \\ i & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ -j & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ i-j & 1 \end{bmatrix}.$$

Since $i \neq j$, the matrix $\alpha_i\alpha_j^{-1}$ is not in $\Gamma_0(p)$. Now compute $\alpha_\infty\alpha_j^{-1}$

$$\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ -j & 1 \end{bmatrix} = \begin{bmatrix} 1+j & -1 \\ 1 & 0 \end{bmatrix}.$$

Since the bottom left entry is 1, $\alpha_\infty\alpha_j^{-1}$ is not in $\Gamma_0(p)$. Therefore the cosets are distinct.

By Theorem 4.8, the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(p)]$ equals $p+1$. Given that there are $p+1$ cosets and the cosets are distinct, this proves the lemma. □

Theorem 3.9. *Let p be prime. The elliptic points of $X_0(p)$ with period 2 are the orbits of $\alpha_j(i)$ for $0 \leq j \leq p$ that satisfy the congruence $j^2 + 1 \equiv 0 \pmod{p}$.*

Proof. Lemma 3.8 gives the coset decomposition

$$\mathrm{SL}_2(\mathbb{Z}) = \bigcup_j \Gamma_0(p)\alpha_j.$$

By Lemma 3.4, $\alpha_j(i)$ is an elliptic point of $\Gamma_0(p)$ with period 2 if $\alpha_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \alpha_j^{-1} \in \Gamma_0(p)$. We directly compute $\alpha_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \alpha_j^{-1}$ for all coset representatives α_j. We first compute $\alpha_\infty \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \alpha_\infty^{-1}$:

$$\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & -2 \\ 1 & -1 \end{bmatrix}$$

which clearly is not an element of $\Gamma_0(p)$.

Next we compute $\alpha_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \alpha_j^{-1}$ for $j \in \{0, \ldots, p-1\}$:

$$\begin{aligned} \begin{bmatrix} 1 & 0 \\ j & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -j & 1 \end{bmatrix} &= \begin{bmatrix} 0 & -1 \\ 1 & -j \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -j & 1 \end{bmatrix} \\ &= \begin{bmatrix} j & -1 \\ j^2 + 1 & -j \end{bmatrix}. \end{aligned}$$

Therefore $\alpha_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \alpha_j^{-1} \in \Gamma_0(p)$ if and only if $j^2 + 1 \equiv 0 \pmod{p}$ and so the elliptic points of $\Gamma_0(p)$ are $\alpha_j(i)$ for all j that satisfy $j^2 + 1 \equiv 0 \pmod{p}$. □

Theorem 3.10. *Let p be prime, the elliptic points of $X_0(p)$ with period 3 are the orbits of $\alpha_j(\rho)$ for all $0 \leq j \leq p$ that satisfy the congruence $j^2 - j + 1 \equiv 0 \pmod{p}$.*

Proof. By Lemma 3.4, all elliptic points in $\Gamma_0(p)$ with period 3 are in the orbit of one of $\alpha_j(\rho)$. Also if $\alpha_j \gamma \alpha_j^{-1} \in \Gamma_0(p)$ then $\alpha_j(\rho)$ is an elliptic point.
We first compute $\alpha_\infty \left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right] \alpha_\infty^{-1}$:

$$\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & -3 \\ 1 & -1 \end{bmatrix}.$$

Therefore $\alpha_\infty \left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right] \alpha_\infty^{-1}$ is not in $\Gamma_0(p)$ and so $\alpha_\infty(\rho)$ is not an elliptic point.
Next we compute $\alpha_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right] \alpha_j^{-1}$ for $j \in \{0, \ldots, p-1\}$:

$$\begin{aligned} \begin{bmatrix} 1 & 0 \\ j & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -j & 1 \end{bmatrix} &= \begin{bmatrix} 0 & -1 \\ 1 & -j+1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -j & 1 \end{bmatrix} \\ &= \begin{bmatrix} j & -1 \\ j^2 - j + 1 & -j+1 \end{bmatrix}. \end{aligned}$$

Therefore $\alpha_j \left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right] \alpha_j^{-1}$ is in $\Gamma_0(p)$ if and only if $j^2 - j + 1 \equiv 0 \pmod{p}$ and so $\alpha_j(\rho)$ is an elliptic point if and only if $j^2 - j + 1 \equiv 0 \pmod{p}$. □

The following table gives the elliptic points of $X_0(N)$ for $1 \leq N \leq 13$. When N is prime we can use Theorem 3.9 and Theorem 3.10 to find the elliptic points. When N is composite one can find coset representatives and use Corollary 3.5 to find the elliptic points.

N	Elliptic points of $X_0(N)$
1	i, ρ
2	$\frac{1}{2} + \frac{1}{2}i$
3	$\frac{1}{2} + \frac{\sqrt{3}}{6}i$
4	None
5	$\frac{3}{10} + \frac{1}{10}i, \frac{2}{5} + \frac{1}{5}i$
6	None
7	$-\frac{5}{14} + \frac{\sqrt{3}}{14}i, -\frac{3}{14} + \frac{1}{14\sqrt{3}}i$
8	None
9	None
10	$\frac{3}{10} + \frac{1}{10}i, \frac{7}{50} + \frac{1}{50}i$
11	None
12	None
13	$\frac{5}{26} + \frac{i}{26}, \frac{8}{65} + \frac{i}{65}, \frac{7}{28} + \frac{\sqrt{3}}{26}i, \frac{19}{182} + \frac{\sqrt{3}}{182}i$

TABLE 3.1: Elliptic points of $X_0(N)$

Chapter 4

Genus and Ramification Degree

In this section we will compute the genera of various modular curves. We will also describe maps between modular curves as well as the ramification degrees of cusps and elliptic points for those maps. We will use the previous discussion of elliptic points and cusps to explicitly give the map for these points.

For the remainder of the chapter let $\Gamma_1 \subset \Gamma_2$ be congruence subgroups and $f : X(\Gamma_1) \to X(\Gamma_2)$ the function given by $\Gamma_1\tau \mapsto \Gamma_2\tau$.

4.1 Ramification degree

4.1.1 Ramification degree formula

Recall the definition of ramification degree:

Definition 4.1. Let $g : X \to Y$ be an analytic, nonconstant function between connected compact Riemann surfaces X and Y. Given $x \in X$ with $y = g(x)$ there exists an integer m_x such that for every neighborhood V of x there is a neighborhood $U \subset V$ of x such that every point, except possibly y, in $g(U)$ has m_x preimages in U. The integer m_x is called the *ramification degree*.

We will now give a method for finding the ramification degree of points in modular curves. Define the projection maps π_1, π_2 from $\mathbb{H}^\star$ to $X(\Gamma_1), X(\Gamma_2)$ by $\tau \mapsto \Gamma_1\tau$ and $\tau \mapsto \Gamma_2\tau$ respectively.

Theorem 4.2. *Let $f : X(\Gamma_1) \to X(\Gamma_2)$ be as above. For each $\pi_1(x_0) \in X(\Gamma_1)$ the ramification degree of $\pi_1(x_0)$ is*

$$[\{\pm I\}Stab_{\Gamma_2}(x_0) : \{\pm I\}Stab_{\Gamma_1}(x_0)].$$

Proof. The following diagram commutes:

$$\begin{array}{ccc} \mathbb{H}^\star & \xrightarrow{\text{Id}} & \mathbb{H}^\star \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\ X(\Gamma_1) & \xrightarrow{f} & X(\Gamma_2). \end{array}$$

Let $x_0 \in \mathbb{H}^\star$. By [DS05, Corollary 2.2.3], for $x_0 \in \mathbb{H}$ there is a neighborhood W of x_0 such that for all $\gamma \in \Gamma_2$, $\gamma(W) \cap W \neq \emptyset$ if and only if $\gamma \in \text{Stab}_{\Gamma_2}(x_0)$. This property also hold for $x_0 \in \mathbb{Q}^\star$. Define the set $\widetilde{V} = \bigcap_{\gamma \in \text{Stab}_{\Gamma_2}(x_0)} \gamma(W)$. If x_0 is not a cusp then $\text{Stab}_{\Gamma_2}(x_0)$ is a finite set so $\widetilde{V}$ is an open set. If x_0 is the

cusp at infinity then $\text{Stab}_{\Gamma_2}(x_0)$ is a group of translations by some integer. Let $V_k = \{z \in \mathbb{H}^\star : \text{Im}(z) > k\}$. For $\gamma \in \text{Stab}_{\Gamma_2}(\infty)$, $\gamma V_k = V_k$. If $x_0 = \delta(\infty)$ is a point in $\mathbb{Q}^\star$, its stabilizer is conjugate to the stabilizer of ∞. Observe if $\delta\gamma\delta^{-1} \in \text{Stab}_{\Gamma_2}(x_0)$ then

$$\delta\gamma\delta^{-1}(\delta V_k) = \delta\gamma V_k = \delta V_k.$$

Therefore $\widetilde{V} = \delta V_k$ is a open neighborhood of x_0 fixed under the action of $\text{Stab}_{\Gamma_2}(x_0)$.

Observe that $\widetilde{V}$ is a neighborhood of x_0 and satisfies $\gamma\widetilde{V} \cap \widetilde{V} \neq \emptyset$ if and only if $\gamma \in \text{Stab}_{\Gamma_2}(x_0)$. (If x_0 is a cusp then this holds for k sufficiently large.) This neighborhood also satisfies $\text{Stab}_{\Gamma_2}(x_0)\widetilde{V} = \widetilde{V}$. Define the sets $U = \pi_1(\widetilde{V})$ and $V = \pi_2(\widetilde{V})$.

Given $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \text{SL}_2(\mathbb{Z})$ not equal to $\pm I$, $x \in \mathbb{C}$ is fixed by A if and only if $cx^2 + (d-a)x - b = 0$. The two solutions are complex conjugates and thus at most one solution is in $\mathbb{H}$. Therefore there is at most one point in $\mathbb{H}$ fixed by A.

Choose $z \in V, z \neq \pi_2(x_0)$. By the uniqueness of a fixed point in $\mathbb{H}$ for a given matrix in $\text{SL}_2(\mathbb{Z})$, when x_0 is not a cusp our choice of $\widetilde{V}$ guarantees that z is not an elliptic point or cusp. When x_0 is a cusp choosing k to be sufficiently large ensures that V_k contains no other cusps. Since $z \in V$, there is $x \in \widetilde{V}$ with $\pi_2(x) = z$.

It suffices to show that the map

$$\psi : \{\pm I\}\text{Stab}_{\Gamma_2}(x_0)/\{\pm I\}\text{Stab}_{\Gamma_1}(x_0) \longrightarrow f^{-1}(z) \cap U$$

defined by $[\gamma] \mapsto \pi_1(\gamma x)$ is a bijection.

First we will show the map is well-defined. Let $[\gamma] = [\gamma']$. So $\gamma = \alpha\gamma'$ for some $\alpha \in \{\pm I\}\text{Stab}_{\Gamma_1}(x_0)$. Therefore

$$\begin{aligned} \pi_1(\gamma x) &= \pi_1(\alpha\gamma' x) \\ &= \pi_1(\gamma' x) \qquad \text{since } \alpha \in \{\pm I\}\Gamma_1. \end{aligned}$$

Also $\gamma \in \{\pm I\}\text{Stab}_{\Gamma_2}(x_0)$ and $x \in \widetilde{V}$, so $\gamma x \in \widetilde{V}$. Therefore $\pi_1(\gamma x) \in U$. Additionally $\pi_2(x) = \pi_2(\gamma x)$ since $\gamma \in \Gamma_2$. By the commutative diagram we can see that $f(\pi_1(\gamma x)) = \pi_2(\gamma x) = z$, which proves that ψ is well-defined.

Next we will show that ψ is injective. Let $\pi_1(\gamma x) = \pi_1(\gamma' x)$ with $\gamma, \gamma' \in \{\pm I\}\text{Stab}_{\Gamma_2}(x_0)$. Then $\gamma x = \beta\gamma' x$ for some $\beta \in \Gamma_1$. Additionally we know that $\beta \in \{\pm I\}\text{Stab}_{\Gamma_1}(x_0)$ since γx and $\gamma' x$ are elements of $\widetilde{V}$. Additionally

$$\gamma^{-1}\beta\gamma' x = x$$

and x is not an elliptic point or cusp of Γ_2 so $\gamma^{-1}\beta\gamma' = \pm I$. Hence $\gamma^{-1}\beta\gamma' \in \{\pm I\}\text{Stab}_{\Gamma_1}(x_0)$ and by the properties of cosets, this proves that

$$\begin{aligned} [\gamma] &= [\beta\gamma'] \\ &= [\gamma'] \qquad \text{since } \beta \in \{\pm I\}\text{Stab}_{\Gamma_1}(x_0), \end{aligned}$$

which proves injectivity.

Last we will prove surjectivity. Let $w \in f^{-1}(z) \cap U$. Since $w \in U$, there exists $x' \in \widetilde{V}$ such that $\pi_1(x') = w$. Since $f(\pi_1(x')) = z$ and $\pi_2(x) = z$, there exists $\gamma \in \Gamma_2$ such that $x' = \gamma x$. Furthermore x' and x are in $\widetilde{V}$ so γ is in $\mathrm{Stab}_{\Gamma_2}(x_0)$. This proves that $\psi([\gamma]) = \pi_1(\gamma x) = w$. Therefore ψ is a bijection which proves the theorem.

□

For the function f as defined in Theorem 4.2, note that if $\pi_2(x)$ is not an elliptic point or a cusp then the stabilizer is trivial and so is not a ramification point.

4.1.2 Ramification degrees of elliptic points

We will now give the ramification degrees for elliptic points.

Proposition 4.3. Let $x \in \mathbb{H}^\star$. The ramification degree of $\Gamma_1 x$ with respect to function f is

$$\begin{cases} |\{\pm I\}\mathrm{Stab}_{\Gamma_2}(x)|/2 & \text{if } x \text{ is an elliptic point of } \Gamma_2 \text{ but not an elliptic point of } \Gamma_1 \\ 1 & \text{if } x \text{ is an elliptic point of both } \Gamma_1 \text{ and } \Gamma_2. \end{cases}$$

Proof. Let x be an elliptic point of Γ_2 but not an elliptic point of Γ_1. Recall that the order of the stabilizer of x is either 3,4 or 6. By Lemma 4.2, the ramification degree is

$$[\{\pm I\}\mathrm{Stab}_{\Gamma_2}(x) : \{\pm I\}\mathrm{Stab}_{\Gamma_1}(x)] = \frac{|\{\pm I\}\mathrm{Stab}_{\Gamma_2}(x)|}{|\{\pm I\}\mathrm{Stab}_{\Gamma_1}(x)|}.$$

Observe that x is not an elliptic point of Γ_1 so $|\{\pm I\}\mathrm{Stab}_{\Gamma_1}(x)| = 2$. Therefore the ramification degree of x equals $|\{\pm I\}\mathrm{Stab}_{\Gamma_2}(x)|/2$.

Let x be an elliptic point of both Γ_1 and Γ_2. We know that $|\{\pm I\}\mathrm{Stab}_{\Gamma_i}(x)| \in \{4, 6\}$ and the ramification degree is an integer so

$$\frac{|\{\pm I\}\mathrm{Stab}_{\Gamma_2}(x)|}{|\{\pm I\}\mathrm{Stab}_{\Gamma_1}(x)|} = 1.$$

Notice that if x is an elliptic point of Γ_1 but not an elliptic point of Γ_2 then $\frac{|\{\pm I\}\mathrm{Stab}_{\Gamma_2}(x)|}{|\{\pm I\}\mathrm{Stab}_{\Gamma_1}(x)|}$ is not an integer so this case is not possible.

□

4.1.3 Ramification degree of cusps

We will now give the ramification degrees for cusps. Notice that for the function f defined in the previous section that cusps are always mapped to cusps.

The stabilizer of ∞ in $\Gamma(1)$ is the group $\{\pm I\}\langle \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] \rangle$. Given $s \in \mathbb{Q}^\star \cup \{\infty\}$, choose $\delta \in \mathrm{SL}_2(\mathbb{Z})$ such that $\delta\infty = s$. Then $\delta^{-1}\mathrm{Stab}_\Gamma(s)\delta$ is a subgroup of finite index in $\mathrm{Stab}_{\Gamma(1)}(\infty)$. Therefore $\mathrm{Stab}_\Gamma(s) = \delta\{\pm I\} \left\langle \left[\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right] \right\rangle \delta^{-1}$ for some positive integer h.

Definition 4.4. The integer h defined above we call the *width* of s.

Let $s \in \mathbb{Q} \cup \{\infty\}$ and denote the widths of the cusp s under Γ_1 and Γ_2 as h_1 and h_2 respectively.

Proposition 4.5. The ramification degree of s with respect to the function f is h_1/h_2.

Proof. By Theorem 4.2 and the fact that index is invariant under conjugation, the ramification degree of s is

$$\left[\{\pm I\}\left\langle \left[\begin{smallmatrix}1 & h_2\\ 0 & 1\end{smallmatrix}\right]\right\rangle : \{\pm I\}\left\langle \left[\begin{smallmatrix}1 & h_1\\ 0 & 1\end{smallmatrix}\right]\right\rangle\right].$$

Since $\left\langle \left[\begin{smallmatrix}1 & h_1\\ 0 & 1\end{smallmatrix}\right]\right\rangle < \left\langle \left[\begin{smallmatrix}1 & h_2\\ 0 & 1\end{smallmatrix}\right]\right\rangle$, we have that $h_2\ell = h_1$ for some integer ℓ. Observe that $\left\langle \left[\begin{smallmatrix}1 & h_1\\ 0 & 1\end{smallmatrix}\right]\right\rangle = \left\langle \left[\begin{smallmatrix}1 & h_2\\ 0 & 1\end{smallmatrix}\right]^{\ell}\right\rangle$, and so the above index is h_1/h_2.

□

To compute the width of a cusp s let $\delta \in \mathrm{SL}_2(\mathbb{Z})$ with $\delta\infty = s$ and Γ a congruence subgroup of level N. It suffices to find the smallest h such that $\delta \left[\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right] \delta^{-1} \in \{\pm I\}\Gamma$. We will use the algorithm given in [Ste07].

1. Given $s = a/b$, find integers c, d such that $ad - bc = 1$ and let $\delta = \left[\begin{smallmatrix}a & c\\ b & d\end{smallmatrix}\right]$.
2. Compute the following matrix in terms of the variable x:
$$\Delta(x) = \delta \begin{bmatrix}1 & x\\ 0 & 1\end{bmatrix} \delta^{-1}.$$
3. Compute when $\Delta(x) \in \{\pm I\}\Gamma$ by reducing to congruence conditions on x. One uses enumeration to find the smallest positive value of x that simultaneously satisfies the congruence conditions.

The following gives the Sage code for implementing this algorithm:

```
def lift(a,b,N):
    """Lift a/b in (Z/NZ)^2 to Q^2."""
    if a==0 or b==0:
        if a==0:
            x=a+N
            y=b
        if b==0:
            y=b+N
            x=a
        return x,y
    if gcd(a,b)==1:
        return a,b
    if gcd(a,b)!=1:
        x =a +N
        y =b
        return x,y
```

```
def width(a,b,N,k):
    """Compute the width of a cusp a/b."""
    m,n = lift(a,b,N)
    x = var('x')
    d,u,v = xgcd(m,n)
    A = Matrix([[m,-v],[n,u]])
    B = Matrix([[1,x],[0,1]])
    Delta = A*B*(A^(-1))
    i=1
    if k==1: #width for Gamma_1(N)
        while true:
            D = Delta.substitute(x=i)
            if ((int(D[0,0])%N==1 and int(D[1,1])%N==1)
               ↪ or (int(D[0,0])%N==(-1%N) and int(D
               ↪ [1,1])%N==(-1%N)))  and int(D[1,0])%N
               ↪ ==0:
                return i
            else:
                i=i+1
    if k==0: #width for Gamma_0(N)
        while true:
            D = Delta.substitute(x=i)
            if int(D[1,0])%N==0:
                return i
            else:
                i=i+1
    if k==2: #width for Gamma(N)
        while true:
            D = Delta.substitute(x=i)
            if int(D[0,0])%N==1 and int(D[1,1])%N==1 and
               ↪ int(D[1,0])%N==0 and int(D[0,1])%N==0:
                return i
            else:
                i=i+1
```

4.2 Genera of modular curves

We will now give a method for computing the genera of the modular curves. Recall from Proposition 1.30 that every Riemann surface is homeomorphic to a sphere with g handles, where g is defined to be the genus of the Riemann surface. Also recall the Riemann-Hurwitz Formula.

Theorem 4.6 (Riemann-Hurwitz Formula)**.** *Let $f : X \to Y$ be a nonconstant map between connected, compact Riemann surfaces. Let g_X be the genus of X, g_Y the genus of Y, d the degree of f, and m_x be the ramification degree of $x \in X$. The following formula holds:*

$$2g_X - 2 = d(2g_Y - 2) + \sum_{x \in X}(m_x - 1).$$

By analyzing the fundamental domain of $X(1)$ given in Proposition 1.18, we can see that the genus of $X(1)$ is 0. Using this fact as well as the fact that $X(1)$ has one cusp and two elliptic points one can modify the Riemann-Hurwitz Formula to produce the following theorem.

Theorem 4.7. *Let Γ be a finite index subgroup of $\Gamma(1)$. Let $n = [\{\pm I\}\Gamma(1) : \{\pm I\}\Gamma]$, let c be the number of cusps of Γ, and for $i \in \{2, 3\}$, let ν_i be the number of elliptic points of period i. Then*

$$g(X(\Gamma)) = 1 + \frac{n}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{c}{2}$$

Proof. [DS05, Theorem 3.1.1] □

To use Theorem 4.7 we need to compute $[\{\pm I\}\Gamma(1) : \{\pm I\}\Gamma(N)]$, $[\{\pm I\}\Gamma(1) : \{\pm I\}\Gamma_1(N)]$ and $[\{\pm I\}\Gamma(1) : \{\pm I\}\Gamma_0(N)]$ as well as the number of cusps and elliptic points for $X(N), X_1(N)$ and $X_0(N)$.

We will give the indices but the derivation can be found in [Shi71, Page 22].

Theorem 4.8. *If $N \geq 3$, then*

$$[\{\pm I\}\Gamma(1) : \{\pm I\}\Gamma(N)] = (N^3/2)\prod_{p|N}(1 - p^{-2})$$
$$[\{\pm I\}\Gamma(1) : \{\pm I\}\Gamma_1(N)] = (N^2/2)\prod_{p|N}(1 - p^{-2})$$
$$[\{\pm I\}\Gamma(1) : \{\pm I\}\Gamma_0(N)] = N\prod_{p|N}(1 + p^{-1}).$$

The degrees for $N = 2$ are $3, 3$ and 6 respectively.

Proof. [Shi71, Page 22] □

Using Theorem 4.8 we give a table with the necessary indices.

N	$[\{\pm I\}\Gamma(1) : \{\pm I\}\Gamma(N)]$	$[\{\pm I\}\Gamma(1) : \{\pm I\}\Gamma_1(N)]$	$[\{\pm I\}\Gamma(1) : \{\pm I\}\Gamma_0(N)]$
2	6	3	3
3	12	4	4
4	24	6	6
5	60	12	6
6	72	12	12
7	168	24	8
8	192	24	12

We now would like to tabulate the number of cusps for the various modular curves. Recall that

$$\begin{aligned}
\#\text{ of cusps of } X(N) &= \frac{1}{2}\sum_{d|N}(N/d)\phi(d)\phi(N/d) \\
\#\text{ of cusps of } X_1(N) &= \frac{1}{2}\sum_{d|N}\phi(d)\phi(N/d) \\
\#\text{ of cusps of } X_0(N) &= \sum_{d|N}\phi(\gcd(d, N/d)).
\end{aligned}$$

The values for the number of cusps are given in the table below.

N	# of cusps of $X(N)$	# of cusps of $X_1(N)$	# of cusps of $X_0(N)$
2	3	2	2
3	4	2	2
4	6	3	3
5	12	4	2
6	12	4	4
7	24	6	2
8	24	6	4

We showed that $X(N)$ contains no elliptic points, and that $X_1(2)$ and $X_1(3)$ both contain one elliptic point. The number of elliptic points of $X_0(N)$ is given in the following theorem.

Theorem 4.9. *The number of elliptic points in $X_0(N)$ is*

$$v_2 = \begin{cases} 0 & \text{if } 4 \mid N \\ \prod_{p|N}\left(1 + \left(\frac{-1}{p}\right)\right) & \text{otherwise} \end{cases}$$

where $(-1/p)$ is ± 1 if $p \equiv \pm 1 \pmod 4$ and is 0 if $p = 2$, and

$$v_3 = \begin{cases} 0 & \text{if } 9 \mid N \\ \prod_{p|N}\left(1 + \left(\frac{-3}{p}\right)\right) & \text{otherwise} \end{cases}$$

where $(-3/p)$ is ± 1 if $p \equiv \pm 1 \pmod 3$ and is 0 if $p = 3$.

Proof. [Shi71, Proposition 1.43] □

The following table gives the number of elliptic points of $X_0(N)$ by the period of the elliptic point.

N	v_2 in $X_0(N)$	v_3 in $X_0(N)$
2	1	0
3	0	1
4	0	0
5	2	0
6	0	0
7	0	2
8	0	0

We have now compiled all the necessary inputs. Plugging these in to the formula

$$g(X(\Gamma)) = 1 + \frac{n}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{c}{2},$$

we can compute the genera of the modular curves $X(N), X_1(N)$ and $X_0(N)$ which are given in the following table.

N	$g(X(N))$	$g(X_0(N))$	$g(X_1(N))$
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	1	0	0
7	3	0	0

4.3 Cuspidal trees

4.3.1 Degree of a map between modular curves

Recall that the degree of a map $\varphi : X(\Gamma_1) \to X(\Gamma_2)$ defined by $\Gamma_1\tau \mapsto \Gamma_2\tau$ is given by

$$\deg(\varphi) = \begin{cases} [\Gamma_2 : \Gamma_1]/2 & \text{if } -I \in \Gamma_2 \text{ and } -I \notin \Gamma_1 \\ [\Gamma_2 : \Gamma_1] & \text{otherwise.} \end{cases}$$

Since $\Gamma(N) \subset \Gamma_1(N)$, $\Gamma_1(N) \subset \Gamma_0(N)$, and $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ we can define the maps

$$\begin{aligned} f &: X(N) \to X_1(N) \\ g &: X_1(N) \to X_0(N) \\ h &: X_0(N) \to X(1) \end{aligned}$$

where $\Gamma(N)\tau \mapsto \Gamma_1(N)\tau$, $\Gamma_1(N)\tau \mapsto \Gamma_0(N)\tau$, and $\Gamma_0(N)\tau \mapsto \mathrm{SL}_2(\mathbb{Z})\tau$ respectively. The degrees of these maps are given by

$$\begin{aligned} \deg(f) &= [\Gamma_1(N) : \Gamma(N)] = N \\ \deg(g) &= [\Gamma_0(N) : \Gamma_1(N)]/2 = (N/2)\prod_{p|N}(1 - p^{-1}) \\ \deg(h) &= [\Gamma(1) : \Gamma_0(N)] = N\prod_{p|N}(1 + p^{-1}). \end{aligned}$$

Explicit computation of the degrees are given in the following table.

N	$\deg(f)$	$\deg(g)$	$\deg(h)$
2	2	1	3
3	3	1	4
4	4	1	6
5	5	2	6
6	6	1	12
7	7	3	8
8	8	2	12

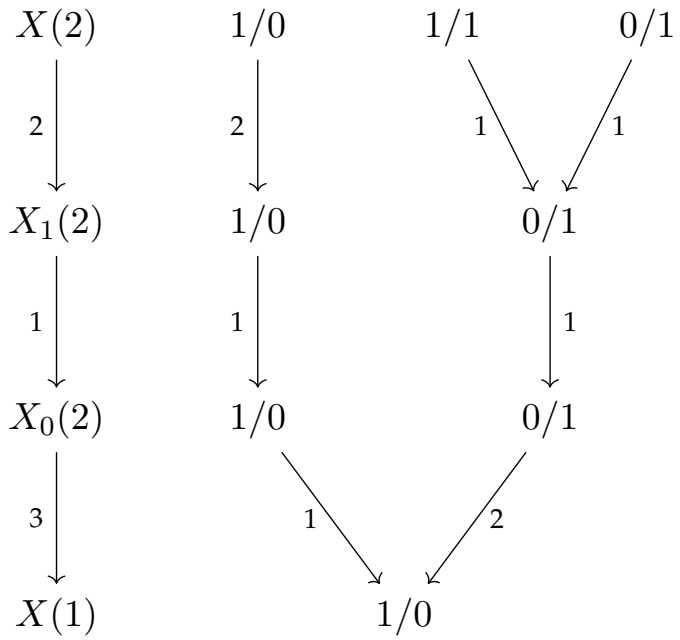
4.3.2 Cuspidal trees

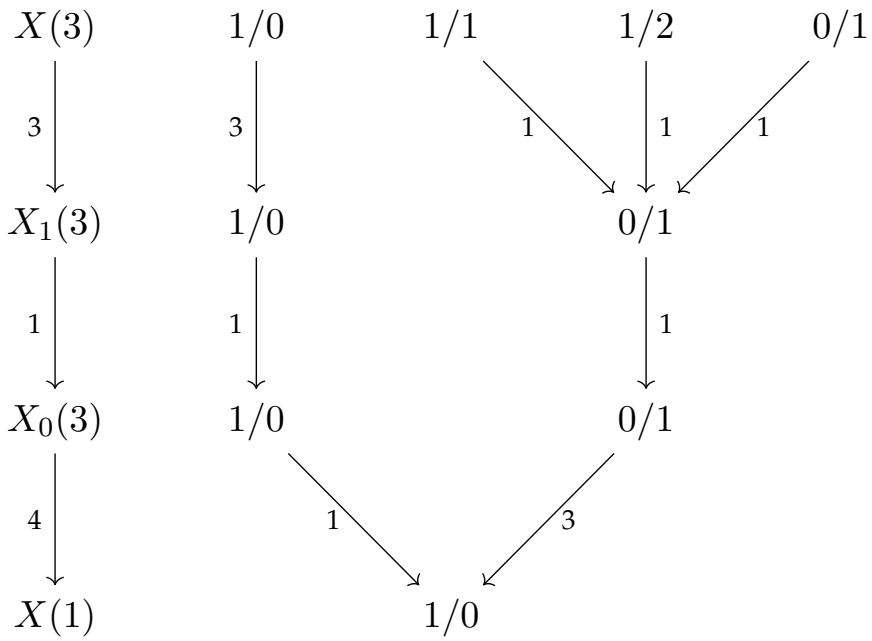
Definition 4.10. The *cuspidal tree* is the stratified weighted digraph where:

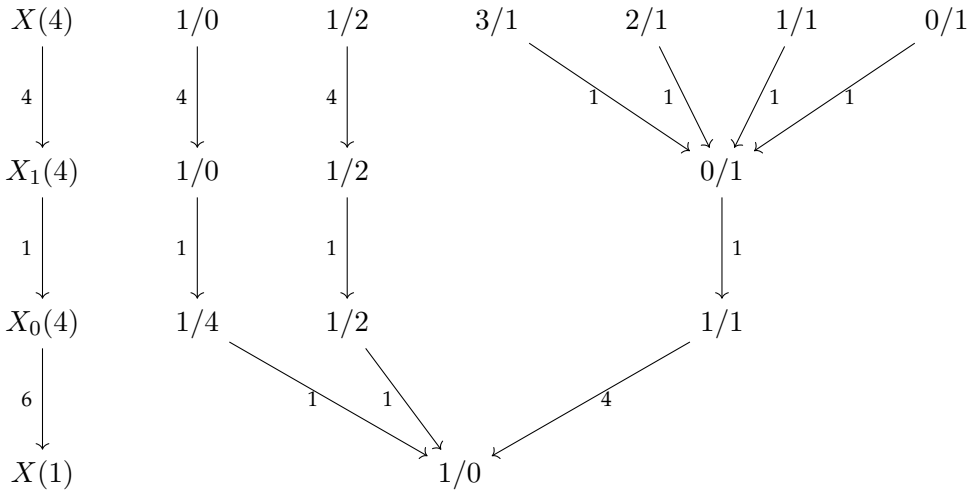
1. vertices are the set of all cusps of all modular curves,
2. there is an edge between two cusps if there exists a nontrivial map taking one cusp to another,
3. the weights of the edges are the ramification degrees, and
4. the stratification is the set of modular curves partially ordered by $X(\Gamma_1) > X(\Gamma_2)$ if $\Gamma_1 \subset \Gamma_2$.

Observe that in this graph if there is an edge between two vertices then these two vertices are in different strata.

The following are some subgraphs of the cuspidal tree. We place the subgraph on the right side with all the cusps in the same strata on the same level and on the left side we give the strata of the cusps as well as the degree of the map between the strata.







4.3.3 Sage code for creating cuspidal trees

We will now give the Sage code that was used to make the necessary computations for creating the cusp trees.

```
def cong1(a,b,c,d,N):
    """Return true if a/b is congruent to c/d in X(\
       ↪ Gamma_1(N))."""
    for i in [0..N-1]:
```

```
        if (a-(c+d*i)%N==0 and (b-d)%N==0) or ((a+(c+d*i)
           ↪ )%N==0 and (b+d)%N==0):
            return true
    return false

def inv(N):
    """Return list of integers relatively prime to N."""
    l=[]
    for i in [1..N-1]:
        if gcd(i,N)==1:
            l.append(i)
    return l

def inv1(x,N):
    """Return the inverse of x mod N."""
    for i in inv(N):
        if (x*i)%N==1:
            return i

def cong2(a,b,c,d,N):
    """Return true if a/b = c/d in X(\Gamma_0(N))."""
    for i in [0..N-1]:
        for j in inv(N):
            if (b*inv1(j,N) - d)%N==0 and (j*a + b*i-c)%N
               ↪ ==0:
                return true
     return false

def gammaN_gamma1N(N):
    """Return [a,b] -> [c,d] if Gamma(N)a/b is mapped to
       ↪ Gamma_1(N)c/d."""
    k = cusp(N)
    l = cusps1(N)
    for i in range(len(k)):
        for j in range(len(l)):
            if cong1(k[i][0],k[i][1],l[j][0],l[j][1],N)==
               ↪ true:
                w = width(k[i][0],k[i][1],N,2)/width(l[j
                   ↪ ][0],l[j][1],N,1)
                print str(k[i]) + "->" + str(l[j]) + "␣␣␣
                   ↪ ␣␣␣the␣ramification␣degree␣is␣" +
                   ↪ str(w)


def gamma1N_gamma0N(N):
    """Return [a,b] -> [c,d] if Gamma_1(N)a/b is mapped
       ↪ to Gamma_0(N)c/d."""
```

```
    k = cusps1(N)
    l = cusps0(N)
    for i in range(len(k)):
        for j in range(len(l)):
            if cong2(k[i][0],k[i][1],l[j][0],l[j][1],N)==
               ↪ true:
                w = width(k[i][0],k[i][1],N,1)/width(l[j
                   ↪ ][0],l[j][1],N,0)
                print str(k[i]) + "->" + str(l[j]) + "␣␣␣
                   ↪ ␣␣␣the␣ramification␣degree␣is␣" +
                   ↪ str(w)


def gamma0N_gamma1(N):
    """Return [a,b] -> [c,d] if Gamma_0(N)a/b is mapped
       ↪ to SL_2(Z)c/d."""
    l = cusps0(N)
    for i in range(len(l)):
        w = width(l[i][0],l[i][1],N,0)
        print  str(l[i])+ "->" + str([1,0]) + "␣␣␣␣␣the␣
           ↪ ramification␣degree␣is␣" + str(w)
```

Bibliography

[DS05] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Springer, New York, 2005.

[Mir95] R. Miranda. *Algebraic Curves and Riemann Surfaces*. Amer Mathematical Society, Providence, RI, 1995.

[Shi71] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Function*. Princeton University Press, New Jersey, 1971.

[Ste07] W. Stein. *Modular Forms, a Computational Approach*. American Mathematical Society, Providence, RI, 2007.