CONSTRUCTION AND ANALYSIS OF THE MODULAR CURVE $X_0(2)$

DYLAN T. COSTA

1. Construction of $Y_0(2)$

In this section, we will construct the modular curve $Y_0(2)$ as a Riemann surface over $\mathbb{C}$. Consider the following action of the group $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane $\mathbb{H}$: given a $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathbb{H}$,

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

We define $Y(1)$ as the quotient of the upper half plane modulo the equivalence relation imposed by the above group action. That is,

$$Y(1) = \mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$$

which is a Riemann surface but not compact. Consider the congruence subgroup

$$\Gamma_0(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \bmod 2 \right\}.$$

We define $Y_0(2)$ as the further quotient

$$Y_0(2) = \mathbb{H}/\Gamma_0(2)$$

which, once again, is a Riemann surface but not compact.

2. Finding Fundamental Domain

The fundamental domain of this surface can be found using the fundamental domain for $Y(1)$. If we let $\mathcal{F}$ be the fundamental domain of $Y(1)$. That is,

$$\mathcal{F} = \left\{ \tau \in \mathbb{H} : |\mathrm{Re}(\tau)| < \frac{1}{2} \right\} \cap \{\tau \in \mathbb{H} : |\tau| \geq 1\}.$$

Finding coset representatives for $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(2)$ will show what points in $\mathbb{H}$ are no longer equivalent (since we are considering the action of a proper subgroup of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$.) The matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, generate $\mathrm{SL}_2(\mathbb{Z})$. So a possible list of coset representatives for the quotient $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(2)$ are

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \right\}.$$

The fundamental domain should be the action of these three coset representatives on $\mathcal{F}$. Put explicitly, the set

$$D = \mathcal{F} \cup S(\mathcal{F}) \cup (ST)(\mathcal{F})$$

is the fundamental domain for $\Gamma_0(2)$. For some intuition behind this, notice that $T \in \Gamma_0(2)$, so any point $\tau \in \mathbb{H}$ can be shift to a point in $\mathbb{H}$ with $|\mathrm{Re}(\tau)| \leq \frac{1}{2}$.

3. Construction of $X_0(2)$ (redo)

To compactify the modular curve $Y_0(2) = \mathbb{H}/\Gamma_0(2)$, we let $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ and define the extended quotient

$$X_0(2) = \mathbb{H}^*/\Gamma_0(2).$$

Now we want to show that this extended quotient is a compact Riemann surface. To do this, we will need to find the cusps of $X_0(2)$. These correspond to all the $\Gamma_0(2)$-equivalence classes of $\mathbb{Q} \cup \{\infty\}$. We can generalize the definition above to primes p as

$$X_0(p) = \mathbb{H}^*/\Gamma_0(p).$$

Proposition 3.1. *Let p be a prime. The modular curve $X_0(p)$ has only two cusps.*

Proof. As previously stated, the cusps on the modular curve $X_0(p)$ correspond to $\Gamma_0(p)$-equivalence classes of $\mathbb{Q} \cup \{\infty\}$. To show that $X_0(p)$ has at least two cusps, we will show that 0 and ∞ can not be in the same equivalence class as each other. Given a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. This matrix acts on the point ∞ as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (\infty) = \frac{a}{c}.$$

If ∞ was in the same $\Gamma_0(p)$-equivalence class as 0 then we would need a matrix with $a = 0$. But this is an immediate contradiction. If $a = 0$ then $c \neq 0$. Moreover, for the determinant of such a matrix to be 1, we would need $c \in \{\pm 1\}$. It follows that such a matrix can never be in the group $\Gamma_0(p)$, which proves the claim. So $X_0(p)$ has at least two cusps, but we want to show there are no more extra cusps. To prove this, we need to show that every rational number is equivalent to 0 or ∞ under the action of $\Gamma_0(p)$.

Note that the matrix $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \Gamma_0(p)$ for all primes p. This sends an element τ to $\tau + n$. It suffices to consider rational number between 0 and 1 in reduced form (that is, $\frac{m}{n}$ where $(m, n) = 1$.) Suppose p divides m. Then p does not divide n and there exists $x, y \in \mathbb{Z}$ such that $pmx + ny = 1$. Consider the matrix $\begin{pmatrix} n & -m \\ px & y \end{pmatrix} \in \Gamma_0(p)$. Then

$$\begin{aligned} \begin{pmatrix} n & -m \\ px & y \end{pmatrix} \left(\frac{m}{n}\right) &= \frac{n\frac{m}{n} - m}{px\frac{m}{n} + y} \\ &= \frac{m - m}{px\frac{m}{n} + y} \\ &= \frac{mn - mn}{pxm + ny} \\ &= 0. \end{aligned}$$

Suppose instead, p divides n meaning p does not divide m. Once again there are $x, y \in \mathbb{Z}$ such that $-mx - ny = 1$. We can take the matrix $\begin{pmatrix} x & y \\ n & -m \end{pmatrix} \in \Gamma_0(p)$ and see

$$\begin{aligned}\begin{pmatrix} x & y \\ n & -m \end{pmatrix}\left(\frac{m}{n}\right) &= \frac{x\frac{m}{n} + y}{n\frac{m}{n} - m} \\ &= \frac{mx + ny}{mn - mn} \\ &= \frac{-1}{0} = \infty.\end{aligned}$$

The final case to consider is when p does not divide m or n. Then there exists $x, y \in \mathbb{Z}$ such that $pmx + ny = 1$. Consider the matrix $\begin{pmatrix} n & -m \\ px & y \end{pmatrix} \in \Gamma_0(p)$. We use the same calculation as in the first case to conclude

$$\begin{pmatrix} n & -m \\ px & y \end{pmatrix}\left(\frac{m}{n}\right) = 0.$$

So all rational number are $\Gamma_0(p)$ equivalent to either 0 or ∞. Thus, the modular curve $X_0(p)$ has exactly two cusps for all primes p. $\square$

This modular curve is a compact Riemann surface that parameterizes elliptic curves having a 2-isogeny. How do we arrive at such a claim? Consider the usual topology on $\mathbb{H}$. Since these curves are defined as a quotient of $\mathbb{H}^*$, we want a nice way to extend the topology on $\mathbb{H}$. Define the neighborhood

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

for any $M > 0$. Now adjoin the usual open sets in $\mathbb{H}$ with the sets

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

to be the neighborhoods of the cusps. We let this be the topology of $\mathbb{H}$. Note that under this topology, each element in $\mathrm{SL}_2(\mathbb{Z})$ acts as a homeomorphism of $\mathbb{H}^*$. We give $X_0(2)$ the quotient topology. Now we want to show that $X_0(2)$ is compact. To do this, we will prove the following lemma:

Lemma 3.2. *The set $\mathcal{F}^* = \mathcal{F} \cup \{\infty\}$ is compact in the $\mathbb{H}^*$ topology.*

Proof. Take an open cover $\{U_\alpha\}$ of $\mathcal{F}^*$. For some α_∞, the set U_{α_∞} contains ∞. Notice that U_{α_∞} must be some $\mathcal{N}_M$ for $M > 0$. The area remaining is the set

$$\{\tau \in \mathcal{F} : \operatorname{Im}(\tau) \leq M\}$$

which is a compact set covered by $\bigcup_{\alpha \neq \alpha_\infty}\{U_\alpha\}$. Since this resulting set is compact, there is a finite subcover $\{V_i\}_{i=1}^N$. Letting $V_0 = U_{\alpha_\infty}$, the finite collection of open sets $\{V_i\}_{i=1}^N$ is a finite subcover of $\mathcal{F}^*$ demonstrating compactness of $\mathcal{F}^*$ in the $\mathbb{H}^*$ topology. $\square$

Proposition 3.3. *The modular curve $X_0(2)$ is compact.*

Proof. By 3.2, we know $\mathcal{F}^*$ is compact in the $\mathbb{H}^*$ topology. Moreover,

$$\mathbb{H}^* = \mathrm{SL}_2(\mathbb{Z})(\mathcal{F}^*).$$

We computed earlier, $\Gamma_0(2)$ is an index 3 subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Let $\{\gamma_i\}_{i=1}^3$ be the collection of coset representatives computed previously, then

$$\begin{aligned}\mathbb{H}^* &= \mathrm{SL}_2(\mathbb{Z})(\mathcal{F}^*)\\ &= \bigcup_{i=1}^{3} \Gamma_0(2)\gamma_i(\mathcal{F}^*).\end{aligned}$$

Then $X_0(2) = \pi(\mathbb{H}^*) = \bigcup_{i=1}^3 \pi(\gamma_i(\mathcal{F}^*))$ where π is the quotient map. Note that π is continuous and every γ_i is continuous and there are only finitely many γ_i to consider since $\Gamma_0(2)$ is a finite index subgroup. The continuous image of a compact set is compact which completes the proof. □

More generally, one can show that the more general quotient $X_0(N) = \mathbb{H}^*/\Gamma_0(N)$ is a connected, compact, Hausdorff Riemann surface for all $N \in \mathbb{Z}$ (see [1].) If we want to know the genus of $X_0(2)$, we use the following theorem:

Theorem 3.4 ([1], 3.1.1)**.** *Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Let $f : X(\Gamma) \to X(1)$ be the natural projection, and let d denote its degree. Let ϵ_2 and ϵ_3 denote the number of elliptic points of period 2 and 3 in $X(\Gamma)$, and ϵ_∞ the number of cusps of $X(\Gamma)$. Then the genus of $X(\Gamma)$ is*

$$g = 1 + \frac{d}{12} - \frac{\epsilon_2}{4} - \frac{\epsilon_3}{3} - \frac{\epsilon_\infty}{2}.$$

For the curve $X_0(2)$, there are 2 cusps, 1 elliptic point of period 2 and $d = 3$. So the genus of $X_0(2)$ is 0. Since we have two points on the surface (those being the cusps), it must be isomorphic to $\mathbb{P}^1$. In the next section, we will show that $X_0(2)$ can be visualized as a curve over $\mathbb{P}^1(\mathbb{Q})$

4. Analysis of Rational Points on $X_0(2)$

In this section, we will find a model for $X_0(2)$ and see what possible j-invariants correspond to elliptic curves with a 2-isogeny. For this, we will look into the function field $\mathbb{C}(X_0(N))$.

Proposition 4.1 ([1], 7.5.1)**.** *The fields of meromorphic functions on $X_0(N)$ are $\mathbb{C}(j, j_N)$. Where $j_N(\tau) = j(N\tau)$.*

To find a model for $X_0(2)$ we will look into the function field at the relationship between j and j_N. This relationship is given by the modular polynomial.

Definition 4.2 ([3])**.** *The modular polynomial Φ_N is the minimal polynomial of j_N over $\mathbb{C}(j) = \mathbb{C}(X(1))$. We may write it as*

$$\Phi_N(Y) = \prod_{i=1}^{r} (Y - j_N(\gamma_i \tau))$$

where $\{\gamma_1, \ldots, \gamma_r\}$ is a set of right coset representatives for $\Gamma_0(N)$ in $\Gamma_0(1)$.

Letting $X = j_2, Y = j$, the modular polynomial for $\Gamma_0(2)$ is

$$\Phi_2(X, Y) = X^3 + 48X^2 - XY + 768X + 4096.$$

This means the function field $\mathbb{C}(X_0(2))$ can be seen as the quotient

$$\mathbb{C}(X_0(2)) = \mathbb{C}(j, j_2) \cong \mathbb{C}[X, Y]/\Phi(X, Y).$$

Rational points (X, Y) that are solutions to $\Phi_2(X, Y) = 0$ correspond to the j-invariant of elliptic curves that have a 2-isogeny defined over $\mathbb{Q}$. We solve for Y in the above equation

$$Y = \frac{X^3 + 48X^2 + 768X + 4096}{X}$$

which is a rational map to $\mathbb{P}^1$ with a simple pole at $X = 0$. For any $X \neq 0$, the corresponding Y value is a possible j-invariant. For example, the point $(-6, -500/3)$ is a point on $\Phi_2(X, Y) = 0$. One possible elliptic curve E with $j(E) = -500/3$ is

$$E : y^2 = x^3 - x^2 - 48x - 420$$

with $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z}$ and LMFDB label 20184.f2 ([2]). The torsion subgroup of E is generated by the point $(10, 0)$. Since E has a 2-torsion point defined over $\mathbb{Q}$, it necessarily also has a 2 -isogeny defined over $\mathbb{Q}$. Let E' with LMFDB label 20184.f1 have model

$$E' : y^2 = x^3 - x^2 - 1208x - 15732.$$

Then there exists an isogeny $\phi : E \to E'$ of degree 2 given by the map

$$\phi(x, y) = \left(\frac{x^2 + 9x + 42}{x - 10}, \frac{x^2y - 20xy - 132y}{x^2 - 20x + 100} \right).$$

In general, the curve $X_0(2)$ is the same as the curve $X_1(2)$ since every elliptic curve defined over a number field K has a 2-isogeny defined over K if and only if it has a point of order 2 defined over K.

References

[1] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005. 3, 3.4, 4.1

[2] The LMFDB Collaboration. The L-functions and modular forms database. `https://www.lmfdb.org`, 2023. [Online; accessed 24 July 2023]. 4

[3] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. 4.2