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

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

Using Magma ([1]), we find the generators of the group $\Gamma_0(2)$ are $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}$. We define $Y_0(2)$ as the further quotient

$$Y_0(2) = Y(1)/\Gamma_0(2)$$

which, once again, is a Riemann surface but not compact. The fundamental domain of this surface is the set

$$D = \{\tau \in \mathbb{H} : 0 \leq \mathrm{Re}(\tau) \leq 1\}$$

which was also computed using Magma. For some intuition behind this, notice that for any $\tau \in \mathbb{H}$, we have

$$S(\tau) = \tau + 1.$$

Moreover, it can be shown that $S^n = \tau + n$ in general for all $n \in \mathbb{Z}$. Thus, any $\tau \in \mathbb{H}$ can be translated into the region D using integer powers of S.

2. Construction of $X_0(2)$

To construct $X_0(2)$ from $Y_0(2)$ we will need to add cusps and make $Y_0(2)$ into a compact Riemann surface. Consider

$$\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}.$$

We need to find the equivalence classes of rational numbers under the action of $\Gamma_0(2)$. By using the fundamental domain, it suffices to check rational numbers $\frac{m}{n}$ with $(m, n) = 1$ such that $0 \leq \frac{m}{n} \leq 1$ and ∞.

Proposition 2.1. *There are only two cusps on the modular curve $X_0(2)$. Those cusps are at 0 and ∞.*

Proof. To prove this claim, we need to show

(1) For any rational number $r = \frac{m}{n}$ in the fundamental domain D of $Y_0(2)$, there exists a $\gamma \in \Gamma_0(2)$ such that either $\gamma(r) = 0$ or $\gamma(r) = \infty$ and
(2) There is no $\gamma \in \Gamma_0(2)$ such that $\gamma(0) = \infty$.

To begin, note that 0 and 1 are equivalent via the matrix transformation

$$S(0) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}(0) = 0 + 1 = 1.$$

We want to show every other rational number $\frac{m}{n} \in D$ in reduced form is in the same equivalence class as 0 under the action of $\Gamma_0(2)$. If $\frac{m}{n}$ is in reduced form, $(m, n) = 1$ and we separate into two cases: when m is even and m is odd.

If m is even, there exists integers x and y such that $2mx+ny = 1$ consider the matrix $\begin{pmatrix} n & -m \\ 2x & y \end{pmatrix}$. The determinant is 1 and

$$\begin{pmatrix} n & -m \\ 2x & y \end{pmatrix}\left(\frac{m}{n}\right) = \frac{n\left(\frac{m}{n}\right) - m}{2x(\frac{m}{n}) + y} = \frac{mn - mn}{2mx + yn} = 0.$$

If m is odd then n can be even or odd. If n is also odd, then

$$S\left(\frac{m}{n}\right) = \frac{m}{n} + 1 = \frac{m+n}{n}.$$

In this case, $m + n$ is even, n is odd, and $(m + n, n) = 1$. This goes back to the case above. If n is even, then there exist integers x and y such that $mx - ny = 1$. So

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

Since n is even, this transformation matrix is in $\Gamma_0(2)$. Now to prove condition (2), suppose a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(2)$ sends 0 to ∞. Then,

$$\frac{a(0) + b}{c(0) + d} = \frac{b}{d} = \infty.$$

Therefore, the only possibility is when $b \in \{\pm 1\}$ and $d = 0$. Either option forces $c \in \{\pm 1\}$ so that $ac - bd = 1$. We get an immediate contradiction since $1 \not\equiv 0 \bmod 2$. We conclude that 0 and ∞ are not equivalent under the action of $\Gamma_0(2)$. □

We let $\mathcal{C} = \{0, \infty\}$ be the set of cusps and define

$$X_0(2) = Y_0(2) \cup \mathcal{C}$$

as the compact Riemann surface that parameterizes elliptic curves with a 2-isogeny. If we want to know the genus of $X_0(2)$, we use the following theorem:

Theorem 2.2 ([2], 3.1.1)**.** *Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Let $f : X(\Gamma) \to X(1)$ be 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*

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

Using Magma, for $X_0(2)$ we know there are 2 cusps, and 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 $\mathbb{P}^1$. Thus, we know there are infinitely many elliptic curves over $\mathbb{Q}$ with a 2-isogeny. Now we will look at a model for $X_0(2)$ defined over $\mathbb{Q}$.

3. 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 3.1 ([2], 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 3.2 ([4])**.** *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*

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

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

A set of coset representatives of $\Gamma(1)/\Gamma_0(2)$ is

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

Letting $X = j_2, Y = j$, Magma computes the modular polynomial as

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

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 $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}$ and LMFDB label 20184.f2 ([3]). 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

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

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] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). 1

[2] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005. 2.2, 3.1

[3] The LMFDB Collaboration. The L-functions and modular forms database. `https://www.lmfdb.org`, 2023. [Online; accessed 24 July 2023]. 3

[4] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. 3.2