Modular Curves

Travis Scholl

February 11 2014

1 Moduli Problems

A *moduli problem* is basically a way to parametrize a family of geometric objects to study some properties. We will be interested in *moduli spaces* which we will use for the parametrization.

Example 1.1. Consider the set of lines through the origin in $\mathbb{R}^2$. Each is of the form $ax + by = 0$ for some $a, b \in \mathbb{R}$. Moreover, two lines agree if and only if their coefficients are a multiple of each other. This means there is a bijection between lines through the origin in $\mathbb{R}^2$ and $\mathbb{P}^1(\mathbb{R})$.

Moreover, this is a nice parameterization because lines through the origin in $\mathbb{Q}^2$ are parametrized by $\mathbb{P}^1(\mathbb{Q})$ which can be thought of as the rational points on $\mathbb{P}^1(\mathbb{R})$. So there is a natural map from lines in $\mathbb{Q}^2$ to lines in $\mathbb{R}^2$ which corresponds with the map $\mathbb{P}^1(\mathbb{Q}) \to \mathbb{P}^1(\mathbb{R})$.

Preview of whats to come: imagine a functor from ***Fields*** to ***Set*** by taking a field k to all lines through the origin in A^2_k. What we said above is similar to saying this functor is represented by $\mathbb{P}^1_k$.

2 Elliptic Curves as Lattices

This section can be summarized by the following.

Theorem 2.1. *There is an equivalence of categories between compact Riemann surfaces, function fields, and irreducible algebraic curves.*

Proof. For compact Riemann surfaces to function fields see [GGD12, Chapter 1 Section 3 Proposition 1.95]. The hardest part is showing there exist non-constant meromorphic functions on a arbitrary compact Riemann surface. For function fields and algebraic curves see [Har77, Chapter 1 Section 6 Corollary 6.12] □

Note 2.2. Here an algebraic curve is a nonsingular projective variety of dimension 1 over $\mathbb{C}$ with dominant morphisms. Basically we need to remove trivial maps in each category.

We will specialize to subcategories of complex tori and elliptic curves.

2.1 Objects

Recall the identification of complex elliptic curves $E/\mathbb{C}$ with complex tori $\mathbb{C}/\Lambda$ for a lattice $\Lambda \subseteq \mathbb{C}$. For example see [Mil06, Chapter III Section 3] or [DS07, Chapter 1 Section 4].

The main points are summarized here.

- Given a lattice (free $\mathbb{Z}$-submodule of rank 2) $\Lambda \subseteq \mathbb{C}$, the field of meromorphic functions on $\mathbb{C}/\Lambda$ is $\mathbb{C}(\wp, \wp')$ where $\wp$ is the Weierstrass $\wp$-function for Λ given by $z \mapsto \sum_{\lambda \in L \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right) + \frac{1}{z^2}$.

- The Wierstrass $\wp$-function satisfies
$$\left(\frac{1}{2}\wp'_\Lambda\right)^2 = \wp^3 + a\wp + b$$
where $a = -15\sum_{\lambda\in L\setminus\{0\}} \frac{1}{\lambda^4}$ and $b = -35\sum_{\lambda\in L\setminus\{0\}} \frac{1}{\lambda^6}$.
- The cubic equation $y^2 = x^3 + ax + b$ (with a,b as above) is non-singular and thus defines a complex elliptic curve E_Λ.
- There is a map $\varphi : \mathbb{C}/\Lambda \to E_\Lambda$ given by $z + \Lambda \mapsto \big(\wp(z), \frac{1}{2}\wp'(z)\big)$. This is an isomorphism as compact Riemann surfaces, nonsingular projective curves (note they have the same function fields), and also as algebraic groups. The last one can be shown by writing out $\wp(z_1 + z_2)$ as a rational function in $\wp, \wp'$ applied to z_1, z_2, then show $z_1 + z_2 + z_3 \in \Lambda \Rightarrow \varphi(z_1), \varphi(z_2), \varphi(z_3)$ are colinear.

This shows every lattice corresponds to a complex elliptic curve. One can show this process is surjective [see just about any reference, including [DS07]], i.e. every elliptic curve corresponds to an elliptic curve given by some (non-unique!) lattice.

2.2 Morphisms

First we need to know what the morphisms of Tori look like.

Theorem 2.3. *Suppose $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ is a meromorphic function sending $0 \mapsto 0$. Then φ is induced by the map $z \mapsto mz$ for some $m \in \mathbb{C}$ such that $m\Lambda \subseteq \Lambda'$. In particular, such a map is an isomorphism if and only if $m\Lambda = \Lambda'$.*

Proof. (See [DS07, Chapter 1 Section 3] or Ralph's notes)

Consider the following diagram.

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\psi} & \mathbb{C} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi'} \\ \mathbb{C}/\Lambda & \xrightarrow{\varphi} & \mathbb{C}/\Lambda' \end{array}$$

The map ψ comes from lifting the map $\varphi \circ \pi$ which is possible as $\mathbb{C}$ is the universal covering space of $\mathbb{C}/\Lambda'$. We can choose ψ such that $\psi(0) = 0$ by the hypothesis on φ. Now ψ is a priori continuous, but we can show it is analytic by noting that π, π' are locally conformal.

Fix some $\lambda \in \Lambda$ and consider the map $f(z) = \psi(z + \lambda) - \psi(z)$. Clearly this is an entire analytic function on $\mathbb{C}$ and moreover
$$\begin{aligned} (\pi' \circ f)(z) &= \pi' \circ \psi(z + \lambda) - \pi' \circ \psi(z) \\ &= \varphi \circ \pi(z + \lambda) - \varphi \circ \pi(z) \\ &= 0 \end{aligned}$$
Hence $\operatorname{Im} f \subseteq \Lambda'$. Since this is a discrete set f is constant and therefore
$$f'(z) = 0 \Rightarrow \psi'(z + \lambda) = \psi'(z).$$
In particular this shows ψ' is Λ-periodic hence bounded. But ψ' is an entire analytic function, so by Louivilles Theorem $\psi' = m$ for some $m \in \mathbb{C}$. Because we constructed ψ so that $0 \mapsto 0$, so $\psi(z) = mz$.

From the commutativity of the diagram we have $\psi(\Lambda) = m\Lambda \subseteq \Lambda'$. □

Note 2.4. Dropping the requirement on 0 will mean analytic maps are of the form $mz + b$. These are *homotheties*. What this means though, is that any map of Tori which fixes 0 is automatically a group homomorphism. This carries over to Elliptic curves as well!

In summary we now have a concrete space of elliptic curves to work with.

Theorem 2.5. *Let $\mathcal{L}$ be the space of lattices. Then the map $\Lambda \mapsto \mathbb{C}/\Lambda$ induces a bijection $\mathcal{L}/\mathbb{C}^* \to \{\mathbb{C}/\Lambda\}/\approx$ where $\approx$ is complex isomorphism of Tori.*

Because of our equivalence of categories this means

Theorem 2.6. *$\mathbb{C}/\Lambda_1 \cong \mathbb{C}/\Lambda_2$ if and only if $E_{\Lambda_1} \cong E_{\Lambda_2}$. Moreover, all the relevant structure (e.g. group structure) is preserved as well.*

3 Preliminaries

There is a left action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane $\mathbb{H}$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$

Define

$$\Gamma(1) := \mathrm{SL}_2(\mathbb{Z})$$

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

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \mod N, a \equiv d \equiv 1 \mod N \right\}.$$

we will see exactly why we these restrictions are exactly what we need.

Now define quotients $Y(1), Y_0(N), Y_1(N)$ as $\Gamma(1)\backslash\mathbb{H}, \Gamma_0(N)\backslash\mathbb{H}, \Gamma_1(N)\backslash\mathbb{H}$. Since the action is nice (besides a few odd points), these are complex manifolds. However, they are not compact.

Define $X(1), X_0(N), X_1(N)$ in the same way using the *extended upper half plane* $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ instead of $\mathbb{H}$. These spaces are compact, and usually referred to as the compactifications of the Y spaces. The equivalence classes of $\mathbb{Q} \cup \{\infty\}$ are called *cusps*. It is not hard to show the X spaces have finitely many cusps. It will follow from a few facts such as the natural map $X_0(N) \to X(1)$, $X(1)$ has one cusp, and $[\mathrm{SL}_2(\mathbb{Z}) \colon \Gamma_0(N)]$ is finite.

Note 3.1. Some people study much more general spaces by using more general subgroups $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$.

Note 3.2. Points in $\mathbb{H}^*$ with non-trivial isotropy subgroup are called *elliptic points*. It turns out elliptic points always have finite cyclic isotropy subgroups. Note $i, \rho = e^{2\pi i/3}$ are the only elliptic points in $Y_1(1)$. In general, there is only a finite number of elliptic points and they are only possibly in the preimage of i, ρ under $X \to X_0(1)$ for any of the X spaces.

One can show all the X spaces are compact Riemann surfaces. The charts are obvious except for at cusps and elliptic points, here you use various power maps. Also the topology is similar to the standard ones except at cusps. A base is given by the circles (Euclidean) tangent to $\mathbb{R}$. This is equivalent to taking the usual topology on $\mathbb{H} \cup \{\infty\}$ and then applying $\mathrm{SL}_2(\mathbb{Z})$ to all the open subsets to get open subsets of $\mathbb{Q}$ points.

It's fun to draw pictures of the *fundamental domain* of these regions. For example the following sage code produces the fundamental domains shown in Figure 1.

```
X0_1 = FareySymbol(Gamma0(1)).fundamental_domain(tesselation=None,show_pairing=True)
X0_3 = FareySymbol(Gamma0(3)).fundamental_domain(tesselation=None,show_pairing=True)
X0_11 = FareySymbol(Gamma0(11)).fundamental_domain(tesselation=None,show_pairing=True)
X0_23 = FareySymbol(Gamma0(23)).fundamental_domain(tesselation=None,show_pairing=True)
```

4 $X(1)$

Let Λ be a lattice and choose a basis $\langle \omega_1, \omega_2 \rangle$. Up to scaling and obvious changes, we can normalize the basis to $\langle \tau, 1 \rangle$ with $\tau = \frac{\omega_1}{\omega_2} \in \mathbb{H}$. We denote Λ_τ as the lattice given by $\langle \tau, 1 \rangle$. However, τ is not unique (for example $\Lambda_{\tau+1} = \Lambda_\tau$ would give the same lattice). It isn't too hard to figure out exactly how to fix the uniqueness.

Theorem 4.1. *$\Lambda_\tau \approx \Lambda_{\tau'}$ if and only if $\tau' = \gamma(\tau)$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. In which case, $(c\tau+d)\Lambda_{\tau'} = \Lambda_\tau$.*

Proof.

($\Leftarrow$): Note γ applied to the basis $\{\tau, 1\}$ gives $\{a\tau + b, c\tau + d\}$. Because $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ we have $\langle \tau, 1 \rangle = \langle a\tau + b, c\tau + d \rangle$. Note the ratio of the second basis is $\frac{a\tau+b}{c\tau+d} = \gamma(\tau) = \tau'$. Hence

$$\Lambda_{\tau'} = \langle \tau', 1 \rangle \approx (c\tau + d) \langle \tau', 1 \rangle = \langle a\tau + b, c\tau + d \rangle = \langle \tau, 1 \rangle = \Lambda_\tau.$$

($\Rightarrow$): If $\Lambda_\tau \approx \Lambda_{\tau'}$ then we can find a number m such that $m\Lambda_{\tau'} = \Lambda_\tau$. Then there is a change of basis $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ taking $\langle \tau, 1 \rangle$ to $\langle m\tau', m \rangle$ (possibly normalizing so determinate is positive). Taking the ratios of the basis gives $\gamma(\tau) = \tau'$.

□

This means we have a bijection between $Y(1)$ and $\mathcal{L}/\mathbb{C}^*$. Combining this result with above, we have the following.

Theorem 4.2. *There is a bijection between points on $Y(1)$ and isomorphism classes of elliptic curves.*

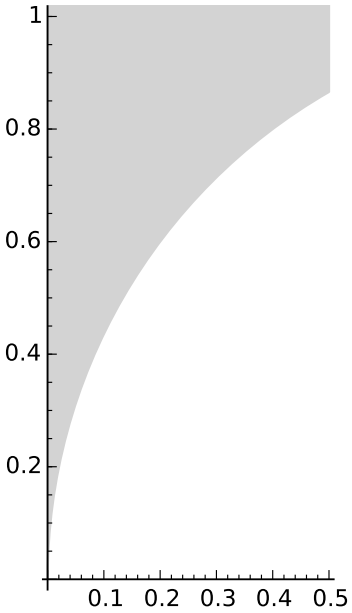
Corollary 4.3. *There is a bijection between the non-cusps of $X(1)$ and isomorphism classes of elliptic curves over $\mathbb{C}$.*

So $X(1)$ is a compact Riemann surface, and hence isomorphic to a projective curve over $\mathbb{C}$. Most of the points correspond to elliptic curves so it looks like a great candidate for a moduli space. The next obvious question is what curve is $X(1)$?

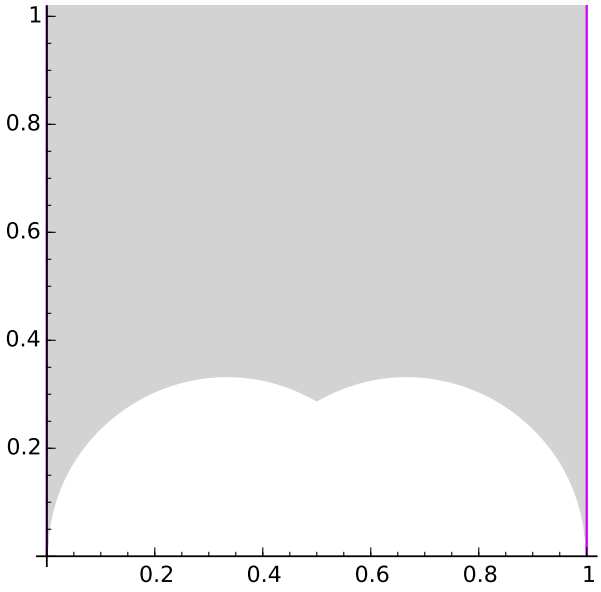
4.1 As a Curve

From the standard fundamental domain, seen in Figure 1a, it's easy to see there are 3 distinct vertices, 2 edges, and 1 face defining the surface $X(1)$. In the picture in, keep in mind the segment on the imaginary axis in and out of the circle are different. Hence it has genus 0 and therefore is conformally equivalent to the Riemann sphere, or $\mathbb{P}^1(\mathbb{C})$.

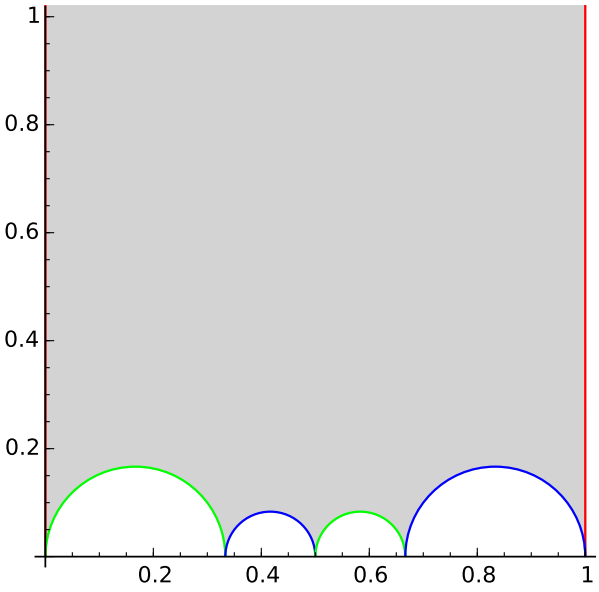
Note 4.4. In general it is possible to compute the genus of $X_0(N)$ by studying the degree of the obvious map $X_0(N) \to X(1)$. It turns out ramification can only happen at i, ρ, or ∞ (i.e. elliptic points and cusps). In [Mil06, Chapter 5 Section 2], Milne references explicit formulas.



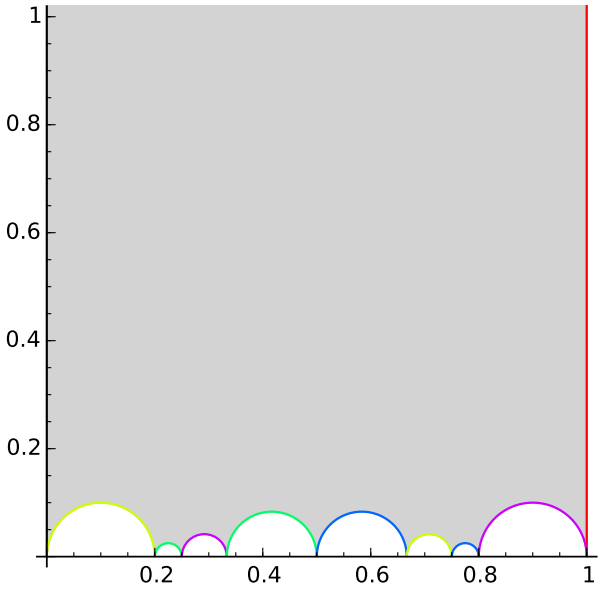
(a) $X_0(1)$



(b) $X_0(3)$



(c) $X_0(11)$



(d) $X_0(23)$

Figure 1: Fundamental Domains

4.2 As a Field

Recall the j-invariant. It can be defined in several ways, but most importantly recall it is a holomorphic function on the upper half plane with a simple pole at ∞ (normalized to have residue 1) and is invariant under $\mathrm{SL}_2(\mathbb{Z})$, i.e. it is a modular function. Hence j descends to a meromorphic function $X(1) \to \mathbb{P}^1(\mathbb{C})$. Because it has one simple pole, general theory of compact Riemann surfaces shows it is conformal. In fact, because we know the automorphisms of $\mathbb{P}^1(\mathbb{C})$ are linear fractional transformations which are uniquely determined by three points, we have proved the following statement.

Theorem 4.5. *j is the unique isomorphism $X(1) \to \mathbb{P}^1(\mathbb{C})$ sending $i \mapsto 1728$, $\rho \mapsto 0$, and $\infty \mapsto \infty$.*

Corollary 4.6. *The field of meromorphic functions on $X(1)$ is $\mathbb{C}(j)$.*

Proof. This follows from considering the associated map on function fields. □

Note that this shows $X(1)$ can actually be defined over k for any subfield $k \subseteq \mathbb{C}$, just as $\mathbb{P}^1(\mathbb{C})$ is the same as $\mathbb{P}^1_k(\mathbb{C})$ where $\mathbb{P}^1_k$ is the rational projective line. This follows from a base change from k to $\mathbb{C}$ which corresponds to field composition $\mathbb{C}k(j) = \mathbb{C}(j)$. So we define $X(1)_k$ to be $\mathbb{P}^1_k$, i.e. the unique curve with function field $k(j)$. Notice $X(1)_k(\mathbb{C}) \approx \mathbb{P}^1_k(\mathbb{C}) = \mathbb{P}^1(\mathbb{C})$ so this definition makes sense.

The j-invariant can be defined completely algebraically based off the coefficients of the elliptic curve. So it still makes sense as a function on elliptic curves over arbitrary fields (though we are only looking at characteristic 0 right now). So for any such k we have a map

$$\{E/k\}/\approx \quad \to \quad \mathbb{P}^1_k = X(1)_k$$

It's looking like we are about to parametrize elliptic curves, but don't get your hopes up.

Fact 4.7. $X(1)$ is NOT a moduli space for isomorphism classes of rational elliptic curves, i.e. the map above is not bijective (even excluding the cusps), it fails injectivity on non-algebraically closed fields. In particular, the rational points on $X(1)_{\mathbb{Q}}$ do not correspond to isomorphism classes of elliptic curves over $\mathbb{Q}$.

Reason. We know the j-invariant works as a parametrization over any algebraically closed field because $E_1 \approx E_2$ if and only if $j(E_1) = j(E_2)$. However this does *not* hold if k is not algebraically closed. It is possible for two curves defined over a field k to be isomorphic only over some extension of k. But the curves will be isomorphic over a finite extension of k (of degree at most 2), see Ralph's notes or [Mil06, Remark II.2.2]. The most common example is a quadratic twist where we go from $y^2 = x^3 + ax + b$ and $dy^2 = x^3 + ax + b$.

So close. But what we have isn't useless, we did learn about the j-line.

5 $X_0(N)$

Next consider the set S_0 of pairs (E, C) where E is an elliptic curve over $\mathbb{C}$ together with a cyclic subgroup of order N. We will call two such pairs isomorphic if there is an isomorphism of curves which also identifies the corresponding torsion groups.

Theorem 5.1. *$X_0(N)$ is a moduli space for S_0, i.e. there is a bijection between points on $Y_0(N)$ (the non-cusps of $X_0(N)$) and elliptic curves with an associated cyclic subgroup C of order N.*

Proof. We will use lattices instead of curves. Let $(\mathbb{C}/\Lambda, C) \in S_0$. Note that C as a subgroup of $\mathbb{C}/\Lambda$ can be viewed as a lattice, $\Lambda' \supseteq \Lambda$. As groups, $[\Lambda' : \Lambda] = N$. So by the structure theorem of finitely generated groups, we can find a basis $\langle \omega_1, \omega_2 \rangle$ for Λ such that $\left\langle \omega_1, \frac{1}{N}\omega_2 \right\rangle$ is a basis for Λ'. Then by dividing by ω_2 (and possibly normalizing sign), we have shown $(\mathbb{C}/\Lambda, C) \approx \left(\mathbb{C}/\Lambda_\tau, \frac{1}{N}\Lambda\right)$ for some $\tau \in \mathbb{H}$.

This gives us a map $S_0 \to Y_0(N)$ sending $\left(\Lambda_\tau, \left\langle \frac{1}{N} \right\rangle\right) \mapsto \tau$. It remains to show it's a well defined bijection. Specifically, we need to show if two such pairs are isomorphic if and only if there is some element of $\Gamma_0(N)$ taking one to the other.

We know from Theorem 4.1 that $\mathbb{C}/\Lambda_\tau \approx \mathbb{C}/\Lambda_{\tau'}$ if and only if $\tau' = \gamma(\tau)$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. But now we have extra torsion data, so we want to know which γ preserve this as well. Also from Theorem 4.1, we know γ induces the isomorphism $\mathbb{C}/\Lambda_{\tau'} \to \mathbb{C}/\Lambda_\tau$ given by $z \mapsto (c\tau + d)z$. It remains to check when this isomorphism respects the extra torsion data. This follows by

$$\left\langle (c\tau + d)\frac{1}{N}\Lambda_{\tau'} \right\rangle = \left\langle \frac{c\tau + d}{N}\Lambda_\tau \right\rangle \equiv \left\langle \frac{1}{N}\Lambda_\tau \right\rangle \mod \Lambda_\tau \quad \Leftrightarrow \quad N \mid c, \text{ i.e. } \gamma \in \Gamma_0(N).$$

□

5.1 As a rational curve.

As before, we will realize $X_0(N)$ as a rational curve by studying its function field. We still have the j function as before. We also have the function $j_N(\tau) = j(N\tau)$. This is a meromorphic function on $X_0(N)$ since

$$\begin{aligned} j_N\left(\frac{a\tau + b}{c\tau + d}\right) &= j_N\left(N\frac{a\tau + b}{c\tau + d}\right) \\ &= j\left(N\frac{a\tau + b}{c\tau + d}\right) \\ &= j\left(\frac{a(N\tau) + Nb}{\frac{c}{N}(N\tau) + d}\right) \\ &= j(N\tau) = j_N(\tau). \end{aligned}$$

Note how we used the hypothesis that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ and that j was $\mathrm{SL}_2(\mathbb{Z})$ invariant.

Theorem 5.2. *j and j_N generate the meromorphic functions on $X_0(N)$, i.e. $\mathbb{C}(X_0(N)) = \mathbb{C}(j, j_N)$. Moreover, the minimal polynomial of j_N over $\mathbb{C}(j)$ is has coefficents in $\mathbb{Q}$.*

Proof. (See [Mil06, Chapter 5 Section 2]). Sketch: Pick coset representatives γ_i for $\Gamma_0(N)\backslash \mathrm{SL}_2(\mathbb{Z})$ so $\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup \Gamma_0(N)\gamma_i$. Note there are precisely $m = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$ representatives. Hence $m = \deg(X_0(N) \to X(1))$ and therefore $m = [\mathbb{C}(X_0(N)) : \mathbb{C}(X(1))] = [\mathbb{C}(X_0(N)) : \mathbb{C}(j)]$. So it is enough to find an element of degree m over $\mathbb{C}(j)$.

Then the minimal polynomial for j_N over $\mathbb{C}(j)$ is turns out to be

$$F(j, Y) = \prod (Y - j(N\gamma_i\tau))$$

which has degree m.

Note that each term is *not* in $\mathbb{C}(j)$, but the symmetric polynomial made by the product is actually invariant under $\mathrm{SL}_2(\mathbb{Z})$, so it is infact a rational function in $\mathbb{C}(j)[Y]$ (since $\mathbb{C}(X(1)) = \mathbb{C}(j)$). Because the product is holomorphic on $\mathbb{H}$, the coefficients must lie in $\mathbb{C}[j, Y]$.

One can show $F(j, Y) \in \mathbb{Q}[j, Y]$ using the fact that j has a rational q-expansion, and hence a relation between j and j_N must lie over $\mathbb{Q}$. □

Corollary 5.3. $\mathbb{C}(X_0(N)) = \mathbb{C}\mathbb{Q}(j, j_N)$.

This allows us to define $X_0(N)_{\mathbb{Q}}$ as the $\mathbb{Q}$ curve corresponding to the function field $\mathbb{Q}(j, j_N)$.

Example 5.4. In the case of $N = 11$ it is possible to explicitly describe $X_0(11)_{\mathbb{Q}}$. The idea is to write down two modular functions x, y for $\Gamma_0(11)$ with a single pole at $i\infty$ of order at most $2, 3$ respectively. It follows from Riemann-Roch (see [Sil09, Chapter II Section 5 Corollary 5.5c]) that $l(D) = \deg D - g + 1$ (with usual notation) so the space of functions with a pole of at most order 6 at $i\infty$ is exactly 6. But we have seven functions, $1, x, y, x^2, xy, y^2, x^3$. Hence we get a non-trivial linear relation which when normalized is exactly a Weirstrass equation.

In [Wes12, Section 4], the author finds such functions x, y. The construction of x, y is complicated so we'll skip it. It uses a lot of complex analysis, theta functions, and modular forms. We end up with (after a lot of hard and clever work) is the equation

$$X_0(11)\colon\ y^2 + y = x^3 - x^2 - 10x - 20$$

This gives us an explicit model over $\mathbb{Q}$ to work with.

5.2 Rational Points on $X_0(N)$

Question 5.5. Is $X_0(N)$ a moduli space for elliptic curves over $\mathbb{Q}$ with Galois invariant subgroups C of $E(\overline{\mathbb{Q}})$ (meaning $\sigma(C) = C$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$) of order N?

First we need to know why did I write "Galois invariant" subgroups. This is because given a Galois invariant subgroup C of a rational curve E, there exists a rational elliptic curve E' and isogeny $E \to E'$ with kernel C. Moreover, E' is unique up to an isomorphism over $\mathbb{Q}$. For a proof, see [Sil09, Chaptr III Ex 3.13e]. The idea is to take all the field automorphisms given by translation by elements of C and then take the corresponding fixed field. We denote E' by E/C.

Now we have a natural map in one direction.

$$(E, C) \mapsto (j(E), j(E/C)) \tag{1}$$

Where the right hand side is a point on the curve $\mathcal{C}_N$ given by the equation $\mathbb{Q}[x, y]/F(x, y)$ where F is the same function as in the proof of Theorem 5.2. To show this map makes sense we have to check the following.

Proposition 5.6. $j(E/C) = j_N(E)$

Proof. If (E, C) is represented by $\left(\mathbb{C}/\Lambda_\tau, \left\langle \frac{1}{N} \right\rangle\right)$ then E/C corresponds to the lattice spanned by $\{\tau, \frac{1}{N}\}$ which we can scale to get the lattice spanned by $\Lambda_{N\tau} = \{N\tau, \frac{1}{N}\}$. Hence $E/C \cong \mathbb{C}/\Lambda_{N\tau}$ so $j(E/C) = j(N\tau) = j_N(E)$. □

Remark 5.7. While $\mathcal{C}_N$ gives us an equation for $X_0(N)$ (hence a model for $X_0(N)_{\mathbb{Q}}$), in practice it is difficult to compute explicitly.

Example 5.8. Let E be the curve $y^2 = x^3 - x$ which has j-invariant 1728. Let P be the point $(x, y) = (-1, 0)$ of order 2. Then with sage we can compute the isogenous curve given by $E/\langle P \rangle$.

```
E1 = EllipticCurve([0,0,0,-1,0])
phi = EllipticCurveIsogeny(E1,E1.torsion_points(2)[0])
E2 = phi.codomain(); E2
E2.j_invariant()
```

```
Elliptic Curve defined by y^2 = x^3 - 11*x + 14 over Rational Field
287496
```

To see this is indeed the right map, we can enter

```
phi.kernel_polynomial()
phi.degree()
```

```
x + 1
2
```

In general, the map in Equation 1 is not surjective as we will see later due to Mazur's Theorem.

Example 5.9. Recall the equation for $X_0(11)$ is $y^2 + y = x^3 - x^2 - 10x - 20$. In sage we can compute

```
E = EllipticCurve([0,-1,1,-10,-20]); E
```

```
Elliptic Curve defined by y^2 + y = x^3 - x^2 - 10*x - 20 over Rational Field
```

```
E.rank()
```

```
0
```

```
E.torsion_order()
```

```
5
```

Thus $X_0(11)$ has 5 rational points. One can show as an exercise that $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(p)] = p + 1$. This means the degree of the map $X_0(11) \to X(1)$ is 12 and hence there are 12 cusps counting multiplicity. In fact it turns out there is only 2 actual cusp points. These do not correspond to elliptic curves because remember the map in Equation 1 lands in $Y_0(N)$. We can not say what exactly the other 3 points mean, so for now they just mean we need a better space.

The following theorem shows how close $X_0(N)$ is to a fine moduli space.

Theorem 5.10. *The map in Equation* 1 *is functorial in* k *and always surjective onto* $Y_0(N)_k$ *for any field* k *of characteristic* 0*. When* k *is algebraically closed it is a bijection.*

Proof. See [Mil06, Chapter V Theorem 2.7]. □

6 $X_1(N)$

Next consider the set S_1 of pairs (E, P) where E is an elliptic curve over $\mathbb{C}$ and P is a point of order N.

Theorem 6.1. *X_1 is a moduli space for S_1, i.e. there is a bijection between points on $Y_1(N)$ and elliptic curves with associated point P of order N.*

Proof. This should follow similarly to Theorem 4.1 and Theorem 5.1.

The first step is to show any pair $(\mathbb{C}/\Lambda, w)$ is isomorphic to a pair $\left(\mathbb{C}/\Lambda_\tau, \frac{1}{N}\right)$ for some τ. From the proof of Theorem 5.1 we know such a pair is isomorphic to $\left(\mathbb{C}/\Lambda_\tau, \frac{c\tau+d}{N}\right)$ for some τ and $c, d \in \mathbb{Z}$.

Now by hypothesis the point $\frac{c\tau+d}{N}$ must have order exactly N. Another way to say this is $(\overline{c}, \overline{d})$ has order N in $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ where $\overline{c}$ is the reduction of c modulo N. This means $\gcd(\overline{c}, \overline{d}) = 1$ so

we can find $a, b \in \mathbb{Z}$ such that $ad - bc \equiv 1 \mod N$, i.e. the matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$ descends to $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Modifying the matrix modulo N (i.e. adding multiples of N to the entries) preserves the point $\frac{c\tau+d}{N}$ so we may choose $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. This is because the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective. Define $\tau' = \gamma(\tau)$ and notice the isomorphism $\mathbb{C}/\Lambda_{\tau'} \to \mathbb{C}/\Lambda_\tau$ is given by multiplication by $c\tau + d$ and hence takes the point $\frac{1}{N}$ to $\frac{c\tau+d}{N}$.

The next step is to show

$$\left(\mathbb{C}/\Lambda_\tau, \frac{1}{N}\right) \approx \left(\mathbb{C}/\Lambda_{\tau'}, \frac{1}{N}\right) \quad \Leftrightarrow \quad \tau' = \gamma(\tau) \quad \text{for some } \gamma \in \Gamma_1.$$

($\Leftarrow$): We know there is an isomorphism $\Lambda_{\tau'} \to \Lambda_\tau$ given by multiplication by $c\tau + d$. Note by definition of Γ_1 we have

$$\frac{1}{N} \mapsto (c\tau + d)\frac{1}{N} \equiv \frac{1}{N} \mod \Lambda_\tau$$

because $c \equiv 0 \mod N$ and $d \equiv 1 \mod N$.

($\Rightarrow$): We can apply the same reasoning as in Theorem 4.1 to find some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ which must induce the isomorphism $\left(\mathbb{C}/\Lambda_{\tau'}, \frac{1}{N}\right) \to \left(\mathbb{C}/\Lambda_\tau, \frac{1}{N}\right)$. By hypothesis we have then that $(c\tau + d)\frac{1}{N} \equiv \frac{1}{N} \mod \Lambda_\tau$. This implies $c \equiv 0 \mod N$ and $d \equiv 1 \mod N$ which is enough as the condition on a is forced by looking at the determinate formula modulo N.

□

6.1 As a Rational Curve

Arguments a little more complicated but similar to those in we used for $X_0(N)$ show that $X_1(N)$ is again a rational curve. There is still a natural map $S_1 \to Y_1(N)$ over $\mathbb{Q}$.

6.2 $X_1(11)$

Fact 6.2. $X_1(11)_{\mathbb{Q}}$ is a fine moduli space (after accounting for cusps as usual) for rational elliptic curves with a given point of order 11.

The proof is difficult but the main reason why $X_1(11)$ works and $X_0(11)$ did not is because of something someone might call "rigidity". Two rational elliptic curves with given Galois invariant subgroups of order N can be isomorphic over $\overline{\mathbb{Q}}$ but not over $\mathbb{Q}$ as we saw above. This is because of the variety of isomorphisms, which can be viewed as "twists" of points on $X_0(11)$.

It turns out that $X_1(N)$ is more rigid. Between any two pairs (E, P) and (E', P') there is at most one isomorphism $E \to E'$ sending P to P'. Assuming this fact, note that given such an isomorphism $\varphi : E \to E'$ we can choose any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and look at $\varphi^\sigma : E^\sigma \to (E')^\sigma$, meaning apply σ to all the coefficients. Because E, E', P, P' are all rational they stay the same and hence by rigidity $\varphi^\sigma = \varphi$ and hence φ is defined over $\mathbb{Q}$.

This doesn't prove it is a fine moduli space, but it does show that the big obstruction for $X_0(11)$ and $X(1)$ doesn't exist for X_1.

6.2.1 Points

First with some combinatorial algebra, one can show $X_1(11)_{\mathbb{Q}}$ has 5 cusps. It is not hard to show $X_1(11)$ has 10 cusps, but then it turns out they are not all "rational". So there are only 5 cusps on $X_1(11)_{\mathbb{Q}}$. These are points on $X_1(11)$ which do not correspond to rational curves in $S_1/\mathbb{Q}$.

We (or somebody very comfortable with modular forms and theta functions) can again somehow calculate a model for $X_1(11)$ as we did for $X_0(11)$. It turns out to be

$$X_1(11): \ y^2 + y = x^3 - x^2$$

Now we can plug this into sage and note

```
E = EllipticCurve([0,-1,1,0,0]); E
```

```
Elliptic Curve defined by y^2 + y = x^3 - x^2 over Rational Field
```

```
E.rank()
```

```
0
```

```
E.torsion_order()
```

```
5
```

Thus we have just shown that *no* rational elliptic curves have a point of order 11. What is even more remarkable, is that Mazur showed $X_1(N)$ fails to have rational points for almost all N. This gave the following theorem.

Theorem 6.3 (Mazur's Torsion Theorem (1977))**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then the torsion subgroup of $E(\mathbb{Q})$ if one of the following* 15 *groups:*

$(1-11)$*: $\mathbb{Z}/N\mathbb{Z}$ for $N = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$.*

$(12-15)$*: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for $N = 1, 2, 3, 4$.*

References

[DS07] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms (Graduate Texts in Mathematics, Vol. 228)*. Springer, 1st edition, 4 2007.

[GGD12] Ernesto Girondo and Gabino Gonzlez-Diez. *Introduction to Compact Riemann Surfaces and Dessins d'Enfants (London Mathematical Society Student Texts)*. Cambridge University Press, 1 edition, 2 2012.

[Har77] R. Hartshorne. *Algebraic Geometry*. Encyclopaedia of mathematical sciences. Springer, 1977.

[Mil06] J.S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006.

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, 2009.

[Wes12] Tom Weston. The modular curves x0(11) and x1(11), 2012.

Travis Scholl
Department of Mathematics, University of Washington, Seattle WA 98195
email: tscholl2@uw.edu