Modular curves as algebraic curves

Ravi Fernando – fernando@berkeley.edu

March 14, 2016*

So far, we have talked about modular curves as complex manifolds. We would like to reinterpret them as algebraic varieties, in order to use the machinery of algebraic geometry. I have two goals in this talk: first, to reassure you that everything works as algebraic curves (even over $\mathbb{Q}$), and second, to outline how it works.

1 Function fields over $\mathbb{C}$

Recall the contravariant equivalence of categories

$$\{\text{projective curves } X \text{ over } k\} \leftrightarrow \{\text{finitely generated } K/k \text{ of transcendence degree 1}\} \quad (1)$$

The $\to$ map is "fraction field"; the $\leftarrow$ map requires writing down a surjection $k[t_1, \ldots, t_n] \to K$ and taking a projective closure of Spec of the image. (A similar equivalence of categories holds in dimension $d > 1$, but something more needs to be said; one way to fix the statement is to consider projective varieties up to birational equivalence.)

Our goal in this section is to begin with our modular curves as complex manifolds, calculate their function fields (i.e. the field of meromorphic functions on them), and then use these fields to translate the curves into the setting of algebraic geometry.

Example: for the level-1 modular curve $X(1)$, the function field $\mathbb{C}(X(1))$ is generated by the j-invariant: $\mathbb{C}(X(1)) = \mathbb{C}(j)$.

Before we write down some functions on modular curves, we first recall the functions

$$\wp_\tau(z) = z^{-2} + \sum_{0 \neq w \in \Lambda} \left((z-w)^{-2} - w^{-2} \right) \quad (2)$$

$$g_2(\tau) = 60 \sum_{0 \neq w \in \Lambda} w^{-4}, \text{ and} \quad (3)$$

$$g_3(\tau) = 140 \sum_{0 \neq w \in \Lambda} w^{-6}, \quad (4)$$

*Notes for a talk given in Sug Woo Shin's reading course on Eichler-Shimura. Main reference: Diamond and Shurman, *Introduction to Modular Forms*.

so that $\wp'_\tau(z)^2 = 4\wp_\tau(z)^3 - g_2(\tau)\wp_\tau(z) - g_3(\tau)$. (Here, $\tau \in \mathcal{H}$ and $z \in \mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$.)

Fix a level N. Let $v = (c, d) \in \mathbb{Z}^2$ be a nonzero vector, and $\overline{v} \in (\mathbb{Z}/N)^2$ its reduction mod N. We define the function $f_0^{\overline{v}} : \mathcal{H} \to \mathbb{C}$ by

$$f_0^{\overline{v}}(\tau) = \frac{g_2(\tau)}{g_3(\tau)} \wp_\tau\left(\frac{c\tau + d}{N}\right). \tag{5}$$

Check: this only depends on $\overline{v}$ (or even $\pm\overline{v}$), not v; it is weight-0 invariant under $\Gamma(N)$; and it is meromorphic on $\mathcal{H}$ and at the cusps. Then it defines a meromorphic function on the modular curve $\overline{(\mathcal{H}/\Gamma(N))} = X(N)$.

We introduce a few more pieces of notation:

$$f_0^{\overline{d}}(\tau) = f_0^{\overline{(0,d)}}(\tau) \text{ for } d \neq 0 \pmod{N}, \tag{6}$$

$$f_0(\tau) = \sum_{d=1}^{N-1} f_0^{\overline{d}}(\tau), \tag{7}$$

$$f_{1,0} = f_0^{\pm\overline{(1,0)}}, \tag{8}$$

$$f_{0,1} = f_1 = f_0^{\pm\overline{(0,1)}}, \tag{9}$$

$$j_N(\tau) = j(N\tau). \tag{10}$$

Now we are ready to state the proposition:

Proposition 1.1. *The fields of meromorphic functions on $X(N), X_1(N)$, and $X_0(N)$ are*

$$\mathbb{C}(X(N)) = \mathbb{C}(j, \{f_0^{\pm\overline{v}} : v \in (\mathbb{Z}/N)^2 - \{(0,0)\}\}) \tag{11}$$

$$= \mathbb{C}(j, f_{1,0}, f_{0,1}), \tag{12}$$

$$\mathbb{C}(X_1(N)) = \mathbb{C}(j, \{f_0^{\pm\overline{d}} : \overline{d} \in (\mathbb{Z}/N) - \{0\}\}) \tag{13}$$

$$= \mathbb{C}(j, f_1), \text{ and} \tag{14}$$

$$\mathbb{C}(X_0(N)) = \mathbb{C}(j, f_0) \tag{15}$$

$$= \mathbb{C}(j, j_N). \tag{16}$$

Proof idea for the first of these (the rest are similar): we know that $\mathbb{C}(X(1)) = \mathbb{C}(j) \subset \mathbb{C}(j, \{f_0^{\pm\overline{v}}\}) \subset \mathbb{C}(X(N))$. Let $\mathrm{SL}_2(\mathbb{Z})$ act on $\mathbb{C}(X(N))$, and show that the kernel of this action is $\{\pm 1\}\Gamma(N)$ and the fixed field is $\mathbb{C}(X(1))$. Then $\mathbb{C}(X(N))/\mathbb{C}(X(1))$ is a Galois extension with Galois group $\mathrm{SL}_2(\mathbb{Z}/N)/\{\pm 1\}$. Finally, calculate that $\mathbb{C}(j, \{f_0^{\pm\overline{v}}\})$ is fixed only by the identity of $\mathrm{SL}_2(\mathbb{Z}/N)/\{\pm 1\}$.

In particular, this implies that there are polynomial relations among the functions given above. The actual relations aren't generally easy to write down (as far as I know), but the fact that there exist such relations tells us that our modular curves can (up to birational equivalence) be embedded into projective space. We will later see that the relations are defined over $\mathbb{Q}$ (or $\mathbb{Q}(\mu_N)$ in the case of $\mathbb{C}(X(N))$), so we get models of these curves over those number fields

instead of over $\mathbb{C}$.

For another description, we introduce the *universal elliptic curve* E_j. For this, we view τ and thus j as variables, and define

$$E_j : y^2 = 4x^3 - \left(\frac{27j}{j-1728}\right)x - \left(\frac{27j}{j-1728}\right) \tag{17}$$

where the coefficients are chosen so that the j-invariant is actually j. This is an elliptic curve over the transcendental field extension $\mathbb{C}(j)$, and it specializes to an elliptic curve over $\mathbb{C}$ for each $j \in \mathbb{C}$ except 0 and 1728. Then it can be shown that $\mathbb{C}(X(N))$ is also equal to $\mathbb{C}(j, x(E_j[N]))$. (Again, the j here is transcendental over $\mathbb{C}$, and $x(E_j[N])$ denotes the x-coordinates of N-torsion points of E_j, viewed as elements of the algebraic closure of $\mathbb{C}(j)$.) For the sake of the following diagram, we also want to consider $\mathbb{C}(j, E_j[N])$, where we have adjoined both the x- and y-coordinates of $E_j[N]$; this is a quadratic extension of $\mathbb{C}(j, x(E_j[N]))$.

Draw diagram here: ramified covers of $X(1)$, extensions of function fields, and the corresponding Galois groups. See page 285.

2 Function fields over $\mathbb{Q}$

We previously discussed the fields $\mathbb{C}(X(N)) = \mathbb{C}(j, f_{1,0}, f_{0,1}) = \mathbb{Q}(j, x(E_j[N]))$, $\mathbb{C}(X_1(N)) = \mathbb{C}(j, f_1)$, and $\mathbb{C}(X_0(N)) = \mathbb{C}(j, f_0) = \mathbb{C}(j, j_N)$, where all of the things we adjoined were functions on the respective modular curves. Now we consider the same fields $\mathbb{Q}(j, E_j[N])$ and so on. We want these fields to have transcendence degree 1 over $\mathbb{Q}$, so that they correspond to curves over $\mathbb{Q}$. It suffices to prove this for the field at the top of our tower, $\mathbb{Q}(j, E_j[N])$, because the rest of the fields we care about lie between this and the pure transcendence degree 1 field $\mathbb{Q}(j)$. But this is actually not hard to see: the equations defining what it means to be N-torsion on E_j are polynomials over $\mathbb{Q}(j)$, so their solutions belong to $\overline{\mathbb{Q}(j)}$.

So all of these fields have transcendence degree 1 over $\mathbb{Q}$, which means that they define curves. In the cases of $X_0(N)$ and $X_1(N)$, the function field extensions involved are just $\mathbb{Q}(j, f_0)$ and $\mathbb{Q}(j, f_1)$ respectively, both over $\mathbb{Q}$. But in the case of $X(N)$, we want the field $\mathbb{Q}(j, f_{1,0}, f_{0,1})$ to be over the base field $\mathbb{Q}(\mu_N)$ instead of just $\mathbb{Q}$. I think this is because $\mathbb{Q}(j, f_{1,0}, f_{0,1}) \cap \overline{\mathbb{Q}} = \mathbb{Q}(\mu_N)$, and if we made it a curve over $\mathbb{Q}$, then it wouldn't be geometrically integral.

Draw a diagram of Galois groups (page 288), and explain how the isomorphism works, by the action of $\mathrm{Gal}(\mathbb{Q}(\mu_N, j, E_j[N]))$ on $E_j[N]$. Mention that $\det \rho : \mathrm{Gal}(\mathbb{Q}(\mu_N, j, E_j[N])/\mathbb{Q}) \to (\mathbb{Z}/N)^\times$ describes the action of that Galois group on μ_N: $\mu^\sigma = \mu^{\det(\rho(\sigma))}$. (The proof uses the Weil pairing.)

3 Modular curves as algebraic curves and Modularity

Theorem 3.1. *(The modularity theorem, version $X_\mathbb{Q}$.) Let E be an elliptic curve over $\mathbb{Q}$. Then for some N there is a surjective morphism of curves $X_0(N)_{\mathrm{alg}} \to E$ over $\mathbb{Q}$.*

Definition 3.2. *The smallest N that for which the above map exists is called the* analytic conductor *of E.*

There also exists a version $X_{\mathbb{C}}$, which says that any elliptic curve $E/\mathbb{C}$ with rational j-invariant[1] admits a surjective holomorphic map $X_0(N) \to E$ of Riemann surfaces. The $X_{\mathbb{Q}}$ version easily implies the $X_{\mathbb{C}}$ version (base change and analytify, after checking that a curve with rational j-invariant admits a model over $\mathbb{Q}$). The reverse implication is true but more difficult, and involves possibly increasing the value of N.

There are a few other versions of the modularity theorem. The version $J_{\mathbb{Q}}$ says the same thing as $X_{\mathbb{Q}}$ but with $X_0(N)_{\text{alg}}$ replaced by its Jacobian $J_0(N)_{\text{alg}}$; the version $A_{\mathbb{Q}}$ uses instead the abelian variety $A'_{f,\text{alg}}$ associated to a newform $f \in \mathcal{S}_2(\Gamma_0(N))$. (Have we talked about this construction before?) The version of modularity that was actually proved is in the language of Galois representations: for every elliptic curve $E/\mathbb{Q}$, the ℓ-adic Galois representation $\rho_{E,\ell}$ arising from it agrees with the ℓ-adic Galois representation arising from some modular form, $\rho_{f,\ell}$.

Why do we care about having a modular parametrization $X_0(N) \to E$? One good reason: it allows us to write down points on an elliptic curve with reasonably small residue fields, possibly even $\mathbb{Q}$. Specifically, the Heegner point construction gives a way to choose some nice points on $X_0(N)$, map them down to E, and apply some Galois symmetrization process to obtain a single point defined over $\mathbb{Q}$ under certain hypotheses. Gross and Zagier showed that this construction essentially proves the Birch and Swinnerton-Dyer conjecture in the rank-1 case. This is very interesting, especially if you or your advisor is named Xinyi Yuan.

Examples of modularity: for some choices of N, $X_0(N)$ has genus 1, so $X_0(N) \cong J_0(N) \cong A'_f$ for the unique (adjectives) newform $f \in \mathcal{S}_2(\Gamma_0(N))$. This holds in particular for $N = p = 11, 17, 19$. (There is even an algorithm to write down equations for A'_f, and thus for $X_0(N)$ in these cases. See page 298.) Then these elliptic curves certainly admit surjective morphisms, in particular isomorphisms, from modular curves.

4 Isogenies and Hecke operators

Isogenies work like you want them to in the algebraic setting; in particular, you can quotient out by finite subgroups (at least over a field that contains the coordinates of the appropriate torsion points), and isogeny is an equivalence relation. (Symmetry comes from dual isogenies; composing gives multiplication by the degree).

Previously we've seen that the Hecke algebra $\mathbb{T}_{\mathbb{Z}} = \mathbb{Z}[T_p, \langle d \rangle]$ acts on the Jacobian $J_1(N) = \text{Pic}^0(X_1(N))$ as a complex manifold. But we now know that $X_1(N)$ is an algebraic variety over $\mathbb{Q}$, so $J_1(N)$ is too. We would like the Hecke operators $\langle d \rangle$ and T_p to act by morphisms over $\mathbb{Q}$. Fortunately, they do.

[1] For reference: $j = 1728\frac{4a^3}{4a^3+27b^2}$.