Outline

- Recap of Proof from 1st Talk (No $E/\mathbb{Q}$ w/ 11-torsion)
- Moduli problems over $\mathbb{Z}$
- Neron model of $J_0(p)$.

Recall 1 (1st talk)**.** Ingredients in proof that no $E/\mathbb{Q}$ has 11-torsion

On board before start of talk

- Considered moduli space $Y_1(11)$ of elliptic curves equipped w/ a point of order 11, then compactified to $X_1(11)$

  In general, we'll look at $X_0(p)$, the moduli space of (generalized) elliptic curves w/ a p-isogeny

- $J_1(11) := \operatorname{Jac} X_1(11)$ is an elliptic curve with $\#J_1(11)(\mathbb{Q})_{\text{tors}} = 5$

  We saw last time that $J_0(p) := \operatorname{Jac} X_0(p)$ is an abelian variety w/ a point of order (dividing) $p-1$.

- Computed Néron model $\mathfrak{X}^0/\mathbb{Z}$ for $J_1(11)$, the smooth locus of the Weierstrass curve $y^2+y = x^3-x$. This had good reduction away from 11 and multiplicative reduction at 11.

  Goal (Today). We'll show that $J_0(p) := \operatorname{Jac} X_0(p)$ has good reduction away from p and completely toric reduction at p

- Performed a "fancy 5-descent" to compute $J_1(11)(\mathbb{Q})$

  In later talks, we'll perform (something like) a "very fancy $(p-1)$-descent" to compute $\operatorname{rank} J_0(p)(\mathbb{Q})$.

$\odot$

1 Defining Various Moduli Problems

Assumption (simplifying assumption)**.** Assume throughout that $N \geq 1$ is squarefree.

Definition 2. Let E/S be a smooth, separated group scheme of relative dimension 1.

- A $\Gamma_0(N)$`-structure` on E is a finite, flat S-subgroup scheme $G \subset E$ of order N such that $\mathscr{O}_E(G)$ is ample.

  ample $\iff$ meets every irreducible component of every fiber

- A $\Gamma_1(N)$`-structure` on E is a homomorphism $\varphi : \mathbb{Z}/N\mathbb{Z} \to E(S)$ such that the effective Cartier divisor $\sum_{n\in\mathbb{Z}/N\mathbb{Z}}[\varphi(n)]$ is ample and a subgroup scheme of E. We will often identify φ with the point $P := \varphi(1) \in E(S)$ (and say P is a `point of exact order` N). $\diamond$

Example 3. Say S is a $\mathbb{Z}[1/N]$-scheme and E/S is elliptic. Then, all group schemes of order N in E are étale, so a $\Gamma_1(N)$-structure on E is simply an embedding $\underline{\mathbb{Z}/N\mathbb{Z}}_S \hookrightarrow E$ of group schemes. $\triangle$

Example 4. Say $E/\overline{\mathbb{F}}_p$ is an elliptic curve, and consider its (non-reduced) order p subgroup scheme $G := \ker\big(\mathrm{Frob} : E \to E^{(p)}\big)$. Then, $G \subset E$ is a $\Gamma_0(p)$-structure on E. Furthermore, as divisors, $G = p[0]$, so $0 \in E(\overline{\mathbb{F}}_p)$ is a $\Gamma_1(p)$-structure on E. $\triangle$

Example 5. Say $E = \mathbb{G}_m \times \underline{\mathbb{Z}/5\mathbb{Z}}$ (think: E is the smooth locus of a Néron 5-gon), then $\mu_5 \subset E$ is a subgroup of order 5, but is *not* a $\Gamma_0(5)$-structure (because it's not ample). However, $\underline{\mathbb{Z}/5\mathbb{Z}} \subset E$ is a $\Gamma_0(5)$-structure. $\triangle$

Definition 6. We define the following two functions $\mathrm{Sch}^{\mathrm{op}} \to \mathrm{Set}$

$$\mathcal{M}_1(N)\colon S \longmapsto \left\{ (E/S, P \in E(S)) \,\middle|\, \begin{array}{l} E \text{ an elliptic scheme} \\ P \text{ a } \Gamma_1(N)\text{-structure} \end{array} \right\} / \simeq$$
$$\mathcal{M}_0(N)\colon S \longmapsto \left\{ (E/S, G \subset E) \,\middle|\, \begin{array}{l} E \text{ an elliptic scheme} \\ G \text{ a } \Gamma_0(N)\text{-structure} \end{array} \right\} / \simeq \quad \diamond$$

Fact. There exists an affine scheme $Y_0(N)/\mathbb{Z}$ along with a natural transformation $\mathcal{M}_0(N) \to Y_0(N)$ which is both initial among maps from $\mathcal{M}_0(N)$ to schemes and which is a bijection on $\mathbb{C}$-points (one says $Y_0(N)$ is the `coarse moduli space` of $\mathcal{M}_0(N)$). Furthermore, $Y_0(N)$ is smooth over $\mathbb{Z}[1/N]$ and $Y_0(N)(\mathbb{C}) = \mathbb{H}/\Gamma_0(N)$.

Fact. The analogous statements hold for $\mathcal{M}_1(N)$ in place of $\mathcal{M}_0(N)$. In fact, $\mathcal{M}_1(N) \to Y_1(N)$ is an isomorphism for $N \geq 4$ (one says that $Y_1(N)$ is the `fine moduli space` of $\mathcal{M}_1(N)$, when $N \geq 4$).

Example 7. $Y(1) := Y_0(1) = Y_1(1) = \mathbb{A}^1_{\mathbb{Z}}$ $\triangle$

Following our outline in the beginning, we should try and compactify these spaces. Complex analytically, this corresponds to adding in the cusps $\mathbb{P}^1(\mathbb{Q})$ to the upper half plane $\mathbb{H}$; what does this correspond to in the modular interpretation?

Example 8. A complex number $\tau \in \mathbb{H}$ corresponds to the elliptic curve $E_\tau = \mathbb{C}/(\mathbb{Z}\oplus\mathbb{Z}\tau)$. What happens as $\tau \to i\infty$? The trick is to realize the exponential map gives an isomorphism $\exp(2\pi i(-)) : E_\tau \xrightarrow{\sim} \mathbb{C}^\times/q^{\mathbb{Z}}$, where $q = e^{2\pi i\tau}$. Note that $\tau \to i\infty$ corresponds to $q \to 0$, which suggests $E_{i\infty} = \mathbb{C}^\times = \mathbb{G}_m(\mathbb{C})$, so the cusps look like they should capture multiplicative reduction. $\triangle$

Recall 9. An elliptic curve $E/\mathbb{Q}$ has multiplicative reduction at p iff the p-special fiber of its minimal proper regular model is (gemetrically) a Néron n-gon (for some n), i.e. is of the form

$$C_n = \frac{\mathbb{P}^1 \times \mathbb{Z}/n\mathbb{Z}}{(\infty, i) \sim (0, i+1) \;\text{ for }\; i \in \mathbb{Z}/n\mathbb{Z}}$$

(after basechange to $\overline{\mathbb{F}}_p$). $\odot$

Definition 10. A `generalized elliptic curve` over S is a tuple $(E/S, +, 0)$ where E is a proper, flat, finitely presented S-scheme,

- $+ : E^{sm} \times_S E \to E$ is a morphism restricting to a commutative addition law on E^{sm} w/ identity $0 \in E^{sm}(S)$ (and which defined a group action of E^{sm} on E); and
- every geometric fiber of E/S is an elliptic curve of a Néron n-gon for some n. $\diamond$

Definition 11. We now define two more functors $\mathrm{Sch}^{\mathrm{op}} \to \mathrm{Set}$

$$\overline{\mathcal{M}}_1(N)\colon S \longmapsto \left\{ (E/S, P \in E^{\mathrm{sm}}(S)) \,\middle|\, \begin{array}{c} E \text{ a generalized elliptic curve} \\ P \text{ a } \Gamma_1(N)\text{-structure} \end{array} \right\} / \simeq$$
$$\overline{\mathcal{M}}_0(N)\colon S \longmapsto \left\{ (E/S, G \subset E^{\mathrm{sm}}) \,\middle|\, \begin{array}{c} E \text{ a generalized elliptic curve} \\ G \text{ a } \Gamma_0(N)\text{-structure} \end{array} \right\} / \simeq \quad \diamond$$

Fact. There exists a proper scheme $X_0(N)/\mathbb{Z}$ along with a natural transformation $\overline{\mathcal{M}}_0(N) \to X_0(N)$ which is both initial among maps from $\overline{\mathcal{M}}_0(N)$ to schemes and which induces a bijection on $\mathbb{C}$-points. Furthermore, $X_0(N)$ is smooth over $\mathbb{Z}[1/N]$ and $X_0(N)(\mathbb{C}) = \mathbb{H}^*/\Gamma_0(N)$.

Remark 12. By the valuative criterion, properness of $X_0(N)$ ultimately follows from the semistable reduction theorem + the theory of Néron models. Given some $(E, G) \in X_0(N)(\mathbb{Q}_p)$, for example, after a finite extension $F/\mathbb{Q}_p$, E will attain good or multiplicative reduction, so its minimal proper regular model over $\mathscr{O}_F$ will be a generalized elliptic curve (take closure of subgroup and then contract fibers to get ampleness). ∘

i.e. semistable reduction

Fact. The analogous statements hold for $\overline{\mathcal{M}}_1(N)$ in place of $X_1(N)$. In fact, $\overline{\mathcal{M}}_1(N) \to X_1(N)$ is an isomorphism (over $\mathbb{Z}[1/N]$) for $N \geq 5$.

I'm confused on if $X_1(N)$ is ever a $\mathbb{Z}$-scheme

Example 13. $X(1) := X_0(1) = X_1(1) = \mathbb{P}^1_{\mathbb{Z}}$. △

Example 14. Let $C_2 = (\mathbb{P}^1 \times \mathbb{Z}/2\mathbb{Z})/((\infty, 0) \sim (0,1), (\infty, 1) \sim (0,0))$ be a Néron 2-gon over $\overline{\mathbb{Q}}$, so $C_2^{\mathrm{sm}} = \mathbb{G}_m \times \mathbb{Z}/2\mathbb{Z}$. Then $P = (i, 1) \in (\mu_4 \times \mathbb{Z}/2\mathbb{Z})(\overline{\mathbb{Q}}) = C_2^{\mathrm{sm}}[4](\overline{\mathbb{Q}})$ is a $\Gamma_1(4)$-structure. Note that P is fixed by the automorphism $(x, n) \mapsto ((-1)^n/x, -n)$ of C_2.[1] This shows that $\Gamma_1(4)$-structures on generalized elliptic curves are not rigid (i.e. they have non-trivial automorphisms). △

Example 15. Let p be prime. From the analytic theory given last time, we know that $X_0(p)(\mathbb{C})$ has two cusps. From the moduli perspective, these cusps are

$$\underbrace{\mu_p \subset C_1}_{\infty} \quad \text{and} \quad \underbrace{\mathbb{Z}/p\mathbb{Z} \subset C_p}_{0}.$$ △

2 $X_0(p)$ mod p

See [DR73, Section V.1.14]

Setup 16. Fix a prime p.

Remark 17. By a theorem of Raynaud, we expect that the Neron model of $J_0(p)_{\mathbb{Q}} = \mathrm{Jac}(X_0(p)_{\mathbb{Q}})$ is related to $\mathrm{Pic}^0_{X_0(p)/\mathbb{Z}}$. In order to prove this (and see what this tells us about $J_0(p)$), we need some understanding of what (a regular model of) $X_0(p)$ looks like mod p. ∘

Remark 18. Let $E/\overline{\mathbb{F}}_p$ be an elliptic curve.

- If E is ordinary, then $E[p] \simeq \mu_p \times \underline{\mathbb{Z}/p\mathbb{Z}}$ has two $\Gamma_0(p)$-structures. Furthermore, $\mu_p = \ker(F : E \to E^{(p)})$ and if $E \simeq E'^{(p)}$, then $\underline{\mathbb{Z}/p\mathbb{Z}} = \ker(V : E'^{(p)} \to E')$.
- If E is supersingular, then $E[p]$ is a nontrivial extension $0 \to \alpha_p \to E[p] \to \alpha_p \to 0$ and so has only one $\Gamma_0(p)$-structure. In this case, $\alpha_p = \ker(F : E \to E^{(p)})$ and one has

$$\begin{tikzcd} E^{(p)} \arrow[r, "V"'] \arrow[rr, bend left, "F"] & E \arrow[r, "\sim"'] & E^{(p^2)} \end{tikzcd}$$ ∘

Theorem 19. $X_0(p)_{\mathbb{F}_p}$ *reduced and consists of two copies of* $X_0(1)_{\mathbb{F}_p} \simeq \mathbb{P}^1_{\mathbb{F}_p}$ *meeting transversally at the supersingular points. In particular, all of its singularities are nodal.*

Proof. Consider the map $\nu := f \sqcup g : X_0(1)_{\mathbb{F}_p} \sqcup X_0(1)_{\mathbb{F}_p} \to X_0(p)_{\mathbb{F}_p}$ given by

$$f(E) := \Big(E, \ker\Big(F : E \to E^{(p)}\Big)\Big) \quad \text{and} \quad g(E) := \Big(E^{(p)}, \ker\Big(V : E^{(p)} \to E\Big)\Big).$$

g only defined below on $Y(1)$, but extends to a morphism on $X(1)$.

Note that every ordinary point of $X_0(p)_{\mathbb{F}_p}$ is hit by exactly one of f, g while each supersingular point of $X_0(p)_{\mathbb{F}_p}$ is hit by them *both* of them ($f(E^{(p)}) = g(E)$ if E is supersingular), so ν is surjective. In addition to this, one has the maps $q, r : X_0(p)_{\mathbb{F}_p} \rightrightarrows X_0(1)_{\mathbb{F}_p}$ given by

$$q(E,G) := E^0 \text{ and } r(E,G) := E/G.$$

E^0 is fiber-wise identity component

One can check that

$$qf = \mathrm{id} = rg \qquad \text{and} \qquad rf = \mathrm{Frob} = qg,$$

so[2] f, g are closed immersions. In fact, $f \sqcup g$ restricts to an isomorphism

$$X(1)^{\mathrm{ord}}_{\mathbb{F}_p} \sqcup X(1)^{\mathrm{ord}}_{\mathbb{F}_p} \xrightarrow{\sim} X_0(p)^{\mathrm{ord}}_{\mathbb{F}_p}$$

on ordinary loci. Hence, $X_0(p)_{\mathbb{F}_p}$ is reduced (smooth even) away from its supersingular points.

Inverse applies either q or r to (E,G) depending on if G is étale.

Fact. $X_0(p)_{\mathbb{F}_p}$ is reduced (even at its supersingular points).

So far, we've shown that $X_0(p)_{\mathbb{F}_p}$ is two copies of $\mathbb{P}^1_{\mathbb{F}_p} \simeq X(1)_{\mathbb{F}_p}$ meeting at supersingular points. The map ν separates tangent vectors at supersingular points because $\mathrm{d}q$ kills one of them (the one coming from g) while $\mathrm{d}r$ kills the other. ■

Application. $X_0(p)_{\mathbb{F}_p}$ is a nodal union of two $\mathbb{P}^1$'s meeting at $\delta := \#\{\text{supsersingular } j\text{-invariants in char } p\}$ points. Furthermore, $X_0(p)$ is $\mathbb{Z}$-flat.[3] Thus,

$$\delta - 1 = p_a(X_0(p)_{\mathbb{F}_p}) = g(X_0(p)_{\mathbb{C}}) = \left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 1 & \text{if } p \equiv -1 \pmod{12} \\ -1 & \text{if } p \equiv 1 \pmod{12} \\ 0 & \text{otherwise.} \end{cases}$$

For cusps, can compute $f(\infty) = \infty$ (non-reduce locus is closed b/c supp of sheaf of 1-forms), so surjectivity forces $g(\infty) = 0$.

To apply Raynaud's theorem, we need an integral version of this result.

Fact. $X_0(p)/\mathbb{Z}$ is smooth away from the supersingular points in characteristic p. At any supersingular point $x = (E, \alpha_p) \in X_0(p)(\overline{\mathbb{F}}_p)$, $X_0(p)$ has an A_{k-1} singularity, where $k := \frac{1}{2}\#\operatorname{Aut}(E)$.[4] That is, $X_0(p)$ is *not* regular at x (if $k > 1$), but this singularity can be resolved into a chain of $(k-1)$ copies of $\mathbb{P}^1$ (each w/ self-intersection -2).

Picture 20. Draw a picture of $X_0(23)$ and its minimal proper regular model. Apparently, $j = 0$ is super singular $\iff p \equiv -1 \bmod 6$ and $j = 1728$ is supersingular $\iff p \equiv -1 \bmod 4$. For $p = 23$, the supersingular j-invariants are $0, 19, 1728$.

Probably omit (doubt there will be time)

Corollary 21. *The special fiber of the minimal proper regular model of $X_0(p)$ is a (reduced) nodal curve, all of whose components are $\mathbb{P}^1$'s.*

Corollary 22 (of Raynaud's theorem)**.** *The identity component of Néron model of $J_0(p) := \operatorname{Jac} X_0(p)_{\mathbb{Q}}$ is $\operatorname{Pic}^0_{X_0(p)/\mathbb{Z}}$, so $J_0(p)$ has good reduction away from p and completely toric reduction at p.*

Saw in Mikayel's talk the Jacobian of a nodal curve is an extension of the Jacobian of its normalization by a torus

(We make no claims on the structure of the component group at p).

[1] In general, $\underline{\mathrm{Aut}}(C_n) = \mu_n \rtimes \mathbb{Z}/2\mathbb{Z}$, where $\zeta \in \mu_n$ acts via $(x, n) \mapsto (\zeta^n x, n)$.

[2] Cancellation
$$\begin{tikzcd} X(1) \arrow[rr, "f"] \arrow[dr, "\mathrm{id}"'] & & X_0(p) \arrow[dl, "q"] \\ & X(1) & \end{tikzcd}$$

[3] e.g. $X_0(p)$ reduced + dominant over $\mathbb{Z}$

[4] Assuming $p \neq 2, 3$, $k = 2$ if $j(x) = 1728$, $k = 3$ if $j(x) = 0$, and $k = 1$ otherwise.

Corollary 23. *Any quotient abelian variety $q : J_0(p) \twoheadrightarrow A$ has good reduction away from p and completely toric reduction at p.*

Proof Sketch. Choose some map $s : B \to A$ such that $qs = [n] : B \to B$ for some integer n. Passing to (identity components of) Néron models, we get

Alternatively, say A is isogenous to $B \times B'$ so get an isogeny $B_p \times B'_p \twoheadrightarrow A_p$

$$\begin{tikzcd} \mathcal{B}^0 \arrow[r, "s"'] \arrow[rr, bend left, "{[n]}"] & \mathcal{A}^0 \arrow[r, "q"'] & \mathcal{B}^0. \end{tikzcd}$$

On each fiber, use the fact that there are no non-trivial maps from a torus, a unipotent group, or an abelian variety to one of the other two. ■

3 Bonus

Define Hecke Correspondences

$\Gamma_0(N;p)$-structure is cyclic subgroup G of order N + cyclic subgroup H of order p s.t. they generate an ample subgroup of order Np.

Remark 24. If $p \nmid N$, then a $\Gamma_0(N;p)$-structure is simply a $\Gamma_0(Np)$-structure ○

We let $X_0(N;p)$ denote the coarse moduli space of $\Gamma_0(N;p)$-structures on (smooth loci of) generalized elliptic curves. Then, we have the `pth Hecke correspondence`

$$\begin{tikzcd} & X_0(N;p) \arrow[dl, "p_1"'] \arrow[dr, "p_2"] & \\ X_0(N) & & X_0(N), \end{tikzcd}$$

where

bar denotes contraction of fibers away from G

$$p_1(E,G,H) := (\overline{E}, G) \quad \text{and} \quad p_2(E,G,H) := (E/H, G/H).$$

These correspondences are defined over $\mathbb{Z}$, they act on $J_0(N) := \mathrm{Jac}(X_0(N)_{\mathbb{Q}})$, and they also act on the Néron model of $J_0(N)$ over $\mathbb{Z}$. More on this next time.

References

[DR73] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349, 1973. 3