Modular Curves and Theorem A

Yiannis Fam

June 2, 2026

Abstract

These are notes from my talk in the London Number Theory study group on Mazur's Eisenstein ideal paper [Maz77], following [Sno13].

The goal of this talk is to prove the following theorem, which reduces the problem of proving the non-existence of rational elliptic curves with rational N-torsion points to the existence of an abelian variety with certain properties.

Theorem 0.1 (Theorem A)**.** *Let $N > 7$ be prime. If there exists an abelian variety A/QQ and a morphism $f : X_0(N) \to A$, where $X_0(N)$ is the modular curve, such that*

- *A has good reduction away from N,*
- *$A(\mathbb{Q})$ has rank 0,*
- *$f(0) \neq f(\infty)$,*

then there is no elliptic curve over $\mathbb{Q}$ with a rational point of order N.

1 Modular curves

We first recall the definition of the modular curve $X_0(N)$. Modular curves represent moduli problems parametrising elliptic curves with prescribed level structure - over $\mathbb{C}$ we recover the classical definition by realising elliptic curves as $\mathbb{C}/\Lambda$ for a lattice Λ. Consider the following moduli problem: when is the functor

$$F_{\Gamma_?(N)} : \text{Schemes}/\mathbb{Z}[1/N] \to \text{Sets}$$
$$S \mapsto \{\text{Isomorphism classes of elliptic curves over } S \text{ with level } \Gamma_?(N)\text{-structure}\}$$

representable, where $\Gamma_?(N) = \Gamma_0(N), \Gamma_1(N), \Gamma(N)$. Here $\Gamma(N)$-level structure on E/S is the data of an isomorphism $(\mathbb{Z}/N\mathbb{Z})^2_S \cong E[N]$, $\Gamma_1(N)$ is the data of a choice of N-torsion point of E, and $\Gamma_0(N)$ is the data of a choice of cyclic N-torsion subgroup of order N.

Taking level $\Gamma(N)$, the representability of $F_{\Gamma(N)}$ explicitly means the existence of an object $Y(N)$ with a morphism $Y(N) \to \text{Spec}\mathbb{Z}[1/N]$ such that, on points,

$$Y(N)(S) = \{\text{Isomorphism classes of elliptic curves over } S \text{ with level } \Gamma(N)\text{-structure}\}.$$

Taking $S = Y(N)$ itself, provided $Y(N)$ exists, there is a canonical elliptic curve $\mathcal{E}(N)$ over $Y(N)$, coming with an isomorphism $(\mathbb{Z}/N\mathbb{Z})^2_{Y(N)} \cong \mathcal{E}(N)[N]$. This is known as the universal elliptic curve with level $\Gamma(N)$ structure. For every morphism $S \to Y(N)$ we form the pullback diagram

$$\begin{array}{ccc} E_S & \longrightarrow & \mathcal{E}(N) \\ \downarrow & & \downarrow \\ S & \longrightarrow & Y(N). \end{array}$$

to produce an elliptic curve E_S/S. Similarly, we may pullback the level $\Gamma(N)$-structure on $\mathcal{E}(N)[N]$ to level $\Gamma(N)$-structure on E_S. This is then meant to realise $Y(N)(S)$ as the set of isomorphism classes of elliptic curves over S with level $\Gamma(N)$-structure.

Take as fact the following result:

Theorem 1.1. *For $N \geq 3$, $F_{\Gamma(N)}$ and $F_{\Gamma_1(N)}$ are representable by a smooth affine scheme over $\mathbb{Z}[1/N]$. The functor $F_{\Gamma_0(N)}$ is only representable by a smooth Deligne–Mumford stack $Y_0(N)$ over $\mathbb{Z}[1/N]$.*

The obstruction to representing $F_{\Gamma_0(N)}$ by a scheme is the existence of nontrivial automorphisms of elliptic curves with level $\Gamma_0(N)$-structure. For example, when $N = 1$ so that we are just considering the moduli problem of isomorphism classes of elliptic curves, we can certainly find non-isomorphic elliptic curves over $\mathbb{Q}$ that are isomorphic when base changed to $\bar{\mathbb{Q}}$. If this functor is representable by $Y(1)$, then the map $Y(1)(\mathbb{Q}) \to Y(1)(\bar{\mathbb{Q}})$ is not injective, and this cannot happen for schemes. The existence of twists of elliptic curves can be rephrased as the existence of non-trivial automorphisms (by composing an isomorphism over $\bar{\mathbb{Q}}$ with a nontrivial Galois action). A stack handles this by keeping track of the isomorphisms between objects of an isomorphism class.

We defined $Y_0(N)$ over $\mathbb{Z}[1/N]$ because in characteristic N, elliptic curves have fewer geometric N-torsion points. To define $Y_0(N)$ over $\mathbb{Z}$ we simply replace in the definition of level structure $\mathbb{Z}/N\mathbb{Z}$ by a finite flat group scheme of order N (where care is required if N is not prime as then the finite flat group scheme need not be 'cyclic').

In the complex setting, one works instead with a compactification of the modular curve by adding cusps. When N is prime, two cusps are added to $Y_0(N)$. To define the (compactified) modular curve $X_0(N)/\mathbb{Z}$ we again add two 'cusps'.

Definition 1.2.

- A scheme E/S is a generalised elliptic curve if it is proper, flat, the smooth locus E^{sm} has a group structure and the geometric fibres of E are either elliptic curves of n-gons for some n.
- An n-gon over a field k is

$$C_n = \mathbb{P}^1_k \times \mathbb{Z}/n\mathbb{Z}/(\infty, i) \sim (0, i+1).$$

As an example, a 1-gon is a nodal cubic. An n-gon consists of n lines ($\mathbb{P}^1$) glued together cyclically. The smooth points of C_n are $C_n^{sm} = \mathbb{G}_m \times \mathbb{Z}/n\mathbb{Z}$. When $n = N$ there are two canonical level structures: $\mu_N \subset \mathbb{G}_m$ and $\mathbb{Z}/N\mathbb{Z}$.

To compactify $Y_0(N)$ into the modular curve $X_0(N)$ we add, over each point of Spec$\mathbb{Z}$ the cusps $\infty := (C_1, \mu_N)$ and $0 := (C_N, \mathbb{Z}/N\mathbb{Z})$. The corresponding moduli problem parametrises generalised elliptic curves over $\mathbb{Z}$ with a finite flat group scheme of order N that in each fibre over $\mathbb{Z}$ meets each irreducible component of E (this explains the choice $\mathbb{Z}/N\mathbb{Z}$ of level structure on C_N). the stack $X_0(N)$ is proper. We can think of a generalised elliptic curve over $\mathbb{Z}$ as a family of objects over $\mathbb{Q}$ and $\mathbb{F}_p$ for all p that are either elliptic curves or degenerate into n-gons.

Example 1.3. The only example that we need in this talk is the following: if $E/\mathbb{Q}$ has everywhere semistable reduction, then its minimal regular model $\mathcal{E}_{\mathrm{reg}}/\mathbb{Z}$ is a generalised elliptic curve. This is because its smooth locus is a group scheme (the Néron model) and its fibres over Spec$\mathbb{Z}$ are by definition either elliptic curves or 1-gons (when we have multiplicative reduction).

2 The proof of Theorem A

To prove Theorem A we use the following reduction steps, proving that $A'' \Rightarrow A' \Rightarrow A$, and then prove Theorem A".

Theorem 2.1 (Theorem A'). *Let $N > 7$ be prime and let A, f be as in Theorem A. Suppose $E/\mathbb{Q}$ is an elliptic curve with a rational point P of order N. Then over $\mathbb{Q}$,*

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mu_N.$$

Remark 2.2. The Weil pairing is a nondegenerate alternating bilinear map

$$\langle , \rangle : E[N] \times E[N] \to \mu_N.$$

Then $\langle P, - \rangle$ is a surjection $E[N] \to \mu_N$ with kernel generated by P. In other words we have a short exact sequence

$$0 \longrightarrow \mathbb{Z}/N\mathbb{Z} \longrightarrow E[N] \longrightarrow \mu_N \longrightarrow 0. \tag{2.0.3}$$

The content of Theorem A' is that this sequence splits.

Theorem 2.4 (Theorem A"). *Let $N > 7$ be prime and let A, f, E, P be as in Theorem A'. For any prime p of bad reduction for E then, over $\mathbb{Q}_p$,*

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mu_N.$$

Proof that $A' \Rightarrow A$. Firstly we show that $X_0(N)(\mathbb{Q})$ is finite. Since $f : X_0(N) \to A$ is a nonconstant morphism ($f(0) \neq f(\infty)$), and $X_0(N)$ is a curve, the fibres are finite. That $X_0(N)(\mathbb{Q})$ is finite follows from the assumption that $A(\mathbb{Q})$ is finite.

We also have the general fact that for any elliptic curve $E/\mathbb{Q}$, we have $\mathrm{End}_{\mathbb{Q}}(E) = \mathbb{Z}$ (even if E has complex multiplication, these morphisms are not defined over $\mathbb{Q}$). It is well known that this endomorphism ring is either $\mathbb{Z}$ or an order in an imaginary quadratic field. But since any endomorphism of $E/\mathbb{Q}$ induces an endomorphism

of its tangent space at the identity, which has endomorphism ring $\mathbb{Q}$ over $\mathbb{Q}$, we must have a ring homomorphism from $\mathrm{End}_{\mathbb{Q}}(E) \to \mathbb{Q}$, so that only $\mathbb{Z}$ is possible.

Now suppose that $E_1/\mathbb{Q}$ is an elliptic curve with rational point P_1 of order N. By assumption, $E_1[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$. Now that μ_N is a subgroup scheme of $E_1[N]$, we may define the elliptic curve $E_2 = E_1/\mu_N$ over $\mathbb{Q}$, so that the image P_2 of P_1 is still a rational point of order N. In this way we produce an infinite sequence of pairs (E_i, P_i). Each pair determines a point of $X_0(N)(\mathbb{Q})$ (by taking the cyclic subgroup generated by P_i to be the level structure) so that there exists $i < j$ such that $(E_i, P_i) \cong (E_j, P_j)$. Identifying them, the isogeny $E_i \to E_j$ induces an endomorphism of E_i of degree N^{j-i} that preserves the N-torsion point P_i. But this is impossible as the endomorphisms of E_i over $\mathbb{Q}$ are $\mathbb{Z}$ and so the degree N^{j-i} isogeny must be $[\pm N^{j-i/2}]$, which kills P_i. This gives the desired contradiction. □

Proof that $A'' \Rightarrow A'$. Consider the action $\rho : \Gamma_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$ of the absolute Galois group of $\mathbb{Q}$ on $E[N]$. From the short exact sequence (2.0.3), ρ takes the form

$$\rho = \begin{pmatrix} 1 & f_0 \\ 0 & \chi \end{pmatrix}$$

where χ is the mod N cyclotomic character and $f_0 : \Gamma_{\mathbb{Q}} \to \mathbb{F}_N$ is a 1-cocycle, so that

$$f_0(\sigma\tau) = f_0(\tau) + \chi(\tau) f_0(\sigma).$$

Let $K = \mathbb{Q}(\mu_N)$ so that $\rho\,|_K = \left(\begin{smallmatrix} 1 & f \\ 0 & 1 \end{smallmatrix}\right)$ for some $f \in \mathrm{Hom}(\Gamma_K, \mathbb{F}_N)$ now a homomorphism.

To have the desired splitting of (2.0.3), we want to show that $f_0 = 0$. It suffices to prove that $f = 0$ so that ρ factors through a representation of a finite group, which is always semisimple. To constrain $\rho\,|_K$ we show the following:

Proposition 2.5. *Given Theorem A", $\rho\,|_K$ is everywhere unramified.*

Proof.

- When $p \neq N$ is a prime of good reduction, $\rho\,|_{\mathbb{Q}_p}$ is unramified by Néron–Ogg–Shafarevich.
- When p is a prime of bad reduction, $E[N] = \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$ over $\mathbb{Q}_p$ by assumption so that $\rho\,|_{\Gamma_{\mathbb{Q}_p}} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \chi \end{smallmatrix}\right)$ and so $\rho\,|_{\Gamma_{\mathbb{Q}_p(\mu_N)}}$ is trivial.
- If $p = N$ is a prime of good reduction, setting $\mathcal{E}$ to be the Néron model of E over $\mathbb{Z}_p$, we have that $\mathcal{E}[N]$ is a finite flat group scheme,

  $$E[N] = \mathcal{E}[N] \times_{\mathbb{Z}_p} \mathbb{Q}_p$$

  and the short exact sequence

  $$0 \to \mathbb{Z}/N\mathbb{Z} \to \mathcal{E}[N] \to \mu_N \to 0$$

  over $\mathbb{Z}_p$. For finite flat group schemes the connected-étale sequence is in the reverse direction, from which we deduce that

  $$\mathcal{E}[N] = \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$$

over $\mathbb{Z}_p$ and hence

$$E[N] = \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$$

over $\mathbb{Q}_p$, from which we conclude as in the case of bad reduction above.

□

As a consequence of this Proposition, we see that the homomorphism f factors through the Galois group of the maximal unramified abelian (since f is a homomorphism to an abelian group) extension of K (the Hilbert class field), so that we view f as a homomorphism $f : Cl(K) \to \mathbb{F}_N$ on the class group of K. The action of $\mathrm{Gal}(K/\mathbb{Q})$ on $Cl(K)$ decomposes the space of homomorphisms $\mathrm{Hom}(Cl(K), \mathbb{F}_N)$ into eigenspaces on which $\mathrm{Gal}(K/\mathbb{Q})$ acts by the various powers of χ (these are the characters of $\mathrm{Gal}(K/\mathbb{Q})$). The cocycle condition on f_0 implies that $f^\sigma = \chi(\sigma)f$ for any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. A theorem of Herbrand implies that any such homomorphism is 0, implying the result. □

Before we begin the proof of Theorem A", we collect some facts and notation about Néron models.

Let R be a DVR and $A/\mathrm{Frac}(R)$ an abelian variety. There exists a Néron model $\mathcal{A}/R$, which is a smooth group scheme characterised by the Néron mapping property. This property in particular gives a bijection $\mathcal{A}(R) \leftrightarrow A(\mathrm{Frac}(R))$. One can also replace R by a Dedekind domain, such as $\mathbb{Z}$ by 'gluing' together these Néron models at DVRs.

In particular, for our elliptic curve $E/\mathbb{Q}$ we may define the Néron model $\mathcal{E}/\mathbb{Z}$. The rational point P lifts by the Néron mapping property to a point $\mathcal{P} \in \mathcal{E}[N]$ of order N. We will denote by $\mathcal{P}_{\mathbb{F}_p}$ the reduction in $\mathcal{E}[N](\mathbb{F}_p)$. Fix this notation for the rest of the notes.

We will also rely heavily on the following consequence of Raynaud's theorem:

Proposition 2.6. *Let $K/\mathbb{Q}_p$ be a finite extension with ramification index $< p-1$. Let $\mathcal{O}$ be the ring of integers of K and k be the residue field. Let A/K be an abelian variety and $\mathcal{A}/\mathcal{O}$ its Néron model. Then the reduction map $\mathcal{A}(\mathcal{O})_{\mathrm{tors}} \to \mathcal{A}(k)_{\mathrm{tors}}$ is injective.*

Proof. [Sno13, Lecture 19]. □

Proof of Theorem A".

Lemma 2.7. *E has everywhere semistable reduction.*

Proof.

- Suppose E has additive reduction at $p \neq N$. The classification of special fibres of Néron models tells us that $\mathcal{E}_{\mathbb{F}_p}$ has at most 4 components. Since $\mathcal{P}_{\mathbb{F}_p}$ has order $N > 7$, by Proposition 2.6 when taking $K = \mathbb{Q}_p$, we must have

  $$\mathcal{P}_{\mathbb{F}_p} \in \mathcal{E}^0_{\mathbb{F}_p} = \mathbb{G}_{a,\mathbb{F}_p}(\mathbb{F}_p) = \mathbb{F}_p,$$

  which is a contradiction as $N \neq p$.

- Suppose that we have additive reduction at N so $\mathcal{E}^0_{\mathbb{F}_N} = \mathbb{G}_{a,\mathbb{F}_N}$. It is a fact that E acquires semistable reduction over an extension $K/\mathbb{Q}_p$ of degree at most 6. Let $\mathcal{E}'/\mathcal{O}$ be the Néron model and $\mathcal{E}'_k$ the special fibre, whose identity component is either an elliptic curve or torus by definition of semistability. Néron models are not well behaved under base change and indeed we have that $\mathcal{E}^0_k = \mathbb{G}_{a,k}$ as the identity component of the base change of the special fibre of our original Néron model $\mathcal{E}$. There is no nontrivial map from $\mathbb{G}_a$ to an elliptic curve or torus. The Néron mapping property induces a morphism $h : \mathcal{E}_{\mathcal{O}} \to \mathcal{E}'$ (since both are models of E/K and have the same K-points). The induced map $\bar{h}$ on the identity component of the special fibres is then trivial. In particular $\bar{h}(\mathcal{P}_{\mathbb{F}_p}) = 0$. But this implies that the point $f(\mathcal{P}) \in \mathcal{E}'[N](\mathcal{O})$ (corresponding to P by the Néron mapping property, so in particular of order N) reduces to 0 in $\mathcal{E}'[N](k)$, contradicting Proposition 2.6. Here we use that $N > 7$.

□

Lemma 2.8. *E has bad (hence multiplicative) reduction at $p = 2, 3$.*

Proof. If E had good reduction at p then $\mathcal{E}_{\mathbb{F}_p}$ is an elliptic curve over $\mathbb{F}_p$, and the Hasse bound for $p = 2, 3$ gives $\#\mathcal{E}_{\mathbb{F}_p}(\mathbb{F}_p) \leq 7.5$, but the reduction map is injective on N-torsion since $N \neq p$, so $\mathcal{E}_{\mathbb{F}_p}(\mathbb{F}_p)$ contains $\mathcal{P}_{\mathbb{F}_p}$, a point of order $N > 7$, a contradiction. □

Lemma 2.9. *Let p be a prime of bad reduction for E. Then $\mathcal{P}_{\mathbb{F}_p} \notin \mathcal{E}^0_{\mathbb{F}_p}(\mathbb{F}_p)$.*

Proof. Since E has everywhere semistable reduction, it has multiplicative reduction at p. Then $\mathcal{E}^0_{\mathbb{F}_p}$ is a rank 1 torus over $\mathbb{F}_p$. The two possibilities are the split torus $\mathbb{G}_m$ or the non-split torus $\mathrm{Res}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\mathbb{G}_m)^{\mathrm{norm}=1}$. These have $p - 1$ and $p + 1$ points over $\mathbb{F}_p$ respectively. Recall that $\mathcal{P}_{\mathbb{F}_p} \in \mathcal{E}_{\mathbb{F}_p}(\mathbb{F}_p)$ is a point of order $N > 7$ by Proposition 2.6.

If $p = 2, 3$ the claim follows from the fact that $p + 1 < N$. If $p = N$ the claim follows from the fact that $p \pm 1$ is coprime to N.

Let $\mathcal{A}/\mathbb{Z}$ be the Néron model for our abelian variety $A/\mathbb{Q}$ in the statement of Theorem A". Since $A(\mathbb{Q})$ is finite, so all torsion, the composition

$$A(\mathbb{Q}) = \mathcal{A}(Z) \hookrightarrow \mathcal{A}(\mathbb{Z}_p) \to \mathcal{A}(\mathbb{F}_p)$$

is injective by Proposition 2.6 for $p > 2$.

Since E has everywhere semistable reduction, $\mathcal{E}_{\mathrm{reg}}$ is a generalised elliptic curve, and together with the group generated by $\mathcal{P}$ defines a point x of $X_0(N)$ over $\mathbb{Z}$. Recall that for the cusp $0 = (C_N, \mathbb{Z}/N\mathbb{Z})$, the level structure is not contained in the identity component, whereas it is for $\infty = (C_1, \mu_N)$.

Let $p \neq 2, 3, N$ be a prime of bad reduction. As we have bad reduction, x reduces to the image of one of 0 or ∞ in $X_0(N)(\mathbb{F}_p)$.

Since E has multiplicative reduction at $p = 3$ and $\mathcal{P}_{\mathbb{F}_3} \notin \mathcal{E}^0_{\mathbb{F}_3}(\mathbb{F}_3)$ as shown above, we deduce that x and 0 reduce to the same point of $X_0(N)(\mathbb{F}_3)$. Since $f(x)$ and $f(0)$ reduce to the same point of $\mathcal{A}(\mathbb{F}_3)$, the injectivity mentioned above implies that $f(x) = f(0)$.

Now if $\mathcal{P}_{\mathbb{F}_p} \in \mathcal{E}^0_{\mathbb{F}_p}(\mathbb{F}_p)$ then x and ∞ reduce to the same point of $X_0(N)(\mathbb{F}_p)$, and the same argument above implies that $f(x) = f(\infty)$. This contradicts $f(0) \neq f(\infty)$. $\square$

We finally prove that $E[N] = \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$ over $\mathbb{Q}_p$. Let G be the subgroup of $E[N]$ reducing into $\mathcal{E}^0_{\mathbb{F}_p}$. This is the kernel of the map from $E[N]$ to the component group Φ of $\mathcal{E}_{\mathbb{F}_p}$. Since $\mathcal{E}_{\mathbb{F}_p}$ is the smooth locus of an n-gon, the component group Φ is cyclic (of order n). As such, the map $E[N] \to \Phi$ is not injective as $E[N]$ is not cyclic. So G is a nontrivial subgroup of $E[N]$ that does not intersect $\mathbb{Z}/N\mathbb{Z} = \langle P \rangle$ by the previous lemma. It follows that G has order N and $E[N] = G \oplus \mathbb{Z}/N\mathbb{Z}$. By the short exact sequence (2.0.3), $G \cong \mu_N$ and we are done. $\square$

References

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186, With an appendix by Mazur and M. Rapoport. MR 488287

[Sno13] A. Snowden, *Course on Mazur's torsion theorem.*, `https://websites.umich.edu/~asnowden/teaching/2013/679/index.html,2013`, 2013.