Proof of Theorem A

Jef Laga

October 8, 2020

Goal

Theorem (Theorem A)

Let $N > 7$ be prime. Suppose there exists an abelian variety $A/\mathbb{Q}$ and a morphism $f : X_0(N) \to A$ with the following properties:

- *A has good reduction outside N.*
- *$f(0) \neq f(\infty)$.*
- *$A(\mathbb{Q})$ has rank zero, i.e. $A(\mathbb{Q})$ is torsion.*

Then no elliptic curve over $\mathbb{Q}$ has a point of order N, i.e. $Y_1(N)(\mathbb{Q}) = \emptyset$.

The proof will be similar to the case of $X_1(31)$, but more involved.

First reduction

Let $E/\mathbb{Q}$ have a point P of order N. Get sequence of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules:

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

It will suffice to prove:

Theorem (1)

The above sequence splits: $E[N] \simeq \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$.

Suppose Theorem (1) holds.

- Set $E_1 = E$, $P_1 = P$.
- Define $E_2 = E_1/\mu_N$, $P_2 =$ image of P_1 in $E_1 \to E_2$. Then $P_2 \in E_2[N](\mathbb{Q})$.

Continuing this, we get a chain of degree N isogenies

$$E_1 \to E_2 \to E_3 \to \dots$$

with rational N-torsion points $P_i \in E_i(\mathbb{Q})$.

First reduction

Such a chain

$$E_1 \to E_2 \to E_3 \to \dots$$

cannot exist! Suppose it does.

$X_1(N)(\mathbb{Q})$ is finite

Reason: $X_1(N) \to X_0(N) \to A$ finite fibres and $A(\mathbb{Q})$ finite.

Then $E_i \simeq E_j$ for some $i < j$. Let $\phi\colon E_i \to E_i$ be the composite

$$E_i \to E_{i+1} \to \cdots \to E_j \simeq E_i.$$

ϕ is multiplication by a power of N.

Reason: $\deg \phi$ is a power of N and $\operatorname{End} E = \mathbb{Z}$.

But then $\phi(P_i) = 0$ is of order N, contradiction!

Strategy for proving Theorem (1)

- Carefully analyze local behaviour of E.
- Prove that $E[N] = \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$ over $\mathbb{Q}_p$ for all primes of bad reduction of E.
- Use non-trivial input from class groups of cyclotomic fields.

Notation

Let $\mathcal{E}/\mathbb{Z}$ be the Néron model of E, $\mathcal{P} \in \mathcal{E}(\mathbb{Z})$ the point extending P.

Important fact

For any $K/\mathbb{Q}_p$ with $e(K/\mathbb{Q}_p) < p-1$ and abelian variety A/K with Néron model $\mathcal{A}/\mathcal{O}_K$, the reduction

$$\mathcal{A}(\mathcal{O}_K)_{tors} \to \mathcal{A}(k) \quad (\mathcal{O}_K/\pi = k)$$

is injective. It's injective on prime-to-p torsion, even if $e(K/\mathbb{Q}_p) \geq p-1$.

Step 1: semistability

Step 1

E is semistable.

Proof.

Let p be a prime of additive reduction. By important fact, $\mathcal{P}_{\mathbb{F}_p} \in \mathcal{E}(\mathbb{F}_p)$ has order N. Since $\#\pi_0(\mathcal{E}_{\mathbb{F}_p}) \leq 4$, $\mathcal{P}_{\mathbb{F}_p}$ lies in fact in $\mathcal{E}^\circ_{\mathbb{F}_p}$. Since $\mathcal{E}^\circ_{\mathbb{F}_p} \simeq \mathbb{G}_a$, we must have $p = N$.

Suppose E acquires semistable reduction after $K/\mathbb{Q}_N$. We may assume that $e(K/\mathbb{Q}_N) \leq 6$. Let $\mathcal{E}'/\mathcal{O}_K$ be the Néron model of E_K. We have a morphism $\phi\colon \mathcal{E} \times_{\mathbb{Z}_N} \mathcal{O}_K \to \mathcal{E}'$. But $\phi(\mathcal{E}^\circ_k) = \{0\}$, so $\phi(\mathcal{P}_k) = 0$. By important fact and assumption $N > 7$, $\mathcal{P}_k$ has order N in $\mathcal{E}'(k)$, contradiction.

□

Step 2: the primes 2,3

Step 2

Let $p \in \{2, 3\}$. Then E has bad reduction at p and $\mathcal{P}_{\mathbb{F}_p} \notin \mathcal{E}^\circ_{\mathbb{F}_p}$.

Proof.

By important fact, $\mathcal{P}_{\mathbb{F}_p} \in \mathcal{E}(\mathbb{F}_p)$ has order N. If E has good reduction at p, then $\#\mathcal{E}(\mathbb{F}_p)$ violates the Hasse bound. By Step 1, E has multiplicative reduction at p. So $\mathcal{E}^\circ_{\mathbb{F}_p} \simeq \mathbb{G}_m$ or a norm 1 torus $N_{\mathbb{F}_{p^2}/\mathbb{F}_p}\mathbb{G}_m$. They have $p-1$ and $p+1$ points respectively, so $\mathcal{P}_{\mathbb{F}_p} \notin \mathcal{E}^\circ_{\mathbb{F}_p}$. □

Step 3: the remaining bad primes

Step 3

Let $p \notin \{2, 3\}$ be a prime of bad reduction for E. Then $\mathcal{P}_{\mathbb{F}_p} \notin \mathcal{E}^\circ_{\mathbb{F}_p}$.

Proof.

Suppose $p = N$. Then $\mathcal{E}^\circ_{\mathbb{F}_N}$ has $N \pm 1$ points, so cannot contain a point of order N.

Suppose $p \neq N$. Consider the modular curve $X_0(N) \to \operatorname{Spec} \mathbb{Z}[1/N]$. It has three relevant $\mathbb{Z}[1/N]$-points:

- The cusp $0 = (\mu_N \subset \mathbb{G}_m)$.
- The cusp $\infty = (\mathbb{Z}/N\mathbb{Z} \subset \mathbb{G}_m \times \mathbb{Z}/N\mathbb{Z})$.
- $x = (E, \langle P \rangle) \in X_0(N)(\mathbb{Q}) = X_0(N)(\mathbb{Z}[1/N])$.

The point x reduces to 0 mod p if $\mathcal{P}_{\mathbb{F}_p} \in \mathcal{E}^\circ_{\mathbb{F}_p}$, and to ∞ otherwise.

□

Step 3: the remaining bad primes

Let $q \neq N$ be an odd prime. Consider

$$\begin{array}{ccc} X_0(N)(\mathbb{Q}) & \xrightarrow{f} & A(\mathbb{Q}) \\ \downarrow & & \downarrow \\ X_0(N)(\mathbb{F}_q) & \xrightarrow{f} & \mathcal{A}(\mathbb{F}_q) \end{array}$$

Step 4

Let p be a prime of bad reduction for E or $p = N$. Then $E[N] \simeq \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$ over $\mathbb{Q}_p$.

Proof.

It suffices to prove that $\mathbb{Z}/N\mathbb{Z} \subset E[N]$ has a complement over $\mathbb{Q}_p$.
Suppose that p is a bad prime. From Steps 2,3, have $\mathcal{P}_{\mathbb{F}_p} \notin \mathcal{E}^{\circ}_{\mathbb{F}_p}$. If $G \subset E[N]$ is the subgroup of points reducing to an element of $\mathcal{E}^{\circ}_{\mathbb{F}_p}$, then G is such a complement.
Supppose $p = N$ and good. Then $\mathcal{E}[N]/\mathbb{Z}_N$ finite flat has a complement by the connected-étale sequence.

□

The endgame

The action of $\Gamma_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[N]$ defines a representation

$$\rho\colon \Gamma_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_N).$$

Let $K = \mathbb{Q}(\zeta_N)$. We will prove that ρ factors through $\mathrm{Gal}(K/\mathbb{Q})$. This implies Theorem (1) since ρ must then be semisimple.

$\rho|_{\Gamma_K}$ is everywhere unramified

Reason: suppose $\mathfrak{p}$ lies above p. If p is a bad prime for E or $p = N$, Step 4 shows that $E[N] \simeq \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$ over $\mathbb{Q}_p$, hence trivial over $K_{\mathfrak{p}}$. Otherwise $p \neq N$ is good hence follows from Neron-Ogg-Shafarevich.

We have $\rho \sim \begin{pmatrix} 1 & f \\ 0 & \chi \end{pmatrix}$ where $\chi\colon \Gamma_{\mathbb{Q}} \to \mathbb{F}_N^{\times}$ is the cyclotomic character and $f : \Gamma_{\mathbb{Q}} \to \mathbb{F}_N$ is a 1-cocycle for χ.

The endgame

Let $f' = f|_{\Gamma_K}$. Then f is a homomorphism $\Gamma_K \to \mathbb{F}_N$ which is everywhere unramified, so factors through $\mathrm{Cl}(K) \to \mathbb{F}_N$.
The group $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{F}_N^\times$ acts on $H = \mathrm{Cl}(K) \otimes \mathbb{F}_N$ and we have a decomposition

$$H = \bigoplus_{0 \leq j \leq N-2} H(\chi^j).$$

This action corresponds to conjugation of $\mathrm{Gal}(K/\mathbb{Q})$ on Γ_K^{ab}. Since $\sigma(f') = \chi(\sigma)f'$, f' is zero on $H(\chi^j)$ if $j \neq -1$.
Punchline:

Herbrand-Ribet Theorem

Let $j > 1$ be odd. Then $H(\chi^j) \neq 0$ if and only if N divides B_{N-j} (Bernoulli number.)

Since $B_2 = 1/6$, $H(\chi^{-1}) = H(\chi^{N-2}) = 0$. Therefore $f' = 0$, hence $\rho|_{\Gamma_K}$ is trivial. Since $\#\,\mathrm{Gal}(K/\mathbb{Q}) = N - 1$ prime to N, ρ must be semisimple.

Summary of the argument

- Suffices to show that $E[N] \simeq \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$ over $\mathbb{Q}$.
- Show that E is semistable.
- Show that $P \notin \mathcal{E}^{\circ}_{\mathbb{F}_p}$ if p is a bad prime of E.
- This implies that $E[N] = \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$ over $\mathbb{Q}_p$ for p a prime of bad reduction or $p = N$.
- Therefore $\rho\colon \Gamma_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ everywhere unramified over $K = \mathbb{Q}(\zeta_N)$.
- Implies by Herbrand's theorem that it is actually trivial over K.
- Since $\#\,\mathrm{Gal}(K/\mathbb{Q})$ prime to N, ρ is semisimple, so $E[N] \simeq \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$.,