12/9 : proof of Mazur's Thm & Eisenstein ideal

AIM of Today:

Theorem. Let N be a prime greater than 7 and not 13. Then no elliptic curve over $\mathbf{Q}$ has a rational point of order N.

By Daniel's talk, we need to show:

Theorem (Theorem 1). Let $N > 7$ be a prime number. Suppose there exists an abelian variety $A/\mathbf{Q}$ and a map of varieties $f: X_0(N) \to A$ satisfying the following conditions:

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

Then no elliptic curve defined over $\mathbf{Q}$ has a rational point of order N.

of Yifu Wang.

Combined with Theorem B from Lecture 1 [PP69BM], we have the following criterion:

Theorem (Theorem 2). Let $N > 7$ be a prime number and let $p \neq N$ be a second prime number. Suppose there exists an abelian variety $A/\mathbf{Q}$ and a map $f: X_0(N) \to A$ satisfying the following:

- A has good reduction away from N.
- A has completely toric reduction at N.
- The Jordan--Holder constituents of $A[p](\overline{\mathbf{Q}})$ are 1-dimensional and either trivial or cyclotomic. JH(p) Condition.
- $f(0) \neq f(\infty)$.

Then no elliptic curve defined over $\mathbf{Q}$ has a rational point of order N.

Let $\rho: G_{\mathbb{Q}} \longrightarrow GL_d(\overline{\mathbb{F}}_p)$ be a residue rep. We call ρ statisfy JH(p) if ρ^{ss} the semi-simplification of ρ $\simeq \oplus \chi_p \oplus 1$ where $\chi_p =$ cyclotomic mod p.

Idea: Find an ideal $I \subseteq \mathbb{T}$ (Tate algebra) so that $A = J_0(N)/I J_0(N)$ satisfies conditions of Thm2, in particular, JH(p).

I p-Eisenstein prime & Eisenstein ideal:

Def Let p be a prime. p- Eisenstein prime $\mathfrak{A}$ is the ideal of $\mathbb{T}$ generated by p & $T_\ell-(\ell+1)$, $\forall \ell \nmid N$.

Lemma 1 If $\mathfrak{A}$ is nontrivial then $\mathbb{T}/\mathfrak{A} \simeq \mathbb{F}_p$. So $\mathfrak{A}$ is max.

proof: We have $\mathbb{Z} \longrightarrow \mathbb{T}/\mathfrak{A}$ is surjective as $T_\ell \in \mathbb{Z}$ in $\mathbb{T}/\mathfrak{A}$. Since $p\mathbb{Z} \subseteq \mathfrak{A}$, we have $\mathbb{F}_p \twoheadrightarrow \mathbb{T}/\mathfrak{A}$ as required.

Now let us explain why $\mathfrak{A}$ relates to $JH(p)$. Recall by Shiang's talk, we have

$$V_p(J_0(N)) \sim \bigoplus \rho_{f,\lambda}$$ where $\rho_{f,\lambda}$ is 2-dim p-adic $G_{\mathbb{Q}}$-rep attached to the weight 2 eigenform f. By the construction of $\rho_{f,\lambda}$, we see that the reduction of $\rho_{f,\lambda}$ corresponds to a max. ideal $\mathfrak{m}$ of $\mathbb{T}$ in the way that. $\operatorname{tr}(\bar{\rho}_{f,\lambda}(Fr_\ell)) = T_\ell \bmod \mathfrak{m}$, $\forall \ell \neq p, N$.

Lemma 2 $\mathfrak{m} = \mathfrak{A} \overset{\Leftarrow}{\Longleftrightarrow} \bar{\rho}_{f,\lambda}^{ss} = \chi_p \oplus 1$.

proof: $\mathfrak{m} = \mathfrak{A} \Longleftrightarrow \operatorname{tr}(\bar{\rho}_{f,\lambda}(Fr_\ell)) = \ell+1$

so if $\bar{\rho}_{f,\lambda}^{ss} = \chi_p \oplus 1$. then $\mathfrak{m} = \mathfrak{A}$ is clear.

Conversely? This is unclear. (I don't think Snowden's proof is correct).

II Find p so that $\mathfrak{A}$ is nontrivial.

Prop 3 ① $[0]-[\infty]$ is nontrivial torsion in $J_0(N)$ killed by $N-1$.

② $T_\ell([0]-[\infty]) = (\ell+1)([0]-[\infty])$, $\forall \ell \nmid N$

proof: ① If $[0]-[\infty]=0$ in $J_0(N)$. $\exists$ meromorphic function f. s.t $\operatorname{div}(f) = [0]-[\infty]$. $\Rightarrow \exists f: J_0(N) \longrightarrow \mathbb{P}^1$. $\therefore J_0(N)$ has genus 0. Not true for $N>7 \neq 13$.

Consider $\Delta(z) \in S_{12}(\Gamma(1))$. $\Rightarrow \Delta(Nz) \in S_{12}(\Gamma(N))$.

By definition of $\Delta(z)$ $\Delta(\tau) \equiv (2\pi)^{12} q \prod_{r=1}^{\infty}(1-q^r)^{24}$. We see that $\Delta(z)$

has no zero on upper half plane $\mathcal{H}$. So $\Delta(z)/\Delta(Nz)$ is a meromorphic function on $X_0(N)$ & holomorphic at $Y_0(N)$. At ∞, we have $f = \Delta(z)/\Delta(Nz) = q^{-(N-1)} + \cdots$, so $\mathrm{div} f = (N-1)([0]-[\infty])$

$\therefore \quad (N-1)([0]-[\infty]) = 0$ in $J_0(N)$.

② consider Hecke correspondence $f, g \quad X_0(N\ell) \longrightarrow X_0(N)$

using facts a) $X_0(N\ell)$ has 4 cusps coming from $X_0(N)$ & $X_0(\ell)$

b) $f(x,y) = g(x,y) = x \in X_0(N)$.

c) study ramification at $(*,0)$, $(*,\infty)$

$\Rightarrow \quad f^*([x]) = \ell[(x,0)] + [(x,\infty)]$

$\therefore \quad T_\ell([x]) = g_* f^*([x]) = \ell+1 \; [x]$.

Coro. 4: pick $p \mid N-1$ so that $\exists$ nontrivial $Q \in J_0(N)[p]$. Then p-Eisenstein prime is nontrivial.

proof Since $V_p(J_0(N)) \sim \oplus \rho_{p,f}$, & semi-simplification of reduction is independent on selection of lattices, we see that $\mathbb{Z}/p\mathbb{Z} \hookrightarrow \bar{\rho}_{f,\lambda}$ for at least one f, λ. As $\det(\bar{\rho}_{f,\lambda}) \simeq \chi_p$.

$\therefore \quad (\bar{\rho}_{f,\lambda})^{ss} = 1 \oplus \chi_p. \Rightarrow \mathfrak{a}$ is nontrivial.

III Construction of A.

Now set $I = \bigcap_{\mathfrak{p} \in S} \mathfrak{p}$ where $S = \{$ prime $\mathfrak{p} \subseteq \mathbb{T}$ & $\mathfrak{p} \subseteq \mathfrak{a}\}$.

& $\quad A = J_0(N)/I J_0(N)$. (I actually am pretty nervous about this quotient. This should be ok at least at $\mathbb{C}$-level).

Now we need to show $f(0) \neq f(\infty)$ where $f: X_0(N) \longrightarrow J_0(N) \twoheadrightarrow A$.

& $A(\mathbb{Q})$ is finite. The second point is much harder & will be discussed in the end.

Let $\mathbb{T}_p = \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \varprojlim_n \mathbb{T}/p^n\mathbb{T}$ & $\mathbb{T}_{\mathfrak{a}} = \varprojlim_n \mathbb{T}/\mathfrak{a}^n$

Fact: $\mathbb{T}_{\mathfrak{a}}$ is a direct summand of $\mathbb{T}_p$ as $\mathbb{T}$ is finite $\mathbb{Z}$-algebra & $\mathfrak{a}$ is max. ideal. (following Hensel's Lemma).

Lemma 5: $J_0(N)[\mathfrak{a}^\infty] \longrightarrow A[\mathfrak{a}^\infty]$ is injection.

proof: Let $X = J_0(N)[p^\infty]$ then X is $\mathbb{T}_p$-module & we have $0 \to IX \to X \to A[p^\infty]$ of $\mathbb{T}_p$-modules.

As $\mathbb{T}_\mathfrak{a}$ is a direct summand of $\mathbb{T}_p$, we have

$$0 \to (I \otimes \mathbb{T}_\mathfrak{a}) X \longrightarrow X \otimes \mathbb{T}_\mathfrak{a} \longrightarrow A[p^\infty] \otimes \mathbb{T}_\mathfrak{a}.$$

It suffices to check $I \otimes \mathbb{T}_\mathfrak{a} = 0$, $J_0(N)[p^\infty] \otimes \mathbb{T}_\mathfrak{a} = J_0(N)[\mathfrak{a}^\infty]$ & $A[p^\infty] \otimes \mathbb{T}_\mathfrak{a} = A[\mathfrak{a}^\infty]$.

First $I \otimes \mathbb{T}_\mathfrak{a}$ = intersection of mini primes in $\mathbb{T}_\mathfrak{a}$, as $\mathbb{T}$ is reduced, $I \otimes \mathbb{T}_\mathfrak{a} = 0$.

$J_0(N)_\mathfrak{a} := J_0(N)[p^n] \otimes \mathbb{T}_\mathfrak{a}$ is finite length $\mathbb{T}_\mathfrak{a}$ module so it is killed by $\mathfrak{a}^m$.

Since $J_0(N)[p^n] \otimes \mathbb{T}_\mathfrak{a} \hookrightarrow J_0(N)[p^n]$, we see $J_0(N)[p^n]_\mathfrak{a} \subseteq J_0(N)[\mathfrak{a}^m]$.

Coro. 6: $f(0) \neq f(\infty)$.

proof: By prop3, $x = [0] - [\infty]$ is nontrivial torsion & $x \in J_0(N)[\mathfrak{a}]$

$\therefore$ $[0] - [\infty]$ is nontrivial in $A[\mathfrak{a}]$ as the above.

IV Estimate $A(\mathbb{Q})$

If we can show $A[p]$ satisfies $HJ(p)$ then we can use Thm 2, this is the case when all eigenform f has Fourier coefficient in $\mathbb{Z}$.

(In this case, $\mathbb{T}/\mathfrak{p}_f \xrightarrow{\sim} \mathbb{Z}$. If $\mathfrak{p}_f \subseteq \mathfrak{a}$ then $\mathfrak{a}$ is the unique max ideal above $\mathfrak{p}_f$. $A \simeq \prod_{\mathfrak{p}_f \subseteq \mathfrak{a}} A_f$ where $A_f = J_0(N)/\mathfrak{p}_f J_0(N)$ are ellipTic curve

& $A_f[p] \simeq A[\mathfrak{a}]$ is admissible).

But for general situation, we have to use $\mathbb{T}_\mathfrak{a}$-part of everything. Recall $\mathbb{T}_\mathfrak{a}$ is a direct summand of $\mathbb{T}_p$.

Lemma 7: suppose M is a finite $\mathbb{Z}$-module & $\mathbb{T}/I$-module. If

$$M \otimes_{\mathbb{T}} \mathbb{T}_\mathfrak{a} \text{ is finite then } M \text{ is finite.}$$

Now we apply the above Lemma $M = A(\mathbb{Q})$. Let $\mathcal{A}$ be the Néron model of with $\mathcal{A}^\circ$ the connected components. We aim to bound $A(\mathbb{Q}) \otimes_{\mathbb{T}} \mathbb{T}_{\mathfrak{n}}$ via similar method in Yifu Wang's talk.

Recall: Let G be admissible group scheme $/\mathbb{Z}$. (G will be $\mathcal{A}[p^n]$, $\mathcal{A}^\circ[p^n]$)

- $\ell(G) = \log_p |G|$.
- $\alpha(G) = \#$ of $\mathbb{Z}/p\mathbb{Z}$ occuring in G.
- $\delta(G) = \ell(G_{\mathbb{Q}}) - \ell(G_{\mathbb{F}_N})$
- $h^i(G) = H^i_{fppf}(\mathrm{spec}(\mathbb{Z}), G)$.

Indeed why $\mathcal{A}[p^n]$ flat $/N$? may be use explicit description $\mathcal{A}|_{\mathbb{F}_N}$.

Then $$h^1(G) - h^\circ(G) \leq \delta(G) - \alpha(G).$$

Now the issue is that $\mathcal{A}[p]$ may not satisfies $HJ(p)$. We have to look up
$$\mathcal{A}[p]_{\mathfrak{n}} = \mathcal{A}[p] \otimes_{\mathbb{T}_p} \mathbb{T}_{\mathfrak{n}} = \mathcal{A}[p] \cap \mathcal{A}[\mathfrak{n}^\infty].$$

Sketch the idea to bound $A(\mathbb{Q})_{\mathfrak{n}} = A(\mathbb{Q}) \otimes_{\mathbb{T}} \mathbb{T}_{\mathfrak{a}}$.

1. $\mathcal{A}[p^n]_{\mathfrak{n}}$ is admissible. we first devissge to reduced to the case $\mathcal{A}[\mathfrak{a}]$. This is generic fiber question. we look at $A[\mathfrak{n}]$ which contains $\mathbb{Z}/p\mathbb{Z}$ from $[0]-[\infty]$. $A[\mathfrak{n}]$ is stable under duality, as $\mathbb{T}$ is self-adjoint operator. so $A[\mathfrak{a}]^{ss} \simeq 1 \oplus \chi_p$. as required.

2. Let $d = \dim_{\mathbb{Q}_p} \mathbb{T}_{\mathfrak{a}}[\frac{1}{p}]$. Then $\alpha(\mathcal{A}[p^n]_{\mathfrak{n}}) = nd + O(1)$.
   use $\mathcal{A}[p^n]_{\mathfrak{a}}$ is self-dual & $\varprojlim_n \mathcal{A}[p^n]_{\mathfrak{a}} = T_p(A)_{\mathfrak{a}}$ which is a finite free $\mathbb{T}_p[\frac{1}{p}]$-module of rank 2.

3. To compute $\delta(\mathcal{A}[p^n]_{\mathfrak{n}})$, the key is to compute $\ell(\mathcal{A}[p^n]_{\mathfrak{a}}|_{\mathbb{F}_N})$ which can be reduced to estimate $V_N(A)^{I_N}_{\mathfrak{a}}$. where $V_N(A)$ is N-adic Tate module & I_N is inertia gp at N. Since A has toric reduction at N, $I_N \curvearrowright V_N(A)$ nilpotently, & indeed $(g-1)^2 = 0$, $\forall g \in I_N$. (using $V_N(A) \simeq \oplus P_{f,\lambda}$)
   $\Rightarrow$ $\dim(V_N(A)^{I_N}) = \frac{1}{2}\dim(V_N(A))$. similar happens to $V_N(A)^{I_N}_{\mathfrak{a}}$.
   $\therefore$ $\delta(\mathcal{A}[p^n]_{\mathfrak{a}}) = nd + O(1)$.
   $\therefore$ $h^1(\mathcal{G}_n) - h^\circ(\mathcal{G}_n) \leq \delta(\mathcal{G}_n) - \alpha(\mathcal{G}_n) = O(1)$.

where $\mathcal{G}_n = \mathcal{A}^\circ[p^n]_{\mathfrak{a}}$. Note $\mathcal{A}$ is replaced by $\mathcal{A}^\circ$ has no problem because a) α is only question on generic fiber A b) δ depends on $\mathcal{A}$ & $\mathcal{A}^\circ$ at N which is only different by $[\mathcal{A}|_{\mathbb{F}_N} : \mathcal{A}^\circ|_{\mathbb{F}_N}]$.

4) Now consider exact sequence $0 \to \mathcal{A}^\circ[p^n] \to \mathcal{A}^\circ \to \mathcal{A}^\circ \to 0$.

which gives $\mathcal{A}^\circ(\mathbb{Z}) \otimes \mathbb{Z}/p^n\mathbb{Z} \hookrightarrow H^1_{fppf}(\mathrm{Spec}(\mathbb{Z}), \mathcal{A}^\circ[p^n])$

Both sides are $\mathbb{T}_p$-algebra, so it makes sense to take $\mathbb{T}_{\mathfrak{a}}$-component,

so $\mathcal{A}^\circ(\mathbb{Z}) \otimes_{\mathbb{T}} \mathbb{T}_p \hookrightarrow \varprojlim H^1_{fppf}(\mathrm{Spec}(\mathbb{Z}), \mathcal{G}_n)$

whose size is bounded by $\delta(\mathcal{G}_n) - \alpha(\mathcal{G}_n) = O(1)$.

Since $\mathcal{A}^\circ(\mathbb{Z}) \subseteq \mathcal{A}(\mathbb{Z}) = A(\mathbb{Q})$ as finite index subgp,

$A(\mathbb{Q}) \otimes_{\mathbb{T}} \mathbb{T}_{\mathfrak{a}}$ is finite set as required.