Talk 1: Overview

Netan Dogra

Thm[1]: $E/\mathbb{Q}$ ell. curve, $P \in E(\mathbb{Q})_{tors}$ then $\mathrm{ord}(P) \leq 10$ or $= 12$. (& we can find possible torsion gps which arise)

- To prove Thm[1], we first reduce to to $\mathrm{ord}(P) = N$ is prime ≥ 11 & not 13 (Mazur–Tate)
- Suppose $E/\mathbb{Q}$ has a pt P of order N, consider

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

ISTS: this SES splits

「Why? If so, let $E_1 = E/\mu_N$ then $E_1[N]$ also has an SES

$$0 \to \mathbb{Z}/N\mathbb{Z} \to E_1[N] \to \mu_N \to 0$$

which also has to split, and so does $E_2 = E_1/\mu_N$ ⋯ ⇝ get ∞-many distinct EC/$\mathbb{Q}$ w/ good redn outside a fixed set of primes ↯ (Shafarevich)」

- ISTS: $[E[N]] \in \mathrm{Ext}^1_{G_{\mathbb{Q}}}(\mu_N, \mathbb{Z}/N\mathbb{Z}) = H^1(G_{\mathbb{Q}}, \mu_N^{-1})$ is unr. ⇔ the extn

$$\bar{\mathbb{Q}}^{\ker E[N]} =: L$$
$$K := \mathbb{Q}(\mu_N) \quad \text{is unr.}$$
$$\mathbb{Q}$$

「Unr. extns of $\mathbb{Q}(\mu_N)$ are classified by $Cl(\mathbb{Q}(\mu_N)) \cong Gal(\mathbb{Q}(\mu_N)/\mathbb{Q})$ & the ones coming from $H^1(\mathbb{Q}, \mu_N^{-1})$ corresp. to $Cl(\mathbb{Q}(\mu_N))^{\chi^{-1}}$ where χ is the cyclotomic char. ↯ (Herbrand)」

To prove that L/K is unr., we need global arguments, although the question is local.

✓ & $L = K$ as desired

Thm: E has semi-stab. redn at all primes.

「Why?

- Thm (Grothendieck): $A/\mathbb{Q}_p$ ab. var., $\ell \neq p$. Then A has semi-stab. redn at p ⇔ I_p ⊂ $T_\ell A$ unipotently.

⇝ can show that E has semi-stab. redn at $p \neq N$

- Hard case: $p = N$. (p. 158, [Maz 77])」

Now, E has semi-stab. redn. at every v, and let $\mathcal{E}$ be its Néron mod. wrt v

Consider

$$0 \to \mathcal{E}^\circ_{\mathbb{F}_v} \to \mathcal{E}_{\mathbb{F}_v} \to \mathcal{E}_{\mathbb{F}_v}/\mathcal{E}^\circ_{\mathbb{F}_v} \to 0$$

Φ torus $\quad$ Φ fin. gp.

Note that E has bad redn at 2 & 3. (point-counting argument); A has good redn at $p \Rightarrow A(\mathbb{Q}_p)_{tors} \hookrightarrow A(\mathbb{F}_p)$)

WTS: At all primes of bad redn, $P \notin \mathcal{E}^\circ_{\mathbb{F}_v}$. Note: At $2, 3, N$, we know that $P \notin \mathcal{E}^\circ_{\mathbb{F}_v}$ for elementary reasons. For other places, we need the theory of modular curves.

- $Y_1(N)$ & $Y_0(N)$ complex analytic
- $y_1(N)$ exact ord N $\quad$ $y_0(N)$ cyc. gp. ord N $\quad$ moduli spaces
- $S \mapsto (E|S, P)$ $\quad$ $S \mapsto (E|S, C)$
- $X_1(N)$ & $X_0(N)$: compactification (+ cusps)
- $x_1(N)$ $\quad$ $x_0(N)$: gen. ell. curves

Note: $0, \infty \in X_0(N)(\mathbb{Q})$.

Fact: $[(E, C)] \in X_0(N)(\mathbb{Q})$: If E has semi-stab. bad redn at $v \nmid N$, then $C \subset \mathcal{E}^\circ \Leftrightarrow \bar{Q} \equiv \bar{O}$ in $X_0(N)(\mathbb{F}_v)$

$C \not\subset \mathcal{E}^\circ \Leftrightarrow \bar{Q} \equiv \bar{\infty}$ in $X_0(N)(\mathbb{F}_v)$.

Given this fact, we are reduced to show: $P \in X_0(N)(\mathbb{Q})$, ℓ_1, ℓ_2 primes different from N. If $\bar{P} \equiv \bar{\infty}\ (\ell_1)$, then $\bar{P} \not\equiv \bar{O}\ (\ell_2)$.

To this end, suppose we had an ab. var. $A/\mathbb{Q}$ of $\mathrm{rk}\ 0$, good redn outside N, & a map

$$X_0(N) \xrightarrow{\tau} A \quad \text{s.t.} \quad \tau(0) \neq \tau(\infty).$$

Then

$$\begin{array}{ccc} X_0(N)(\mathbb{Q}) & \longrightarrow & A(\mathbb{Q}) \\ \downarrow & & \downarrow \iota \\ X_0(N)(\mathbb{F}_{\ell_i}) & \longrightarrow & A(\mathbb{F}_{\ell_i}) \end{array} \qquad A(\mathbb{Q})_{tors} = A(\mathbb{Q})$$

WLOG, $\tau(\infty) = O_A$ & $\bar{P} \equiv \bar{\infty}\ (\ell_1)$. Then injectivity of $\iota \Rightarrow \tau(P) = O_A$.

Similarly, $\bar{P} \equiv \bar{O}\ (\ell_2) \Rightarrow \tau(P) = \tau(0)$. Contradiction!

Q: How to find A?

See §I.3 [Maz 77] for a nice picture explaing this

There is an univ. map from X to an ab. var., sending a given $b \in X(k)$ to 0, which is

$$X \to Jac(X), \quad x \mapsto [x] - [b]$$

So, we are led to find a rk 0 quotient of Jacobian $J_0(N)$.

- If we map $X_0(N)$ to $J_0(N)$ via ∞, then the image of 0 is torsion (one can construct modular units in $\mathbb{Q}(X_0(N))^\times$ w/ divisor $n([\infty] - [0])$ where n = numerator $\left(\frac{N-1}{12}\right)$).
- $J_0(N) \sim \prod A_f$, $f \in$ "$S_2(\Gamma_0(N))$ normalized eigenform / $G_{\mathbb{Q}}$-action" $\leftrightarrow$
- $\not\exists\, L(A_f, s) = L(f, s) \Rightarrow$ a nat'l choice of the quotient would be those A_f's w/ f having analytic rk 0. Kolyvagin: This implies rk $A_f(\mathbb{Q}) = 0$.

Q: How to show that a quotient A of $J_0(N)$ has rk. 0?

- $A(\mathbb{Q}) \otimes \mathbb{F}_p \hookrightarrow H^1(G_{\mathbb{Q}}, A[p])$
- $X_0(N)$ has good redn outside $N \Rightarrow$

  $J_0(N)$ — " —

  A — " —

  $\rightsquigarrow$ can replace $G_{\mathbb{Q}}$ w/ $G_{\mathbb{Q}, \{N, p\}}$
- Choose / define A by requiring $A[p]$ is built out of simple pieces (μ_p & $\mathbb{Z}/p\mathbb{Z}$) + control what happens at p $\rightsquigarrow$ "flat descent"
- We know characteristic polys of Frob_ℓ on $V_p A_f$ in terms of the T_ℓ action on f (Eichler - Shimura)

  $\rightsquigarrow$ "Eisenstein ideal"