Shafarevich-Tate Groups of Elliptic Curves of Rank ≥ 2

talk notes

§1 Finiteness of Ш(E/ℚ)

E = elliptic curve/ℚ

$X = \{(E,p)$: rank$(E) \geq 2$, $Ш(E/\mathbb{Q})(p)$ finite$\}$

Conj: X is infinite. (since Ш(E/ℚ) is supposed to be finite)

Theorem (Bhargava, Ho, –):

(or $\#Ш(E/\mathbb{Q})[2] = \square$ for all E
[3] "
or rank$(E) \equiv r_{an}(E) \pmod 2$ all E) $\Rightarrow$ X is infinite

Fix E:

$X_E = \{p$: $Ш(E/\mathbb{Q})(p)$ finite$\}$

or

$X_E^\circ = \{p$: $Ш(E/\mathbb{Q})[p] = 0\}$

Conj: X_E is infinite

Strategies:
- Iwasawa theory / p-adic
- Heegner points

§1.1 p-adic Methods

Thm (Coates-Sujatha-Liang): E: $y^2 = x^3 - 82x$ (CM curve, rank = 3)

$X_E^\circ \supseteq \{p$: $p < 30000$ prime, $p \equiv 1 \pmod 4$, $p \neq 41\}$

"Thm" (Stein-Wuthrich): For all non-CM E with $N_E \leq 30{,}000$, $r_E \geq 1$,

(over 99% done) $X_E^\circ \supseteq \{p$: $5 \leq p \leq 1000$, p good ordinary, $\bar{\rho}_{E,p}$ surjective$\}$

Ex: E = 389a, rank 2

$X_E^\circ \supseteq \{p$: $5 \leq p \leq 1000$, $p \neq 107, 599\}$

So $\#X \geq 10^6$, at least...

I have No hope to show X infinite this way.

§1.2 Heegner Points

(13)

Thm (Kolyvagin only, 1980s): E = $X_0(17)$ Then Ш(E/ℚ) finite.

($r_E = 0$)

Proof: {Heegner points on $X_0(17)$} ⇝ {cohomology classes in $H^1(K, E[p^\infty])$} ↪ {uniform bound on Ш(E

Does not use Gross-Zagier, Wiles, etc.!

Hope: Extend to show X_E infinite for an E of rank 2?

§2. Heegner Points on 389a

E 389a $E(\mathbb{Q}) = \mathbb{Z}(-1,1) \oplus \mathbb{Z}(0,0)$ (P, Q)

$K = \mathbb{Q}(\sqrt{-7})$ · class number 1 · N=389 splits

$\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/389\mathbb{Z}$

$r_{an}(E/K) = 3$

$X = X_0(389)$ genus 32

$x_1 = (\mathbb{C}/\mathcal{O}_K, \mathcal{N}^{-1}/\mathcal{O}_K) \in X(K)$

Φ_E deg 40

E

$0 = y_1 \in E(K)$

$p \in I$ = inert primes = $\{3, 5, 13, 17, 19, \ldots\}$ ($3, 5, 6 \pmod 7$)

$\mathcal{O}_p = \mathbb{Z} + p\mathcal{O}_K$, $\mathcal{N}_p = \mathcal{O}_p \cap \mathcal{N}$.

$x_p = (\mathbb{C}/\mathcal{O}_p, \mathcal{N}_p^{-1}/\mathcal{O}_p) \in X(K_p)$

$y_p \in E(K_p)$

Thm (–): For all $p \in I$, y_p has infinite order.

Proof: $E(K_p)_{tor} = 0$ by Galois theory, so y_p torsion $\Rightarrow y_p = 0$.

X $x_p, \sigma(x_p), \ldots$ $2(p+1)$ $\mathrm{Gal}(K_p/\mathbb{Q})$-conjugates by CM theory

Φ_E

E 0

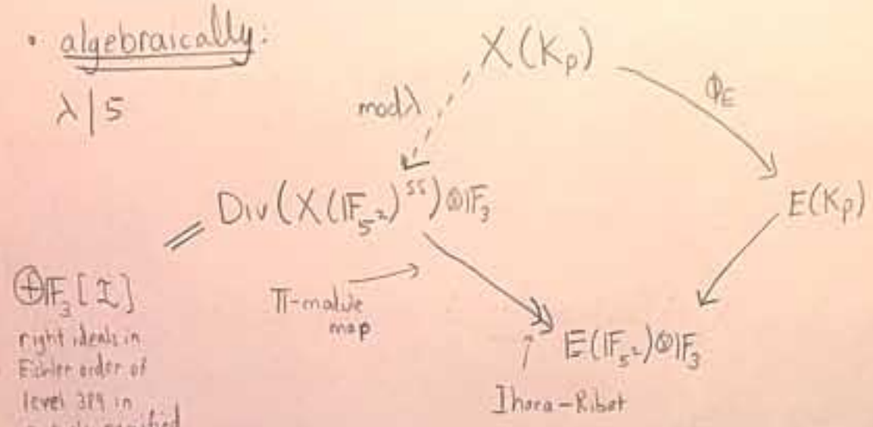
But $40 = \deg(\Phi_E) \geq \Phi_E^{-1}(0) \geq 2(p+1)$

so $p \leq 19$

Check each $p \leq 19$:

- numerically, e.g., $y_3 \sim (.63-.73i, -.47+.63i) \neq 0$ FAST
- algebraically:

$\lambda | 5$



SLOW (but groundbreaking)

(see [Jetchev-Lauter-Stein, §3])

But $\mathrm{Tr}_{K_p/K}(y_p) = 0 \in E(K)$...

§3. Elements of Selmer. E is still 389a.

n positive integer. M number field

$$0 \to E(M)/nE(M) \xrightarrow{\delta} Sel^{(n)}(E/M) \to Ш(E/M)[n] \to 0$$

$$\cap\!| \qquad\qquad \cap\!|$$

$$H^1(M, E[n]) \to H^1(M, E)[n] \to$$

§1.

For $p \in I$, let $n_p = \gcd(p+1, \#E(\mathbb{F}_p))$.

p	3	5	13	17	19
n_p	2	3	1	6	5

$\mathrm{Gal}(K_p/K) = \langle \sigma_p \rangle$ choice

$$\left[\sum_{i=1}^{p} i\sigma_p^i(y_p)\right] \in \left(E(K_p)/n_pE(K_p)\right)^{\mathrm{Gal}(K_p/K)} \xrightarrow{c\,\delta} H^1(k_p, E[n_p])^{\mathrm{Gal}(K_p/\mathbb{Q})}$$

$$\uparrow \wr$$

$$H^1(\mathbb{Q}, E[n_p])$$

$$\cup\!|$$

$$T_p \in Sel^{(n_p)}(E/\mathbb{Q})$$

Theorem (Kolyvagin)

- $\ell \mid \mathrm{order}(T_p)$ for some $p \in I \Rightarrow Ш(E/\mathbb{Q})(\ell)$ finite
- $\mathrm{ord}_\ell(\mathrm{order}(T_p)) = \mathrm{ord}_\ell(n_p) > 0 \Longrightarrow Ш(E/\mathbb{Q})[\ell] = 0$.

Conj_ℓ (Kolyvagin): There's p with $\ell \mid \mathrm{order}(T_p)$...

$\mathrm{Conj}_\ell \Rightarrow X_E$ infinite (would be a major result!)

§4: Kolyvagin's conjecture: ideas.

(a): [Jetchev-Lauter-Stein] nonrigorous numerical comp of T_5

"$\mathrm{order}(T_5) = 3$"

(b) [-]: new paper. Use idea of algebraic proof above to prove

$\mathrm{ord}_w(T_5) = 3$
$\mathrm{order}(T_{19}) = 5$

(and similar for dozen curves)
various K

Prop: $X_E^0 \supseteq \{3,5\}$). (not as impressive as p-adic result)

(c) [-]: congruences/visibility. (37 splits in K)

$\exists f_E \equiv_3 g \in S_2(\Gamma_0(389 \cdot 37))$

$\updownarrow$

$F: 14313.1$, $r_F = 0$, $Ш(F/K) \simeq (\mathbb{Z}/3\mathbb{Z})^2$,

$T_{E,5} \to T_{F,5} \neq 0$ (since $r_{an}(F/K) = 1$ and $Ш(F/K)(3) \neq 1$) $\Rightarrow T_{E,5} \neq 0$.

This strategy generalizes: Main input $\#Ш(F/K) \geq \#Ш(F/K)_{an}$ (3)-part version