

1. The BSD Conjecture

E : "389a" $y(y+1) = x(x-1)(x+2)$

$E(\mathbb{Q}) = \langle (0,0), (-1,1) \rangle \cong \mathbb{Z}^2$

$r_{\text{alg}} = 2$

$r_{\text{an}} = \text{ord}_{s=1} L(\bar{E}, s) = 2$

$c_{389} = 1$ Tamagawa number

Contents:

1. The BSD Conjecture
2. The BSD Template
3. Computing Kolyvagin Classes
4. Generalizing Gross-Zagier

(Switch board) E/\mathbb{Q} any elliptic curve

Conj (BSD):

- $r_{\text{alg}} = r_{\text{an}}$
- $L^{(n)}(E/\mathbb{Q}, 1)/r! = \text{Reg}(E/\mathbb{Q}) \cdot \prod c_p \cdot \Omega_E \cdot \#III(E) \cdot \#E(\mathbb{Q})_{\text{tor}}^{-2}$

Theorem (Gross, Zagier, Kolyvagin, Wiles, --- Bump, Breuil, Conrad, Diamond, Taylor)

$r_{\text{an}} \leq 1 \Rightarrow r_{\text{alg}} = r_{\text{an}}$ and algorithm to verify formula.
nonpractical (!)

Theorem (-) ^{Students}: BSD (E, p) true for $N_E \leq 1000$, $r_{\text{alg}} \leq 1$, $\bar{P}_{E,p}$ irred, E non CM, $p \mid \prod c_q$.

See my Math. Comp. 2009 paper.
 Being extended by Robert Miller now (Ph.D. thesis)

Prop (Boothby & Bradshaw): Formula to 10,000 digits, assuming $\#III(E) = 1$.

[1-week calculation; 10^6 digits takes million weeks]

[Ad: Provable Dokchitser... (Bradshaw thesis)]

Prop (Stein-Wuthrich): $III(E)[p] = 0$ for $p < 2466$ ordinary (excludes $p=107, 599, 1049$)

Use: modular symbols, p -adic L-series, p -adic heights (new Mazur-Stein-Tate alg), Kato's theorem, Schneider's theorem, ... and Sage!

§ 2. The BSD Template

$$\boxed{r_{an}(E^D) \leq 1}$$

$K = \mathbb{Q}(\sqrt{D})$ s.t. $l \mid N \Rightarrow l$ splits,

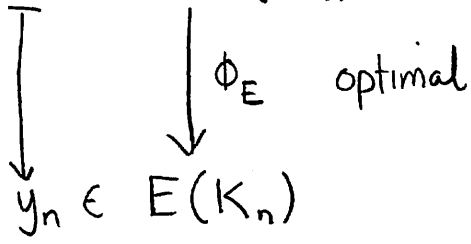
$n \in \mathbb{Z}$ coprime to N

$$\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$$

$I \subseteq \mathcal{O}_K$ s.t. $\mathcal{O}_K/I \cong \mathbb{Z}/N\mathbb{Z}$

$$I_n = I \cap \mathcal{O}_n$$

$$(\mathcal{O}/\mathcal{O}_n, I_n^{-1}/\mathcal{O}_n) = x_n \in X_0(N)(K_n)$$



constellation of Heegner points over class fields

Case $r_{an}(E/\mathbb{Q}) \leq 1$:

Gross-Zagier: $P_1 = \text{Tr}_{K_1/K}(y_1) \in E(K)$



Kolyvagin:

$$\{y_n\} \rightsquigarrow \{\tau_n\} \subseteq H^1(K, E[p^\infty])$$

$\xrightarrow{\text{thm}}$ rank $(E(K)) \leq 1$ with equality $\Leftrightarrow \text{III}(E/K)(p)$ finite.

"philosophy: compare w/ BSD" (ignore Manin constant)

$$\Omega_E \cdot \Omega_{E^D/\mathbb{C}^\times}$$

$$L'(E/K, 1) \stackrel{\text{Thm}}{=} \text{Reg}_1(\langle P_1 \rangle) \cdot \Omega_{E/K}$$

Case $r_{an}(E/\mathbb{Q}) = 2$:

Gross-Zagier: $\langle P_1 \rangle \subseteq E(K)$ for

Generalize: $\frac{L^{(3)}(E/K, 1)}{3!} \stackrel{\text{conj}}{=} \text{Reg}_3(W_\ell) \cdot \Omega_{E/K}$

Define using all P_A 's somehow.

trivial rank $(E(K)) \geq 3$

Kolyvagin: Hypothesis: some $\tau_\ell \neq 0 \xrightarrow{\text{Thm}}$ rank $(E(K)) \leq 3$

equality $\Leftrightarrow \text{III}(E/K)(p)$ finite

(over - Mazur quote)

Mazur: "Things become particularly interesting, not when templates fit perfectly, but rather when they don't quite fit, and yet despite this, their explanatory force, their unifying force, is so intense that we are impelled to recognize the very constellation they are supposed to explain, so as to make them fit."

— Visions, Dreams, and Mathematics

(in fact an article about CM elliptic curves!)

& Kronecker's dream

I am impelled to make this template fit.

§3. Computing Kolyvagin Classes

• E 389 a again, $K = \mathbb{Q}(\sqrt{-7})$

First ever!

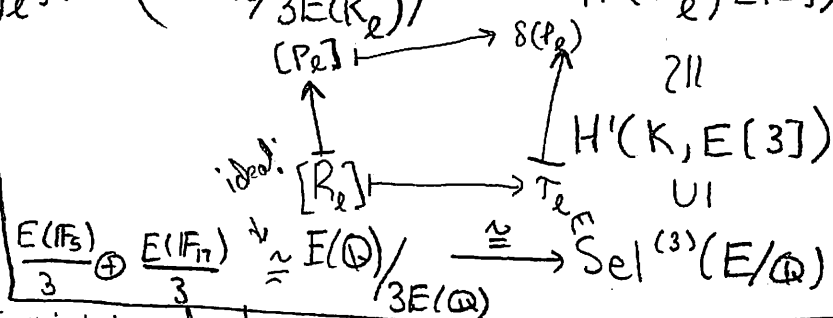
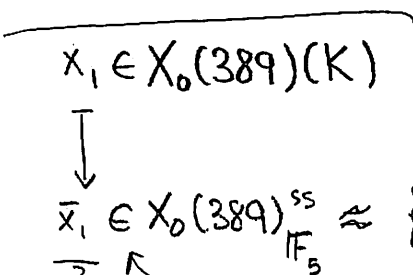
(also same for some other curves and $p=3,5,7$)

Theorem (-): $0 \neq T_\ell \in \text{Sel}^{(3)}(E/\mathbb{Q})$ for many ℓ .

ℓ inert in K with $3 \nmid \gcd(a_\ell, \ell+1)$.

$G = \text{Gal}(K \xleftarrow{\text{ring class field}} / K) = \langle \sigma \rangle$ (order $\ell+1$)

$[P_\ell] = \sum_{i \in \mathbb{Z}/\ell+1\mathbb{Z}} i \sigma^i([y_\ell]) \in (E(K)/3E(K))^G \xrightarrow{\delta} H^1(K_\ell, E[3])^G$



• compute \bar{x}_1 by finding $\mathcal{O}_K \hookrightarrow I$ using ternary forms.

(motivation: [Jatkech-Kane], [Gross], [Cornut], [Vatsal])

$[P_\ell] = \sum i \sigma^i(x_\ell) \in \bigoplus \mathbb{Z}[I]$

• compute $[P_\ell]$ by unwinding def'n's. Surprised it worked!
 Since no direct Galois action!

$*R_\ell \in E(\mathbb{F}_5)/3E(\mathbb{F}_5)$

Use $\mathcal{O}_K \hookrightarrow I$; $\sigma \leftrightarrow \alpha \in (\mathcal{O}_K/\ell\mathcal{O}_K)^* / (\mathbb{Z}/\ell\mathbb{Z})^*$

• compute using linear algebra, Hecke actions, $3 \mid \deg(\Phi_E)$, and Ihara's theorem. (same idea as Cornut, made explicit)

Trac #6616

ℓ	5	17	41	59	83	173	227	269	479	503
$\bar{r}_{\ell,0}$	$*(1,1)$	$(0,0)$	$(1,2)$	$(0,1)$	$(1,2)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(1,1)$ ← <u>some basis!</u>

Theorem (Rubin, -, J. Weinstein) 2. Characterize $T^* T_\ell = \delta(*R_\ell)$ in terms of

3-division polynomials of basis of $E(K)/3E(K)$. Get density result (explains $(0,0)$'s).

- Next:
- rank 3 curve — T_{ℓ_1, ℓ_2}
 - ab. varieties
 - less hypo.
 - $h_K \neq 1$.

§4. Generalizing Gross-Zagier

"It is always a good idea to try to prove true theorems."

• My Ribet conference talk,

$$E, r_{an} \geq 1$$

D s.t. $r_{an}(E^p) \leq 1$. $D \leq -5$ Heegner hypothesis.

p prime

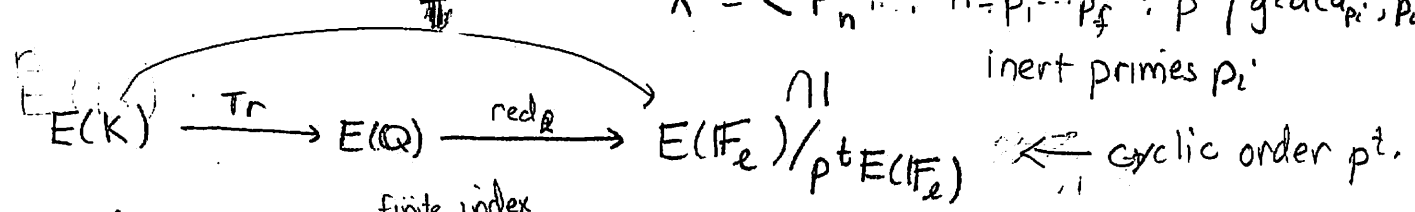
l inert prime

$$p^t \parallel \gcd(a_e, l+1)$$

$$f = r_{an}(E/\mathbb{Q}) - 1$$

$$X = \langle \bar{P}_n \dots : n = p_1 \dots p_f : p^t \mid \gcd(a_{p_i}, p_i+1) \rangle$$

inert primes p_i



$$W_e = \pi^{-1}(X), \subseteq E(K)$$

finite index.

Theorem (-): Assume p odd s.t. $\bar{\rho}_{E,p}$ surjective

- BSD conj
- Koly. conj⁺

If $[E(K):W_e]$ maximal (among all W_e) then

$$\frac{L^{(r)}(E/K, 1)}{r!} = \text{Reg}_r(W_e) \times \Omega_{E/K}^{\times} \text{ (p-adic unit)}$$

$$[r = r_{an}(E/K)]$$

Plans: • $E \rightsquigarrow$ modular abvar. A_f

- all primes p .

** \rightarrow • construct in $J_1(N)$ over K_1 like Gross-Zagier. \leftarrow **

(example \rightarrow)

$$\text{Reg}_r(W) = \text{Reg}(\wedge^r W).$$

Example:

$$E: 53,295,337a \quad y^2 + xy = x^3 - x^2 + 94x + 9$$

$$E(\mathbb{Q}) = \langle (10,3), (8,31) \rangle$$

$$P_1 \quad P_2$$

$$W_{167} = \langle 3P_1, P_2 \rangle \subseteq \frac{1}{3} E(K)$$

$$W_{503} = \langle 3P_1, 8P_1 + P_2 \rangle \subseteq \frac{1}{2} E(K)$$

Numerically

$$\frac{L^{(3)}(E/K, 1)}{3!} \doteq \text{Reg}(W_{167}) \cdot \Omega_{E/K}.$$