2009-11-04 (1)
William Stein

§1. The BSD Conjecture

Contents:

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

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

$r_{alg} = 2$

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

$c_{389} = 1$ Tamagawa number

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

Conj (BSD):

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

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

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

Theorem (– + students): BSD(E,p) true for $N_E \leq 1000$, $r_{alg} \leq 1$, $\bar{\rho}_{E,p}$ 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 $\#Ш(E)=1$.

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

[Ad: Provable Dokchitser ... (Bradshaw thesis)]
(general motivic L-functions)

Prop (Stein-Wuthrich): $Ш(E)[p]=0$ 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!

2099-11-04 ②
William Stein

§2. The BSD Template

$K = \mathbb{Q}(\sqrt{D})$ s.t. $\ell \mid N \Rightarrow \ell$ splits, $\boxed{r_{an}(E^D) \le 1}$

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

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

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

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

constellation of Heegner points over class fields

$$\begin{array}{ccc} (\mathbb{C}/\mathcal{O}_n,\ I_n^{-1}/\mathcal{O}_n) = x_n & \in & X_0(N)(K_n) \\ \downarrow & & \downarrow \phi_E \text{ optimal} \\ y_n & \in & E(K_n) \end{array}$$

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

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

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

$\Omega_E \cdot \Omega_{E^D}/c_\infty$

$L'(E/K,1) \overset{\text{Thm}}{=} \mathrm{Reg}_1(\langle P_1\rangle)\cdot \Omega_{E/K} \Longrightarrow \mathrm{rank}(E(K)) \ge 1$

$E(K)$

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

$\overset{\text{thm}}{\Longrightarrow} \mathrm{rank}(E(K)) \le 1$ with equality $\Leftrightarrow$ Ш$(E/K)(p)$ finite.

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

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

~~Define~~ using all P_n's somehow.

Generalize: $\dfrac{L^{(3)}(E/K,1)}{3!} \overset{\text{conj}}{=} \mathrm{Reg}_3(W_\ell)\cdot \Omega_{E/K} \overset{\text{trivial}}{\Longrightarrow} \mathrm{rank}(E(K)) \ge 3$

Kolyvagin: Hypothesis: some $\tau_\ell \ne 0 \overset{\text{Thm}}{\Longrightarrow} \mathrm{rank}(E(K)) \le 3$

equality $\Leftrightarrow$ Ш$(E/K)(p)$ 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.

2009-11-04

W. Stein

③

§3. Computing Kolyvagin Classes

First ever!

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

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

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

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

$G = \mathrm{Gal}(K_\ell/K) = \langle\sigma\rangle$ (order $\ell+1$), where K_ℓ is the ring class field.

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

$$\begin{array}{ccc}
[P_\ell] & \longmapsto & \delta(P_\ell) \\
\uparrow & & \uparrow \\
 & & H^1(K_\ell, E[3])^G \cong H^1(K, E[3]) \\
 \text{ideal: } [R_\ell] & \longmapsto & \tau_\ell \in \\
 & & \cup \\
\frac{E(\mathbb{F}_5)}{3} \oplus \frac{E(\mathbb{F}_{17})}{3} \cong E(\mathbb{Q})/3E(\mathbb{Q}) & \xrightarrow{\cong} & \mathrm{Sel}^{(3)}(E/\mathbb{Q})
\end{array}$$

$x_1 \in X_0(389)(K)$

$\downarrow$

$\bar{x}_1 \in X_0(389)^{ss}_{\mathbb{F}_5} \approx \{\text{right ideal classes } [I] \text{ in Eichler order}\}$

- compute $\bar{x}_1$ by finding $\mathcal{O}_K \hookrightarrow I$ using ternary forms.
  (motivation: [Jetchev-Kane], [Gross], [Cornut], [Vatsal])

$\downarrow$

$[\bar{P}_\ell] = \sum i\sigma^i(\bar{x}_\ell) \in \bigoplus \mathbb{Z}[I]$

- compute $[\bar{P}_\ell]$ by unwinding defn's. Surprised it worked, since no direct Galois action!!
  Use $\mathcal{O}_K \hookrightarrow I$; $\sigma \leftrightarrow \alpha \in (\mathcal{O}_K/\ell\mathcal{O}_K)^*/(\mathbb{Z}/\ell\mathbb{Z})^*$, $\alpha \longmapsto \bar{x}(\alpha)$

$\downarrow$

$*\bar{R}_\ell \in E(\mathbb{F}_5)/3E(\mathbb{F}_5)$

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

Trac #6616

ℓ	5	17	41	59	83	173	227	269	479	503
$\tau_{\ell,\sigma}$	*(1,1)	(0,0)	(1,2)	(0,1)	(1,2)	(0,0)	(0,0)	(0,0)	(0,0)	(1,1)

← Some basis!

Theorem (Rubin, −, J. Weinstein): Use B. Howard's thesis + reciprocity law to characterize $\tau_\ell = \delta(*R_\ell)$ in terms of 3-division polynomials of basis of $E(K)/3E(K)$. Get density result (explains (0,0)'s).

Next:
- rank 3 curve — $\tau_{\ell_1\ell_2}$
- ab. varieties
- less hypo.
- $h_K \neq 1$.

§4. Generalizing Gross–Zagier

- "It is always a good idea to try to prove true theorems." – Birch, when we were walking through a field in Durham, UK 1998
- My Ribet conference talk.

E, $r_{an} \geq 1$

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

p prime

ℓ inert prime

$p^t \,\|\, \gcd(a_\ell, \ell+1)$

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

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

$$\begin{array}{c} \\ E(K) \xrightarrow{\mathrm{Tr}} E(\mathbb{Q}) \xrightarrow{\mathrm{red}_\ell} \end{array} \begin{array}{c} \cap\!| \\ E(\mathbb{F}_\ell)/p^t E(\mathbb{F}_\ell) \end{array} \twoheadleftarrow \text{cyclic order } p^t.$$

$W_\ell = \pi^{-1}(X) \underset{\text{finite index}}{\subseteq} E(K)$

Theorem (–): Assume • p odd s.t. $\bar{\rho}_{E,p}$ surjective
• BSD conj
• Koly. conj$^+$.

If $[E(K) : W_\ell]$ maximal (among all W_ℓ) then

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

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

Plans: • $E \rightsquigarrow$ modular abrvar. A_f
• all primes p.

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

(example $\rightarrow$)

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

Example:

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

$E(\mathbb{Q}) = \langle \underset{P_1}{(0,3)}, \underset{P_2}{(8,31)} \rangle$

$W_{167} = \langle 3P_1, P_2 \rangle \underset{3}{\subsetneq} E(K)$

$W_{503} = \langle 3P_1, 8P_1+P_2 \rangle \underset{3}{\subsetneq} E(K)$

Numerically

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