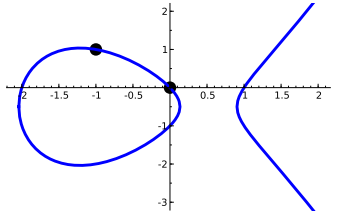
# The Birch and Swinnerton-Dyer Conjecture: A Template

http://www.wstein.org

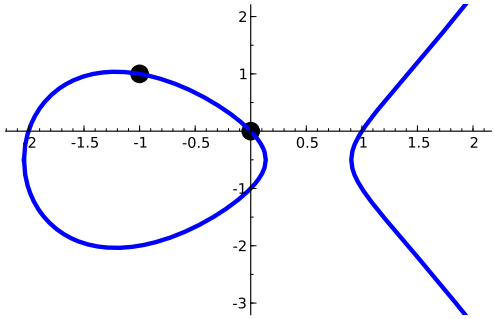
William Stein[1]

[1]Department of Mathematics
University of Washington, Seattle

January 14, 2010



# The Rank 2 Curve 389a




$$E : \mathbf{y(y+1) = x(x-1)(x+2)}$$

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

$$L(E,s) = \sum \frac{a_n}{n^s} \qquad \text{(Hasse-Weil } L\text{-series)}$$

$$r_{\text{alg}} = 2 \qquad \text{(algebraic rank)}$$

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

$$c_{389} = 1 \qquad \text{(Tamagawa number)}$$

# The BSD Conjecture

Let $E/\mathbb{Q}$ be any elliptic curve.

**Conjecture (Birch and Swinnerton-Dyer)**

We have $r_{\text{alg}} = r_{\text{an}}$ and (for $r = r_{\text{an}}$)

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

**Theorem (Gross-Zagier, Kolyvagin, Wiles, Bump, et al.)**

*If $r_{\text{an}} \leq 1$ then $r_{\text{alg}} = r_{\text{an}}$ and there is a* **not-necessarily-practical** *algorithm to verify the formula.*

Proof uses modularity of elliptic curves (Wiles et al.), Heegner points (Birch, Gross-Zagier, et al.), Euler systems (Kolyvagin), and results about nonvanishing of twists (Bump, Murty, et al.).

# Explicit Verification: Rank $\leq 1$

BSD is almost known for curves of conductor $\leq 1000$ of rank $\leq 1$:

**Theorem (–)**

*BSD formula holds at all primes $\ell$ for all non-CM elliptic curves $E$ with conductor $\leq 1000$, rank $\leq 1$, $E[\ell]$ irreducible, and $\ell \nmid \prod c_p$.*

- [Stein, 2009 Math. Comp.] Use 2-descent, 3-descent, refinements of Kolyvagin's Euler system, Kato's Euler system, and many computer computations (with Sage).
- Currently being extended by my Ph.D. student, Robert Miller.

# Explicit Verification: Rank 2

BSD formula not known for a single curve of rank $\geq 2$.
BSD rank not known for a single curve of rank $\geq 4$.
$E$: 389a above; has **rank** 2.

**Proposition (Boothby, Bradshaw)**

BSD holds to 10,000 decimal digits, assuming $\#Ш(E) = 1$.

About 1 week CPU time; complexity $O(\text{prec}^3)$, so a million digits might take a million weeks CPU time.

**Proposition (Stein-Wuthrich)**

$Ш(E)[p] = 0$ for all primes $p < 2466$ except possibly $p = 107, 599,$ and 1049 (these are non-ordinary).

Use modular symbols, $p$-adic $L$-series, $p$-adic heights (new Mazur-Stein-Tate algorithm), Iwasawa theory, Kato's theorem, Schneider's theorem, and Sage!

# The Proof Template: Rank $\leq 1$

**Kolyvagin's bright idea:** Prove BSD over $K$ instead.

- $K = \mathbb{Q}(\sqrt{D})$ quadratic imag. field such that all $p \mid N$ split and $L'(E/K, 1) \neq 0$,
- **Heegner points:** $y_n \in E(K[n])$, $K[n]$ = ring class field,
- $y_K = \mathrm{Tr}_{K[1]/K}(y_1) \in E(K)$.

**Bound from below:**

**Theorem (Gross-Zagier, 1980s)**

$L'(E/K, 1) = h(y_K) \cdot \Omega_{E/K} \implies \mathrm{rank}(E(K)) \geq 1$ *(big calculation)*

**Bound from above:**

**Theorem (Kolyvagin, 1980s)**

$h(y_K) \neq 0 \implies \mathrm{rank}\, E(K) \leq 1$ *(using Euler systems)*

But if rank $\geq 2$ then $h(y_K) = 0$, so this doesn't work!!

# Generalization of the Proof Template: Rank $\geq 2$

**New definition (!):** $y_K \in \bigwedge^r E(K)$, where $r = \mathrm{ord}_{s=1} L(E/K, s)$.

**Bound from below:**

**Conjecture (-)**

$L^{(r)}(E/K, 1)/r! = h(y_K) \cdot \Omega_{E/K}$

**Theorem (Kolyvagin, -)**

$h(y_K) \neq 0 \implies \bigwedge^r E(K)$ *nontorsion* $\implies \mathrm{rank}(E(K)) \geq r.$

**Bound from above:**

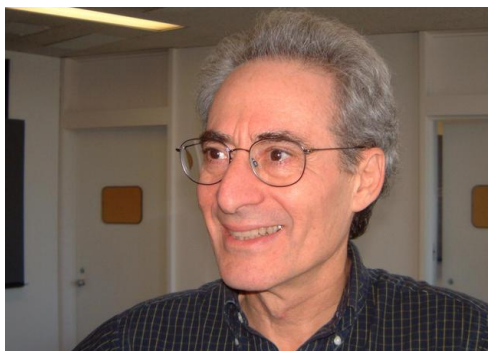
**Theorem (Kolyvagin, -)**

$h(y_K) \neq 0 \implies \mathrm{rank}\, E(K) \leq r$ *(Euler systems)*

# When Templates Don't Quite Fit

*"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."*

– *Barry Mazur,* Visions, Dreams, and Mathematics



The above "template" has led to many new definitions, algorithms, and interesting questions...