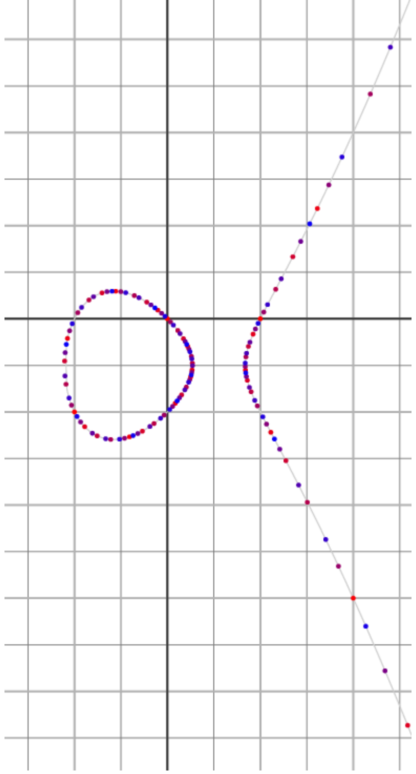
Verifying the Birch and Swinnerton-Dyer Conjecture for Specific Elliptic Curves

William Stein
Harvard University
`http://modular.fas.harvard.edu/talks/bsd2005ucsd/`

UCSD: February 1, 2005

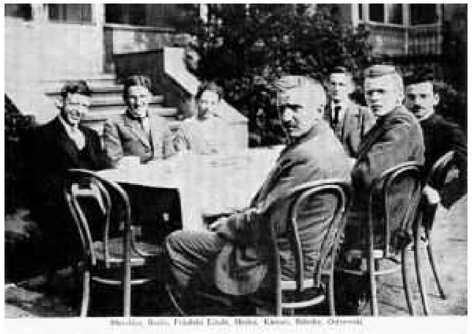


This talk reports on a project to verify the Birch and Swinnerton-Dyer conjecture for all elliptic curves over $\mathbb{Q}$ in John Cremona's book.

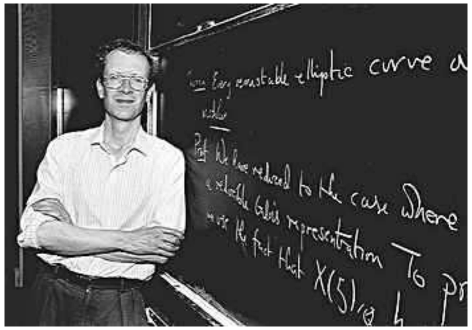
Joint Work: Stephen Donnelly, Andrei Jorza, Stefan Patrikis, Michael Stoll.

Thanks: John Cremona, Ralph Greenberg, Grigor Grigorov, Barry Mazur, Robert Pollack, Nick Ramsey, and Tony Scholl.

Birch and Swinnerton-Dyer (Utrecht, 2000)



The L-Function



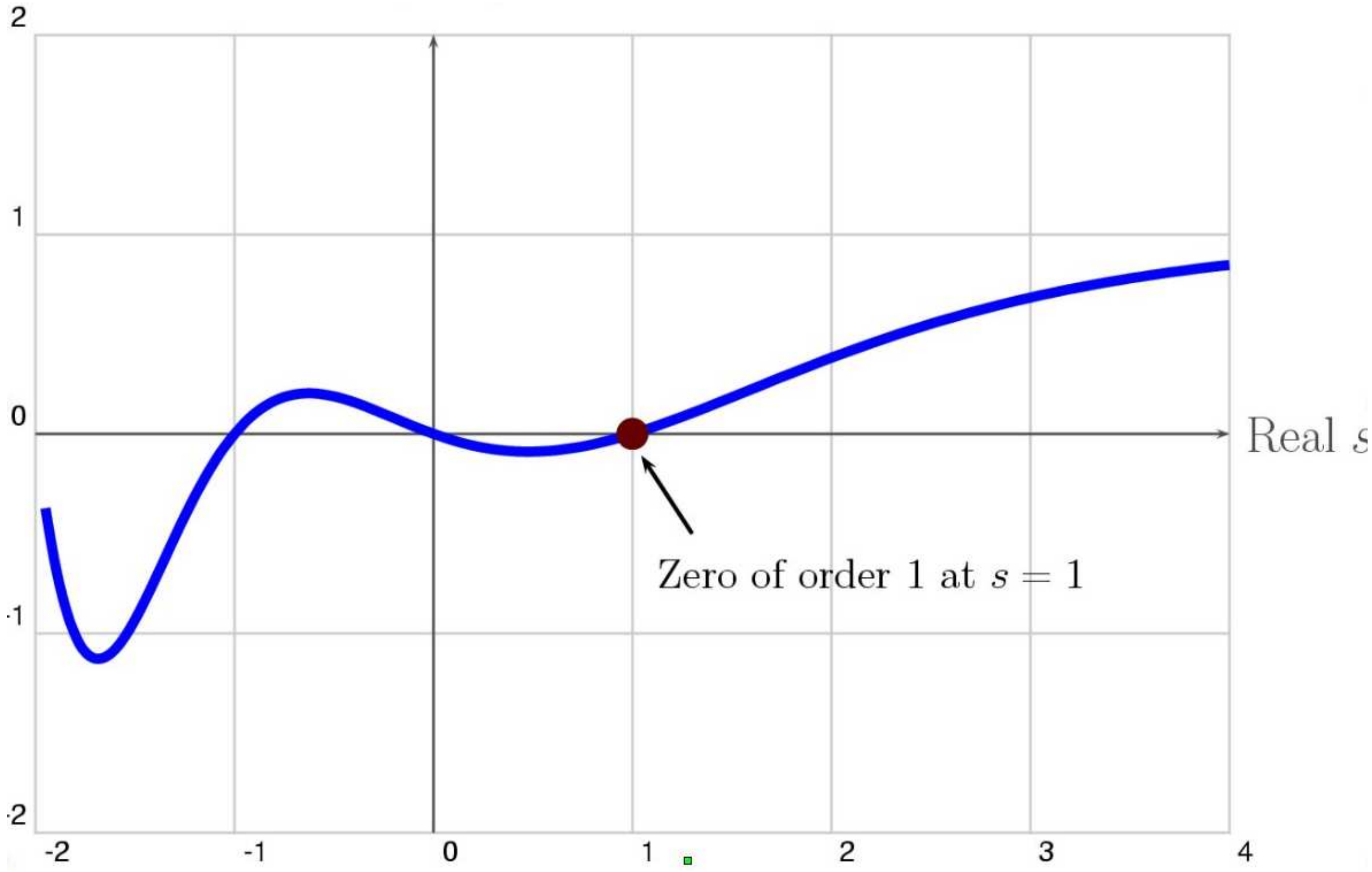
Theorem (Wiles et al., Hecke) The following function extends to a holomorphic function on the whole complex plane:

$$L(E,s) = \prod_{p \nmid \Delta} \left(\frac{1}{1 - a_p \cdot p^{-s} + p \cdot p^{-2s}} \right).$$

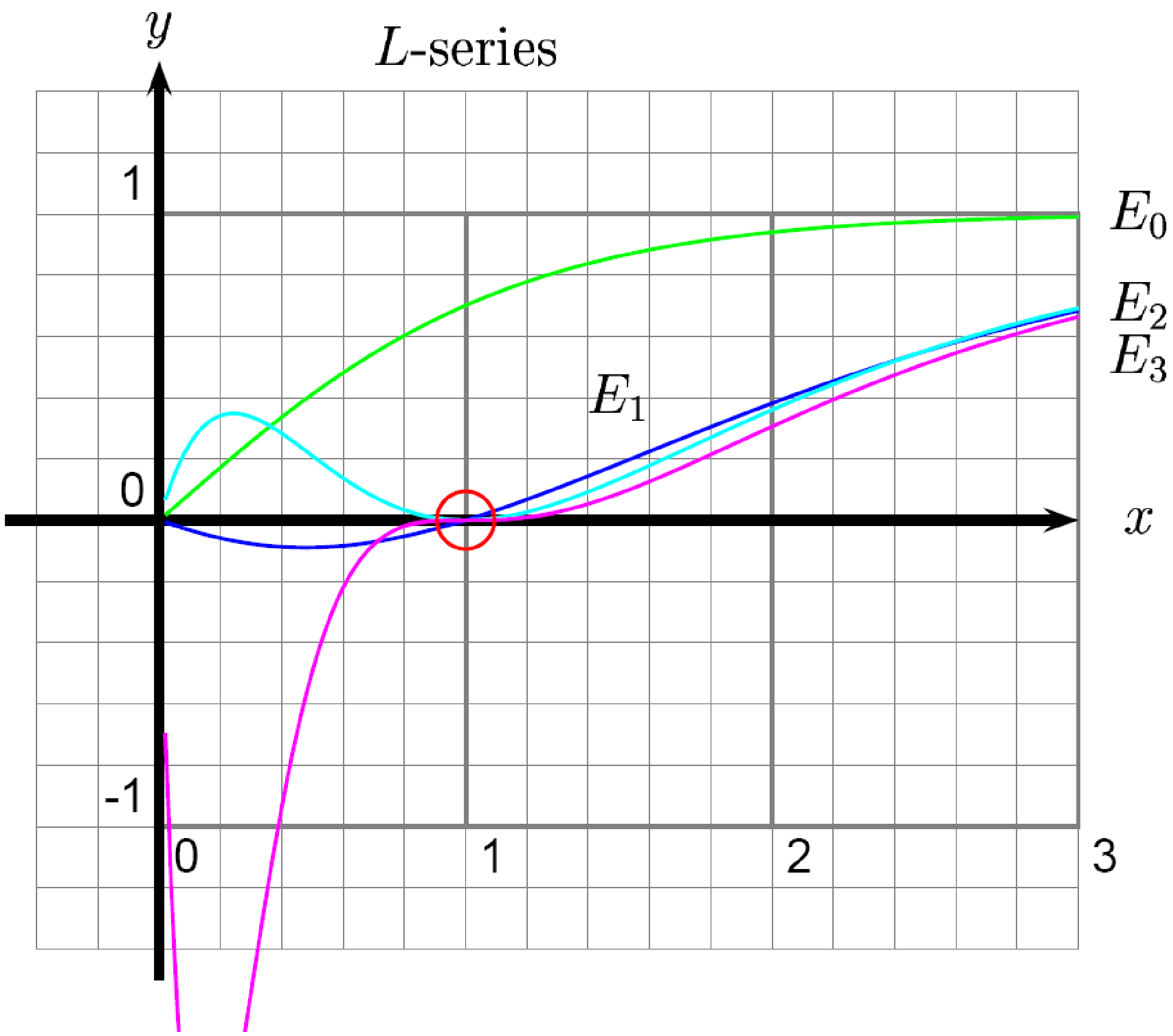
Here $a_p = p + 1 - \#E(\mathbb{F}_p)$ for all $p \nmid \Delta_E$. Note that formally,

$$L(E,1) = \prod_{p \nmid \Delta} \left(\frac{1}{1 - a_p \cdot p^{-1} + p \cdot p^{-2}} \right) = \prod_{p \nmid \Delta} \left(\frac{p}{p - a_p + 1} \right) = \prod_{p \nmid \Delta} \frac{p}{N_p}$$

Real Graph of the L-Series of $y^2+y=x^3-x$



More Graphs of Elliptic Curve L-functions



The Birch and Swinnerton-Dyer Conjecture

Conjecture: Let E be any elliptic curve over $\mathbb{Q}$. The order of vanishing of $L(E,s)$ as $s=1$ equals the rank of $E(\mathbb{Q})$.

The Kolyvagin and Gross-Zagier Theorems

Theorem: If the ordering of vanishing $\mathrm{ord}_{s=1} L(E, s)$ is ≤ 1, then the conjecture is true for E.

The Birch and Swinnerton-Dyer **Formula**

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega_E \cdot \mathrm{Reg}_E \cdot \prod_{p|N} c_p}{\#E(\mathbb{Q})^2_{\mathrm{tor}}} \cdot \#\text{Ш}(E)$$

1. $L(E,s)$ is an entire L-function that encodes $\{\#E(\mathbb{F}_p)\}$, p prime.
2. $\#E(\mathbb{Q})_{\mathrm{tor}}$ – **torsion** order
3. c_p – **Tamagawa numbers**
4. Ω_E – **real volume** $\int_{E(\mathbb{R})} \omega_E$
5. Reg_E – **regulator** of E
6. $\text{Ш}(E) = \mathrm{Ker}(\mathrm{H}^1(\mathbb{Q}, E) \to \bigoplus_v \mathrm{H}^1(\mathbb{Q}_v, E))$ – **Shafarevich-Tate group**

Motivating Problem 1

Motivating Problem 1. Compute every quantity appearing in the BSD conjecture **in practice.**

NOTES:

1. This is **not** meant as a theoretical problem about computability, though by compute we mean "compute with proof."

2. I am also very interested in the same question but for modular abelian varieties.

Status

1. When $r_{\text{an}} = \text{ord}_{s=1} L(E,s) \leq 3$, then we can compute r_{an}.
   Open Problem: Show that $r_{\text{an}} \geq 4$ for some elliptic curve.

2. Relatively "easy" to compute $\#E(\mathbb{Q})_{\text{tor}}$, c_p, Ω_E.

3. Computing Reg_E essentially same as computing $E(\mathbb{Q})$; interesting and sometimes very difficult.

4. Computing $\#\text{Ш}(E)$ is currently **very very difficult**.
   Theorem (Kolyvagin):
   $$r_{\text{an}} \leq 1 \implies \text{Ш}(E) \text{ is finite (with bounds)}$$
   Open Problem:
   Prove that $\text{Ш}(E)$ is finite for some E with $r_{\text{an}} \geq 2$.

Victor Kolyvagin

Kolyvagin's work on Euler systems is crucial to our project.

Motivating Problem 2: Cremona's Book

Motivating Problem 2. Prove BSD for every elliptic curve over $\mathbb{Q}$ of conductor at most 1000, i.e., in Cremona's book.

1. By Tate's isogeny invariance of BSD, it suffices to prove BSD for each **optimal** elliptic curve of conductor $N \leq 1000$.

2. **Rank part** of the conjecture has been verified by Cremona for all curves with $N \leq 25000$.

3. All of the quantities in the conjecture, **except** for $\#\text{Ш}(E/\mathbb{Q})$, have been computed by Cremona for conductor ≤ 25000.

4. **Cremona (Ch. 4, pg. 106):** We have $\text{Ш}(E)[2] = 0$ for **all** optimal curves with conductor ≤ 1000 except 571A, 960D, and 960N. So we can mostly ignore 2 henceforth.

John Cremona

John Cremona's software and book are crucial to our project.

The Four Nontrivial Ш's

Conclusion: In light of Cremona's book, the problem is to show that $\text{Ш}(E)$ is *trivial* for all but the following four optimal elliptic curves with conductor at most 1000:

Curve	a-invariants	$\text{Ш}(E)_?$
571A	[0,-1,1,-929,-105954]	4
681B	[1,1,0,-1154,-15345]	9
960D	[0,-1,0,-900,-10098]	4
960N	[0,1,0,-20,-42]	4

We first deal with these four.

Divisor of Order:

1. Using a 2-descent we see that $4 \mid \#Ш(E)$ for 571A, 960D, 960N.

2. For $E = 681B$: Using visibility (or a 3-descent) we see that $9 \mid \#Ш(E)$.

Multiple of Order:

1. For $E = 681B$, the mod 3 representation is surjective, and $3 \,||\, [E(K) : y_K]$ for $K = \mathbb{Q}(\sqrt{-8})$, so (our refined) Kolyvagin theorem implies that $\#\text{Ш}(E) = 9$, as required.

2. Kolyvagin's theorem and computation $\implies$ $\#\text{Ш}(E) = 4^{?}$ for 571A, 960D, 960N.

3. Using MAGMA's `FourDescent` command, we compute $\mathrm{Sel}^{(4)}(E/\mathbb{Q})$ for 571A, 960D, 960N and deduce that $\#\text{Ш}(E) = 4$. (Note: MAGMA Documentation currently misleading.)

The Eighteen Optimal Curves of Rank > 1

There are 18 curves with conductor ≤ 1000 and rank > 1 (all have rank 2):

389A, 433A, 446D, 563A, 571B, 643A, 655A, 664A, 681C,
707A, 709A, 718B, 794A, 817A, 916C, 944E, 997B, 997C

For these E **nobody** currently knows how to show that $Ш(E)$ is finite, let alone trivial. (But mention, e.g., p-adic L-functions.)

Motivating Problem 3: Prove the BSD Conjecture for all elliptic curve over $\mathbb{Q}$ of conductor at most 1000 and rank ≤ 1.

SECRET MOTIVATION: Our actual motivation is to unify and extend results about BSD and algorithms for elliptic curves. The computational challenge is there to see what interesting phenomena occur in the data.

Our Goal

- There are 2463 optimal curves of conductor at most 1000.
- Of these, 18 have rank 2, which leaves 2445 curves.
- Of these, 2441 are conjectured to have trivial Ш.

Thus our **goal** is to prove that

$$\#\text{Ш}(E) = 1$$

for these 2441 elliptic curves.

Our Strategy

1. [**Refine**] Prove a refinement of Kolyvagin's bound on $\#\text{Ш}(E)$ that is suitable for computation.

2. [**Algorithm**]
   Input: An elliptic curve over $\mathbb{Q}$ with $r_{\text{an}} \leq 1$.
   Output: Odd $B \geq 1$ such that if $p \nmid 2B$, then $p \nmid \#\text{Ш}(E)$.

3. [**Compute**] Run the algorithm on our 2441 curves.

4. [**Descent**] If $p \mid B$ and $E[p]$ is reducible: Use p-descent?

5. [**New Methods**] If $p \mid B$ and $E[p]$ irreducible: Try Kato when $r_{\text{an}} = 0$. When $r_{\text{an}} = 1$, use Schneider's theorem, Kato's work, explicit computations with p-adic heights and p-adic L-functions. Also, visibility and level lowering? Further refinement of Kolyvagin's theorem?

Our Algorithm to Bound $Ш(E)$

INPUT: An elliptic curve E over $\mathbb{Q}$ with $r_{\text{an}} \leq 1$.
OUTPUT: Odd $B \geq 1$ such that if $p \nmid 2B$, then $Ш(E/\mathbb{Q})[p] = 0$.

1. [**Choose K**] Choose a quadratic imaginary field $K = \mathbb{Q}(\sqrt{D})$ that satisfy the Heegner hypothesis, such that E/K has analytic rank 1, and Disc(K) is divisible by **two primes**. (Or two such K each divisible by a single prime.)

2. [**Find p-torsion**] Decide for which primes p there is a curve E' that is $\mathbb{Q}$-isogenous to E such that $E'(\mathbb{Q})[p] \neq 0$. Let A be the product of these primes.

3. [**Compute Mordell-Weil**]

   (a) If $r_{\text{an}} = 0$, compute generator z for $E^D(\mathbb{Q})$ mod torsion.

   (b) If $r_{\text{an}} = 1$, compute generator z for $E(\mathbb{Q})$ mod torsion.

4. [**Height of Heegner point**] Compute the height $h_K(y_K)$, e.g., using the Gross-Zagier formula (and/or directly).

5. [**Index of Heegner point**] Compute
$$I_K = \sqrt{h_K(y_K)/h_K(z)} = [E(K)_{/\text{tor}} : \mathbb{Z}y_K].$$

6. [**Refined Kolyvagin**] Output $B = A \cdot I_K$.

Theorem (refinement of Kolyvagin): $p \nmid 2B \implies p \nmid \#Ш(E/\mathbb{Q})$.

First Attempt to Run the Algorithm

- Using Magma and the MECCAH cluster, I implemented and ran the algorithm on the curves of conductor ≤ 1000, but stopped runs if they took over 30 minutes.

- The computation for 318 curves didn't finish. We do not include them below. Also, I don't trust some of Magma's elliptic curves functions, since the documentation is unclear. However, we assume correctness for the rest of this talk.

- **Future plan:** run each computation without timeouts using `mwrank` and `PARI`.

Results of the First Attempt

1. For 1363 curves we have $B = 1$. For these curves we have proved the full BSD conjecture!

2. There are 94 curves for which $B \geq 11$. Of these, 6 have rank 0 (so we can likely use Kato's theorem).

3. There are 39 curves for which $B \geq 19$. For *all* of these curves the rank is 1.

4. The largest B is 77, for the rank 1 curves 618F and 894G.

5. The largest prime divisor of any B is 31, for the rank 1 curve 674C.

6. When E has rank 0, the algorithm is much more difficult, so more likely to time out.

Major Obstruction: Tamagawa Numbers

Serious Issue: The Gross-Zagier formula and the BSD conjecture together imply that if an odd prime p divides a Tamagawa number, then $p \mid [E(K) : \mathbb{Z}y_K]$.

- If E has $r_{\mathrm{an}} = 0$, and $p \geq 5$, and $\rho_{E,p}$ is surjective, then Kato's theorem (and Mazur, Rubin, et al.) imply that

$$\mathrm{ord}_p(\#\text{Ш}(E)) \leq \mathrm{ord}_p(L(E,1)/\Omega_E),$$

so squareness of $\#\text{Ш}(E)$ frequently saves us.

- Unfortunately, in many cases there is a big Tamagawa number and $r_{\mathrm{an}} = 1$, so Kato doesn't apply.

An Example

The elliptic curve E called 141A and given by $y^2 + y = x^3 + x^2 - 12x + 2$ has rank 1 and $c_3 = 7$. We compute that

$$\#\text{Ш}(E) = 49^{???}.$$

The representation $\rho_{E,7}$ is surjective, but E has rank 1.

Ralph Greenberg's suggestion: Compute a p-adic L-function, a p-adic regulator, and use theorems of Kato and Peter Schneider to show that $7 \nmid \#\text{Ш}(E)$. I hope to do this soon.

What Next?

1. [**Efficiency**] Make the algorithm more efficient. The reason the discriminant must be divisible by two primes, or we choose two fields is so we can weaken the surjectivity hypothesis that Kolyvagin imposed. However, in many cases we have surjectivity and could directly use Kolyvagin's theorem. Also **Byungchul Cha's** 2003 Johns Hopkins Ph.D. thesis weakens Kolyvagin's hypothesis in another way. Combining all this should speed up the algorithm.

2. [**Finish!**] Run the algorithm to completion on all curves of conductor up to 1000. Hard part is finding $E^D(\mathbb{Q})$ for rank 1 E^D, where D has 3 digits (so the conductor has $\sim$ 12 digits).

3. [**New Theory**] Find a strategy that works when $r_{\mathrm{an}} = 1$ and E has a Tamagawa number ≥ 5. Either refine Kolyvagin, use visibility and level lowering, or Schneider and Kato's results on the p-adic main conjecture.