Verifying the Birch and Swinnerton-Dyer Conjecture for Specific Elliptic Curves: A Status Report

William Stein
Harvard University
http://modular.fas.harvard.edu/talks/bsd2005/

AMS Session: January 8, 2005

Abstract

This 20-minute talk reports on a project to verify the Birch and Swinnerton-Dyer conjecture for all elliptic curves over $\mathbb{Q}$ in Cremona's book.

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

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

1 The Birch and Swinnerton-Dyer Conjecture

BSD Conjecture: Let E be an elliptic curve over $\mathbb{Q}$, and let $r = r_{\mathrm{an}} = \mathrm{ord}_{s=1} L(E,s)$. Then

$$r_{\mathrm{an}} = \text{rank } E(\mathbb{Q})$$

and

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

Notation:

1. $L(E,s)$ is an entire L-function that encodes $\{\#E(\mathbb{F}_p)\}$
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. $Ш(E) = \mathrm{Ker}(\mathrm{H}^1(\mathbb{Q},E) \to \bigoplus_v \mathrm{H}^1(\mathbb{Q}_v,E))$ – **Shafarevich-Tate group**

2 Birch and Swinnerton-Dyer

Birch and Swinnerton-Dyer in Leiden, Netherlands, Summer 2000.

3 Motivating Problem 1

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

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

2. Easy to compute $\#E(\mathbb{Q})_{\mathrm{tor}}$, c_p, Ω_E.

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

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

4 Victor Kolyvagin

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

Kolyvagin in New York's Chinatown, 2003.

5 Motivating Problem 2: Cremona's Book

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

We have:

1. By Tate's isogeny invariance theorem, it suffices to prove BSD for each $X_0(N)$-**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 all curves of 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.

6 John Cremona

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

Cremona in Nottingham, UK, 2001.

7 The Four Nontrivial Ш's

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

Curve	a-invariants	$Ш(E)_?$
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

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 $3 \mid\mid [E(K) : y_K]$ for $K = \mathbb{Q}(\sqrt{-8})$, so (our refined) Kolyvagin theorem implies that $\#Ш(E) = 9$, as required.
2. Kolyvagin's theorem and computation $\implies$ $\#Ш(E) = 4^?$ 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 $\#Ш(E) = 4$. (Note: Documentation currently misleading.)

8 The Eighteen Optimal Curves of Big Rank

There are 18 curves with conductor ≤ 1000 and rank ≥ 2 (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., Perrin-Riou's work.)

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 just to see what interesting phenomena occur in the data.

9 The Plan

The Dataset:

- 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 $Ш$.

Strategy:

1. [Refine] Prove a refinement of Kolyvagin's bound on $\#Ш(E)$ that is suitable for computation. Also take into account refinement of Kato's theorem (Kato assumes $r_{\mathrm{an}} = 0$).
2. [Algorithm] Create an Algorithm:

   Input: An elliptic curve over $\mathbb{Q}$ with $r_{\mathrm{an}} \leq 1$.
   Output: Odd $B \geq 1$ such that if $p \nmid 2B$, then $p \nmid \#Ш(E)$.
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, ????????. Kato when $r_{\mathrm{an}} = 0$. When $r_{\mathrm{an}} = 1$, maybe use Schneider's theorem and explicit computations with heights and p-adic L-functions? Visibility and level lowering? Further refinement of Kolyvagin's theorem?

10 The Algorithm of Step 2

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 TWO distinct quadratic imaginary fields K_1 and K_2 that both satisfy the Heegner hypothesis and such that E/K_1 and E/K_2 have analytic rank 1.
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 a generator z for $E^D(\mathbb{Q})$ modulo torsion.

   (b) If $r_{\text{an}} = 1$, compute a generator z for $E(\mathbb{Q})$ modulo torsion.
4. [Height of Heegner point] Compute the height $h_K(y_K)$, e.g., using the Gross-Zagier formula.
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 (our refinement of Kolyvagin): $p \nmid 2B \implies Ш(E/\mathbb{Q})[p] = 0$.

11 Result of Running 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.

Results:

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, only 6 have rank 0.
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 the rank of E is 0, the algorithm is much more difficult, so more likely to time out.

12 Major Obstruction: Big 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 $r_{\mathrm{an}} = 1$.

13 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 know that

$$Ш(E) \overset{?}{=} 49.$$

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

- [Visibility?] The Jacobian $J_0(47)$ is of rank 0 and is simple of dimension 4, and we find that $E[7]$ sits in the old subvariety of $J_0(3\cdot 47)$. Hope: Proving something about the Shafarevich-Tate group of the simple rank 0 abelian variety $J_0(47)$ will imply something about $Ш(E)[7]$. Note that $L(J_0(47),1)/\Omega = 16/23$.

- [p-Adic Approach?] Maybe a p-adic L-function computation will imply that $7 \nmid \#Ш(E)$???

14 What Next?

1. [Efficiency] Make the algorithm more efficient. The reason we chose two fields is so we can weaken the surjectivity hypothesis that Kolyvagin (or at least Gross, in his article) imposed. However, in many cases one does 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 significantly when $r_{\mathrm{an}} = 0$.

2. [Finish!] Run the algorithm to completion on all curves of conductor up to 1000. The hard part is finding the full Mordell-Weil group of rank 1 curves of the form E^D, where D has 3 digits (so the conductor has about 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.

Questions?