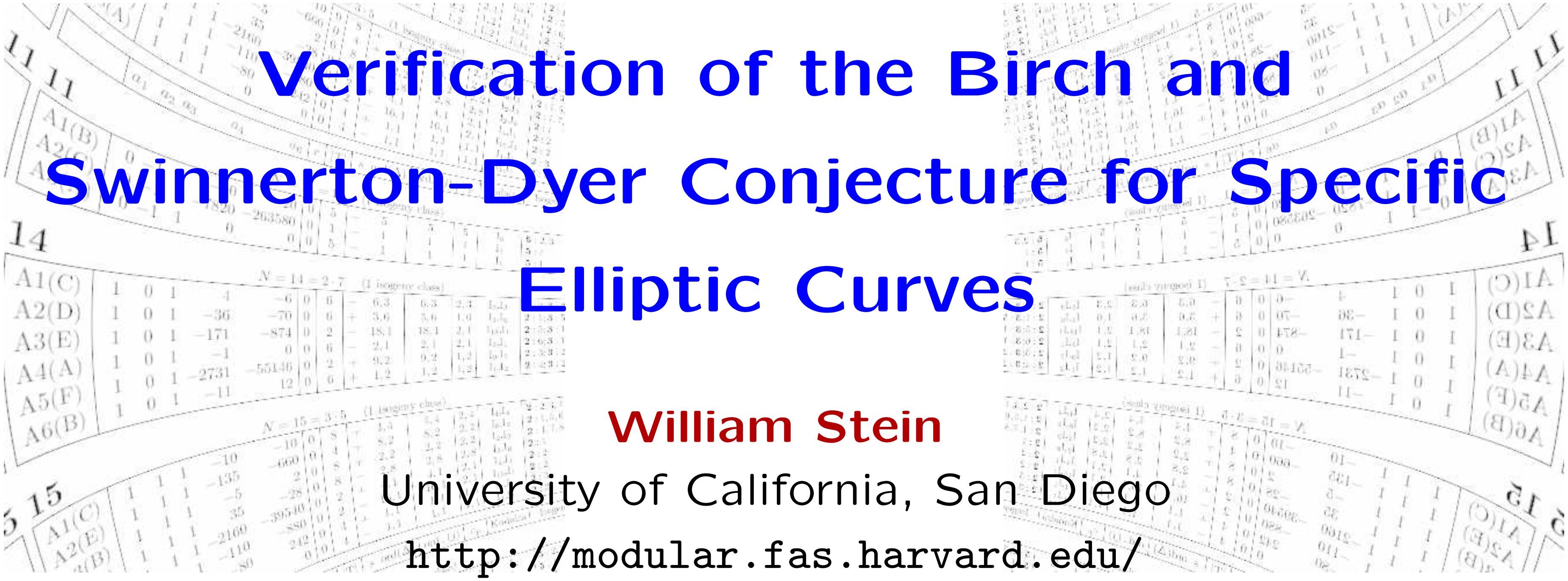


Verification of the Birch and Swinnerton-Dyer Conjecture for Specific Elliptic Curves

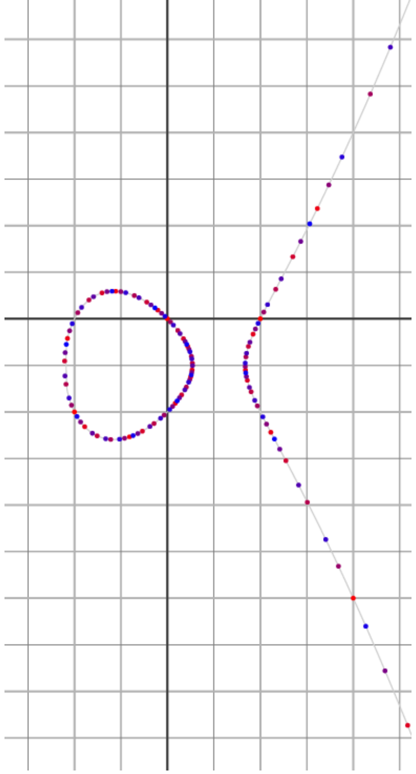
William Stein

University of California, San Diego

`http://modular.fas.harvard.edu/`

Bremen: July 2005

This talk reports on a long-term collaborative project to verify the Birch and Swinnerton-Dyer conjecture for specific elliptic curves.
Step 1 is done.



Collaborators: Grigor Grigorov, Andrei Jorza, Stefan Patrikis, Corina Tarnita-Patrascu (and Stephen Donnelly, Michael Stoll).

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

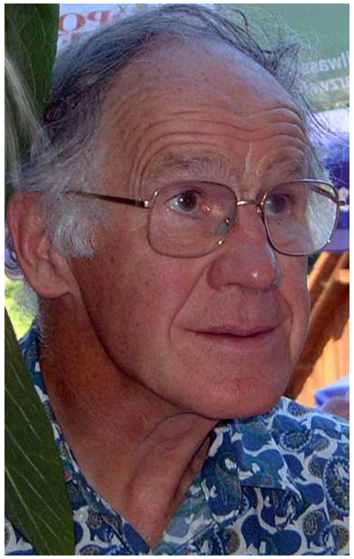
Manin Constant Assumption

For the rest of this talk I will officially assume that the Manin constant of every elliptic curve of conductor ≤ 1000 is 1. It's not completely clear to me that Cremona has verified this, though it seems very likely.

Main Theorem

Suppose E is a non-CM elliptic curve of conductor ≤ 1000 and rank ≤ 1 and p is a prime that does not divide any Tamagawa number of E and that E has no p-isogeny. Then the p-part of the full BSD conjectural formula is true for E.

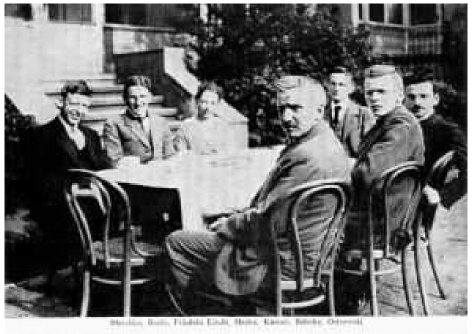
Once upon a time...



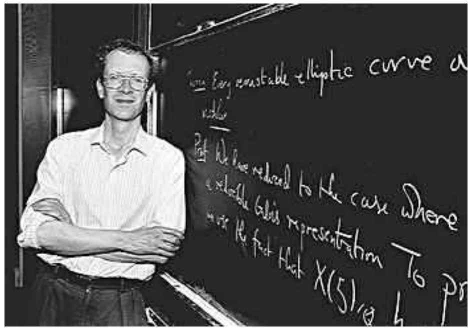
Conjectures Proliferated

"The subject of this lecture is rather a special one. I want to describe some computations undertaken by myself and Swinnerton-Dyer on EDSAC, by which we have calculated the zeta-functions of certain elliptic curves. As a result of these computations we have found an analogue for an elliptic curve of the Tamagawa number of an algebraic group; and conjectures have proliferated. [...] though the associated theory is both abstract and technically complicated, the objects about which I intend to talk are usually simply defined and often machine computable; **experimentally we have detected certain relations between different invariants**, but we have been unable to approach proofs of these relations, which must lie very deep." – Birch 1965

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:

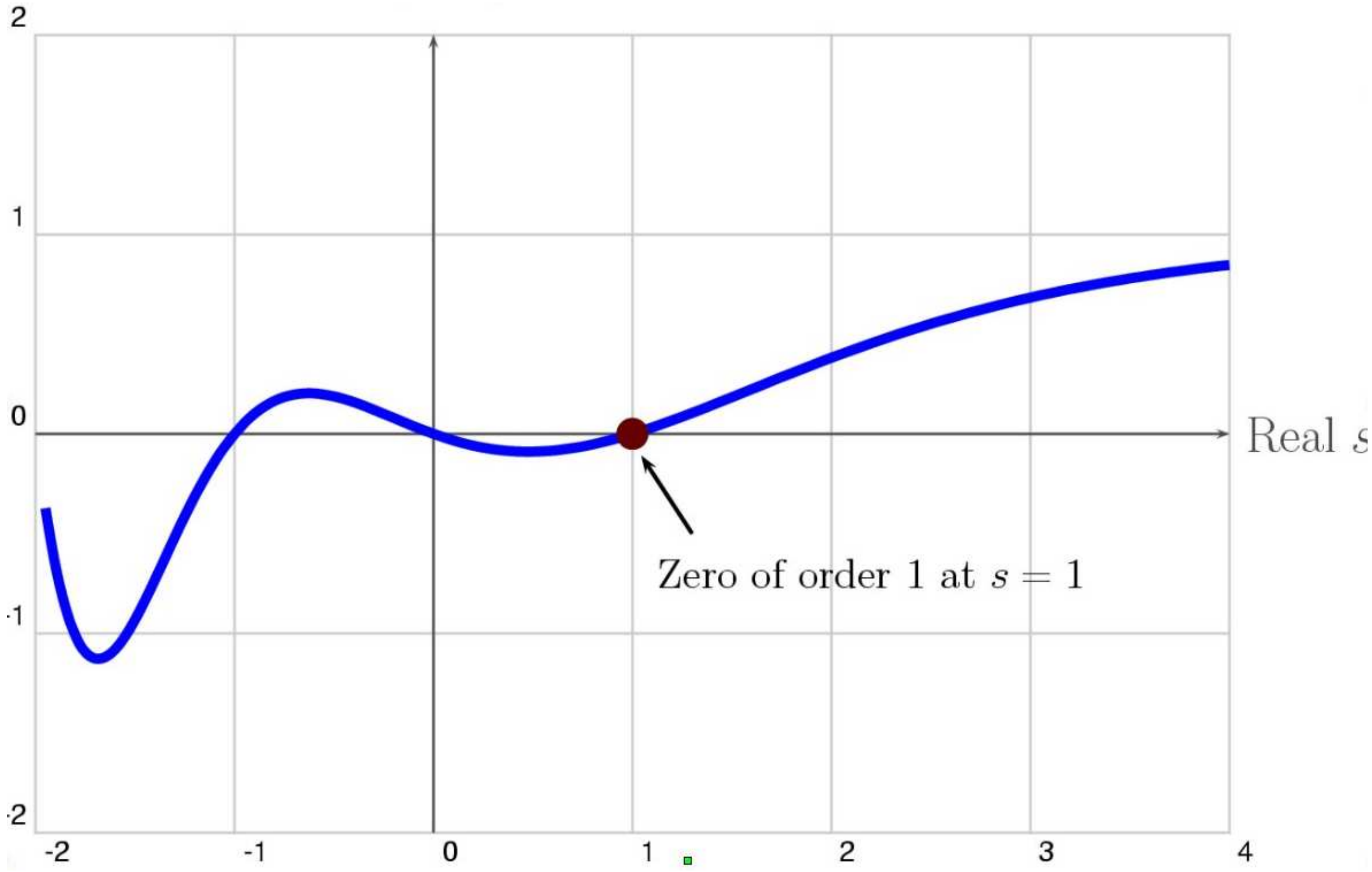
$$L^*(E,s) = \prod_{p \nmid \Delta} \left(\frac{1}{1 - a_p \cdot p^{-s} + p \cdot p^{-2s}} \right).$$

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

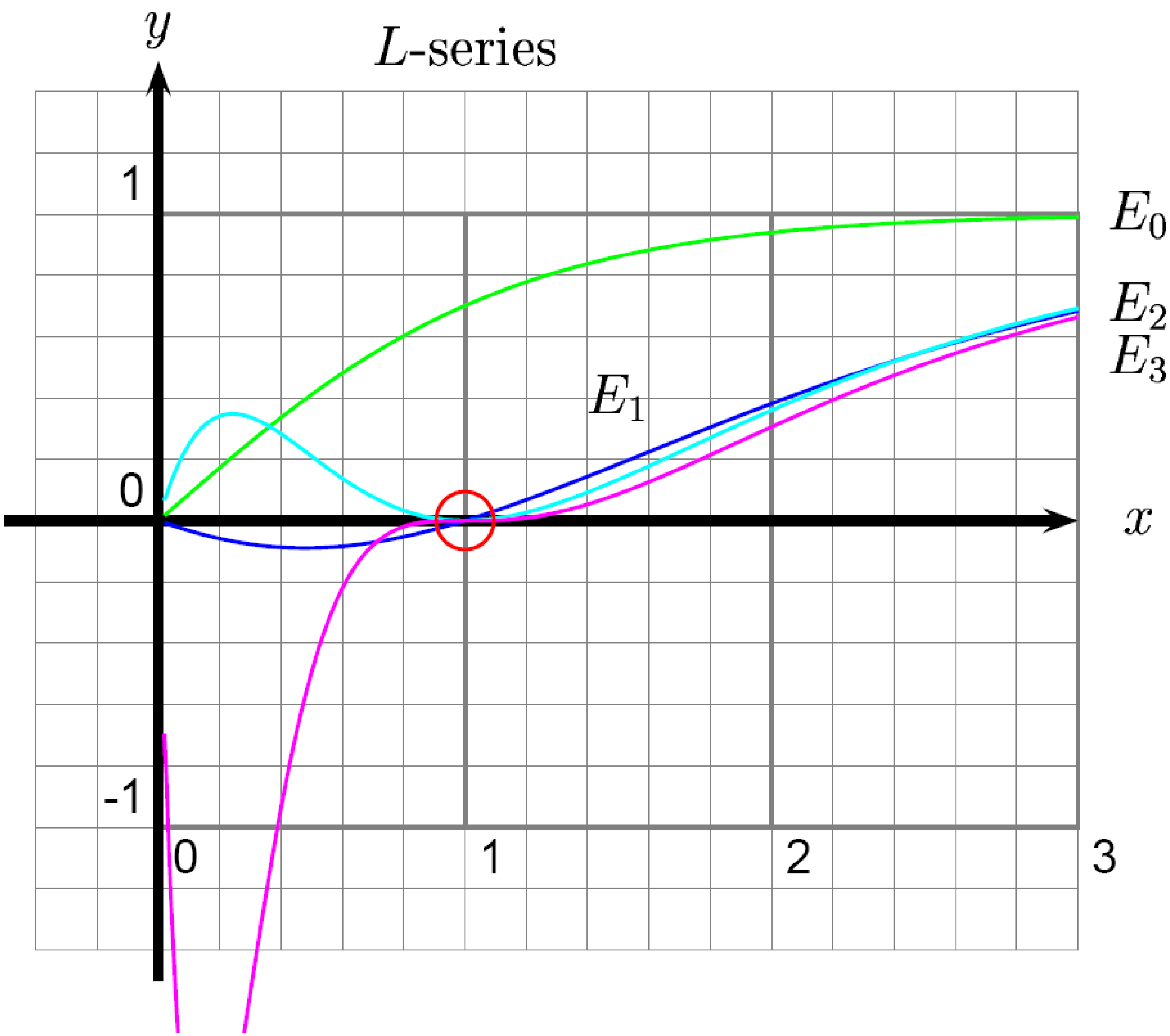
$$L^*(E,1) = \prod_{p \nmid \Delta} \left(\frac{1}{1 - a_p \cdot p^{-1} + p \cdot p^{-2}} \right) = \prod_{p \nmid \Delta} \left(\frac{p}{p - a_p + 1} \right) = \prod_{p \nmid \Delta} \frac{p}{N_p}$$

Standard extension to $L(E,s)$ at bad primes.

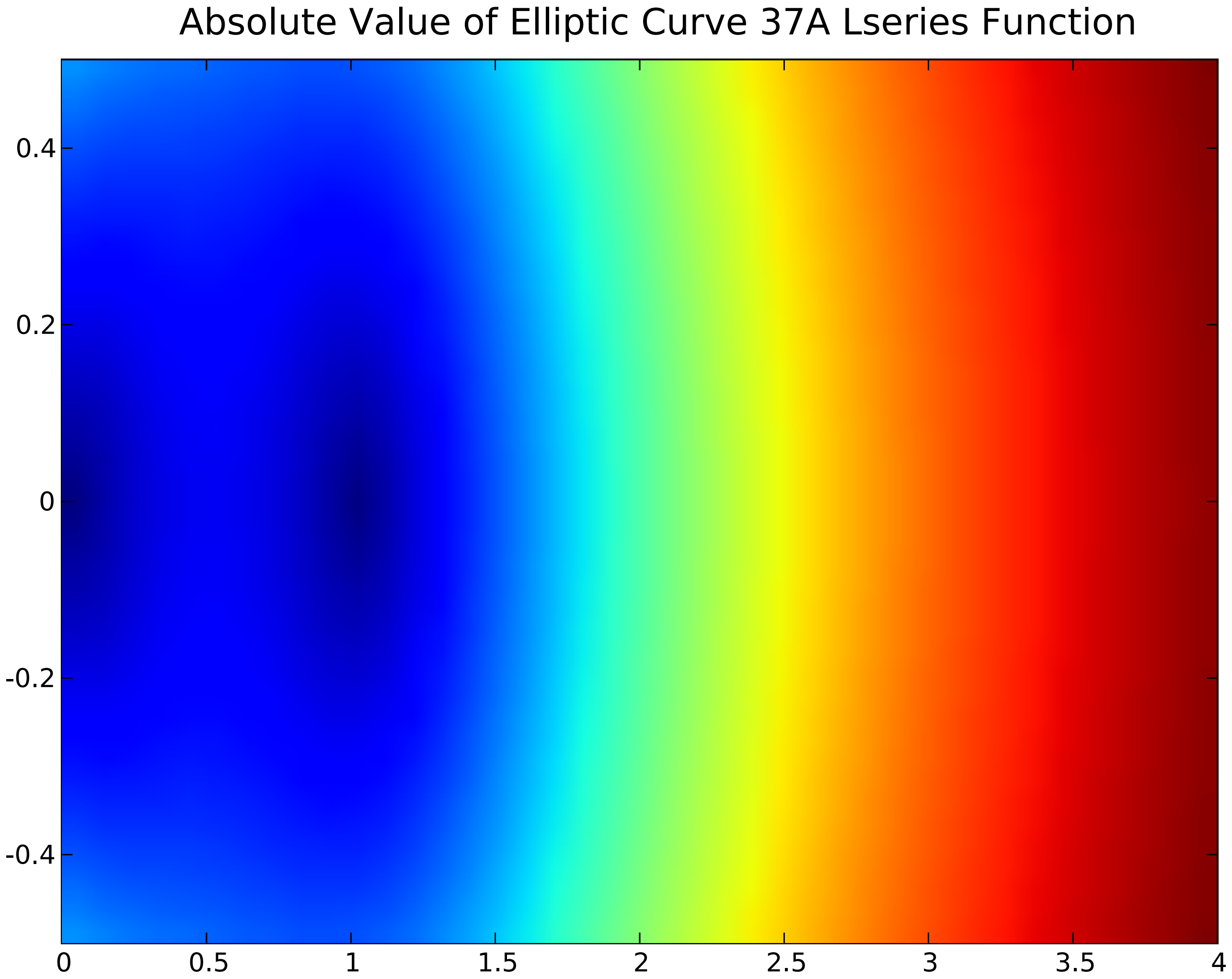
Real Graph of the L-Series of $y^2 + y = x^3 - x$



More Graphs of Elliptic Curve L-functions



Absolute Value of L-series on Complex Plane for $y^2 + y = x^3 - x$



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 $\text{ord}_{s=1} L(E, s)$ is ≤ 1, then the BSD rank conjecture is true for E.

Refined BSD **Conjectural Formula**

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

- $\#E(\mathbb{Q})_{\mathrm{tor}}$ – order of **torsion**
- c_p – **Tamagawa numbers**
- Ω_E – **real volume** $= \int_{E(\mathbb{R})} \omega_E$
- Reg_E – **regulator** of E
- $\text{Ш}(E) = \mathrm{Ker}\left(\mathrm{H}^1(\mathbb{Q}, E) \to \bigoplus_v \mathrm{H}^1(\mathbb{Q}_v, E)\right)$ – **Shafarevich-Tate group**

The Shafarevich-Tate Group

$$Ш(E) = \mathrm{Ker}\left(\mathrm{H}^1(\mathbb{Q}, E) \to \bigoplus_v \mathrm{H}^1(\mathbb{Q}_v, E)\right)$$

The elements of $Ш(E)$ correspond to (classes of) genus one curves X with Jacobian E that have a point over each p-adic field and $\mathbb{R}$. E.g., the curve $3x^3 + 4y^3 + 5z^3 = 0$ is in $Ш(x^3 + y^3 + 60z^3 = 0)$.

Computing $Ш(E)$ in practice is challenging! It took decades until the first example was computed (by Karl Rubin).

John Cremona's Book

Main **Theorem**

Suppose E is a non-CM elliptic curve of conductor ≤ 1000 and rank ≤ 1 and p is a prime that does not divide any Tamagawa number of E and that E has no p-isogeny. Then the p-part of the full BSD conjectural formula is true for E.

The rest of this talk is about the proof.

Tools

- SAGE: I did much of this computation using

  SAGE: **S**ystem for **A**lgebra and **G**eometry **C**omputation
  `http://modular.fas.harvard.edu/sage`

  which is a new computer algebra system that incorporates mwrank, PARI, etc., under one hood.

- MAGMA: I used MAGMA for some 3 and 4-descents.

BSD Conjecture at p

Conjecture 1 (BSD(E,p)). *Let* (E,p) *denote a pair consisting of an elliptic curve* E *over* $\mathbb{Q}$ *and a prime* p*. The* BSD conjecture at p *(denoted* BSD(E,p)*) is the BSD conjecture, but with the weaker claim that* $\mathrm{ord}_p(\#\text{Ш}(E)[p^\infty]) = \mathrm{ord}_p\left(\dfrac{L^{(r)}(E,1)\cdot(\#E(\mathbb{Q})_{\mathrm{tor}})^2}{r!\cdot\Omega_E\cdot\mathrm{Reg}_E\cdot\prod_p c_p}\right)$.

Tate: The truth of BSD(E,p) is invariant under isogeny.

Computational Evidence for BSD

All of the quantities in the BSD conjecture, **except** for $\#\text{Ш}(E/\mathbb{Q})$, have been computed by Cremona for conductor ≤ 70000.

- **Cremona (Ch. 4, pg. 106):** In Cremona's book, exactly four optimal curves with conjecturally nontrivial $\text{Ш}(E)$: 571A, 681B, 960D, 960N

- Cremona verified BSD$(E, 2)$ for all curves in his book, except 571A, 960D, and 960N.

Victor Kolyvagin

Kolyvagin: When $r_{\text{an}} \leq 1$, get computable multiple of $\#Ш(E)$.

Let K be a quadratic imaginary field in which all primes dividing the conductor of E split. Let $y_K \in E(K)$ be the corresponding **Heegner point**.

Theorem 2 (Kolyvagin). *Suppose E is a non-CM elliptic curve and p is an odd prime such that $\overline{\rho}_{E,p}$ is surjective and $E(K)$ has rank 1. Then*

$$\text{ord}_p(\#Ш(E/K)) \leq 2 \cdot \text{ord}_p([E(K) : \mathbb{Z}y_K]).$$

Victor Kolyvagin

Kato

Kato: When $r_{\text{an}} = 0$, get bound on $\#Ш(E)$.

Theorem 3 (Kato). *Let E be an optimal elliptic curve over $\mathbb{Q}$ of conductor N, and let p be a prime such that $p \nmid 6N$ and $\overline{\rho}_{E,p}$ is surjective. If $L(E,1) \neq 0$, then $Ш(E)$ is finite and*

$$\mathrm{ord}_p(\#Ш(E)) \leq \mathrm{ord}_p\left(\frac{L(E,1)}{\Omega_E}\right).$$

This theorem follows from the existence of an "optimal" Kato Euler system...

The Four Nontrivial Ш's

Conclusion: BSD for the curves in Cremona's book is the assertion 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

We can deal with these four curves...

Divisor of Order

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

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

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 Kolyvagin's 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 $\#Ш(E) = 4$.

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 perhaps **nobody** currently knows how to show that $\text{Ш}(E)$ is finite, let alone trivial. (But p-adic L-functions, Iwasawa theory, Schneider's theorem, etc., would give a finite interesting list of p for a given curve.)

Summary

- There are 2463 optimal curves of conductor at most 1000.
- Of these, 18 have rank 2, which leaves 2445 curves.
- Of these, 2441 have conjecturally trivial Ш.
- Of these, 44 have CM.

We prove $\mathrm{BSD}(E, p)$ *for the remaining* 2397 *curves at primes* p *that do not divide Tamagawa numbers and for which* $\overline{\rho}_{E,p}$ *is irreducible.*

Determining $\mathrm{im}(\overline{\rho}_{E,p}) \subset \mathrm{Aut}(E[p])$

Theorem 4 (Cojocaru, Kani, and Serre). *If E is a non-CM elliptic curve of conductor N, and*

$$p \geq 1 + \frac{4\sqrt{6}}{3} \cdot N \cdot \prod_{\text{prime } \ell | N} \left(1 + \frac{1}{\ell}\right)^{1/2},$$

then $\overline{\rho}_{E,p}$ is surjective.

Proposition 5 (–, et al.). *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and let $p \geq 5$ be a prime. For each prime $\ell \nmid p \cdot N$ with $a_\ell \not\equiv 0 \pmod{p}$, let*

$$s(\ell) = \left(\frac{a_\ell^2 - 4\ell}{p}\right) \in \{0, -1, +1\},$$

where the symbol $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol. If -1 and $+1$ both occur as values of $s(\ell)$, then $\overline{\rho}_{E,p}$ is surjective. If $s(\ell) \in \{0, 1\}$ for all ℓ, then $\mathrm{im}(\overline{\rho}_{E,p})$ is contained in a Borel subgroup (i.e., reducible), and if $s(\ell) \in \{0, -1\}$ for all ℓ, then $\mathrm{im}(\overline{\rho}_{E,p})$ is a nonsplit torus.

This $+$ division polynomials $\Longrightarrow$ efficient algorithm to compute image. (Tables now available online.)

Generalizations of Kolyvagin's Theorem

Theorem 6 (Cha). *If $p \nmid D_K$, $p^2 \nmid N$, and $\overline{\rho}_{E,p}$ is irreducible, then*

$$\mathrm{ord}_p(\#\text{Ш}(E/K)) \leq 2 \cdot \mathrm{ord}_p([E(K) : \mathbb{Z}y_K]).$$

Example 7. Let E be the elliptic curve 608B, which has rank 0. Then BSD$(E, 5)$ is true for E by Cha's theorem, but not Kato's since $\overline{\rho}_{E,5}$ irreducible but not surjective.

The following theorem began with Stoll and Donnelly, and was essential in proving our main theorem.

Theorem 8 (–). *Suppose E is a non-CM elliptic curve over $\mathbb{Q}$. Suppose K is a quadratic imaginary field that satisfies the Heegner hypothesis and p is an odd prime such that $p \nmid \#E'(K)_{\mathrm{tor}}$ for any curve E' that is $\mathbb{Q}$-isogenous to E. Then*

$$\mathrm{ord}_p(\#\text{Ш}(E)) \leq 2\,\mathrm{ord}_p([E(K) : \mathbb{Z}y_K]),$$

unless disc(K) *is divisible by exactly one prime ℓ, in which case the conclusion is only valid if $p \neq \ell$.*

Computing Indexes of Heegner Point

Use the Gross-Zagier formula to compute $h(y_K)$ from special values of L-functions (very fast).

When $E(K)$ can be computed, (e.g., if $E(\mathbb{Q})$ known, or using 4-descent), we obtain the index using properties of heights.

If $E(K)$ too difficult to compute, can sometimes use the Cremona-Prickett-Siksek bound to quickly bound $[E(K) : \mathbb{Z}y_K]$.

Example 9. Let E be 546E and $K = \mathbb{Q}(\sqrt{-311})$. Let F be the quadratic twist of E by -311. We have

$$h(y_K) \sim 7315.20688,$$

CPS bound for F is $B = 13.0825747$. Search for points on F of naive logarithmic height ≤ 18, and find no points, so

$$[E(K) : \mathbb{Z}y_K] < \sqrt{7320/(2 \cdot (18 - 13.0825747))} \sim 27.28171 < 28.$$

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

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

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

- In many cases with $r_{\text{an}} = 1$, there is a big Tamagawa number—there are 91 optimal curves up to conductor 1000 with Tamagawa number divisible by a prime $p \geq 7$.

Conclusion

Throw in exlicit 3 and 4-descents to deal with a handful of reluctant cases. Everything works out so that *all* our techniques are just enough to complete the proof. If Cremona's book were larger, this might not have been the case.

Please see

`http://modular.fas.harvard.edu/papers/bsdalg/`

for the finished write-up.

Next Step: Write a Paper with Me!!

1. [**CM**] Verify the BSD conjecture for CM curves up to some conductor. About half of rank 0 and half of rank 1. Very extensive theory here, beginning with Rubin—should be relative "easy", especially for rank 0.

2. [**Manin**] Rigorously verify that $c = 1$ for curves up to conductor 70000.

3. [**Extend**] Consider curves of conductor > 1000. Have to verify nontriviality of big $Ш(E)$'s; use visibility and Grigor Grigorov's thesis.

4. [**Big Rank**] Verify BSD at all primes $p \leq 100$ for some curve of rank 2.

5. [**Isogenies**] Verify the BSD conjecture at primes p that are the degree of an isogeny from E. Mazur's "Eisenstein descent" does prime level case; but then $p = 2$. Perhaps direct p-descent is doable, or use congruences...

6. [**Tamagawa**] Verify the BSD conjecture at primes p that divide a Tamagawa number. Prove a refinement of Kolyvagin's theorem and/or develop p-adic methods.

7. [**Abelian Varieties**] Verify the full BSD conjecture for modular Jacobians $J_0(N)$, for $N \leq 100$.