Verifying the Full Birch and Swinnerton-Dyer Conjecture in Specific Cases

William Stein

University of Waterloo: December 2006

This talk reports on a collaborative project to verify the Birch and Swinnerton-Dyer conjecture for specific elliptic curves.

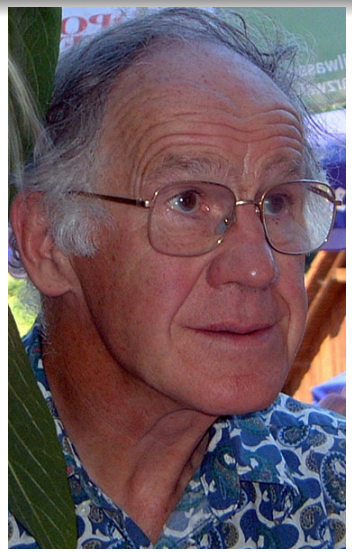
Joint Paper: Grigor Grigorov, Andrei Jorza, Stefan Patrikis, Corina Tarnita-Patrascu. (All were Harvard *students*!) And Aron Lum (UCSD).

Acknowledgement: John Cremona, Stephen Donnelly, Noam Elkies, Ralph Greenberg, Barry Mazur, Robert Pollack, Nick Ramsey, Tony Scholl, Michael Stoll, and Cristian Wuthrich.

Main Theorem

Main Thereom. *Suppose E is a non-CM elliptic curve of conductor $N \leq 1000$ and rank ≤ 1 and p is a prime that does not divide any Tamagawa number of E and that E has no rational p-isogenies, or that E has CM and $p^2 \nmid N$. Then the p-part of the full Birch and Swinnerton-Dyer conjectural formula is true for E.*

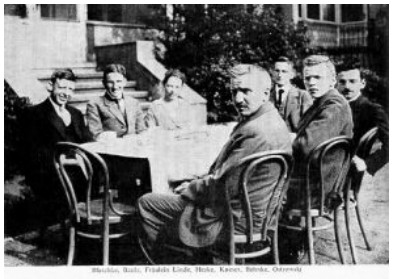
Once upon a time...



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:

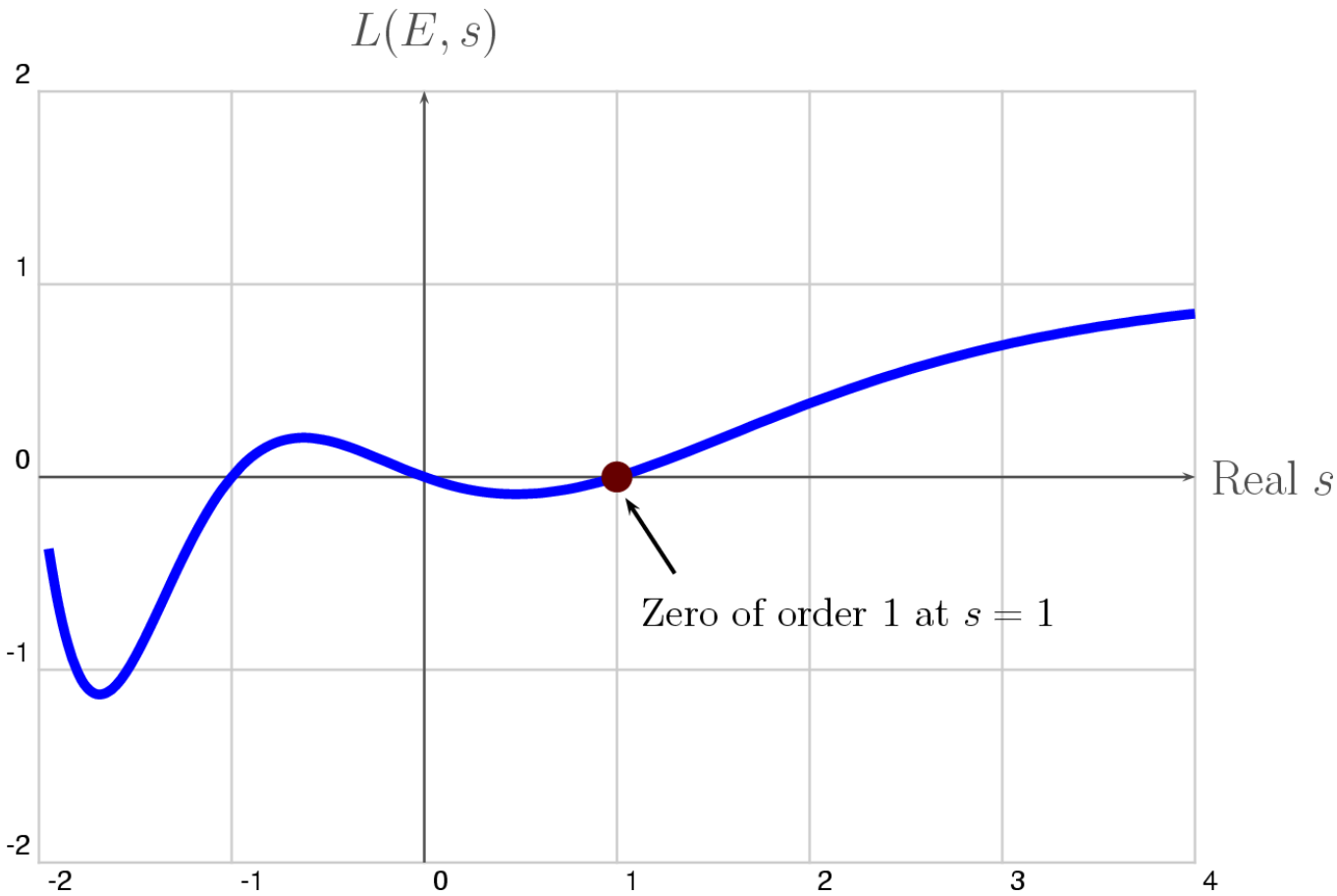
$$L^*(E,s) = \prod_{p \nmid \Delta} \left(\frac{1}{1 - a_p \cdot p^{-s} + p \cdot p^{-2s}} \right).$$

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

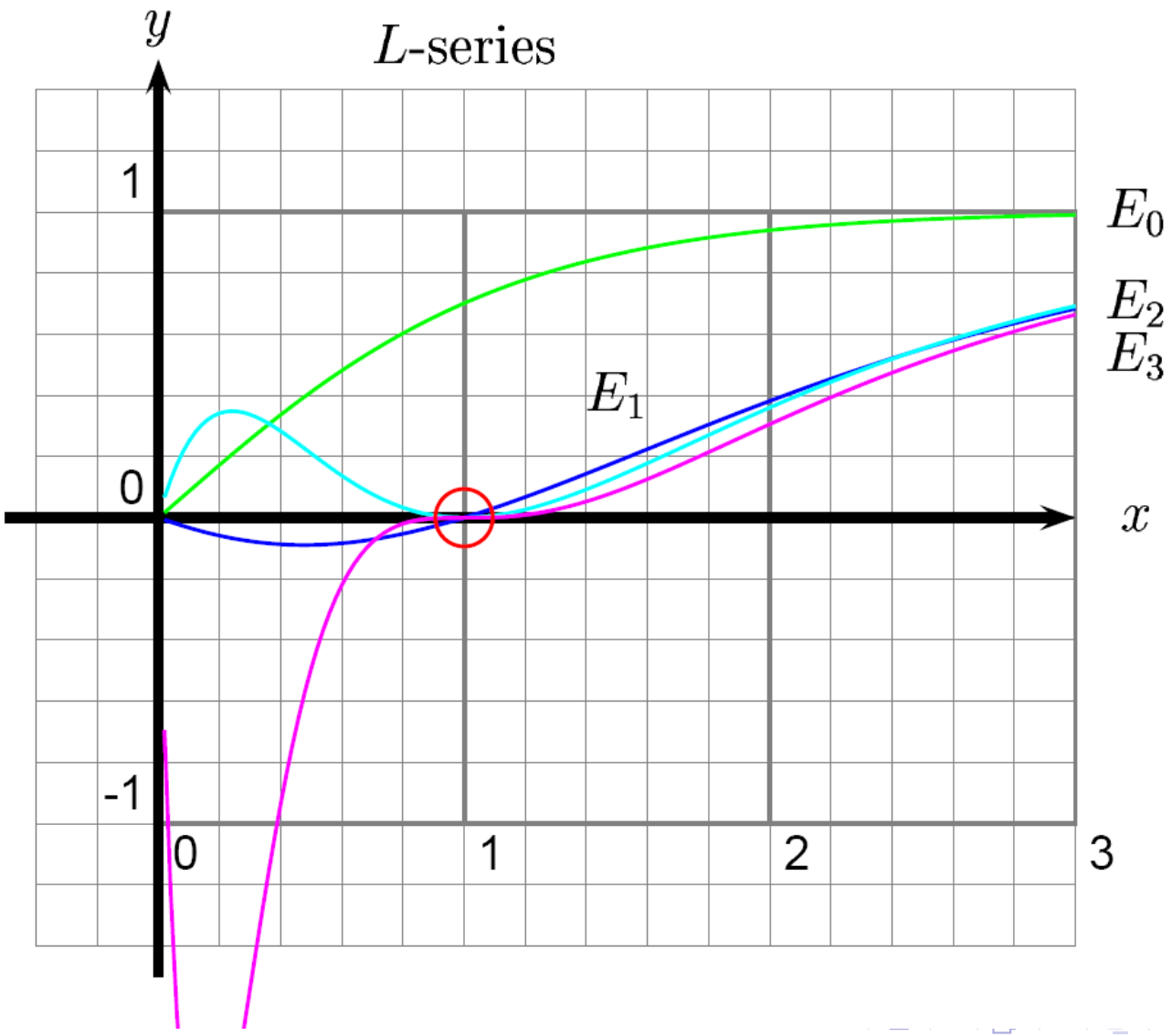
$$L^*(E,1) = \prod_{p \nmid \Delta} \left(\frac{1}{1 - a_p \cdot p^{-1} + p \cdot p^{-2}} \right) = \prod_{p \nmid \Delta} \left(\frac{p}{p - a_p + 1} \right) = \prod_{p \nmid \Delta} \frac{p}{N_p}$$

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

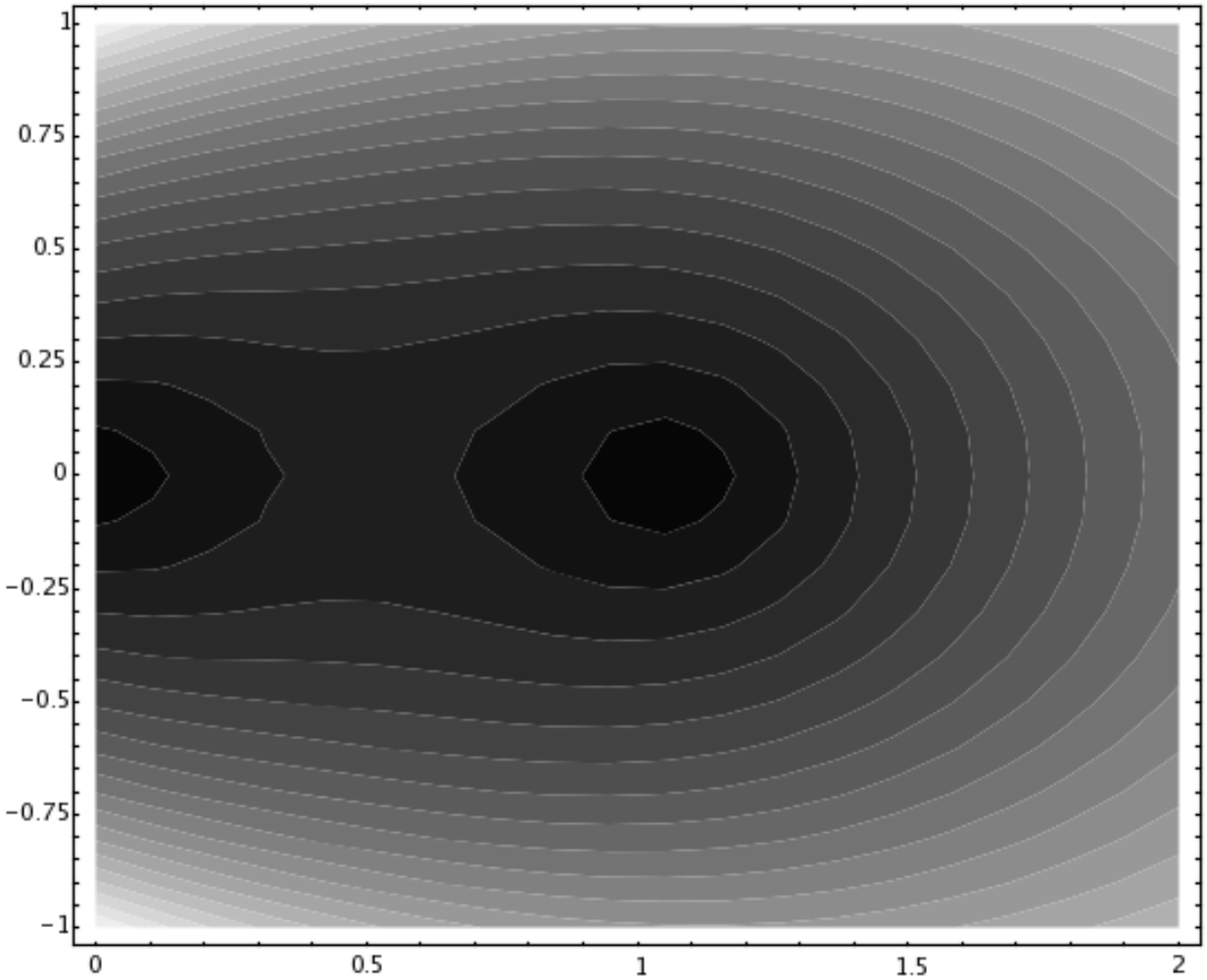
Real Graph of the L-Series of $y^2 + y = x^3 - x$



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 $E(\mathbb{Q})$.

Kolyvagin and Gross-Zagier



Theorem (Kolyvagin, Gross, Zagier, et al.) If the ordering of vanishing $\mathrm{ord}_{s=1} L(E,s)$ is ≤ 1, then the BSD rank conjecture is true for E.

Refined BSD Conjectural Formula

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

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

Thereom *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 rational p-isogenies. 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 most of this computation using

  SAGE: **S**ystem for **A**lgebra and **G**eometry **C**omputation

  See my other talk for more about SAGE.

- Google search: `sage.math`

- Magma: I used Magma only for some 3 and 4-descents, since **unfortunately** the world's only implementation of 3 and 4-descents is in Magma.

BSD Conjecture at p

Conjecture (BSD(E,p))

Let (E,p) denote a pair consisting of an elliptic curve E over $\mathbb{Q}$ and a prime p. Then $E(\mathbb{Q})$ has the predicted rank, $Ш(E)[p^\infty]$ is finite and

$$\mathrm{ord}_p(\#Ш(E)[p^\infty]) = \mathrm{ord}_p\left(\frac{L^{(r)}(E,1)\cdot(\#E(\mathbb{Q})_{\mathrm{tor}})^2}{r!\cdot\Omega_E\cdot\mathrm{Reg}_E\cdot\prod_p c_p}\right).$$

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

Remark (Zagier): Implicit is that the fraction on the right is an integer. I think this is not known for even a single curve of rank ≥ 2.

Computational Evidence for BSD

All of the quantities in the BSD conjecture, **except** for $\#Ш(E/\mathbb{Q})$, have been computed by Cremona for conductor ≤ 130000.

- **Cremona (Ch. 4, pg. 106):** In Cremona's book, there are exactly four **optimal** curves with conjecturally nontrivial $Ш(E)$:

  571A, 681B, 960D, 960N

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

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

As we will see, we can deal with these four curves...

Victor Kolyvagin

Kolyvagin's Theorem

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

Let K be a quadratic imaginary field in which all primes dividing the conductor of E split (assume $\mathrm{disc}(K) < -4$ is coprime to conductor). Let $y_K \in E(K)$ be the corresponding **Heegner point**.

Theorem (Kolyvagin)

Suppose E is a non-CM elliptic curve and p is an odd prime such that $\overline{\rho}_{E,p}$ is surjective and $\mathrm{ord}_{s=1} L(E/K, s) = 1$. Then

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

Kato's Theorem

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

Theorem (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 recent work of Matsuno; see also work of Mazur-Rubin.

Divisor of Order

Back to our four curves...

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 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 18 Optimal Curves of Rank ≥ 2

There are 18 optimal 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 perhaps **nobody** currently knows how to show that $Ш(E)$ 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.
Current joint work with Cristian Wuthrich.

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 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 (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.

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

Proposition (–, Grigorov, Serre (Inv. 1972))

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 proposition and division polynomials leads to an algorithm to compute the image of $\overline{\rho}_{E,p}$ for all p. (Tables now available online.)

Generalizations of Kolyvagin's Theorem

Theorem (Cha)

If $p \nmid D_K$, $p^2 \nmid N$, and $\overline{\rho}_{E,p}$ is irreducible, then

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

Theorem (Donnelly, Jorza, Patrikis, Stoll, –)

If E is a non-CM curve over $\mathbb{Q}$, 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

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

unless $\mathrm{disc}(K)$ *is divisible by exactly one prime ℓ, in which case we only deduce the conclusion when $p \neq \ell$.*

Dimitar Jetchev: Berkeley Ph.D. thesis in progress with further deeper refinements.

Computing Indexes of Heegner Point

Use the Gross-Zagier formula to compute $h(y_K)$ from special values of L-functions. When we can compute $E(K)$ we obtain the index using properties of heights. If $E(K)$ is too difficult to compute, we can use the Cremona-Prickett-Siksek height bound and direct search to bound $[E(K) : \mathbb{Z}y_K]$:

Example

Let E be 906E1 which has rank 0. All $\overline{\rho}_{E,p}$ are surjective. Kato's theorem implies only $2, 3, 151$ could divide $\#Ш(E)$. What about 151?? The first few Heegner discriminants are

$$-23, -71, -119, -143, -263, -335.$$

Grozz-Zagier implies heights $\sim 7705, 20400, 33785, 19284, 39658, 63256$. Finding these Heegner points could be difficult. Let F be the quadratic twist of E by -23. The CPS bound for F is $B = 13.649\ldots$. Search for points on F of naive logarithmic height < 21, and find no points, so

$$[E(K) : \mathbb{Z}y_K] \leq \sqrt{7705/(2 \cdot (21 - 13.649))} \sim 22.89 < 23.$$

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 $p \mid [E(K) : \mathbb{Z}y_K]$.

- **Rank** 0**:** 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

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

  so squareness of $\#Ш(E)$ frequently helps.
- **Rank** 1**:** In many cases with $r_{\mathrm{an}} = 1$, 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 explicit 3 and 4-descents to deal with a handful of reluctant cases. Everything works out so that *all* our techniques are just enough to prove the main theorem. If Cremona's book were larger, this might not have been the case. (His website now includes data up to conductor 130,000.)

For complete details, see:

`http://sage.math.washington.edu/papers/bsdalg/`

Future Projects

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. (Mostly done project with UCSD grad student **Aron Lum**.)
2. [**Tamagawa**] Verify the BSD conjecture at primes p that divide a Tamagawa number. Use Schneider's theorems about p-adic BSD, computation of p-adic regulators and p-adic height pairings. (Joint project with **Cristian Wuthrich**.) Also D. Jetchev, Berkeley grad student, has results in this direction by refining Kolyvagin's theorem.
3. [**Big Rank**] Verify the p-part of the BSD conjecture at many primes $p \leq 100$ for a single curve of rank 2. (Assuming analytic $Ш(E)$ is an integer.) Related to recent paper of Perrin-Riou that uses p-adic BSD.
4. [**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...
5. [**Extend**] Consider curves of conductor > 1000. Have to verify nontriviality of big $Ш(E)$'s; use visibility and Grigor Grigorov's thesis.