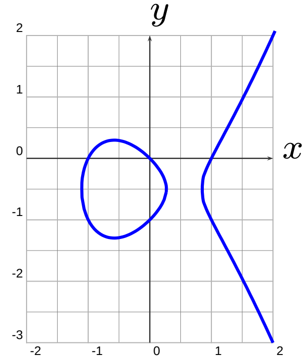
Elliptic Curves over the Rational Numbers $\mathbb{Q}$

An elliptic curve is a nonsingular plane cubic curve with a rational point (possibly "at infinity").



$y^2 + y = x^3 - x$

EXAMPLES

$$y^2 + y = x^3 - x$$

$$x^3 + y^3 = z^3 \text{ (projective)}$$

$$y^2 = x^3 + ax + b$$

$$\cancel{3x^3 + 4y^3 + 5z^3 = 0}$$

Mordell's Theorem

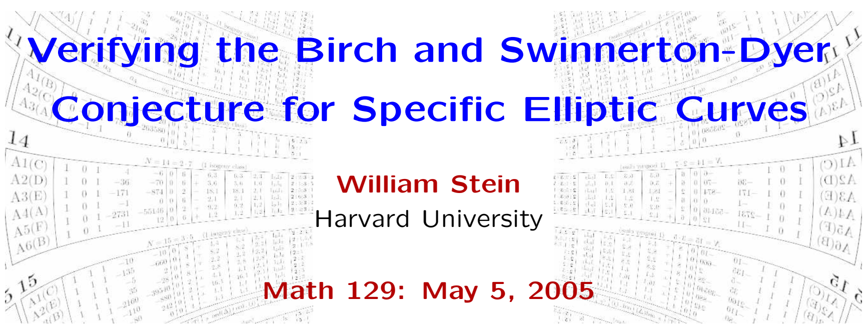
Theorem (Mordell). The group $E(\mathbb{Q})$ of rational points on an elliptic curve is a finitely generated abelian group, so

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T,$$

with $T = E(\mathbb{Q})_{\text{tor}}$ finite.

Mazur classified the possibilities for T.

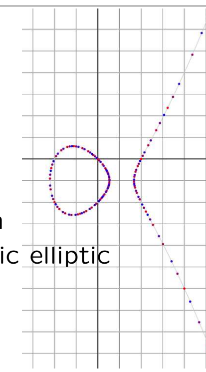
Folklore conjecture: r can be arbitrary, but the biggest r ever found is (probably) 24.



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

William Stein
Harvard University

Math 129: May 5, 2005

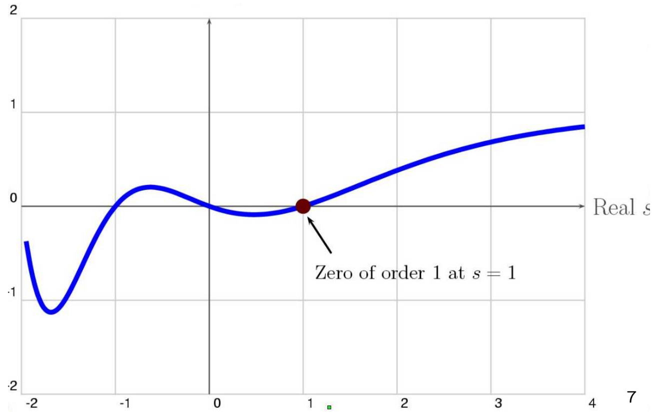


This talk reports on a project to verify the Birch and Swinnerton-Dyer conjecture for many specific elliptic curves over $\mathbb{Q}$.

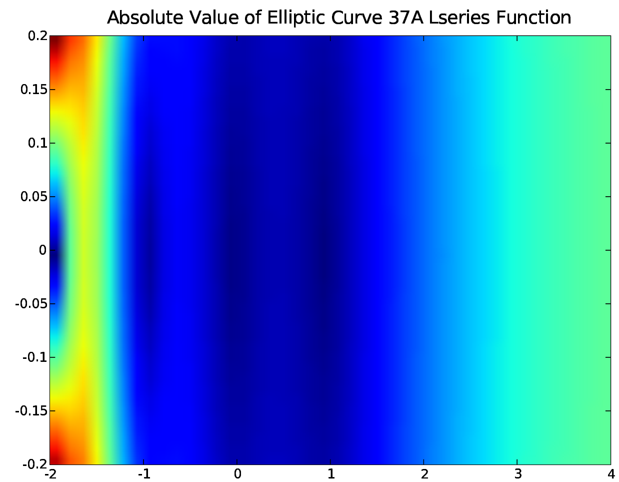
Joint Work: Grigor Grigorov, Andrei Jorza, Corina Patrascu, Stefan Patrikis

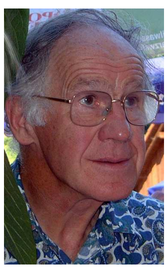
Thanks: John Cremona, Stephen Donnelly, Ralph Greenberg, Grigor Grigorov, Barry Mazur, Robert Pollack, Nick Ramsey, Tony Scholl, Micahel Stoll.

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



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

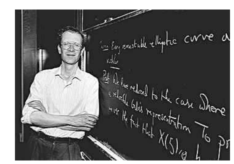




Conjectures Proliferated

"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

The L-Function

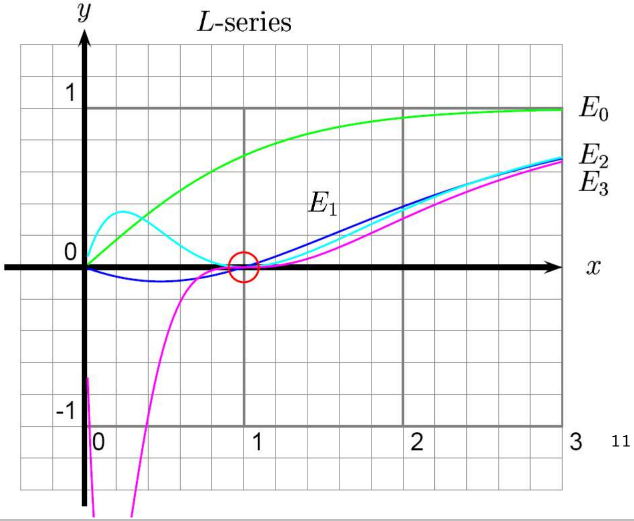


Theorem (Wiles et al., Hecke) The following function extends to a holomorphic function on the whole complex plane:

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

Here $a_p = p + 1 - \#E(\mathbb{F}_p)$ for all $p \nmid \Delta$, where Δ is divisible by the primes of bad reduction for E. We do not include the factors $L_p(E,s)$ at bad primes here.

What about Taylor series of $L(E, s)$ around $s = 1$?



Taylor Series

For $y^2 + y = x^3 - x$, the **Taylor series** about 1 is

$$L(E, s) = 0 + (s - 1)0.3059997\ldots$$

$$+(s - 1)^2 0.18636\ldots + \cdots$$

In general, it's

$$L(E, s) = c_0 + c_1 s + c_2 s^2 + \cdots.$$

Big Mystery: Do these Taylor coefficients c_n have any deep arithmetic meaning?

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.

Motivating Problem 1

Motivating Problem 1. For specific curves, compute every quantity appearing in the BSD formula conjecture **in practice.**

NOTE:

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

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):
   $r_{\text{an}} \leq 1 \implies \text{Ш}(E)$ is finite (with bounds)
   Open Problem:
   Prove that $\text{Ш}(E)$ is finite for some E with $r_{\text{an}} \geq 2$.

BSD Formula Conjecture

Let $r = \text{ord}_{s=1} L(E,s)$. Then Birch and Swinnerton-Dyer made a famous guess for the first nonzero coefficient c_r:

$$c_r = \frac{\Omega_E \cdot \text{Reg}_E \cdot \prod_{p|N} t_p}{\#E(\mathbb{Q})^2_{\text{tor}}} \cdot \#\text{Ш}(E)$$

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

What about c_{r+1}, c_{r+2}, etc?

I think nobody has even a **wild and crazy** guess for an interpretation of these.

They are probably not "periods" like c_r is, so perhaps should not have any nice interpretation...

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 and the above results, 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

We first deal with these four.

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 $N \leq 40000$.
3. All of the quantities in the conjecture, **except** for $\#Ш(E/\mathbb{Q})$, have been computed by Cremona for conductor ≤ 40000.
4. **Cremona (Ch. 4, pg. 106):** We have $2 \nmid \#Ш(E)$ for **all** optimal curves with conductor ≤ 1000 except 571A, 960D, and 960N. So we can mostly ignore 2 henceforth.

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 $3 \,\|\, [E(K) : y_K]$ for $K = \mathbb{Q}(\sqrt{-8})$, so Kolyvagin's 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 $\text{Ш}(E)$ 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. Also, the computations give rise to many surprising and interesting examples.

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 $\Sha$.

Thus our **goal** is to prove that

$$\#\Sha(E) = 1$$

for these 2441 elliptic curves.

Our Strategy

1. [**Find an Algorithm**] Based on deep work of Kolyvagin, Kato, et al.
   Input: An elliptic curve over $\mathbb{Q}$ with $r_{\mathrm{an}} \leq 1$.
   Output: $B \geq 1$ such that if $p \nmid B$, then $p \nmid \#\Sha(E)$.
2. [**Compute**] Run the algorithm on our 2441 curves.
3. [**Reducible**] If $E[p]$ is reducible say nothing.

Kolyvagin Bound on $\#\Sha(E)$

INPUT: An elliptic curve E over $\mathbb{Q}$ with $r_{\mathrm{an}} \leq 1$.
OUTPUT: Odd $B \geq 1$ such that if $p \nmid 2B$, then $p \nmid \#\Sha(E/\mathbb{Q})$.

1. [**Choose K**] Choose a quadratic imaginary field $K = \mathbb{Q}(\sqrt{D})$ with certain properties, such that E/K has analytic rank 1. Assume $\mathbb{Q}(E[p])$ has degree $\#\,\mathrm{GL}_2(\mathbb{F}_p)$.
2. [**Compute Mordell-Weil**]
   (a) If $r = 0$, compute generator z for $E^D(\mathbb{Q})$ mod torsion.
   (b) If $r = 1$, compute generator z for $E(\mathbb{Q})$ mod torsion.

3. [**Index of Heegner point**] Compute the "Heegner point" $y_K \in E(K)$ associated to K. This is a point that comes from the "modularity" map $X_0(N) \to E$.
4. [**Finished**] Output $B = I \cdot A$, where A is the product of primes such that $\mathbb{Q}(E[p])$ has degree less than $\#\,\mathrm{GL}_2(\mathbb{F}_p)$.

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