Elliptic Curves and the Birch and Swinnerton-Dyer Conjecture

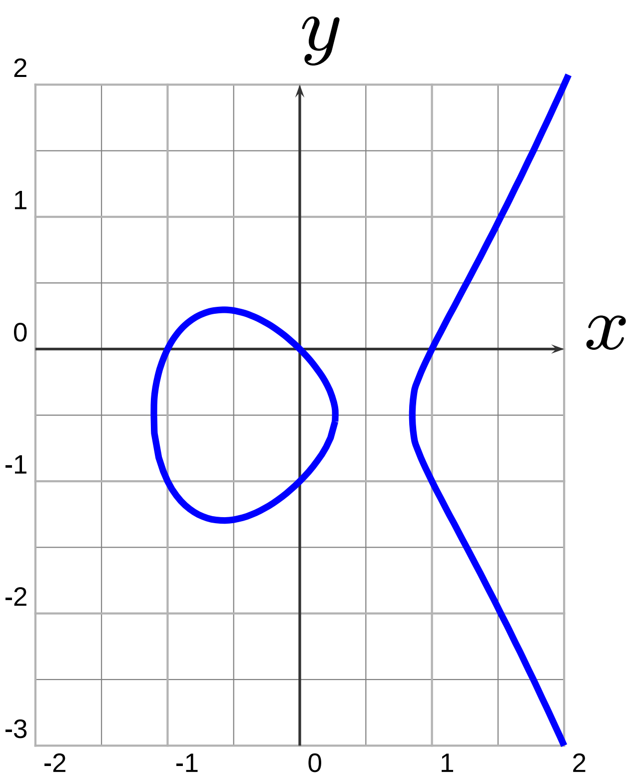
William Stein
Harvard University
http://modular.fas.harvard.edu/129-05/

Math 129: April 5, 2005

This talk is a first introduction to
elliptic curves and the
Birch and Swinnerton-Dyer conjecture.

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

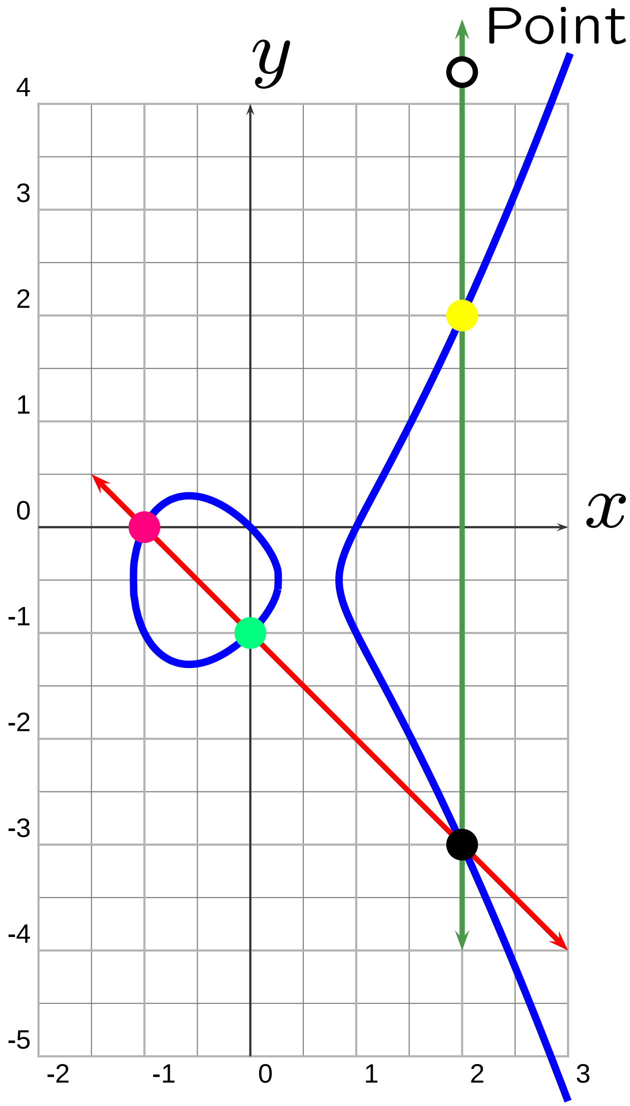
$$y^2 + y = x^3 - x$$

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

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

~~$3x^3 + 4y^3 + 5z^3 = 0$~~

The Group Operation



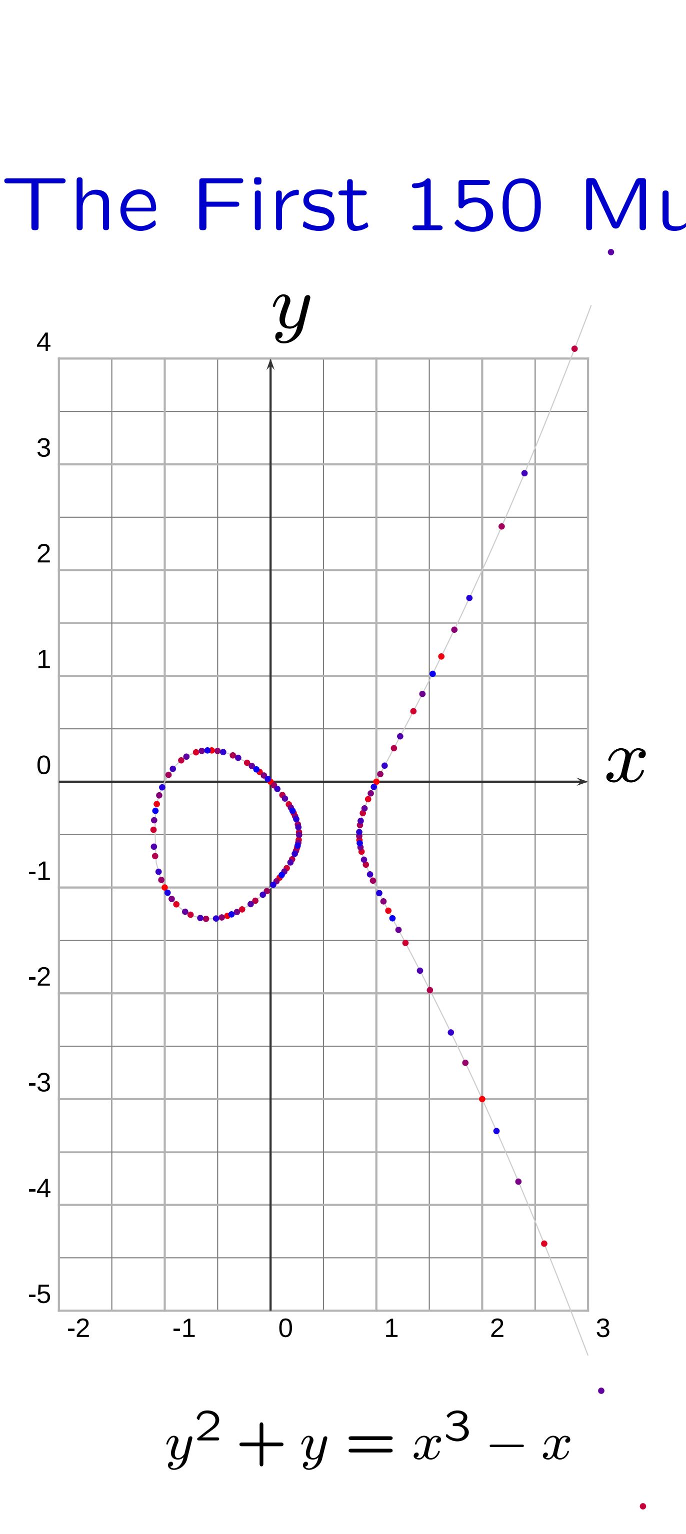
$y^2 + y = x^3 - x$

● $\oplus$ ● $=$ ●

$(-1, 0) \oplus (0, -1) = (2, 2)$

The set of rational points on E forms an abelian group.

The First 150 Multiples of $(0, 0)$



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

(The bluer the point, the bigger the multiple.)

Fact: The group $E(\mathbb{Q})$ is infinite cylic, generated by $(0, 0)$.

In contrast, $y^2 + y = x^3 - x^2$ has only 5 rational points!

Mordell's Theorem

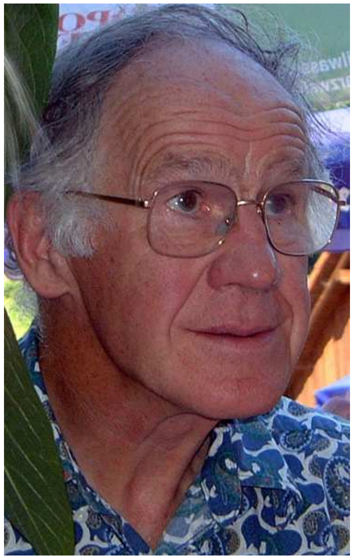
Theorem (Mordell). The group $E(\mathbb{Q})$ of rational points on an elliptic curve is a finitely generated abelian group, so

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

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.



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:

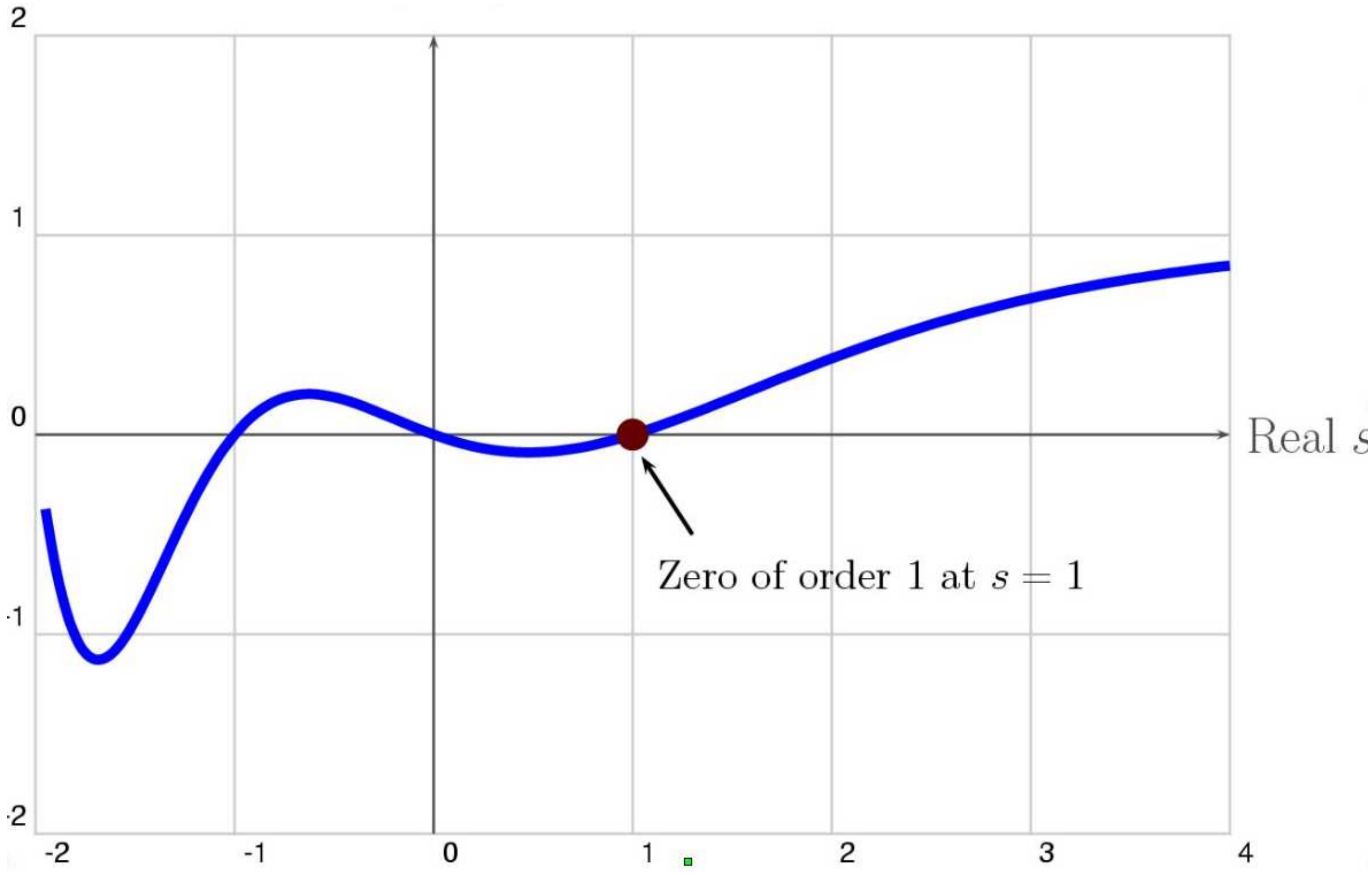
$$L^*(E,s) = \prod_{p\nmid\Delta} \left(\frac{1}{1 - a_p \cdot p^{-s} + p \cdot p^{-2s}} \right).$$

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

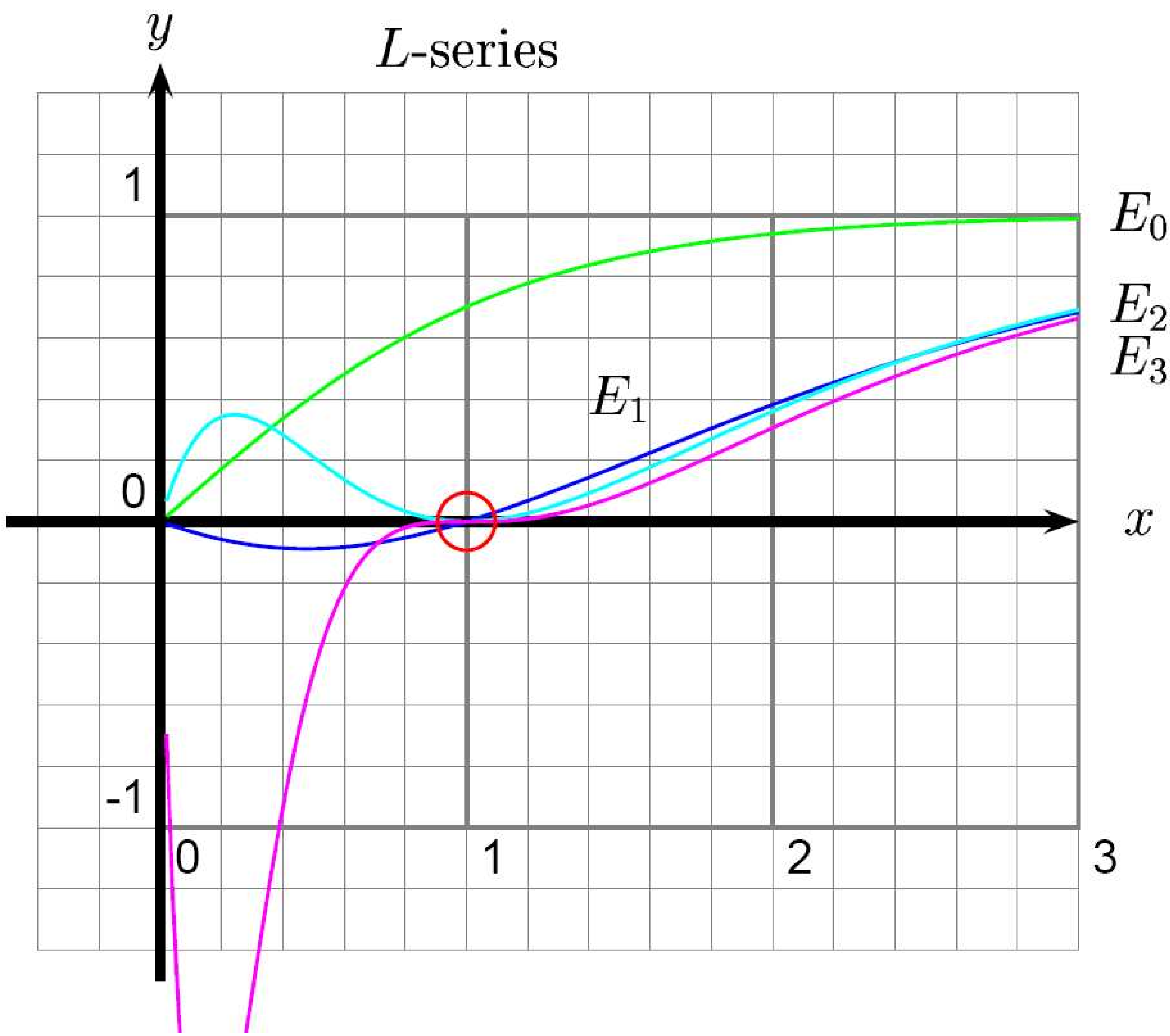
$$L^*(E,1) = \prod_{p\nmid\Delta} \left(\frac{1}{1 - a_p \cdot p^{-1} + p \cdot p^{-2}} \right) = \prod_{p\nmid\Delta} \left(\frac{p}{p - a_p + 1} \right) = \prod_{p\nmid\Delta} \frac{p}{N_p}$$

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



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.

BSD **Conjectural Formula**

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

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

One of My Research Projects

Project. Find ways to 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.

3. Working with Harvard Undergrads: Stephen Patrikas, Andrei Jorza, Corina Patrascu.