The Birch and Swinnerton-Dyer Conjecture

William A. Stein
University of California, Berkeley

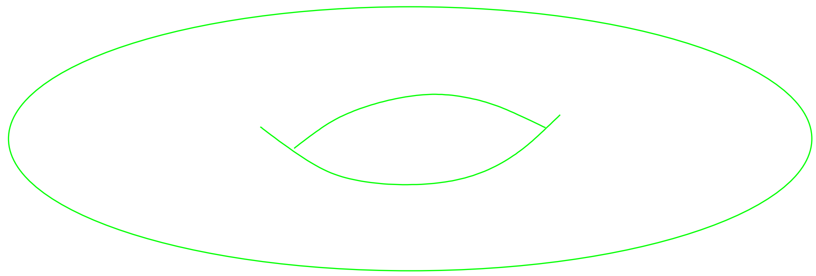
January 10, 2000

Elliptic Curves

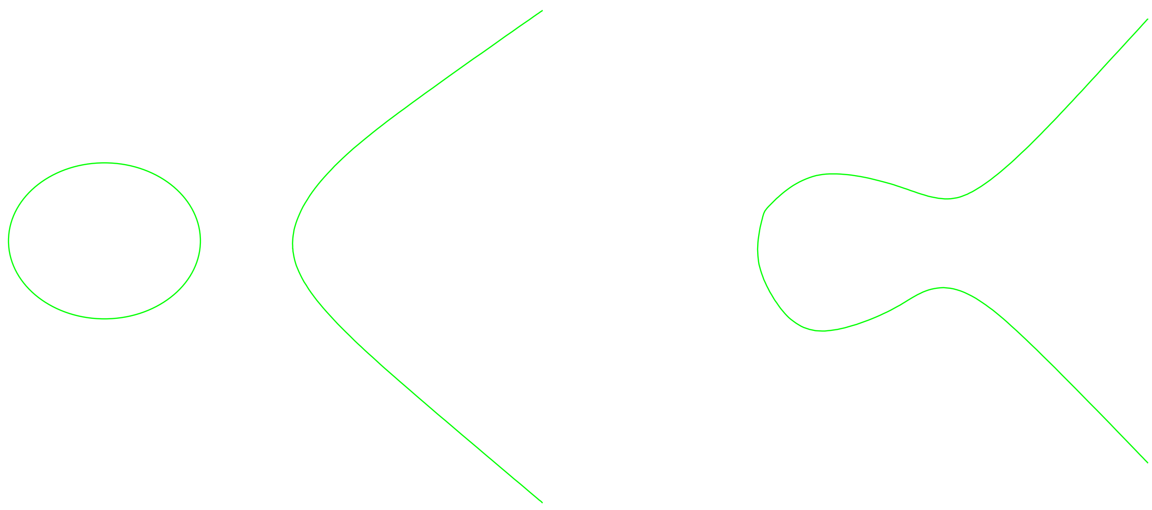
An *elliptic curves* is given by:

$$y^2 = x^3 - ax - b.$$

(Assume a and b are integers.) The complex solutions $(x, y) \in \mathbf{C} \times \mathbf{C}$ are topologically a torus:



The real points look like a cross-section:



Application: FLT

Fermat's Last Theorem. In 1600s Fermat claimed that if $n \geq 3$ and a, b, and c are positive integers such that

$$a^n + b^n = c^n,$$

then $abc = 0$; his margin was too small to support a proof.

Taylor and Wiles showed that for $abc \neq 0$ the *elliptic curve* E given by

$$y^2 = x(x - a^n)(x + b^n)$$

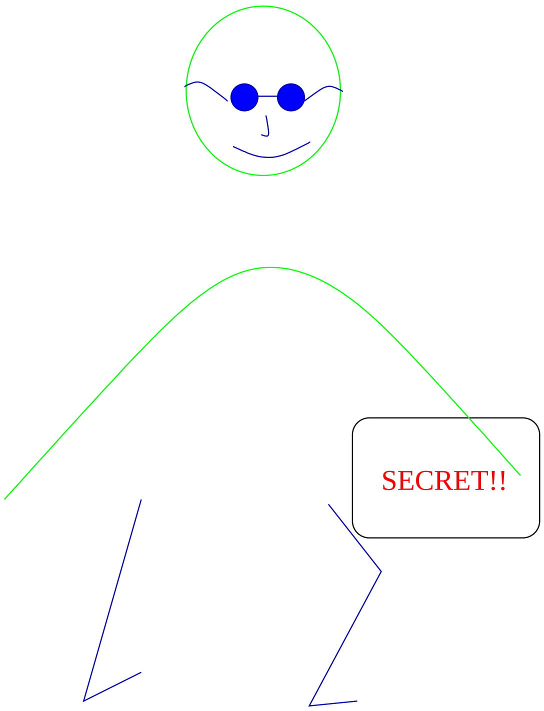
is modular. Ribet had earlier proved that for $n \geq 11$ prime, E is *not* modular, proving Fermat's assertion!

This approach is now central in problems ranging from diophantine equations to the Langlands program.

Application: Cryptography

Elliptic curves help in electronic commerce.

Cryptography. The points on an elliptic curve over a *finite field* form a *finite* group. This group is often an excellent place on which to *implement cryptosystems*.



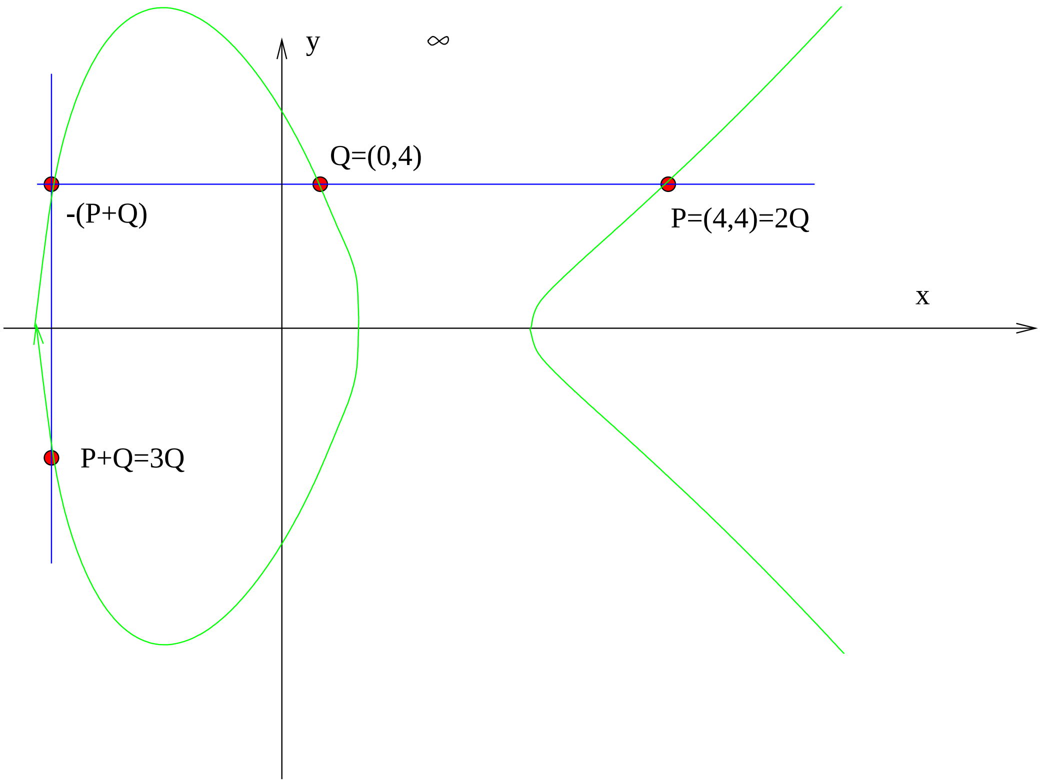
See work of Atkin, Elkies, Koblitz, Schoff.

The Group Law

Two points on an elliptic curve can be *added together* to obtain a third point on the curve. This turns the collection of points into a *group*.

y-axis at the wrong point!!

37A : $\quad y^2 = x^3 - 16x + 16$



The Mordell-Weil Group

Mordell proved the amazing theorem that *every single* point on E with rational coordinates can be obtained from a finite set using the group law! Thus

$$E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus E(\mathbf{Q})_{\text{tors}}$$

with $E(\mathbf{Q})_{\text{tors}}$ a finite group.

Example: *All* points on $y^2 = x^3 - 16x + 16$:

$$\{Q = (0,4), (0,-4), 2Q = (4,4), -2Q = (4,-4),$$

$$\pm 3Q, \pm 4Q, \pm 5Q, \pm 6Q \ldots\}$$

The L-series

There is a complex function attached to E.

$$L(E,s) := \sum_{n\geq 1} a_n n^{-s}$$

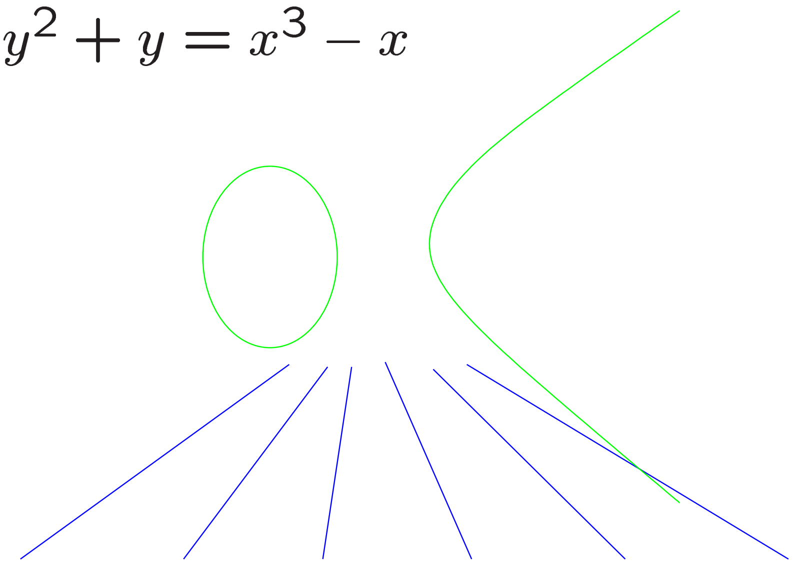
For almost all primes p,

$$a_p = 1 + p - \#E(\mathbf{F}_p).$$

The function $L(E,s)$ is, a priori, defined only for $\Re(s) > \frac{3}{2}$. By the Breuil, Conrad, Diamond, Taylor theorem $L(E,s)$ extends to the whole complex plane.

Examples of $L(E,s)$

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



$\mathbf{F}_2$	$\mathbf{F}_3$	$\mathbf{F}_5$	$\mathbf{F}_7$	$\mathbf{F}_{11}$	$\mathbf{F}_{13}$	
5	7	8	9	17	16	num points

$$\begin{aligned} L(E,s) = & 1 - 2\cdot 2^{-s} - 3\cdot 3^{-s} + 2\cdot 4^{-s} \\ & - 2\cdot 5^{-s} + 6\cdot 6^{-s} - 7^{-s} + 6\cdot 9^{-s} \\ & + 4\cdot 10^{-s} - 5\cdot 11^{-s} - \\ & 6\cdot 12^{-s} - 2\cdot 13^{-s} + \cdots \end{aligned}$$

The Real Volume

Let $E/\mathbf{Q}$ be an elliptic curve. There is a certain cubic model

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

which has *minimal discriminant*. The *real volume* Ω_E is the integral of $\omega = dx/(2y+a_1x+a_3)$ over the real points of this model.

Component groups

For each prime p, the *component group* of E at p measures the "complexity" of the "reduction" of E at p. Let c_p denote its order. (Assume $p \geq 5$, for simplicity.)

- "nonsingular" reduction implies $c_p = 1$ ($x^3 + ax + b$ has distinct roots mod p)

- "cuspidal" reduction implies $c_p \leq 4$ ($x^3 + ax + b$ has a triple roots mod p)

- "nodal" reduction implies c_p can be large, but easy to compute. ($x^3 + ax + b$ has a double roots mod p)

examples, with pictures, above.

The Shaferevich-Tate group

The *Shafarevich-Tate group* $Ш(E)$ measure of the failure of the "local-to-global principle". It is conjectured to be finite. (Omit) For the experts

$$0 \to Ш(E) \to H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), E(\bar{\mathbf{Q}})) \to \prod_v H^1(\mathrm{Gal}(\bar{\mathbf{Q}}_v/\mathbf{Q}_v), E(\bar{\mathbf{Q}}_v)).$$

$Ш$ is the *most mysterious* invariant attached to E.

The Birch and Swinnerton-Dyer conjecture

MAKE FIRST!! **Conjecture.**

$$\frac{L(E,1)}{\Omega_E} = \frac{\#\text{Ш}(E) \cdot \prod c_p}{\#(E(\mathbf{Q}))^2}$$

There is an analogous conjecture when $E(\mathbf{Q})$ is infinite.

BSD: Example

$$E : y^2 = x^3 - 1496259x - 693495810$$

$$\begin{aligned}
E(\mathbf{Q}) &= \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} \\
L(E,s) &= 1 + 2^{-s} - 3^{-s} - 4^{-s} + 2 \cdot 5^{-s} + \cdots \\
L(E,1) &= 1.845756\ldots \\
\Omega_E &= 0.820336\ldots \\
c_3 &= 2 \\
c_{227} &= 2 \\
\#\text{Ш}(A) &= 9(probably!!)
\end{aligned}$$

$$\frac{L(E,1)}{\Omega_E} = \frac{9}{4} = \frac{9 \cdot 2 \cdot 2}{4 \cdot 4} = \frac{\#\text{Ш}(E) \cdot \prod c_p}{\#(E(\mathbf{Q}))^2}$$

[BUT WE DON'T REALLY KNOW!!]

Some Evidence

- Cremona's systematic computations (1000s of examples). Only computes conjectural order of Ш; it "looks right".

- Kolyvagin's work, explicit!!

- Amazing theorem of Kolyvagin and Kato: $L(E, 1) \neq 0$ implies $Ш(E)$ is finite, and p-part of RHS divides left hand side for all but possibly finitely many p.

The Modularity Theorem

There is a family of *abelian varieties*

$J_0(1), J_0(2), \ldots, J_0(11), J_0(12), \ldots, J_0(37), \ldots.$

These are *higher dimensional analogues* of elliptic curves. For example, $J_0(37)$ is an algebraic surface (a 4-dimensional real manifold).

Modularity. For some N there is a surjective "morphism" $J_0(N) \to E$.

The $J_0(N)$'s have a *massive amount* of structure and help us to study E.

Diagram showing E's covered by J's.

Tate's Higher Dimensional Analogue of BSD

Tate found an analogue of BSD that applies, in particular, to any quotient A of $J_0(N)$. It's almost the same:

$$\frac{L(A,1)}{\Omega_A} = \frac{\#\text{Ш}(A)\cdot\prod c_p}{\#A(\mathbf{Q})\cdot\#A^\vee(\mathbf{Q})}$$

where $A^\vee$ is the "dual of A".

Example

$A = J_0(23)$, dimension $A = 2$.

$$\begin{aligned} A(\mathbf{Q}) &= \mathbf{Z}/11\mathbf{Z} \\ A^\vee &= A \\ L(A,s) &= 1 - 2^{-s} - 2\cdot 4^{-s} - 2\cdot 5^{-s} + \cdots \\ L(A,1) &= 0.2484318\ldots \\ \Omega_A &= 2.7327505\ldots \\ c_{23} &= 11 \\ \#Ш(A) &= 1 \qquad \text{(? proved ?)} \end{aligned}$$

$$\frac{L(A,1)}{\Omega_A} = \frac{1}{11} = \frac{1\cdot 11}{11\cdot 11} = \frac{\#Ш(A)\cdot \prod c_p}{\#A(\mathbf{Q})\cdot \#A^\vee(\mathbf{Q})}$$

Tools for Investigation

There are many approaches...

- Kato and Kolyvagin's results generalize, but not all written down.

- *Numerical evidence:* (ONLY THIS ONE!!!) Flynn, Leprévost, Schaefer, Stein, Stoll, Wetherell. Some dimension 2.

- *More evidence:* Agashe, Stein, (plus Mazur and Merel). Compute some invariants of higher dimensional A; use *visibility* plus Kato to try to prove BSD in particular cases.

- *Iwasawa-theory approach:* Greenberg, Perrin-Riou. Get something like p-part for a fixed p for families of A's.

- *Motifs:* Diamond, Flach. Proved some BSD-like conjectures for certain "motifs", i.e., a nearby conjecture.

Component Groups

I found a computable formula for the order of the component group in many interesting cases. This has been very useful in investigations and produced some surprising data.

surprising data

Rational Part of L-function

Amod Agashe and I together obtained results that allowed me to write a program to compute the rational number $L(A,1)/\Omega_A$, up to a "Manin constant" c_A, which we were able to control by following a method of Mazur. For example, if N is square free then c_A is a small power of 2.

Examples...

Visibility

The elliptic curve E of the BSD example before sits inside $J_0(681)$. There is another elliptic curve F with $F(\mathbf{Q})$ infinite and

$$E \cap F = \mathbf{Z}/3 \times \mathbf{Z}/3.$$

Thus E and F are linked at 3; the big Mordell-Weil group of F can probably be used to *explain* the Shafarevich-Tate group of E! This is an example in which $Ш(E)$ is *visible* in $J_0(681)$.

We hope that when BSD predicts nontrivial $Ш$, visibility can be used to prove that BSD is right.

Examples of Visibility

Future Directions

- Find an algorithm for computing the visible subgroup (flat cohomology, congruence theory).

- Combine Kato's work and visibility to produce a healthy list of examples in which the *full BSD conjecture is proved*.

- Determine just how far visibility might take us towards BSD. More precisely, is Ш always visible in a controlled location?