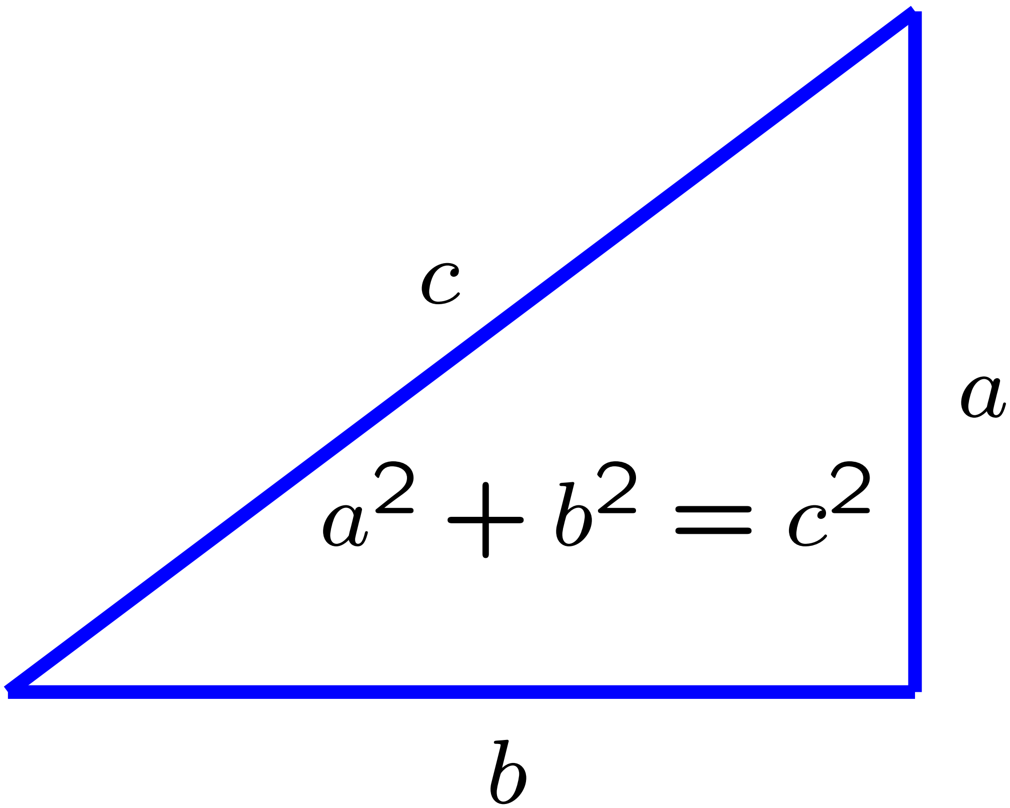
Solving Cubic Equations: An Introduction to the Birch and Swinnerton-Dyer Conjecture

William Stein (`http://modular.ucsd.edu/talks`)

December 1, 2005, UCLA Colloquium

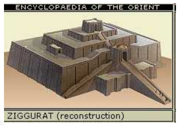
The Pythagorean Theorem



Pythagoras
Approx 569–475BC

$(3, 4, 5)$
$(5, 12, 13)$
$(7, 24, 25)$
$(9, 40, 41)$
$(11, 60, 61)$
$(13, 84, 85)$
$(15, 8, 17)$
$(21, 20, 29)$
$(33, 56, 65)$
$(35, 12, 37)$
$(39, 80, 89)$
$(45, 28, 53)$
$(55, 48, 73)$
$(63, 16, 65)$
$(65, 72, 97)$
$(77, 36, 85)$
$\vdots$

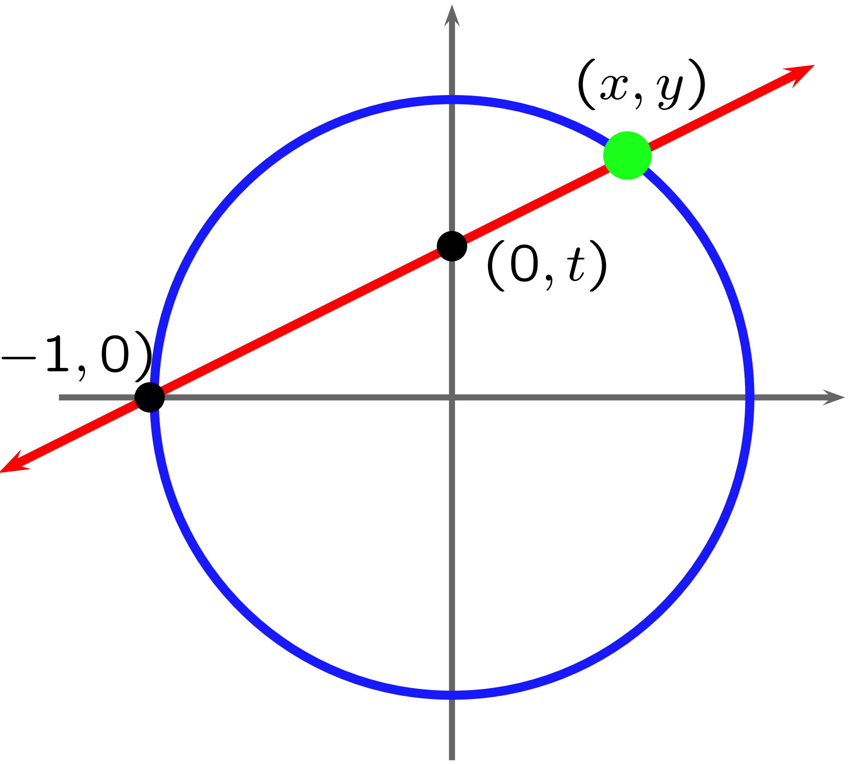
Pythagorean Triples



Triples of integers a, b, c such that

$$a^2 + b^2 = c^2$$

Enumerating Pythagorean Triples



$$\text{Slope} = t = \frac{y}{x+1}$$

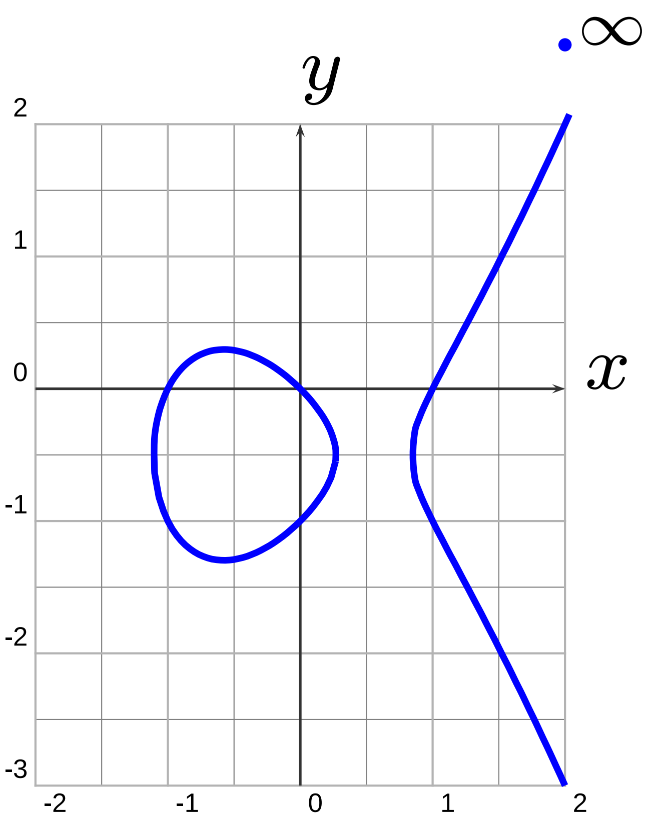
$$x = \frac{1-t^2}{1+t^2}$$

$$y = \frac{2t}{1+t^2}$$

If $t = \frac{r}{s}$, then $a = s^2 - r^2, \quad b = 2rs, \quad c = s^2 + r^2$
is a Pythagorean triple, and all primitive unordered triples arise in this way. **We can solve two-variable quadratic equations.**

What About Two-variable Cubic Equations?

Elliptic curve: a (smooth) plane **cubic curve** with a rational point (possibly "at infinity").



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

EXAMPLES

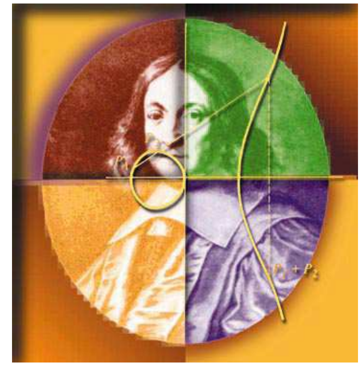
$$y^2 + y = x^3 - x$$

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

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

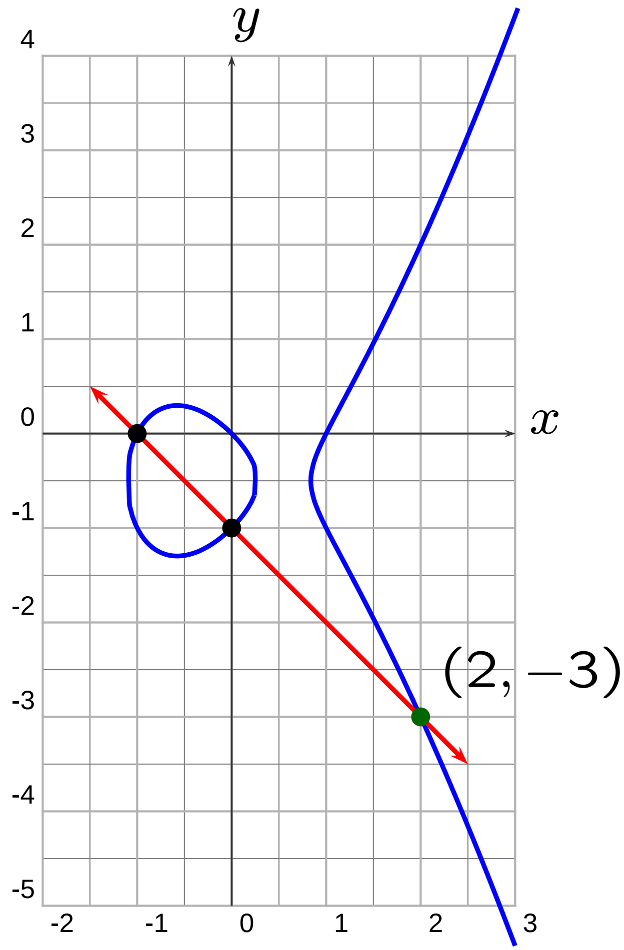
~~$3x^3 + 4y^3 + 5z^3 = 0$~~

The Secant Process



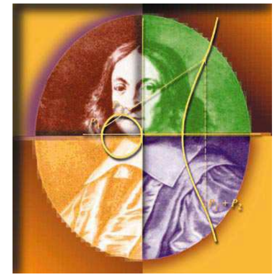
Fermat?

Obtain a third
rational!) solution from
wo (rational) solutions.

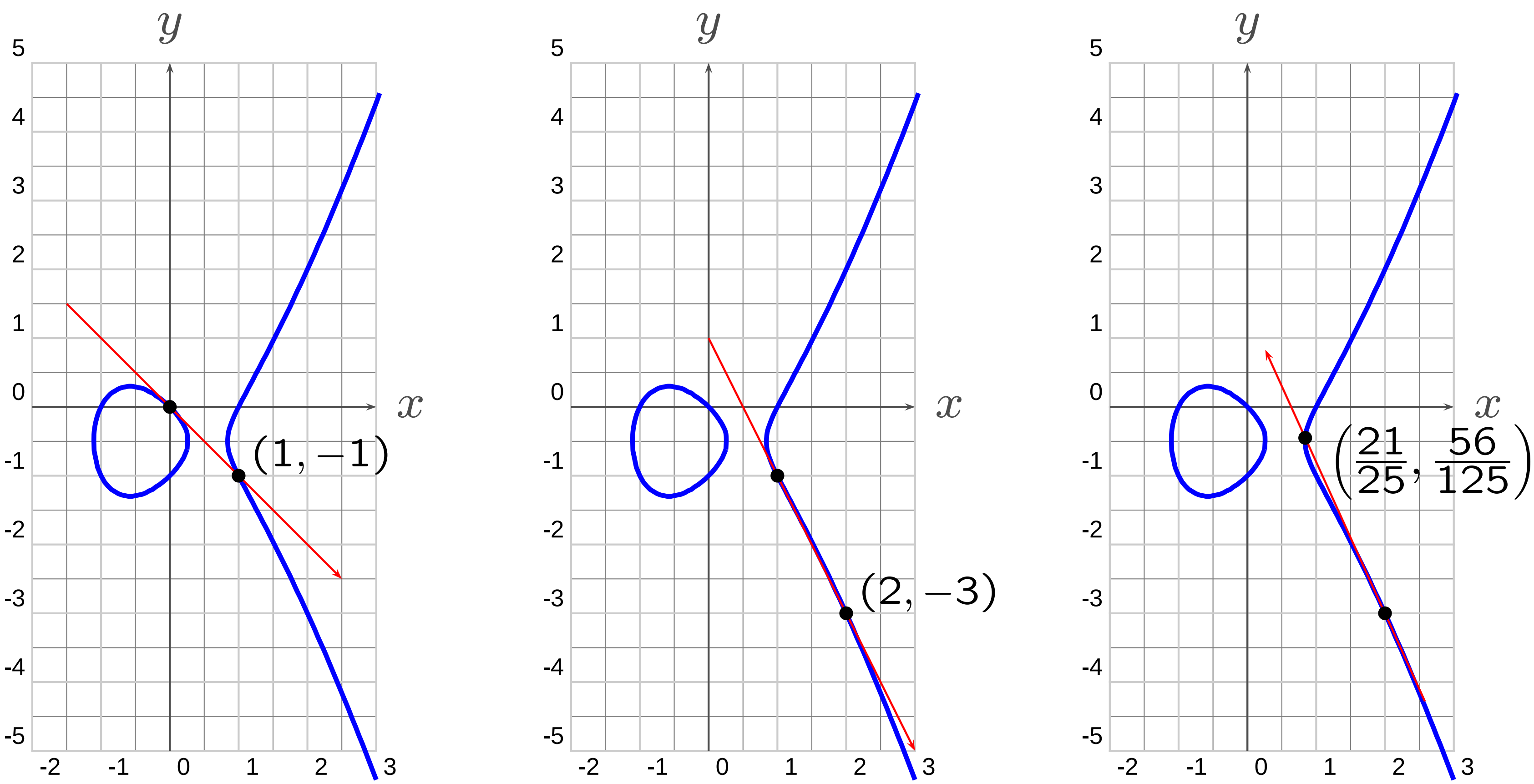


$$y^2 + y = x^3 - x$$

The Tangent Process



New rational point from a single rational point.



Iterate the Tangent Process

Fermat

$$(0,0)$$

$$(1,-1)$$

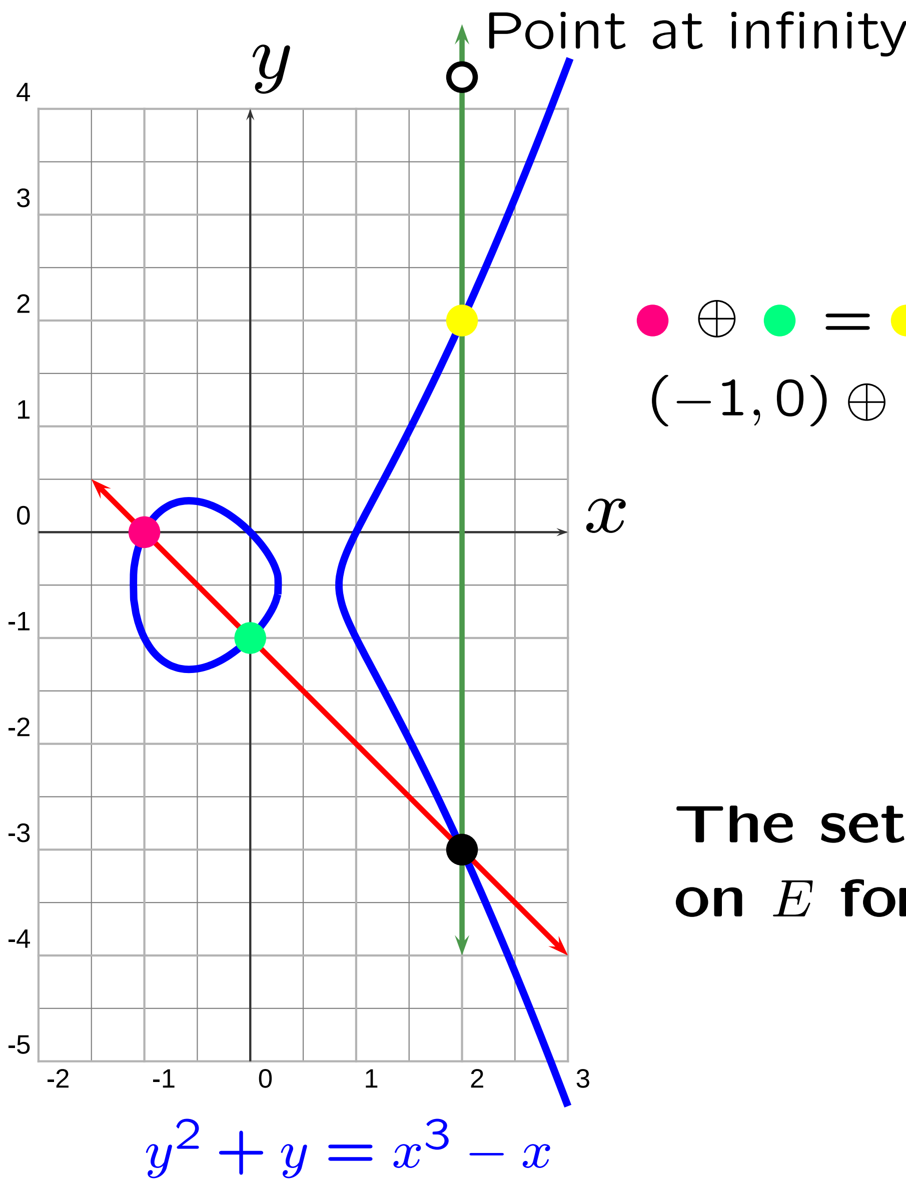
$$(2,-3)$$

$$\left(\frac{21}{25},-\frac{56}{125}\right)$$

$$\left(\frac{480106}{4225},\frac{332513754}{274625}\right)$$

$$\left(\frac{53139223644814624290821}{1870098771536627436025},-\frac{12282540069555885821741113162699381}{80871745605559864852893980186125}\right)$$

The Group Operation



● ⊕ ● = ●

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

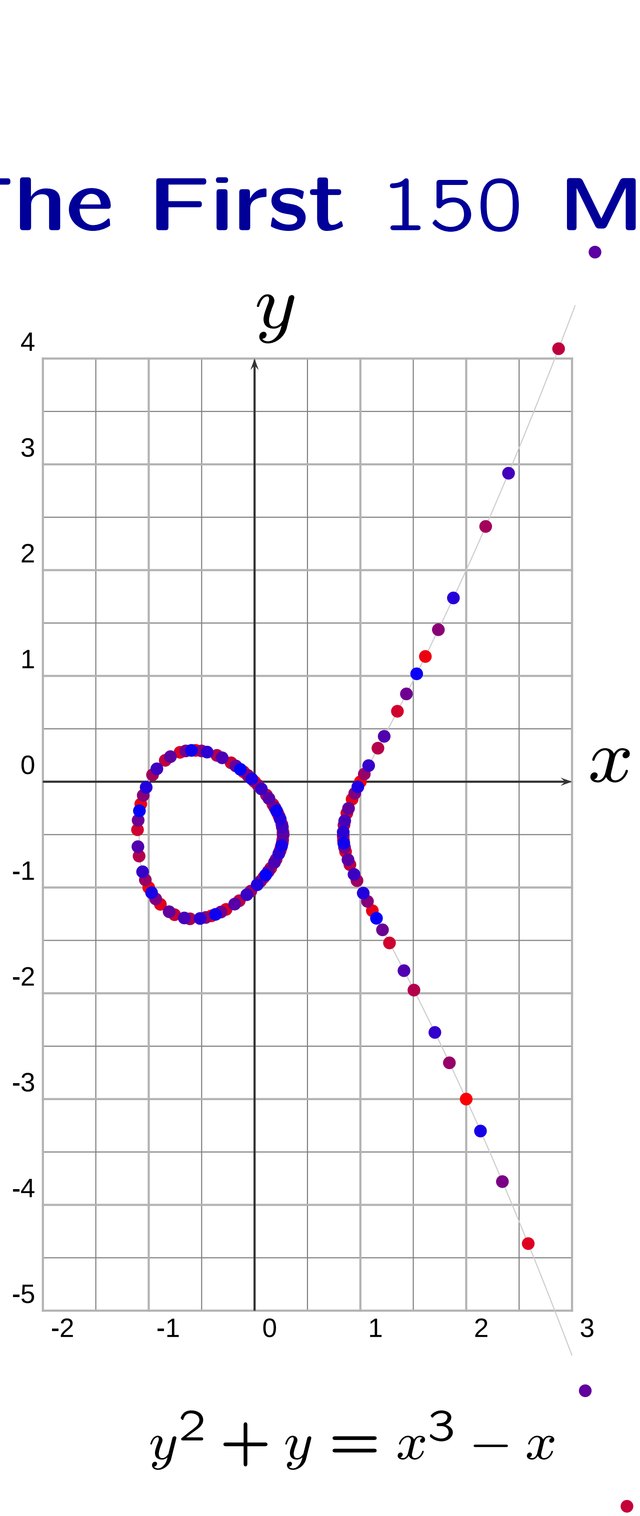
The set of rational points on E forms an abelian group.

SAGE: Software for Algebra and Geometry Experimentation

```
------------------------------------------------------------------------
  SAGE Version 0.7.8, Export Date: 2005-10-05-1650
  Distributed under the terms of the GNU General Public License (GPL)
  IPython shell -- for help type <object>?, <object>??, %magic, or help
------------------------------------------------------------------------
sage: E = EllipticCurve([0,0,1,-1,0])
sage: E
      Elliptic Curve defined by y^2 + y = x^3 - x over Rational Field
sage: P = E([0,0])
sage: 2*P
      (1, 0)
sage: 10*P
      (161/16, -2065/64)
sage: 20*P
      (683916417/264517696, -18784454671297/4302115807744)
sage: 50*P
      (248546717237538199213808226493127519656532099575056065 61/
               29418784545883822188243570198416287437001335203340988816,
      -6534369814499044642835743913597788112480422111355449250724355329451290467397317 3265/
       15956479862127170000582892993100200844174480457307028261899769400071404523797969 2864)
```

Help wanted! `http://modular.ucsd.edu/sage`

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 generated by $(0, 0)$.

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

What is going on here?

Mordell's Theorem

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

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

with T finite.

Mazur classified the possibilities for T. It is conjectured that r can be arbitrary, but the biggest r ever found is (probably) 24.

The Simplest Solution Can Be Huge

Simplest solution to $y^2 = x^3 + 7823$:

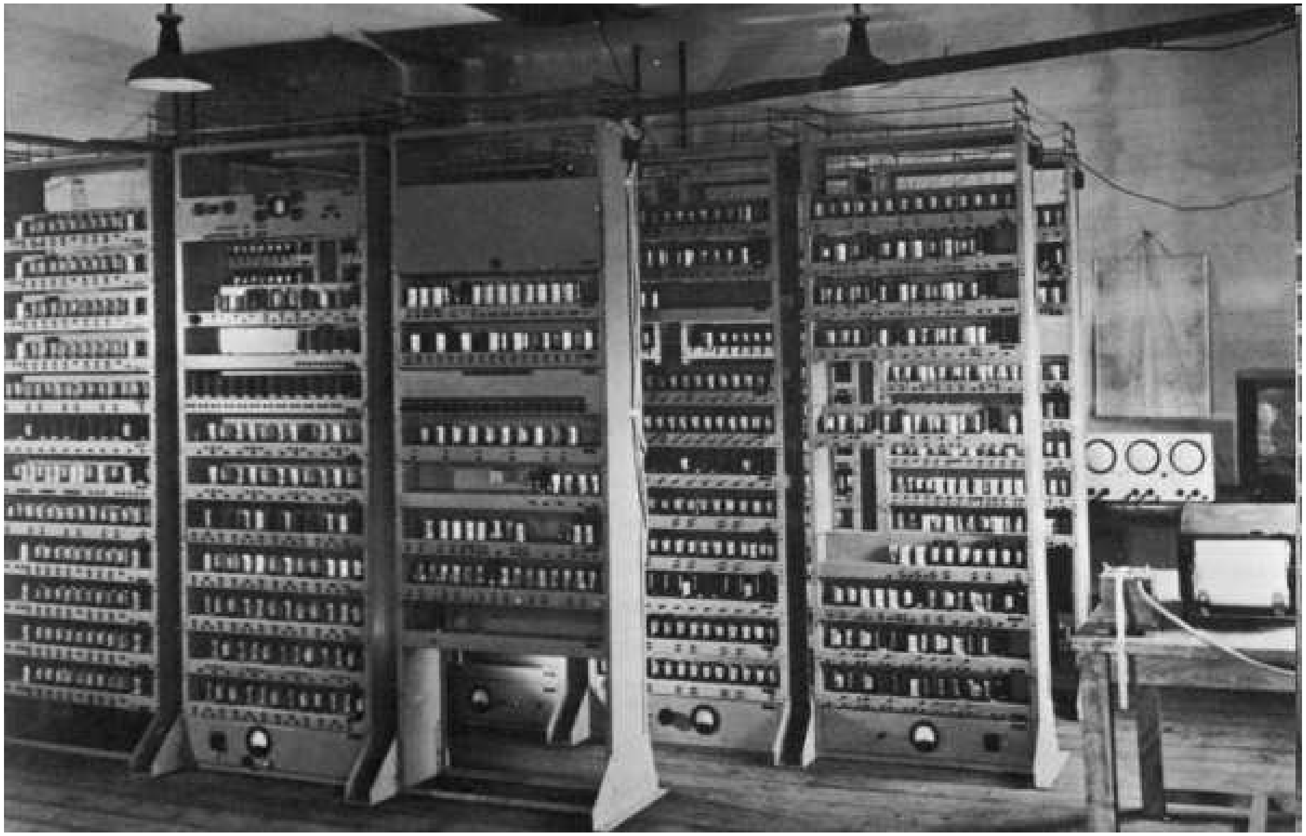
$$x = \frac{2263582143321421502100209233517777}{143560497706190989485475151904721}$$

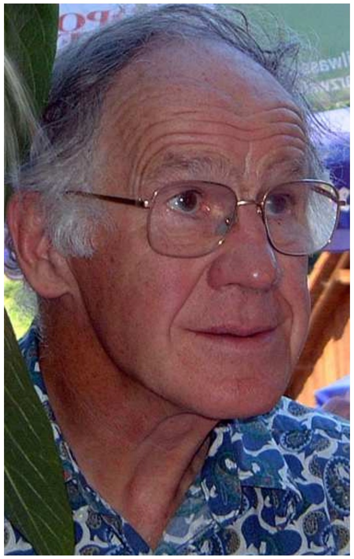
$$y = \frac{186398152584623305624837551485596770028144776655756}{1720094998106353355821008525938727950159777043481}$$

(Found by Michael Stoll in 2002.)

The Central Question

When does an elliptic curve have infinitely many solutions?





Conjectures Proliferated

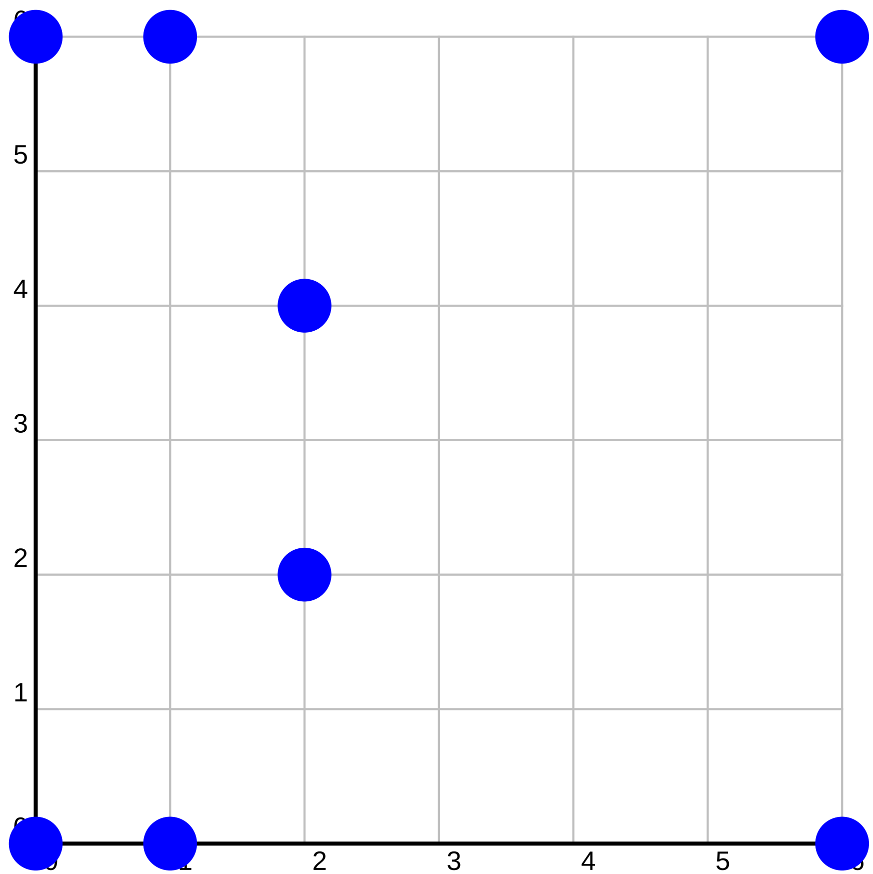
"The subject of this lecture is rather a special one. I want to describe some computations undertaken by myself and Swinnerton-Dyer on EDSAC, by which we have calculated the zeta-functions of certain elliptic curves. As a result of these computations we have found an analogue for an elliptic curve of 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

Counting Solutions Modulo p

$$N(p) = \#\ \text{of solutions}\ \pmod{p}$$

$$y^2 + y = x^3 - x \pmod{7}$$

∞



$$N(7) = 9$$

The Error Term

Let

$$a_p = p + 1 - N(p).$$

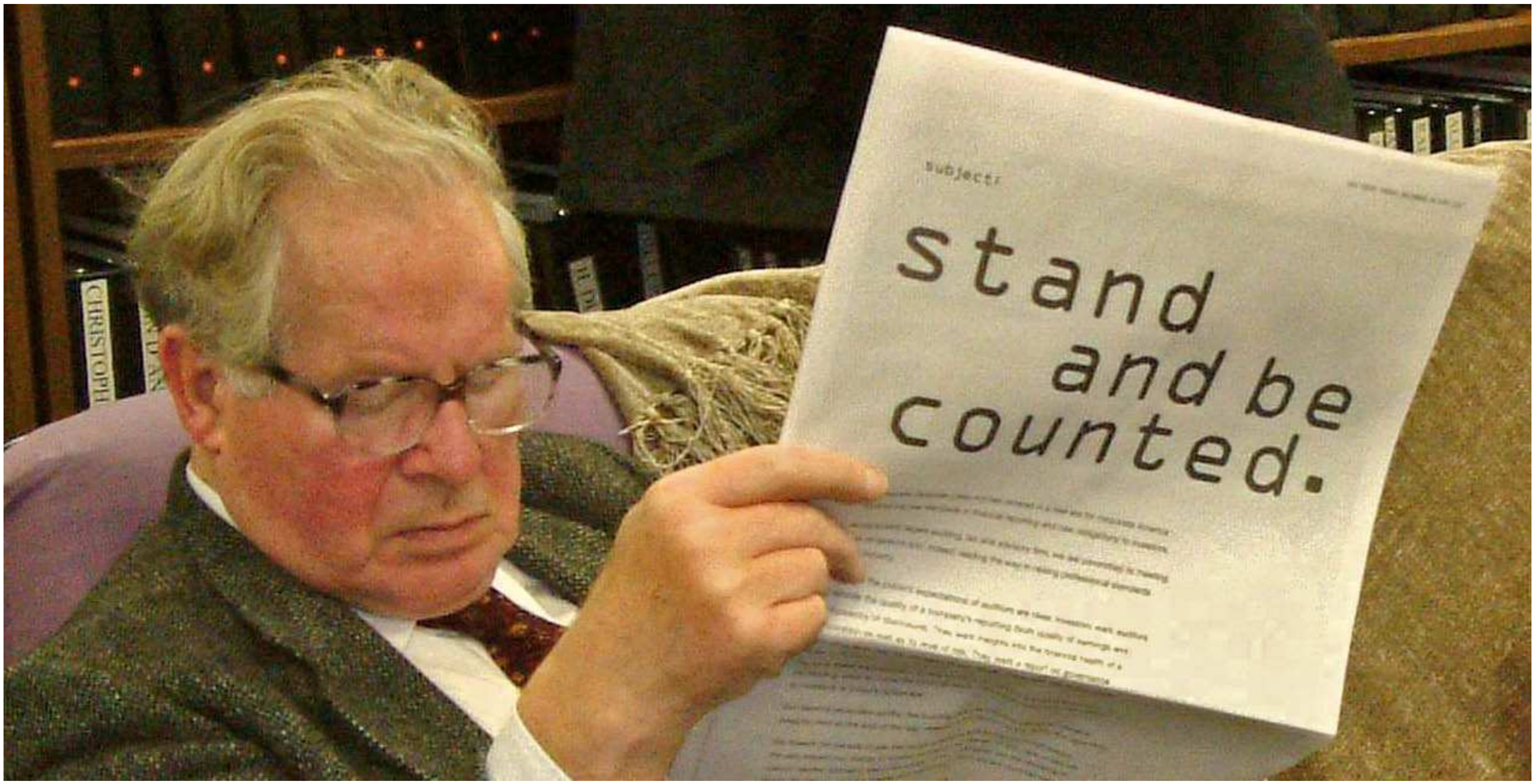
Hasse proved that

$$|a_p| \leq 2\sqrt{p}.$$

$a_2 = -2, \quad a_3 = -3, \quad a_5 = -2, \quad a_7 = -1, \quad a_{11} = -5, \quad a_{13} = -2,$

$a_{17} = 0, \quad a_{19} = 0, \quad a_{23} = 2, \quad a_{29} = 6, \quad \ldots$

Stand and Be Counted



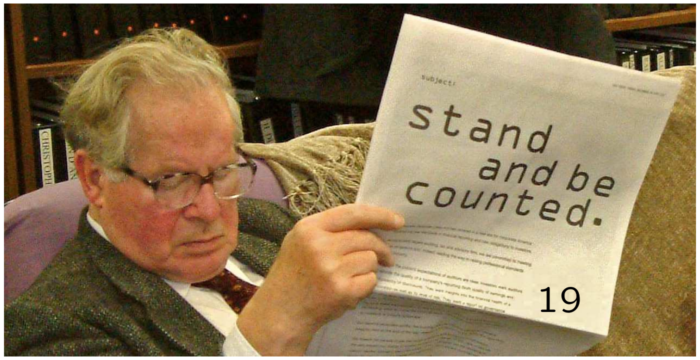
Swinnerton-Dyer

Birch and Swinnerton-Dyer's Guess

If an elliptic curve E has positive rank, then perhaps $N(p)$ is on average larger than p, for many primes p. Maybe

$$f_E(x) = \prod_{p \leq x} \frac{p}{N(p)} \to 0 \textbf{ as } x \to \infty$$

exactly when E **has infinitely many solutions**?



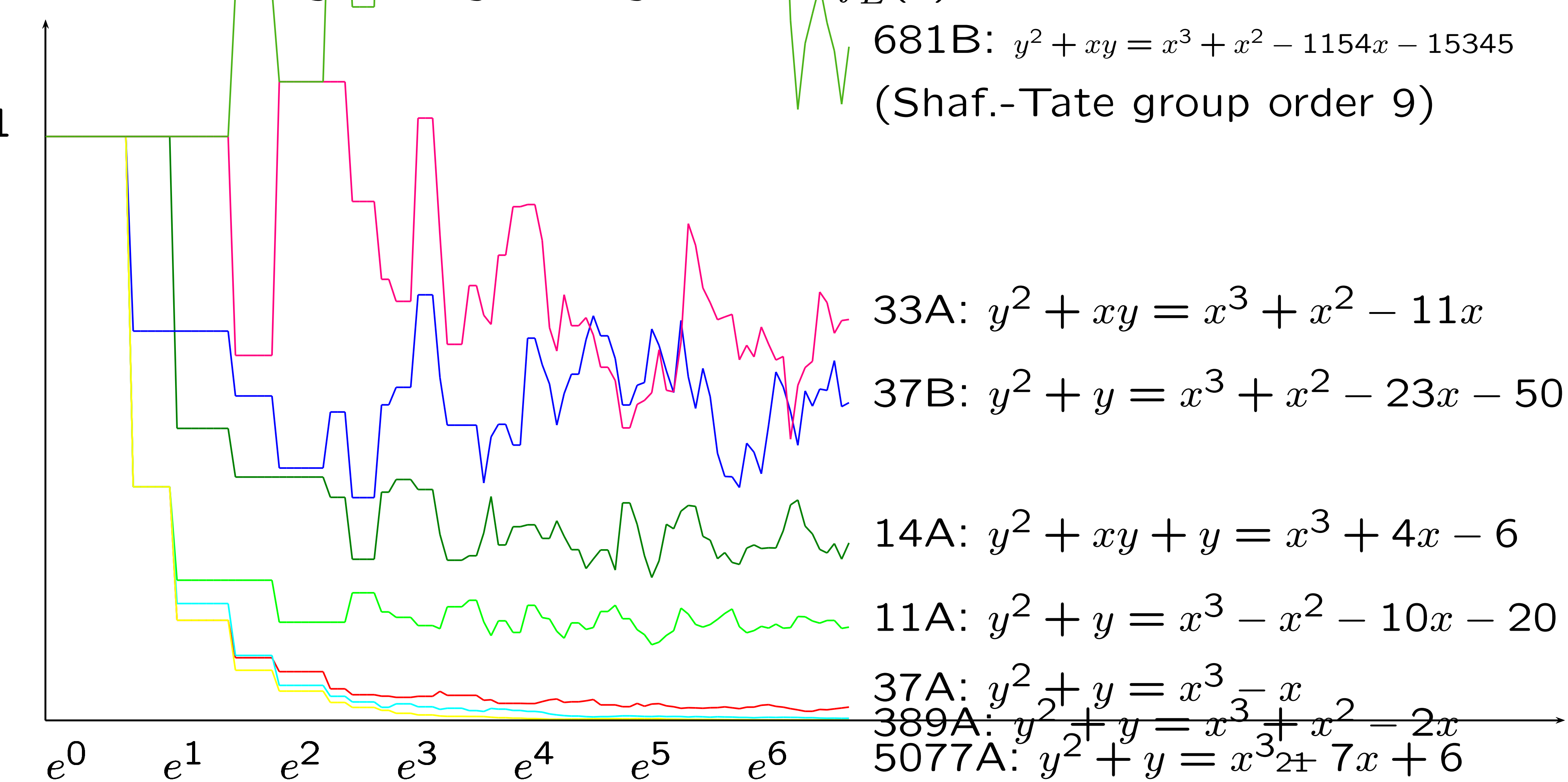
Swinnerton-Dyer

Compute $f_E(x) = \prod_{p \le x} \frac{p}{N(p)}$

```
sage: E = EllipticCurve([0,0,1,-1,0])
sage: E.Np(7)
9
sage: def f(x): return mul([p / E.Np(p) for p in primes(x)])
   ...:
sage: f(3)
      6/35
sage: f(20)
      2717/69120
sage: f(20)*1.0
      0.0393084490740741
sage: def f(x): return mul([float(p / E.Np(p)) for p in primes(x)])
sage: sage: f(10000)
      0.0126925608355528
sage: f(20000)
      0.0136770159557063
sage: f(100000)
      0.0102764628233952
```

Graphs of $f_E(x) = \prod_{p \le x} \frac{p}{N(p)}$

The following are log-scale graphs of $f_E(x)$:



Something Better: The L-Function

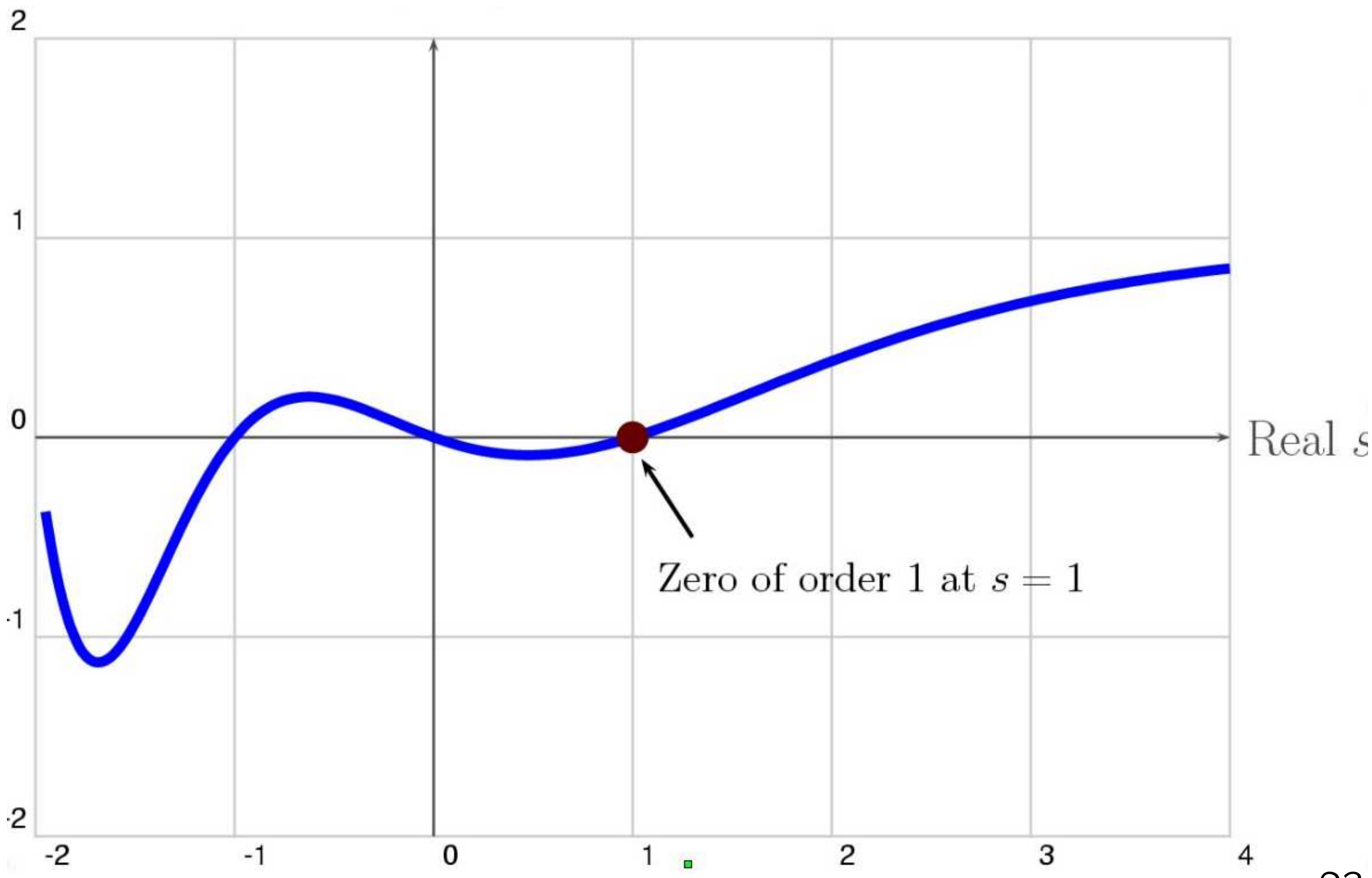
Theorem (Wiles et al., Hecke) This function extends to a holomorphic function on the whole complex plane:

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

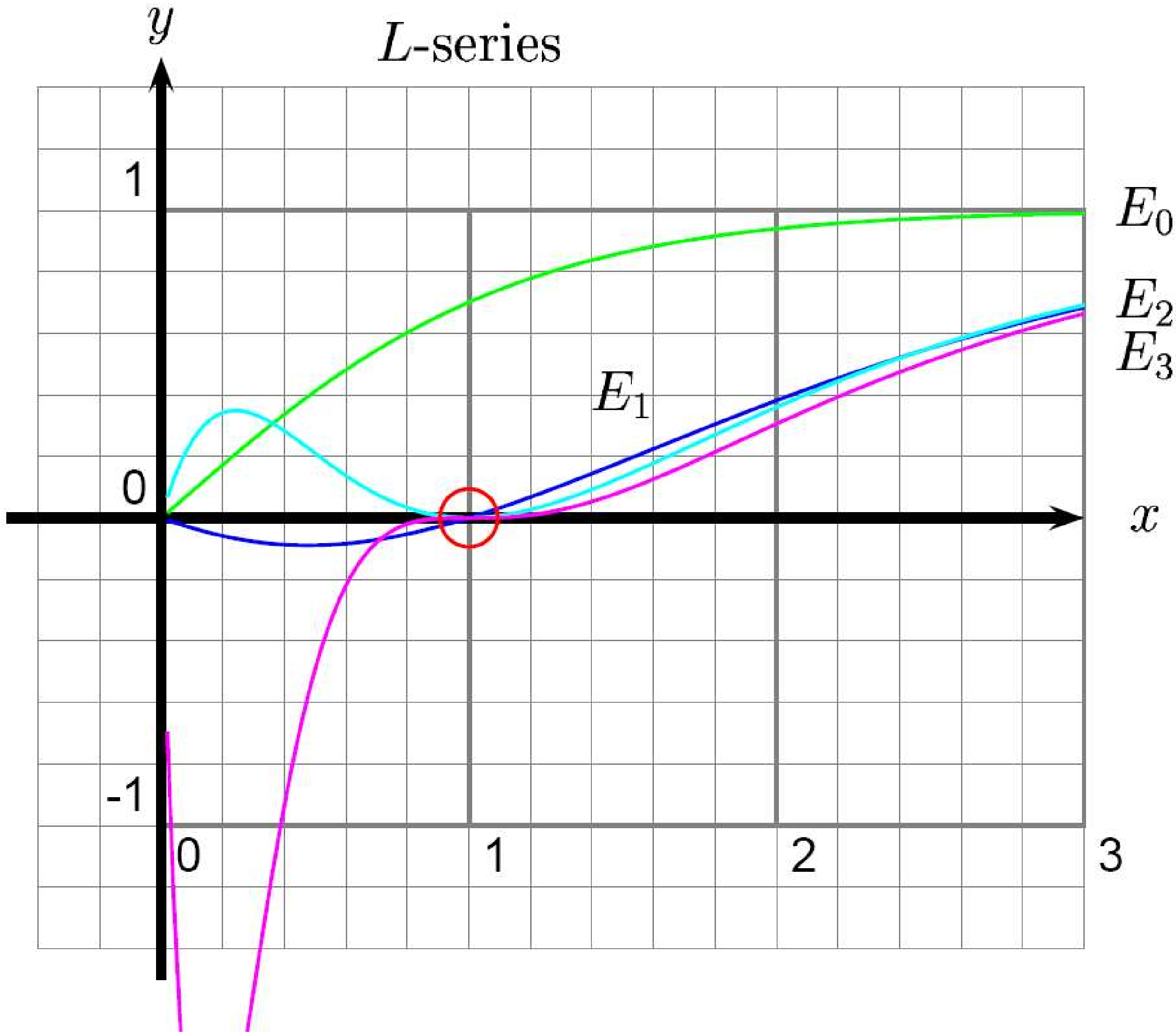
Note that *formally*,

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

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 $\mathbb{Q}$. *Then* E *has infinity many solutions if and only if* $L(E, 1) = 0$*.* (More precisely, the order of vanishing of $L(E, s)$ as $s = 1$ equals the rank of $E(\mathbb{Q})$.)

The Kolyvagin, Gross-Zagier, Kato Theorem

Theorem 1: If $L(E,1) \neq 0$ then E has only finitely many solutions. If $L(E,1) = 0$ but $L'(E,1) \neq 0$, then $E(\mathbb{Q})$ has rank 1.

Ranks of Elliptic Curves

Order elliptic curves by conductor.

Folklore Conjecture: 100% of elliptic curves satisfy the hypothesis of Theorem 1, i.e., have $\text{ord}_{s=1} L(E, s) \leq 1$.
Moreover the average rank is $1/2$.

Should we believe this folklore conjecture?

Joint work with: Barry Mazur, Mark Watkins, Baur Bektemirov

Genus

Question Suppose C is an algebraic curve with a rational point. How likely is it that C will have infinitely many rational points?

- **Genus** 0 – probability 1 (e.g., Pythagorean triples)

- **Genus** 1 – probability 1/2??? (elliptic curves)

- **Genus** ≥ 2 – probability 0 (Faltings's theorem)

A Story

1. **The minimalist conjecture.** As above, it has long been a folk conjecture that the average rank of elliptic curves is $1/2$.

2. **Refined heuristics for special families.** For $y^2 = x^3 - d^2x$, prediction that number of those with even parity and infinitely many rational points is asymptotic to

$$F(D) = c \cdot D^{3/4} \log(D)^{11/8} \tag{1}$$

3. **A random matrix heuristic.**

4. **Contrary numerical data.**

Manjul Bhargava

A new **non-minimalist** **theorem** for number fields.

Theorem. *When ordered by absolute discriminant,* a positive proportion *(approximately 0.09356) of quartic fields have associated Galois group* D_4*. The remaining approximately 0.90644 of quartic fields have Galois group* S_4*.*

Goldfeld's Conjecture

Family E_d of quadratic twists, e.g., $y^2 = x^3 - d^2x$.

Conjecture. The average rank of the curves E_d is $\frac{1}{2}$, in the sense that

$$\lim_{D\to\infty} \frac{\sum_{|d|<D} \mathrm{rank}(E_d)}{\#\{d : |d| < D\}} = \frac{1}{2}.$$

(Here the integers d are squarefree.)

Random Matrix Theory Heuristic (Watkins)

Conjecture:

- Number of curves of even rank ≥ 2 up to conductor X is

$$\sim X^{19/24} \exp(c_1 \sqrt{\log X}).$$

- Number of elliptic curves of conductor up to X is

$$\sim X^{5/6} \exp(c_2 \sqrt{\log X}).$$

Note that $19/24 \sim 0.792$ and $5/6 \sim 0.833$.

Brumer-McGuinness Rank Distribution

Rank	0	1	2	3	4	5
Proportion	0.300	0.461	0.198	0.038	0.003	0.000

Average Rank: 0.982

Rank Distribution of Cremona's Database (Conductor ≤ 120000)

Rank	0	1	2	3
Proportion	0.404	0.505	0.090	0.001

Average Rank: 0.688

The Stein-Watkins Database

Any $E/\mathbb{Q}$ is given by exactly one equation of the form

$$y^2 = x^3 - 27c_4x - 54c_6, \qquad (2)$$

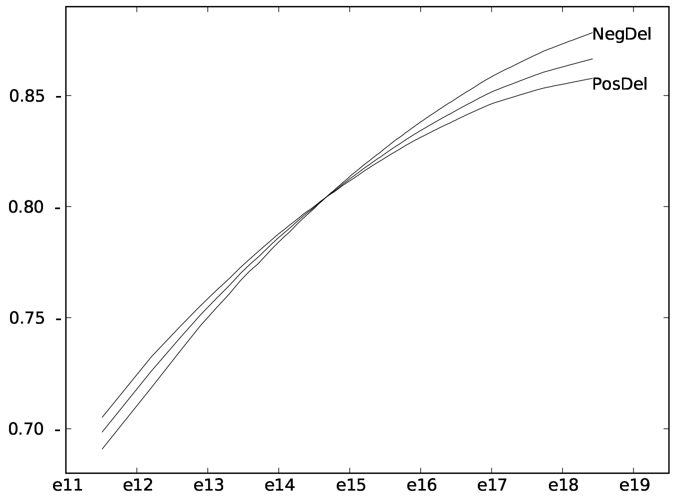
with $c_4, c_6, \Delta = (c_4^3 - c_6^2)/1728 \in \mathbb{Z}$ and for which there is no prime p with $p^4 \mid c_4$ and $p^{12} \mid \Delta$.

Stein-Watkins Database: All $E/\mathbb{Q}$ with $|c_4| < 1.44 \cdot 10^{12}$, $|\Delta| < 10^{12}$ and composite conductor $< 10^8$ or prime conductor $< 10^{10}$. Plus all quadratic twists and isogenous curves.

Type	**Number**
Curves with conductor $\leq 10^8$	136832795
Curves with square-free conductor $\leq 10^8$	21841534
Curves with prime conductor $\leq 10^{10}$	11378911
Curves with prime conductor $\leq 10^8$	312435

Rank Distribution Among All Curves of Conductor $\leq 10^8$

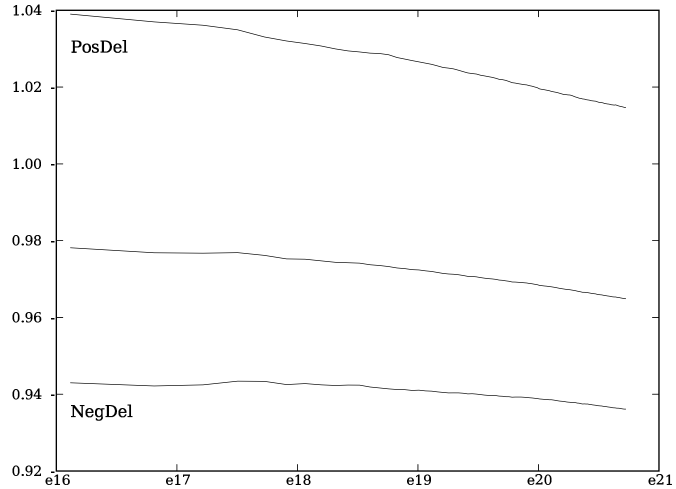
Rank	0	1	2	3	≥ 4
Proportion	0.336	0.482	0.163	0.019	0.000



Average Rank: 0.865

Rank Distribution for Prime Conductor $\leq 10^{10}$

Rank	0	1	2	3	≥ 4
Proportion	0.309	0.462	0.188	0.037	0.004



Average Rank: 0.964

Rank Distribution For About 150000 Random Curves With Prime Discriminant Near 10^{14}

Rank	0	1	2	3	≥ 4
Proportion	0.332	0.471	0.164	0.029	0.003

Average Rank: 0.901