The Birch and Swinnerton-Dyer Conjecture

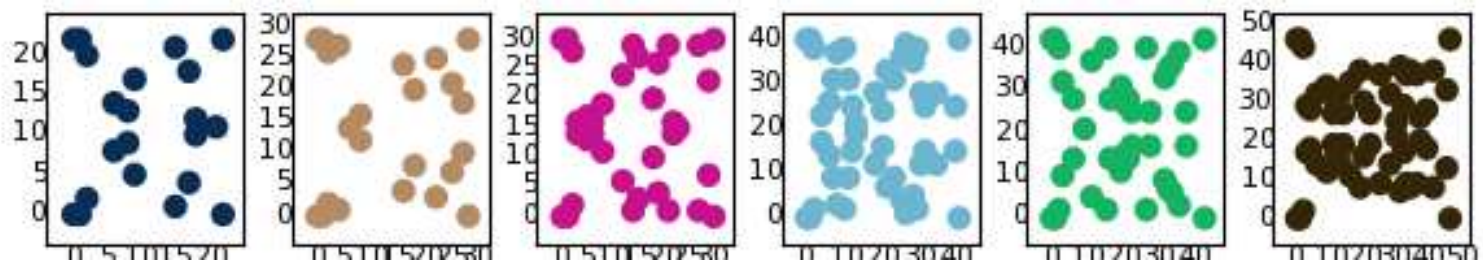
William Stein

June 1, 2007, Math 480 Final Class

The Millenium Problems

In 2000, the Clay Mathematics Institute, offered one million dollars each for seven problem in different areas of mathematics. The algebraic number theory problem they chose is the Birch and Swinnerton-Dyer conjecture.

> Supported by much experimental evidence, this conjecture relates the number of points on an elliptic curve mod p to the rank of the group of rational points. Elliptic curves, defined by cubic equations in two variables, are fundamental mathematical objects that arise in many areas: Wiles' proof of the Fermat Conjecture, factorization of numbers into primes, and cryptography, to name three.



Points on an elliptic curve modulo primes

Degree

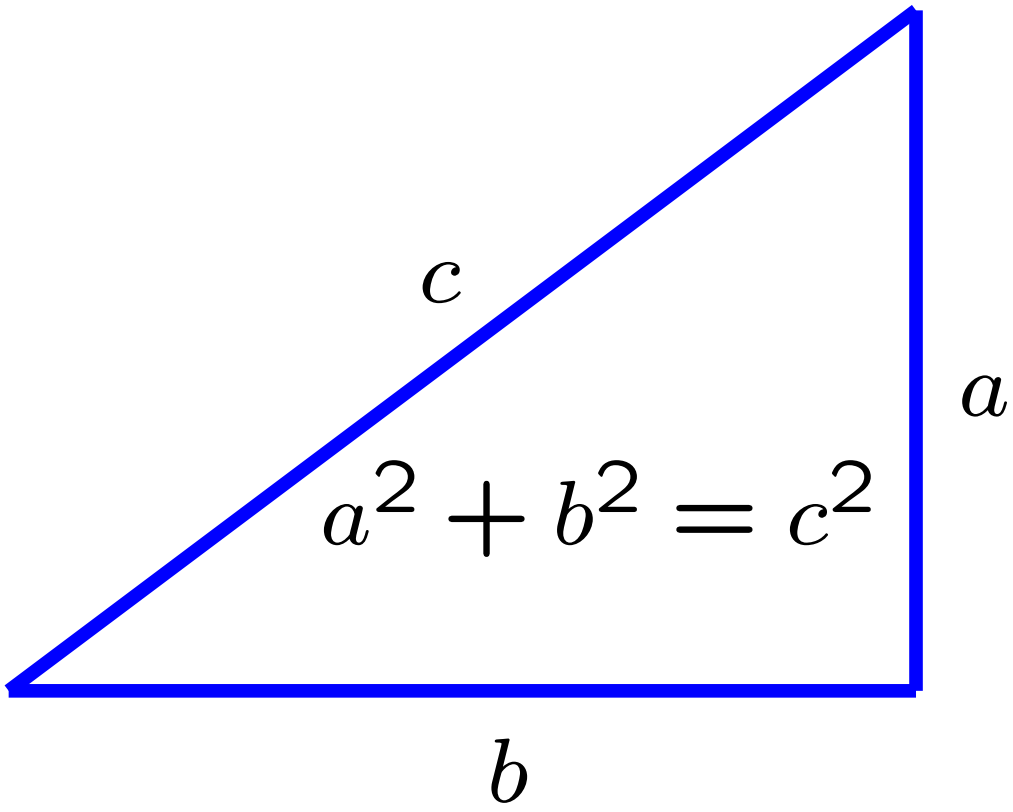
Consider nonsingular plane curves.

- **Ancient Theorem:** A curve of **degree 1 or 2** has infinitely many solutions or no solutions. **E.g.,** $x^2 + y^2 = 1$

- **Faltings Theorem:** A curve of **degree 4 or greater** has finitely many rational solutions. **E.g.,** $x^n + y^n = 1$ **with** $n \geq 4$

- **The Birch and Swinnerton-Dyer Conjecture:** A curve of **degree 3** has either no solutions, a nonzero finite number of solutions, or infinitely many solutions, and there are is a fairly simple way to decide which. **E.g.,** $x^3 + y^3 = 1$

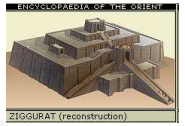
The Pythagorean Theorem

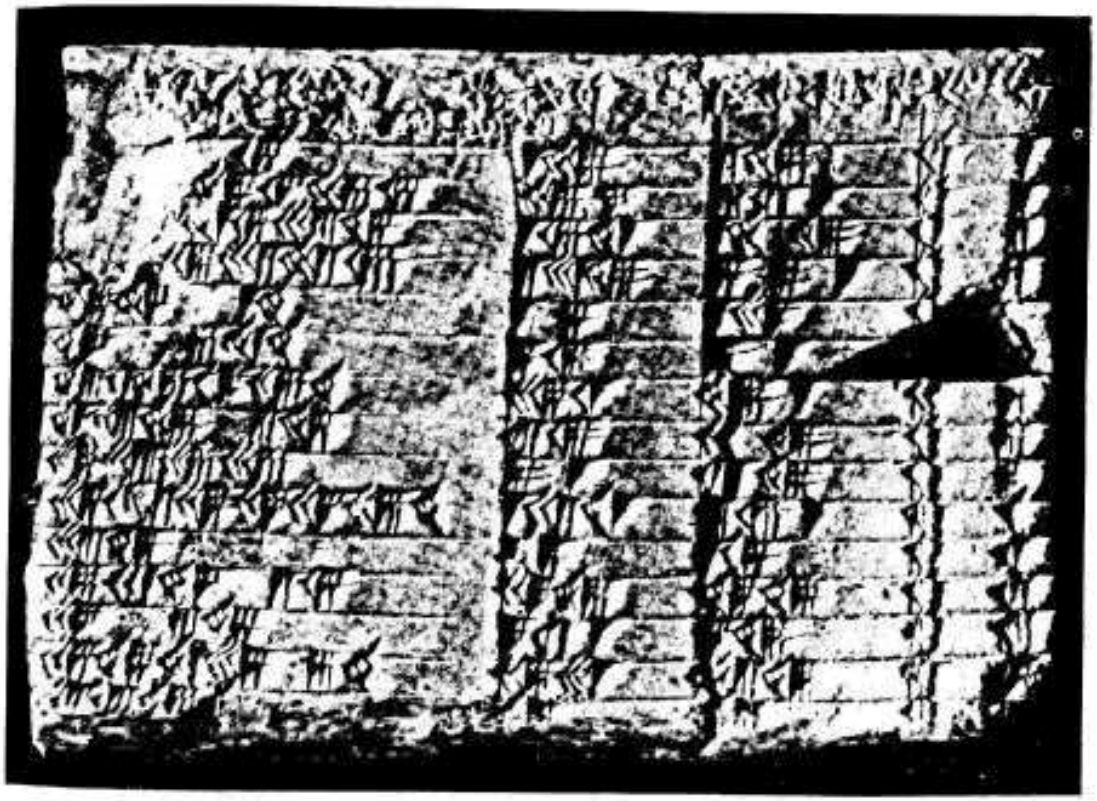


Pythagoras
Approx 569–475BC

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

Pythagorean Triples

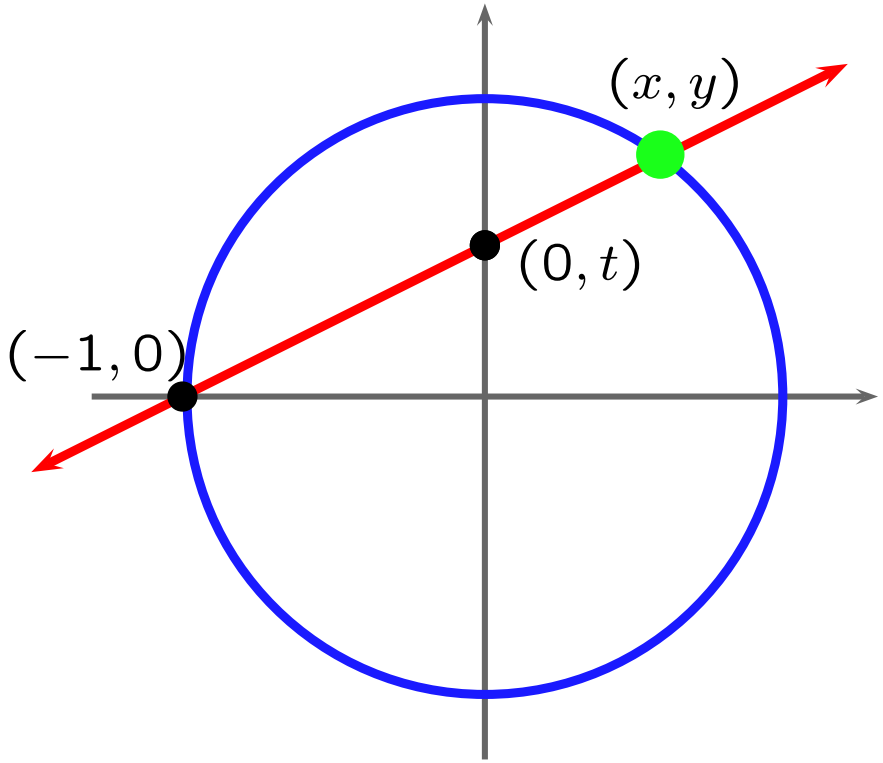




Triples of integers a, b, c such that

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

Enumerating Pythagorean Triples



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

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

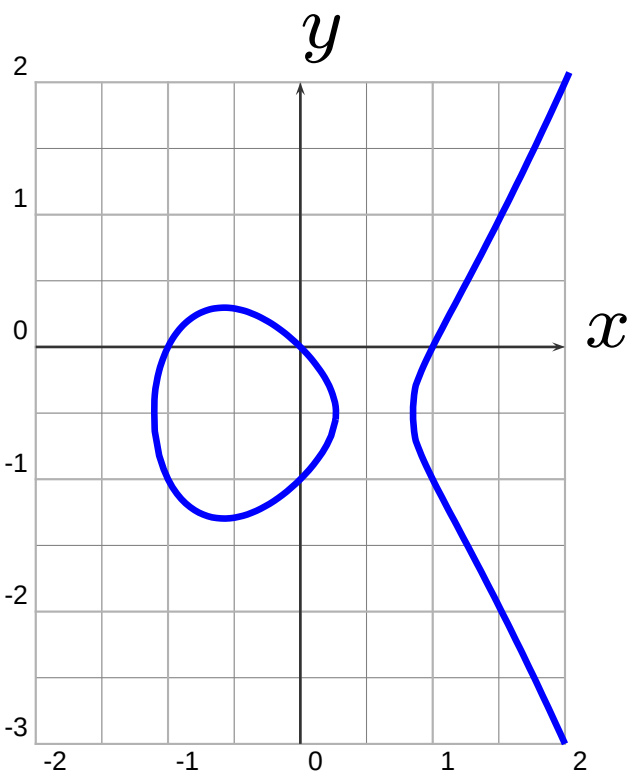
$$y = \frac{2t}{1+t^2}$$

If $t = \frac{r}{s}$, then $\quad a = s^2 - r^2, \quad b = 2rs, \quad c = s^2 + r^2$

is a Pythagorean triple, and all primitive unordered triples arise in this way.

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

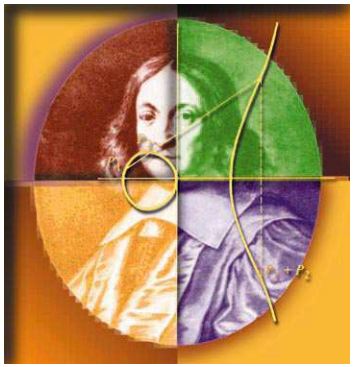
$$y^2 + y = x^3 - x$$

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

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

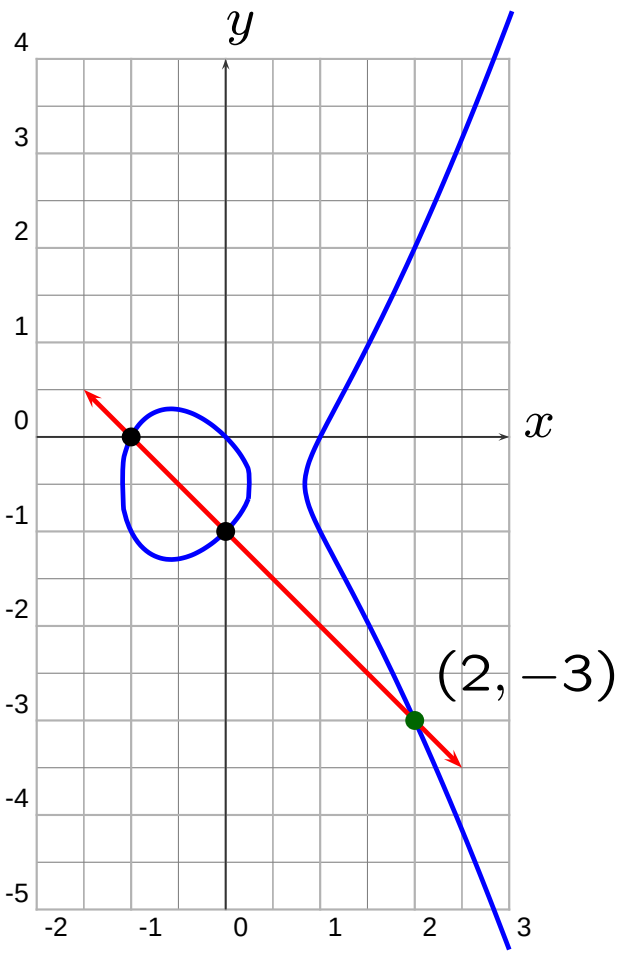
~~$3x^3 + 4y^3 + 5z^3 = 0$~~

The Secant Process



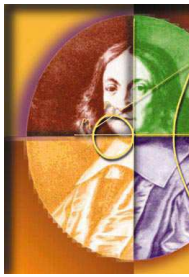
Fermat

Obtain a third rational point from two rational points.

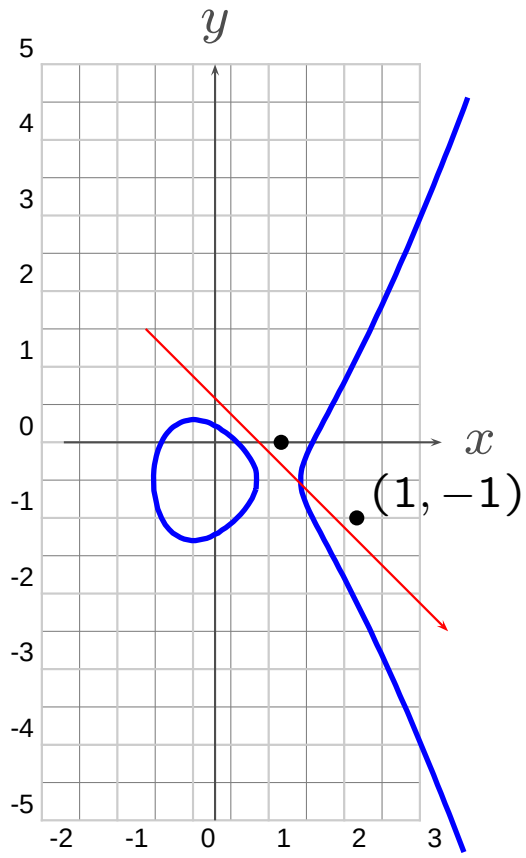


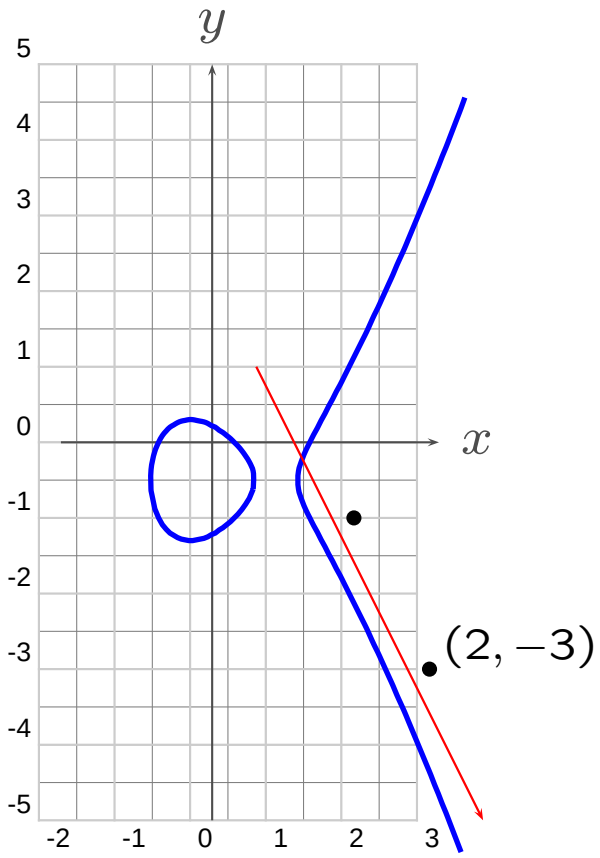
$y^2 + y = x^3 - x$

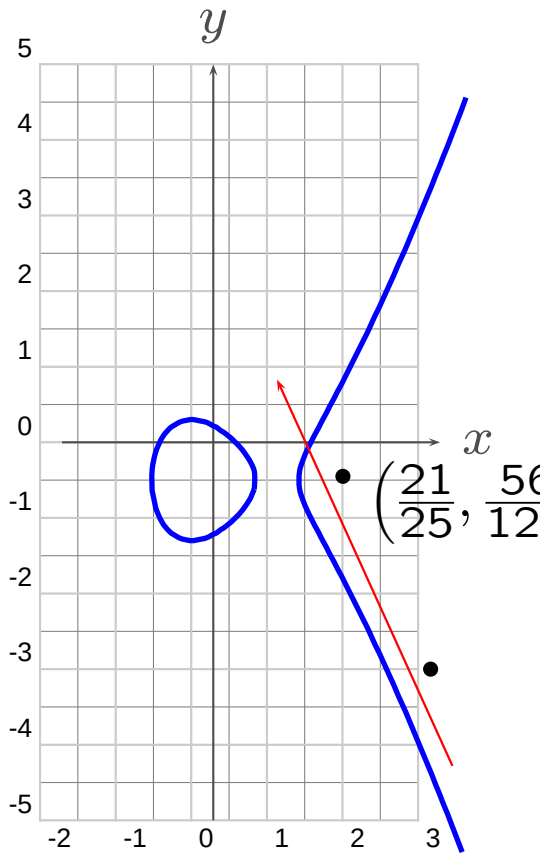
The Tangent Process



New rational point from a single rational point.







Iterate the Tangent Process

$$(0,0)$$

$$(1,-1)$$

$$(2,-3)$$

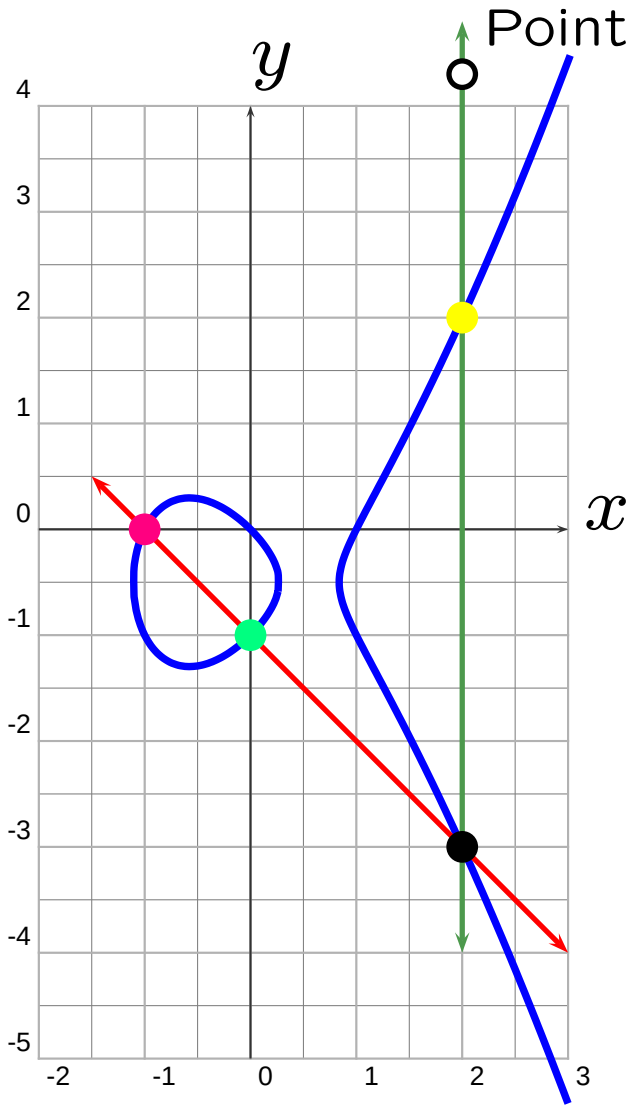
$$\left(\frac{21}{25},-\frac{56}{125}\right)$$

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

Fermat

$$\left(\frac{5313922364481462429082 1}{1870098771536627436025},-\frac{1228254006955588582174111316269938 1}{8087174560555986485289398018612 5}\right)$$

The Group Operation



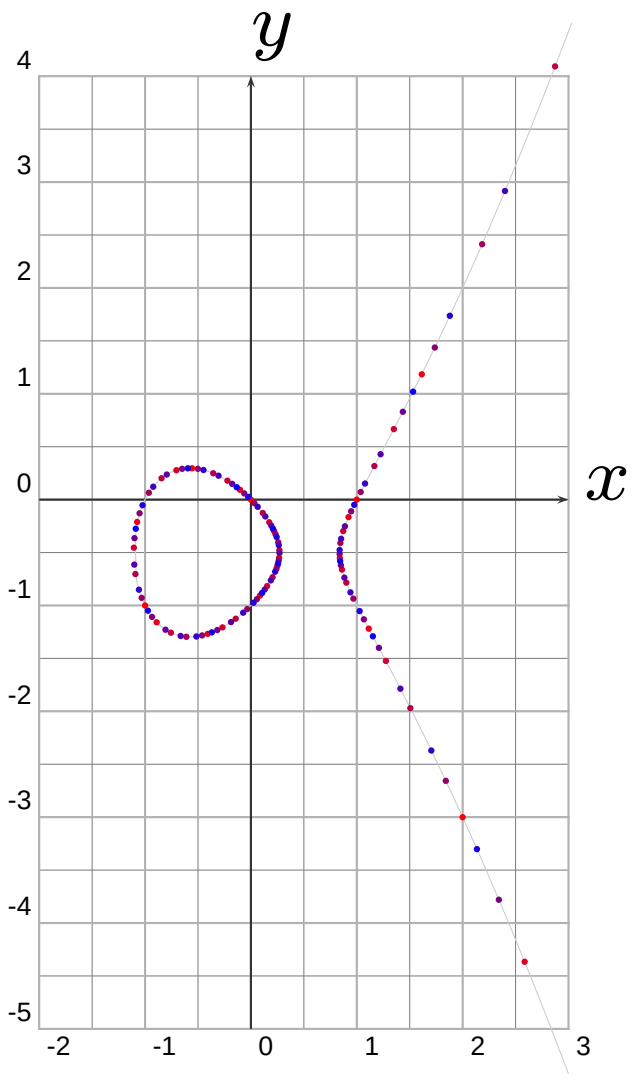
$y^2 + y = x^3 - x$

● ⊕ ● = ●

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

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!

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**, so

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

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

Mazur classified the possibilities for T. It is conjectured that r can be arbitrary, but the biggest r ever found is (probably) 28 (by Noam Elkies).

The Simplest Solution Can Be Huge

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

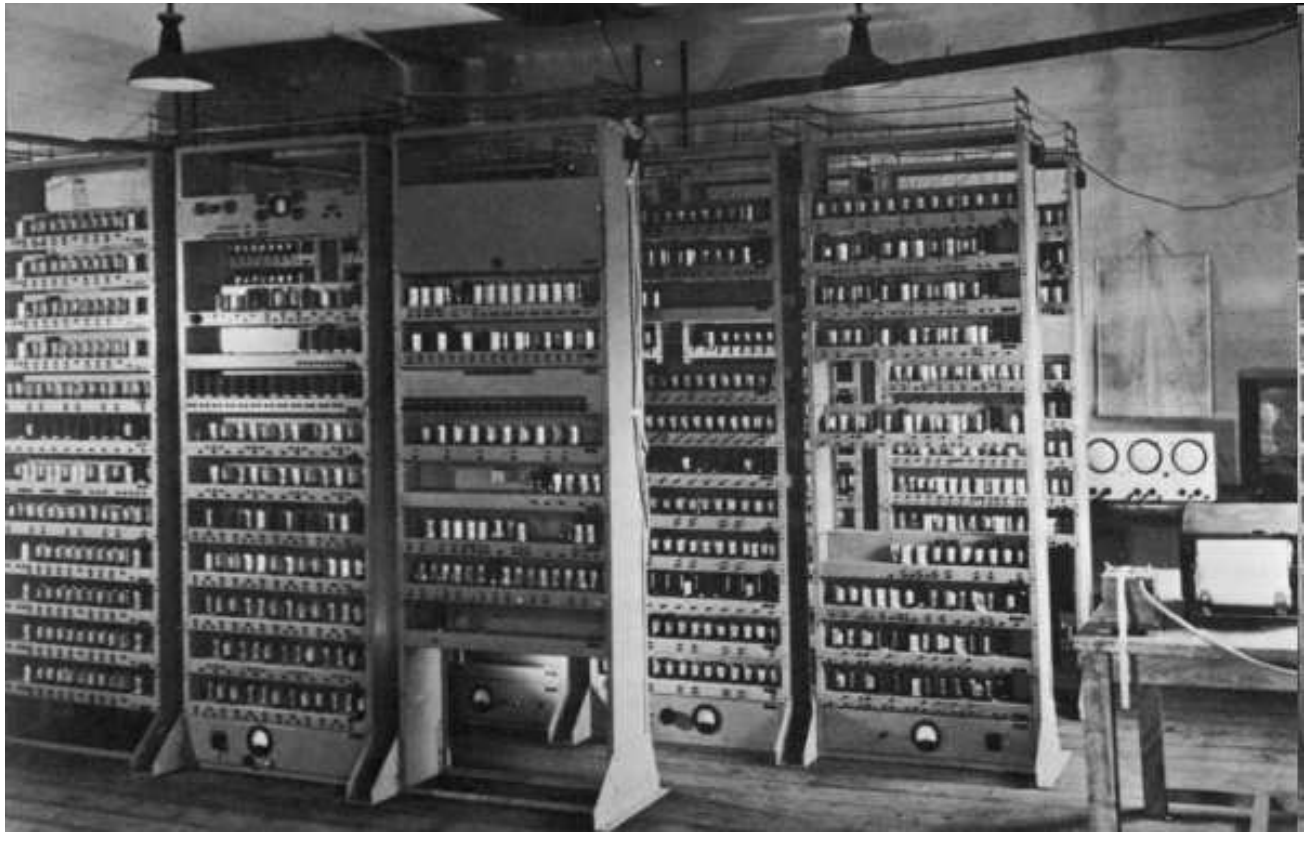
$$x = \frac{2263582143321421502100209233517777}{143560497706190989485475151904721}$$

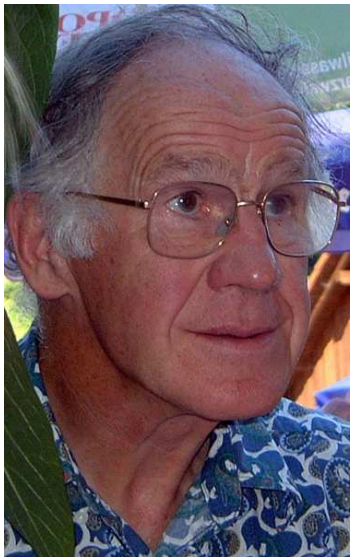
$$y = \frac{18639815258462330562483755148559677002814477665575 6}{17200949981063533558210085259387279501597770434 81}$$

(Found by Michael Stoll in 2002.)

The Central Question

Given an elliptic curve,
what is its rank?





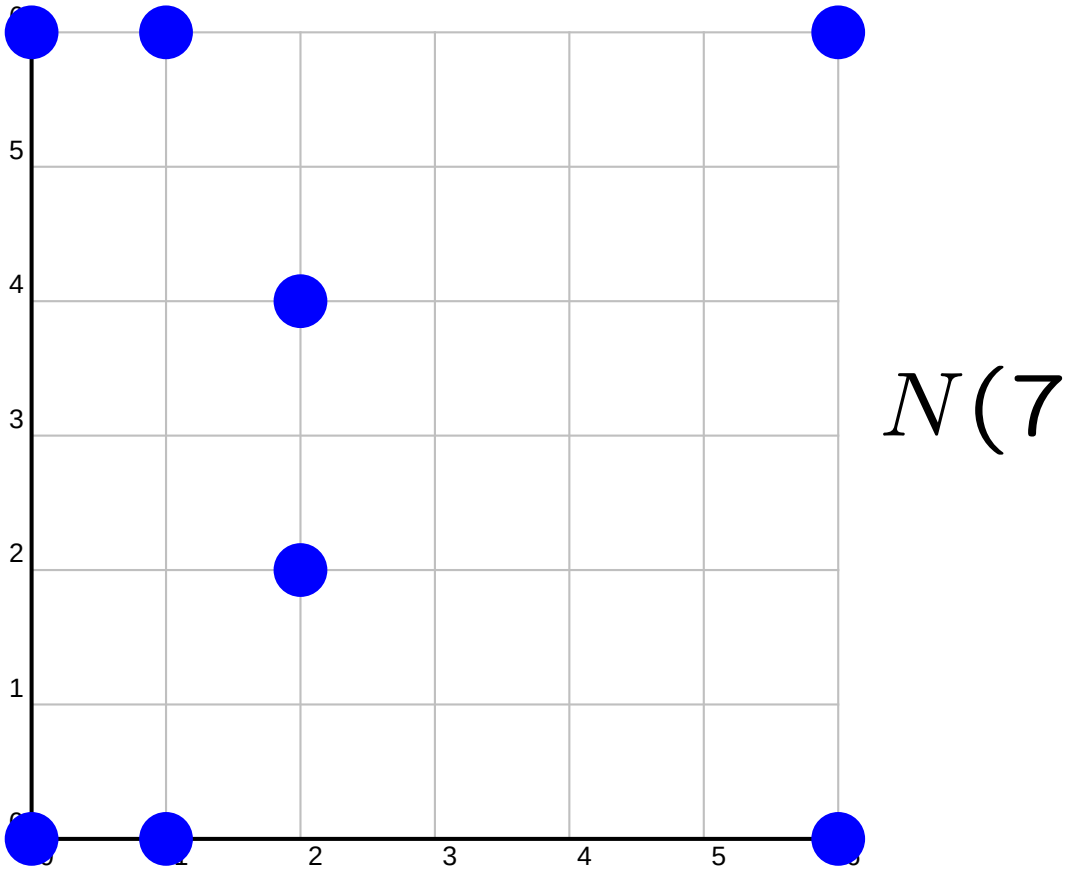
Conjectures Proliferated

"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

$N(p) = \#$ of solutions (mod 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

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

$a_2 = -2, \quad a_3 = -3, \quad a_5 = -2, \quad a_7 = -1, \quad a_{11} = -5, \quad a_{13} = -2, \quad a_{17} =$

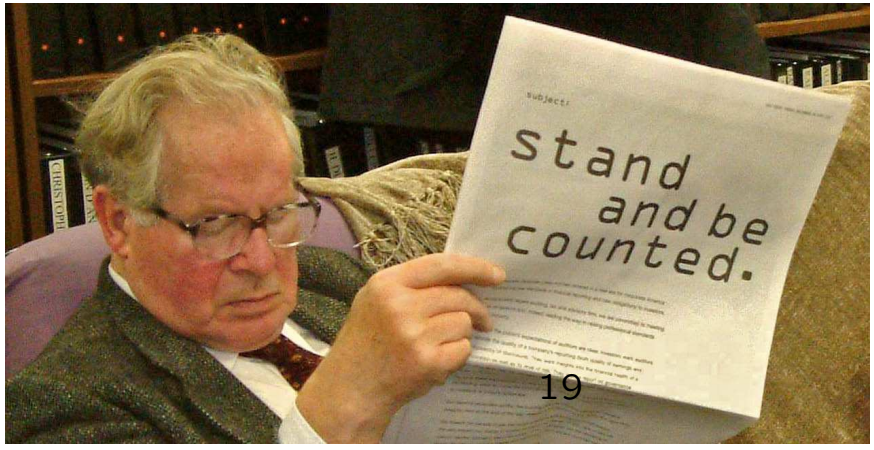
$a_{19} = 0, \quad a_{23} = 2, \quad a_{29} = 6, \quad \ldots$

Guess

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

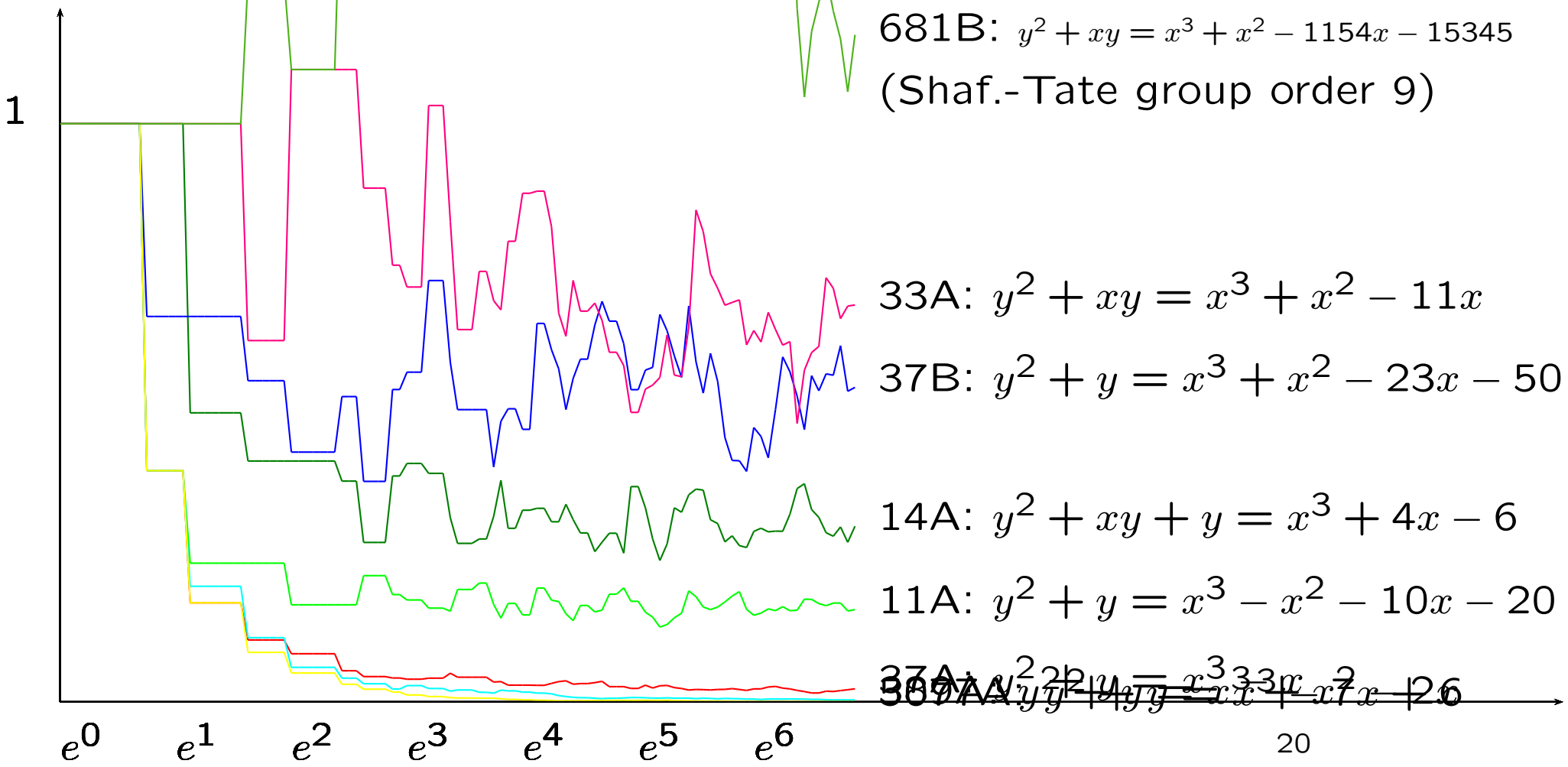
$$f_E(x) = \prod_{p \leq x} \frac{p}{N(p)} \to 0 \text{ as } x \to \infty$$

exactly when E has positive rank??



Graphs of $f(x) = \Pi_{p \leq x} \frac{p}{N(p)}$

The following are graphs, on a log scale, of $f_E(x)$:



681B: $y^2 + xy = x^3 + x^2 - 1154x - 15345$
(Shaf.-Tate group order 9)

33A: $y^2 + xy = x^3 + x^2 - 11x$

37B: $y^2 + y = x^3 + x^2 - 23x - 50$

14A: $y^2 + xy + y = x^3 + 4x - 6$

11A: $y^2 + y = x^3 - x^2 - 10x - 20$

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

Something Better: The L-Function

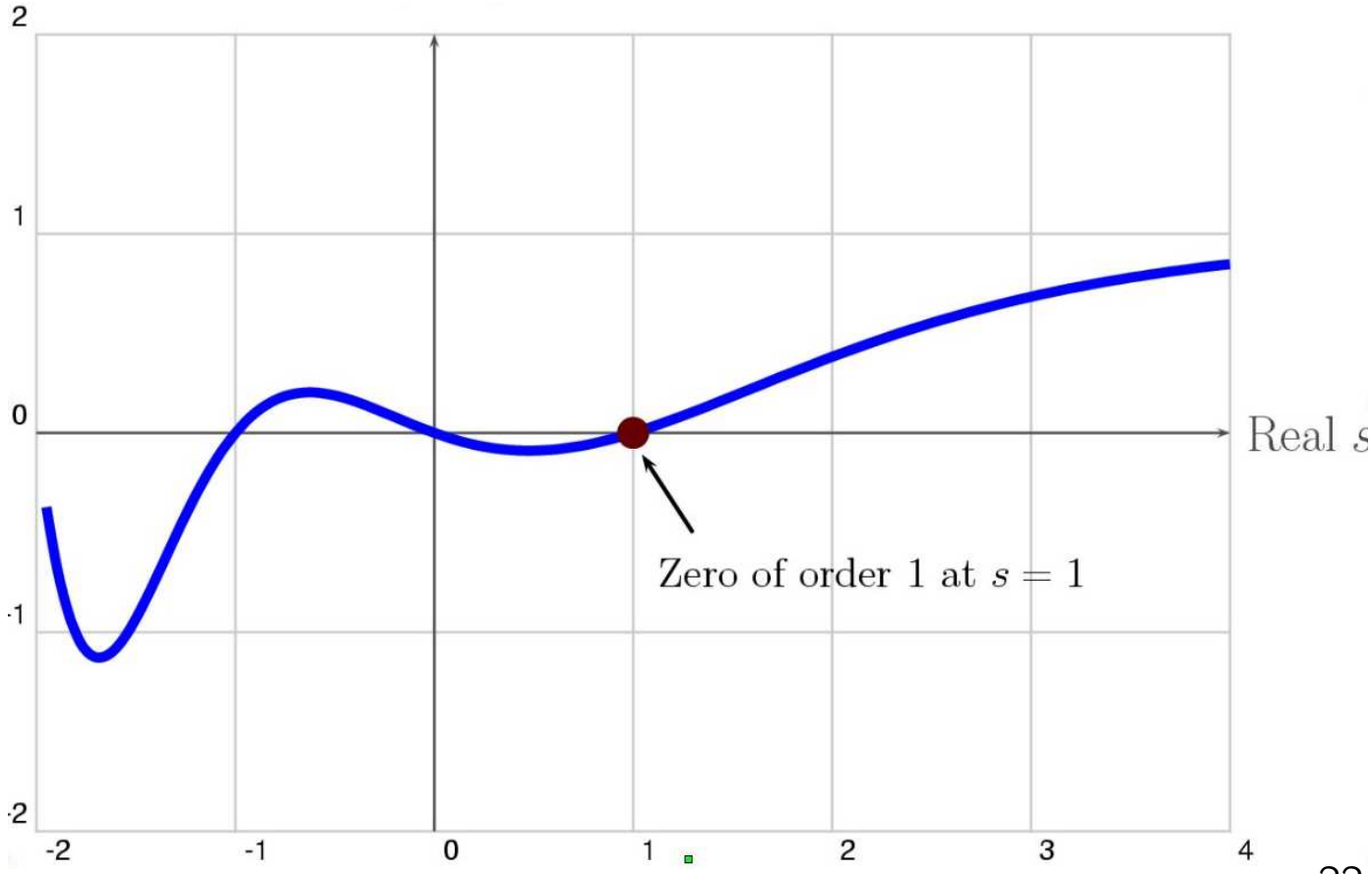
Theorem (Wiles et al., Hecke) The following function extends uniquely to an analytic function (i.e., given by a power series everywhere) on the whole complex plane:

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

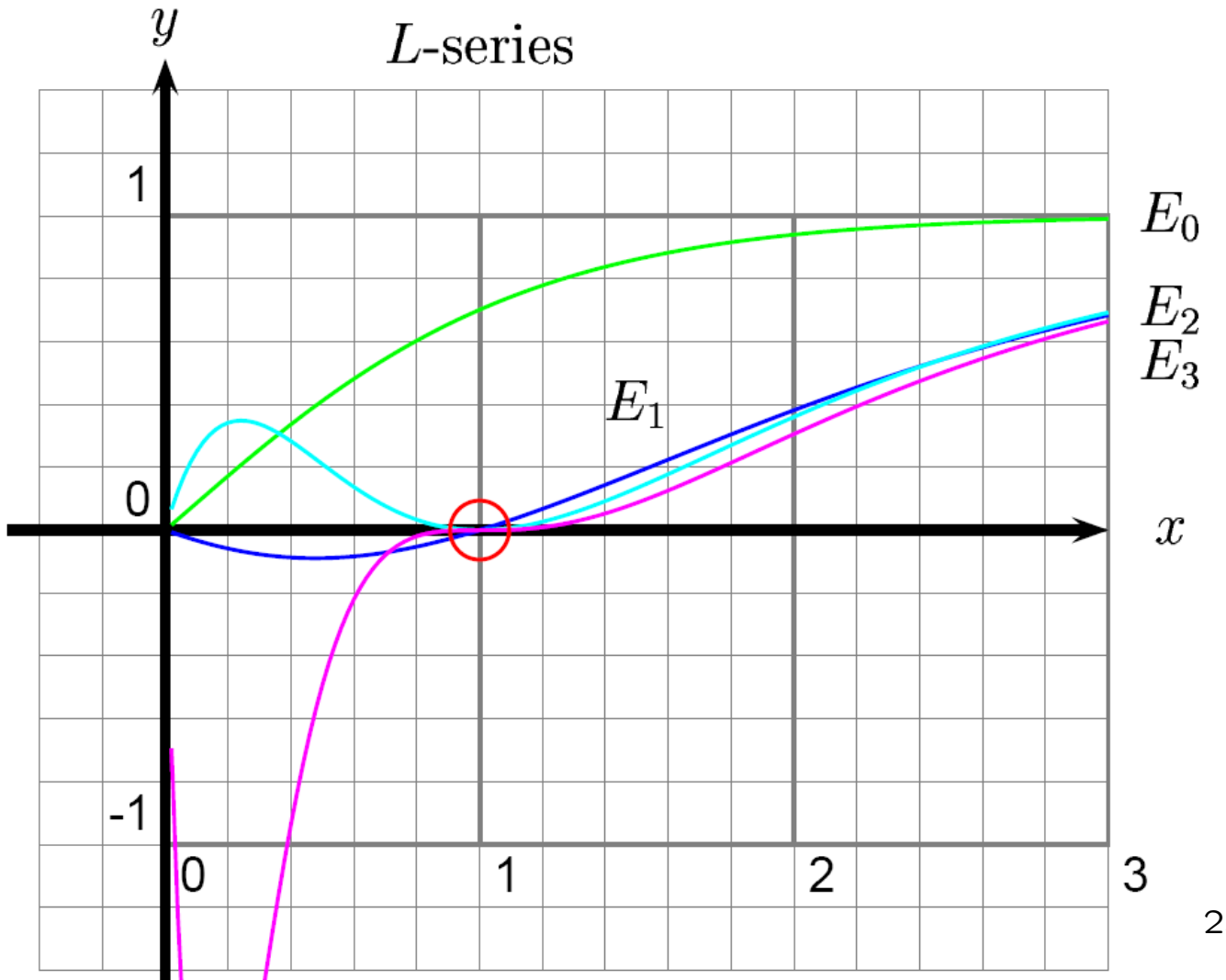
Note that formally,

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

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: $L(E,s) = c(s-1)^r +$ higher terms, with $c \neq 0$ and $E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$.

The Kolyvagin and Gross-Zagier Theorem

Theorem: If the ordering of vanishing $\mathrm{ord}_{s=1} L(E,s)$ is ≤ 1, then the conjecture is true for E.