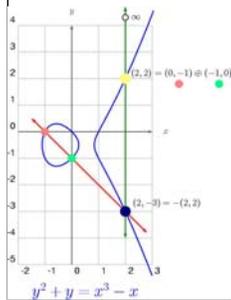
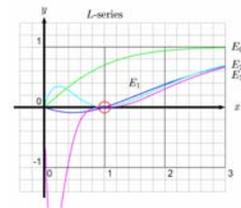


# An Introduction to the Birch and Swinnerton-Dyer Conjecture

November 3, 2004  
Univ. of Washington, Seattle



**William Stein**  
<http://modular.fas.harvard.edu>

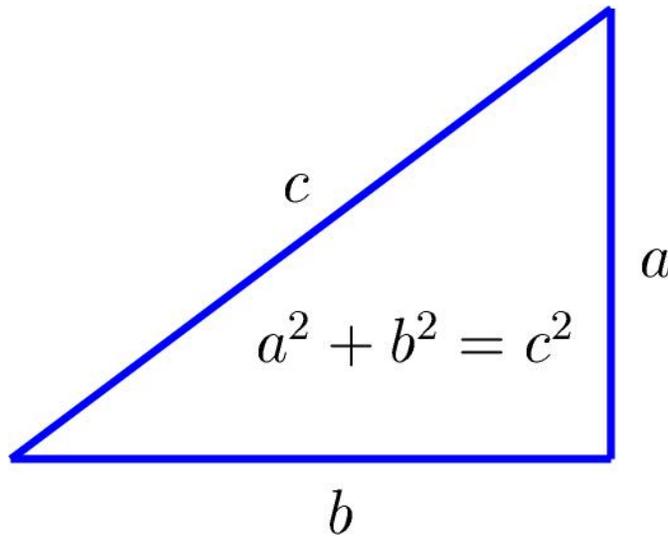


Read the title. Point out that the slides are available on that web page.

Thank person for inviting me.

My talk is about a beautiful area of pure mathematics. This area has applications to secure communications and physics, but I will only try to convey the intrinsic beauty and excitement of the area, rather than convince you of its applicability to everyday life.

# Pythagorean Theorem



Pythagoras  
approx 569-475 B.C.

The Pythagorean theorem asserts that if  $a$ ,  $b$ , and  $c$  are the sides of a right triangle with hypotenuse  $c$ , then  $a^2 + b^2 = c^2$ . Pythagoras (and others before him) were interested in systematically finding solutions to the equation  $a^2 + b^2 = c^2$ , with  $a$ ,  $b$ ,  $c$ , all integers.

# Babylonians



BABYLON, IRAQ: LION STATUE

1800-1600 B.C.

The painting on the upper right is “Artist's conception of the thriving city state of Babylon

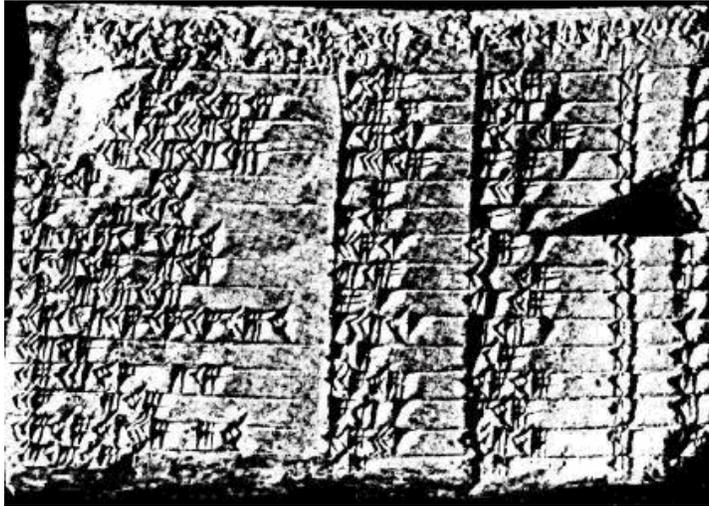
(circa 7th Century B.C.), including the Hanging Gardens.” The photo on the lower right is from modern Babylon: “Its ruins are found 90 km south of modern Baghdad in Iraq.”

The big tablet illustrates the Pythagorean relation with  $a=b=1$  and  $c=\sqrt{2}$ . Notice that if we view the lengths of the four short sides of the small triangles as 1, then the area of the big square is twice the area of a  $1 \times 1$  square (pick up a small triangle and move it to the other side). Thus the area of the square made from all four small triangles is 2, so that square must have side length  $\sqrt{2}$ . Note that  $1^2+1^2 = (\sqrt{2})^2$ .

## Pythagorean Triples



(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)  
⋮



Triples of whole numbers  $a$ ,  $b$ ,  $c$  such that

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

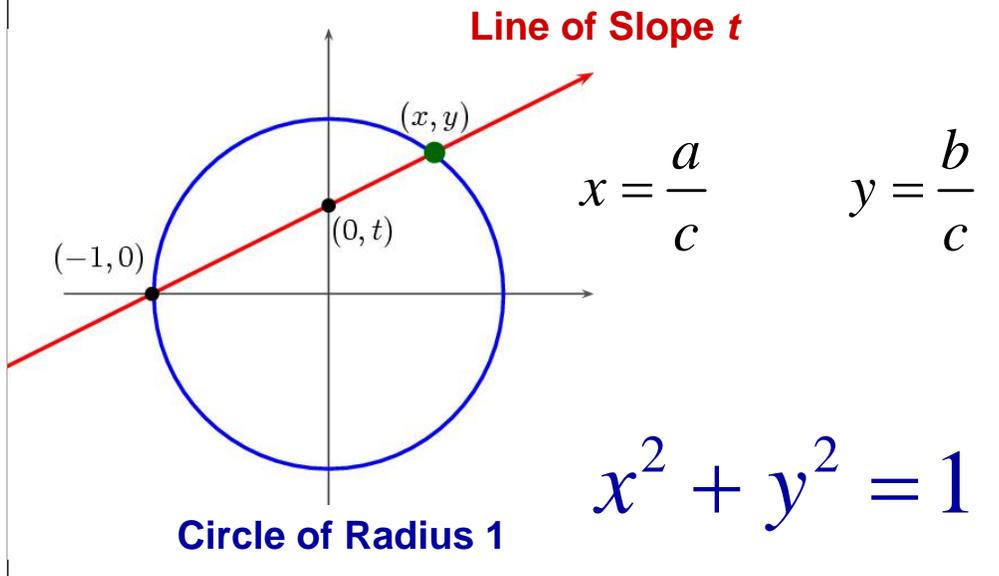
This tablet is Plimpton 322, a BABYLONIAN tablet from 1900-1600BC. (It's supposed to be at Columbia University.) The second and third columns list integers  $a$  and  $c$  such that  $a$  and  $c$  are the side lengths of the base and hypotenuse of a right triangle with integer side lengths. Thus if  $b = \sqrt{c^2 - a^2}$ , then  $(a, b, c)$  is a Pythagorean triple. The first row contains  $a=119$  and  $c=169=13^2$ , so  $b=120$ . The other rows also contain rather large triples.

The picture in the upper right is mainly to add color to the slide. It is a Ziggurat, which was a "house of god" built by the Babylonians from around 2200BC to 500BC, and there are about 25 left today.

The left side of the slide lists all the Pythagorean triples so that  $a, b, c$  all have at most two digits.

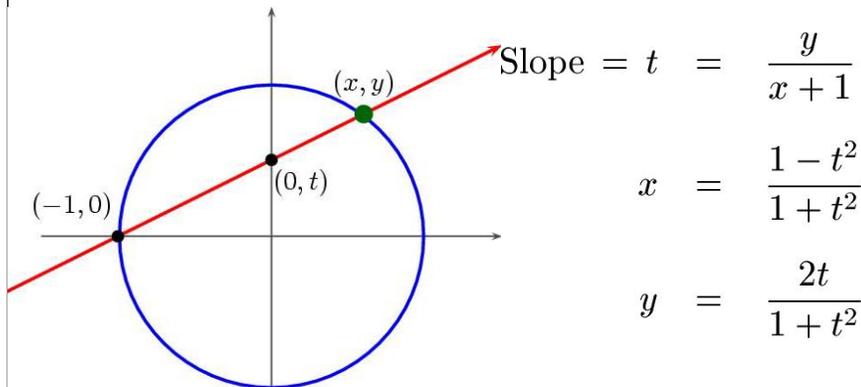
Question: How can we systematically enumerate Pythagorean triples?

## Enumerating Pythagorean Triples



This slide illustrates a method to enumerate all of the Pythagorean triples. The blue circle is a circle about the origin of radius 1. It is defined by the equation  $x^2 + y^2 = 1$ , so any point  $(x, y)$  on the circle satisfies  $x^2 + y^2 = 1$ . The red line has slope  $t$ , and is defined by the equation  $y = tx + t = t(x + 1)$ . Using elementary algebra, one sees that if  $t$  is a rational number, then the intersection point  $(x, y)$  has rational coordinates. By clearing denominators we obtain a Pythagorean triple, and (up to scaling) one can show that every Pythagorean can be obtained in this way. So finding the rational solutions to  $x^2 + y^2 = 1$ , or what's the same, the integral solutions to  $a^2 + b^2 = c^2$  is reasonably straightforward: there are infinitely many and they are parameterized by the rational slopes  $t$ .

# Enumerating Pythagorean Triples



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

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

If  $t = \frac{r}{s}$  then

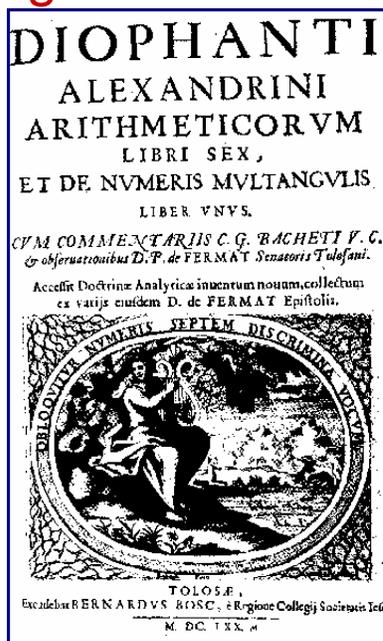
$$a = s^2 - r^2 \quad b = 2rs \quad c = s^2 + r^2$$

is a Pythagorean triple.

We can solve explicitly for  $x$  and  $y$  in terms of  $t$ . The first upper-right equation gives the equation of the red line. We then solve for  $x$  and  $y$  in terms of  $t$  by solving the two equations  $y=t*(x+1)$  and  $x^2+y^2=1$  for  $x$  and  $y$ . (subst first into second for  $y$  and get equation in  $x$  and  $t$ , then solve for  $x$  using algebra).

Finally, at the bottom of the slide I've listed the correspondence very explicitly. If  $t$  is a rational number  $r/s$  in lowest terms, then the displayed formulas define a (primitive) Pythagorean triple. When give example, note that  $r/s$  should be between 0 and 1 as indicated in the diagram.

# Integer and Rational Solutions



Mathematicians have long been interested in solving equations in the integers or rational numbers. The contents of most of Diophantus's works were totally lost, but a version of this book remains. It contains many interesting questions that boil down to "what are the [or here are some] rational solutions to an algebraic equation in two variables." The picture on the right is of Andrew Wiles looking at a copy of this very book, along with a zoom of the book. Fermat wrote in the margin of his copy of Diophantus his famous assertion that  $x^n + y^n = z^n$  has no rational solutions besides those with  $|x|=1$  or  $|y|=1$ . Wiles proved the conjecture in 1995.

# Elliptic Curves

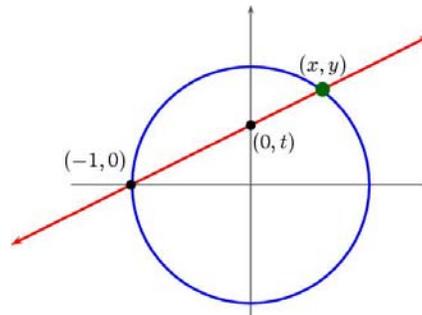
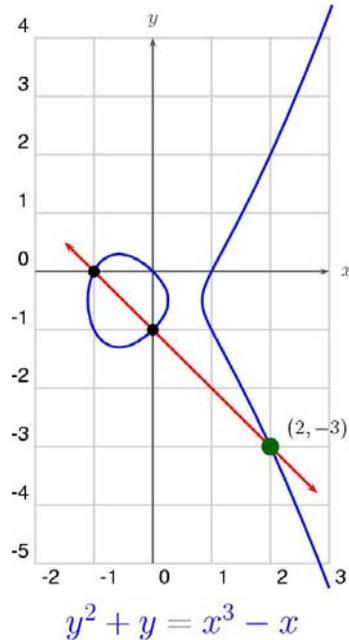
$$x^3 + y^3 = 1$$

$$y^2 = x^3 + ax + b$$
~~$$3x^3 + 4y^3 + 5 = 0$$~~

Cubic algebraic equations in two unknowns  $x$  and  $y$ .  
Exactly the 1-dimensional compact algebraic groups.

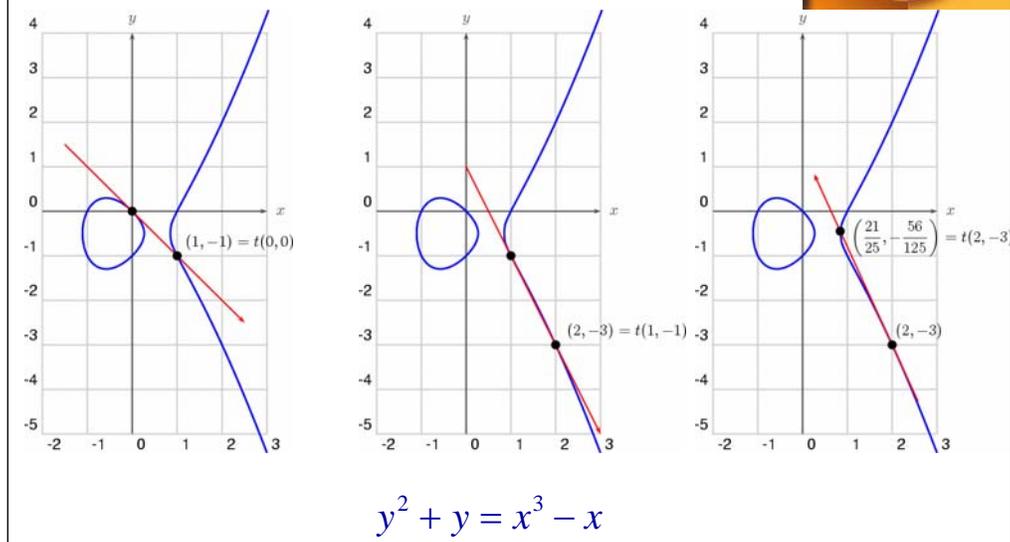
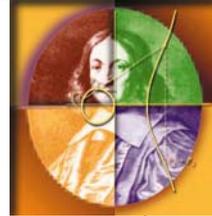
The simplest class of equations in 2 variables are the linear and quadratic equations. Solving linear equations in two variables is straightforward (back substitute). The circle trick for enumerating Pythagorean triples works well in general for enumerating the solutions to a quadratic equation in two variables (and there is an effective local-to-global procedure for deciding whether a degree two equation has any solutions). The next more complicated equation in 2 variables is a cubic equation. The first cubic equation on the slide is the Fermat equation for exponent 3 – Fermat’s famous conjecture is the assertion that this equation has no solutions (besides the obvious ones with  $x$  or  $y$   $\pm 1$ ). The third equation is an example of a cubic equation that has no rational solutions at all (not even “at infinity”)--- it is an **open problem** to give an algorithm that can decide whether any given cubic equation in 2 variables has a rational solution. Any cubic equation that has some rational solution (possibly “at infinity”) can be put in the third form  $y^2 = x^3 + ax + b$ . Such curves are called elliptic curves. Their graphs are definitely not ellipses (which are graphs of quadratic equations). The name “elliptic” arises because these curves appear naturally when trying to understand integration formulas for arc lengths of ellipses.

# The Secant Process



Recall that before given the point  $(-1,0)$  on the circle of radius 1, we found all other rational solutions by drawing a line through  $(-1,0)$  and finding the other point of intersection. Fermat introduced a similar process for elliptic curves. If we have TWO points on an elliptic curve, both with rational coordinates, we obtain a third point with rational coordinates by drawing the line they determine and finding the third point of intersection. In the example on the left, the blue curve is the graph of  $y^2+y=x^3-x$  “when is the product of two consecutive numbers equal to the product of three consecutive numbers?”, and there are two “obvious” rational solutions  $(-1,0)$  and  $(0,-1)$ . Using the secant process of Fermat we find the less-obvious solution  $(2,-3)$ .

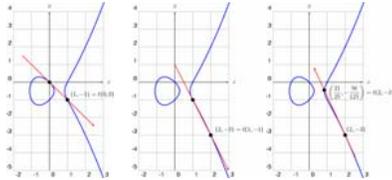
# The Tangent Process



Even if we only know one point on the curve, we can hope to find others using the tangent process. Draw a tangent line through the point and find the third point of intersection. For example, from  $(0,0)$  we get  $(1,-1)$ ; from  $(1,-1)$  we get  $(2,-3)$ , and (surprise!) from  $(2,-3)$  we get  $(\frac{21}{25}, -\frac{56}{125})$ .

Sometimes this process cycles around, and the corresponding points are called “torsion points”, but we will not discuss them further today.

# Big Points From Tangents



$$(0, 0)$$

$$(1, -1)$$

$$(2, -3)$$

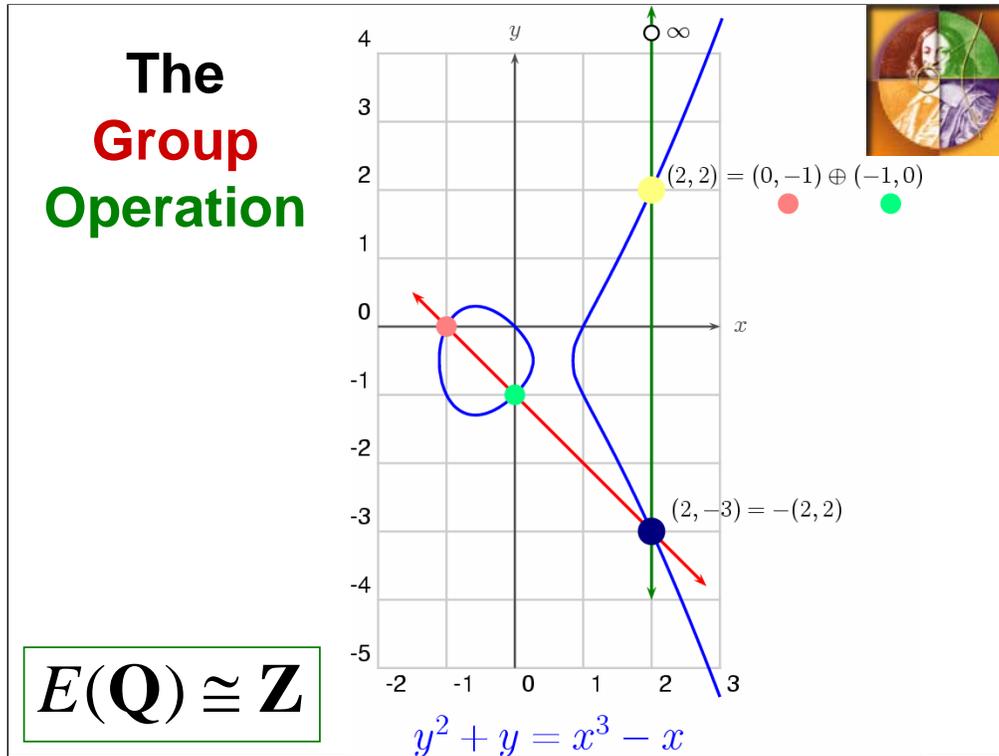
$$\left(\frac{21}{25}, -\frac{56}{125}\right)$$

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

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



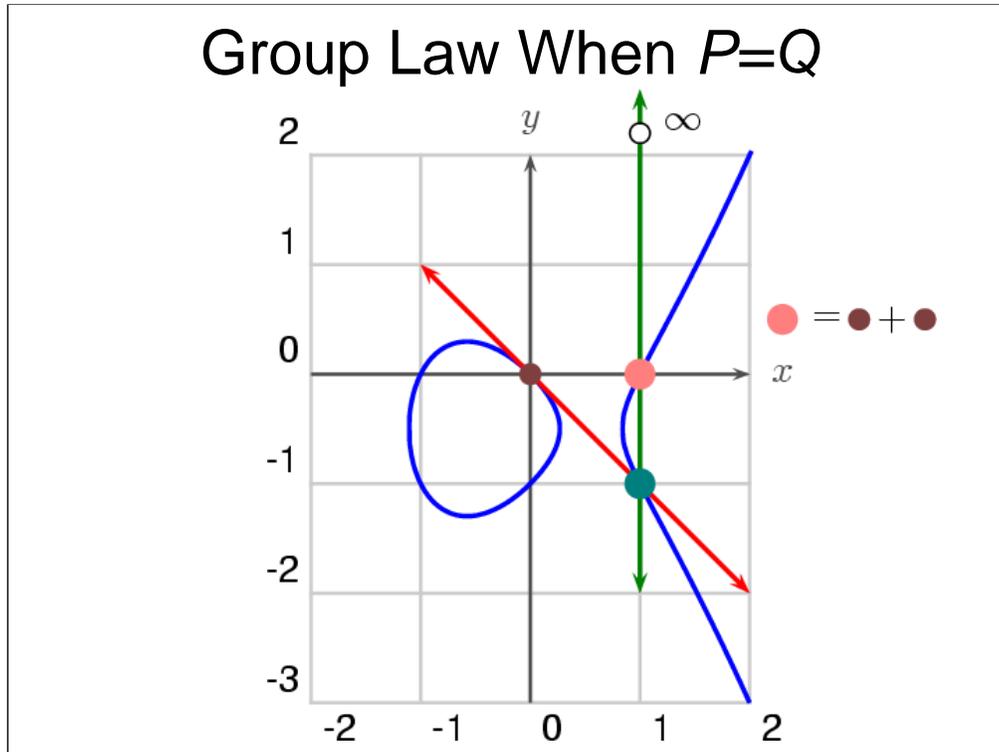
Continuing this process we immediately obtain SHOCKINGLY large points. Does every solution appear in this way, up to sign?? Answer – NO!! But, if we combine tangent with secant correctly, we get everything. More precisely, the points on the curve form a free abelian group of rank 1, and the tangent process corresponds to  $P$  goes to  $-2*P$ .



One can prove that the set of point on an elliptic curve with coordinates in  $\mathbf{Q}$  forms a group with *identity element* the point “at infinity” (which is a rational point in the projective closure). The group operation is defined as follows: To add the orange and green points, draw the red line they determine, find the third (blue) point of intersection. That third point is the negative of the sum of the two points. Now draw the (vertical) line determined by the blue dot and infinity. The third (yellow) point of intersection is the sum of the organge and blue dots in the group.

The secant process is  $P, Q \rightarrow -(P+Q)$

## Group Law When $P=Q$



In the “limiting case” when  $P=Q$ , the line determined by  $P$  and  $Q$  is simply the tangent line. Thus, e.g.,  
 $(0,0) + (0,0) = -(1,-1) = (1,0)$ . The tangent process is  $P \rightarrow -2P$ .

# Mordell's Theorem

The group  $E(\mathbb{Q})$  of rational points on an elliptic curve is finitely generated. Thus every *rational* point can be obtained from a *finite* number of solutions, using some combination of the secant and tangent processes.



1888-1972

Mordell proved that given any cubic equation in two variables, there exists a finite number of solutions such that each solution on the cubic can be obtained from that finite number by iteration of the secant and tangent processes applied to those points. Mordell did not give a method to find such a “finite basis” of starting solutions, and in fact, there is no PROVABLY correct algorithm known even today for doing this! It is an open problem.

# The Simplest Solution Can Be Huge



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

Stolls

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

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

(Found by Michael Stoll in 2002)

It was a deep theorem (which is a special case of a much more general theorem that I will discuss later) that the rather simple looking equation  $y^2 = x^3 + 7823$  has infinitely many solutions, but many years passed and nobody was able to write one down explicitly. For every other curve of the form  $y^2 = x^3 + d$ , with  $d < 10000$ , such a solution had been written down when the general theory predicted it would be there. I suggested finding one to high school student Jen Balakrishnan as a Westinghouse project; she didn't find one, but did some cool stuff anyways. Finally, in 2002, Michael Stoll found the simplest solution, which is quite large. *Every* solution can be obtained from this one (and from  $(x, -y)$ ) by using the secant and tangent process.

The photo is from a short video clip I shot of Michael Stoll and his son when I visited them in Bonn, Germany in 2000.

Stoll found the solution by doing a "4-descent". He found another curve  $F=0$  which maps to  $y^2 = x^3 + 7823$  by a map of degree 4. Then he found a smaller point on the curve  $F=0$  and mapped that small point to the point above. This method of descent goes from more complicated points to less complicated points, which are easier to find by a brute force search, and conjecturally (but not yet provably!) it should always succeed in finding points.

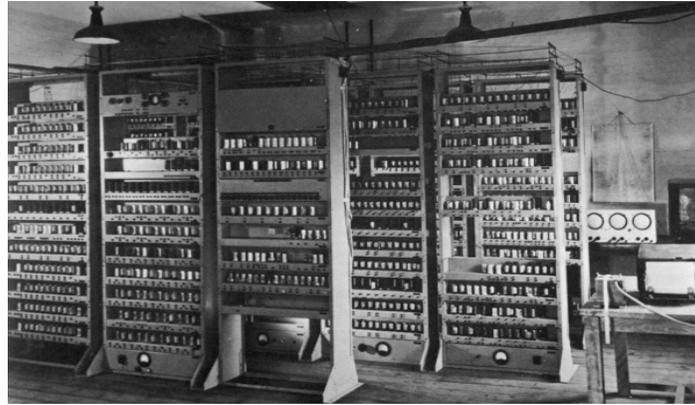
This same point should also be find-able using an analytic method due to Benedict Gross and Don Zagier, but in practice it wasn't because of complexity issues.

## Central Question

How many solutions are needed to generate all solutions to a cubic equation?



Birch and Swinnerton-Dyer



EDSAC in Cambridge, England

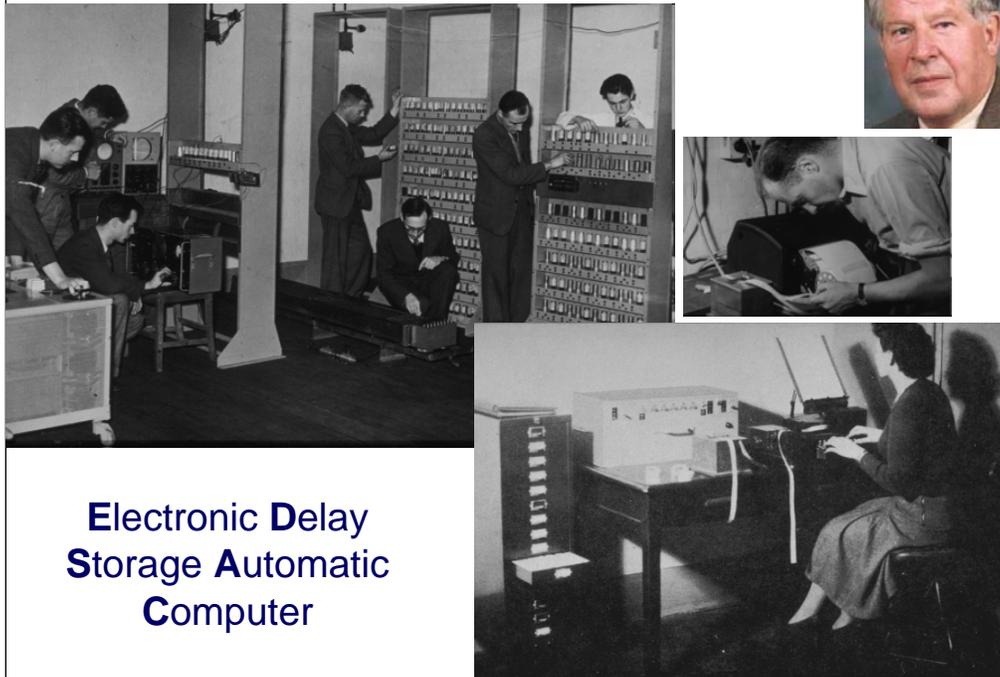
In the 1960s Birch and Swinnerton-Dyer set up computations on EDSAC (pictured below, but maybe the version B-SD used was a little more “modern”?), to try to find a conjecture about how many points are needed to generate all solutions to a cubic equation. Mordell’s theorem ensures that only finitely many are needed, but says nothing about the actual number in particular cases.

These EDSAC photos are genuine and come from the EDSAC simulator web page.

EDSAC: “The EDSAC was the world’s first stored-program computer to operate a regular computing service. Designed and built at Cambridge University, England, the EDSAC performed its first calculation on 6th May 1949.” (from EDSAC simulator web page)

The picture in the upper right is a picture I took of Birch and Swinnerton-Dyer in Utrecht in 1999.

## More EDSAC Photos



Construction and key punching.

TELL Swinnerton-Dyer operating system story? SD is the guy in the photo in the upper right.

I ate dinner with him and others at “high table” at Trinity College, Cambridge. It was dark and very formal, and there were servants. Lots of tradition and nice suits. After dinner we went to the formal smoke room, where these posh old professors chewed fine tobacco and drank wine. It was all quite surreal for a young graduate student. I sat next to Swinnerton-Dyer and he started telling me stories about his young days as a computer wiz. He told me that when EDSAC was completed they needed a better operating system. He learned how the machine worked, wrote an operating system, they loaded it, and it worked the first time. Presumably this made him favored by the computing staff, which might be part of why he got extensive computer time to do computations with elliptic curves.

From simulator page: “EDSAC, Electronic Delay Storage Automatic Computer, was built by Maurice Wilkes and colleagues at the University of Cambridge Mathematics Lab, and came into use in May 1949. It was a very well-engineered machine, and Wilkes designed it to be a productive tool for mathematicians from the start. It used mercury delay line tanks for main store (512 words of 36 bits) and half megacycle/S serial bit rate. Input and output on paper tape, easy program load, nice rememberable machine order-code. See Resurrection issue 2 for some of Wilkes' design decisions.”



## Conjectures Proliferated

### Conjectures Concerning Elliptic Curves

By B.J. Birch, pub. 1965

“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 (due to ourselves, due to Tate, and due to others) 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.”

Read the above excerpt paper by Birch, from the 1960s.

I took the photo of Birch during lunch in the middle of a long hike in Oberwolfach, Germany.

## Solutions Modulo $p$

Consider solutions modulo a prime number:

$$p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \dots$$

We say that  $(a, b)$ , with  $a, b$  integers, is a **solution modulo  $p$**  to

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

if

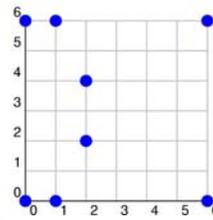
$$b^2 + b \equiv a^3 - a \pmod{p}.$$

For example,

$$4^2 + 4 \equiv 2^3 - 2 \pmod{7}.$$

This idea generalizes to any cubic equation.

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



To describe the conjecture of Birch and Swinnerton-Dyer about how many solutions are needed to generate all solutions, we do something rather sneaky and strange. We count the number of solutions modulo  $p$  for lots of primes  $p$ . This is a very general technique in number theory (both computational and theoretical) --- to understand something "over  $\mathbb{Q}$ ", try to understand it well modulo lots of primes. (For example, to find echelon form of a dense matrix over  $\mathbb{Q}$ , find it mod  $p$  for many primes, use chinese remainder theorem, and rational reconstruction.)

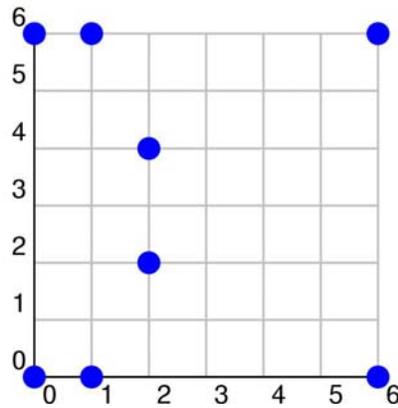
Note that we just consider pairs  $(x, y)$  of integers.

The graph in the upper right corner is of the solutions modulo 7 to  $y^2 + y = x^3 - x$ . This is the graph of the equation mod 7. [Check some of the points.]

# Counting Solutions

$$N(p) = \# \text{ of solutions } (\text{mod } p) \leq p^2$$

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



$$N(7) = 8$$

Notice that there are 8 solutions and 8 is close to 7.

## The **Error Term** (Hasse's Bound)



Write  $N(p) = p + A(p)$  with  
error term

$$|A(p)| \leq 2\sqrt{p}$$

1898-1979

For example,  $N(7) = 8$  so  $A(7) = 1$ .

Note for experts:  $A(p) = -a_p$

It is a general fact about cubic curves that the number of solutions mod  $p$  is very close to  $p$ , it is at most  $2\sqrt{p}$  from  $p$ .

This is Hasse's theorem from about 1933, and was proved in response to a challenge by Davenport.

## More Primes

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

$$A(2) = 2$$

$$A(3) = 3$$

$$A(5) = 2$$

$$A(7) = 1$$

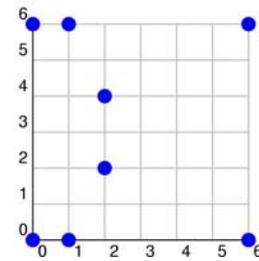
$$A(11) = 5$$

⋮

Thus  $N(p) > p$  for these primes  $p$ .

Continuing:  $A(13) = 2$ ,  $A(17) = 0$ ,  $A(19) = 0$ ,  $A(23) = -2$ ,  $A(29) = -6$ ,  $A(31) = 4$ , ....

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



$N(p)$  = number of soln's

$$N(p) = p + A(p)$$

In this slide we list the error (the amount that you have to add to  $p$  to get the number of points) for primes 2,3,5,7, and 11.

# Commercial Break: Cryptographic Application

**TOP SECRET**

Commercial Plug: The set of solutions modulo  $p$  to an elliptic curve equation (along with one extra point “at infinity”) forms a finite abelian group on which the “discrete logarithm problem” appears to usually be very difficult. Such groups are immensely useful in cryptography. The books listed on this slide are about using elliptic curves over finite fields to build cryptosystems, for example, for securing bank transactions, or e-commerce. This cryptosystems appear to be better than the RSA system because the key size need for a given level of security seems to be much smaller.

## Guess

If a cubic curve has infinitely many solutions, then probably  $N(p)$  is **larger** than  $p$ , for many primes  $p$ .

Thus maybe the product of terms

$$\prod_{p \leq M} \frac{p}{N(p)}$$

will tend to 0 as  $M$  gets larger.

$M$	$\prod_{p \leq M} \frac{p}{N(p)}$
10	0.083...
100	0.032...
1000	0.021...
10000	0.013...
100000	0.010...



Swinnerton-Dyer at AIM

The guess that Birch and Swinnerton-Dyer made was that if  $E$  has infinitely many solutions, then  $N(p)$  will be “big” on average, which should mean “bigger than  $p$ ”, hence the partial products of  $p/N(p)$  will probably tend to 0 as  $M$  gets large. Thus maybe we can decide if a cubic equation has infinitely many solutions by counting points and forming these products.

The table on the right lists the partial products for various  $M$  for  $y^2 + y = x^3 - x$ . The same numbers for the Fermat cubic, which has finitely many solutions, are  $M=10$ : 0.432,  $M=100$ , 0.425...,  $M=1000$ , 0.383;  $M=10000$ , 0.4738...;  $M=100000$ , 0.3714, these are small, but do not seem to be tending to 0.

# The $L$ -function



Swinnerton-Dyer

$$L(E, s) = \prod \frac{1}{1 + A(p) \cdot p^{-s} + p \cdot p^{-2s}}$$

The product is over all primes  $p$ . (At a finite number of primes the factor must be slightly adjusted.)

Product converges

Formally:

for

$$\operatorname{Re}(s) > \frac{3}{2}$$

$$L(E, 1) = \prod \frac{p}{N(p) + 1}$$

Formally, define a function  $L(E, s)$  by the infinite product over primes of factors, as indicated above. Note that the factors at a finite number of “primes of bad reduction” must be slightly adjusted. The product converges for  $\operatorname{Re}(s) > 3/2$ .

The product reminds us of the Riemann Zeta function.

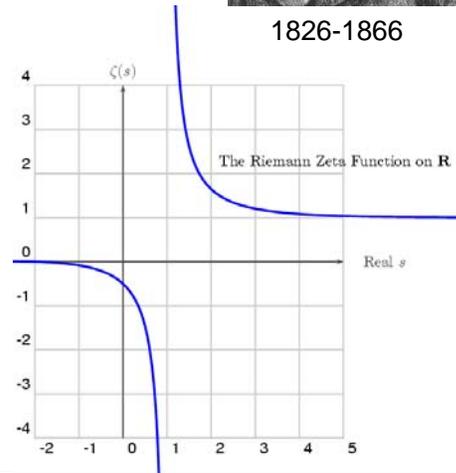
# The Riemann Zeta Function



1826-1866

$$\zeta(s) = \prod_{\text{all primes } p} \frac{1}{1 - p^{-s}}$$

Zeta **extends** to an analytic function everywhere but at  $s=1$ .



The definition of Zeta is similar to  $L(E,s)$ , and zeta has good analytic properties on all  $\mathbb{C}$ . The graph is of zeta restricted to the real line. If you zoom in really close on the left, it makes an interesting sqiggle, which is not visible from this resolution.

$L(E,s)$  also extends!!

## The Modularity Theorem

**Theorem** (2000, Wiles, Taylor, and Breuil, Conrad, Diamond) *The curve  $E$  arises from a “modular form”, so  $L(E,s)$  extends to an analytic function on the whole complex plane.*

(This modularity theorem is the key input to Wiles’s proof of Fermat’s Last Theorem.)

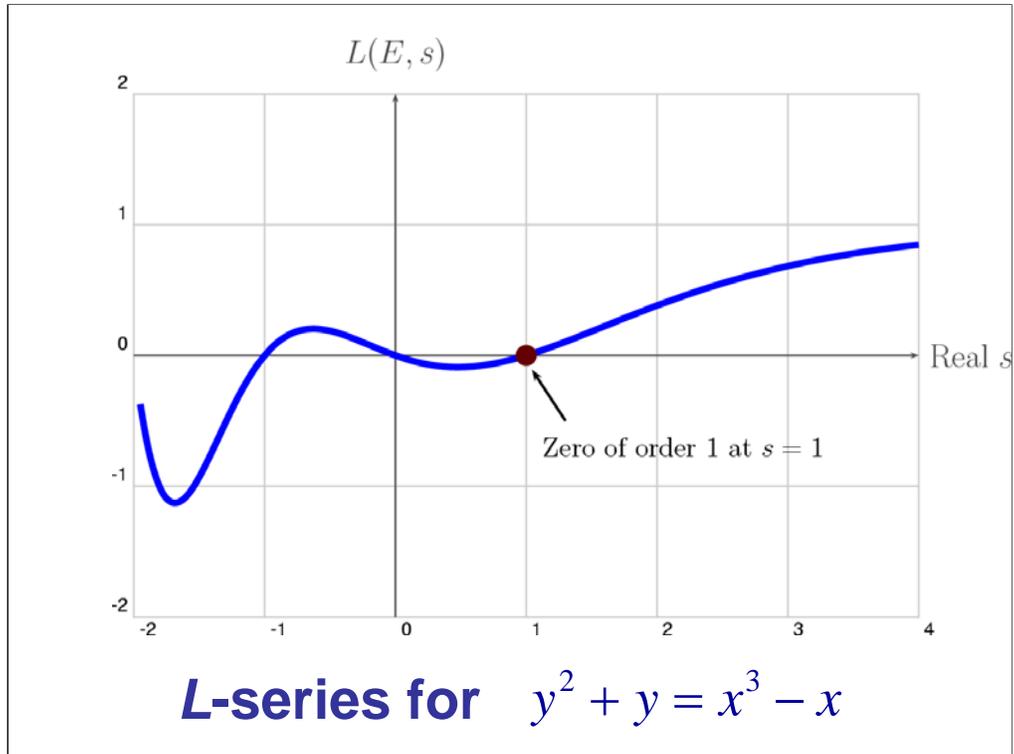


A. Wiles



R. Taylor

The function is analytic on the entire complex plane (a fact not known until 2000 work of Breuil, Conrad, Diamond, Taylor, and WILES).



This is a graph (that I computed using PARI) of  $L(E, s)$  for real  $s$ . Notice that indeed  $L(E, s)$  appears to vanish to order 1 at  $s=1$ , as predicted by BSD.

## The Birch and Swinnerton-Dyer Conjecture

The order of vanishing of

$$L(E, s)$$

at 1 equals the rank of the group  $E(\mathbf{Q})$  of all rational solutions to  $E$ :

$$\text{ord}_{s=1} L(E, s) = \text{rank } E(\mathbf{Q})$$

(CMI: \$1000000 reward for a proof.)



Bryan Birch

The conjecture of Birch and Swinnerton-Dyer is that the order of vanishing of  $f$  at 1 is the number of solutions needed to generate.

This is a one million dollar Clay Math Inst. Prize problem. -- THE problem for arithmetic geometry.

Emphasize that we throw in the torsion points for free, since they are easy to compute.

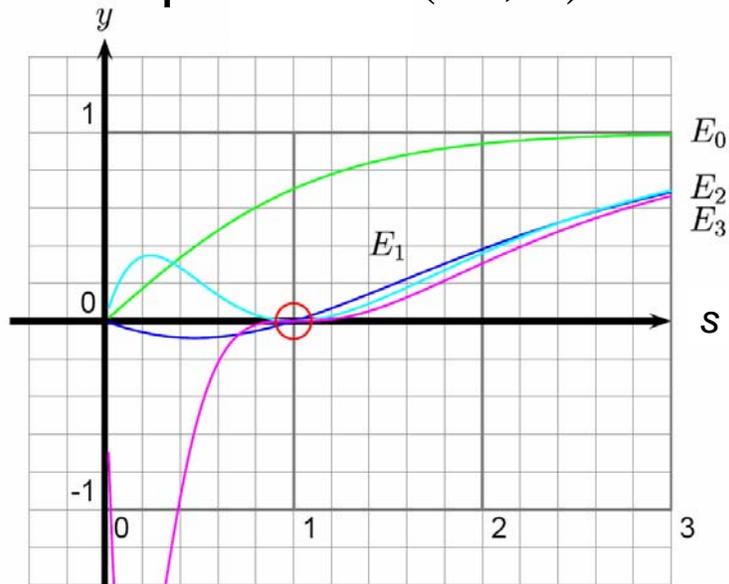
This conjecture relates the order of vanishing of a function at a point at which it isn't known to be defined to the order of a group that we don't know how to compute.

## Birch and Swinnerton-Dyer



This is a picture I took of Birch and Swinnerton-Dyer in Utrecht, Netherlands.

## More Graphs of $L(E, s)$ for $s$ real



The graph of  $L(E_r, s)$  vanishes to order  $r$  at 1.

These are graphs of four more function  $f_E(x)$ . The curve  $E_r$  has group of rational points minimally generated by  $r$  elements. Note that the order of vanishing of the corresponding functions appear to match up with the expectation of Birch and Swinnerton-Dyer.

The equations of the curves are  $[0,0,0,0,1]$ ,  $[0,0,1,-1,0]$ ,  $[0,1,1,-2,0]$ ,  $[0,0,1,-7,6]$

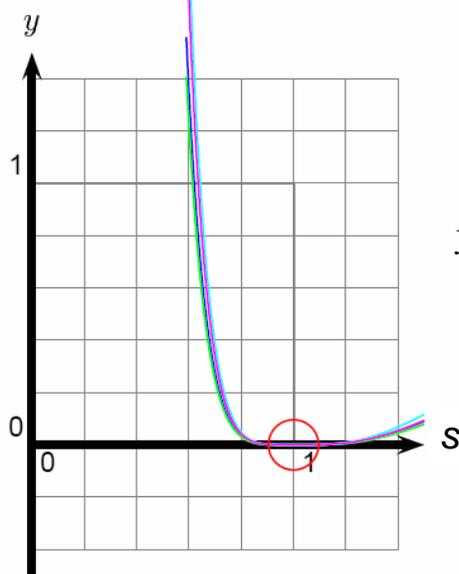
Green:  $E_0$

Blue:  $E_1$

Light blue:  $E_2$

Purple:  $E_3$

## Examples of $L(E, s)$ that **appear to vanish to order 4**



$$y^2 + xy = x^3 - x^2 - 79x + 289$$

**Open Problem:** For this  $E$ , prove that  $L(E, s)$  Vanishes to order 4 at  $s=1$ .

These are some graphs of the L-series attached to curves that require 4 generators. It is an OPEN PROBLEM to prove that  $f_E(s)$  really vanishes to order 4 for any curve --- we only know the function vanishes to order at least 2, and that  $f''(1) = 0.000000\dots$

# Congruent Number Problem

**Open Problem:** Decide whether an integer  $n$  is the area of a right triangle with rational side lengths.

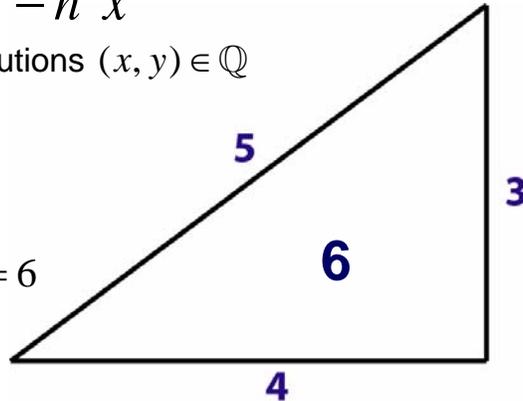
Fact: Yes, precisely when the cubic equation

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

has infinitely many solutions  $(x, y) \in \mathbb{Q}$

$$n = 6$$

$$A = \frac{1}{2} b \times h = \frac{1}{2} 3 \times 4 = 6$$



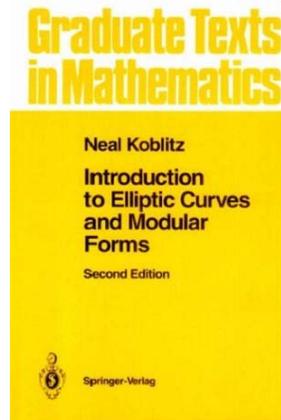
Application:

The congruent number problem has been an open problem for about a thousand years, at least. It asks for an algorithm to decide, with a finite amount of computation, whether a given integer is the area of a right triangle with rational side lengths.

The congruent number problem looks at first like it has nothing to do with cubic equations. However, some algebraic manipulation shows that it does.

## Connection with BSD Conjecture

**Theorem (Tunnell):** The Birch and Swinnerton-Dyer conjecture implies that there is a simple algorithm to decide whether or not a given integer  $n$  is a congruent number.



See [Koblitz] for more details

And, Jerrold Tunnell proved that if the Birch and Swinnerton-Dyer conjecture is true, then there is a simple algorithm for deciding whether or not an integer  $n$  is a congruent number. Nonetheless, still not enough of the conjecture is known, and the congruent number problem remains a tantalizing open problem. I would not be surprised if this 1000 year old problem is solved in the next decade. In fact, it has already been solved for many classes of integers  $n$ , because of deep theorems of Benedict Gross, Don Zagier, Victor Kolyvagin, and others.



## The Gross-Zagier Theorem



Benedict Gross

Don Zagier

When the order of vanishing of  $L(E, s)$  at  $s=1$  is one, then  $E$  has rank at least one.

Subsequent work of Kolyvagin showed that if the order of vanishing is exactly 1, then the rank equals 1, so the Birch and Swinnerton-Dyer conjecture is true in this case.

The Gross-Zagier theorem says that the conjecture of Birch and Swinnerton-Dyer is true when the order of vanishing is exactly 1. That is, if the function vanishes to order exactly 1, then one solution can be used to generate them all. This is the case for our example curve  $y^2+y=x^3-x$ .

## Kolyvagin's Theorem



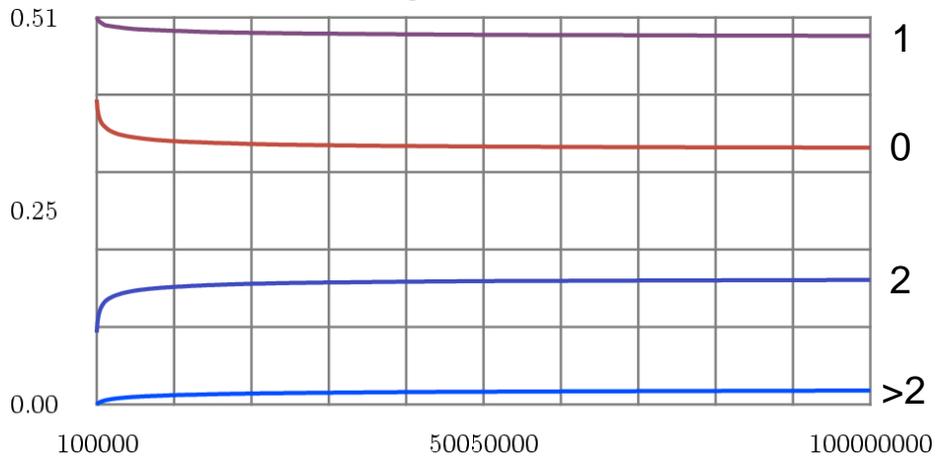
**Theorem.** If the order of vanishing of  $L(E,s)$  at  $s=1$  is at most 1, then the Birch and Swinnerton-Dyer conjecture is true for  $E$ .

Kolyvagin's theorem asserts that the conjecture is true when  $f$  vanishes to order 0, i.e, when  $f(1)$  is nonzero.

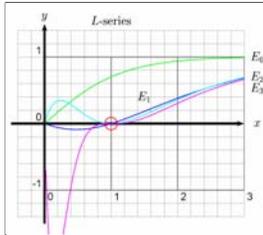
Very little is known when  $f$  vanishes to order 2 or higher. Also, not a single example is known where we can prove that  $f$  really does vanishes to order bigger than 3 (though it appears to).

Kolyvagin's an intense Russian mathematician. I snapped this photo of him recently after I spoke at CUNY and he went to dinner with us.

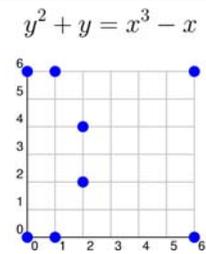
## How Many Curves Are Covered by Kolyvagin's Theorem?



Proportion of curves of rank 1, 0, 2, and >2 as a function of the "conductor" for the more than 130 million elliptic curves with discriminant  $< 10^{12}$ ,  $c_4 < 1.44 \cdot 10^{12}$  in the Stein-Watkins database.



$$\text{ord}_{s=1} L(E, s) = \text{rank } E(\mathbf{Q})$$



# Thank You



## Acknowledgments

- Benedict Gross
- Keith Conrad
- Ariel Shwayder (graphs of  $L(E, s)$ )

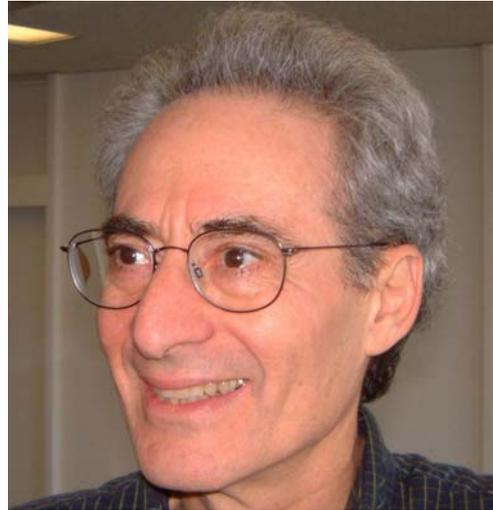
Thank everyone.

## Mazur's Theorem

For any two rational  
 $a, b$ , there are at  
most 15 rational  
solutions  $(x, y)$  to

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

with finite order.



*Theorem (8). — Let  $\Phi$  be the torsion subgroup of the Mordell-Weil group of an elliptic curve defined over  $\mathbf{Q}$ . Then  $\Phi$  is isomorphic to one of the following 15 groups:*

*or:*

$\mathbf{Z}/m \cdot \mathbf{Z}$	for	$m \leq 10$	or	$m = 12$
$(\mathbf{Z}/2 \cdot \mathbf{Z}) \times (\mathbf{Z}/2^v \cdot \mathbf{Z})$	for	$v \leq 4$ .		

In the 1970s Barry Mazur wrote a huge paper that answered a pressing question, which I mentioned earlier. How do you know if the tangent process will eventually cycle around or keep producing large and larger points? Either possibility can and does occur, but how do you know in a particular case? Mazur showed that if you get at least 16 distinct points by iterating the tangent process, then the tangent process will never cycle around on itself, and you will always get new points. This is an extremely deep theorem, and the method of proof opened many doors.

The picture on the right is one I took of Mazur outside his Harvard office. The boxed theorem is the statement of this theorem from the paper "Modular Curves and the Eisenstein Ideal" in which it appears. For those who know group theory: The set of solutions to a cubic equation (plus one extra "0" element) form an abelian group. Mazur's theorem then gives an explicit list of the possible torsion subgroups of this group.