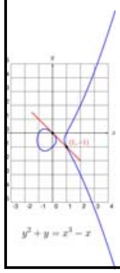
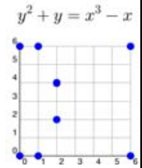
Solving Certain Cubic Equations: An Introduction to the Birch and Swinnerton-Dyer Conjecture

February 28, 2004 at Brown SUMS



William Stein

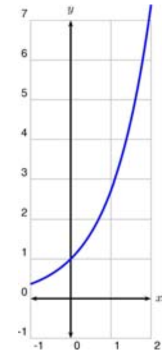
`http://modular.fas.harvard.edu/sums`



Two Types of Equations

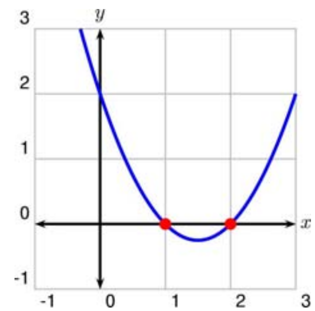
Differential

$$f'(x) = f(x)$$

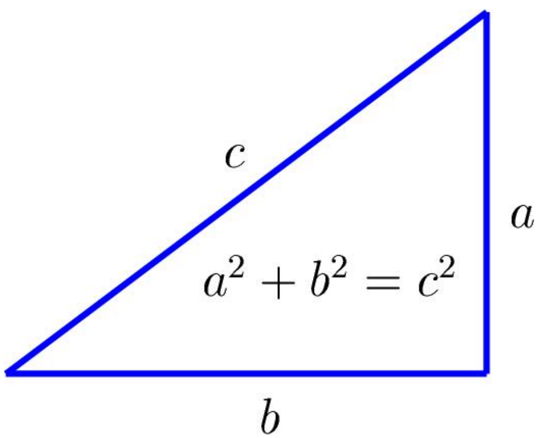


Algebraic

$$x^2 - 3x + 2 = 0$$

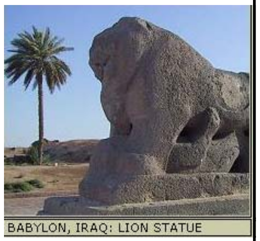


Pythagorean Theorem



Pythagoras
lived approx 569-475 B.C.

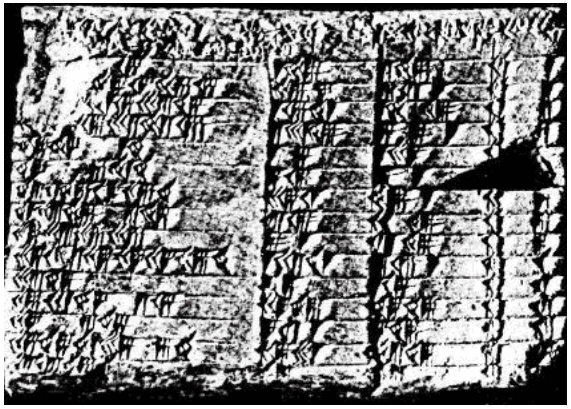
Babylonians



1800-1600 B.C.

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

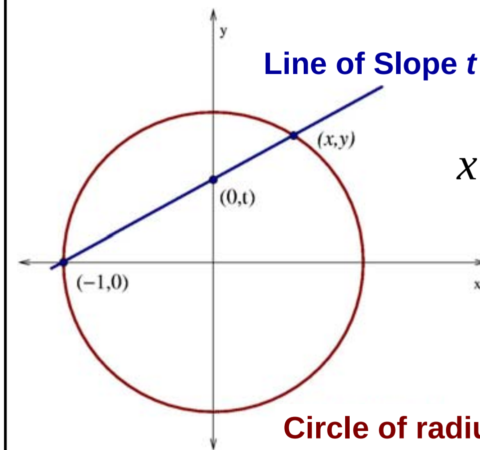
Pythagorean Triples



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

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

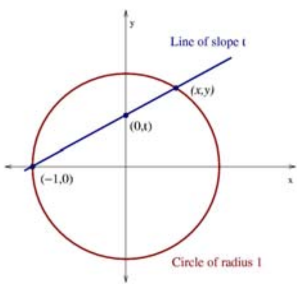
Enumerating Pythagorean Triples



$$x = \frac{a}{c} \qquad y = \frac{b}{c}$$

$$x^2 + y^2 = 1$$

Enumerating Pythagorean Triples



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

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

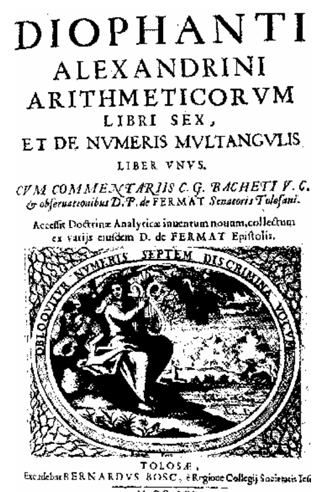
$$y = \frac{2t}{1+t^2}$$

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

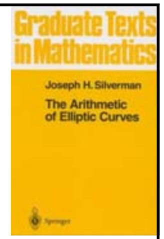
$$a = s^2 - r^2 \qquad b = 2rs \qquad c = s^2 + r^2$$

is a Pythagorean triple.

Integer and Rational Solutions


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& obseruationibus D. P. de FERMAT Senatoris Tolosani.
Accessit Doctrinæ Analyticæ inuentum nouum, collectum
ex varijs eiusdem D. de FERMAT Epistolis.
TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Iesu.
M. DC. LXX.

Cubic Equations & Elliptic Curves



A great book on elliptic curves by **Joe Silverman**

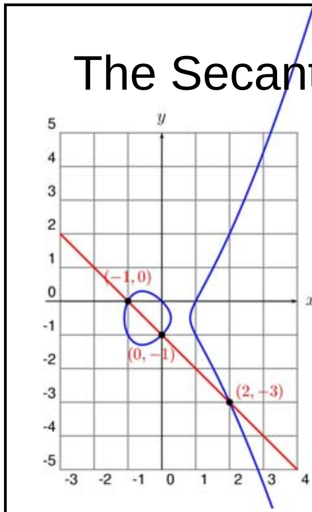
$$x^3 + y^3 = 1$$

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

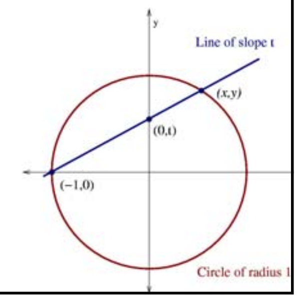
$$y^2 = x^3 + ax + b$$

Cubic algebraic equations in two unknowns *x* and *y*.

The Secant Process

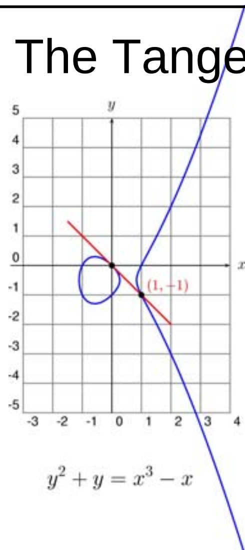


$(-1,0)$ & $(0,-1)$ give $(2,-3)$



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

The Tangent Process



$(0,0)$

$(1,-1)$

$(2,-3)$

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

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

$\left(\frac{531392236448146242908 21}{1870098771536627436025}, -\frac{1228254006955588582174111316269 9381}{8087174560555986485289398018 6125}\right)$

Mordell's Theorem

The rational solutions of a cubic equation are ***all*** obtainable from a ***finite*** number of solutions, using a combination of the secant and tangent processes.

1888-1972

The Simplest Solution Can Be Huge

M. Stoll

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

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

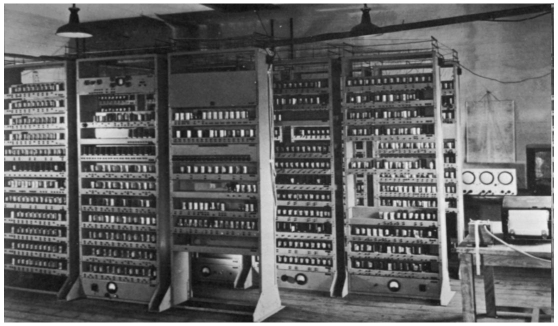
$$y = \frac{186398152584623305624837551485596770028144776655756}{1720094998106353355821008525938727950159777043481}$$

(Found by Michael Stoll in 2002)

Central Question

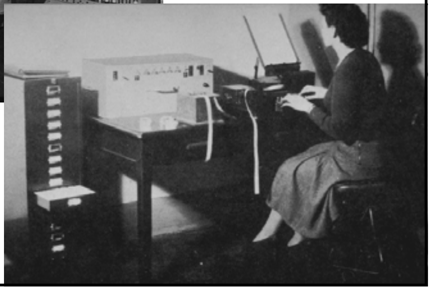
How many solutions are needed to generate all solutions to a cubic equation?

Birch and Swinnerton-Dyer



EDSAC in Cambridge, England

More EDSAC Photos



Electronic **D**elay **S**torage **A**utomatic **C**omputer

Conjectures Proliferated

Conjectures Concerning Elliptic Curves
By B.J. Birch

"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."

Mazur's Theorem

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

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

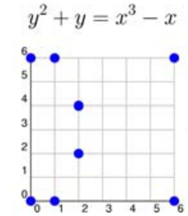
with finite order.

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

$\mathbf{Z}/m.\mathbf{Z}$ *for* $m \leqslant 10$ *or* $m = 12$

or: $(\mathbf{Z}/2.\mathbf{Z}) \times (\mathbf{Z}/2\nu.\mathbf{Z})$ *for* $\nu \leqslant 4$.

Solutions Modulo p



A *prime number* is a whole number divisible only by itself and 1. The first few primes are

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

We say that (x,y), with x,y integers, is a **solution modulo p** to

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

if p is a factor of the integer

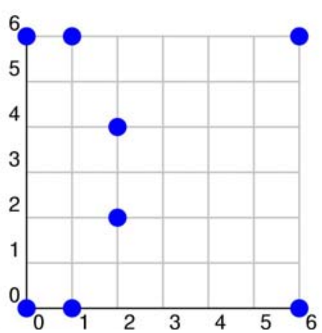
$$y^2 + y - (x^3 - x)$$

This idea generalizes to any cubic equation.

Counting Solutions

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

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



$$N(7) = 8$$

The Error Term

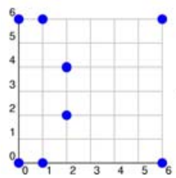
Write $N(p) = p + A(p)$ with error term

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

More Primes

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

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



$$A(2) = 2$$
$$A(3) = 3$$
$$A(5) = 2$$
$$A(7) = 1$$
$$A(11) = 5$$
$$\vdots$$

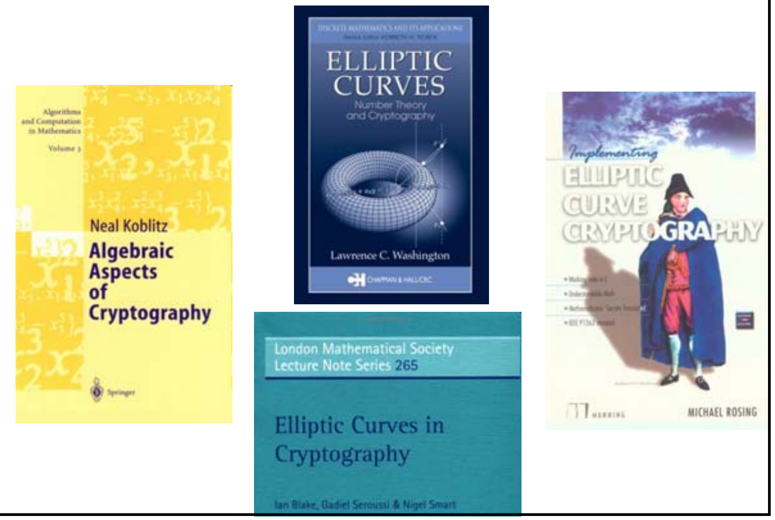
$N(p)$ = number of soln's

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

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

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

Cryptographic Application



Guess

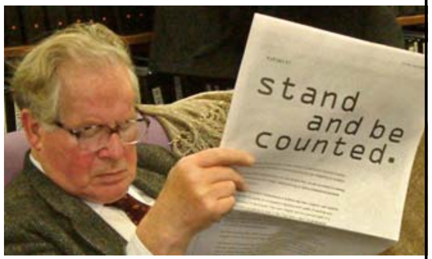
M	$\prod_{p \le M} \frac{p}{N(p)}$
10	0.083…
100	0.032…
1000	0.021…
10000	0.013…
100000	0.010…

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

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

will tend to 0 as M gets larger.



Swinnerton-Dyer

A Differentiable Function

Swinnerton-Dyer

More precisely, Birch and Swinnerton-Dyer defined a differentiable function $f_E(x)$ such that formally:

$$f_E(1) = \text{“}\prod \frac{p}{N(p)}\text{”}$$

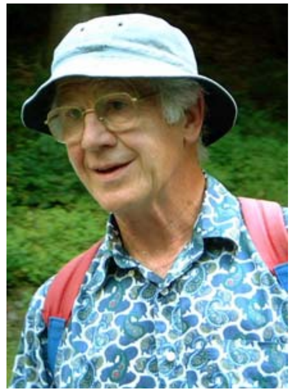
The Birch and Swinnerton-Dyer Conjecture

The order of vanishing of

$$f_E(x)$$

at 1 is the number of solutions required to generate all solutions (we automatically include finite order solutions, which are trivial to find).

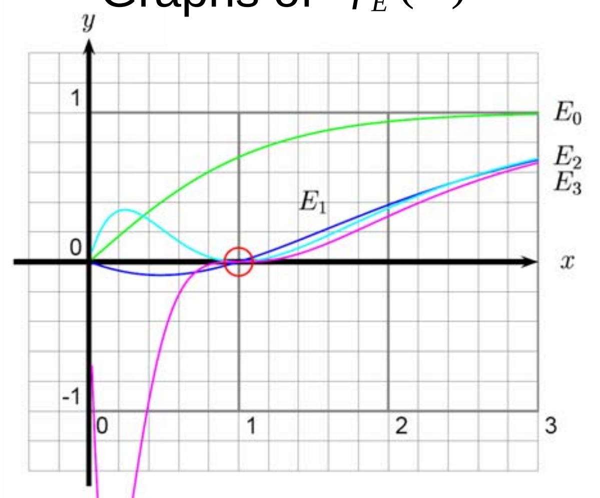
CMI: $1000000 for a proof!



Bryan Birch

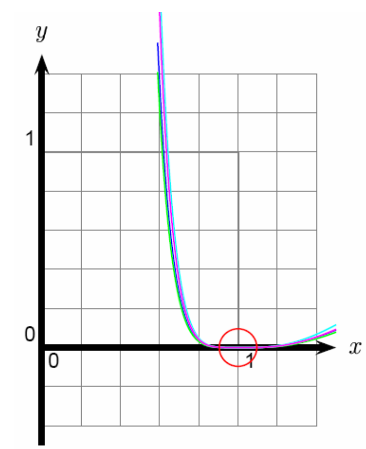
Birch and Swinnerton-Dyer

Graphs of $f_E(x)$



The graph of $f_{E_r}(x)$ vanishes to order r.

Examples of $f_E(x)$ that appear to vanish to order 4



Congruent Number Problem

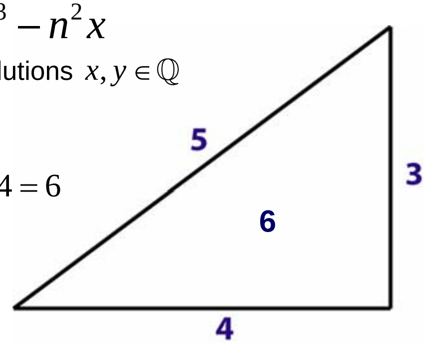
Open Problem: Decide whether an integer *n* is the area of a right triangle with rational side lengths.

Fact: Yes, precisely when the cubic equation

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

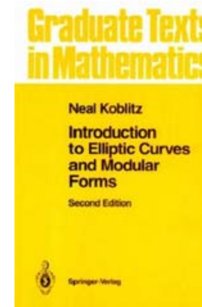
has infinitely many solutions $x, y \in \mathbb{Q}$

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



Connection with BSD Conjecture

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



See Koblitz for more details.

Gross-Zagier Theorem

Benedict Gross

Don Zagier

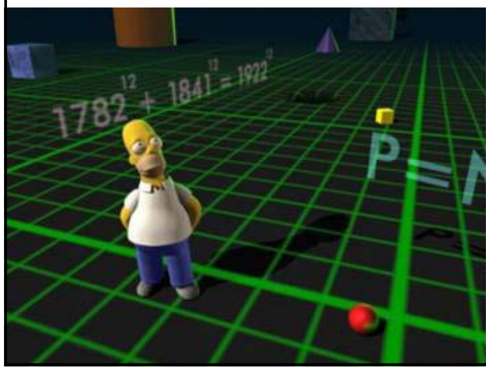
When the order of vanishing of $f_E(x)$ at 1 is exactly 1, then there is a nontorsion point on E.

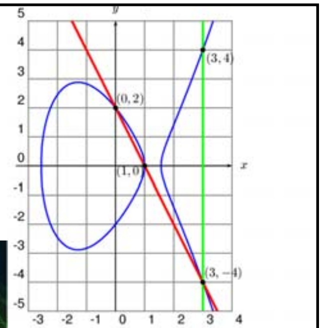
Subsequent work showed that this implies that the Birch and Swinnerton-Dyer conjecture is true when $f_E(x)$ has order of vanishing 1 at 1.

Kolyvagin's Theorem

Theorem. If $f_E(1)$ is nonzero then there are only finitely many solutions to *E.*

Thank You





The Group Law: $(1,0)+(0,2)=(3,4)$ on $y^2=x^3-5x+4$

Acknowledgements

- Benedict Gross
- Keith Conrad
- Ariel Shwayder (graphs of $f_E(x)$)