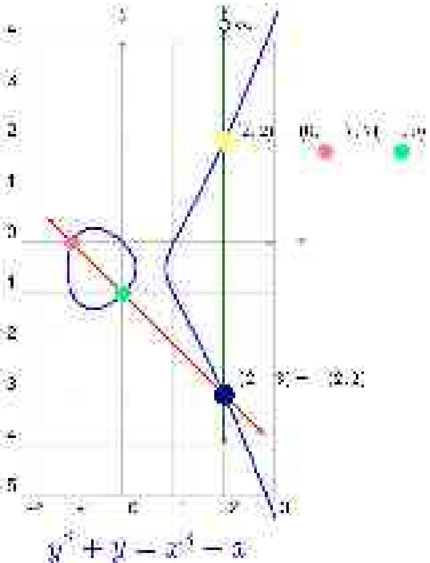
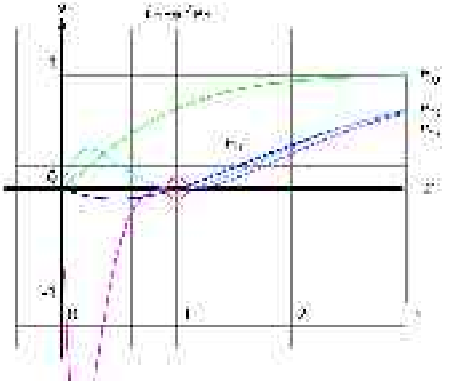
An Introduction to the Birch and Swinnerton-Dyer Conjecture

November 3, 2004
Univ. of Washington, Seattle

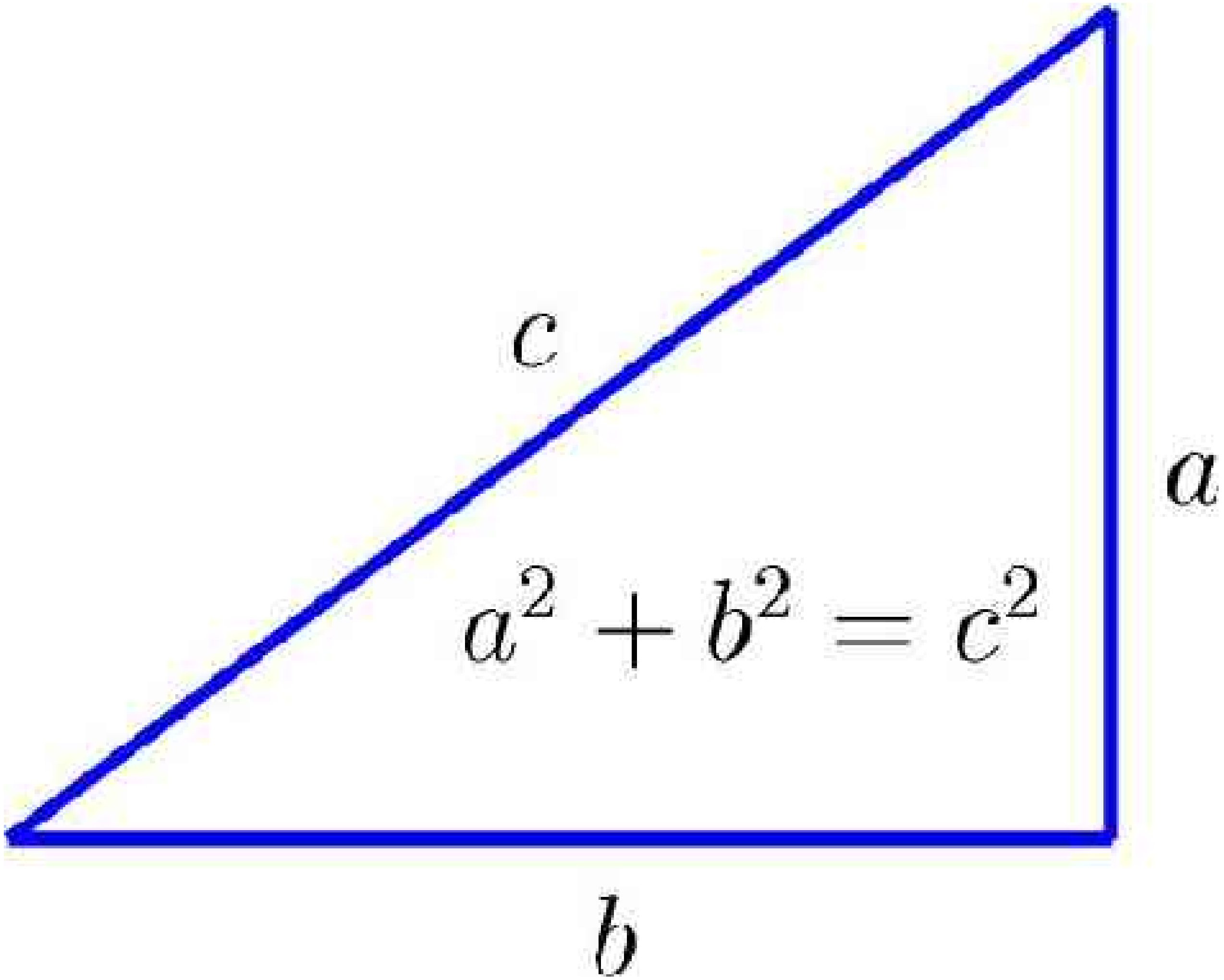


William Stein

http://modular.fas.harvard.edu

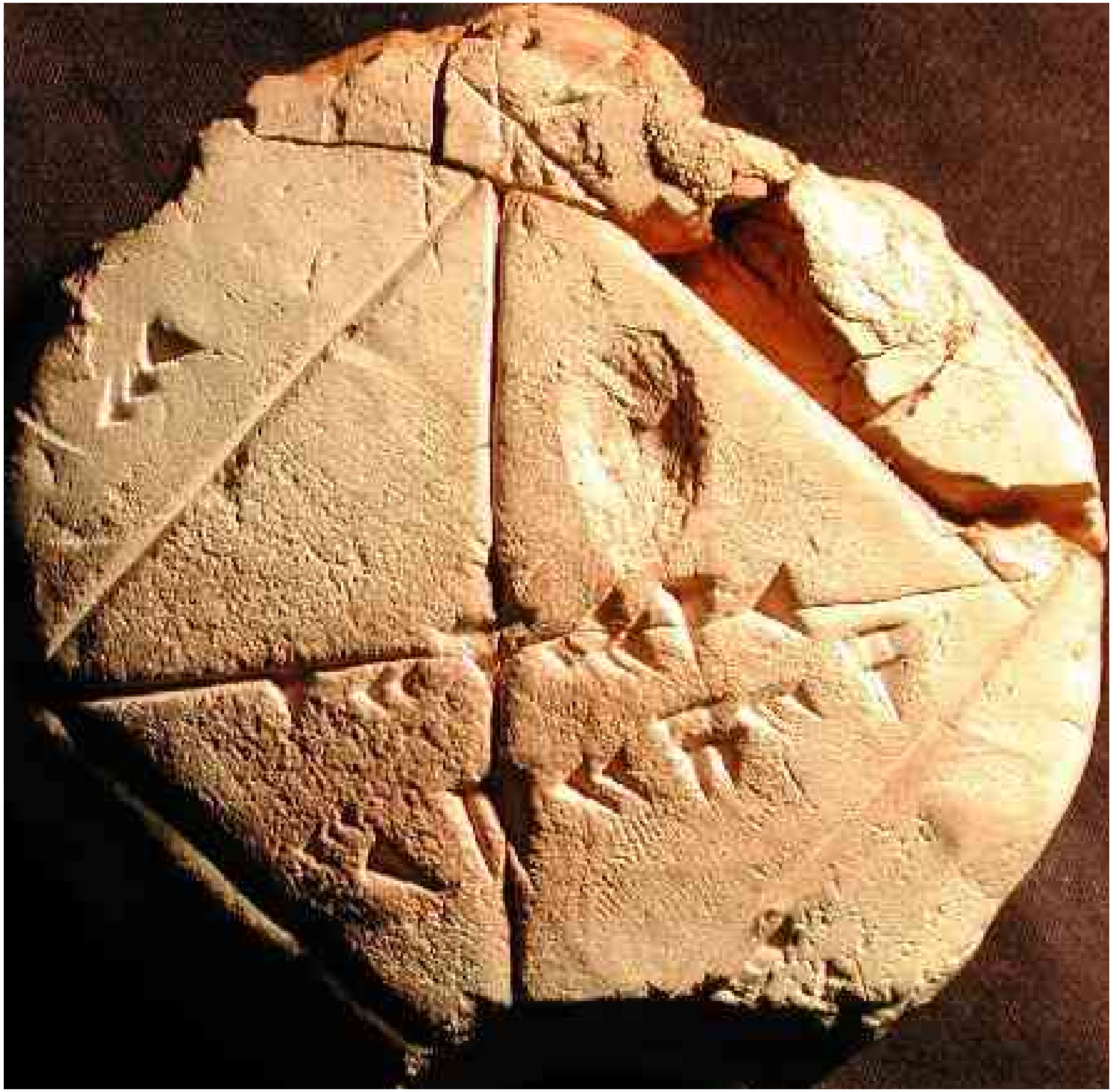


Pythagorean Theorem

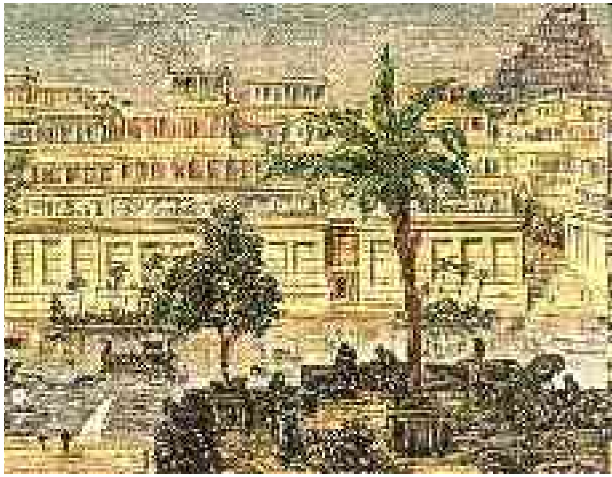


Pythagoras
approx 569-475 B.C.

Babylonians

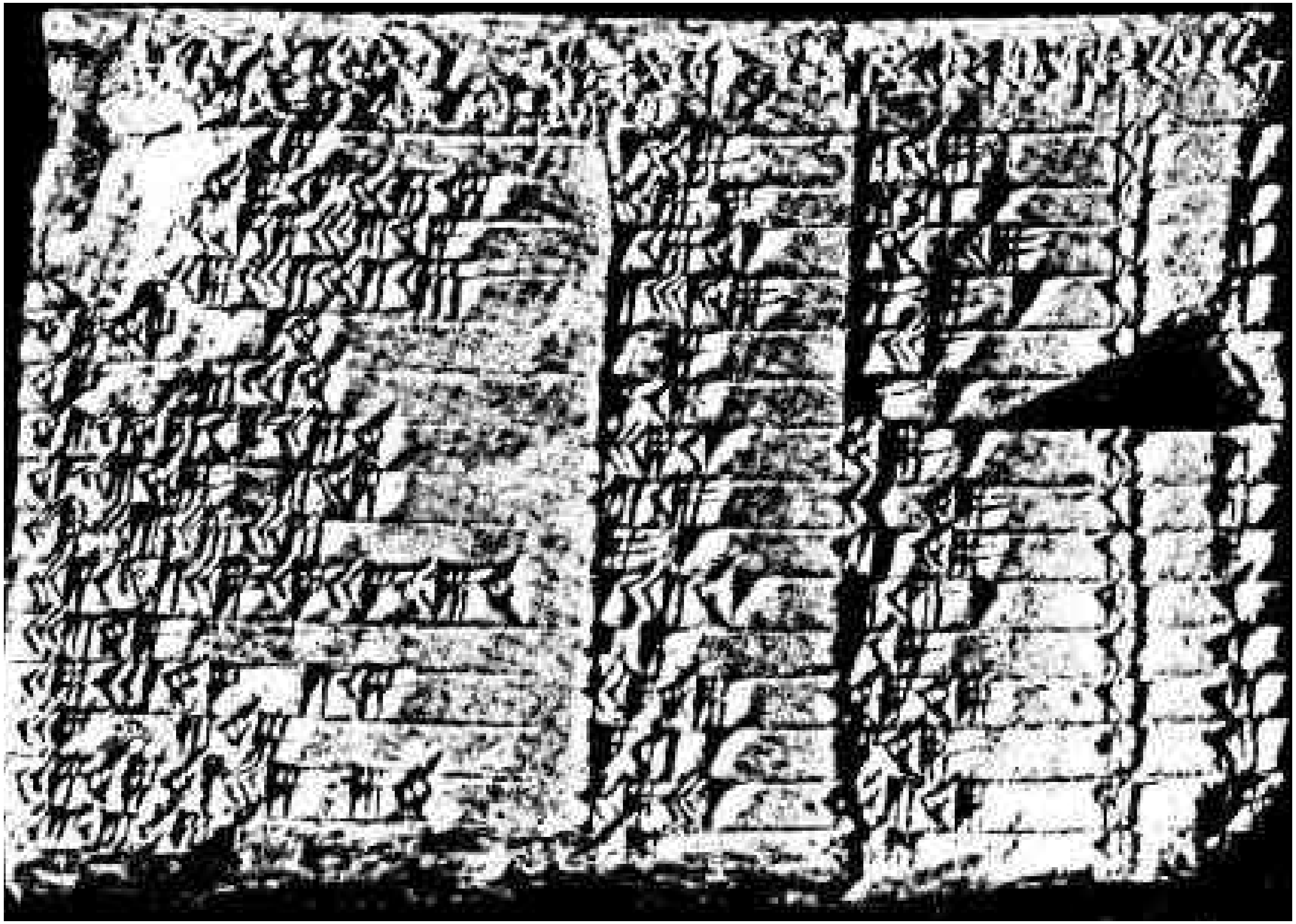


1800-1600 B.C.



Pythagorean Triples

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

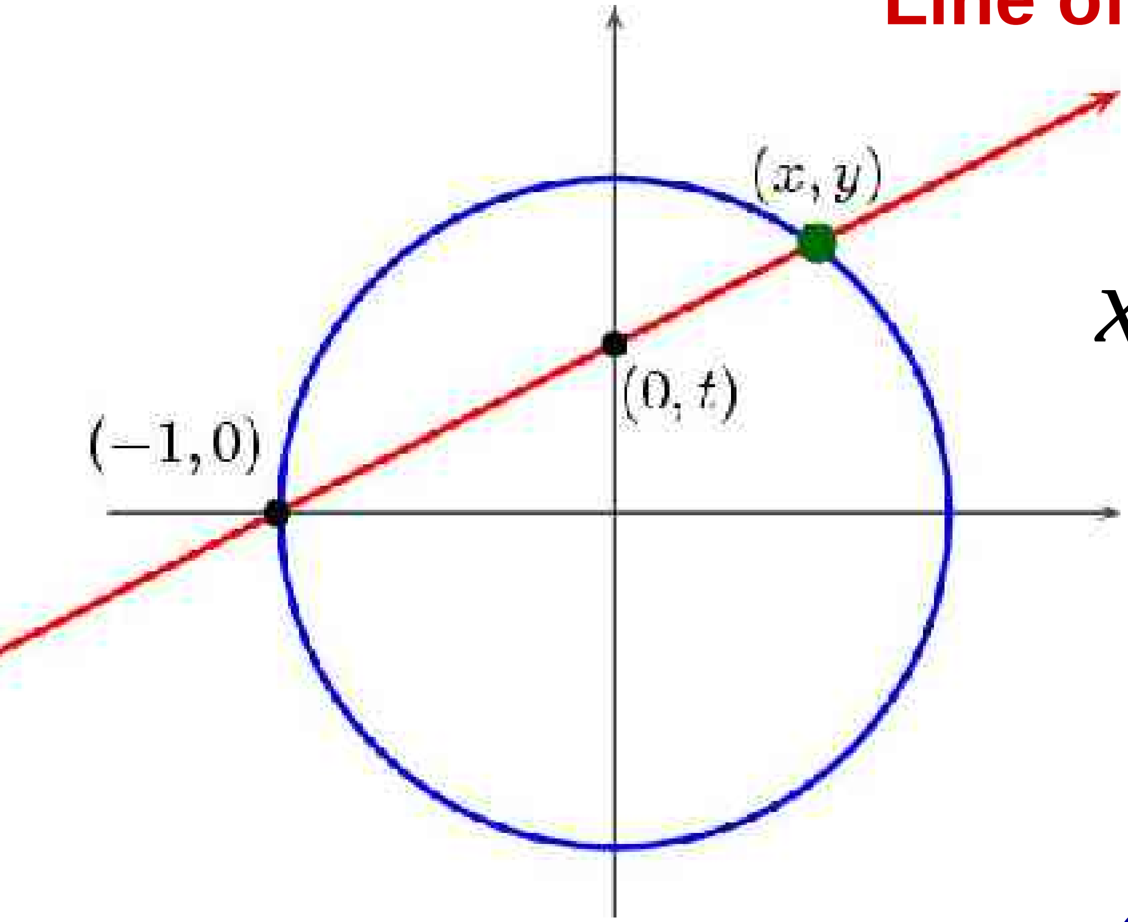


Triples of whole numbers *a*, *b, c* such that

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

Enumerating Pythagorean Triples

Line of Slope *t*

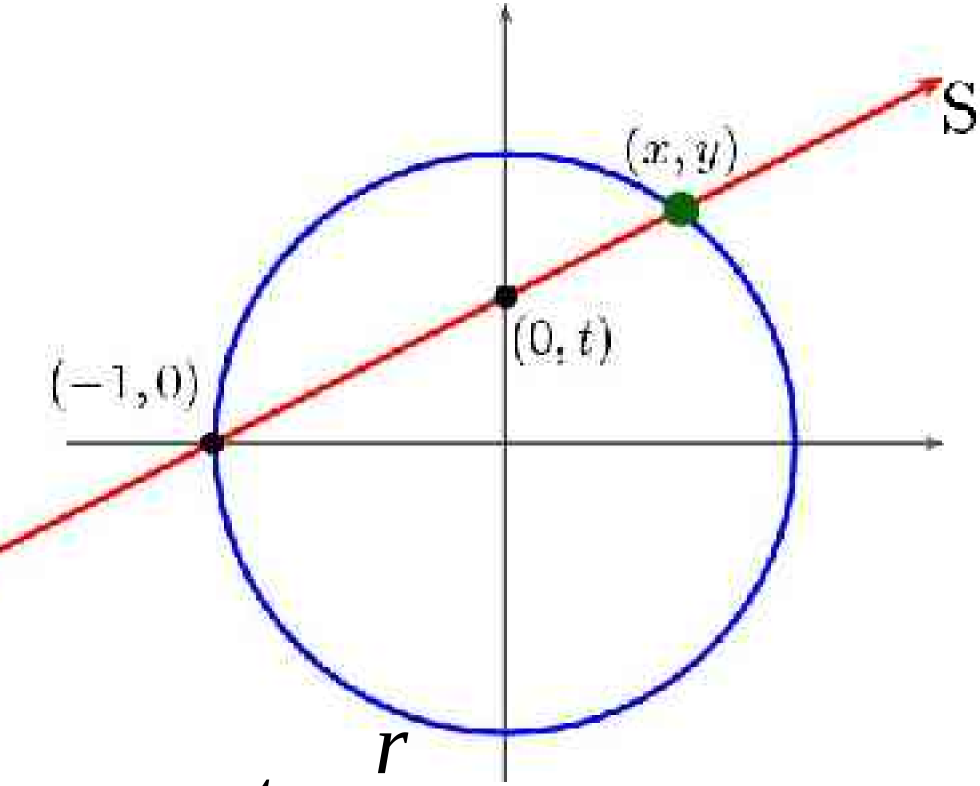


Circle of Radius 1

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

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

Enumerating Pythagorean Triples



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

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

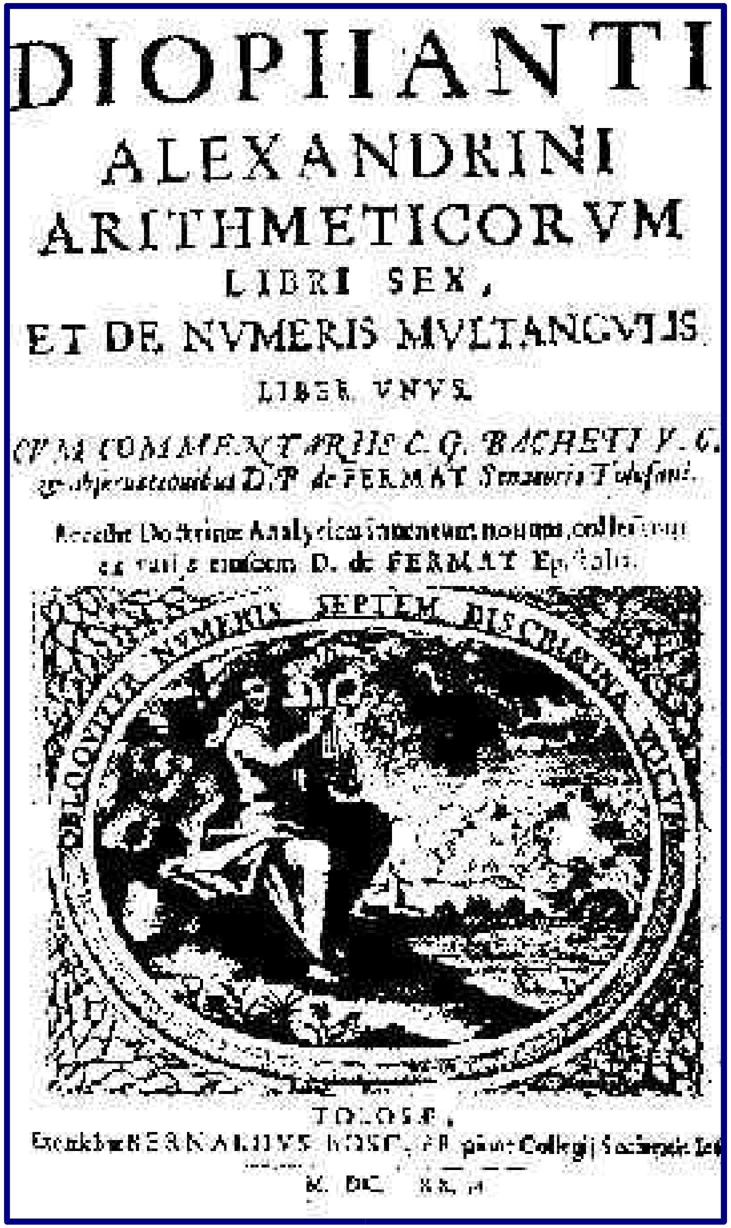
$$y = \frac{2t}{1+t^2}$$

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

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

is a Pythagorean triple.

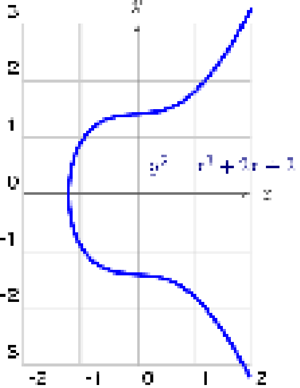
Integer and Rational Solutions



DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& obſervationibus D. P. de FERMAT Senatoris Tolofani.
Acceſſit Doctrinæ Analyticæ inventum novum, collectum
ex varijs eiuſdem D. de FERMAT Epiſtolis.

ELOQVITVR NVMERIS SEPTEM DISCRIMINA VOCVM

TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Iesu.
M. DC. LXX.

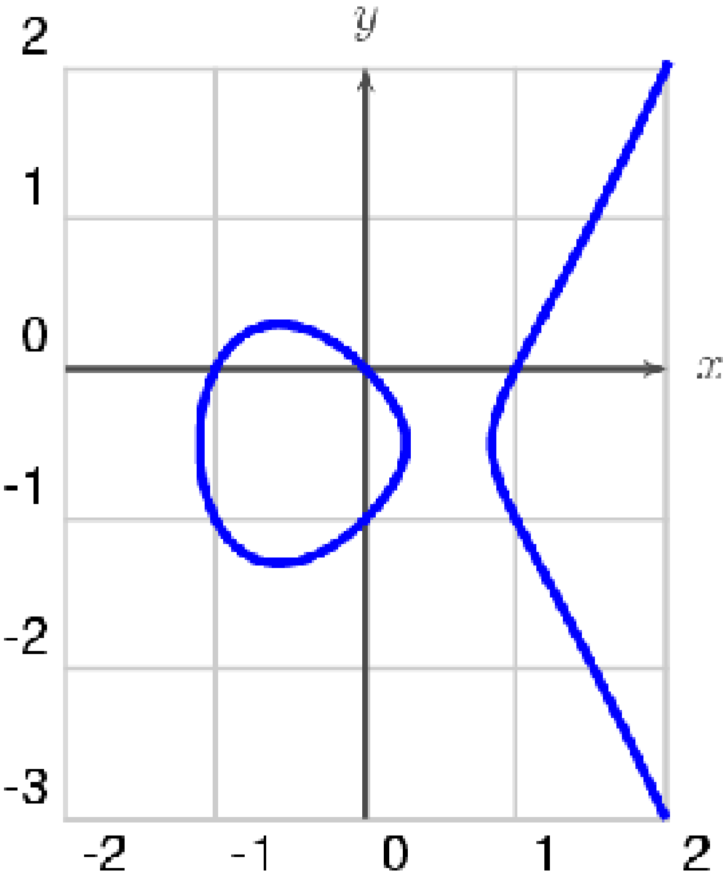


Elliptic Curves

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

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

$$\xcancel{3x^3 + 4y^3 + 5 = 0}$$

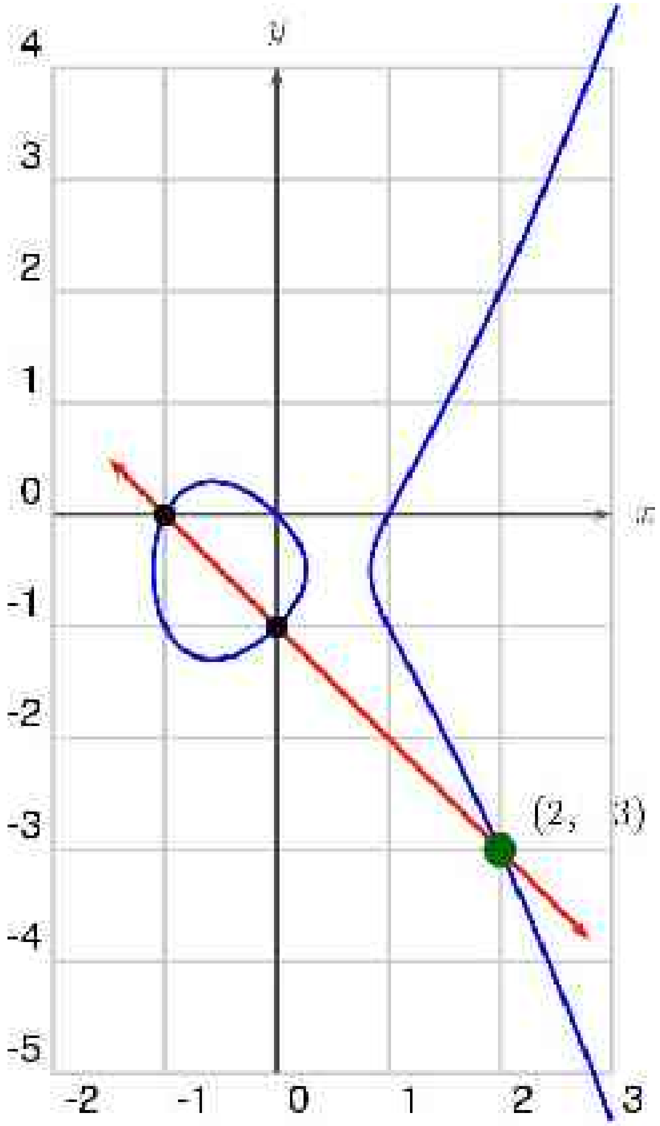


$$y^2 + y = x^3 - x$$

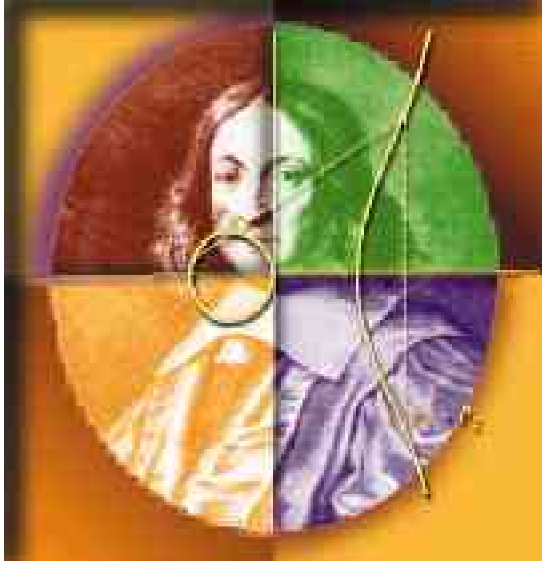
Cubic algebraic equations in two unknowns *x* and *y*.

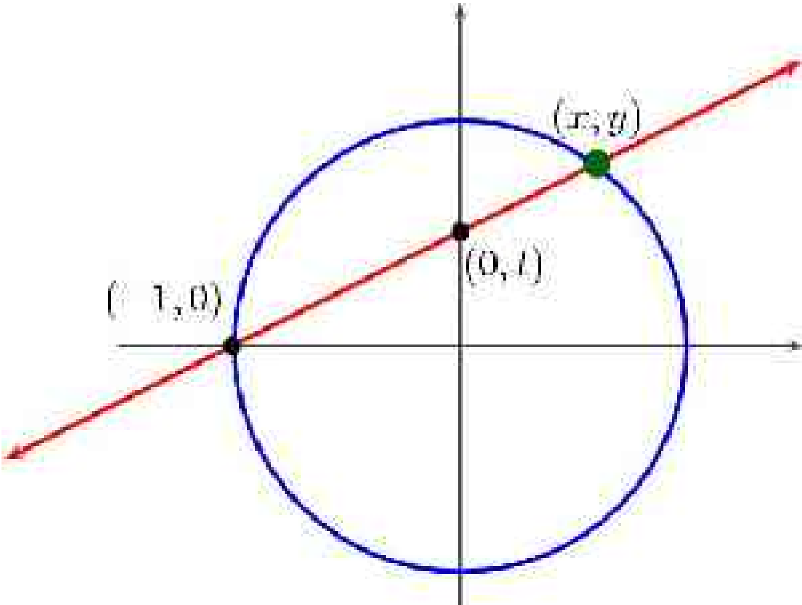
Exactly the 1-dimensional compact algebraic groups.

The Secant Process

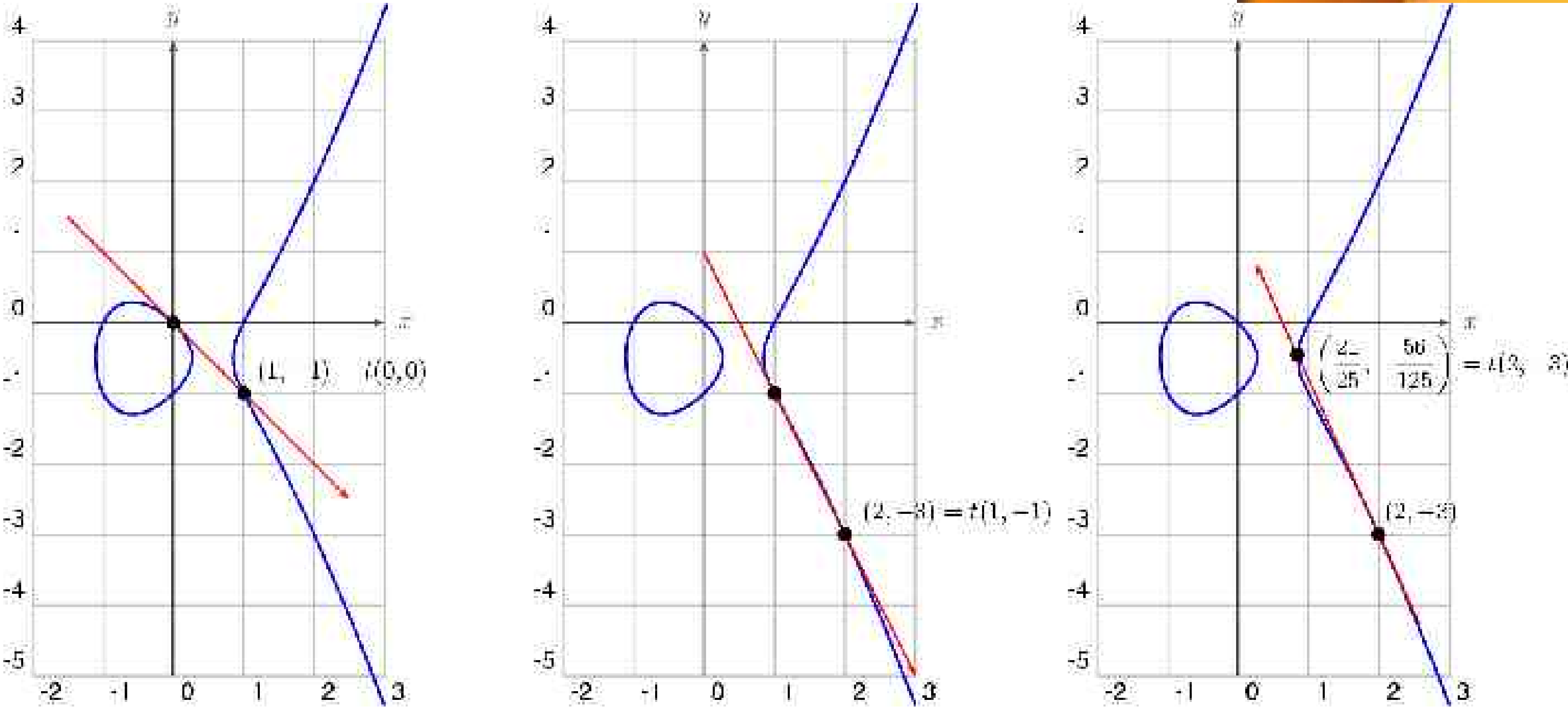


$y^2 + y = x^3 - x$



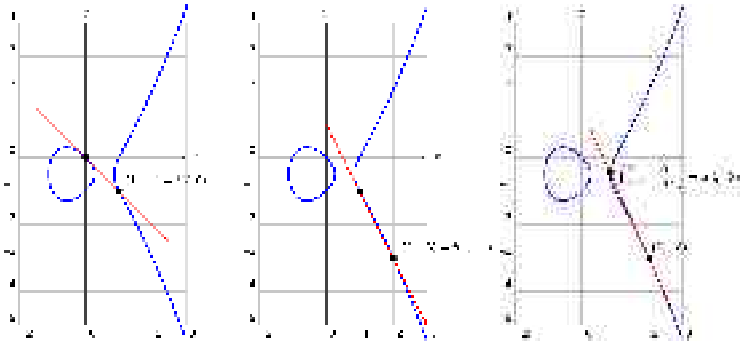


The Tangent Process



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

Big Points From Tangents



$$(0,0)$$

$$(1,-1)$$

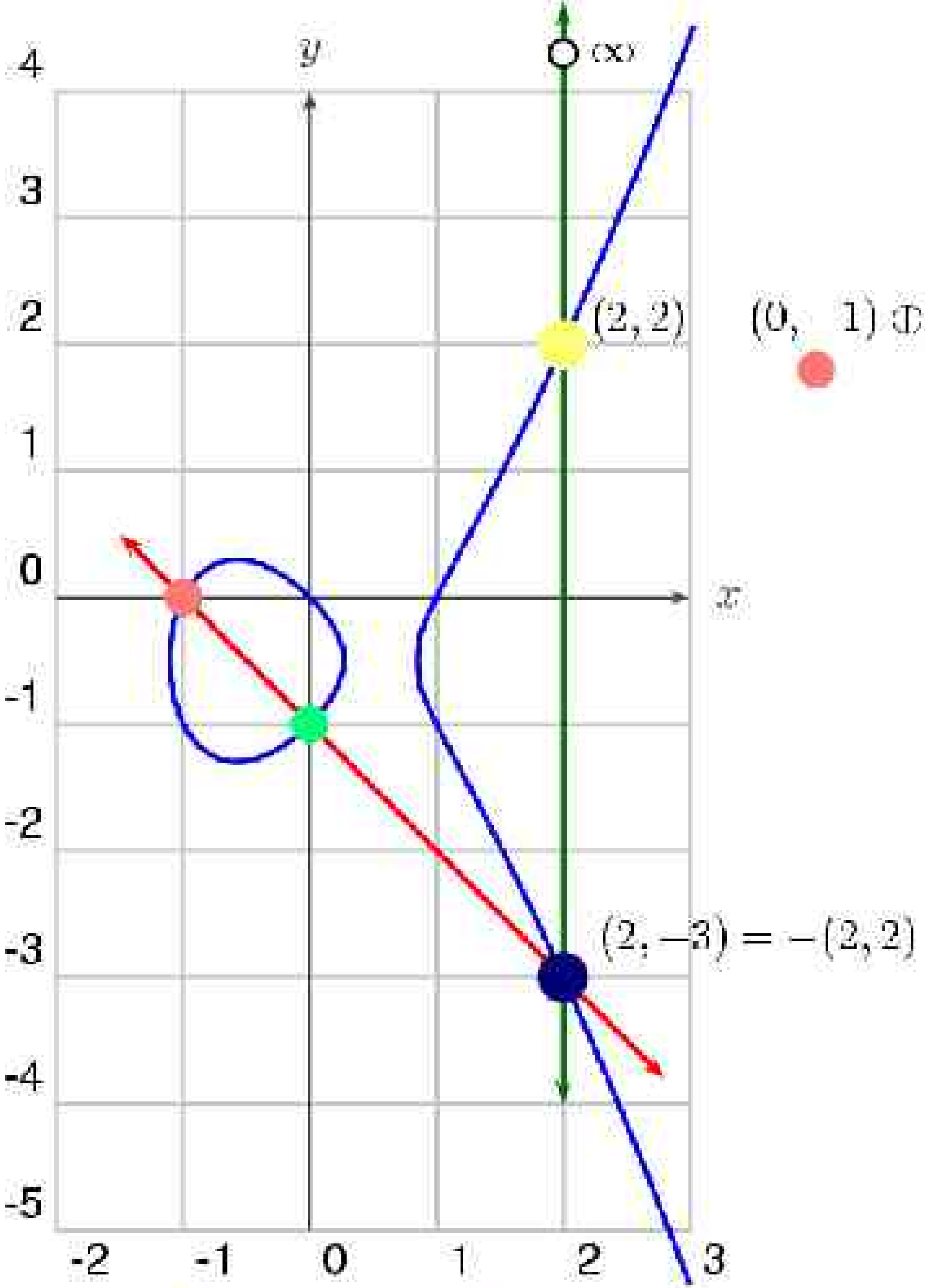
$$(2,-3)$$

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

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

$$\left(\frac{5313922364481462429082 1}{18700987715366274360 25};-\frac{122825400695558582174111316269938 1}{80871745605559864852893980186125}\right)$$

The Group Operation

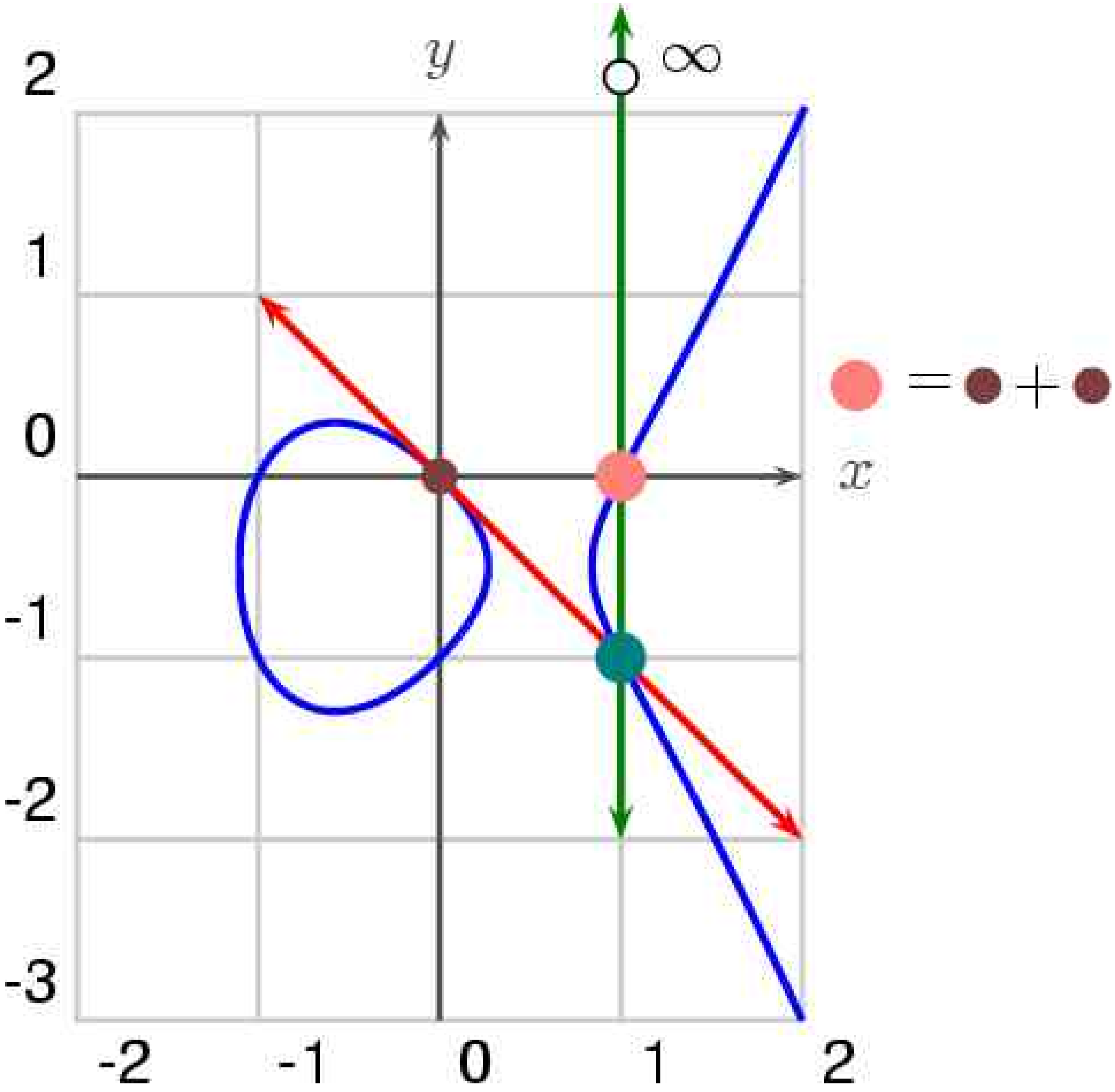


$$y^2 + y = x^3 - x$$

(0, 1) ⊕ (1, 0)

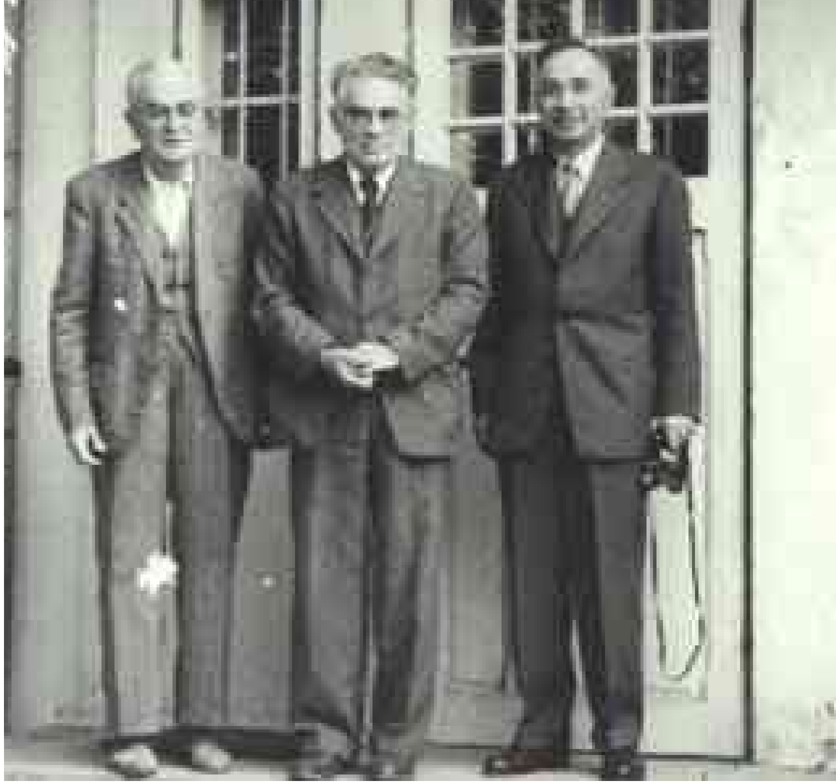
$$\boxed{E(\mathbf{Q}) \cong \mathbf{Z}}$$

Group Law When *P*=*Q*



Mordell's Theorem

The group $E(\mathbf{Q})$ 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

The Simplest Solution Can Be Huge

Stolls

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

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

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

(Found by Michael Stoll in 2002)

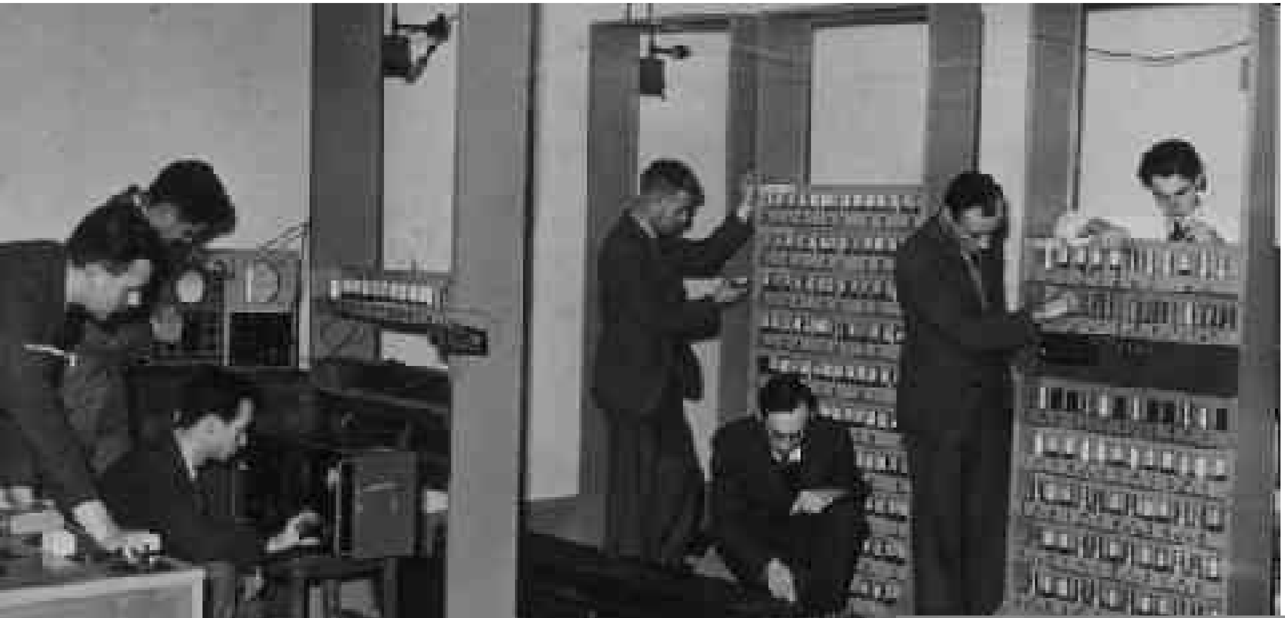
Central Question

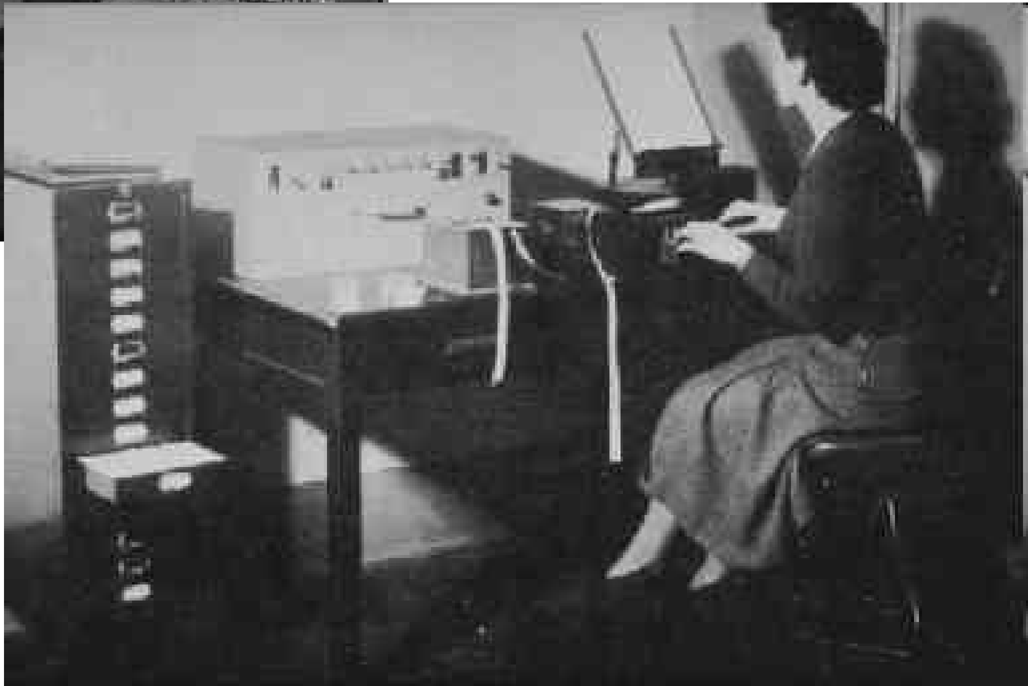
How many solutions are needed to generate all solutions to a cubic equation?

Birch and Swinnerton-Dyer

EDSAC in Cambridge, England

More EDSAC Photos





Electronic **D**elay
Storage **A**utomatic
Computer

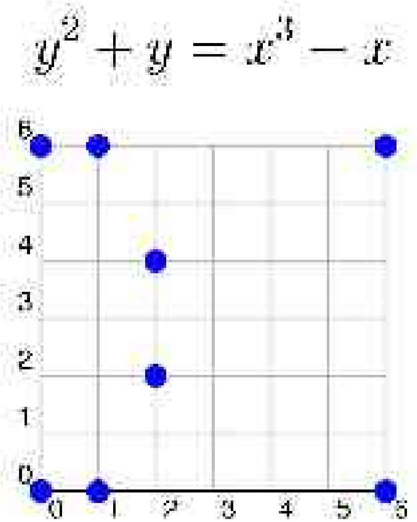
Conjectures Proliferated

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.”

Solutions Modulo *p*



Consider solutions modulo a prime number:

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

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,

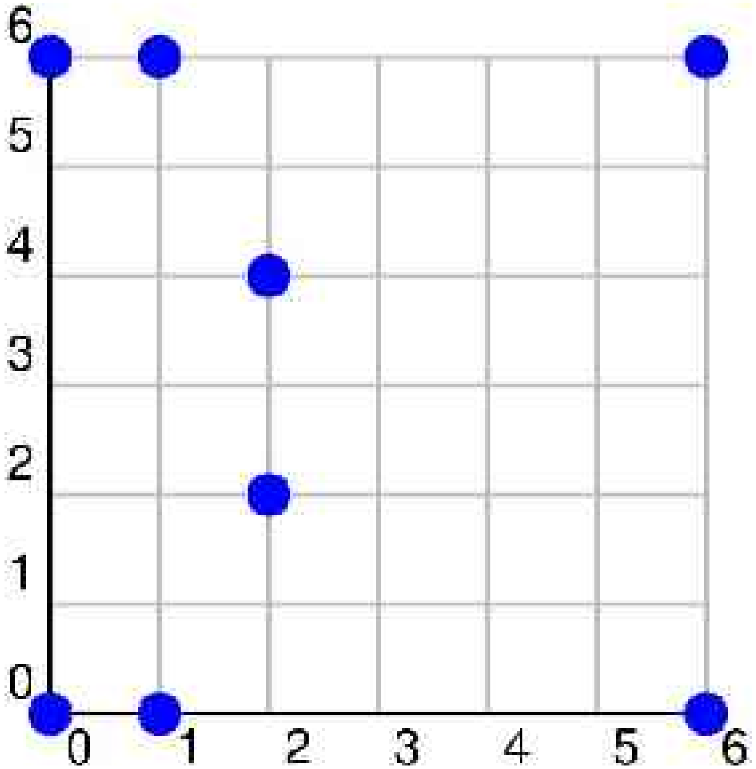
$$4^2 + 4 \equiv 2^3 - 2 \pmod{7}.$$

This idea generalizes to any cubic equation.

Counting Solutions

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

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



$$N(7) = 8$$

The Error Term
(Hasse's Bound

1898-1979

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

error term

$$\boxed{|A(p)| \le 2\sqrt{p}}$$

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

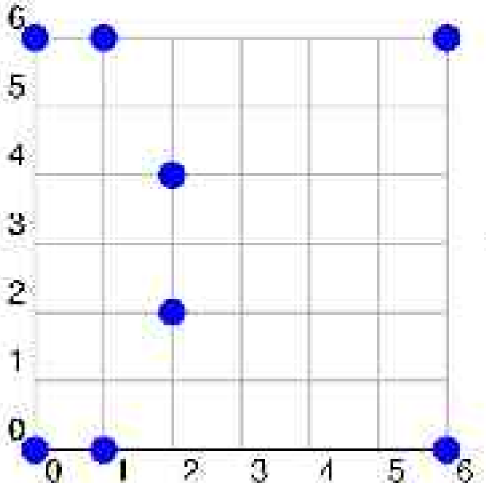
Note for experts: $A(p) = -a_p$

More Primes

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

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

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



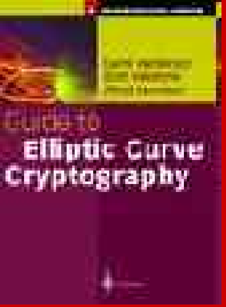
$N(p) =$ number of soln's

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

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

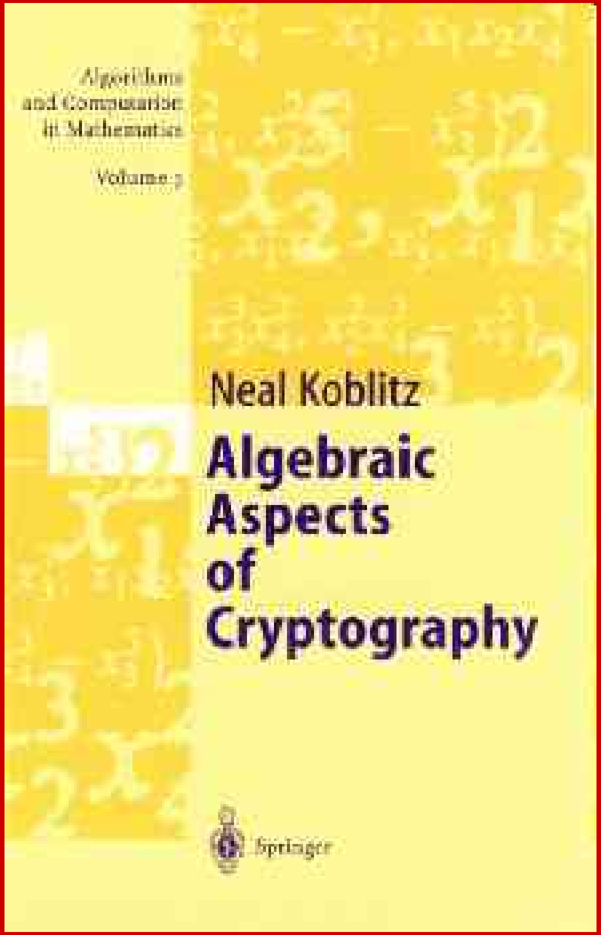
Continuing: $A(13) = 2,\ A(17) = 0,\ A(19) = 0,\ A(23) = \text{-}2,\ A(29) = \text{-}6,\ A(31) = 4,\ \ldots.$

Commercial Break: Cryptographic Application



Guide to
Elliptic Curve
Cryptography

NATIONAL SECURITY AGENCY



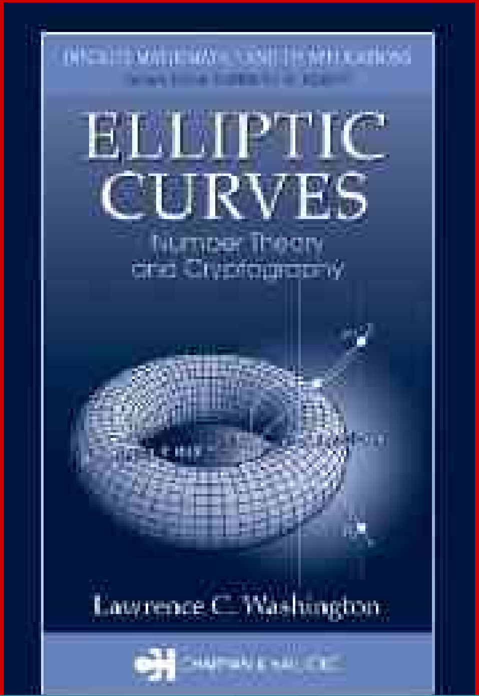
Algorithms
and Computation
in Mathematics

Volume 3

Neal Koblitz

Algebraic Aspects of Cryptography

Springer

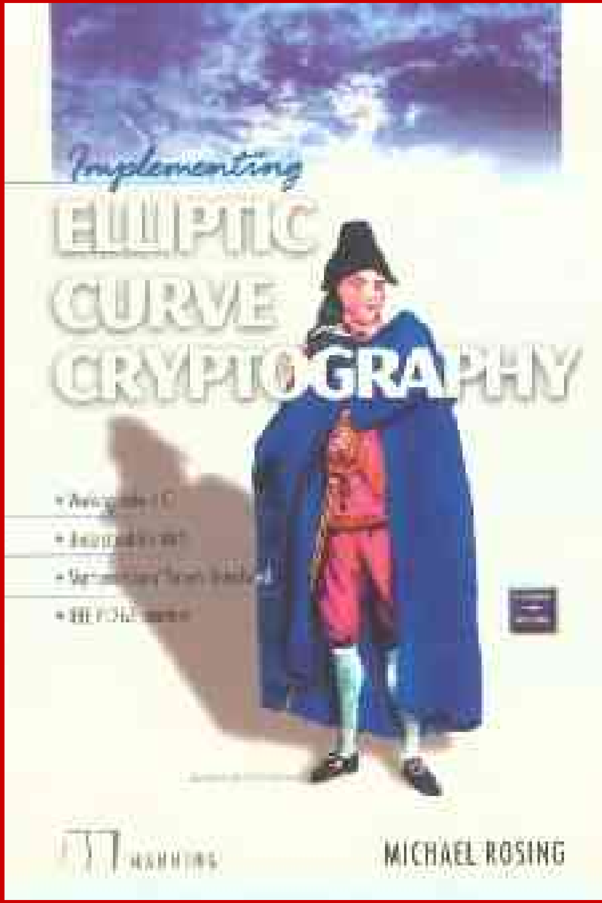


ELLIPTIC CURVES

Number Theory
and Cryptography

Lawrence C. Washington

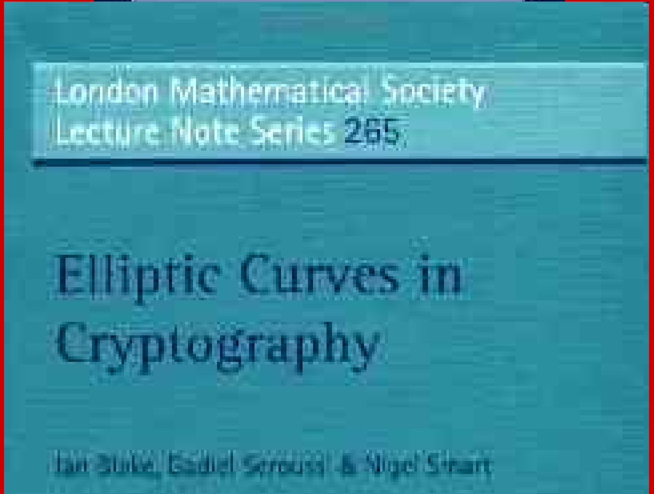
CHAPMAN & HALL/CRC



Implementing
ELLIPTIC CURVE CRYPTOGRAPHY

MANNING

MICHAEL ROSING



London Mathematical Society
Lecture Note Series 265

Elliptic Curves in
Cryptography

Ian Blake, Gadiel Seroussi & Nigel Smart

TOP SECRET

Guess

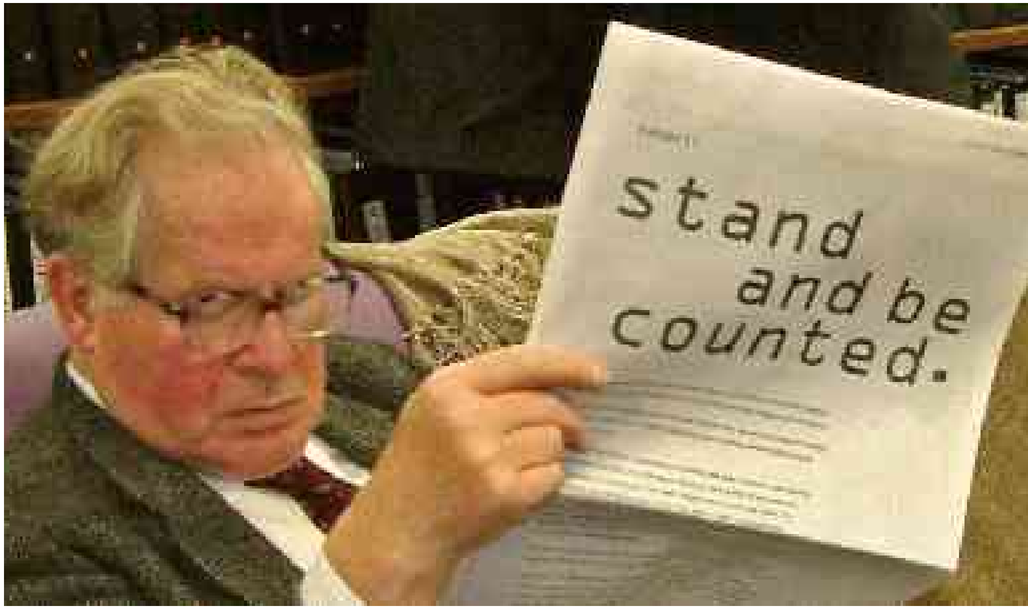
If a cubic curve has infinitely many solutions, then probably $N(p)$ is **larger** than p, for many primes p.

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 *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 for

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

Formally:

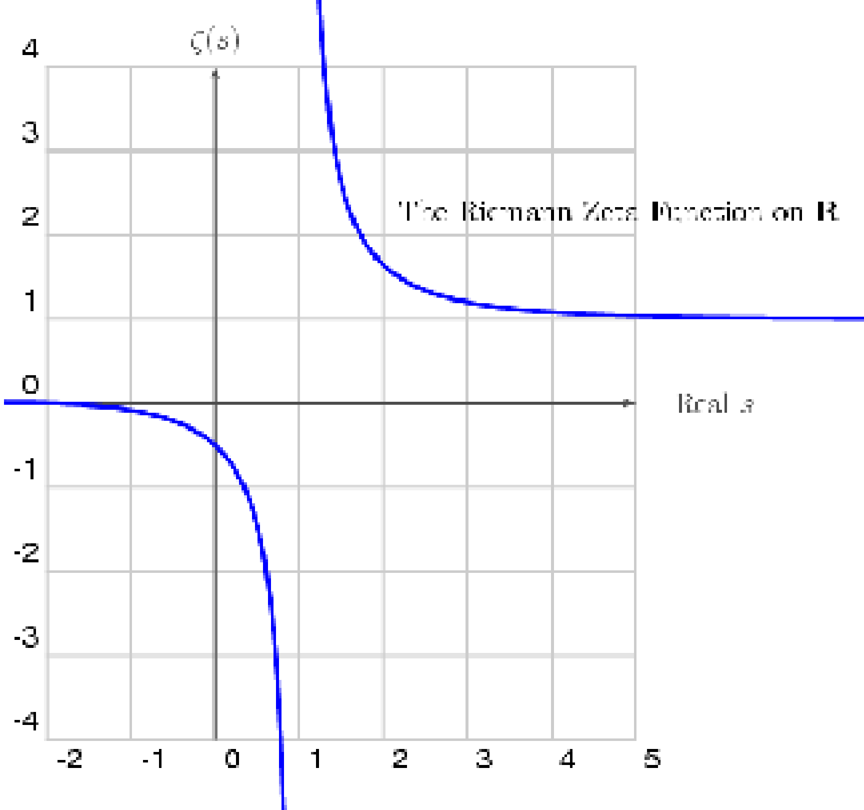
$$L(E,1) = \text{"}\prod \frac{p}{N(p)+1}\text{"}$$

The Riemann Zeta Function

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

1826-1866

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



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

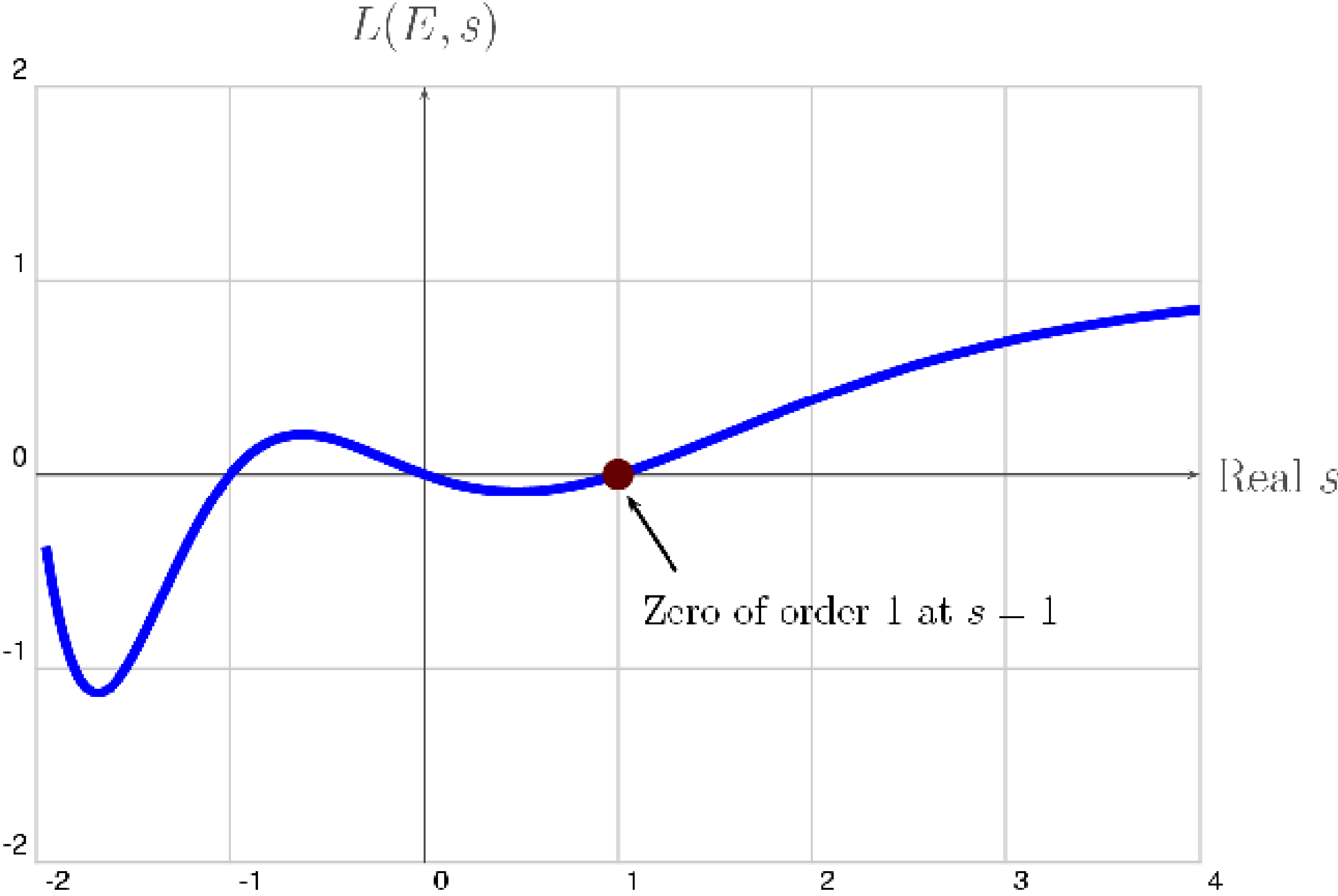
The Modularity Theorem

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



***L*-series for** $y^2 + y = x^3 - x$

The Birch and Swinnerton-Dyer Conjecture

The order of vanishing of

$$L(E,s)$$

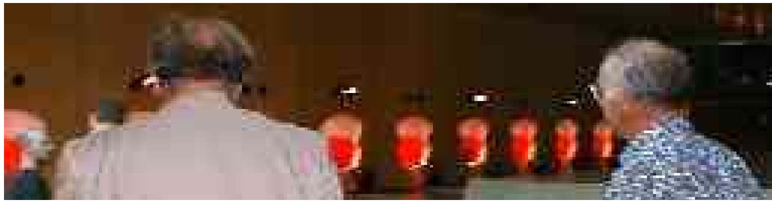
at 1 equals the rank of the group $E(\mathbf{Q})$ of all rational solutions to E:

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

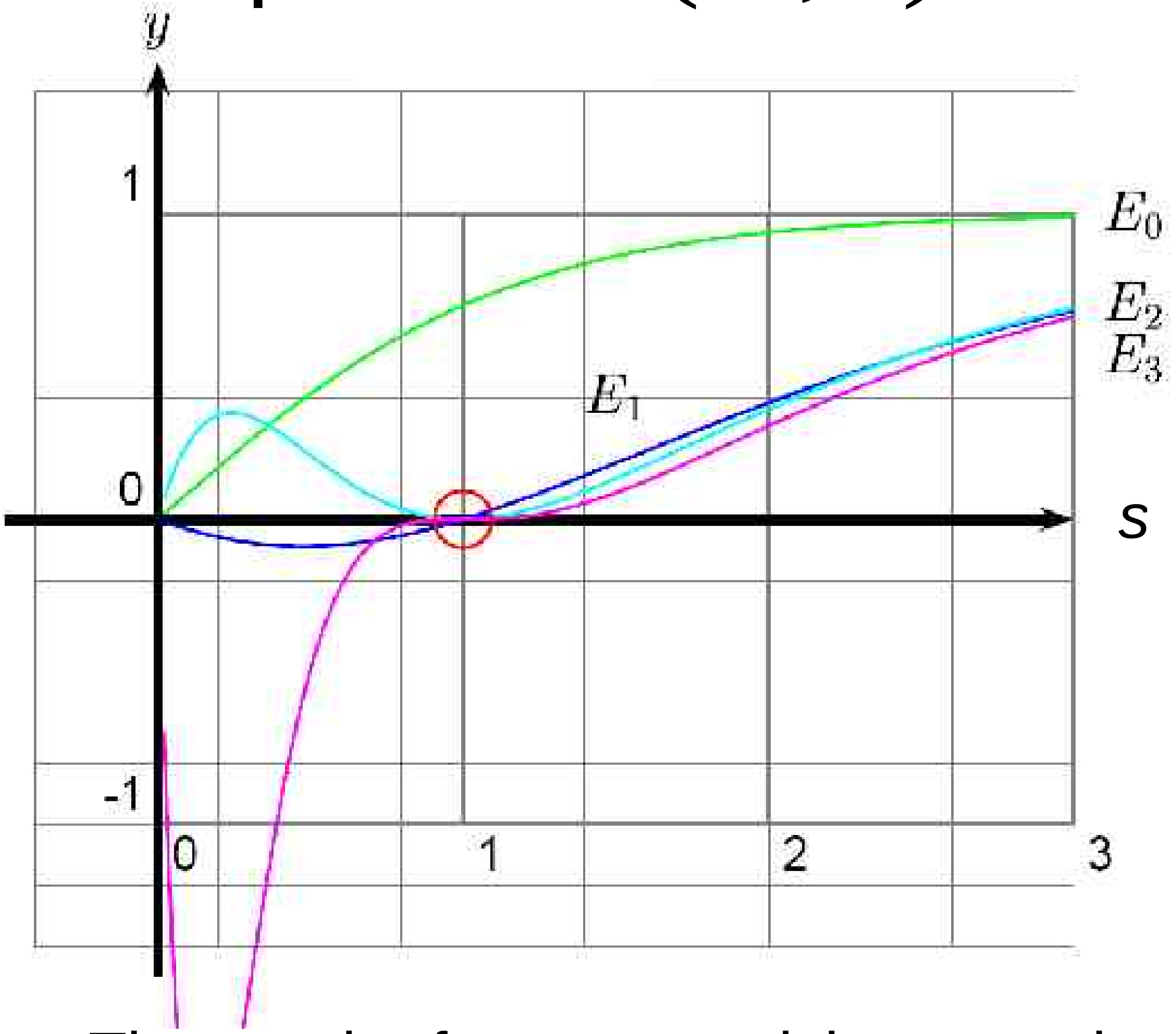
(CMI: *$1000000 reward for a proof.)*

Bryan Birch

Birch and Swinnerton-Dyer

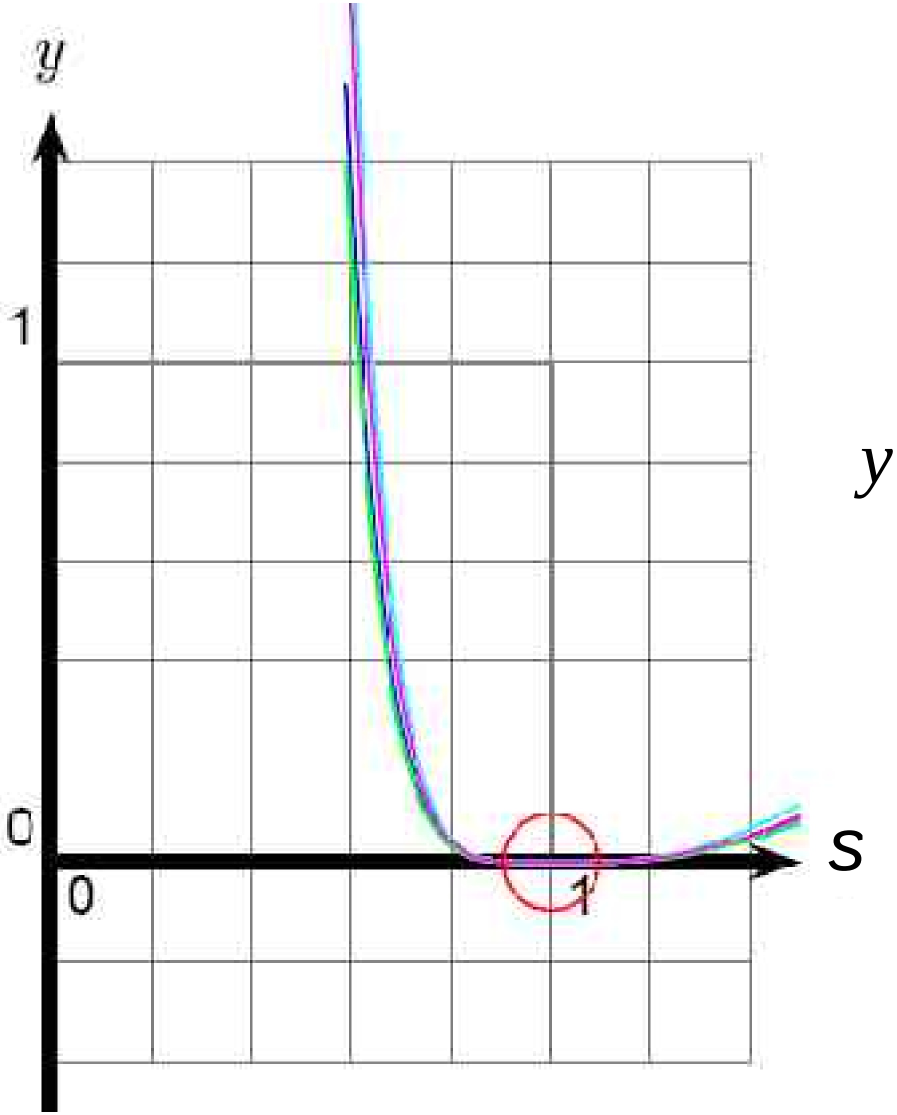


More Graphs of $L(E,s)$ for s real



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

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.*

Congruent Number Problem

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

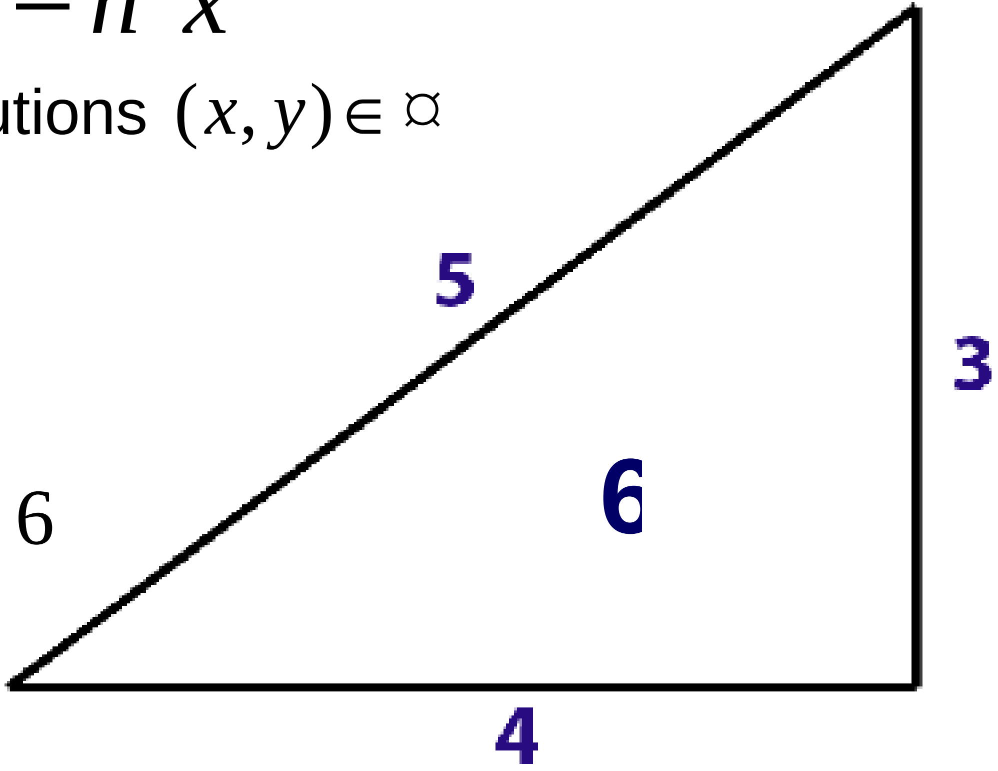
Fact: Yes, precisely when the cubic equation

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

has infinitely many solutions $(x, y) \in$ ¤

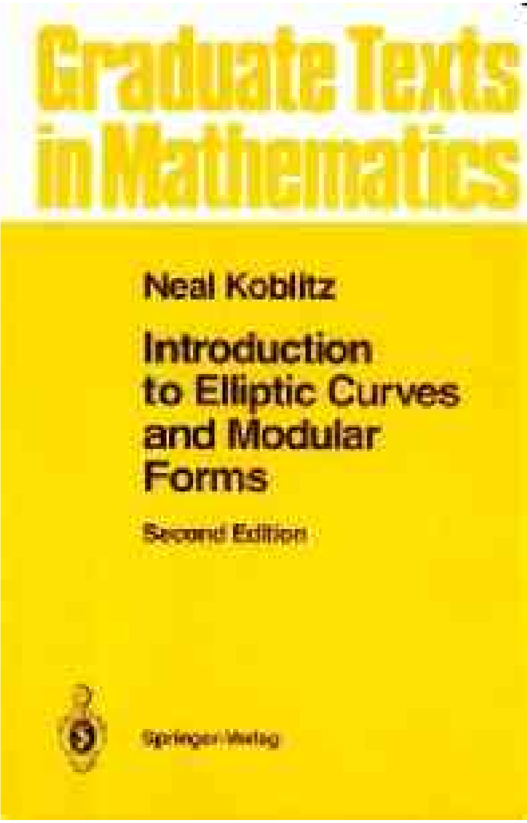
$$n = 6$$

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



Connection with BSD Conjecture

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



Graduate Texts in Mathematics

Neal Koblitz

Introduction to Elliptic Curves and Modular Forms

Second Edition

Springer-Verlag

See [Koblitz] for more details

Benedict Gross

The Gross-Zagier Theorem

Don Zagier

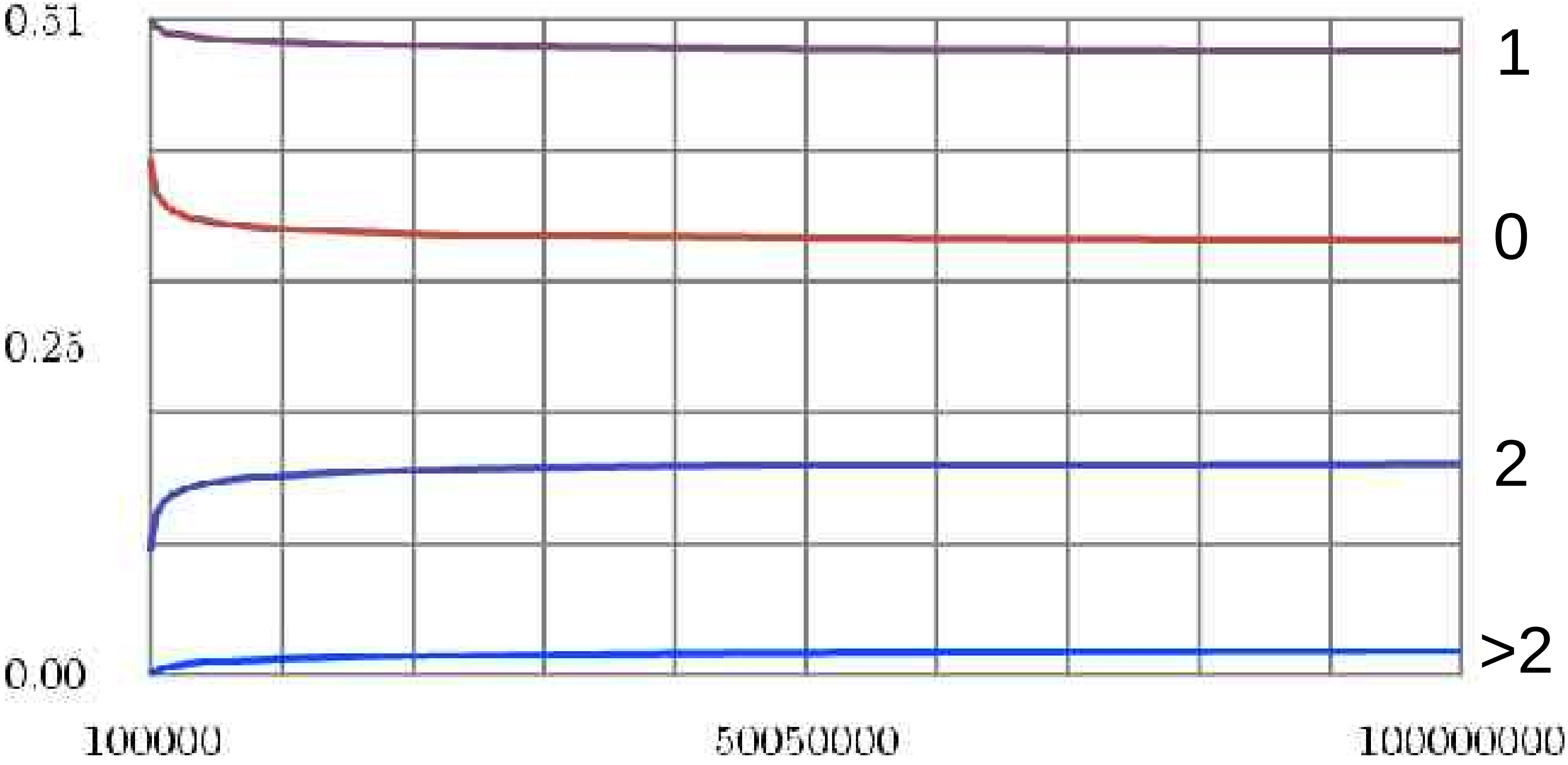
When the order of vanishing of $L(E,s)$ at s=1 is one, then E has rank at least one.

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.

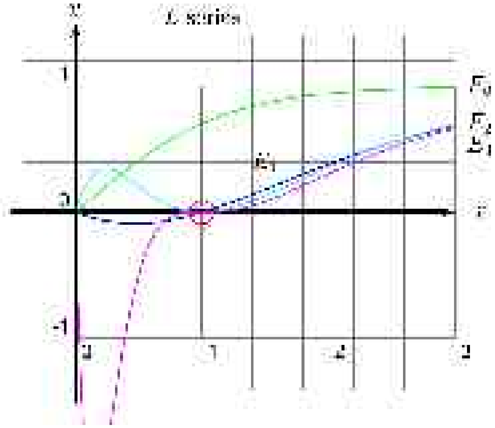
Kolyvagin’s Theorem

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*.

How Many Curves Are Covered by Kolyvagin’s Theorem?

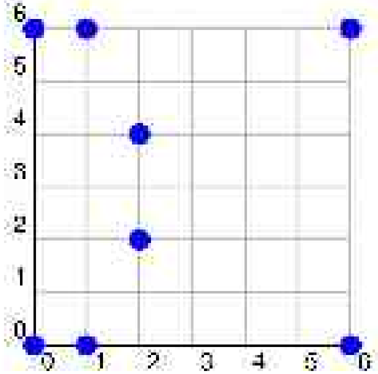


Proportion of curves of rank 1, 0, 2, and >2 as a function of the “conductor” for the more than 130 million elliptic curves with discriminant < 10^12, c4<1.44*10^12 in the Stein-Watkins database.



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

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



Thank You

Acknowledgments

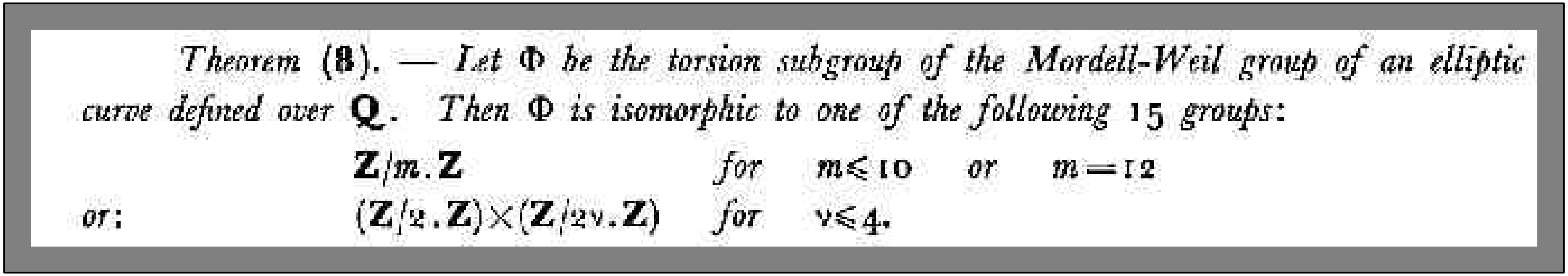
- Benedict Gross
- Keith Conrad
- Ariel Shwayder (graphs of $L(E,s)$)

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* **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* $\nu \leqslant 4$.