Rational Points on Modular Elliptic Curves

I. Elliptic Curves

Hedrick Lecture Series

MAA MathFest
Boulder, Colorado
August 2003

http://www.math.mcgill.ca/darmon
/slides/slides.html

Elliptic Curves

Definition: An *elliptic curve* over the field $\mathbf{Q}$ of rational numbers is an equation of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in \mathbf{Q}$. (The variables are x and y.)

Simpler form:

$$\boxed{y^2 = x^3 + ax + b,}$$

with $\Delta := 4a^3 - 27b^2 \neq 0$.

Question. Why study such a special type of equation?

Diophantine equations

A *Diophantine Equation* is a (system of) polynomial equation(s)

$$f_1(x_1, \ldots, x_m) = 0$$

$$f_2(x_1, \ldots, x_m) = 0$$

$$\vdots$$

$$f_n(x_1, \ldots, x_m) = 0$$

with *integer* or *rational coefficients*, of which one is interested in *integer* or *rational* solutions.

Theorem (Matijasevich). There is no general algorithm to decide whether any given Diophantine equation admits an integer solution.

(In other words: A number theorist cannot be replaced by a computer.)

Some Diophantine equations

$$3x + 7y = 0$$

$$x^n + y^n = z^n \text{ (Fermat)}$$

$$x^2 - Dy^2 = 1 \text{ (Fermat-Pell)}$$

$$x^3y + y^3z + z^3x = 0 \text{ (Klein)}$$

$$y^2 = x^3 + ax + b \text{ (Fermat, ..., Wiles, ...)}$$

$$x^{17}y^{11}w^5 - 27xy^3z^2 + 119xw - 121w - 93 = 0$$

Challenge: to identify, in the chaotic, non-computable wilderness of all Diophantine equations, the ones that are the most *natural* and *interesting*.

In this quest, *history* and *tradition* often serve as guides.

The equations that are the most studied today are often *the same* as those that fascinated the mathematicians of the 17th, 18th and 19th centuries (Fermat, Euler, Lagrange, Legendre, Gauss, Kummer, Kronecker, Klein, Fricke, ...)

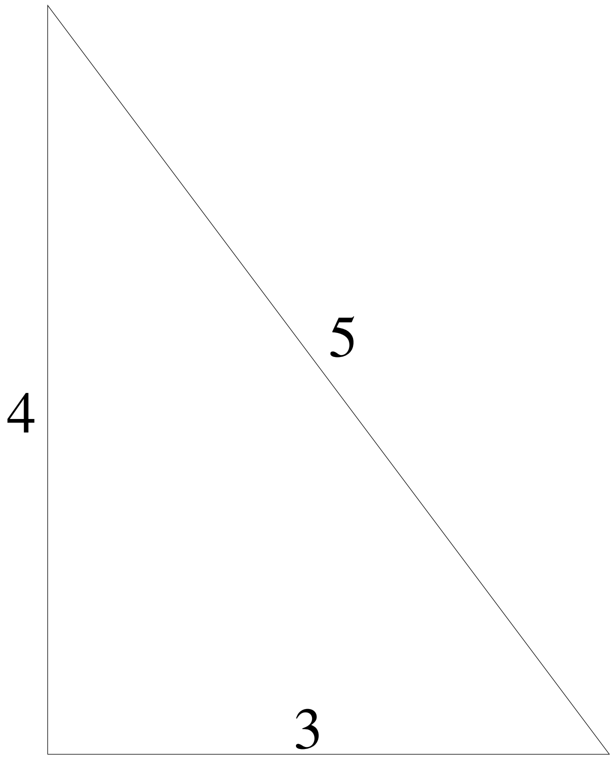
Principle. A Diophantine equation is *interesting* if it gives rise to a rich, well-structured theory, with strong connections to the main themes of the subject (reciprocity laws, modular forms, ...)

The *main goal* of this lecture series is to explain why elliptic curves enjoy this feature.

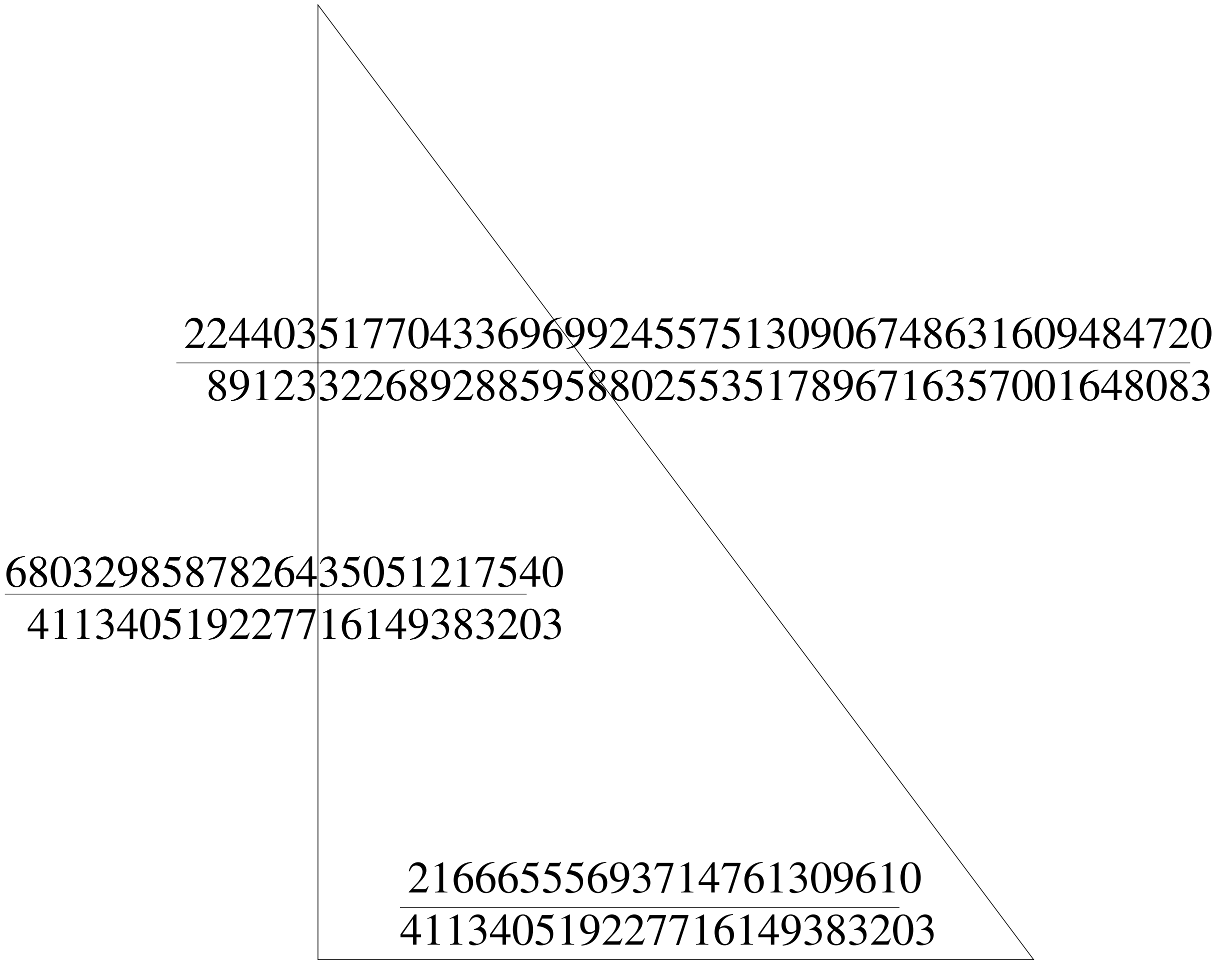
The congruent number problem

Definition. An integer n is a *congruent number* if it is the area of a right-angled triangle with rational side lengths.

Examples: 6 is a congruent number...



... and so is 157!



$$\frac{224403517704336969924557513090674863160948472}{0891233226892885958802553517896716357001648083}$$

$$\frac{6803298487826435051217540}{411340519227716149383203}$$

$$\frac{21666555693714761309610}{411340519227716149383203}$$

Congruent numbers and elliptic curves

Elementary manipulations show:

Theorem n is a congruent number if and only if the elliptic curve

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

has a non-trivial solution (with $y \neq 0$).

One is thus led to a question about elliptic curves!

Question: Study the set of rational solutions to the equation E_n.

Fermat

Theorem (Fermat) The elliptic curve

$$\boxed{\ y^2 = x^3 - x}$$

has no non-trivial solution (i.e., 1 is *not* a congruent number).

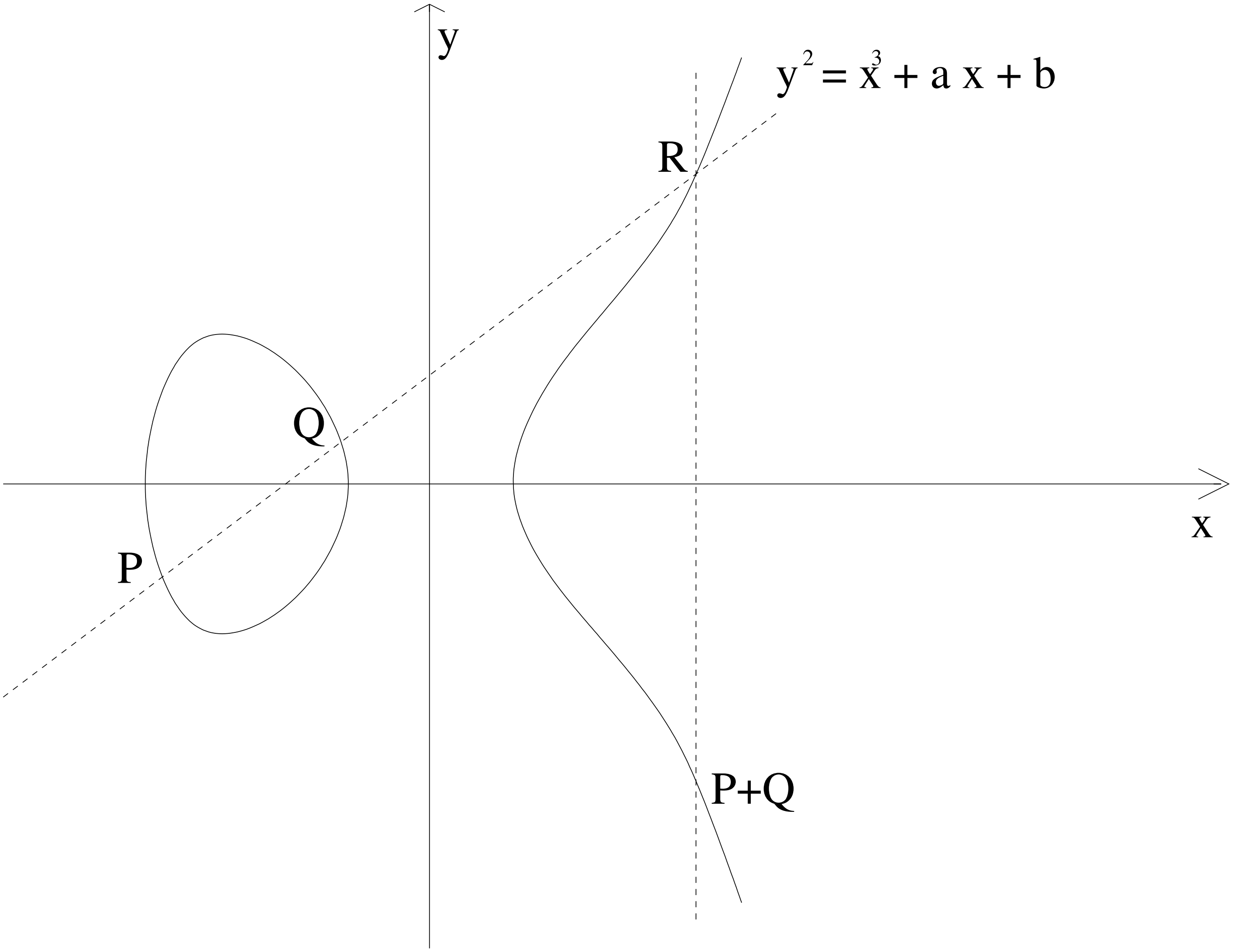
By elementary manipulations, this is equivalent to:

$\boxed{x^4 + y^4 = z^2}$ has no non-trivial solution.

Fermat's descent: Most importantly, Fermat introduced a general approach, the *method of descent*, for checking (in some cases) whether an elliptic curve has a rational solution or not.

The group law

Elliptic curves are endowed with a structure of *algebraic group*.



The addition law on an elliptic curve

The Mordell-Weil Theorem

In particular, the set $E(\mathbf{Q})$ of rational solutions to E is an *abelian group* in a natural way.

Theorem: The group $E(\mathbf{Q})$ is a finitely generated abelian group.

$$E(\mathbf{Q}) \simeq \mathbf{Z}^r \oplus T.$$

The integer r is called the *rank* of $E(\mathbf{Q})$.

Problem. Is there an algorithm for computing

- the rank r

- a system of generators of $E(\mathbf{Q})$?

This is the main outstanding open question in the arithmetic theory of elliptic curves.

An example of Bremner and Cassels

The elliptic curve

$$E : y^2 = x^3 + 877x$$

has rank one and generator given by:

$$x = \frac{612776083187947368101^2}{78841535860683900210^2}$$

$$y = \frac{\begin{array}{r} 25625626798892680938877 \\ 68340455130896486691 \\ 53204356603464786949 \end{array}}{78841535860683900210^3}$$

The calculation of Mordell-Weil groups in specific instances is no small task!

Fermat's Descent

A candidate method: Fermat's descent.

Problem: It is not known to terminate.

The *complexity* of the descent method, for a given E, is measured by a certain group attached to E:

The *Shafarevich-Tate group* Ш_E.

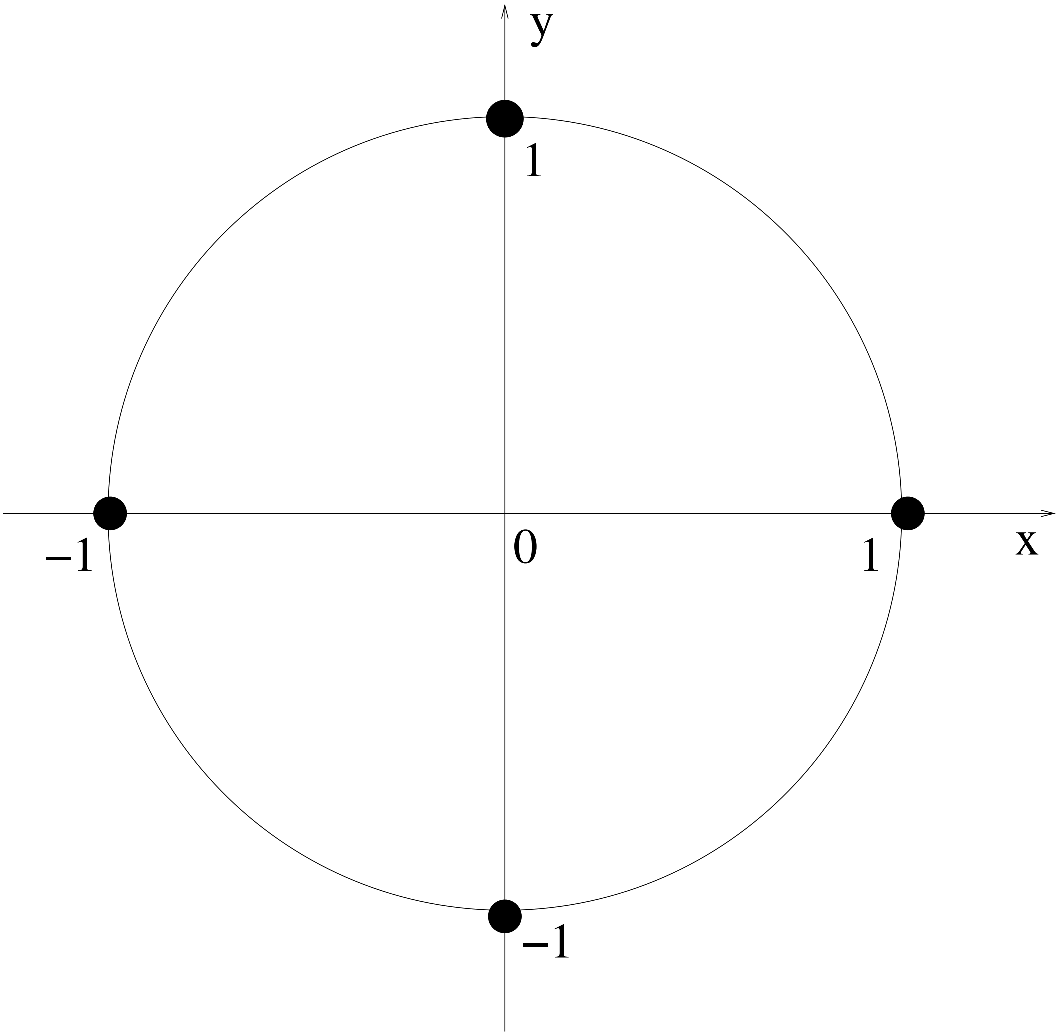
Shafarevich-Tate conjecture. Ш_E is finite.

This conjecture would imply that Fermat's descent procedure always eventually terminates, i.e., constitutes an algorithm.

Other than descent, the only approach to understanding rational points on elliptic curves is via the celebrated *Birch and Swinnerton-Dyer conjecture*.

A digression: the circle

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



has 4 integer solutions $(x, y) = (\pm 1, 0), (0, \pm 1)$.

We set $\boxed{N_{\mathbf{Z}} = 4}$.

Key principle: To understand a Diophantine equation like

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

it is useful to study

- the same equation over the *real numbers*;
- the corresponding congruence equation:

$$x^2 + y^2 \equiv 1 \pmod{p},$$

for all primes p.

Let

$$N_p = \#\{1 \leq x, y \leq p : x^2 + y^2 \equiv 1 \pmod{p}\}.$$

$$N_{\mathbf{R}} = 2\pi.$$

Evaluating N_p

Parametric solution

$$(x,y) = \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right).$$

So letting $t = 0, 1, \ldots, p-1, \infty$:

$$N_p = \begin{cases} p+1 & \text{if } -1 \text{ is not a square mod } p; \\ p-1 & \text{if } -1 \text{ is a square mod } p. \end{cases}$$

Quadratic reciprocity. If p is odd,

$$N_p = \begin{cases} p+1 & \text{if 4 divides } p+1; \\ p-1 & \text{if 4 divides } p-1. \end{cases}$$

A mysterious identity

Consider the expression $\prod_p \frac{N_p}{p}$.

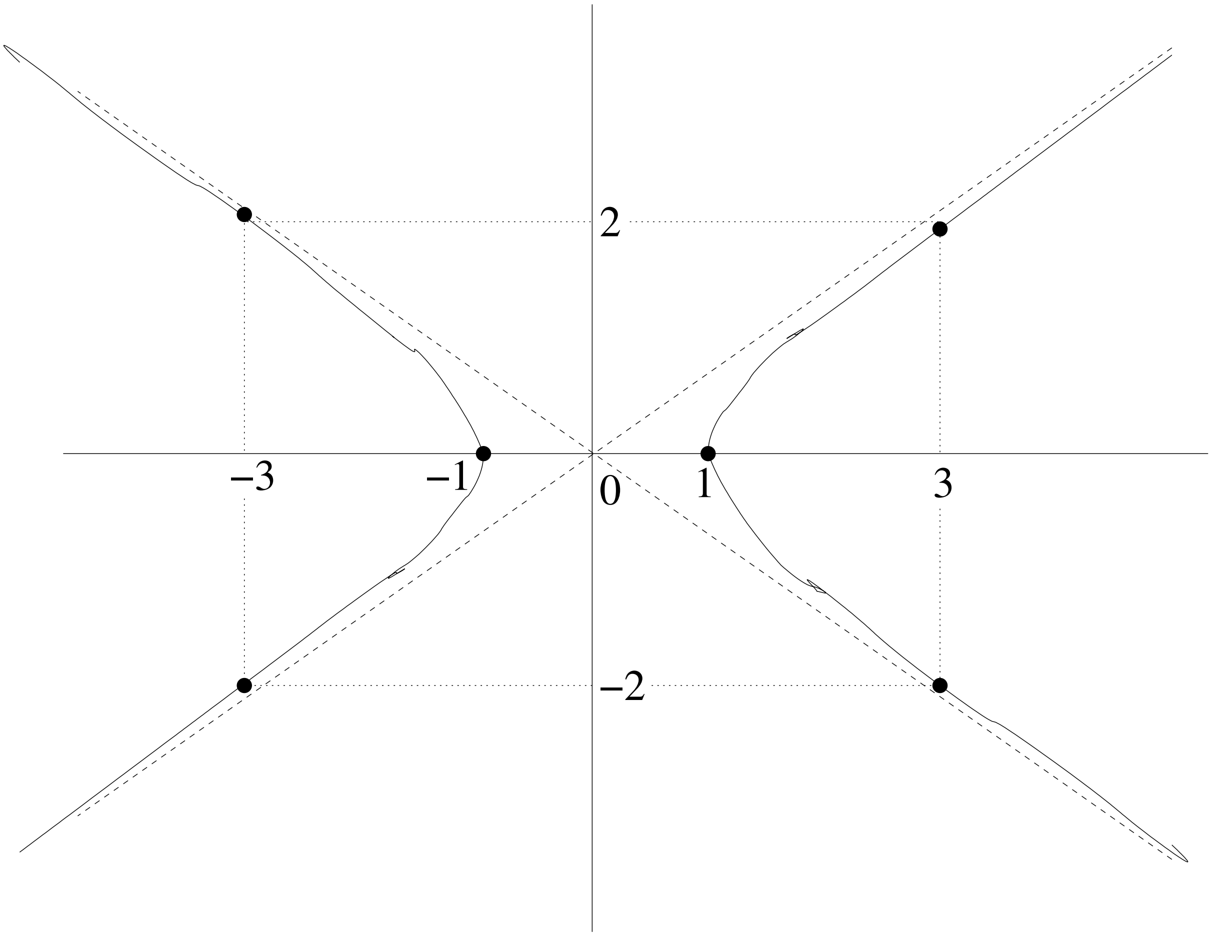
$$\begin{aligned}
\prod_p \frac{p}{N_p} &= \frac{1}{1+\frac{1}{3}} \times \frac{1}{1-\frac{1}{5}} \times \cdots \\
&= (1-\frac{1}{3}+\frac{1}{9}-\cdots) \times \\
&\quad (1+\frac{1}{5}+\frac{1}{25}+\cdots) \times \cdots \\
&= 1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{9}-\cdots \\
&= \frac{\pi}{4} \qquad \text{(Leibniz).}
\end{aligned}$$

This yields the mysterious identity:

$$\boxed{\prod_p \frac{N_p}{p} \cdot N_{\mathbf{R}} = 2N_{\mathbf{Z}}}$$

Another digression

The *Fermat-Pell equation* $x^2 - 2y^2 = 1$



has $N_{\mathbf{Z}}, N_{\mathbf{R}} = \infty$.

We set $\boxed{\dfrac{N_{\mathbf{R}}}{N_{\mathbf{Z}}} = \dfrac{\log(3+2\sqrt{2})}{2\sqrt{2}}}$.

Another mysterious identity

A direct (and elementary) evaluation yields

$$\boxed{\prod_p \frac{N_p}{p}\frac{N_{\mathbf{R}}}{N_{\mathbf{Z}}} = 1}$$

Note: This can be rewritten

$$\boxed{2\sqrt{2}\prod_p \frac{p}{N_p} = \log(3+2\sqrt{2}).}$$

In particular, evaluating the infinite product on the left allows us to *calculate numerically* a solution to the Pell equation!

Birch and Swinnerton-Dyer

To understand the equation

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

we consider as before

$$N_p := \#\{1 \le x, y \le p : y^2 \equiv x^3 + ax + b\}.$$

Idea (Birch and Swinnerton-Dyer).

The asymptotic behaviour of the N_p should reflect the rank r of $E(\mathbf{Q})$.

BSD Conjecture. (Rough form)

$$\prod_{p<X} \frac{N_p}{p} \approx C_E (\log X)^r.$$

Difficulty: This product is not easy to control.

L-functions

Let $a_p := p - N_p$.

Hasse's inequality: $|a_p| \leq 2\sqrt{p}$.

To E we associate the L-*function*

$$L(E, s) = \prod_p (1 - a_p p^{-s} + p^{1-2s})^{-1} =: \sum_n a_n n^{-s}.$$

This series converges for $Re(s) > \frac{3}{2}$.

Formally, $L(E, 1) = \prod_p \frac{p}{N_p}$.

BSD Conjecture: The L-function $L(E, s)$ extends to an analytic function of $s \in \mathbf{C}$, and

$$\operatorname{ord}_{s=1} L(E, s) = r.$$

Clay Institute Millenium Prize problem.

The BSD conjecture

More precise form:

$$L^{(r)}(E,1) = \#\text{Ш}_E \cdot R_E \# E(\mathbf{Q})_{\text{tor}}^{-2} \prod_v \Omega_v,$$

where

•$\text{Ш}_E =$ Shafarevich-Tate group of E;

•$R_E =$ regulator:

$$R_E = \det(\langle P_i, P_j \rangle)_{1 \leq i,j \leq r},$$

where $P_1, \ldots, P_r$ generates $E(\mathbf{Q})$ (modulo torsion), and $\langle\ ,\ \rangle$ is the *Néron-Tate canonical height*.

•$\Omega_v =$ "local term" attached to the place v.

Tate (1974) "... this remarkable conjecture relates the behaviour of a function L at a point where it is at present not known to be defined to the order of a group Ш which is not known to be finite."

Wiles' theorem

Theorem (Wiles, Taylor, Diamond, Conrad, Breuil) The function $L(E, s)$ has an analytic continuation to all of $\mathbf{C}$; in particular the value $L(E, s)$ makes sense near $s = 1$.

This theorem is a consequence, (thanks to work of Hecke) of a result which related the L-series $L(E, s)$ to modular forms.

More on this in the second lecture!

The Gross-Zagier-Kolyvagin theorem

Theorem (Gross-Zagier, Kolyvagin). If

$$\mathrm{ord}_{s=1} L(E,s) \leq 1,$$

then

$$\mathrm{ord}_{s=1} L(E,s) = r,$$

and Ш_E is finite. Furthermore there is an *efficient method* to compute $E(\mathbf{Q})$ in this case.

It is believed that the "bulk" of elliptic curves satisfy the hypothesis of the theorem. Hence for "most" elliptic curves over $\mathbf{Q}$, the BSD conjecture is known!

Yet alot of mystery still remains.

The congruent number problem

$$E_n : y^2 = x^3 - n^2x.$$

Tunnell's theorem: Suppose n is odd and square-free. Then $L(E_n, 1) = 0$ if and only if

$$\#\{x, y, z \in \mathbf{Z} : 2x^2 + y^2 + 8z^2 = n\} =$$

$$2 \times \#\{x, y, z : 2x^2 + y^2 + 32z^2 = n\}.$$

Corollary. If

$$\#\{x, y, z \in \mathbf{Z} : 2x^2 + y^2 + 8z^2 = n\} \neq$$

$$2 \times \#\{x, y, z : 2x^2 + y^2 + 32z^2 = n\},$$

then n is *not* a congruent number. Otherwise, *assuming the BSD conjecture*, n is a congruent number.

Difficulty. To show that $L(E,1)=0$ implies the existence of a rational point of infinite order in $E(\mathbf{Q})$.

Number theory disposes of a *very limited* arsenal of methods for producing solutions to Diophantine equations (as opposed to showing they do not exist.)

Understanding the mysterious process whereby the vanishing of an L-function $L(E,s)$ forces the presence of a rational point on $E(\mathbf{Q})$ would be a great step forward.