A crash course...
Day 3: Elliptic Curves

Sharon Anne Garthwaite

Bucknell University

March 2008

Let's start with some more questions about numbers...

- If $k \geq 6$ is an even number, can you write k as the sum of two prime numbers?
  Maybe. Goldbach's Conjecture
- If $k \geq 1$, can you express k as the sum of four squares?
  Yes! Lagrange (1770)
- Can you find an integer solution to $X^2 + Y^2 = 1234567890123$?
  No.
- If p is prime, can you find integer solutions to $X^2 + Y^2 = p$?
  No if $p \equiv 3 \pmod 4$. Yes otherwise.
- If can you find nontrivial integer solutions to $X^3 + Y^3 = Z^3$?
  No! Fermat's Last Theorem (Wiles)

Congruent number problem

For which integers n does there exist a right triangle with rational sides and area n?

i.e. Need three rational numbers X, Y, Z with

$$X^2 + Y^2 = Z^2, \qquad \frac{1}{2}XY = n.$$

These n are called congruent numbers

Equivalent Problem

Find $x \in \mathbb{Q}$ so that $x, x+n, x-n$ are all squares of rational numbers.

Bijection:

$$X, Y, Z \mapsto x = \left(\frac{Z}{2}\right)^2$$

$$x \mapsto X = \sqrt{x+n} - \sqrt{x-n}, \quad Y = \sqrt{x+n} + \sqrt{x-n}, \quad Z = 2\sqrt{x}.$$

Suppose we had such a triangle...

$$X, Y, Z \in \mathbb{Q}, \quad X^2 + Y^2 = Z^2, \quad \frac{1}{2}XY = n.$$

Check:

$$(X+Y)^2 = X^2 + 2XY + Y^2 = (X^2+Y^2) + 4\left(\frac{1}{2}XY\right) = Z^2 + 4n.$$

$$(X-Y)^2 = X^2 - 2XY + Y^2 = (X^2+Y^2) - 4\left(\frac{1}{2}XY\right) = Z^2 - 4n.$$

Multiply these together:

$$(X^2 - Y^2)^2 = Z^4 + 16n^2,$$

or

$$\left(\frac{X^2-Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 + n^2.$$

Suppose we had such a triangle. . .

$$X, Y, Z \in \mathbb{Q}, \quad X^2 + Y^2 = Z^2, \quad \frac{1}{2}XY = n.$$

$$\left(\frac{X^2 - Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 + n^2.$$

Multiply by $\left(\frac{Z}{2}\right)^2$:

$$\left(\left(\frac{X^2 - Y^2}{4}\right)\left(\frac{Z}{2}\right)\right)^2 = \left(\frac{Z}{2}\right)^6 + n^2\left(\frac{Z}{2}\right)^2.$$

Let $x = \left(\frac{Z}{2}\right)^2$, $y = \left(\frac{X^2-Y^2}{4}\right)\left(\frac{Z}{2}\right)$.
We have

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

Hence, given (X, Y, Z) we get a point on this curve (x, y).

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

If we have a point on the curve, do we have a triangle?
Yes, if:

1. x is the square of a rational number
2. If $x = \frac{p}{q}$ with $(p, q) = 1$ then $2 \mid q$.
3. If $x = \frac{p}{q}$ with $(p, q) = 1$ then $(q, n) = 1$.

We have reduced the problem to studying points on the curve

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

Definition (Elliptic Curve over $\mathbb{Q}$)

Any curve of the form

$$y^2 = f(x) = x^3 + ax + b, \quad a, b \in \mathbb{Q}$$

where $f(x)$ has three distinct (complex) roots.

More generally:

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Can make rational change of variables to get this in the other form.

Group Law

Addition of Points

- Identity: Point at ∞.
- Inverse of (x, y) is $(x, -y)$.
- Three points that lie on the same line sum to identity.

Group Law

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

If $P_1 + P_2 = P_3,\ P_i = (x_i, y_i)$, then

$$x_3 = \begin{cases} -x_1 - x_2 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2, & P_1 \neq P_2 \\ -2x_1 + \left(\frac{3x_1^2 - n^2}{2y_1}\right)^2 & P_1 = P_2 \end{cases}$$

$$y_3 = \begin{cases} -y_1 \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3), & P_1 \neq P_2 \\ -y_1 \left(\frac{3x_1^2 - n^2}{2y_1}\right)(x_1 - x_3), & P_1 \neq P_2 \end{cases}$$

When will a point have finite order?

Recall, (Normalized) Eisenstein series

For even $k \geq 4$,

$$E_k(z) := 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n,$$

where the rational (Bernoulli) numbers B_k are

$$\sum_{n=0}^{\infty} B_n \cdot \frac{t^n}{n!} = \frac{t}{e^t - 1} = 1 - \frac{1}{2}t + \frac{1}{12}t^2 + \cdots,$$

and

$$\sigma_{k-1}(n) = \sum_{1 \leq d | n} d^{k-1}.$$

Example:

- $E_4(z) := 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n$
- $E_6(z) := 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n$

Eisenstein series

$$E_k(z) := \frac{1}{2\zeta(k)} G_k(z)$$

where

$$\zeta(k) = \sum_{n \in \mathbb{N}} \frac{1}{n^k}.$$

and

$$G_k(z) := \sum_{\substack{(m,n) \in \mathbb{Z}^2 \\ (m,n) \neq (0,0)}} \frac{1}{(mz + n)^k}$$

This sum is absolutely convergent for $k > 2$.

Can think of this as a sum over a lattice.

Lattices

For fixed $z \in \mathbb{C} - \mathbb{R}$,

$$L := \{m + nz : m, n \in \mathbb{Z}\}$$

is the lattice generated by 1, z.

More generally:

$$L := \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\},$$

where $\omega_1, \omega_2 \in \mathbb{C}$ and $\omega_1/\omega_2 \notin \mathbb{R}$.

Sums over lattices

Extend the definition $G_k(z)$ to sums over lattices

$$L := \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\} :$$

$$G_k(L) := G(\omega_1, \omega_2) := \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(m\omega_1 + n\omega_2)^k}$$

For any $E : y^2 = x^3 + ax + b$, it is possible to find a lattice L so that

$$y^2 = x^3 - 60G_4(L)x - 140G_6(L)$$

describes the same elliptic curve.

Example

- $y^2 = x^3 - x$ is associated to lattice $L(1, i)$.
- $y^2 = x^3 - n^2 x$ is a multiple of this lattice.

Elliptic Curves and Lattices

There is a one-to-one correspondence between points in the fundamental parallelogram of L and

$$E : y^2 = x^3 - 60G_4(L)x - 140G_6(L)$$

given by "Weierstrass" map:

$$z \mapsto (2\wp(z), \sqrt{2}\wp'(z)) \qquad z \neq 0$$
$$0 \mapsto \infty$$

where

$$\wp(z) := \frac{1}{z^2} + \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \left(\frac{1}{(z-(m\omega_1+n\omega_2))^2} - \frac{1}{(m\omega_1+n\omega_2)^2} \right).$$

- Doubly-periodic map
- Gives $\mathbb{C}$ modulo the lattice and the curve compatible addition laws.

Consequence of this map

- It is easy to see points of finite order (torsion points) over $\mathbb{C}$:

$$a\omega_1/n + b\omega_2/n.$$

  Common Notation: $E[n]$ denotes points of order n.
- Much harder to see the torsion points over $\mathbb{Q}$.
- What about non-torsion points?

Recall,

- We saw
$$E(\mathbb{Q}) = \{(x,y) \in \mathbb{Q}^2 : (x,y) \text{ on } E\}$$
is an abelian group with an addition law.
- The group law is based on secant lines and tangent lines.
- The identity is the point at ∞.

Mordell's Theorem

In 1923 Mordell proved $E(\mathbb{Q})$ is finitely generated.
This means the abelian group has the form

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$$

for some r.

We call r the rank of the elliptic curve.

Rank

Rank is hard to determine!

Conjecture: There exist elliptic curves over $\mathbb{Q}$ of arbitrarily large rank.

Torsion

In 1972 Mazur proved that $E(\mathbb{Q})_{\mathrm{tors}}$ is one of 16 finite abelian groups:

- $\mathbb{Z}/n\mathbb{Z}$ for $n \leq 10$ or $n = 12$,
- $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2n\mathbb{Z})$ for $n \leq 4$.

How to win a million dollars doing math...

The Birch Swinnerton-Dyer Conjecture (BSD)
(Contact the Clay Mathematics Institute for details.)

Reduction of E modulo p

Given E defined over $\mathbb{Q}$, make a change of variables to give E integer coefficients.
For each prime p we can reduce E modulo p.

Example. $y^2 = x^3 - 11x^2 + 24x = x(x-3)(x-8)$.

- Modulo 3 $y^2 \equiv x^3 + x^2 \equiv x^2(x-1) \pmod 3$
- Modulo 5 $y^2 \equiv x^3 + 4x^2 + 4x \equiv x(x+2)^2 \pmod 5$
- Modulo 7 $y^2 \equiv x^2 - 4x^2 + 3x \equiv x(x-1)(x-3) \pmod 7$

We now only check points $\{(x,y) : 0 \leq x, y \leq p-1\} \cup \{\infty\}$.

We say E has good reduction modulo p if E is still an elliptic curve modulo p. i.e. We need E to have distinct roots modulo p.

Good reduction

We say E has good reduction modulo p if E is still an elliptic curve modulo p.
i.e. We need E to have distinct roots modulo p.

Can check this with the discriminant of the elliptic curve.
For

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

define

$$\Delta(E) := -16(27b^2 + 4a^3)$$

p is a prime of good reduction if and only if $p \nmid \Delta(E)$.

- Not quite an invariant, but close (minimal discriminant).
- Contains the same reduction information as the conductor, which is harder to define.

If p is a prime of good reduction, define

$$a(p) := p + 1 - \text{ number of points on } E \pmod{p}$$

Example: Compute $a(p)$, $p = 3, 5, 7$ for $E : y^2 = x^3 - x$
Theorem (Hasse): $|a_p| \leq 2\sqrt{p}$ for good p.

Define the L -function of E by:

$$L(E, s) := \prod_{p \text{ good}} \frac{1}{1 - a(p)p^{-s} + p^{1-2s}} \prod_{p \text{ bad}} \frac{1}{1 - a(p)p^{-s}}.$$

- The $a(p)$ for p bad are in $\{-1, 0, 1\}$.

Can write this as a "Dirichlet series"

$$L(E, s) = \sum_{n \geq 1} \frac{a_E(n)}{n^s}.$$

BSD

$$L(E,s) := \prod_{p\text{good}} \frac{1}{1-a(p)p^{-s}+p^{1-2s}} \prod_{p\text{bad}} \frac{1}{1-a(p)p^{-s}}.$$

(Simplified) BSD Conjecture: The Taylor expansion of $L(E,s)$ at $s=1$ has form

$$L(E,s) = c(s-1)^r + \text{ high order terms}$$

for some $c \neq 0$ where $r = \text{rank}(E(\mathbb{Q}))$.

The c is conjectured in terms of invariants of the curve, including one that is not known to be finite.

Connection to Congruent Numbers

For which integers n does there exist a right triangle with rational sides and area n?
Reduced to finding points on

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

If we have a point on the curve, do we have a triangle?
Yes, if:

1. x is the square of a rational number
2. If $x = \frac{p}{q}$ with $(p, q) = 1$ then $2 \mid q$.
3. If $x = \frac{p}{q}$ with $(p, q) = 1$ then $(q, n) = 1$.

Torsion points are $\{(0,0), (\pm n, 0), \infty\}$
n is congruent if and only if $r(E) \geq 1$.
Example. $n = 1$. $L(E, 1) \approx 0.655514388573 \cdots \neq 0$

Problems

1. Prove that 5 is a congruent number by finding a triangle with rational sides and area 5. Use this to find 3 non-trivial points on $y^2 = x^3 - 25x$.
2. Let $\sum b(n)q^n = \eta^2(4z)\eta^2(8z)$. Let E be the elliptic curve $y^2 = x^3 - x$. Find $a(p)$ for many primes p.
   2.1 Do you notice a pattern?
   2.2 Compare to $b(p)$. Do you notice a pattern?
3. Prove BSD.