Expository presentation on congruent numbers

Jack Yoshikawa

July 2026

Congruent numbers

- We will call a number *congruent* if it is the area of a right triangle with rational sides.

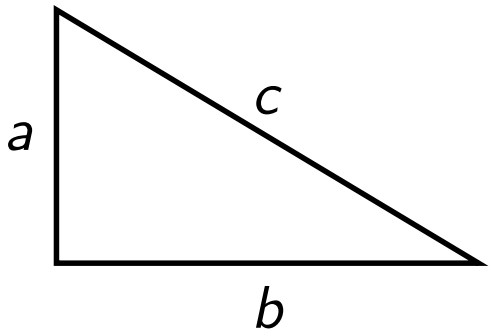
Congruent numbers

- We will call a number *congruent* if it is the area of a right triangle with rational sides.
- For example, 6 is a congruent number because it is the area of the right triangle with sides $3, 4, 5$.

Congruent numbers

- This is a very difficult problem with a very long history, investigated by people like Fermat.

A concrete (and enormous) example



$$a = \frac{6803298487826435051217540}{411340519227716149383203}$$

$$b = \frac{411340519227716149383203}{21666555693714761309610}$$

$$c = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}$$

Figure: A rational right triangle with area 157, numbers taken from Koblitz, computed by Don Zagier.

Congruent numbers

- One may wonder how to know if a number is congruent. In this talk we will sketch a proof of a criterion due to Tunnell that gives a conjecturally complete characterization of numbers of this form.

Theorem (Tunnell's Theorem)

A square free number n is congruent if and only if (Conditional on BSD)

$$S_n(2,1,8) = 2S_n(2,1,32) \quad \text{if } n \text{ is odd}$$
$$S_n(8,2,16) = 2S_n(8,2,64) \quad \text{if } n \text{ is even}$$

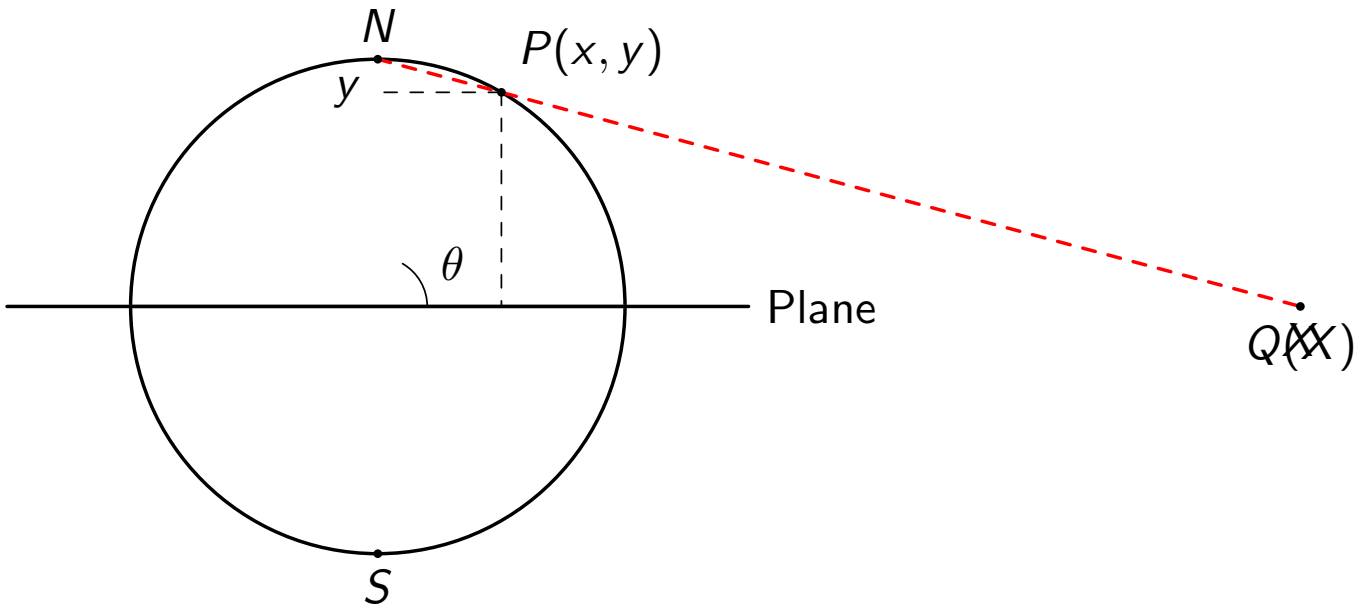
in this case $S_n(a,b,c) = \#\{x,y,z \in \mathbb{Z} : ax^2 + by^2 + cz^2 = n\}$

-

How to prove this and why is this hard

- We rewrite the equation into the form

$$a^2 + b^2 = c^2, \quad \frac{ab}{2} = n$$



- After many manipulations we get that there is a one to one correspondence between solutions to this elliptic curve

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

and congruent numbers given that $y \neq 0$.

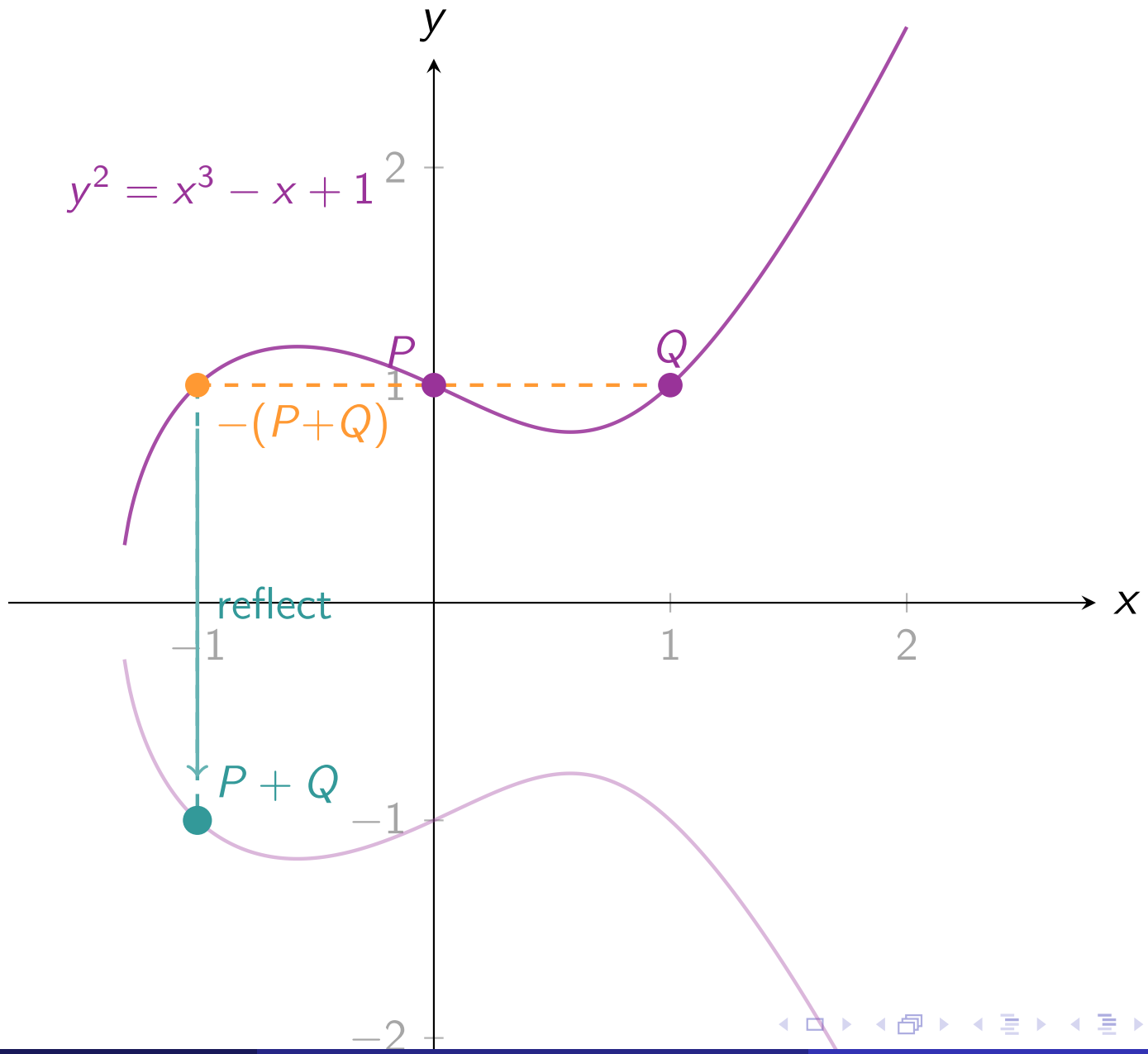
What is an elliptic curve?

- An elliptic curve is a curve of the form $f(x) = y^2$ with $f(x)$ a polynomial of the form $x^3 + ax + b$ (with some smoothness constraints)(but those do not matter)

The group law on an elliptic curve

- Given a pair of points $(x_1, y_1), (x_2, y_2)$ on the elliptic curve, the line between them (with slope λ) meets the curve at exactly one more point (x_3, y_3), whose x-coordinate satisfies $x_1 + x_2 + x_3 = \lambda^2$ by Vieta's formula. (If $(x_1, y_1) = (x_2, y_2)$, we use the tangent line at that point instead, with λ its slope.)
- Reflecting this third point across the x-axis, i.e. taking $(x_3, -y_3)$, defines the sum of the two points; this addition law makes the set of points on the elliptic curve an abelian group, with the identity given by a single "point at infinity," denoted ∞, which we use whenever the line through the two points is vertical and so never meets the curve again.

A worked example



The group of points: rank and torsion

- On the previous slides, we saw that the set of points on a curve forms an abelian group. Some points P satisfy $nP = \infty$ (the identity) for some n, while others never do.
- Every abelian group of this type has the form $\mathbb{Z}^r \times T$; we call r the rank, and T a finite abelian group called the torsion subgroup.
- For E_n *all* torsion points, are equal to $\infty, (n, 0), (-n, 0), (0, 0)$

Why is this easier?

- Instead of finding all rational points on E_n, we can count its points modulo a prime p. Write $a_p = p + 1 - \#E_n(\mathbb{F}_p)$. These numbers are the coefficients of an L-function:

$$L(E_n, s) = \prod_{p \nmid 4n} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

- Counting points modulo p is far easier than finding all rational points on E_n directly.

An example: counting points mod 7

- We will now compute, a_7 for E_6 we know that there are 7 points, so $a_7 = 0$ this is in fact true for all primes equal to 3 mod 4.

From L-functions to modular forms

- Written as a series in n^{-s}, the coefficients of $L(E_n, s)$ turn out to be "modular": if

$$L(E_n, s) = \sum_{m=1}^{\infty} \frac{c_{m,n}}{m^s},$$

the function

$$F_n(z) = \sum_{m=1}^{\infty} c_{m,n} q^m$$

with $q = e^{2\pi i z}$ is a "modular form" of weight two, meaning it satisfies some nice properties with respect to some subgroup of the set of transformations, $\frac{az+b}{cz+d}$. Namely $F(\frac{az+b}{cz+d}) = \chi(d)(cz+d)^2 F(z)$. and this gives $L(E_n, s)$ an analytic continuation to the whole complex plane. Via taking the Mellin transform.

- Conjecturally (Birch–Swinnerton-Dyer), E_n has a rational point of infinite order exactly when $L(E_n, 1) = 0$; if $L(E_n, 1) \neq 0$, it does not. No one currently knows how to prove this in general.

How this all ties together

- It turns out that $L(E_n, 1)$ is, up to a nonzero factor, equal to the nth coefficient of a certain modular form squared built from Tunnell's quadratic forms, namely

$$S_n(2, 1, 32) - \frac{1}{2} S_n(2, 1, 8)$$

(with the analogous expression for even n). The proof is more delicate for even versus odd n, which is why Tunnell's criterion bifurcates. The key point is: this coefficient vanishes exactly when $L(E_n, 1) = 0$, which (conjecturally) happens exactly when E_n has a nontrivial rational point, which happens exactly when n is congruent.

Shimura's and Waldspurger's theorems

- To make the previous slide precise we need two deep theorems relating *half-integral* weight modular forms (like our theta series) to *integral* weight ones (like the form attached to E_n).

Theorem (Shimura)

Let $f = \sum a_n q^n$ be an eigenform of half-integral weight $k/2$ with "Hecke eigenvalues" $T_{p^2} f = \lambda_p f$. Then the Shimura lift $F = \sum b_n q^n$, defined by

$$\sum_{n=1}^{\infty} \frac{b_n}{n^s} = \prod_p \frac{1}{1 - \lambda_p p^{-s} + \chi(p)^2 p^{k-2-2s}},$$

is a modular form of integral weight $k-1$ and character χ^2.

- So an eigenform of weight $3/2$ lifts to an eigenform of weight 2 exactly the weight of the modular form attached to E_n.

Theorem (Waldspurger)

If f is a half-integral weight eigenform with Shimura lift F, then its Fourier coefficients $a(t)$ at squarefree t satisfy

$$a(t)^2 = c_t \cdot L(F, 1) \cdot \sqrt{t}$$

for an explicit nonzero constant c_t depending only on t mod 8. In particular, $a(t) = 0 \iff L(F, 1) = 0$.

Completing the proof of Tunnell's theorem

- Let $\Theta(z) = \sum_{m \in \mathbb{Z}} q^{m^2}$, a weight $1/2$ theta series. For n odd, consider the weight $3/2$ form

$$f(z) = \Theta(z)\Theta(2z)\Theta(32z) - \tfrac{1}{2}\,\Theta(z)\Theta(2z)\Theta(8z).$$

- Its nth Fourier coefficient counts representations by Tunnell's quadratic forms:

$$a(n) = S_n(2,1,32) - \tfrac{1}{2} S_n(2,1,8),$$

  which vanishes exactly when $S_n(2,1,8) = 2S_n(2,1,32)$, i.e. exactly when Tunnell's condition holds.
- By Shimura's theorem, f lifts to (a multiple of) the weight 2 form F_n attached to E_n, so $L(F,1) = L(E_n,1)$.
- By Waldspurger's theorem, $a(n) = 0 \iff L(E_n,1) = 0$.
- Assuming BSD, $L(E_n,1) = 0 \iff E_n$ has a rational point of infinite order $\iff n$ is congruent. Chaining these equivalences together (with the even case handled analogously) gives exactly Tunnell's theorem.