Who Wants to Be a Millionaire? (The Hard Way)

Philippe Michaud-Rodgers

Warwick Maths Society Talks Series

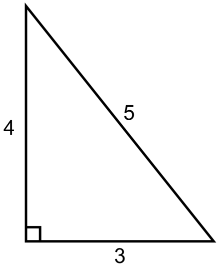
01.12.2020

Table of Contents

Table of Contents

Congruent Numbers

- $n \in \mathbb{N}$ is a **congruent number** if $n =$ Area $(\Delta_{a,b,c})$, for some right-angled triangle with side lengths $a, b, c \in \mathbb{Q}$.
- **Long** history: Diophantus (3rd century), 10th century Arab mathematicians, Fermat, Euler, + many more!
- Example: Set $a = 3, b = 4, c = 5$.



- Area $= \frac{3 \cdot 4}{2} = 6$.
- So 6 is a congruent number.
- Is 3 a congruent number?
- If not, why not?

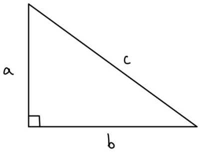
The Million Dollar Question

Get Rich Quick

Given $n \in \mathbb{N}$, is n congruent? Give a way of testing this.

If the Birch and Swinnerton-Dyer (**BSD**) conjecture holds, then we can do this!
Prize $=$ 1 million dollars (Clay Institute Millenium Prize Problem).
You will win 0.9 million dollars after I take my 10% commission (**PS** please don't be a Perelman).

First Observations



- $n = \frac{ab}{2}$ and $a^2 + b^2 = c^2$ with $a, b, c \in \mathbb{Q}$.

Then

$$\left(\frac{a+b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 + n \text{ and } \left(\frac{a-b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 - n.$$

Set

$$x := \left(\frac{c}{2}\right)^2,$$

so that $x - n, x, x + n$ are all (rational) squares.
So

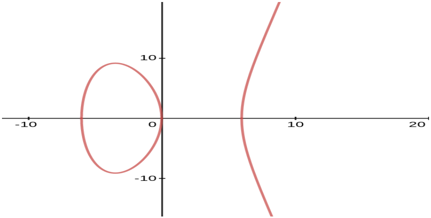
$$(x-n)(x)(x+n) = y^2 \qquad \text{for some } y \in \mathbb{Q}.$$

First Observations (Continued)

We have
$(x-n)x(x+n) = y^2$ for some $y \in \mathbb{Q}$ and $x = (c/2)^2 \in \mathbb{Q}$.
So $P = (x, y)$ is a **rational point** on the curve

$$E_n : Y^2 = X(X+n)(X-n).$$

We write $P \in E_n(\mathbb{Q})$.
Example: E_6



Even More First Observations

We have $P = (x, y) \in E_n(\mathbb{Q}) : Y^2 = X(X+n)(X-n)$.
Claim: $y \neq 0$.
If $y = 0$ then $(c/2)^2 = x = 0, n,$ or $, -n$.

- $(c/2)^2 = 0 \Rightarrow c = 0 \quad ↯$
- $(c/2)^2 = n \Rightarrow a = b \Rightarrow c^2 = 2a^2 \quad ↯$
- $(c/2)^2 = -n \quad ↯$

So $y \neq 0$, proving the claim.
Summary: if n is congruent, then $\exists P = (x, y) \in E_n(\mathbb{Q})$ with $y \neq 0$.

From Curves to Congruent Numbers

Summary: if n is congruent, then $\exists P = (x, y) \in E_n(\mathbb{Q})$ with $y \neq 0$.
What about the converse?
Let $P = (x_1, y_1) \in E_n(\mathbb{Q})$ with $y_1 \neq 0$.
Can assume $y_1 > 0$ by flipping sign if necessary.
Set

$$a = \frac{x_1^2 - n^2}{y_1}, \qquad b = \frac{2nx_1}{y_1}, \qquad c = \frac{x_1^2 + n^2}{y_1}.$$

- $a, b, c \in \mathbb{Q}$.
- $a^2 + b^2 = c^2$.
- $n = ab/2$.
- $ab = 2n > 0$, so $a, b > 0$ by flipping signs if necessary. $c > 0$ too.
- So n is a congruent number!

A new problem

Main Theorem V1

$n \in \mathbb{N}$ is a congruent number if and only if $\exists P = (x, y) \in E_n(\mathbb{Q})$ with $y \neq 0$.

So we want to understand $E_n(\mathbb{Q})$.
Isn't this a harder question?
Kind of! But, E_n is a special type of curve...

Table of Contents

What is an Elliptic Curve?

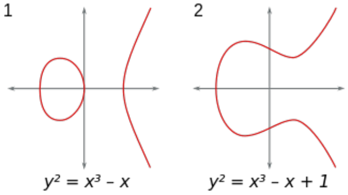
Definition

An elliptic curve (over $\mathbb{Q}$) is a smooth curve given by an equation

$$Y^2 = X^3 + AX + B,$$

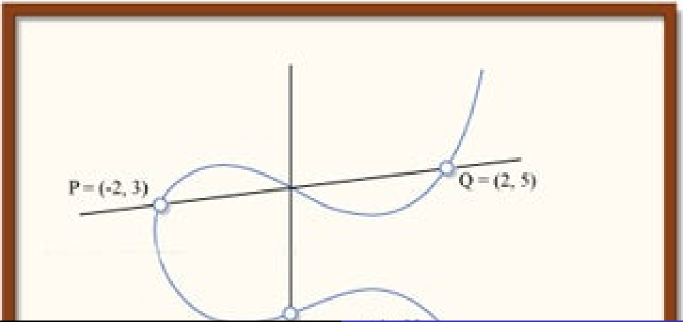
where $A, B \in \mathbb{Q}$.

For E_n we have $A = -n^2$ and $B = 0$.



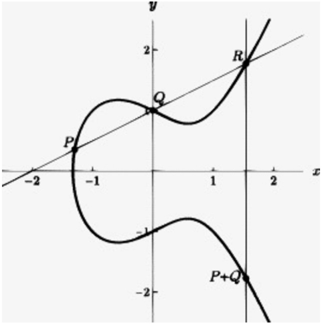
Rational Points

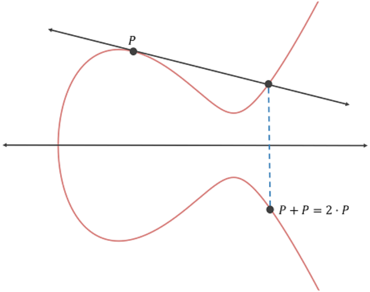
- $E : Y^2 = X^3 + Ax + B$.
- A point $P = (x, y)$ is a *rational point* on E if P lies on E, and $x, y \in \mathbb{Q}$.
- We write $E(\mathbb{Q})$ for the set of rational points.
- Example: $Y^2 = X^3 + 17, \quad (2, 5) \in E(\mathbb{Q})$



$E(\mathbb{Q})$ is a group!

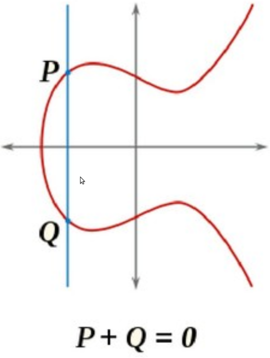
- Let $P, Q \in E(\mathbb{Q})$. Then $P \oplus Q \in E(\mathbb{Q})$. What is $P \oplus Q$?

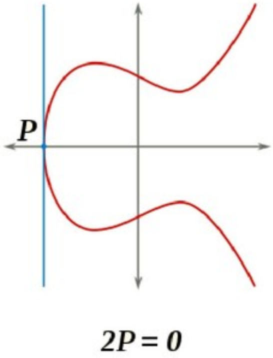




Group Law Continued

What is the identity in the group? It is 0 (or ∞):





Group Structure

- $E(\mathbb{Q})$ is an *abelian* group (clear).
- **Mordell-Weil Theorem:** $E(\mathbb{Q})$ is a *finitely generated* abelian group.
- So $E(\mathbb{Q}) = E(\mathbb{Q})_{\mathrm{tors}} \oplus \mathbb{Z}^r$, $r = \mathrm{rank}(E)$.
- Here, $E(\mathbb{Q})_{\mathrm{tors}} = \{P \in E(\mathbb{Q}) : mP = 0 \text{ for some } m \geq 1\}$.
- If $r = 0$, then $E(\mathbb{Q}) = E(\mathbb{Q})_{\mathrm{tors}}$.
- Let $P = (x, y) \in E(\mathbb{Q})$. Then $|P| = 2 \Leftrightarrow y = 0$.

Table of Contents

Main Theorem V2

Recall:
Main Theorem V1: $n \in \mathbb{N}$ is a congruent number if and only if $\exists P = (x, y) \in E_n(\mathbb{Q})$ with $y \neq 0$.

Since $|P| = 2 \Leftrightarrow y = 0$:

Main Theorem V2

$n \in \mathbb{N}$ is a congruent number if and only if $\exists P \in E_n(\mathbb{Q}) \backslash \{\infty\}$ with $|P| \neq 2$.

Main Theorem V3

Torsion Proposition

$\#E_n(\mathbb{Q})_{\mathrm{tors}} = 4$. So $E_n(\mathbb{Q})_{\mathrm{tors}} = \{\infty, (0,0), (n,0), (-n,0)\}$.

Main Theorem V2: $n \in \mathbb{N}$ is a congruent number if and only if $\exists P \in E_n(\mathbb{Q})\backslash\{\infty\}$ with $|P| \neq 2$.

Main Theorem V3

$n \in \mathbb{N}$ is a congruent number if and only if $\mathrm{rank}(E_n) > 0$.

Proof: Let $n \in \mathbb{N}$ be congruent. By V2, $\exists P \in E_n(\mathbb{Q})\backslash\{\infty\}$ with $|P| \neq 2$. By Proposition, $P \notin E_n(\mathbb{Q})_{\mathrm{tors}}$, so $r > 0$.
Conversely, if $r > 0$, then $\exists P \in E_n(\mathbb{Q})\backslash\{\infty\}$ with $|P| \neq 2$. So n is congruent by V2. $\square$

Table of Contents

Lutz-Nagell and Reduction

Torsion Proposition: $\#E_n(\mathbb{Q})_{\mathrm{tors}} = 4$.

We work now with $E : Y^2 = X^3 + Ax + B, \quad A, B \in \mathbb{Z}$.

Lutz-Nagell

If $Q = (x, y) \in E(\mathbb{Q})_{\mathrm{tors}}$, then $x, y \in \mathbb{Z}$.

Reduction Theorem

fabfm primes p, $\overline{E}$ is an elliptic curve over $\mathbb{F}_p$, and

$$\begin{aligned} r_p : E(\mathbb{Q})_{\mathrm{tors}} &\longrightarrow \overline{E}(\mathbb{F}_p) \\ (x, y) &\longmapsto (\overline{x}, \overline{y}) \end{aligned}$$

is an injective group homomorphism.

More On Reduction

Reduction Theorem: fabfm p, $\overline{E}$ is an elliptic curve over $\mathbb{F}_p$ and $r_p : E(\mathbb{Q})_{\text{tors}} \to \overline{E}(\mathbb{F}_p)$ is an injective group homomorphism.

- $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ = finite field with p elements.
- $\overline{E}$ means the same equation, but $A, B \in \mathbb{Z}$ are reduced mod p.
- $\overline{E}$ is an elliptic curve over $\mathbb{F}_p$ means that it is 'smooth'.
- $\overline{E}(\mathbb{F}_p)$ is the set of points (x, y), with $x, y \in \mathbb{F}_p$ satisfying the equation of $\overline{E}$, and $\overline{\infty}$. This set is finite.

Consequence: $\#E(\mathbb{Q})_{\text{tors}} \mid \#\overline{E}(\mathbb{F}_p)$ fabfm p.

Example: $E_7 : Y^2 = X(X^2 - 49)$. Let $p = 5$. Then

$$\overline{E_7} : Y^2 = X(X^2 + \overline{1}),$$

and $r_5(7, 0) = (\overline{2}, \overline{0}) \in \overline{E_7}(\mathbb{F}_5)$.

Torsion Proof: Step 1 of 3

Torsion Proposition: $\#E_n(\mathbb{Q})_{\text{tors}} = 4$.
Suppose $\#E_n(\mathbb{Q})_{\text{tors}} > 4$. Then

- Either $\exists P \neq \infty$ of **odd** order m;
- Or every $P \neq \infty$ has even order.

So $\#E_n(\mathbb{Q})_{\text{tors}}$ has a subgroup S of size m, with m odd or $m = 8$.

Then $m = \#S \mid \#E_n(\mathbb{Q})_{\text{tors}} \mid \#\overline{E_n}(\mathbb{F}_p)$ fabfm p.

So $m \mid \#\overline{E_n}(\mathbb{F}_p)$ fabfm p.

Torsion Proof: Step 2 of 3

By Step 1: $m \mid \#\overline{E_n}(\mathbb{F}_p)$ fabfm p, where m is odd, or $m = 8$.

Claim: $\#\overline{E_n}(\mathbb{F}_p) = p + 1$ fabfm $p \equiv 3 \pmod 4$.

Proof of Claim: $\overline{E_n} : Y^2 = X(X^2 - \overline{n}^2)$.
We have 4 disctinct points: $\infty, (\overline{0}, \overline{0}), (\overline{n}, \overline{0}), (-\overline{n}, \overline{0})$.

Then for each set $\{-x, x\}$ with $x \in \mathbb{F}_p \backslash \{\overline{0}, \overline{n}, -\overline{n}\}$, we have two points (i.e. two values of y) because $X(X^2 - \overline{n}^2)$ is an odd function and $p \equiv 3 \pmod 4$ (so precisely one of $x(x^2 - \overline{n}^2)$ and $-x(x^2 - \overline{n}^2)$ gives rise to a non-zero square).

So $\#\overline{E_n}(\mathbb{F}_p) = 4 + 2(\frac{p-3}{2}) = p + 1$. Proving the claim

Torsion Proof: Step 3 of 3

We have: $m \mid p+1$ fabfm $p \equiv 3 \pmod 4$, with $m = 8$ or m odd.
Equivalently: $p \equiv -1 \pmod m$ fabfm $p \equiv 3 \pmod 4$, with $m = 8$ or m odd.

- $m = 8$: only finitely many $p \equiv 3 \pmod 8$.
- $3 \nmid m$: only finitely many $p \equiv 3 \pmod{4m}$.
- $3 \mid m$: only finitely many $p \equiv 7 \pmod{12}$.

In all 3 cases, we contradict **Dirichlet's Theorem on Primes in Arithmetic Progressions:** there are infinitely primes $p \equiv a \pmod b$ if $\gcd(a, b) = 1$.
So we have proven the torsion proposition: $\#E_n(\mathbb{Q})_{\text{tors}} = 4$. $\square$

Table of Contents

L-series of an elliptic curve

Main Theorem V3

$n \in \mathbb{N}$ is a congruent number if and only if $\mathrm{rank}(E_n) > 0$.

How to test if $\mathrm{rank}(E_n) > 0$? We can do this for 'small' n already. But we don't know how to for large n, **unless** we assume the *BSD Conjecture*.

L-series of an elliptic curve

Let E be an elliptic curve over $\mathbb{Q}$. Then

$$L(E, s) := \prod_{p \nmid 2\Delta_E} \frac{1}{1 - a_p p^{-s} + p^{1-2s}},$$

for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 3/2$, where $a_p := p + 1 - \#\overline{E}(\mathbb{F}_p)$ and $\Delta_E := -16(4A^3 + 27B^2)$.

Statement of the BSD Conjecture

Fact: $L(E,s)$ is defined for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 3/2$, **but** can be *analytically extended* to the whole of $\mathbb{C}$.

Conjecture (Birch and Swinnerton-Dyer)

The Taylor expansion of $L(E,s)$ at $s = 1$ has the form

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

with $c \neq 0$ a constant, and $r = \mathrm{rank}(E)$.

So: $\mathrm{rank}(E) > 0 \Leftrightarrow L(E,1) = 0$.

So $n \in \mathbb{N}$ is congruent $\Leftrightarrow \mathrm{rank}(E_n) > 0 \Leftrightarrow L(E_n,1) = 0$, and this is something we can test!

Summary

$n \in \mathbb{N}$ is a congruent number.

$\Updownarrow$

$\exists P = (x, y) \in E_n(\mathbb{Q})$ with $y \neq 0$. (V1)

$\Updownarrow$

$\exists P \in E_n(\mathbb{Q}) \backslash \{\infty\}$ with $|P| \neq 2$. (V2)

$\Updownarrow$

$\mathrm{rank}(E_n) > 0$. (V3)

$\Updownarrow$

$L(E_n, 1) = 0$. (BSD)

Thank you for listening! :)