Congruent Numbers and Elliptic Curves

Talk

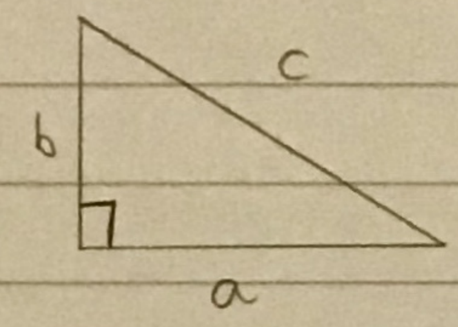
[Introduce + Thank]

(· History : · Ancient Greeks (Pythagoras, Euclid, Diophantus, etc.)

· Arab mathematicians ~ 10th century

· Fermat, Euler, and others)

· $n \in \mathbb{N}_{>0}$ is a congruent number if $n = \text{area}(\triangle abc)$, $a, b, c \in \mathbb{Q}$.



e.g. $a=3, b=4, c=5$ shows 6 is a congruent number.

But 3 is not.

$$\begin{cases} a^2 + b^2 = c^2 \\ n = ab/2 \end{cases}$$

So $\quad (a+b/2)^2 = (c/2)^2 + n$

$\quad\quad (a-b/2)^2 = (c/2)^2 - n.$

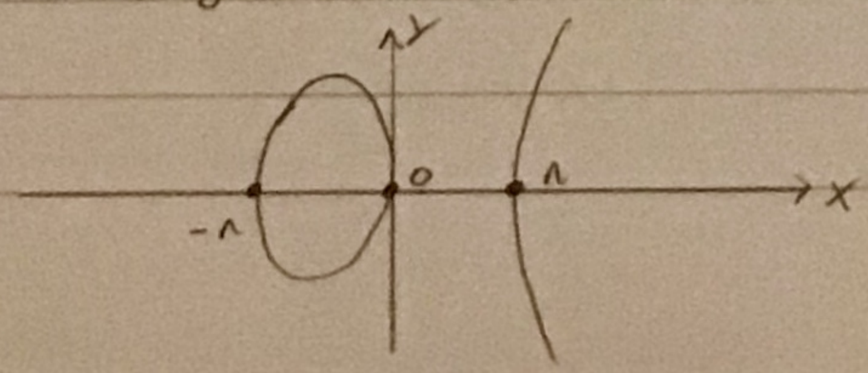
Set $x = (c/2)^2$

(Then $x-n$, x, $x+n$ are all squares, so)

$$(x-n)\,x\,(x+n) = y^2, \quad y \in \mathbb{Q}$$

So $y^2 = x(x^2 - n^2)$

So $(x, y) \in E_n$: $Y^2 = X(X^2 - n^2)$



Moreover $(x,y) \in E_n(\mathbb{Q})$ (a rational point)

(For the moment, E_n is just a curve).

Also $y \neq 0$:

o/w $x = 0$, n, or $-n$

$x=0$ ↯ ; $x = n$; but $x = (\frac{c}{2})^2 \geq 0$ ↯

$c = 0$ ↯ ; $c = 2\sqrt{n}$,

So $a^2+b^2 = 4n = 2ab$

$\Rightarrow a = b \Rightarrow 2a^2 = c^2$ ↯

(clear denom. and consider prime factorisations)

(So n a congruent number tells us that we have $(x,y) \in E_n(\mathbb{Q})$ with $y \neq 0$)

Converse? Suppose $(x_1, y_1) \in E_n(\mathbb{Q})$, $y_1 \neq 0$.

(Can assume $y_1 > 0$ (by flipping sign if necessary))

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

Then $a, b, c \in \mathbb{Q}$, $a^2+b^2 = c^2$, $n = ab/2$.

$c > 0$.

Since $ab = 2n$, if $a, b < 0$ flip signs.

Conclusion :

n congruent $\Leftrightarrow \exists (x,y) \in E_n(\mathbb{Q})$, $y \neq 0$.

(Two Qu's : • Where do the formulae for a, b, c come from? • How we simplified the problem?

Answers : Elliptic Curves and Yes)

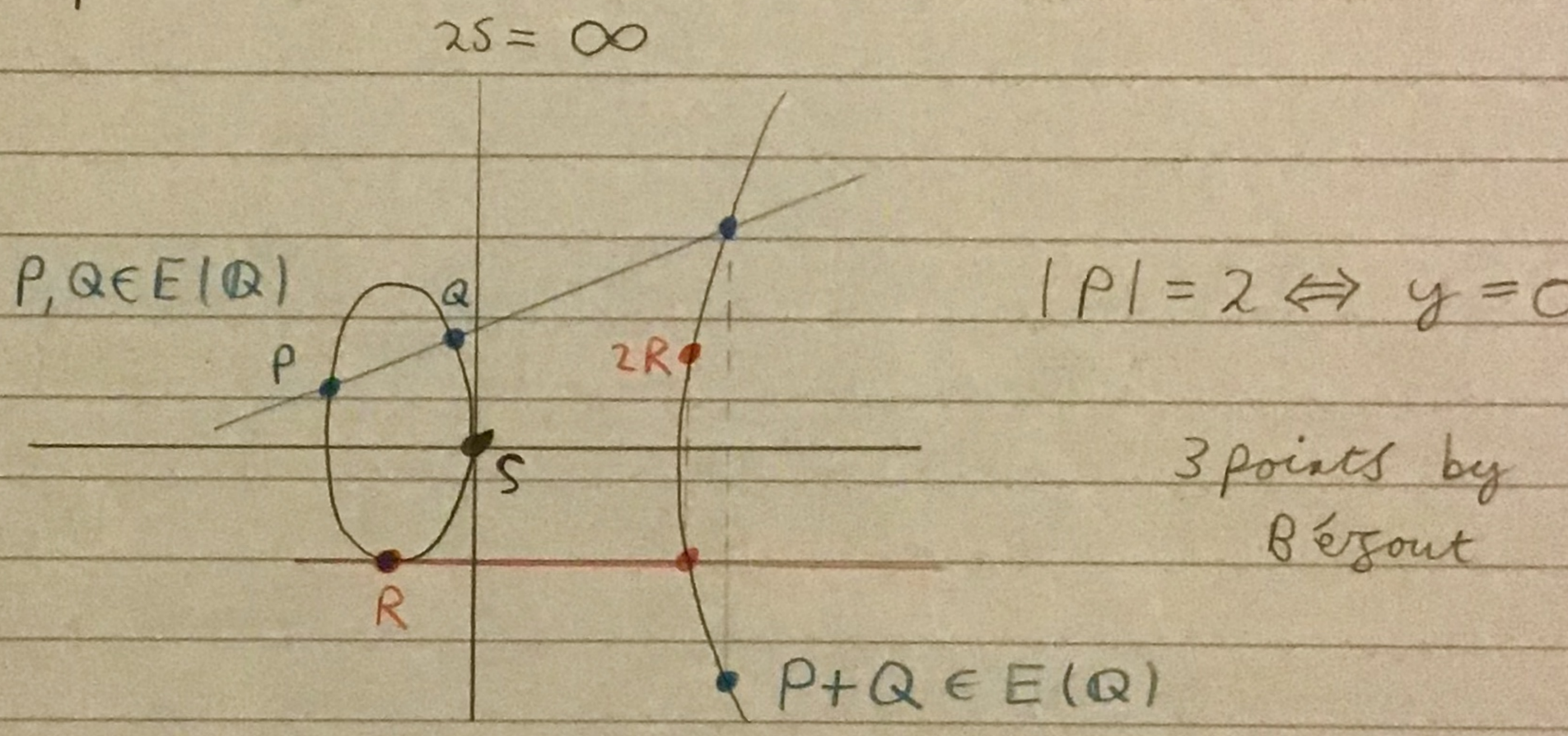
• Elliptic curve (over $\mathbb{Q}$) is a smooth plane cubic of the form $Y^2 = X^3 + AX + B$, $A, B \in \mathbb{Q}$

($A = -\lambda^2$, $B = 0$ for us)

(Interested in $E(\mathbb{Q})$, the rational points)

Fact: $E(\mathbb{Q})$ is a finitely generated abelian group (Mordell-Weil).

Group Law:



$\infty = O =$ additive identity.

$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$, $r = rank(E)$.

(Now we answer how a, b, c formulae arise)

$P = (x_1, y_1) \in E_\lambda(\mathbb{Q})$, $y_1 \neq 0$.

Natural Guess: $c = 2\underbrace{\sqrt{x}}$ but likely $\notin \mathbb{Q}$.

(Rather than use the x-coordinate of P, use the x-coordinate of $P+P = 2P$.
Note $2P \neq \infty$ because $y_1 \neq 0$)

Calculate: $x_2 = \left(\frac{x_1^2 + n^2}{2y_1}\right)^2$ ($y_2 \neq 0$, see why later)

Then set $c = 2\sqrt{x_2}$

Check $x_2 - n$ and $x_2 + n$ are also squares, allows us to get a, b.

---

n congruent $\Leftrightarrow \exists P \in E_n(\mathbb{Q}) \setminus \{\infty\}$ with $|P| \neq 2$.

(Already a good start, can carry out 2-descent relatively easily on E_n to explicitly calculate $E_n(\mathbb{Q})$,
but we can go further!)

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

‖Consequence: n congruent $\Leftrightarrow$ rank$(E_n) \neq 0$‖

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

- Reduction Theorem: r_p (prime): $E(\mathbb{Q})_{tors} \to \bar{E}(\mathbb{F}_p)$ is an injective group homomorphism.
$r_p: (x,y) \mapsto (x \bmod p, y \bmod p)$
$\bar{E}(\mathbb{F}_p)$ is an elliptic curve over $\mathbb{F}_p$ for all but finitely many primes p (in fact is $p \nmid 2n$).

Example: $E_7 : y^2 = x(x^2 - 49)$

$\overline{E_7}(\mathbb{F}_5) = y^2 = x(x^2 + \bar{1})$

$r_5 : (0, 7) \longmapsto (0, \bar{2}) \in \overline{E_7}(\mathbb{F}_5)$.

In particular $\#E(\mathbb{Q})_{tors} \mid \#\overline{E}(\mathbb{F}_p)$ (Lagrange)
(for all but finitely many p)

Proof: Suppose $\#E_n(\mathbb{Q})_{tors} > 4$.

↗ Subgroup of odd order.

- Either non-trivial point of odd order;
- Or all non-trivial points have even order:

then $E_n(\mathbb{Q})_{tors}$ is a 2-group of order ≥ 8, and
so has a subgroup of order 8
(use FTFGAB, or Sylow)

$S \leq E_n(\mathbb{Q})_{tors}$, $|S| = m$, m odd or $m = 8$

$\downarrow$

$r_p(S) \leq \overline{E_n}(\mathbb{F}_p)$. $\quad |S| = m \mid \#E_n(\mathbb{Q})_{tors} \mid \#\overline{E_n}(\mathbb{F}_p)$

By injectivity, $m \mid \#\overline{E_n}(\mathbb{F}_p)$ (FABFM p)

Claim: Suppose $p \equiv 3 \bmod 4$, we have $\#\overline{E_n}(\mathbb{F}_p) = p + 1$

Proof of claim [if time]

$\overline{E_n}(\mathbb{F}_p) : y^2 = \delta(x)$,
$\delta(x) = x(x^2 - \bar{n}^2)$ is odd.

∞, $(\bar{0}, \bar{0})$, $(\bar{n}, \bar{0})$, $(-\bar{n}, \bar{0})$ are 4 distinct points.

Then pair off $\{x, -x\}$. (As $p \equiv 3 \bmod 4$,
precisely one of each pair will be a square,
giving 2 points per pair)

So in total $\# \overline{E}_n(\mathbb{F}_p) = 4 + 2(p-3/2)$
$= p+1.$

So FABFM $p \equiv 3 \bmod 4$, $n \mid p+1$
So " $p \equiv -1 \bmod n$.

- $n = 8$: only finitely many $p \equiv 3 \bmod 8$
- n odd, $3 \nmid n$: " $p \equiv 3 \bmod 4n$
- n odd, $3 \mid n$: " $p \equiv 7 \bmod 12$

as if $p \equiv 7 \bmod 12$ and $p \equiv -1 \bmod n$
then $3 \mid n \mid p+1 = 12k+8$ for some k.

Contradiction in all 3 cases to
Dirichlet's Theorem on Primes in Arithmetic Progressions.

□

(It is still a hard problem to determine whether the rank of E_n is $=0$ or not for large n. The following result gives a relatively fast way of testing this, assuming the weak BSD conjecture for curves E_n)

(1983)

Theorem (Tunnell): Let $n > 0$ be squarefree.
If n is odd, then n is congruent $\Leftrightarrow$
$\# \{(x,y,z) \in \mathbb{Z}^3 \mid n = 2x^2+y^2+32z^2\}$ ($\Leftarrow$ dependent on BSD)
$= \frac{1}{2} \# \{(x,y,z) \in \mathbb{Z}^3 \mid n = 2x^2+y^2+8z^2\}$
(Similar if n even).

(This gives some congruence conditions on n)

Weak BSD: $L(E_n, 1) = 0 \Leftrightarrow \operatorname{rank}(E_n) > 0$.