The Congruent number problem, Elliptic curves, & the Birch–Swinnerton-Dyer conjecture

Tour of Mathematics
Chris Williams

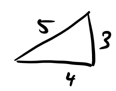
Common theme in research-level mathematics:

look for "surprising" connections between different fields.

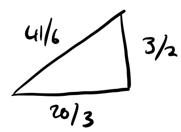
Today: congruent number problem, and its surprising connection to algebra and analysis.

§1: Congruent numbers

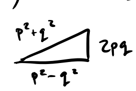
__Def'n__: Let $N \in \mathbb{Z}_{\geq 1}$. We say N is __congruent__ if $\exists$ a right angled triangle with __rational__ side lengths and area N.

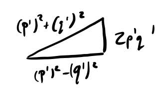
e.g. a) 6 is congruent: 

.

b) 5 is congruent: 

c) 1 is __not__ congruent (theorem of Fermat, 1670)

↳ idea of proof: infinite descent, 

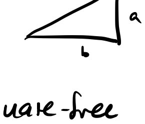
$\rightsquigarrow$ 

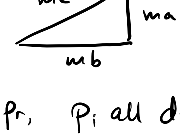
, $p'<p,\ q'<q$

__Ancient problem__: which N are congruent?

↳ appears in manuscripts from 10th century! ... to this day, we can only guess the answer.

__Note__: If $N, m \in \mathbb{N}$, then $(N \text{ congruent}) \iff (Nm^2 \text{ congruent})$





$\rightsquigarrow$ reduce to studying __square-free__ numbers $N = p_1 \cdots p_r$, p_i all distinct primes.

Examples of square-free congruent numbers ≤ 40: (circled in red)

1	~~9~~	17	~~25~~	33
2	10	~~18~~	26	34
3	11	19	~~27~~	35
~~4~~	~~12~~	~~20~~	~~28~~	~~36~~
5	13	21	29	37
6	14	22	30	38
7	15	23	31	39
~~8~~	~~16~~	~~24~~	~~32~~	~~40~~

($\times$ = not square-free, $\bigcirc$ = congruent)

ie. $\begin{cases} \text{Congruent numbers: } & 5,6,7,\ 13,14,15,\ 21,22,23,\ 29,30,31,34,\dots \\ \text{Non-congruent numbers: } & 1,2,3,\ 10,11,17,19,26,33,\dots \end{cases}$

... clear patterns: $-$ $N \equiv 5,6,7 \pmod 8 \overset{?}{\rightsquigarrow} N$ is congruent

$-$ $N \equiv 1,2,3 \pmod 8 \overset{?}{\rightsquigarrow} N$ is (usually!!) not congruent

§2: The congruent number curve (algebra)

Let $E_N : y^2 = x^3 - N^2 x$, ie.

$$E_N(\mathbb{Q}) = \{(x,y) \in \mathbb{Q}^2 : y^2 = x^3 - N^2 x\}.$$

Some "trivial" solutions:

$$(x,y) = (0,0),\ (N,0),\ (-N,0). \qquad \text{(all w/ } y=0\text{)}.$$

Do there exist any more?

Examples:

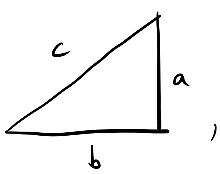
- $(-4,6) \in E_5(\mathbb{Q})$
- $(-3,9) \in E_6(\mathbb{Q})$
- $E_1(\mathbb{Q}) = \{(0,0),(\pm 1,0)\}$

N, $\exists (x,y) \in E_N(\mathbb{Q})$ with $y \neq 0$: 5, 6, 7, 13, 14, 15, 21, 22, 23, 29, 30, 31, 34, ...

N, All $(x,y) \in E_N(\mathbb{Q})$ have $y = 0$: 1, 2, 3, 10, 11, 17, 19, 26, 33, ...

<u>Proposition:</u> N is congruent $\iff$ $\exists (x,y) \in E_N(\mathbb{Q})$ with $y \neq 0$.

Pf: (Sketch). Suppose N is congruent. Let



, $a,b,c \in \mathbb{Q}$, with

(1): $a^2+b^2=c^2$,

(2): area $= \frac{ab}{2} = N$.

Then:

(3): (1) $+ 4 \times$ (2) $\Rightarrow (a+b)^2 = c^2+4N$

(4): (1) $- 4 \times$ (2) $\Rightarrow (a-b)^2 = c^2-4N$

(3) $\times$ (4) $\rightsquigarrow (a^2-b^2)^2 = c^4 - 16N^2$

$$\rightsquigarrow \left(\frac{a^2-b^2}{4}\right)^2 = \left(\frac{c}{2}\right)^4 - N^2.$$

$$\rightsquigarrow \left(\frac{(a^2-b^2)c}{8}\right)^2 = \left(\frac{c}{2}\right)^6 - N^2\left(\frac{c}{2}\right)^2.$$

Let $X = \left(\frac{c}{2}\right)^2$, $Y = \frac{(a^2-b^2)c}{8}$. Then have

$$Y^2 = X^3 - N^2 X, \quad Y \neq 0.$$

Converse is similar, but harder. $(\square)$

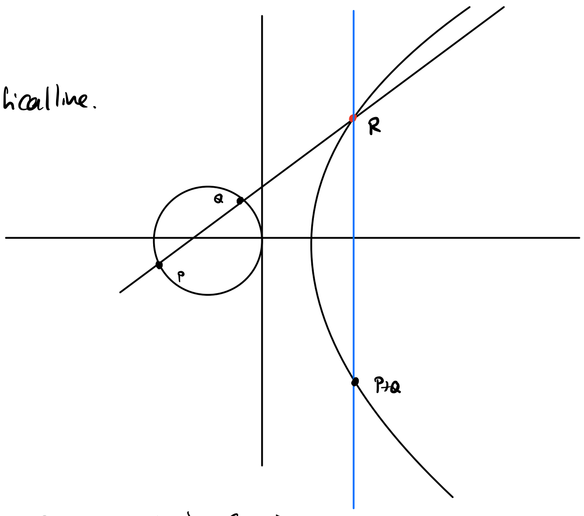
Question: When does $\exists (x,y) \in E_N(\mathbb{Q})$ with $y \neq 0$?

$\longrightarrow$ key thing: E_N is an elliptic curve.

∞

§3: Elliptic curves (geometry)

$E_N : y^2 = x^3 - N^2 x$. Let "∞" = end of vertical line.



Remarkable property: we can do arithmetic on the solutions of E_N!

Suppose $P = (x, y)$, $Q = (x', y')$ are pts.

- Draw the line between them. This hits a 3rd* point $R \in E_N(\mathbb{Q}) \cup \{\infty\}$.
- draw the vertical line through R. This hits another point in $E_N(\mathbb{Q}) \cup \{\infty\}$. Call it $P+Q$.

(Amazing!!) Fact: $E_N(\mathbb{Q}) \cup \{\infty\}$ is an abelian group.

Let $P = (x,y) \in E_N(\mathbb{Q})$. Write $2P = P+P$, $3P = 2P+P$, etc.

* all counted with multiplicity; this is Bezout's theorem.

Examples: - Always have $P + \infty = P$.

- In $E_N(\mathbb{Q})$, have

$$2\cdot(0,0) = 2(N,0) = 2(-N,0) = \infty.$$

- $P = (-4,6) \in E_5(\mathbb{Q})$. Then

$$2P = \left(\frac{1681}{144}, -\frac{62279}{1728}\right), \quad 3P = \left(-\frac{2439844}{5094049}, \frac{39601568754}{11497268593}\right), \quad \ldots$$

... getting increasingly complicated.

Fact: $\{P, 2P, 3P, 4P, \ldots\}$ are all distinct $\iff y \neq 0$.

$\hookrightarrow$ $\exists$ one point with $y \neq 0 \iff \exists$ infinitely many!!

Corollary: N is a congruent number $\iff E_N(\mathbb{Q})$ is infinite.

$\hookrightarrow$ Q: when is $E_N(\mathbb{Q})$ infinite?

9

§4: L-functions: connecting to analysis

For each prime p, let $a_p := p+1 - \#E_N(\mathbb{F}_p)$

$\uparrow := \{(x,y) \in \mathbb{F}_p^2 : y^2 = x^3 - N^2 x\}$.

Let $$L_p(E_N, s) = \frac{1}{1 - a_p p^{-s} - p^{-2s}}, \quad s \in \mathbb{C}$$

Let

$$L(E_N, s) = \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s) \prod_{p \text{ prime}} L_p(E_N, s)$$

Theorem: $L(E_N, s)$ defines a unique analytic function $\mathbb{C} \longrightarrow \mathbb{C}$.

(converges absolutely for $\mathrm{Re}(s) > 3/2$ and has analytic continuation to $\mathbb{C}$.)

Theorem: (1) If $N \equiv 5,6,7 \pmod 8$ squarefree, then $L(E_N,s)$ is skew-symmetric around $s=1$, ie.

$$L(E_N,s) = -L(E_N,2-s).$$

(2) If $N \equiv 1,2,3 \pmod 8$ squarefree, then $L(E_N,s)$ is symmetric around $s=1$, ie.

$$L(E_N,s) = L(E_N,2-s).$$

N w/ $L(E_N,s)$ skew-symmetric: $5,6,7,\ 13,14,15,\ 21,22,23,\ 29,30,31,\ldots$

N w/ $L(E_N,s)$ symmetric: $1,2,3,\ 10,11,\ 17,19,\ 26,\ 33,\ 34,\ldots$

$\rightsquigarrow$ the value $L(E_N,1)$ is very important! ie. if $N \equiv 5,6,7 \pmod 8$, then

$$L(E_N,1) = -L(E_N,1) = 0.$$

Examples:

- N s.t. $L(E_N,1) = 0$: $5,6,7,\ 13,14,15,\ 21,22,23,\ 29,30,31,\ 34,\ldots$
- N s.t. $L(E_N,1) \neq 0$: $1,2,3,\ 10,11,\ 17,19,\ 26,\ 33,\ldots$

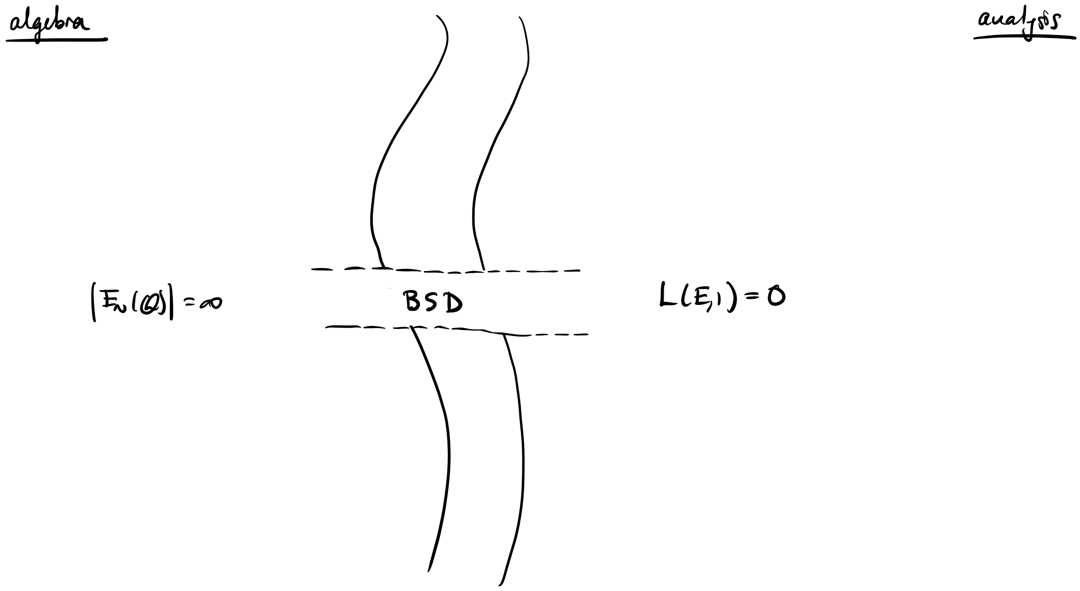
§5: BSD: connecting algebra and analysis

Conjecture: (Birch–Swinnerton-Dyer). $L(E_N,1) = 0 \iff E_N(\mathbb{Q})$ is infinite.

Corollary: If $N \equiv 5,6,7 \pmod 8$, then $L(E_N,1) = 0$

$$\overset{BSD}{\iff} E_N(\mathbb{Q}) \text{ infinite}$$

$$\iff N \text{ is congruent.}$$



How do we prove this?!

$\rightsquigarrow$ idea: look for <u>other</u> bridges

$\rightsquigarrow$ change the way we view distance.