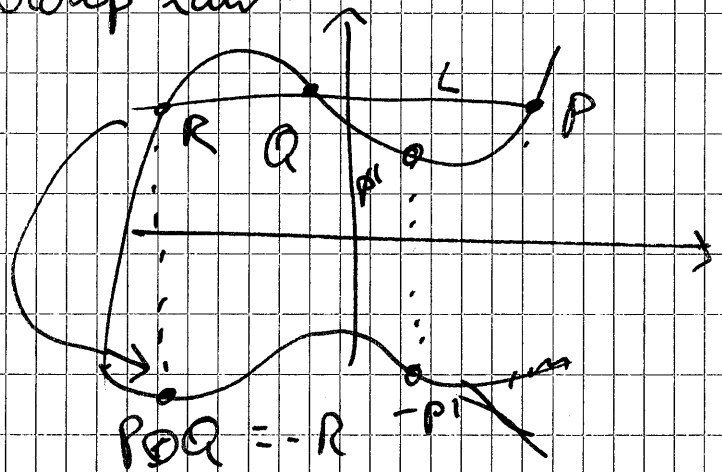
Brian Conrad, day 3

Notation: E = elliptic curve

$[n]: E \longrightarrow E$

$P \longmapsto \underbrace{P \oplus \cdots \oplus P}_{n \text{ times}}$ (if $n > 0$)

Group law:

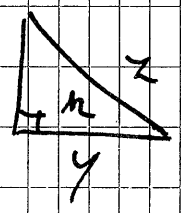


$P \oplus Q \oplus R = O$ (at ∞)

$\Leftrightarrow P \oplus Q = -R$

1) Congruent number problem

$n > 0$



$\frac{1}{2} xy = n$ → removes homogeneity

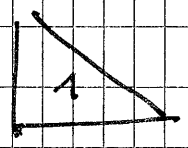
$x^2 + y^2 = z^2$

$x, y, z \in \mathbb{Q}$.

Q1 • For which n does such a rational right Δ exist? (if yes, n is called "congruent number")

Q2 • If n is a congruent number, are there infinitely many right triangles?

Ex. $n = 1$



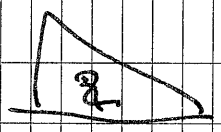
$\frac{1}{2} xy = 1$

$x^2 + y^2 = z^2$

$x^2 + \frac{4}{x^2} = z^2$

$x^4 + 4 = (xz)^2$

$u^2 = x^4 + 4$

$n = 2$ 

$\frac{1}{2}xy = 2$ ↙ $x^2 + \frac{16}{x^2} = z^2$

$x^2 + y^2 = z^2$ ↙ $x^4 + z^4 = a^2$ $(a = xz)$

Suppose there exist such $x, a \in \mathbb{Q}$, say common denominator k: multiply by k^4:

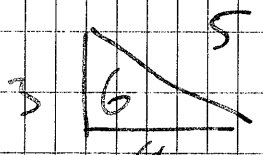
$(kx)^4 + (2k)^4 = (k^2 a)^2$

$x^4 + y^4 = z^2$ $\quad x, y, z \in \mathbb{Z}^+$

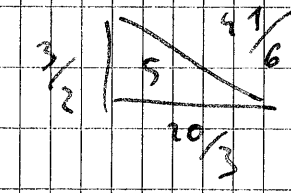
↳ Fermat showed this has no solution in $\mathbb{Z}^+$ by "infinite descent"
↳ one solution → descending chain ↯ contradiction

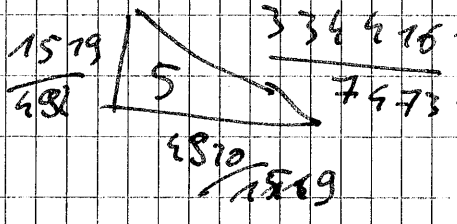
↳ Theorem: other proof.

→ 2 is not a congruent number
Fermat showed 1 is not a congruent number.

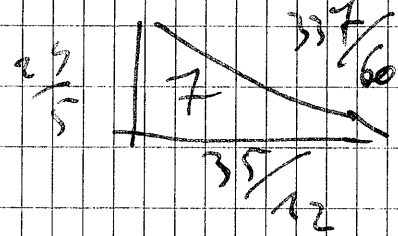
Ex: 

(6 is congruent number)
+ more with area 6?





+ more?



use $\frac{p}{q}$

1	2	3	4	5	6	7	...	10 →
X	X	X	?	✓	✓	✓		✓

Fermat Euler

$p, q \sim 10^2$

Question 1 has a known solution conditional on "Birch and Swinnerton-Dyer conjecture" (criterion for $\#E(\mathbb{Q}) = \infty$) → BSD

Theorem (Tunnell):

n odd, squarefree, on BSD:

n is congruent number $\Leftrightarrow$ $\#\{(a,b,c) \in \mathbb{Z}^3 \mid 2a^2+b^2+8c^2 = n\}$

$= 2 \cdot \#\{(a,b,c) \in \mathbb{Z}^3 \mid 2a^2+b^2+32c^2 = n\}$

2) The link with elliptic curves

→ with algebraic coeffs

(Realsborg: $y^2 =$ (cubic in x) is also an elliptic curve)

Fix $n \geq 1$. $E_n = \{y^2 = x^3 - n^2 x\} \cup \{\infty\}$

$= x(x+n)(x-n)$

$E_n[2] = \{\infty, (0,0), (n,0), (-n,0)\}$

$\{(x,y,z) \in \mathbb{Q}^3 \mid \frac{1}{2}xy = n,\ x^2+y^2 = z^2\} \longrightarrow \{(s,t) \in \mathbb{Q}^2 \mid s^2 - 4t^2 = \square,\ st \neq 0\}$

$\{\text{sides of triangles we're looking for}\} \longleftarrow$

$\cong E_n(\mathbb{Q}) - E_n[2]$

$$(x,y,z) \longmapsto \left(\frac{-xy}{x+z}, \frac{2xz}{\underbrace{x+z}_{\neq 0}}\right)$$

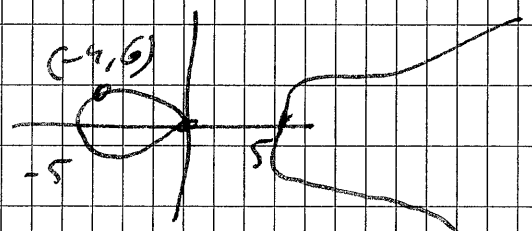
$$\left(\frac{u^2-v^2}{s}, -\frac{2uv}{s}, \frac{u^2+v^2}{s}\right) \longleftarrow (u,v)$$

↳ you can try to do this using Pythagorean parametrization.

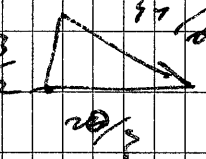
Can we find $P \in E_n(\mathbb{Q})$, $P=(x,y)$, $y \neq 0$ (i.e., $[2]P \neq 0$) ?

↳ Try $P \oplus$ (2-torsion)
$[2]P$, $[3]P$, ...

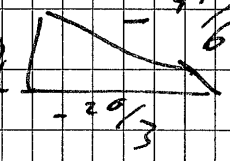
Ex $n=5$ $\quad y^2 = x^3 - 25x$



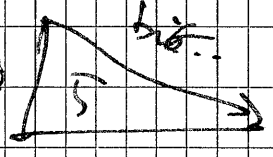
$$(-4,6) \longleftrightarrow \frac{3}{2}$$



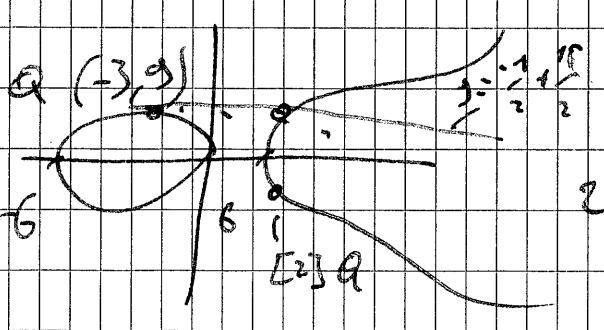
$$(-4,-6) \longleftrightarrow -\frac{3}{2}$$



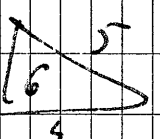
$$[2]P = \left(\frac{1681}{144}, \frac{41 \cdot 1519}{2^6 \cdot 3^3}\right) \longleftrightarrow \frac{1513}{492}$$



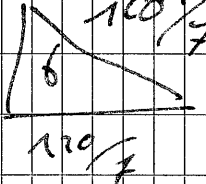
Ex. $n=6$ $\quad y^2 = x^3 - 36x$



$$y = -\frac{1}{2}x + \frac{15}{2} \quad (-3,9) \longleftrightarrow 3$$



$$2[Q] \longleftrightarrow \frac{7}{16}$$



3) Application of the arithmetic theory of elliptic curves

On Friday we'll use „Dirichlet's Theorem" on primes in arithmetic progressions to prove:

Theorem: $E_n(\mathbb{Q})_{\text{torsion}} = E_n[2]$

→ any $(r, s) \in E_n(\mathbb{Q})$ with $s \neq 0$ has infinite order!

Flavor of BSD conjecture:
E = elliptic curve over $\mathbb{Q}$
For large p: $E(\mathbb{F}_p)$ „makes sense"
How large is $\#E(\mathbb{F}_p)$?

Fact (Hasse): (Reimann hypothesis for ell. curves over $\mathbb{F}_p$)
$$|\#E(\mathbb{F}_q) - q + 1| \leq \mathcal{O}(\sqrt{q})$$

BSD roughly says if $\#E(\mathbb{F}_p) \approx p + 1 + 2\sqrt{p}$ rather than $\approx p + 1 - 2\sqrt{p}$ for large p, then $\#E(\mathbb{Q}) = \infty$

What is special about E_n? (for those, BSD's theoretical criterion becomes more useful (Tunnell))

→ $E_n: y^2 = x^3 - n^2 x$

$E_n(\mathbb{C})$ is abelian group so $\mathbb{Z}$-module, ie have endomorphisms $[a]: E_n(\mathbb{C}) \to E_n(\mathbb{C})$

$[i] : (x,y) \mapsto (-x, iy)$

$[i] \circ [i] : (x,y) \mapsto (x, -y) = [-1](x,y)$

Combine $\mathbb{Z}$-action with $[i]$ on $E_n(\mathbb{C})$,
get $\mathbb{Z}[i]$-action: $E_n(\mathbb{C}) = \mathbb{Z}[i]$-module.

→ connection with imaginary quadratic fields!