Introduction Why elliptic curves?

Arithmetic Geometry: study of diophantine equations

↝ Diophantus

Dioph. eq'n: $f(x_1, x_2, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n] = \mathbb{Z}[\bar{x}]$

$$f(\bar{x}) = 0$$

- Are there soln's to $f(\bar{x}) = 0$ over $\mathbb{Z}$? over $\mathbb{Q}$?
- If so can we find any? all?

(Hilbert #10, is there an algorithm)

↝ Matiyasevich 70's **NO!** (1Z)

- Solving diophantine eqn's.

(1 var) $f(x) = 0$, a polynomial

Thm $a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 = 0$, $a_i \in \mathbb{Z}$, $a_n \neq 0$

and suppose $x_0 = \frac{s}{t}$, $s, t \in \mathbb{Z}$, $t \neq 0$ is a root.

Then $s \mid a_0$, $t \mid a_n$.

(2 var, deg=1) $L: ax + by = c$, a, b, c non-zero integers

Thm $L(\mathbb{Z}) \neq \emptyset \iff \gcd(a,b) \mid c$.

↳ construct all $\mathbb{Z}$-points.

(2 var, deg=2) $C: ax^2 + bxy + cy^2 + dx + fy + g = 0$ coeffs in $\mathbb{Q}$. (smooth conic)

Thm (Legendre, Hasse-Minkowski)

$C(\mathbb{Q}) \neq \emptyset \iff C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p)$ for all prime p.

(global - local principle)

lines + conics : genus 0 → no $\mathbb{Q}$-pts (e.g. $x^2+y^2=-1$) or ∞'ly many $\mathbb{Q}$ pts

(2 vars, deg = 3) smooth (proj space) curve, ~~deg 3~~, genus 1.

$C: ax^3 + bx^2y + \dots = 0$

- no $\mathbb{Q}$-pts
- or fin. many $\mathbb{Q}$-pts
- or ∞'ly many $\mathbb{Q}$ pts

WARNING! LOCAL-TO-GLOBAL PRINCIPLE FAILS!!

EXAMPLE (SELMER): $3x^3 + 4y^3 + 5z^3 = 0$

has soln's over $\mathbb{R}$ and $\mathbb{Q}_p$ (all p)

BUT no $\mathbb{Q}$ solutions.

Selmer, "The diophantine eq'n $ax^3+by^3+cz^3=0$"
Acta. Arith. 85 (1951), 203-362.

(genus > 1) Thm (Mordell conjecture, Faltings's Theorem)

If $C/\mathbb{Q}$ is a curve of genus > 1, then $C(\mathbb{Q})$ is a finite set.

Examples of diophantine equations.

- (The Hundred Fowls Problem)
  One rooster is worth 5 qian, one hen is 3 qian, and 3 chicks is 1 qian. If we bought 100 fowls with 100 qian, how many roosters, hens, and chicks did we buy?
  $\hookrightarrow$ $\mathbb{Z}$-points on a line.
- Find all the $\mathbb{Q}$-points on $x^2 - 3xy + y^2 = 5$.