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 dioph. eqn's.

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

  Thm $a_n x$