

NUMBER FIELDS

V/S

ELLIPTIC CURVES

$K = \mathbb{Q}(\alpha)$ where $f(\alpha) = 0$, $f(x) \in \mathbb{Z}[x]$.

\mathcal{O}_K ring of integers of K
(those $\beta \in K$ roots of monic $g(x) \in \mathbb{Z}[x]$)

THM: \mathcal{O}_K is a finitely generated abelian group.

\mathcal{O}_K^\times units in \mathcal{O}_K .

THM: \mathcal{O}_K^\times is a fin. gen. ab. gp. of rank $r_1 + r_2 - 1$
(DIRICHLET'S UNIT THEOREM) where

$$[K : \mathbb{Q}] = n = r_1 + 2r_2$$

$$\Rightarrow \mathcal{O}_K^\times \cong \underbrace{(\mathcal{O}_K^\times)_{\text{tors}}}_{\mu(K) \text{ roots of unity in } K} \oplus \mathbb{Z}^{r_1 + r_2 - 1}$$

$Cl(K) = \frac{\text{fract. ideals of } K}{\text{princ. ideals}}$ } failure of local-to-global princip
ideal class gp "arithmetic complexity" of \mathcal{O}_K

$E: y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Q}$, smooth (projective)

$$E(\mathbb{Q}) = \{ (x, y) \in E : x, y \in \mathbb{Q} \} \cup \{ [0:1:0] \}$$

THM (Mordell-Weil) $E(\mathbb{Q})$ is a f.g. ab. gp

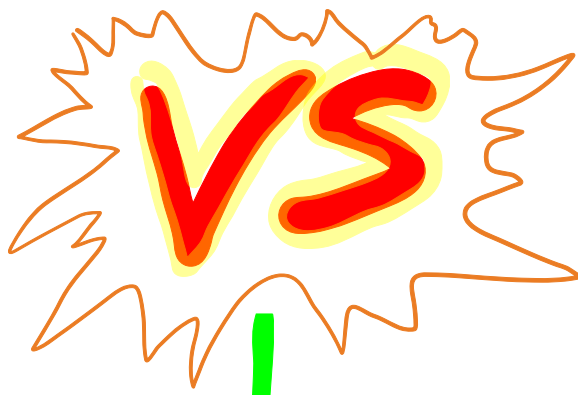
$$\Rightarrow E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^{r_{E/\mathbb{Q}}}$$

\mathbb{Q} : DESCRIPTION OF $r_{E/\mathbb{Q}}$??

$III(E/\mathbb{Q})$ - Shafarevich-Tate group
"arithmetic complexity of $E(\mathbb{Q})$ "

determines the failure of the local-to-global principle for E/\mathbb{Q} .

NUMBER FIELDS



ELLIPTIC CURVES

NUMBER FIELDS

$$K = \mathbb{Q}(\sqrt{5})$$

$$\mathcal{O}_K = \mathbb{Z} \left[\underbrace{\frac{1+\sqrt{5}}{2}}_{\text{root of } x^2-x-1=0} \right]$$

$$\mathcal{O}_K = \mathbb{Z} + \left(\frac{1+\sqrt{5}}{2} \right) \mathbb{Z}$$

$$\mathcal{O}_K^\times \quad \text{rank } 2 + 0 - 1 = 1.$$

$$= \left\{ \pm \left(\frac{1+\sqrt{5}}{2} \right)^n : n \in \mathbb{Z} \right\}$$

$$\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}.$$

$$\begin{aligned} [K:\mathbb{Q}] &= 2 \\ &= 2 + 2 \cdot 0 \\ r_1 &= 2 \\ r_2 &= 0 \end{aligned}$$

ELLIPTIC CURVES

$$E: y^2 = x^3 - 2x$$

$$E(\mathbb{Q}) = \langle (0,0), (2,2) \rangle$$

$$\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} \quad \text{rank}_{E/\mathbb{Q}} = 1.$$

