§1 Ellipt. Curves

Def EC / field k $\underset{def}{=}$ $(E, +)$ k-group scheme with $E \to \operatorname{Spec} k$ proper smooth connected curve.

How do ECs behave?

0) Always commutative (explains why I wrote "+")

1) For every group scheme $(G, m) \xrightarrow{p} \operatorname{Spec} k$,

$$\Omega^1_{G/k} \cong p^* e^* \Omega^1_{G/k} \qquad e : \operatorname{Spec} k \to G$$

unit section.

In prtic, $\forall$ ECs (E, m), $\Omega^1_{E/k} \cong \mathcal{O}_E$.

($\Omega^1_{E/k}$ is a line bundle since E/k is smooth + 1-dim'l.

Thus $e^* \Omega^1_{E/k}$ is a 1-dim'l k-vsp.)

So for the genus:

$$g(E) = h^0(\Omega^1_{E/k}) = h^0(\mathcal{O}_E) = 1.$$

2) **Key Lem** $\mathcal{L}$ lb on E, $\deg \mathcal{L} \geq 1$. Then

$$h^0(\mathcal{L}) = \deg \mathcal{L}, \quad h^1(\mathcal{L}) = 0.$$

Serre duality: $h^1(\mathcal{L}) = h^0(\Omega^1_{E/k} \otimes \mathcal{L}^\vee) = 0$

since $\deg \Omega^1 \otimes \mathcal{L}^\vee < 0$.

Riemann-Roch:

$$h^0(\mathcal{L}) = \deg \mathcal{L} + \underbrace{1 - g + h^1(\mathcal{L})}_{=0 \text{ by prev arguments.}}$$

3) <u>ECs are cubics</u> $e \in E(k)$ identity of grp str.

Key Lemma implies

$$\dim_{\bar{k}} H^0(\mathcal{O}_{E_{\bar{k}}}(3 \cdot [e])) - \dim_{\bar{k}} H^0(\mathcal{O}_{E_{\bar{k}}}(3[e] - [x] - [y])) = 2$$

$\xRightarrow{\text{Std. Criterion}}$ $\mathcal{O}(3[e])$ very ample.

$\Longrightarrow$ $E \hookrightarrow \mathbb{P}^2_k$ embeds

Necessarily $E = V_+(\text{cubic polynomial})$

since $g(E) = 1$.

4) Converse to above: <u>Thm</u> E/k genus 1, $e \in E(k)$.

Then $\exists!$ group sch. str. $(E, +)$ w/ identity e.

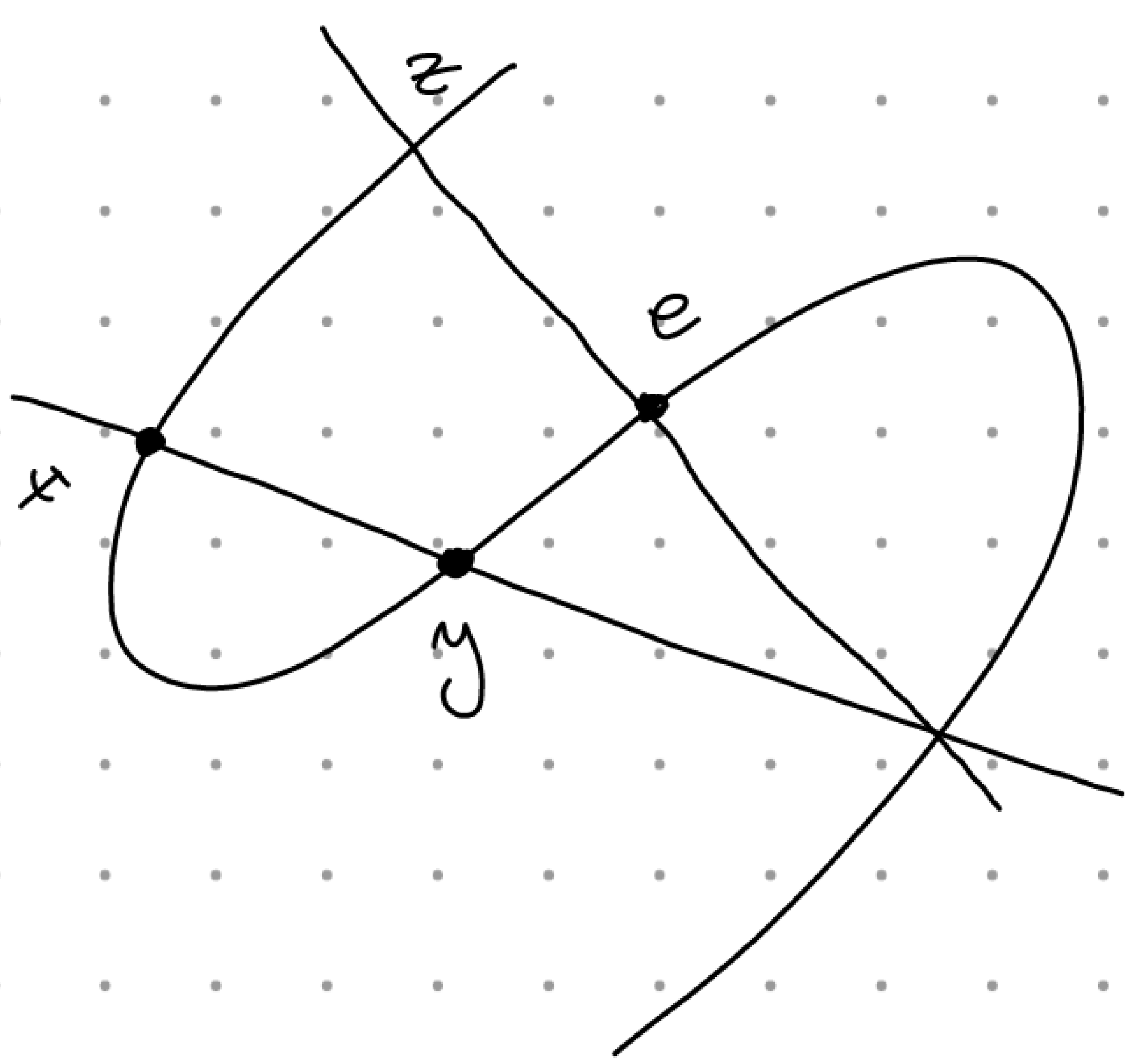
<u>Idea</u> Given $x, y \in E(k)$, need to define $x+y \in E(k)$

Key Lem $\Rightarrow$ $h^0(\mathcal{O}_E([x]+[y]-[e])) = 1$

i.e. $\exists!$ section s up to $k^\times$.

Then $\mathcal{O}_E([x]+[y]-[e]) / \mathcal{O}_E \cdot s \cong i_{z,*} k$ @

for unique $z \in k^\times$. Put $z = x+y$.



Two ways to make rigorous:

a) Express in coords, show given by morphism $+ : E \times E \to E$.
[Sil. III.2]

b) Develop argument @ in more generality.
[AVs Lect. 8]

§2 The group $E(k)$

$E(k)$ is an abelian group.

1) Case $k = \mathbb{C}$

Then $E(\mathbb{C})$ is underlying set of a Riemann surface of form (compatible w/ group str.)

$$\mathbb{C}/\Lambda \,, \qquad \Lambda \cong \mathbb{Z}^2 \subseteq \mathbb{C} \text{ lattice}$$

As topological group just $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$,
but

$$\mathbb{C}/\Lambda_1 \cong \mathbb{C}/\Lambda_2 \text{ as R.S.} \iff \Lambda_2 = \lambda \cdot \Lambda_1$$

for some $\lambda \in \mathbb{C}^\times$.

2) Case $k \cong \mathbb{F}_q$ finite

Then $E(\mathbb{F}_q) \subseteq \mathbb{P}^2(\mathbb{F}_q)$ finite abelian group.

Thm (Hasse)

$$\left| \# E(\mathbb{F}_q) - q - 1 \right| \leq 2\sqrt{q}.$$

3) Case k global i.e. $k/\mathbb{Q}$ or $k/\mathbb{F}_p(t)$ finite

Thm (Mordell-Weil)

$E(k)$ is a fin gen abelian group

$$E(k) \cong E(k)_{tors} \oplus \mathbb{Z}^r, \quad r := \text{rank of } E.$$

What is known?

Thm (Mazur 1978) $k = \mathbb{Q}$. Then $|E(\mathbb{Q})_{tors}| \leq 16$.

(Bounds exist for all number fields.)

Rank r is very mysterious by comparison:

·) Known record (Elkies 2006):

Explicit $E/\mathbb{Q}$ w/ $\operatorname{rk} E(\mathbb{Q}) \geq 28$.

·) Statistical results:

When enumerating all ECs $E/\mathbb{Q}$,

50% rank 0

50% rank 1

0% rank ≥ 2.

·) Open question:

Is $\{ \operatorname{rk} E(\mathbb{Q}) \mid E/\mathbb{Q} \text{ EC} \}$ bounded?

Heuristics suggest that $\exists$ fin. many E with $\operatorname{rk} E(\mathbb{Q}) > 21$, but this is open.

(Park-Poonen-Wood-Voight 2016)

§3 Birch and Swinnerton-Dyer Conj

Consider quadrics first: $X = V_+(\text{quadratic}) \subseteq \mathbb{P}^2_{\mathbb{Q}}$ smooth.

Then $X(\mathbb{Q}) \neq \emptyset \iff X \cong \mathbb{P}^1$.

<u>Hasse principle</u> $X(\mathbb{Q}) \neq \emptyset \iff X(\mathbb{Q}_p) \neq \emptyset \ \forall p$ & $X(\mathbb{R}) \neq \emptyset$.

For EC $E/\mathbb{Q}$, we already have $E(\mathbb{Q}) \neq \emptyset$ since $e \in E(\mathbb{Q})$.

The question is instead: How large is r?

<u>Conjectural answer (BSD Conj)</u>

·) $\mathcal{E} \longrightarrow \operatorname{Spec} \mathbb{Z}[D^{-1}]$ smooth proj model of E

For example, write $E = V_+(P) \subseteq \mathbb{P}^2_{\mathbb{Q}}$

$P \in \mathbb{Q}[X,Y,Z]$.

Pick d s.th. $P \in \mathbb{Z}[d^{-1}][X,Y,Z]$, consider

$\tilde{\mathcal{E}} = V_+(P) \xrightarrow{\pi} \operatorname{Spec} \mathbb{Z}[d^{-1}]$

Then $\operatorname{Spec} \mathbb{Q} \times_{\operatorname{Spec} \mathbb{Z}[d^{-1}]} \tilde{\mathcal{E}} \cong E$ and is

in ptic smooth.

Smooth locus is open, so $\exists\, E \subset U \subseteq \tilde{\mathcal{E}}$ open

s.th. $U \to \operatorname{Spec} \mathbb{Z}[d^{-1}]$ is smooth.

Then $Z = \tilde{\mathcal{E}} \setminus U$ closed.

$\tilde{\mathcal{E}} \to \operatorname{Spec} \mathbb{Z}[d^{-1}]$ proj, in ptic proper,

so $\pi(Z) = V(e) \subseteq \operatorname{Spec} \mathbb{Z}[d^{-1}]$ closed.

Put $D = d \cdot e$. Then

$$\mathcal{E} := \operatorname{Spec} \mathbb{Z}[D^{-1}] \times_{\operatorname{Spec} \mathbb{Z}[d^{-1}]} \tilde{\mathcal{E}} \longrightarrow \operatorname{Spec} \mathbb{Z}[D^{-1}]$$

is smooth proj. as required.

·) By val crit of properness, get lifting of identity:

$$\begin{tikzcd}
\operatorname{Spec} \mathbb{Q} \arrow[r, "e_{\mathbb{Q}}"] \arrow[d] & \mathcal{E} \arrow[d] \\
\operatorname{Spec} \mathbb{Z}[D^{-1}] \arrow[r, equal] \arrow[ur, dotted, "e"] & \operatorname{Spec} \mathbb{Z}[D^{-1}]
\end{tikzcd}$$

·) Genus of a curve is constant in flat families,

so $\forall p \nmid D$, $E_p = \mathbb{F}_p \otimes_{\mathbb{Z}[D^{-1}]} \mathcal{E} \,/\, \mathbb{F}_p$ is

of genus 1.

Section $e \in \mathcal{E}(\mathbb{Z}[D^{-1}])$ gives $e_p \in E_p(\mathbb{F}_p)$

Thm from §1 4) applies:

E_p in unique way an EC w/ unit e_p.

·) Set $N_p := \# E_p(\mathbb{F}_p) = \# \mathcal{E}(\mathbb{F}_p)$

<u>Conj (BSD)</u> (1960s) $\prod_{p \leq x} \frac{N_p}{p} \approx C \cdot \log(x)^r$ as $x \to \infty$.

Note that $\frac{N_p}{p} \in 1 + \frac{1}{p} + \left[-\frac{2}{\sqrt{p}}, \frac{2}{\sqrt{p}}\right]$ (Hasse)

<u>Heuristics:</u> If $E_p(\mathbb{F}_p)$ is slightly larger on average, then r is larger.

Plausible since red. crit. of prop. gives group homs

$E(\mathbb{Q}) \to E_p(\mathbb{F}_p)$ for all p.

What is known? If $\prod_{p \leq x} \frac{N_p}{p} \approx C \cdot \log(x)^r$

with $r = 0, 1$, then $\mathrm{rk}_{\mathbb{Z}} E(K) = 0$ resp 1.

Converse direction & cases $r \geq 2$ open.

Many mathematicians involved, relevant for us:

Wiles & Taylor-Wiles (2001)

All ECs $E/\mathbb{Q}$ are modular:

$\exists\ N \geq 1$ + dominant map $M_N \xrightarrow{f_E} E$ from

modular curve M_N of level N.

Gross-Zagier (1986)

In certain situations (concerns ~50% of ECs of rank 1)

$f_E(P_E)$ is non-torsion,

where $P_E \in M_N$ is a specific point.

(Heegner point)

§4 About M_N (Will all be explained during course.)

·) Curve over $\mathbb{Q}$, parametrizes ECs w/ level-N-structure:

Morphisms $S \to M_N$ are the same as isoclasses of (E,α) with

$E = (E,+) \to S$ relative EC

$\alpha : \underline{(\mathbb{Z}/N\mathbb{Z})^{\oplus 2}}_S \xrightarrow{\cong} E[N]$

·) To appreciate M_N may be complicated as an abstract curve, e.g. genus $g(M_N)$ might be large.

But description in terms of (E,α) makes it very special and allows all kinds of arguments.

·) Moduli description allows to define P_E, to define + study integral models $\mathcal{M}_N/\mathbb{Z}$, to define maps $M_N \to M_{N'}$ etc...