$E/k$ EC, $k = \bar{k}$ $\quad$ char $k = p$ (possibly $p = 0$)

<u>Have</u>

$$\mathrm{QIsog}(E) \cong \begin{cases} \prod'_{\ell} \{\Lambda_\ell \subseteq V_\ell E\} & p = 0 \\ \underbrace{\left\{ \begin{matrix} \mathbb{Z} \\ \mathbb{Z}\times\mathbb{Z} \end{matrix} \right\}}_{\nu_p} \times \prod'_{\ell \neq p} \{\Lambda_\ell \subseteq V_\ell E\} & p \neq 0 \end{cases}$$

Restricted prod.: almost all $\Lambda_\ell = T_\ell E$.

ordin. $\quad$ supersing

$$\mathrm{End}(E) = \left\{ g \in \mathrm{End}^\circ(E) \;\middle|\; \begin{matrix} g T_\ell E \subseteq T_\ell E \ \forall \ell \\ + \ \nu_p(g) \geq \begin{cases} 0 \\ (0,0) \end{cases} \end{matrix} \right\}$$

<u>Claim from last time</u> $\quad$ In p'tic, order

$$\mathrm{End}(E)_p \subseteq \mathrm{End}^\circ(E)_p$$

is maximal.

Already seen: $\begin{cases} V(\mu_{p^r}) & r \geq 0 \\ V(\mu_{p^r}), & E[p^r]^{red}_k \end{cases}$

form chains, hence $\begin{cases} \nu_p \\ \text{each component of } \nu_p \end{cases}$

are valuations on $\mathrm{End}^\circ(E)$.

Left open: Case $E$ ordinary, $K = \mathrm{End}^\circ(E) \neq \mathbb{Q}$.

Write $\mathrm{ikv}_p = (v_1, v_2)$, then

$v_1 \neq v_2$ (as valuations on $K$.)

Proof $v_1, v_2$ related by

$$v_1(\alpha) + v_2(\alpha) = \log_p \deg_p(\alpha) = \log_p \alpha\alpha^*.$$

& $*$ is non-trivial involution on $K$. $\square$

We then saw:

Thm (Uniformization of isogeny class of EC's)

$A = \mathrm{End}^\circ(E)$, $k = \bar{k}$. Then

$$\{E' \text{ isogenous to } E\}/\cong \xrightarrow{\sim} A^\times \backslash X \quad @$$

$\exists$ isogeny $E \to E'$

$$X = \begin{cases} \prod_\ell \{\Lambda_\ell \subseteq V_\ell E\} \\ \{\mathbb{Z}_{\mathbb{Z}\times\mathbb{Z}}\} \times \prod_{\ell \neq p} \{ \text{—''—} \} \end{cases}$$

Choices $V = \mathbb{Q}^2 \supseteq \mathbb{Z}^2$

$$\gamma_\ell : T_\ell E \cong \mathbb{Z}_\ell^2 \qquad \ell \neq p$$

$$\gamma_p : (r,s) \mapsto \begin{cases} p^{-r}\mathbb{Z}_p^2 \subseteq \mathbb{Q}_p^2 \\ p^{-r}\mathbb{Z}_p \oplus p^{-s}\mathbb{Z}_p . \end{cases}$$

In this way, view (non-canonical)

$$X \hookrightarrow \{\mathbb{Z}\text{-lattices } \Lambda \subseteq V\}$$

Case $A = \mathbb{Q}$ $\quad A^\times \backslash X \xrightarrow{\cong}$ lattices $\Lambda \subseteq V$

(+ specific form of $\Lambda_p$) up to homothety

$$\Lambda \sim \lambda \cdot \Lambda \quad \lambda \in \mathbb{Q}^\times .$$

Case $A = K$ (Exercise 1 on sheet)

May choose $V = K$, pick $\gamma$'s $K$-linearly.

$$A^\times \backslash X \cong K^\times \backslash \{\Lambda \subseteq K \ (\text{+ specific at } p)\}$$

$$= \coprod_{f \geq 1} \mathrm{Pic}(\mathbb{Z} + f \cdot \mathcal{O}_K)$$

(+ $(f,p) = 1$ if $p \neq 0$)

Case $A = B$

Then $\Lambda_\ell \longmapsto \mathrm{Stab}(\Lambda_\ell) \subseteq B_\ell \cong M_2(\mathbb{Q}_\ell)$

is a maximal order.

In this way

$$X \xrightarrow{\cong} \{ \text{Max orders } \mathcal{O} \subseteq \overset{\substack{\mathrm{End}^0(E) \\ \shortparallel}}{B} \}$$

$$B^\times \backslash X \xrightarrow{\cong} \{ \text{Max orders } \mathcal{O} \text{ up to conjugacy.} \}$$

Only case where $A^\times \backslash X$ is finite!

Prop $E/k$, $k = \bar{k}$, char $k = p$.

Then

$E$ supersingular $\iff$ $\mathrm{End}^0(E) = B$ is quaternion.

Proof Already seen: $\Leftarrow$ - direction since

( $\nexists$ $B \to \mathbb{Q}_p$ $\mathbb{Q}_p$-alg homomorphism

& $E$ ordinary would imply $B \subset V_p E$ )

Conversely $E$ supersingular.

$$\Rightarrow \quad E[p] = V(\mu_{p^2})$$

$$= \ker\left(F^{(p)} \circ F : E \longrightarrow E^{(p)} \longrightarrow E^{(p^2)}\right)$$

$$\Rightarrow \quad E \cong E^{(p^2)}$$

$$\Rightarrow \quad j(E) = j(E^{(p^2)}) = j(E)^{p^2}$$

since $E^{(p^2)} = \operatorname{Spec} k \underset{x \mapsto x^{p^2}, \operatorname{Spec} k}{\times} E$

Recall $E \cong E'$ over alg closed field
$\Leftrightarrow j(E) = j(E')$

$\Rightarrow \exists$ only fin many isom classes of supersing elliptic curves (uses $k = \bar{k}$)

(use that supersing. is isogeny invariant.)

$\Rightarrow$ Above classification of $A^\times \backslash X$, cases $A = \mathbb{Q}, K$ are excluded. $\square$

**Prop** 1) $\{EC/k\} \longrightarrow k$

$E \longmapsto j(E)$ surjective.

2) $k = \bar{k}$, bijective

If $k \neq \bar{k}$, may happen that $j(E) = j(E')$, but $E \not\cong E'$ over $k$.

(E.g. quadratic twists.)

<u>@</u>: $\{E' \text{ over } k \mid \exists \text{ isogeny } E \to E'\}/\cong$

$$\cap$$

$\{E'/k \ EC\}/\cong$

Uniformization

<u>Compare</u> $QIsog(E) = \{(E', \phi) \mid \phi : E \to E' \text{ isogeny}\}/\cong$