Thm: 1) The map $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell E)$ is injective;

2) For $\varphi \in \mathrm{End}(E)$

$$\det(T_\ell \varphi) = \deg \varphi \quad , \quad \mathrm{tr}(T_\ell \varphi) = t(\varphi) = 1 + \deg \varphi - \deg(\mathrm{id} - \varphi)$$

3) The polynomial $X^2 - t(\varphi) X + \deg \varphi$ vanishes on φ (in $\mathrm{End}(E)$) and has negative (≤ 0) discriminant.

Proof: 1) OK

2) Fix a basis $u = (u_n)$, $v = (v_n)$ of $T_\ell E$. $\quad T_\ell E = \varprojlim E[\ell^n]$, $u_n \mapsto (u_n)$, $v_n \mapsto (v_n)$

$\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ = matrix of $T_\ell \varphi$ in this basis.

$$e(T_\ell \hat{\varphi} \circ T_\ell \varphi(u), v) = e(T_\ell \varphi(u), T_\ell \varphi(v)) = e(au + bv, cu + dv)$$

$T_\ell[\deg \varphi]$ = $\deg \varphi \; e(u,v)$; $T_\ell \varphi$, $T_\ell \hat{\varphi}$ are adjoint ; $T_\ell \mathbb{G}_m \cong \mathbb{Z}_\ell$; Weil's pairing is skew symmetric

$$(ad - bc)\, e(u,v)$$

Since $e(u,v) \in \mathbb{Z}_\ell$ is non zero (because Weil's pairing is non degenerate) we have $\deg \varphi = ad - bc = \det T_\ell \varphi$.

$A \in M_2(k) \qquad \mathrm{tr}(A) = 1 + \det(A) - \det(A - 1\mathrm{d})$.

$\det(A - 1\mathrm{d}) = 1^2 - \mathrm{tr}A + \det A$.

3) By Cayley–Hamilton,

$$f(x) = x^2 - t(\varphi) X + \deg \varphi \text{ vanishes on } T_\ell \varphi \text{ (in } \mathrm{End}(T_\ell E)).$$

$\Longrightarrow$ $f(x)$ vanishes on φ (in $\mathrm{End}(E)$).

$\mathrm{End}(E) \hookrightarrow \mathrm{End}(T_\ell E)$ inj

In order to show that the discriminant is negative, it suffices to show that $f(x) \geq 0$ for all $x \in \mathbb{R}$. By continuity it suffices to show it for $x = \frac{r}{s} \in \mathbb{Q}$, $s > 0$.

$$s^2 f\left(\tfrac{r}{s}\right) = s^2 \deg \varphi - rs\, t(\varphi) + r^2 = \det(r \cdot \mathrm{id} - T_\ell(\varphi \circ [s])$$

$$\| \deg([r] - \varphi \circ [s]) \geq 0$$

ENDOMORPHISM RING

Let E be an elliptic curve over a perfect field k.

Lemma: $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{R}$ is a division $\mathbb{R}$-algebra (not necessarily commutative).

Up to isomorphism, the only possibilities are: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ (quaternions).

Proof: Remark that $\dim_{\mathbb{R}} \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{R} = \mathrm{rk}_{\mathbb{Z}_\ell} \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \leq 4$.

with ℓ prime $\neq \mathrm{char}(k)$.

The map $\varphi \mapsto \hat{\varphi}$ is additive, so it extends by linearity to $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{R}$ and the extension is continuous. In particular,

$$\deg(\varphi) \geq 0 \quad \text{for all } \varphi \in \mathrm{End}(E).$$

$\varphi \mapsto \deg \varphi$ is a positive definite quadratic form on $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{R}$.

$\deg(\varphi\psi) = \deg\varphi \deg\psi \geq 1$ if φ, ψ are non constant.

$\Longrightarrow \varphi\psi \neq 0$. Therefore $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{R}$ has no non trivial zero divisors. Since $\dim_{\mathbb{R}} \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{R} < +\infty$, every non zero element is invertible. □

Cor: The $\mathbb{Q}$-algebra $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ may take the following forms:

- $\mathbb{Q}$ ($\mathbb{R} \otimes_{\mathbb{Z}} \mathrm{End}\, E = \mathbb{R}$)
- an imaginary quadratic extension of $\mathbb{Q}$. ($\mathbb{R} \otimes_{\mathbb{Z}} \mathrm{End}(E) = \mathbb{C}$)
- a quaternion algebra with center $\mathbb{Q}$, non split over $\mathbb{R}$. ($\mathbb{R} \otimes_{\mathbb{Z}} \mathrm{End}(E) = \mathbb{H}$).

Moreover, if $\mathrm{char}(k) = 0$, only the first two possibilities can happen ($\mathrm{End}(E) \hookrightarrow k$ if $\mathrm{char}(k) = 0$).

Recall:

- An imaginary quadratic extension K of $\mathbb{Q}$ is of the form $\mathbb{Q}(\alpha) = \mathbb{Q} \oplus \mathbb{Q}\alpha$ with $\alpha^2 < 0$.
- A quaternion algebra over a field K is a division K-algebra D of dimension 4 and center K.

$\Rightarrow$ K'/K is a field extension

If K'/K ...

$D \otimes_K K'$ — division algebra — non-split over K' (definite)

$D \otimes_K K'$ — $\cong M_2(K')$ — split over K'

Here, in the case $D = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\dim_{\mathbb{Q}} D = 4$, then $D \otimes_{\mathbb{Z}} \mathbb{R}$ is non-split.

$$D = \mathbb{Q} \oplus \mathbb{Q}\alpha \oplus \mathbb{Q}\beta \oplus \mathbb{Q}\alpha\beta, \quad \alpha^2, \beta^2 \in \mathbb{Q}_{<0}$$

$$\alpha\beta = -\beta\alpha.$$

Rmk: Suppose that $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a quaternion algebra. Therefore $\mathrm{char}(k) = p > 0$. Take ℓ prime $\neq p$.

$$\underbrace{\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell}_{\dim 4} \hookrightarrow \underbrace{\mathrm{End}(T_\ell E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell}_{\dim 4} \cong M_2(\mathbb{Q}_\ell)$$

(the inclusion is an isomorphism)

This means that $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ is split. One can see that there is only one quaternionic algebra D_p over $\mathbb{Q}$ s.t. $D_p \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is split for each $\ell \neq p$ and $D_p \otimes_{\mathbb{Q}} \mathbb{R}$ is non split.

One sees that $D_p \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is non split.

[Serre, A course in Arithmetic.]

Fix a prime p

Prop. There are only finitely many isomorphism of supersingular elliptic curves, and they can all be defined over $\mathbb{F}_{p^2}$.

Proof. On Friday. □

Prop. Let $E/\overline{\mathbb{F}}_p$ be an elliptic curve. Then,

- if E is ordinary, then $\mathrm{End}(E) \otimes \mathbb{Q}$ is quadratic;
- if E is supersingular, then $\mathrm{End}(E) \otimes \mathbb{Q}$ is quaternionic.

Proof: First of all, let q be a power of p st. E is defined over $\mathbb{F}_q$ (Take q so big that it contains all the coefficients of a Weierstrass equation.) In this case $E^{(q)} = E$, so that

$$F_q : E \to E^{(q)} = E \quad \text{is an endomorphism.}$$

Suppose E is ordinary. Then $E[p^n] = E[p^n](\overline{\mathbb{F}_p}) \simeq \mathbb{Z}/p^n\mathbb{Z}$.

$$T_p E = \varprojlim_n E[p^n] \simeq \mathbb{Z}_p.$$

($T_p E$: p-adic Tate module)

$$T_p : \mathrm{End}(E) \longrightarrow \mathrm{End}_{\mathbb{Z}_p}(T_p E) \simeq \mathbb{Z}_p.$$

Since $E[p^\infty] = \bigcup_{n\geq 0} E[p^n]$ is infinite in $\overline{E}$, then T_p is injective. In particular

$$\mathrm{End}(E) \text{ is commutative.}$$

We want to show that F_q is not in $\mathbb{Z}$. Suppose by contradiction $[m] = F_q$, then

$$m^2 = \deg[m] = \deg F_q = q.$$

$$\longrightarrow q = p^{2r} \text{ and } F_q = [p^r].$$

This implies that $[p^r]$ is purely inseparable, thus $[p]$ is purely inseparable. This contradicts the fact that E is ordinary. ($\hat{F}_p$ is separable by definition.)

Suppose $R \subseteq \mathrm{End}(E)$ commutative. So $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} = K$ is a field extension of $\mathbb{Q}$ of degree ≤ 2.

Claim: There are infinitely many prime numbers ℓ s.t. $R/\ell R$ is an integral domain.

Proof: If $R = \mathbb{Z}$, then it is ok. Suppose $K/\mathbb{Q}$ is a quadratic. Then $R \subseteq \mathcal{O}_K$ = ring of integers of K

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & R & \longrightarrow & \mathcal{O}_K & \longrightarrow & \mathcal{O}_K/R \to 0 \\
 & & \downarrow \ell & & \downarrow \ell & & \downarrow \ell \\
0 & \to & R & \longrightarrow & \mathcal{O}_K & \longrightarrow & \mathcal{O}_K/R \to 0. \\
 & & \downarrow & & \downarrow & & \\
0 & \to & R/\ell R & \to & \mathcal{O}_K/\ell & \to & \cdots
\end{array}$$

finite abelian group. $\ell \nmid \#(\mathcal{O}_K/R)$.

↑ this is injective.

So it suffices to find such an infinite set for $\mathcal{O}_K$.

Now $\mathcal{O}_K = \mathbb{Z}[x]/(f)$ ← some degree 2 polynomial w/ coeff in $\mathbb{Z}$.

f is irreducible modulo ℓ for infinitely many ℓ. □

$\mathcal{L} = \{\ell \mid \text{prime s.t } R/\ell R \text{ is a domain}\} \supset \{p\}$.
↑ in particular ℓ is not ramified

$\longrightarrow$ $R \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_\ell$ is a discrete valuation ring

$\longrightarrow$ $\varphi \in R$ can be written uniquely as $\varphi' \circ [\ell^n]$
with $\varphi' \in (R \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_\ell)^*$ $\Longrightarrow$ $T_\ell \varphi'$ is invertible
$\ell \nmid \det T_\ell \varphi' = \deg(\varphi')$.

$\Longrightarrow v_\ell(\deg \varphi) = v_\ell(\deg [\ell^n]) = 2n$ is even. (for all $\ell \in \mathcal{L}$).
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \| \ell^{2n}$

For $\ell \in \mathcal{L}$ pick an isogeny of degree ℓ (over $\overline{\mathbb{F}_p}$):

$\varphi_\ell : E \longrightarrow E_\ell$ = quotient by the subgroup generated by a point of order ℓ.

Rmk: If $\ell = \ell'$, then $E_\ell, E_{\ell'}$ are not isomorphic. Suppose they are

$$\begin{array}{ccc} E & & E \\ {\scriptstyle \varphi_\ell}\downarrow & & \downarrow{\scriptstyle \varphi_{\ell'}} \uparrow \hat{\varphi}_{\ell'} \\ E_\ell & \xrightarrow[\alpha]{} & E_{\ell'} \end{array}$$

$\deg \hat{\varphi}_{\ell'} = \ell' \Longrightarrow \deg(\underbrace{\hat{\varphi}_{\ell'} \circ \alpha \circ \varphi_\ell}_{\varphi}) = \ell\ell'$

$v_\ell(\varphi)$ is even $\Longrightarrow$ φ cannot exist.

Rmk: If E is supersingular, then E_ℓ is supersingular.

$[p]_{E_\ell} \circ \varphi_\ell = \varphi_\ell \circ [p]$

$\deg_i([p]) = p^2$.
$\qquad\qquad\quad \uparrow$ φ_ℓ is separable
$\qquad\qquad\quad \deg \varphi_\ell = \ell \neq p$.
$\deg_i([p]_{E_\ell}) = \deg([p]) = p^2 \Longrightarrow E_\ell$ is supersingular

$\deg_i(\varphi \circ \psi) = \deg_i(\varphi) \cdot$ [illegible]

E supersing $\Rightarrow \{E_\ell\}_{\ell \in L}$ is an infinite family of non-isomorphic supersingular elliptic curves.

But there are only finitely many of those. $\lightning$ $\square$

Weierstrass equation (again)

Suppose given a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

whose associated curve is not necessarily non singular.

There is a definition of Δ and j for this Weierstrass equation and it can be seen to behave as follows under transformations of the form

$$\left.\begin{aligned} x' &= u^2x + r \\ y' &= u^3y + u^2sx + t \end{aligned}\right\} \longrightarrow \begin{aligned} \Delta' &= u^{12}\Delta \\ j' &= j. \end{aligned}$$

"Simplified" Weierstrass equation

- $\mathrm{char}(k) \neq 2, 3$ then we can reduce to an equation of the form

$$y^2 = x^3 + a_4x + a_6 \qquad \left(\text{unique up to } (x,y) \mapsto (u^2x, u^3y)\right).$$

$$\Delta = -16(4a_4^3 + 27a_6^2)$$

$$j = 1728 \cdot \frac{4a_4^3}{4a_4^3 + 27a_6^2}$$

(compare this with the complex case!)

- $\mathrm{char}(k) = 3$ then we can reduce to one of the following forms:

* $y^2 = x^3 + a_4x + a_6$ $\qquad \left(\text{unique up to } (x,y) \mapsto (u^2x + r, u^3y)\right)$

$$\Delta = -a_4^3 \qquad j = 0.$$

* $y^2 = x^3 + a_2x^2 + a_6$ $\qquad \left(\text{unique up to } (x,y) \mapsto (u^2x, u^3y).\right)$

$$\Delta = -a_2^3a_6 \qquad j = -\frac{a_2^3}{a_6}$$

- $\mathrm{char}(k) = 2$ then we can reduce to the following forms:

  * $y^2 + a_3 y = x^3 + a_4 x + a_6$ — unique up to $(x,y) \mapsto (u^2x + s^2,\ u^3y + u^2sx + t)$

    $\Delta = a_4^3 \qquad j = 0$

  * $y^2 + xy = x^3 + a_2 x^2 + a_6$ — $\left(\text{unique } (x,y) \mapsto (u^2x,\ u^3y)\right)$.

    $\Delta = a_6 \qquad j = \frac{1}{a_6}$

Rmk: If the Weierstrass equation has form $y^2 = f(x)$, then $\Delta = 16\,\mathrm{disc}(f)$, and if $f(x) = (x-x_1)(x-x_2)(x-x_3)$

$$\Delta = 16\,(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2.$$

Lemma: A Weierstrass equation is non singular iff $\Delta \neq 0$.
If $\Delta = 0$, then there is a unique singular point.

Rmk: j is invariant under isomorphism of elliptic curve.
Two elliptic curves are isomorphic iff they have same j-invariant.

Rmk: If $\mathrm{char}(k) = p$, then $j(E^{(p)}) = j(E)^p$. This is because the coefficients of the W. equation of $E^{(p)}$ are the p-th power of the coefficients of that of E.

If E is supersingular, then $E^{(p)} \xrightarrow[\hat{F}_p]{} E$ is purely inseparable

$$\begin{array}{ccc} E^{(p)} & \xrightarrow{\hat{F}_p} & E \\ {\scriptstyle F_p}\downarrow{\scriptstyle p} & \nearrow_{\sim}\ {\scriptstyle 1} & \\ E^{(p^2)} & & \end{array} \quad \Longrightarrow \quad E^{(p^2)} \xrightarrow{\sim} E.$$

$$j(E^{(p^2)}) = j(E)^{p^2}$$

$$\Longrightarrow \quad j(E) \in \mathbb{F}_{p^2}.$$

In particular, there are only finitely many supersingular elliptic curves

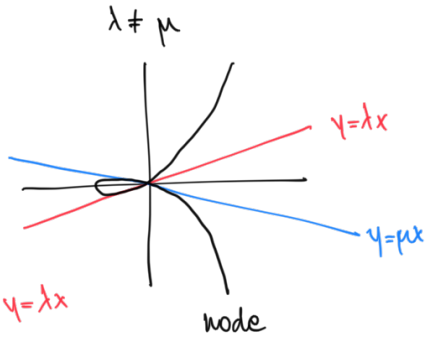
Singular Weierstrass equations: Suppose $\Delta = 0$. We can see that the W. equation can be reduced to the form (by moving the singular point to (0,0) if it is k-rational

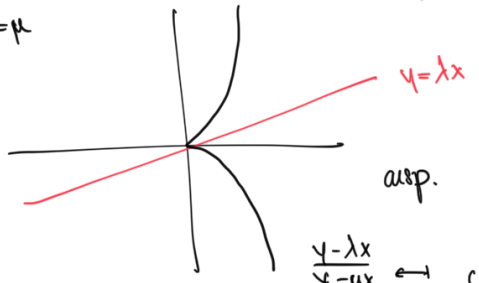
(*) $\underline{y^2 + a_1xy - a_2x^2 = x^3}$

k'/k be the splitting field of $t^2 + a_1 t - a_2$ — because it is fixed under Galois.

There are $\lambda, \mu \in k'$ s.t.

$$(y - \lambda x)(y - \mu x) = x^3$$





$$\frac{y-\lambda x}{y-\mu x} \longleftarrow (x,y)$$

- $\lambda \neq \mu$ $\quad \alpha : \mathbb{G}_m \xrightarrow{\sim} C_{reg}$ $\quad C = \{f=0\}$ in $\mathbb{P}^2$

  $\mathbb{G}_m = \mathbb{P}^1 - \{0, \infty\}$ $\quad C_{reg}$ set of regular points.

  $$t \longmapsto \left[\frac{(t-1)^3}{t(\mu-\lambda)^2} : t-1 : \mu t - \lambda\right].$$

- $\lambda = \mu$ $\quad \beta : \mathbb{A}^1 \longrightarrow C_{reg}$

  $$u \longmapsto [u^3 : u : 1 + \lambda u]$$

Lemma: There is a unique group law on $C_{reg}(\bar{k})$ s.t. $[0:0:1]$ is the neutral element and $p+q+r=e$ iff $[p]+[q]+[r]$ is the intersection of a line with C_{reg}.

Moreover, the maps α, β are group isomorphisms.

Over a non-Archimedean field

R = DVR $\quad K = \mathrm{Frac}(R)$ perfect field $\quad R \to k$, $x \mapsto \bar{x}$

k = residue perfect.

Residue map:

$$\begin{array}{ccc} \mathbb{P}^n(K) & \longrightarrow & \mathbb{P}^n(k) \\ \cup & & \\ [x_0 : \dots : x_n] & \longmapsto & [\bar{x}_0 : \dots : \bar{x}_n] \end{array}$$

($\bar{x}_i$ ← at least one of $\bar{x}_i$ is nonzero)

$x_0, \dots, x_n \in R \quad \min(v(x_0), \dots, v(x_n)) = 0.$ (← nonzero)

The valuation v can be extended to an alg. closure $\bar{K}$ of K

$$\begin{array}{ccc} \mathbb{P}^n(K) & \xrightarrow{\text{residue map}} & \mathbb{P}^n(k) \\ \downarrow & \circlearrowright & \downarrow \\ \end{array}$$

$$\begin{array}{ccc} \mathbb{P}^n(\overline{K}) & \xrightarrow{\text{residue map}} & \mathbb{P}^n(\overline{k}) \\ \cup & & \cup \\ \mathrm{Gal}(\overline{K}/K) & & \\ \cup & & \\ G = \{ g v = v \} & \longrightarrow & \mathrm{Gal}(\overline{I}/k) \end{array}$$

Reduction of a Weierstrass equation:

$\mathbb{P}^2_K \supseteq C : f(x,y) = y^2 + a_1 xy + a_3 y - (x^3 + a_2 x^2 + a_4 x + a_6)$. $a_i \in R$

$\mathbb{P}^2_k \supseteq \overline{C} : \overline{f}(x,y) = y^2 + \overline{a_1} xy + \overline{a_3} y - (x^3 - \overline{a_2} x^2 + \overline{a_4} x + \overline{a_6})$

$$\begin{array}{ccc} C(\overline{K}) & \xrightarrow{\text{red}} & \overline{C}(\overline{I}) \\ \cap & & \cap \\ \mathbb{P}^2(\overline{K}) & \xrightarrow{\text{red}} & \mathbb{P}^2(\overline{k}) \end{array}$$

Even though C is non singular, $\overline{C}$ may be singular (if $v(\Delta) > 0$ but $\Delta \neq 0$)

$C^0_{reg} = \{ x \in C_{reg} : \mathrm{red}(x) \in \overline{C}_{reg} \}$.

Lemma: C^0_{reg} is stable under the group law and

$\mathrm{red} : C^0_{reg}(\overline{K}) \longrightarrow \overline{C}_{reg}(\overline{I})$ is a group morphism.

Thm: Suppose $\overline{\Delta} \neq 0$. Then E, C and $\overline{C} = \overline{E}$ are elliptic curves.

Let $m \in \mathbb{N} \setminus \{0\}$ s.t. $\mathrm{char}(k) \nmid m$. Then

(k: residue field)

$$\mathrm{red} : E[m](\overline{K}) \longrightarrow \overline{E}[m](\overline{k})$$

is an isomorphism.

Thm (Mordell): If E is an elliptic curve over $\mathbb{Q}$, then $E(\mathbb{Q})$ is a finitely generated group.