Master Seminar – Elliptic Curves – Talk 7

Elliptic curves over finite fields

Marco Morosin

21.12.2020

Topics

- Reduction mod p and torsion points
- The number of points on $E/\mathbb{F}_q$
- The Weil conjectures
- The endomorphism ring of E/K, $\mathrm{char}(K) = p$
- Calculating the Hasse invariant

Reduction mod p and torsion points

$\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ induces:

$$y^2 = f(x) = x^3 + ax^2 + bx + c \;\; (a, b, c \in \mathbb{Z}) \implies y^2 = x^3 + \overline{a}x^2 + \overline{b}x + \overline{c}$$

elliptic curve over $\mathbb{F}_p$ iff $p \nmid \operatorname{disc}(f)$

and we have a map

$$\left\{ \left(\frac{m_1}{n_1}, \frac{m_2}{n_2} \right) \in E(\mathbb{Q}) \;\middle|\; p \nmid n_1, p \nmid n_2 \right\} \to E_p(\mathbb{F}_p), \qquad \left(\frac{m_1}{n_1}, \frac{m_2}{n_2} \right) \mapsto \left(\frac{\overline{m_1}}{\overline{n_1}}, \frac{\overline{m_2}}{\overline{n_2}} \right)$$

in particular, by the Nagell-Lutz theorem, torsion points have $\mathbb{Z}$ coordinates, so

$$\operatorname{Tors}(E(\mathbb{Q})) \to E_p(\mathbb{F}_p), \qquad \begin{aligned} P = (x, y) &\mapsto (\overline{x}, \overline{y}) = \overline{P} \\ O &\mapsto \overline{O} \end{aligned}$$

This is a group homomorphism: using explicit formulas

- $\overline{-P} = \overline{(x, -y)} = (\overline{x}, -\overline{y}) = -\overline{P}$
- $P_1 + P_2 + P_3 = O \implies \overline{P_1} + \overline{P_2} + \overline{P_3} = \overline{O}$?
  (we show it in the case of distinct points)

$x_3 = \lambda^2 - a - x_1 - x_2, \quad y_3 = \lambda x_3 + \nu \quad (y = \lambda x + \nu$ line through $P_1, P_2, P_3)$
Hence $\lambda, \nu \in \mathbb{Z}$.

$$x^3 + ax^2 + bx + c - (\lambda x - \nu)^2 = (x - x_1)(x - x_2)(x - x_3)$$
$$\implies x^3 + \overline{a}x^2 + \overline{b}x + \overline{c} - (\overline{\lambda}x - \overline{\nu})^2 = (x - \overline{x_1})(x - \overline{x_2})(x - \overline{x_3})$$

$$\overline{y_i} = \overline{\lambda}\overline{x}_i \quad \text{for } i = 1, 2, 3$$

Hence, $y = \overline{\lambda}x + \overline{\nu}$ intersects E_p at $\overline{P}_1, \overline{P}_2, \overline{P}_3$, i.e.

$$\overline{P_1} + \overline{P_2} + \overline{P_3} = \overline{O}$$

Moreover, the kernel is $\{O\}$, hence it is injective.

Conclusion

Let $E/\mathbb{Q}$: $y^2 = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$
If $p \nmid \operatorname{disc}(f)$, then the reduction modulo p map

$$\operatorname{Tors}(E(\mathbb{Q})) \to E_p(\mathbb{F}_p), \qquad \begin{aligned} P = (x, y) &\mapsto (\overline{x}, \overline{y}) = \overline{P} \\ O &\mapsto \overline{O} \end{aligned}$$

induces an isomorphism of $\operatorname{Tors}(E(\mathbb{Q}))$ onto a subgroup of $E_p(\mathbb{F}_p)$.

Example: determining $\mathrm{Tors}(E(\mathbb{Q}))$

$$E\colon y^2 = x^3 + 3$$

$\mathrm{disc}(f) = -243 = -3^5$, so for $p > 3$ $\mathrm{Tors}(E(\mathbb{Q}))$ is isomorphic to a subgroup of $E_p(\mathbb{F}_p)$.
It is easy to check that

$$\#E_p(\mathbb{F}_5) = 6 \qquad \text{and} \qquad \#E_p(\mathbb{F}_7) = 13$$

hence

$$\#\mathrm{Tors}(E(\mathbb{Q})) \mid 6 \qquad \text{and} \qquad \#\mathrm{Tors}(E(\mathbb{Q})) \mid 13$$

therefore $\#\mathrm{Tors}(E(\mathbb{Q})) = 1$.

Alternatively, using the Nagell-Lutz theorem, we should have checked the non-existence of points in $(x, y) \in E(\mathbb{Q})$ with

$$y \in \{\pm 1, \pm 3, \pm 9, \pm 27, \pm 81, \pm 243\}$$

The number of points of $E(\mathbb{F}_q)$

$E/\mathbb{F}_q$ elliptic curve, q a power of p.

$\#E(\mathbb{F}_q)$ is $1 +$ the number of solutions $(x, y) \in \mathbb{F}_q^2$ of

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

Every x gives at most two values of y. Hence $\#E(\mathbb{F}_q) \leqslant 1 + 2q$.

Theorem (Hasse)

$E/\mathbb{F}_q$ elliptic curve; we have $|\#E(\mathbb{F}_q) - q - 1| \leqslant 2\sqrt{q}$

Proof

Let $\varphi\colon E \to E$, $(x, y) \mapsto (x^q, y^q)$
$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ topologically generated by $(x \mapsto x^q)$, hence for $P \in E(\overline{\mathbb{F}}_q)$ we have

$$P \in E(\mathbb{F}_q) \iff \varphi(P) = P \qquad \text{i.e. } E(\mathbb{F}_q) = \ker(1 - \varphi)$$

We need two results:

- $E/\mathbb{F}_q$, φ its q-Frobenius; then $m + n\varphi$ is separable iff $p \nmid m$. In particular, $1 - \varphi$ is separable.
- for f nonzero isogeny, $\#f^{-1}(Q) = \deg_s f$ for all Q. In particular, if f is separable, then $\# \ker f = \deg f$

Hence, $\deg(1 - \varphi) = \# \ker(1 - \varphi) = \# E(\mathbb{F}_q)$.

$\deg\colon \operatorname{End}(E) \to \mathbb{Z}$ is a positive definite quadratic form.
$d\colon A \to \mathbb{Z}$ (A abelian group) is a positive definite quadratic form if:

- $d(f) = d(-f)$ for all $f \in A$
- the function $L(f, g) := d(f + g) - d(f) - d(g)$ is $\mathbb{Z}$-bilinear
- $d(f) \geqslant 0$ for all $f \in A$, with equality iff $f = 0$

Lemma (Cauchy-Schwarz)

A positive definite quadratic form d satisfies, for all f, g:
$|L(f, g)| \leqslant 2\sqrt{d(f)d(g)}$

In our case this would be:
$|\#E(\mathbb{F}_q) - 1 - q| = |\deg(1-\varphi) - \deg(1) - \deg(\varphi)| \leqslant 2\sqrt{\deg(\varphi)} = 2\sqrt{q}$

Proof of the Cauchy-Schwarz lemma

$d(mf) = m^2 d(f)$ follows from bilinearity of $L(f,g) = d(f+g) - d(f) - d(g)$ and from $d(f) = d(-f)$:

$$0 = L(f,0) = d(f) - d(f) - d(0) \implies d(0) = 0$$

$$-2d(mf) = L(mf,-mf) = m^2 L(f,-f) = -2m^2 d(f) \implies d(mf) = m^2 d(f)$$

Since f is positive definite:

$$0 \leqslant d(mf+ng) = m^2 d(f) + mnL(f,g) + n^2 d(g) \quad \text{for all } m,n \in \mathbb{Z}$$

Choose $m = -L(f,g)$ and $n = 2d(g)$:

$$0 \leqslant d(f)(4d(f)d(g) - L(f,g)^2)$$

if $d(f) \neq 0$, i.e. $f \neq 0$, we have $|L(f,g)| \leqslant 2\sqrt{d(f)d(g)}$
if $f = 0$: trivial.

$\square$

Application

Let $\mathrm{char}(\mathbb{F}_q) \geqslant 3$, $E/\mathbb{F}_q$ given by $E\colon y^2 = f(x)$,
$f(x)$ cubic polynomial in $\mathbb{F}_q[x]$ with distinct roots

$$x \in \mathbb{F}_q \text{ gives } \begin{cases} \text{no points on } E \text{ if } f(x) \text{ is not a square in } \mathbb{F}_q \\ 1 \text{ point } (0,0) \text{ if } f(x) = 0 \\ 2 \text{ points if } f(x) \text{ is a square in } \mathbb{F}_q^\times \end{cases}$$

$$\chi\colon \mathbb{F}_q \to \{\pm 1\} \cup \{0\}, \qquad x \mapsto \begin{cases} 1 & \text{if } x \text{ is a square in } \mathbb{F}_q^\times \\ -1 & \text{if } x \text{ is not a square in } \mathbb{F}_q^\times \\ 0 & \text{if } x = 0 \end{cases}$$

Hence $\#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q}(1 + \chi(f(x))) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(f(x))$.
By the previous estimate we get

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \leqslant 2\sqrt{q}$$

$(\chi(f(x)))_{x \in \mathbb{F}_q}$ looks like a random sequence, i.e. the values of $f(x)$ tend to be equally distributed among squares and non-squares.

Hence, $f(x)$ is a square in $\mathbb{F}_q$ for approximately $(q-1)/2$ values of x; therefore, $\#E(\mathbb{F}_q)$ is approximately

$$1 + 2\frac{q-1}{2} = 1 + q.$$

This explains intuitively the result

$$|\#E(\mathbb{F}_q) - q - 1| \leqslant 2\sqrt{q}$$

$V/\mathbb{F}_q$ projective variety

Definition (Zeta function of $V/\mathbb{F}_q$)

$$Z(V/\mathbb{F}_q;T) := \exp\left(\sum_{n=1}^{\infty}(\#V(\mathbb{F}_{q^n}))\frac{T^n}{n}\right) \in \mathbb{Q}[\![T]\!]$$

where $\exp(F(T)) := \sum_{k=0}^{\infty}\frac{F(T)^k}{k!}$

- We can recover $\#V(\mathbb{F}_{q^n}) = \frac{1}{(n-1)!}\frac{d^n}{dT^n}\log Z(V/\mathbb{F}_q;T)\,|_{T=0}$

Example (Zeta function of $\mathbb{P}^N/\mathbb{F}_q$)

$\mathbb{P}^N(\mathbb{F}_{q^n})$ are the points $[x_0 : \cdots x_N]$ with all $x_i \in \mathbb{F}_{q^n}$

- $\#\mathbb{P}^N(\mathbb{F}_{q^n}) = \frac{q^{n(N+1)}-1}{q^n-1} = \sum_{i=0}^{N} q^{ni}$
- $\log Z(\mathbb{P}^N/\mathbb{F}_q;T) = \sum_{n=1}^{\infty}\left(\sum_{i=0}^{N} q^{ni}\right)\frac{T^n}{n} = \sum_{i=0}^{N} -\log(1-q^iT)$

hence

$$Z(\mathbb{P}^N/\mathbb{F}_q;T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^NT)} \in \mathbb{Q}(T)$$

$V/\mathbb{F}_q$ smooth projective variety of dimension N

Weil Conjectures

1. (rationality): $Z(V/\mathbb{F}_q;T) \in \mathbb{Q}(T)$
2. (functional equation): there is $\varepsilon \in \mathbb{Z}$ such that

$$Z(V/\mathbb{F}_q; 1/q^N T) = \pm q^{N\varepsilon/2} T^{\varepsilon} Z(V/\mathbb{F}_q; T)$$

3. (Riemann Hypothesis):

$$Z(V/\mathbb{F}_p; T) = \frac{P_1(T)P_3(T)\cdots P_{2N-1}(T)}{P_0(T)P_2(T)\cdots\cdots P_{2N}(T)}$$

for $P_i(T) \in \mathbb{Z}[T]$ satisfying

- $P_0(T) = 1 - T$ and $P_{2N}(T) = 1 - q^N T$
- $P_i(T)$ factors over $\mathbb{C}$ as $P_i(T) = \prod_{j=1}^{\deg P_i}(1 - \alpha_{ij}T)$ where $|\alpha_{ij}| = q^{i/2}$

We will prove them for elliptic curves.

$\mathrm{End}(E) \to \mathrm{End}(T_\ell(E)), \quad \psi \mapsto \psi_\ell$

- $E \xrightarrow{\psi} E \implies E[\ell^n] \xrightarrow{\psi} E[\ell^n] \implies T_\ell(E) \xrightarrow{\psi_\ell} T_\ell(E)$ $\mathbb{Z}_\ell$-linear
- $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$; choosing a basis we can speak of $\det(\psi_\ell)$, $\mathrm{tr}(\psi_\ell)$
- Proposition: $\det(\psi_\ell) = \deg(\psi)$ and $\mathrm{tr}(\psi_\ell) = 1 + \deg(\psi) - \deg(1 - \psi)$

Theorem

$E/\mathbb{F}_q$ elliptic curve, $\varphi\colon E \to E$, $(x, y) \mapsto (x^q, y^q)$, $a := q + 1 - \#E(\mathbb{F}_q)$

1. *Consider $T^2 - aT + q$, let $\alpha, \beta \in \mathbb{C}$ be its roots. Then*

$$\beta = \overline{\alpha}, \quad |\alpha| = |\beta| = \sqrt{q}$$

and

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n \quad \text{for all } n \geqslant 1$$

2. *$\varphi^2 - a\varphi + q = 0$ in* End E

Proof of 1.

$$\det(\varphi_\ell) = \deg(\varphi) = q$$
$$\operatorname{tr}(\varphi_\ell) = 1 + \deg(\varphi) - \deg(1 - \varphi) = 1 + q - \#E(\mathbb{F}_q) = a$$

Hence the characteristic polynomial of φ_ℓ is

$$\begin{aligned}\det(T - \varphi_\ell) = T^2 - \operatorname{tr}(\varphi_\ell)T + \det(\varphi_\ell) &= T^2 - aT + q \in \mathbb{Z}[T] \\ &= (T - \alpha)(T - \beta)\end{aligned}$$

It is non-negative for all $m/n \in \mathbb{Q}$ (hence also on $\mathbb{R}$):

$$\det\left(\frac{m}{n} - \varphi_\ell\right) = \frac{\det(m - n\varphi_\ell)}{n^2} = \frac{\deg(m - n\varphi)}{n^2} \geqslant 0$$

Therefore, it has either complex conjugate roots or a double real root; in any case $\beta = \overline{\alpha}$, so $|\alpha| = |\beta|$ and

$$|\alpha|^2 = \alpha\overline{\alpha} = \alpha\beta = q$$

Proof of $\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n$ for all $n \geqslant 1$:

$$\#E(\mathbb{F}_{q^n}) = \deg(1 - \varphi^n) = \det(1 - \varphi_\ell^n)$$

Note that $\det(T - \varphi_\ell^n) = (T - \alpha^n)(T - \beta^n) = T^2 - (\alpha^n + \beta^n)T + q^n$.
Hence

$$\#E(\mathbb{F}_{q^n}) = \det(1 - \varphi_\ell^n) = 1 - \alpha^n - \beta^n + q^n$$

Proof of 2. ($\varphi^2 - a\varphi + q = 0$ in $\mathrm{End}(E)$)

$\varphi_\ell^2 - a\varphi_\ell + q = 0$ (Cayley-Hamilton).

$$\deg(\varphi^2 - a\varphi + q) = \det(\varphi_\ell^2 - a\varphi_\ell + q) = \det(0) = 0$$

hence $\varphi^2 - a\varphi + q$ is the zero map.

$\square$

Theorem (Weil conjectures for elliptic curves)

$E/\mathbb{F}_q$ elliptic curve, $a = q + 1 - \#E(\mathbb{F}_q)$, α, β roots of $T^2 - aT + q$. Then:

$$Z(E/\mathbb{F}_q; T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)} = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

and $|\alpha| = |\beta| = \sqrt{q}$. Moreover, the functional equation is satisfied with $\varepsilon = 0$:

$$Z(E/\mathbb{F}_q; 1/qT) = Z(E/\mathbb{F}_q; T)$$

Proof

$$\begin{aligned}\log Z(E/\mathbb{F}_q; T) &= \sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \frac{T^n}{n} = \sum_{n=1}^{\infty} (1 - \alpha^n - \beta^n + q^n) \frac{T^n}{n} \\ &= -\log(1-T) + \log(1-\alpha T) + \log(1-\beta T) - \log(1-qT)\end{aligned}$$

$$\text{so } Z(E/\mathbb{F}_q; T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

We already proved $|\alpha| = |\beta| = \sqrt{q}$.
$(1-\alpha T)(1-\beta T) = 1 - (\alpha+\beta)T + \alpha\beta T^2 = 1 - aT + qT^2$.
The functional equation is a direct check.

$\square$

On the Riemann Hypothesis

Set $T = q^{-s}$ for $s \in \mathbb{C}$.
The function

$$\zeta_{E/\mathbb{F}_q}(s) := Z(E/\mathbb{F}_q; q^{-s}) = \frac{(1-\alpha q^{-s})(1-\beta q^{-s})}{(1-q^{-s})(1-q^{1-s})}$$

satisfies

$$\zeta_{E/\mathbb{F}_q}(s) = \zeta_{E/\mathbb{F}_q}(1-s)$$

and moreover

$$\zeta_{E/\mathbb{F}_q}(s) = 0 \implies |q^s| = \sqrt{q} \iff \mathrm{Re}(s) = 1/2$$

The Endomorphism Ring

Theorem

K field of characteristic p, E/K elliptic curve, $\varphi_r \colon E \to E^{(p^r)}$ p^r-Frobenius, $\widehat{\varphi_r} \colon E^{(p^r)} \to E$ its dual (i.e. $\widehat{\varphi_r} \circ \varphi_r = [\deg \varphi_r]$)

1. The following are equivalent:
   1.1 $E[p^r] = 0$ for one (all) $r \geqslant 1$
   1.2 $\widehat{\varphi_r}$ is purely inseparable for one (all) $r \geqslant 1$
   1.3 $[p] \colon E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$
   1.4 $\operatorname{End}(E)$ is an order in a quaternion algebra $\mathcal{K}$, that is, a subring which is finitely generated as a $\mathbb{Z}$-module and with $\operatorname{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathcal{K}$
   1.5 The formal group $\widehat{E}/K$ associated to E has height 2. Recall: $\operatorname{ht}(\widehat{E}) \coloneqq \operatorname{ht}([p])$ is the largest h such that $[p](T)$ can be written as $g(T^{p^h})$ for some $g \in K[\![T]\!]$
2. If these conditions do not hold, then

$$E[p^r] = \mathbb{Z}/p^r\mathbb{Z} \text{ for all } r \geqslant 1 \qquad \text{and} \qquad \widehat{E}/K \text{ has height } 1$$

   If also $j(E) \in \overline{\mathbb{F}}_p$, then $\operatorname{End}(E)$ is an order of a quadratic imaginary field.

If E has one of the equivalent properties, we say it is *supersingular* or that it has *Hasse invariant 0*.
Otherwise we say E is *ordinary* or that it has *Hasse invariant 1*.

Proof of 1.

Recall that $\varphi := \varphi_1 = p$-Frobenius is purely inseparable.
(1) $\iff$ (2):

$$\#E[p^r] = \#[p^r]^{-1}(O) = \deg_s[p^r] = (\deg_s[p])^r = (\deg_s(\widehat{\varphi} \circ \varphi))^r = (\deg_s \widehat{\varphi})^r$$

(2) $\iff$ (5): So

$$\deg_i \widehat{\varphi} = \frac{\deg_i[p]}{p} = \frac{p^{\mathrm{ht}([p])}}{p} = \frac{p^{\mathrm{ht}(\widehat{E})}}{p}$$

(2) $\implies$ (3): also $[p] = \widehat{\varphi} \circ \varphi$ is purely inseparable. To show $j(E) \in \mathbb{F}_{p^2}$: factor $\widehat{\varphi} = \lambda \circ \varphi'$ with φ' p-Frobenius on $E^{(p)}$ and λ separable, in this case of degree 1.

$$\begin{tikzcd}
E^{(p)} \arrow[r, "\widehat{\varphi}"] \arrow[dr, "\varphi'"'] & E \\
& E^{(p^2)} \arrow[u, "\lambda"']
\end{tikzcd}$$

A map of degree 1 between smooth curves is an isomorphism, hence $j(E) = j(E^{(p^2)}) = j(E)^{p^2}$, so $j(E) \in \mathbb{F}_{p^2}$.

(3) $\implies$ (4) Recall: $\mathrm{End}(E)$ is either $\mathbb{Z}$, an order in an imaginary quadratic field or an order in a quaternion algebra.
So, if (4) is false, $\mathcal{K} := \mathrm{End}(E) \otimes \mathbb{Q}$ is either $\mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$.

Let E' be isogenous to E, $\psi\colon E \to E'$.
By assumption $[p] \in \mathrm{End}(E)$ purely inseparable; using $\psi \circ [p] = [p] \circ \psi$ and comparing degrees we get $[p] \in \mathrm{End}(E')$ purely inseparable, so

$$\#E'[p] = \deg_s[p] = 1$$

Using ($1 \implies 2 \implies 3$) we get $j(E') \in \mathbb{F}_{p^2}$. In particular, there are only finitely many elliptic curves isogenous to E.

Choose $\ell \in \mathbb{Z} \setminus \{p\}$ which stays prime in $\mathrm{End}(E')$ for every E' isogenous to E.

Recall $E[\ell^i] \cong \mathbb{Z}/\ell^i\mathbb{Z} \times \mathbb{Z}/\ell^i\mathbb{Z}$. Choose subgroups

$$\Phi_1 \subset \Phi_2 \subset \cdots \subset E \qquad \text{with } \Phi_i \cong \mathbb{Z}/\ell^i\mathbb{Z}$$

There is a unique elliptic curve $E_i := E/\Phi_i$ with a separable isogeny $\varphi_i \colon E \to E_i$ such that $\ker \varphi = \Phi_i$

Finitely many distinct $E_i \implies \exists\, m, n > 0$ with $E_{m+n} \cong E_m$.

$$\lambda \colon (E_m \xrightarrow{\text{proj}} E_{m+n} \cong E_m) \in \operatorname{End}(E_m)$$

$\ker \lambda = \Phi_{m+n}/\Phi_m$ cyclic of order ℓ^n

ℓ prime in $\operatorname{End}(E_m) \implies \lambda = u \circ [\ell^{n/2}]$ with $u \in \operatorname{Aut}(E_m)$

But $\ker[\ell^{n/2}] = E_m[\ell^{n/2}] \cong \mathbb{Z}/\ell^{n/2}\mathbb{Z} \times \mathbb{Z}/\ell^{n/2}\mathbb{Z}$ is not cyclic for $n > 0$, contradiction.
Hence $\operatorname{End}(E)$ is an order in a quaternion algebra.

(4) $\implies$ (2) Suppose (2) false, i.e. $\widehat{\varphi}_r$ separable for all r.
We prove $\mathrm{End}(E)$ is commutative, contradicting (4).

We show $\mathrm{End}(E) \hookrightarrow \mathrm{End}(T_p(E))$:

$$\begin{aligned} \psi \mapsto 0 &\implies \psi(E[p^r]) = 0 \text{ for all } r \geqslant 1 \\ &\implies \ker\psi \supset \ker[p^r] = \ker(\widehat{\varphi}_r \circ \varphi_r) = \varphi_r^{-1}(\ker\widehat{\varphi}_r) \\ &\implies \varphi_r(\ker\psi) \supset \ker\widehat{\varphi}_r \\ &\implies \#\ker\psi \geqslant \#\varphi_r(\ker\psi) \geqslant \#\ker\widehat{\varphi}_r \end{aligned}$$

but on the other hand $\#\ker\widehat{\varphi}_r = \deg_s\widehat{\varphi}_r = \deg\widehat{\varphi}_r = \deg\varphi_r = p^r$, so $\#\ker\psi \geqslant p^r$ for all r.
However, if $\psi \neq 0$, then $\#\psi^{-1}(O) = \deg_s\psi$ is finite. Hence, $\psi = 0$.

Recall: $T_p(E)$ is 0 or $\mathbb{Z}_p$. We are assuming (2) false, equivalently (1) false, so $E[p] \neq 0$. Then $T_p(E) = \mathbb{Z}_p$, so we conclude:

$$\mathrm{End}(E) \hookrightarrow \mathrm{End}(T_p(E)) \cong \mathrm{End}(\mathbb{Z}_p) \cong \mathbb{Z}_p$$

If the equivalent conditions do not hold, then

$$E[p^r] = \mathbb{Z}/p^r\mathbb{Z} \text{ for all } r \geqslant 1 \qquad \text{and} \qquad \widehat{E}/K \text{ has height } 1$$

Proof of 2.

$E[p^r]$ is either 0 or $\mathbb{Z}/p^r\mathbb{Z}$. Hence if (1) is false, $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geqslant 1$.

(5) does not hold $\implies$ $\mathrm{ht}(\widehat{E}) \neq 2$. Recalling that $\mathrm{ht}(\widehat{E}) \in \{1, 2\}$ for elliptic curves in positive characteristic, we conclude $\mathrm{ht}(\widehat{E}) = 1$.

We omit the proof of the following:
If, moreover, $j(E) \in \overline{\mathbb{F}}_p$, then $\mathrm{End}(E)$ is an order of a quadratic imaginary field.

Calculating the Hasse invariant

There are only finitely many supersingular elliptic curves over $\overline{\mathbb{F}}_p$ because we must have $j(E) \in \mathbb{F}_{p^2}$.

Over $\overline{\mathbb{F}}_2$: the only supersingular elliptic curve up to $\overline{\mathbb{F}}_2$-isomorphism is $E\colon y^2 + y = x^3$.

Theorem

Let $\mathbb{F}_q$ be a finite field of characteristic $p \geqslant 3$.

1. let $E/\mathbb{F}_q$ be given by $y^2 = f(x)$ for $f(x) \in \mathbb{F}_q[x]$ cubic polynomial with distinct roots. E is supersingular iff the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$ is zero
2. let $m = (p-1)/2$, define $H_p(t) := \sum_{i=0}^{m} \binom{m}{i}^2 t^i$. Let $\lambda \in \overline{\mathbb{F}}_q \setminus \{0, 1\}$. Then $E\colon y^2 = x(x-1)(x-\lambda)$ is supersingular iff $H_p(\lambda) = 0$
3. $H_p(t)$ has distinct roots in $\overline{\mathbb{F}}_q$. For $p = 3$ there is one supersingular curve; for $p \geqslant 5$ the number is given by

$$\left[\frac{p}{12}\right] + \begin{cases} 0 & \text{if } p \equiv 1 \mod 12 \\ 1 & \text{if } p \equiv 5 \mod 12 \\ 1 & \text{if } p \equiv 7 \mod 12 \\ 2 & \text{if } p \equiv 11 \mod 12 \end{cases}$$

Proof of 1.

$\chi\colon \mathbb{F}_q^\times \to \{\pm 1\}$, extend it to $\mathbb{F}_q$ by $\chi(0) = 0$.

$$\#E(\mathbb{F}_q) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(f(x))$$

Since $\mathbb{F}_q^\times$ is cyclic of order $q-1$, for any $x \in \mathbb{F}_q$ we have $\chi(x) = x^{(q-1)/2}$, hence

$$\#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} f(x)^{(q-1)/2} \quad \text{in } \mathbb{F}_q$$

Since $\mathbb{F}_q^\times$ is cyclic of order $q-1$,

$$\sum_{x \in \mathbb{F}_q} x^i = \begin{cases} -1 & \text{if } q-1 \mid i \\ 0 & \text{if } q-1 \nmid i \end{cases}$$

expanding the product $f(x)^{(q-1)/2}$, we have terms x^n for $0 \leqslant n \leqslant 3(q-1)/2$. Summing over $x \in \mathbb{F}_q$, the only nonzero term comes from x^{q-1}

$$\#E(\mathbb{F}_q) = 1 - A_q \quad \text{in } \mathbb{F}_q \text{, i.e. mod } p$$

Let $\varphi\colon E \to E$ be the q-power Frobenius,

$$\#E(\mathbb{F}_q) = \deg(1-\varphi) = 1 - a + q \qquad \text{for } a = 1 - \deg(1-\varphi) + \deg(\varphi)$$

Hence $\#E(\mathbb{F}_q) = 1 - A_q = 1 - a$ in $\mathbb{F}_q \implies a = A_q$ in $\mathbb{F}_q$.

$E/\mathbb{F}_q$, φ its q-Frobenius; then $m + n\varphi$ is separable iff $p \nmid m$
Note that $\widehat{\varphi} = [a] - \varphi$:

$$([a]-\varphi)\varphi = [a]\varphi - \varphi\varphi = [1 - \deg(1-\varphi) + \deg\varphi]\varphi - \varphi\varphi =$$
$$= \varphi - (1-\varphi)(1-\widehat{\varphi})\varphi + \varphi\widehat{\varphi}\varphi - \varphi\varphi = \varphi\varphi + \widehat{\varphi}\varphi - \varphi\varphi = [\deg\varphi]$$

hence

$$a \equiv 0 \mod p \iff \widehat{\varphi} \text{ inseparable} \iff E \text{ supersingular}$$

hence $A_q = 0 \iff E$ supersingular.
Finally, $A_q = 0 \iff A_p = 0$:

$$f(x)^{(p^{r+1}-1)/2} = f(x)^{(p^2-1)/2}(f(x)^{(p-1)/2})^{p^r}$$

$A_{p^{r+1}} = A_{p^r} A_p^{p^r}$ and we conclude by induction.

Proof of 2.

$E\colon y^2 = x(x-1)(x-\lambda)$ supersingular $\iff$ zero coefficient of x^{p-1} in

$$(x(x-1)(x-\lambda))^{(p-1)/2}$$

$\iff$ zero coefficient of $x^{(p-1)/2}$ in

$$((x-1)(x-\lambda))^{(p-1)/2}$$

Let $m := (p-1)/2$

This coefficient is

$$\sum_{i=0}^{m} \binom{m}{i} (-\lambda)^i \binom{m}{m-i} (-1)^{m-i} = (-1)^m \sum_{i=0}^{m} \binom{m}{i}^2 \lambda^i = \\ = (-1)^m H_p(\lambda)$$

hence it is zero iff $H_p(\lambda) = 0$.

Proof of 3.

Verify that

$$4t(1-t)H_p''(t) + 4(1-2t)H_p'(t) - H_p(t) = 0$$

then the only possible multiple roots in $\overline{\mathbb{F}}_q$ are $t=0$ and $t=1$ (otherwise, $H_p(\alpha) = 0 = H_p'(\alpha) \implies H_p''(\alpha) = 0$ and writing successive derivatives in terms of the above relation says that α is a zero of infinite order)

But $H_p(0) = 1$ and $H_p(1) = \binom{p-1}{m} \equiv (-1)^m \mod p$
so there are no multiple roots.

Each root λ gives a supersingular elliptic curve $E_\lambda\colon y^2 = x(x-1)(x-\lambda)$

- $p = 3$: $H_p(t) = 1 + t \implies$ only one supersingular elliptic curve
- $p \geqslant 5$: $\lambda \mapsto j(E_\lambda) = 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$ is 6:1 except over $j = 0$ (2:1) and over $j = 1728$ (3:1)

  $$j(\lambda) = j(\lambda') \implies E_\lambda \cong E_{\lambda'} \implies E_{\lambda'} \text{ supersingular} \implies H_p(\lambda') = 0$$

$\#\{$supersingular elliptic curves in characteristic $p \geqslant 5\} =$

$$\begin{aligned}
&\frac{1}{6}\left(\frac{p-1}{2} - 2\varepsilon_p(0) - 3\varepsilon_p(1728)\right) + \varepsilon_p(0) + \varepsilon_p(1728) = \\
&= \frac{p-1}{12} + \frac{2}{3}\varepsilon_p(0) + \frac{1}{2}\varepsilon_p(1728)
\end{aligned}$$

where $\varepsilon_p(j) = \begin{cases} 1 & \text{if the curve with such } j\text{-invariant } j \text{ is supersingular} \\ 0 & \text{if the curve with such } j\text{-invariant } j \text{ is ordinary} \end{cases}$

We are going to compute

$$\varepsilon_p(0) = \begin{cases} 0 & \text{if } p \equiv 1 \mod 3 \\ 1 & \text{if } p \equiv 2 \mod 3 \end{cases} \qquad \varepsilon_p(1728) = \begin{cases} 0 & \text{if } p \equiv 1 \mod 4 \\ 1 & \text{if } p \equiv 3 \mod 4 \end{cases}$$

which will conclude.

$E\colon y^2 = f(x)$, for which primes $p \geqslant 5$ is $E/\mathbb{F}_p$ supersingular?

$j = 0$: $y^2 = x^3 + 1$

Compute the coefficient of x^{p-1} in $(x^3+1)^{(p-1)/2} = \sum_{k=0}^{(p-1)/2} \binom{(p-1)/2}{k} x^{3k}$:

- for $p \equiv 2 \mod 3$: it is 0 $(3k \neq p-1)$ $\implies$ E is supersingular
- for $p \equiv 1 \mod 3$: it is $\binom{(p-1)/2}{(p-1)/3} \not\equiv 0$ $\implies$ E is ordinary

$j = 1728$: $y^2 = x^3 + x$

Compute the coefficient of x^{p-1} in $(x^3+x)^{(p-1)/2} = \sum_{k=0}^{(p-1)/2} \binom{(p-1)/2}{k} x^{\frac{4k+p-1}{2}}$:

- for $p \equiv 3 \mod 4$: it is 0 $\implies$ E is supersingular
- for $p \equiv 1 \mod 4$: it is $\binom{(p-1)/2}{(p-1)/4} \not\equiv 0$ $\implies$ E is ordinary

- if E given by a Weierstrass equation with integer coefficients has complex multiplication over $\overline{\mathbb{Q}}$, then it is supersingular for half of the primes p
- if E does not have complex multiplication, supersingular primes are rare.
  Example: $E\colon y^2 + y = x^3 - x^2 - 10x - 20$
  the only supersingular primes < 100 are 2,19,29;
  27 supersingular primes < 31500.
- for $E/\mathbb{Q}$, there are infinitely many primes such that E is ordinary
- for $E/\mathbb{Q}$ without complex multiplication, there are infinitely many supersingular primes
- for $E/\mathbb{Q}$ without complex multiplication, the set of supersingular primes has density 0, i.e. $\#\{p < x \mid E/\mathbb{F}_p \text{ is supersingular}\}/x \xrightarrow{x\to\infty} 0$; for every $\varepsilon > 0$ we have $\#\{p < x \mid E/\mathbb{F}_p \text{ is supersingular}\} \ll x^{\frac{3}{4}+\varepsilon}$
- **Conjecture**: for $E/\mathbb{Q}$ without complex multiplication, $\#\{p < x \mid E/\mathbb{F}_p \text{ is supersingular}\} \sim \frac{c\sqrt{x}}{\log x}$ for some constant $c > 0$ depending on E.