Ex. 1 Let $E/\mathbb{F}_q$ be an elliptic curve. Then

E is supersingular $\iff$ $\#E(\mathbb{F}_q) \equiv 1 \pmod p$.

Sol. $\#E(\mathbb{F}_q) = \deg(\mathrm{id} - F_q)$ because $\mathrm{id} - F_q$ is separable and $E(\mathbb{F}_q)$ is the kernel of $\mathrm{id} - F_q$.

$$[\#E(\mathbb{F}_q)] = [\deg(\mathrm{id} - F_q)] = (\mathrm{id} - F_q)(\mathrm{id} - F_q)^{\wedge} = \mathrm{id} - F_q - \hat{F}_q - \underbrace{F_q \circ \hat{F}_q}_{[q]}$$

$\uparrow$ def of dual isogeny; $(\mathrm{id} - F_q)^{\wedge} = (\hat{\mathrm{id}} - \hat{F}_q) = (\mathrm{id} - \hat{F}_q)$

Write $\#E(\mathbb{F}_q) = 1 + q - a \implies [a] = F_q + \hat{F}_q$

$\hat{F}_q = [a] - F_q$

E supersingular $\iff \hat{F}_q$ is purely inseparable

$\iff \lambda_{[a]-F_q} = a = 0$ (where $\varphi^* \omega = \lambda_\varphi \omega$ with ω an invariant diff in $\mathbb{F}_q$) □

Ex. $p > 2$, let $\chi : \mathbb{F}_q^* \to \{\pm 1\}$ be the unique character s.t. $\chi(x) = \begin{cases} 1 & \text{if } x \text{ is a square} \\ -1 & \text{otherwise} \end{cases}$. ($\chi(x) \equiv x^{\frac{q-1}{2}}$ in $\mathbb{F}_q$)

Then, $\#E(\mathbb{F}_q) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(f(x))$. where $\chi(0) = 0$.

Let E be an elliptic curve over $\mathbb{F}_q$ with equation $y^2 = f(x)$ with $f \in \mathbb{F}_q[x]$ of degree 3.

Proof. Of course we have the point $e = [0:0:1] \in E(\mathbb{F}_q)$.

The other points are of the form $(x, y) \in \mathbb{F}_q^2$ s.t.

$$y^2 = f(x).$$

Take $x \in \mathbb{F}_q$. There are 3 possibilities

$f(x) = 0 \longrightarrow$ 1 point $(x, 0)$

$1 + 0 = 1 + \chi(f(x))$

$f(x) = a^2 \neq 0$ is a square $\longrightarrow$ 2 points $(x, \pm a)$.

$1 + 1 = 1 + \chi(f(x))$

$f(x)$ is not a square $\longrightarrow$ 0 points.

is not a square $\quad 1 - \square = 1 + \chi(f(x))$

$$\Longrightarrow \quad \#E(\mathbb{F}_q) = \underbrace{1}_{\uparrow} + \sum_{x \in \mathbb{F}_q} \left(1 + \chi(f(x))\right) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(f(x))$$

$[0:0:1]$ □

Ex.3. Let $p>2$, and E an elliptic curve over $\mathbb{F}_q$ with equation

$$y^2 = f(x).$$

Then E is supersingular iff the coefficient of x^{p-1} in $f(x)^{\frac{p-1}{2}}$ is 0.

Pf: We use the previous two exercises. It suffices to show that E is supersingular iff $\sum_{x \in \mathbb{F}_q} f(x)^{\frac{q-1}{2}} = 0$ in $\mathbb{F}_q$.

$$\sum_{x \in \mathbb{F}_q} x^n = e\left(\sum_{x \in \mu_d} x\right) = e \cdot \begin{cases} 0 & \text{if } d \geq 1 \\ 1 & \text{if } d = 1. \end{cases}$$

$e = (n, q-1) \qquad d = \frac{q-1}{e} \qquad x^d - 1 = 0$

$\iff e = q-1$

$\iff q-1 \mid n$

$$\sum_{x \in \mathbb{F}_q} f(x)^{\frac{q-1}{2}} = c_q^{(q-1)} = -c_q = \text{coefficient of } x^{q-1} \text{ in } f(x)^{\frac{q-1}{2}}.$$

$f(x)$: of degree 3; $f(x)^{\frac{q-1}{2}}$: of degree $3 \cdot \frac{q-1}{2}$.

There is only one monomial of degree divisible by $q-1$: it is x^{q-1}

So $\sum_{x \in \mathbb{F}_q} f(x)^{\frac{q-1}{2}}$ vanishes iff c_q does.

$$q = p^{r+1} \qquad q-1 = p^{r+1} - p^r + p^r - 1 = p^r(p-1) + p^r - 1$$

$$f(x)^{\frac{q-1}{2}} = f(x)^{\frac{p^r-1}{2}} \left(f(x)^{\frac{p-1}{2}}\right)^{p^r}.$$

c_q = coefficient of x^{q-1} in $f(x)^{\frac{q-1}{2}}$

c_{p^r} = ——— x^{p^r-1} in $f(x)^{\frac{p^r-1}{2}}$

c_p = ——— x^{p-1} in $f(x)^{\frac{p-1}{2}}$

$c_q = c_{p^r} c_p^{p^r}$ (exercise...)

Ex. Suppose $E: y^2 = x(x-1)(x-\lambda)$. Then E is supersingular if and only if $H_p(\lambda) = \sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i}^2 \lambda^i = 0$.

Proof: By the previous exercise, it suffices to compute the coefficient of x^{p-1} in $\left(x(x-1)(x-\lambda)\right)^{\frac{p-1}{2}}$.

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

It suffices to compute the coefficient of $x^{\frac{p-1}{2}}$ in

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

$$(x-1)^{\frac{p-1}{2}} = \sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i} (-1)^{m-i} x^i \qquad m = \frac{p-1}{2}$$

$$(x-\lambda)^m = \sum_{j=0}^{m} \binom{m}{j} (-\lambda)^{m-j} x^j.$$

coefficient of x^m is

$$\sum_{i+j=m} \binom{m}{i}\binom{m}{j} (-1)^{m-(i+j)} \lambda^{m-j}$$

$j = m-i$ $\quad \binom{m}{m-i} = \binom{m}{i}$

$$= \sum_{i=0}^{m} \binom{m}{i}^2 \lambda^i \qquad \square$$

In particular, there are supersingular elliptic curves!

Ex: Let $p \geq 5$. Consider the elliptic curve

$$y^2 = x^3+1. \qquad j=0$$

Show that E is supersingular iff $p \equiv 2 \pmod 3$.

Solution: Let's compute

$m = \frac{p-1}{2}$ $\qquad (x^3+1)^{\frac{p-1}{2}} = \sum_{i=0}^{m} \binom{m}{i} x^{3i}$

We have to look at the term x^{p-1}. We look for i s.t. $3i = p-1$

This is possible iff $p \equiv 1 \pmod 3$. The coefficient of x^{p-1} in $(x^3+1)^{\frac{p-1}{2}}$ is 0 if $p \equiv 2 \pmod 3$. If $p \equiv 1 \pmod 3$, then the coefficient is $\binom{\frac{p-1}{2}}{\frac{p-1}{3}} \neq 0$ in $\mathbb{F}_p$. Therefore E is ordinary.

Then E is supersingular.

$\blacksquare$

because $a, b < p$

$$\binom{a}{b} \neq 0$$

Ex. Let $p \geq 5$. The elliptic curve $y^2 = x^3 + x$ is supersingular iff $p \equiv 3 \ (4)$. $\quad j = 1728$

Solution: Let's compute the coefficient of x^{p-1} in $(x^3+x)^{\frac{p-1}{2}}$.

$$(x^3+x)^{\frac{p-1}{2}} = x^{\frac{p-1}{2}} (x^2+1)^{\frac{p-1}{2}}$$

It suffices to compute the coefficient of $x^{\frac{p-1}{2}}$ in $(x^2+1)^{\frac{p-1}{2}}$

$m = \frac{p-1}{2}$ $\qquad (x^2+1)^m = \sum_{i=0}^{m} \binom{m}{i} x^{2i}$

- So, if $p \equiv 3 \pmod 4$ then there are non integers i s.t. $2i = \frac{p-1}{2}$. Therefore E is supersingular.
- If $p \equiv 1 \pmod 4$, then the coefficient of $x^{\frac{p-1}{2}}$ is

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \neq 0 \pmod p.$$

Thus E is ordinary.

Rmk: Let $i \in \overline{\mathbb{F}_p}$ a square root of -1. Then

$$\alpha : (x, y) \mapsto (-x, iy)$$

is an automorphism of $E: y^2 = x^3 + x$. The Frobenius F_p is an endomorphism of E:

$$(x,y) \xrightarrow{\alpha} (-x, iy) \xrightarrow{F_p} (\underbrace{(-1)^p}_{-1} x^p, i^p y^p)$$

$$(x,y) \xrightarrow{F_p} (x^p, y^p) \xrightarrow{\alpha} (-x^p, i y^p).$$

Therefore α and F_p commute if and only if $i^p = i$, that is, if and only if $i \in \mathbb{F}_p$, i.e. $p \equiv 1 \pmod 4$.

Now we know that $\overline{E}$ is supersingular iff $\mathrm{End}(\overline{E})$ is not commutative.

Let's look at $p=3$.

$$H_3(\lambda) = \sum_{i=0}^{\frac{3-1}{2}} \binom{1}{i} t^i = 1+t.$$

There is only one supersingular curve (up to iso), and it is

$$y^2 = x(x+1)(x-1) = x^3 - x.$$

Let's look at $p=2$: look at the curve

$$y^2 + y = x^3$$

Let's compute $E(\mathbb{F}_2)$:

$x=0$ $\quad y^2+y=0 \longrightarrow$ two solutions.

$x=1$ $\quad y^2+y=1 \longrightarrow$ no solutions.

$\Longrightarrow \#E(\mathbb{F}_2) = 3 \equiv 1 \pmod 2 \Longrightarrow E$ supersingular

---

The j-invariant: let k be algebraically closed, $\mathrm{char}(k) \neq 2$.

Given an elliptic curve E, we can find a Weierstrass equation of the form

$$y^2 = f(x) \qquad \deg f = 3.$$

Look at the points

$$\underbrace{([0:0:1]}_{\infty}, a, b, c) \text{ where } f(a) = f(b) = f(c) = 0.$$

2-torsion points.

Form the cross-ratio of (∞, a, b, c): $\frac{c-a}{b-a}$

[Recall that the cross of z_1, z_2, z_3, z_4 in $\mathbb{P}^1(k)$ is

$$(z_1, z_2; z_3, z_4) = \frac{(z_3 - z_1)}{(z_3 - z_2)} \cdot \frac{(z_4 - z_2)}{(z_4 - z_1)} \in \mathbb{P}^1(k)$$

$$(\infty, a, b, c) = \frac{c-a}{b-a}.$$

$a, b, c \in k$

The cross ratio is invariant under $PGL_2(k)$ and two ordered 4-tuples (made of distinct points)

pairwise

(z_1, z_2, z_3, z_4) are conjugated by $PGl_2(k)$
(z_1', z_2', z_3', z_4) iff they have same cross ratio.

The problem is that the cross ratio depends on the chosen order on the points. If $\lambda = (z_1, z_2; z_3, z_4)$, then the other cross ratios that one can obtain by permuting the elements are

$$\lambda, \ \frac{1}{\lambda}, \ 1-\lambda, \ \frac{1}{1-\lambda}, \ \frac{\lambda-1}{\lambda}, \ \frac{\lambda}{\lambda-1}.$$

Set $j(\lambda) = 256 \ \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$ is invariant under permutation of the points.

Prop. Let $z_1, \dots, z_4 \in \mathbb{P}^1(k)$ and $z_1', \dots, z_4' \in \mathbb{P}^1(k)$ be 4-tuples of pairwise distinct points.

$$\lambda = (z_1, z_2; z_3, z_4)$$

$$\lambda' = (z_1', z_2'; z_3', z_4')$$

Then $j(\lambda) = j(\lambda')$ iff $\exists \sigma \in \mathfrak{S}_4$ and $g \in PGl_2(k)$ s.t.

$$g z_i = z'_{\sigma(i)} \quad \text{for all } i = 1, \dots, 4.$$

Back to elliptic curves:

Ex: For an elliptic curve $E : y^2 = f(x)$ set

$k = \bar{k}$

$$j(E) = j(\lambda) \quad \text{where} \quad \lambda = (\infty, a; b, c)$$

a, b, c the roots of f.

Then, j is invariant under isomorphism of elliptic and sets a bijection

$$j : \{\text{elliptic curves}\}/\text{iso} \xrightarrow{\sim} k.$$

Pf: (Well-defined) We have to show that it is invariant under isomorphisms of elliptic curves

$$\varphi : E \xrightarrow[\text{iso}]{\sim} E'$$

$$y^2 = f(x) \qquad y'^2 = f'(x')$$

$x \in H^0(2[\infty]) \setminus H^0([\infty])$ and similarly here.

$y \in H^0(\mathcal{O}_E(1) \setminus H_{\text{ram}})$

$(\varphi^* y')^2 = f'(\varphi^* x')$ is a linear relation in $H^0(\mathcal{O}_E(1))$

There is only one such linear equation (up to scalar multiples)

$$(\varphi^* y')^2 - f'(\varphi^* x') = u\left[y^2 - f(x)\right]$$

(*) $\varphi^* x' = \lambda x + \mu$

$\varphi^* y' = \nu y + \underline{\rho x + \tau}$ since the coefficient of xy and y are 0 in $y^2 = f(x)$ $\rho = 0$ and $\tau = 0$.

[If the coefficient of x^2 in $f(x)$ is zero then $\mu = 0$]

a, b, c = roots of f

a', b', c' = ——— f'

$a' = \lambda a + \mu \qquad c' = \lambda c + \mu$

$\Longrightarrow \quad b' = \lambda b + \mu$

(*) up to permutation $\Longrightarrow \quad j(E) = j(E')$

(Surjective) Let's look at the curve $y^2 = x(x-1)(x-\lambda)$.

$(\infty, 0; 1; \lambda) = \dfrac{\lambda - 0}{1 - 0} = \lambda.$

Given $j \in k$ it suffices to find λ s.t.

$$256\,\frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2 (\lambda - 1)^2} = j \iff 256(\lambda^2 - \lambda + 1)^3 = j\,(\lambda - 1)^2 \lambda$$

has a solution.

(Injective) Suppose now $j(E) = j(E')$.

$E : y^2 = f(x)$ $\quad a, b, c$ roots of f

$E' : y'^2 = f'(x')$ $\quad a', b', c'$ ——— f'.

$j(E) = j(E')$ up to renaming the roots we have

$$\frac{c - a}{b - a} = \frac{c' - a'}{b' - a'} \quad (*)$$

We look λ, μ s.t.

$$\begin{cases} \lambda a + \mu = a' \\ \lambda b + \mu = b' \\ \lambda c + \mu = c' \end{cases} \longrightarrow \lambda(b-a) = b'-a' \longrightarrow \lambda(c-a) = c'-a'$$

$$\frac{c'-a'}{c-a} = \lambda = \frac{b'-a'}{b-a}$$ This is possible because of (*).

$$\mu = a' - \lambda a = a' - \frac{b'-a'}{b-a}a = \frac{1}{b-a}\left[a'b - \cancel{a'a} - b'a + \cancel{a'a}\right.$$

$$\left. a'b - bb' + bb' - b'a\right]$$

$$= b' - \frac{b'-a'}{b-a}b = b' - \lambda b$$

$$= c' - \lambda c$$

So λ, μ do the job.

Now the polynomials $f(x)$ and $f'(\lambda x + \mu)$ has the same zeroes, therefore there is $u \in k^*$ s.t.

$$f'(\lambda x + \mu) = u f(x).$$

Take $Y' = vY$ with $v^2 = u$ we have

$$(vY)^2 = f'(\lambda x + \mu) = u f(x)$$

$$\| \qquad\qquad \Longrightarrow \quad Y^2 = f(x)$$

$$v^2 Y^2$$

The transformation $(x,y) \mapsto (\lambda x + \mu, vy)$ gives an isomorphism $\varphi : E \xrightarrow{\sim} E'$. □

Let's look at the map

$$j : \mathbb{A}^1 \setminus \{0,1\} \longrightarrow \mathbb{A}^1 \quad \text{surjective.}$$

$$k \setminus \{0,1\} \qquad k$$

$$\lambda \longmapsto 256\,\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$$

I would like to compute the ramification points. For instance

$$j(\lambda) = 0 \iff (\lambda^2 - \lambda + 1)^3 = 0.$$

If $\lambda^2 - \lambda + 1 = 0$, then

So if w_1, w_2 s.t. $w_1 - w_2 \in \Lambda$

$$\mathrm{ord}_{w_i}(j) = 3$$

By Hurwitz formula:

$$\underbrace{(2g-2)}_{-2} = 6\underbrace{(2g-2)}_{-12} + \underbrace{\deg(R_j)}_{10}$$

$j^{-1}(\infty) = \{0, 1, \infty\}$ $\quad \mathrm{ord}_0(j) = \mathrm{ord}_1(j) = \mathrm{ord}_\infty(j) = 2.$

$$R_j = \underbrace{[0] + [1] + [\infty] + 2[w_1] + 2[w_2]}_{\text{degree } 7}$$

I claim that the other ramification points are over 1728:
there are 3 points $z_1, z_2, z_3 \in k$ s.t. $j(z_i) = 1728$
and $\mathrm{ord}_{z_i}(j) = 2$.

$y^2 = x^3 + 1$ $\quad j = 0$ $\quad \tau = \rho = e^{2\pi i/3}$

$y^2 = x^3 + x$ $\quad j = 1728$ $\quad \tau = i$

Exercise: Let k be a perfect field, of $\mathrm{char}(k) \neq 2$.

$$\mathcal{C}_2 = \{ (E, \alpha) : E \text{ elliptic curve over } k \}$$
$$\alpha : E[2](k) \longrightarrow (\mathbb{Z}/2\mathbb{Z})^2$$

i.e. the 2-torsion are k-rational and we fix an order on them

$(E, \alpha) \sim (E', \alpha')$ if there is an isomorphism $\varphi : E \to E'$ respecting the order on the 2-torsion points given by α and α'.

Then

$$\mathcal{C}_2/\sim \longrightarrow k - \{0,1\} \quad \text{is bijective.}$$

$$(E, \alpha) \longmapsto \text{cross ratio of } a_1, a_2, a_3.$$

∞, a_1, a_2, a_3
2-torsion points