Elliptic Curves
Example Class 2.

Q1: Can check the points:

$\pm P = (3, \pm 3)$

$\pm 2P = (10, \pm 12)$

$\pm 3P = (12, \pm 4)$

$\pm 4P = (7, \pm 11)$.

To check cyclic, must triple one of the points, check is not order 3.

To find not cyclic, e.g. $X^3 + 3X + 6$.
or just construct one with all 2-torsion points in E.

To prove only at most 2 generators required:

$\mathbb{Z}/(n_1) \times \mathbb{Z}/(n_2) \times \mathbb{Z}/(n_3)$. $n_1 | n_2 | n_3$.

Consider $p | n_1$ $(\mathbb{Z}/p)^t$

Use: $\#E[p] \leq \deg [p] = p^2$

Q2: $q: A \to \mathbb{Z}$ satisfies parm identity.

$x' = y' = 0$ $\quad q(0) = 0$

$x' = 0$ $\quad q(y) = q(-y')$.

To prove $q(nx) = n^2 q(x)$.

Do $x' = (n-1)x$, $y' = x$, and apply induction.

(need two base case $n=0$, $n=1$)

Then must prove $\langle x+y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$

(quite a messy thing to check)

- Write out what to prove. Want to show:

$$q(x+y+z) + q(x) + q(y) + q(z) = q(x+y) + q(y+z) + q(x+z).$$

Use parallelogram law 4 times

Use it with $(x+y)+z$, $(x+y)-z$

$x-y-z$ $\quad x+y-z$

$x-y-z$ $\quad x+y+z$.

Take a lin ob, write it out several times.

(Details in answer.)

Q3: Differential we want is $\frac{dx}{x} = w$

If $\lambda : x \longmapsto ax$

then $\lambda^*\left(\frac{dx}{x}\right) = \frac{d(ax)}{ax} = \frac{dx}{x}$

If $\phi : x \longmapsto x^n$

then $\phi^*\left(\frac{dx}{x}\right) = \frac{d(x^n)}{x^n} = \frac{n x^{n-1} dx}{x^n} = n\left(\frac{dx}{x}\right)$

Is w unique? If $w = f(x)\,dx$

We want: $f(ax)\,d(ax) = f(x)\,dx$

$\Rightarrow f(ax)\,a\,dx = f(x)\,dx$

$\Rightarrow a\,f(ax) = f(x)$ for all a.

Taking $x = 1$, gives $f(a) = \frac{f(1)}{a}$, thus w unique, up to a constant.

$\therefore w = \frac{c\,dx}{x}$, c constant.

QQ: $\psi : E_1 \longrightarrow E_2$] all defined over $\mathbb{F}_q$

(ψ rational function with coeff in $\mathbb{F}_q$).

$(x,y) \longmapsto (\xi(x,y), \eta(x,y))$.

ξ, η coeff in $\mathbb{F}_q$.

ϕ_i = q-power Frobenius map on E_i.

$$\begin{aligned}\phi_2 \psi(x,y) &= (\xi(x,y)^q, \eta(x,y)^q) \\ &= (\xi(x^q, y^q), \eta(x^q, y^q)) \\ &= \psi\, \phi_1 (x,y).\end{aligned}$$

Thus: $\phi_2 \circ \psi = \psi \circ \phi_1$

Why is $\xi(x,y)^q = \xi(x^q, y^q)$?

Note $\mathrm{char}(\mathbb{F}_q) = p \mid q$.

Note: If $f(x) = c_n X^n + \dots + c_0 \in \mathbb{F}_q[X]$

Then $c_i^q = c_i$ & so $f(x)^q = f(X^q)$.

When taking q^{th} powers, cross-terms disappear, note is also true for rational function (same argument as polynomial)

To prove: $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$:

$$\psi(1-\phi_1) = (1-\phi_2)\psi$$

$$\Rightarrow \deg\psi \cdot \underbrace{\deg(1-\phi_1)}_{\#E_1(\mathbb{F}_q)} = \underbrace{\deg(1-\phi_2)}_{\#E_2(\mathbb{F}_q)} \deg\psi.$$

Note, not claiming ψ is isomorphism!!

Q5: Or doesn't need all the power of Zeta functions. ϕ = 13-power Frobenius.

$$\deg(1-\phi^2) = \underbrace{\deg(1-\phi)}_{q}\deg(1+\phi)$$

Use 11th law: $\deg(1+\phi) + \underbrace{\deg(1-\phi)}_{9} = 2 + \underbrace{2\deg(\phi)}_{13}$

$\therefore$ Get 171 points

$\therefore$ Group either $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/57\mathbb{Z}$ or $\mathbb{Z}/171\mathbb{Z}$.

But need element of order 9.

$\therefore$ Cannot be $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/57\mathbb{Z}$.

Q6: Could do this using 2×2 matrices for over $\mathbb{C}$, Can do for arbitrary curves using Tate modules.

Can also do using elementary approach:

$\langle \phi, \psi \rangle = \deg(\phi+\psi) - \deg(\phi) - \deg(\psi)$.

Def: $\operatorname{tr}(\phi) = \langle \phi, 1 \rangle$.

$$\deg([n]+\phi) = \tfrac{1}{2}\langle [n]+\phi, [n]+\phi \rangle$$
$$= \deg[n] + \langle [n], \phi \rangle + \deg\phi$$
$$= n^2 + n(\operatorname{tr}\phi) + \deg\phi.$$

(i) $\operatorname{tr}(\phi+\psi) = \langle \phi+\psi, 1\rangle = \langle \phi, 1\rangle + \langle \psi, 1\rangle$
$= \operatorname{tr}\phi + \operatorname{tr}\psi.$

[Most of the work in part (ii) or (iii)]

[or deg multiplicative]

(ii) NB! Use $1-\phi^2 = (1-\phi)(1+\phi)$

$\Rightarrow \deg(1-\phi^2) = \deg(1-\phi)\deg(1+\phi)$

$\Rightarrow 1 - \operatorname{tr}(\phi^2) + \deg(\phi^2)$
$= (1 - \operatorname{tr}\phi + \deg\phi)(1 + \operatorname{tr}\phi + \deg\phi)$
$= (1+\deg(\phi))^2 - (\operatorname{tr}\phi)^2$
$= 1 + (\deg(\phi^2) + 2\deg\phi = \operatorname{tr}(\phi)^2$

$\therefore \operatorname{tr}(\phi^2) = (\operatorname{tr}\phi)^2 - 2\deg\phi.$

Q6:

(ii) Now, if trace is 0, not sufficient!!

$E/\mathbb{F}_3 : y^2 = x(x+1)(x-1)$

$\#E(\mathbb{F}_3) = 4 = p+1$

Thus, Frobenius has trace 0, but certainly not 0 map.

Now, degree of map is pos. int. Thus $\deg = 0$ implies zero map $\longrightarrow$

Lemma: If $\phi \in \mathrm{End}(E)$ & $\mathrm{tr}\,\phi = 2n$, $\deg(\phi) = n^2$, then $\phi = [n]$.

Proof: $\deg([n] - \phi) = n^2 - n\,\mathrm{tr}\,\phi + \deg\phi$

$= n^2 - n(2n) + n^2$

$= 0$ $\longrightarrow$

Thus: $[n] - \phi = 0$ $\longrightarrow$ □.

RTP: $\phi^2 - (\mathrm{tr}\,\phi)\,\phi = -(\deg\phi)$

Suffices to show:

a) $\mathrm{tr}(\phi^2 - (\mathrm{tr}\,\phi)\,\phi) = -2\deg\phi$

b) $\deg(\phi^2 - (\mathrm{tr}\,\phi)\,\phi) = (\deg\phi)^2$

a): Use (ii) & tr is linear

b) $\deg(\phi^2 - (\mathrm{tr}\,\phi)\,\phi) = (\deg\phi)\,\deg(\phi - \mathrm{tr}\,\phi)$

$(\mathrm{tr}\,\phi)^2 - (\mathrm{tr}\,\phi)^2 + \deg\phi$

Thus proves it!

Q7: Point of the question is (iii)

$\varphi: (x, y) \longmapsto (\xi, \eta)$

$E \qquad\qquad E'$

(i) To show T of order 3, verify $2T = -T$.

$y = \lambda x + \nu, \quad \lambda = \frac{\partial x^3}{\partial y} = 0 \quad \nu = \sqrt{d}.$

$x^3 = 0$

$3T = 0_E \Rightarrow T$ has order 3.

T is point of inflection.

$\xi = x(P) + x(P+T) + x(P+2T). \qquad P = (x_0, y_0).$

$y = \lambda x + \nu$

$\lambda = \frac{y_0 - \sqrt{d}}{x_0}, \quad \nu = \sqrt{d}.$

Just any chord-tangent process.

$$\left(\frac{y_0 - \sqrt{d}}{x_0}\right)^2 x^2 + \frac{2\sqrt{d}(y_0 - \sqrt{d})}{x_0} x + d = x^3 + d$$

$$x(P+T) = \left(\frac{y_0 - \sqrt{d}}{x_0}\right)^2 - x_0$$

$$x(P+2T) = \left(\frac{y_0 + \sqrt{d}}{x_0}\right)^2 - x_0$$

(ii). $\eta^2 - \xi^3 = \frac{y^2(x^3 - 8d)^2 - (x^3 + 4d)^3}{x^6} = \frac{-27dx^6}{x^6} = D.$

(iii) Consider pullback of $\frac{dx}{y}$, $\quad w = \frac{dx}{y}$.

$$\varphi^*(w) = \frac{d\xi}{d\eta} = \frac{d\left(x + \frac{4d}{x^2}\right)}{y\left(1 - \frac{8d^3}{x^3}\right)} = \frac{dx}{y}.$$

Thus $w = \frac{dx}{y}$ is invariant differential.

We can construct ξ, η based on methods to get $\phi^*(\omega) = \omega$

See: Velu formulae (his original paper was 4 pages)

What if we repeat construction:
$$d \rightsquigarrow -3^2 d \rightsquigarrow (-3^2)^2 d = 3^6 d.$$
which gives back same curve

Get dual isogeny.
(proves 'isogenous' is equivalence relation)

Q8: Now, for $Re(s) >> 0$ (sufficiently large real part) then $\zeta_k(s) = Z_E(q^{-s})$

$$Z_E(T) = \frac{1 - qT + qT^2}{(1-T)(1-qT)}.$$

$$Z_E\left(\frac{1}{qT}\right) = \ldots = Z_E(T).$$

(upto scaling by some appropriate pow of q, things are palindromic)

Can use weak form of analytic continuation to get meromorphic on $\mathbb{C}$.

Q9: Think of quadratic twists.

$E/\mathbb{F}_p$: $y^2 = f(x)$ Let $\left(\frac{u}{p}\right) = -1$.

Define: E': $uy^2 = f(x)$.

$\mathbb{F}_p^* / (\mathbb{F}_p^*)^2$

Thus, for quadratic twists, get either original curve, or twist curve E'.

Now: $\#E(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{f(x)}{p}\right)\right)$

↑ Gives 0, 1, 2 depending on cases.

$= p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p}\right)$.

$\#E'(\mathbb{F}_p) = p + 1 - \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p}\right)$

(as $\left(\frac{u}{p}\right) = -1$ instead -1).

Alternate solution: Consider Q4.

$\psi: E \xrightarrow{\sim} E'$

$(x, y) \longmapsto \left(x, \frac{1}{\sqrt{u}} y\right)$.

ϕ, ϕ' = p-power Frobenius on E, E'.

Now, Frob on E' fix $\frac{1}{\sqrt{u}}$, instead gives minus.

$\therefore \phi' \circ \psi = -\psi \circ \phi$

$\therefore \underbrace{\deg(1 - \phi')}_{\#E'(\mathbb{F}_p)} \deg \psi = \deg \psi \deg(1 + \phi)$

Use 11th law on Frobenius.

$$\deg(1-\phi) + \deg(1+\phi) = 2 + 2\deg\phi$$

$$\#E(\mathbb{F}_p) + \#E'(\mathbb{F}_p) = 2(p+1).$$

For last part $\deg(1-\phi^2) = \deg(1-\phi)\deg(1+\phi)$.
gives the result

Counter e.g.: $E/\mathbb{F}_p$: $y^2 = x(x-1)(x+1)$

$$E(\mathbb{F}_p)[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$$
$$E'(\mathbb{F}_p)[2] \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

Product of these grps has too many elems of order 2, so can't be isomphic to $E(\mathbb{F}_{p^2})$.

Note: Didn't need to pick a prime, but $p=3$ works ✓.

Q10:

(i). Use use Q.6.

(ii). ψ separable $\Rightarrow$ All but finitely many fibres have size $\deg(\psi)$. But group homo.
$\therefore$ All fibres have size $\deg(\psi)$

$\Rightarrow \#\ker(\psi) = \deg(\psi) = p$.

Note: $\phi: (x,y) \longmapsto (x^p, y^p)$] injective.

$E[p] = \ker(\phi \circ \psi) = \ker(\psi)$
(by injectivity.

$\therefore \# E[p] = p$.

For p^r, can use ψ sep $\Rightarrow \psi^r$ sep.
By similar arg with $(\phi\circ\psi)^r$, get $\# E[p^r] = p^r$.

Note: $\# E[p^r] > \# E[p^{r-1}]$.
$\therefore$ E has a point of order p^r.
$\therefore E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$.

OR: Just from $E[p] = p$, can apply structure thm:

$$E[p^r] \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z}$$
$$d_1 \mid d_2 \mid \cdots \mid d_t \mid p^r.$$

$\Rightarrow E[p] \cong (\mathbb{Z}/p\mathbb{Z})^t$ $\therefore$ $t = 1$ hypothesis
thus, p^r torsion must be cyclic.

Just use $[p]$ a surjective map, and apply

repeatedly to get part of order $p^2, p^3, \ldots$

(iii): $\psi = a - \phi$

$\psi^* w = (a - \phi)^* w = aw - \phi^* w^0$

ψ insep $\Rightarrow a \equiv 0 \pmod p$.

But, by Hasse $|a| \leq 2\sqrt{p}$, and as $p \geq 5$, this forces $a = 0$ $\longrightarrow$ D.