

Elliptic Curves - Example Sheet 2.

Proof of Claim By induction on n . Cases $n=0, 1$ ✓.
 Suppose true for $n-1$ and n .

$$\begin{array}{c} \text{1. (i)} \\ \begin{array}{c|cccccccccccccc} x & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ \hline x^3+x+5 & 5 & 7 & 2 & \textcircled{9} & 8 & 5 & 6 & \textcircled{4} & 5 & 2 & \textcircled{1} & 8 & \textcircled{3} \end{array} \\ \text{Quadratic residues mod 13 are } 1, 3, 4, 9, 10, 12. \\ \therefore \# E(\mathbb{F}_{13}) = 9. \end{array}$$

$$\begin{aligned} \text{Let } P &= (3, 3). \quad \text{Tangent line has slope } \frac{3x^2+1}{2y}|_{(3,3)} = 9 \\ \Rightarrow x(2P) &= q^2 - 2 \cdot 3 = 10 \\ -y(2P) &= 9(10-3)+3 = 1 \end{aligned} \Rightarrow 2P = (10, 12)$$

$$\begin{aligned} \text{Check joining } P &= (3, 3) \& 2P = (10, 12) \text{ has slope } \frac{12-3}{10-3} = 5 \\ \Rightarrow x(3P) &= 5^2 - 3 - 10 = 12 \\ -y(3P) &= 5(12-3) + 3 = 9 \end{aligned} \Rightarrow 3P = (12, 4)$$

Since $3P \neq \mathcal{O}$ we have $E(\mathbb{F}_{13}) \cong \mathbb{Z}/q\mathbb{Z}$ (i.e. group is cyclic)

$$\left(\text{In fact we have } \pm P = (3, \pm 3), \pm 2P = (10, \pm 12), \pm 3P = (12, \pm 4), \pm 4P = (7, \pm 11) \right)$$

$$\begin{aligned} \text{(ii)} \quad E : y^2 &= x^3 - x \text{ has } E(\mathbb{F}_{13})([2]) \cong (\mathbb{Z}/q\mathbb{Z})^2 \\ \therefore E(\mathbb{F}_{13}) &\text{ is not cyclic} \end{aligned}$$

$$\begin{aligned} \text{(iii)} \quad \text{With } E(\mathbb{F}_{13}) &\cong \mathbb{Z}/q\mathbb{Z} \times \cdots \times \mathbb{Z}/q\mathbb{Z} \quad d_1 d_2 \cdots | d_q \\ \text{pick a prime } p \mid d_1 \\ \text{then } E(\mathbb{F}_{13})[\rho] &\cong (\mathbb{Z}/p\mathbb{Z})^t \\ \text{But } \# E[\rho] &\leq \deg[\rho] = \frac{p^2}{\rho^2} \quad \therefore t \leq 2. \end{aligned}$$

$$\begin{aligned} \text{3. Let } \omega &= \frac{dx}{x}. \\ \text{If } \lambda : x &\mapsto ax \text{ then } \lambda^*(\omega) = \frac{d(ax)}{ax} = \frac{a dx}{ax} = \omega \\ \text{If } \phi : x &\mapsto x^n \text{ then } \phi^*(\omega) = \frac{d(x^n)}{x^n} = \frac{nx^{n-1} dx}{x^n} = n \omega \\ \text{Remark} \quad \text{If } f(x) dx \text{ is translation invariant then} \\ f(ax) \&d(ax) = f(n) dx \quad \forall a \in K^* \\ \Rightarrow f(ax) &= \frac{f(n)}{a} \quad \forall a \in K^* \end{aligned}$$

$$\begin{aligned} \text{2. Taking } x=y=0 \text{ shows } q(0) &= 0 \\ \text{Taking } x=0 \text{ shows } q(y) &= q(-y) \end{aligned}$$

$$\begin{aligned} \text{Claim} \quad q(nx) &= n^2 q(x) \quad \forall n \geq 0 \end{aligned}$$

$$\begin{aligned} q((n+1)x) + q((n-1)x) &= 2q(nx) + 2q(x) \\ \Rightarrow q((n+1)x) &= (2n^2 + 2 - (n-1)^2) q(x) \\ &= (n+1)^2 q(x) \end{aligned} \quad \square$$

Remains to show $(x, y) \mapsto q(x+y) - q(x) - q(y)$ is \mathbb{Z} -linear.
 $\leftarrow (x+y, 2) = (x, 2) + (y, 2)$
 $\iff q(x+y+2) - q(x+y) - q(2) = q(x+2) - q(x) - q(2) + q(y+2) - q(y) - q(2)$
 $\iff q(x+y+2) + q(x) + q(y) + q(2) = q(x+y) + q(y+2) + q(x+2)$

$$\begin{aligned} \text{By the parallelogram law we have} \\ q(x+y+2) + q(x+y-2) &= 2q(x+y) + 2q(2) \quad \text{--- (1)} \\ q(x-y-2) + q(x+y-2) &= 2q(x-2) + 2q(y) \quad \text{--- (2)} \\ q(x-y+2) + q(x+y+2) &= 2q(y+2) + 2q(x) \quad \text{--- (3)} \\ \text{--- (1) --- (2) --- (3)} \\ \frac{\text{--- (1) --- (2) --- (3)}}{2} \text{ gives} \quad q(x+y+2) - q(x+y) - q(y+2) \\ &= q(x) + q(2) - q(y) - q(x-2) \\ &= q(x+2) - q(x) - q(y) - q(2). \end{aligned}$$

$$\begin{aligned} \text{Putting } x=1 \text{ shows } f(a) &= \frac{\text{const}}{a} \\ \therefore f(n) dx &\text{ is a scalar multiple of } \omega = \frac{dx}{x}. \end{aligned}$$

4. we note that if $f(x) = c_n x^n + \dots + c_1 x + c_0 \in \mathbb{F}_q[x]$
 $c_i q = c_i \quad \forall i$, so $f(x)^q = f(x^q)$

Let $\psi : E_1 \rightarrow E_2$; $(x, y) \mapsto (\bar{\psi}(x, y), \bar{\psi}(x, y))$
 ψ defined over $\mathbb{F}_q \Rightarrow$ can take $\bar{\psi}, \bar{\psi}$ rational functions in x, y with coefficients in \mathbb{F}_q

$$\begin{aligned} \therefore \psi_2(\psi(x, y)) &= (\bar{\psi}(x, y))^4, \bar{\psi}(x, y)^q \\ &= (\bar{\psi}(x^4, y^q), \bar{\psi}(x^q, y^q)) \\ &= \psi(\bar{\psi}_1(x, y)) \\ \therefore \psi_2\psi = \psi\psi_1 &\Rightarrow \psi((1-\phi_1)\psi) = ((1-\phi_2)\psi) \\ &\Rightarrow \deg(\psi \deg((1-\phi_1))) = \deg((1-\phi_2)) \deg(\psi) \\ &\Rightarrow \#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q) \end{aligned}$$

$$\begin{aligned} 5. \text{ By the parallelogram law } \deg(1+\phi) + \deg(\underbrace{(1-\phi)}_{1/1}) &= 2 + 2 \deg \underbrace{\phi}_{1/1} \\ \therefore \deg(1+\phi) &= 19 \\ \therefore \deg(1-\phi^2) &= \deg(1-\phi) \deg(1+\phi) = 9 \times 19 = 171 \\ \therefore E'(\mathbb{F}_{171}) &\cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/57\mathbb{Z} \text{ or } \mathbb{Z}/171\mathbb{Z} \end{aligned}$$

Dual $\Rightarrow \mathbb{Z}/9\mathbb{Z}$ is a subgroup $\Rightarrow E(\mathbb{F}_{171}) \cong \mathbb{Z}/171\mathbb{Z}$

6. Let $\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$
 we know \langle , \rangle is \mathbb{Z} -linear.
 To show $\phi = \psi$ shows $\langle \phi, \phi \rangle = 2 \deg(\phi)$

$$\deg(n + \phi) = \frac{1}{2} \langle n + \phi, n + \phi \rangle = n^2 + n \langle 1, \phi \rangle + \deg \phi$$

$\deg(\phi)$ (definition)

$$\begin{aligned} (i) \quad \deg(\phi + \psi) &= \langle 1, \phi + \psi \rangle = \langle 1, \phi \rangle + \langle 1, \psi \rangle = \deg(\phi) + \deg(\psi) \\ (ii) \quad \deg((1-\phi)^2) &= \deg(1-\phi) \deg(1+\phi) \\ &\Rightarrow 1 - \deg(\phi^2) + (\deg \phi)^2 = ((1 + \deg \phi)^2 - (\deg \phi)^2) \\ &\Rightarrow \deg(\phi^2) = (\deg \phi)^2 - 2 \deg \phi \end{aligned}$$

$$\begin{aligned} (iii) \quad \text{Lemma} \quad \text{let } \phi \in \text{End}(E), \quad n \in \mathbb{Z} \\ \text{tr}(\phi) = 2n \\ \deg(\phi) = n^2 \end{aligned} \quad \Leftrightarrow \quad \phi = [n]$$

$$\begin{aligned} \text{Proof "}" \Leftarrow \text{ clear} \\ \text{ "}" \Rightarrow \quad \deg(n - \phi) = n^2 - n \text{tr}(\phi) + \deg \phi = n^2 - n(2n) + n^2 = 0 \\ \Rightarrow \phi = [n] \end{aligned}$$

$$\begin{aligned} \text{here } \phi \in \text{End}(E), \quad a = \text{tr}(\phi), \quad n = \deg(\phi) \\ \text{we claim that } \phi^2 - a\phi = -n \\ \text{By the lemma it suffices to compute the trace \& degree of LHS.} \\ \text{tr}(\phi^2 - a\phi) = (a^2 - 2n) - a^2 = -2n \quad (\text{using (ii)}) \\ \deg(\phi^2 - a\phi) = \deg \phi \deg(\phi - a) = n(a^2 - a^2 + n) = n^2 \end{aligned}$$

$$\begin{aligned} 7. \quad E : y^2 = x^3 + d \quad T = (0, \sqrt{d}) \\ (i) \quad \text{Tangent line at } T \text{ has equation } y = \sqrt{d} \\ \text{Putting } y = \sqrt{d} \text{ in equation for } E \text{ gives } x^3 = 0 \\ \therefore L \cap E = \{T\}, \text{ ie. } T \text{ has order 3.} \\ x(P+T) = \left(\frac{y - \sqrt{d}}{x}\right)^2 - x = \frac{y^2 - 2\sqrt{d}y + d - x^3}{x^2} = \frac{-2\sqrt{d}y + 2d}{x^2} \\ x(P-T) = \left(\frac{y + \sqrt{d}}{x}\right)^2 - x = \dots = \frac{2\sqrt{d}y + 2d}{x^2} \\ \therefore x(P+T) + x(P-T) + x(P-T) = \frac{x^3 + 4d}{x^2} = \frac{3}{x^2} \end{aligned}$$

$$\begin{aligned} (ii) \quad \mathcal{N}^2 = \frac{y^2(x^3 - 8d)^2}{x^6} = \frac{(x^3 + d)(x^6 - 16x^3d + 64d^2)}{x^6} \\ = \frac{x^9 - 15dx^6 + 48d^2x^3 + 64d^3}{x^6} \\ \boxed{D = -27d} \end{aligned}$$

$$\begin{aligned} (iii) \quad \Phi^* \left(\frac{dx}{y} \right) &= \frac{(x^3 + 4d)^2 - 27dx^6}{x^6} = \frac{\mathcal{N}^3 - 27d}{x^3} - 27d \\ &= \frac{\left(1 - \frac{8d}{x^3}\right)dx}{y} = \frac{dx}{y} \end{aligned}$$

(N.B. This could be used to motivate the choice of n .)

8.

$$\text{For } \operatorname{Re}(s) > 0 \text{ we have } Z_K(s) = Z_E(q^{-s}) \text{ where } Z_E(\tau) = \frac{1 - \alpha\tau + q\tau^2}{(1-\tau)(1-q\tau)}$$

The RHS is meromorphic on \mathbb{C} .

$$Z_E\left(\frac{1}{q\tau}\right) = \frac{1 - \frac{\alpha}{q\tau} + \frac{1}{q\tau^2}}{\left(1 - \frac{1}{q\tau}\right)\left(1 - \frac{1}{\tau}\right)} = \frac{q\tau^2 - \alpha\tau + 1}{(q\tau - 1)(\tau - 1)} = Z_E(\tau)$$

Part 4 a group homomorphism, so all fibres are sets of finite many $Q \in E$ be numbered. Therefore $\#\operatorname{ker}(\psi) = \deg \psi = p$

$$\therefore Z_K(1-s) = Z_E\left(\frac{1}{q^{1-s}}\right) = Z_E(q^{-s}) = \overline{Z}_K(s)$$

9. (i) Method 1

$$E: y^2 = f(x) \quad \left(\frac{dy}{dx}\right)_P = -1$$

$$\# E(F_p) = 1 + \sum_{x \in F_p} \left(1 + \left(\frac{f'(y)}{p}\right)\right) \Rightarrow \# E(\bar{F}_p) + \# E'(\bar{F}_p)$$

$$\# E'(\bar{F}_p) = 1 + \sum_{x \in \bar{F}_p} \left(1 - \left(\frac{f'(y)}{p}\right)\right) = 2(p+1)$$

Method 2 Let $\psi: E \xrightarrow{\sim} E'$ (defined over \bar{F}_{p^2})

$$\text{Let } \phi, \phi' \text{ be } p\text{-power Frobenius on } E, E'$$

Then

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

$$\Rightarrow \deg(1 - \phi') = \deg(1 + \phi)$$

Parallelogram law gives

$$\deg((1 - \phi) + \frac{\deg(1 + \phi)}{p}) = 2 + 2 \frac{\deg \phi}{p}$$

$$\# E(F_p) \# E'(\bar{F}_p) = \deg(1 - \phi) \deg(1 + \phi) = \deg(1 - \phi^2) = \# E(\bar{F}_{p^2})$$

But taking $E: y^2 = x^3 - x$ gives (for any odd prime p)

$$\begin{cases} E(\bar{F}_p)[2] \cong (\frac{4p+2}{2})^2 \\ E'(\bar{F}_p)[2] \cong (\frac{4p+2}{2})^2 \\ \vdash E(\bar{F}_{p^2}) \not\cong E(\bar{F}_p) \times E'(\bar{F}_p) \\ \vdash E(\bar{F}_{p^2}) \cong (\mathbb{Z}/p^2\mathbb{Z})^2 \end{cases}$$

10. We have $\operatorname{tr}(\phi) = a$, $\deg(\phi) = p$. $\psi = a - \phi$

$$(i) \quad \text{Quadratic } \theta \Rightarrow \phi^2 - a\phi + p = 0 \Rightarrow \phi\psi = \psi\phi = a\phi - \phi^2 = p$$

$$(ii) \quad \psi \text{ separable} \Rightarrow \#\psi^{-1}(Q) = \deg \psi \text{ for all but}$$

finitely many $Q \in E$

we also have $\deg \phi \deg \psi = p^2 \Rightarrow \deg \psi = p$.

If $O \neq P \in \operatorname{ker}(\phi)$, say $P = (x, y)$, then $(x^p, y^p) = O$ \nparallel

so $\operatorname{ker}(\phi) = O$.

By (i) we have $E[\rho] = \operatorname{ker}(\phi\psi) = \operatorname{ker}(\psi)$

by structure $\therefore E[\rho] \cong \mathbb{Z}/p^r\mathbb{Z}$

Let $0 \neq T \in E[\rho]$. Since $[p^{r-1}] : E \rightarrow E$ is surjective

we have $p^{r-1}S = T$ for some $S \in E$.

Then S has order p^r

$\therefore E[\rho] \cong \mathbb{Z}/p^r\mathbb{Z}$

(iii) $E[\rho] = 0 \Rightarrow \psi$ inseparable

$\Rightarrow 0 = \psi^*\omega = (a - \phi)^*\omega = a\omega$

$\Rightarrow a \equiv 0 \pmod{p}$

Hensel's thm $\Rightarrow |a| \leq 2\sqrt{p}$

If $p \geq 5$ then $2\sqrt{p} < p$, so $a = 0$ & $\#E(\bar{F}_p) = p+1$

11. Existence use constant a sequence of polynomials

$$g_n(x), n \geq 1 \text{ such that}$$

$$(i) \quad F(x, g_n(x)) \equiv 0 \pmod{x^{n+1}}$$

$$(ii) \quad g_{n+1}(x) \equiv g_n(x) \pmod{x^{n+1}}$$

we take $g_1(x) = -x$

then $F(x, -x) = x + \gamma + x\gamma(-\dots)$

$$\Rightarrow F(x, -x) \equiv 0 \pmod{x^2}$$

Now suppose
 $F(X, g_n(X)) \equiv cX^{n+1} \pmod{X^{n+2}}$ and $c \in R$
 let $g_{n+1}(X) = g_n(X) + bX^{n+1}$ where $b \in R$ to be chosen later.

$$\begin{aligned} F(X, g_{n+1}(X)) &= F(X, g_n(X) + bX^{n+1}) \\ &\equiv (b+c)X^{n+1} \pmod{X^{n+2}} \end{aligned}$$

Taking $b = -c$ completes the induction step.

$$\text{Now } g(X) = \lim_{n \rightarrow \infty} g_n(X) \text{ satisfies } F(X, g(X)) = 0.$$

Uniqueness Suppose $F(X, g(X)) = F(X, h(X)) = 0$.

$$\begin{aligned} \text{Then } g(X) &= F(g(X), 0) = F(g(X), P(X, h(X))) \\ &= F(P(g(X), X), h(X)) = F(O, h(X)) = h(X). \end{aligned}$$

$$\text{From : } F(x, \tau) = (1+x)(1+\tau) - 1$$

$$\text{use rule } L(X) = \frac{1}{1+X} - 1 = -X + X^2 - X^3 + \dots$$

12. Lemma For each $n \geq 1$,
 $f'(g(\tau)) g^{(n)}(\tau)$ = an integer coefficient polynomial
 in $f^{(n)}(g(\tau))$ and
 $g'(\tau), \dots, g^{(n)}(\tau)$

$$\begin{aligned} \text{Proof} \quad f(g(\tau)) &= T \\ \Rightarrow f'(g(\tau)) g'(\tau) &= 1 \end{aligned}$$

This proves the case $n=1$.

The induction step works by differentiating each side \square

Putting $\tau = 0$ we deduce

$a_1 b_n =$ an integer coefficient polynomial in
 the a_i and b_1, \dots, b_{n-1}

Since $a_i \in R^\times$ and $a_i \in R$ it follows by induction that
 all $b_n \in R$.