

## Elliptic Curves - Example Sheet 2.

$x$	0	1	2	3	4	5	6	7	8	9	10	11	12
$x^3 + x + 5$	5	7	2	9	8	5	6	4	5	2	1	8	3

Quadratic residues mod 13 are 1, 3, 4, 9, 10, 12.

$$\therefore \# E(\mathbb{F}_{13}) = 9.$$

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

Chord joining  $P = (3, 3)$  &  $2P = (10, 12)$  has slope  $\frac{12-3}{10-3} = 5$   
 $\Rightarrow x(3P) = 5^2 - 3 - 10 = 12 \quad \}$   
 $-y(3P) = 5(12-3) + 3 = 9 \quad \} \Rightarrow 3P = (12, 4)$

Since  $3P \neq 0$  we have  $E(\mathbb{F}_{13}) \cong \mathbb{Z}/9\mathbb{Z}$  (i.e. group is cyclic)  
 (In fact we have  
 $\pm P = (3, \pm 3), \pm 2P = (10, \pm 12), \pm 3P = (12, \pm 4), \pm 4P = (7, \pm 11)$ )

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

(iii) Write  $E(\mathbb{F}_{13}) \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_t\mathbb{Z}$   $d_1 | d_2 | \dots | d_t$   
 Pick a prime  $p \nmid d_i$ .

$$\text{Then } E(\mathbb{F}_{13})[p] \cong (\mathbb{Z}/p\mathbb{Z})^t$$

$$\text{But } \# E[p] \leq \deg[p] = p^2 \quad \therefore t \leq 2.$$

2. Taking  $x = y = 0$  shows  $q(0) = 0$

Taking  $x = 0$  shows  $q(y) = q(-y)$

Claim  $q(nx) = n^2 q(x) \quad \forall n \geq 0$

Proof of Claim By induction on  $n$ . Cases  $n=0, 1$  ✓.

Suppose true for  $n-1$  and  $n$ .

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

Remains to show  $(x, y) \mapsto q(x+y) - q(x) - q(y)$  is  $\mathbb{Z}$ -bilinear.

$$\begin{aligned} \langle x+y, z \rangle &= \langle x, z \rangle + \langle y, z \rangle \\ \iff q(x+y+z) - q(x+y) - q(z) &= q(x+z) - q(x) - q(z) + q(y+z) - q(y) - q(z) \\ \iff q(x+y+z) + q(x) + q(y) + q(z) &= q(x+y) + q(y+z) + q(x+z) \end{aligned}$$

By the parallelogram law we have

$$q(x+y+z) + q(x+y-z) = 2q(x+y) + 2q(z) \quad \text{--- (1)}$$

$$q(x-y-z) + q(x+y-z) = 2q(x-z) + 2q(y) \quad \text{--- (2)}$$

$$q(x-y-z) + q(x+y+z) = 2q(y+z) + 2q(x) \quad \text{--- (3)}$$

$$\frac{\text{(1)} - \text{(2)} + \text{(3)}}{2} \text{ gives } \begin{aligned} q(x+y+z) - q(x+y) - q(y+z) \\ = q(x) + q(z) - q(y) - q(x-z) \\ = q(x+z) - q(x) - q(y) - q(z). \end{aligned}$$

3. Let  $\omega = \frac{dx}{x}$ .

$$\begin{aligned} \text{If } \lambda : x \mapsto ax \text{ then } \lambda^*(\omega) &= \frac{d(ax)}{ax} = \frac{a dx}{ax} = \omega \\ \text{If } \phi : x \mapsto x^n \text{ then } \phi^*(\omega) &= \frac{d(x^n)}{x^n} = \frac{n x^{n-1} dx}{x^n} = \frac{dx}{x} = n \omega \end{aligned}$$

Remark If  $f(x) dx$  is translation invariant then

$$\begin{aligned} f(ax) d(ax) &= f(n) dx \quad \forall a \in K^* \\ \Rightarrow f(ax) &= \frac{f(x)}{a} \quad \forall a \in K^* \end{aligned}$$

$$\text{Putting } x=1 \text{ shows } f(a) = \frac{\text{const}}{a}$$

$\therefore f(n) dx$  is a scalar multiple of  $\omega = \frac{dx}{x}$ .

(N.B. This will be used to motivate the claim of (i).)

$$\frac{y}{\frac{dy}{dx}} = \frac{\frac{dy}{dx} - 1}{\frac{dy}{dx}(\frac{dy}{dx} - 1)} = (\frac{y}{\frac{dy}{dx}}) * \phi \quad (\text{iii})$$

$$D = -27x^6 = \frac{x^6}{(x^3 + 4x^2)^2 - 27x^6} =$$

$$= \frac{x^6}{x^9 - 15x^6x^3 + 48x^2x^3 + 64x^3} =$$

$$\frac{x^6}{(x^3 + 4x^2)^2} = \frac{x^6}{y^2(x^3 - 8x^2)^2} = \frac{x^6}{(x^3 + 4x^2)(x^6 - 16x^3x^2 + 64x^2)} =$$

$$\frac{x^6}{x^6} = \frac{x^6}{x^6} = x(P-T) + x(P+T) = (P-T) \quad \therefore$$

$$\frac{x^6}{2\sqrt{y+2x}} = x - \frac{x}{\sqrt{y+2x}} = (P-T) =$$

$$\frac{x^6}{2\sqrt{y+2x}} = x - \frac{x}{\sqrt{y-2\sqrt{y+2x}}} = x(P-T) =$$

$$\therefore L(E) = 3(T), \text{ i.e., } L \text{ has sum 3.}$$

Putting  $y = \sqrt{d}$  in equation for  $E$  gives

$$0 = x^3 - 3x^2 + d \quad (\because \text{ Tangent line at has equation } y = \sqrt{d})$$

$$E : y^2 = x^3 + d \quad T = (0, \sqrt{d})$$

$$\deg(\phi^2 - a\phi) = \deg \phi \deg(\phi - a) = n(a^2 - a^2 + n) = n^2$$

$$\deg(\phi^2 - a\phi) = (a^2 - 2n) - a^2 = -2n$$

By the lemma it suffices to compute the two degrees of LHS.

$$\text{we claim that } \phi^2 - a\phi = n - n = 0 \quad \text{but } \phi \in E_n(E), a = \tau(\phi), n = \deg(\phi)$$

□

$$0 = u + (n_2)u - u = \phi \deg + (\phi - n)n = (\phi - n) \deg \quad \Leftrightarrow$$

$$[u] = \phi \Leftrightarrow \left\{ \begin{array}{l} \deg(\phi) = n_2 \\ \tau(\phi) = n \end{array} \right. \quad \text{but } \deg \text{ " " } \text{and } \tau \text{ " " } \text{are}$$

$$\text{Lemmas } \log \phi \in E_n(E), n \in \mathbb{Z}$$

$$\deg \phi - \tau(\phi) = (\tau(\phi))^2 - (\deg \phi)^2 = (1 - \phi^{-1}) \deg \phi = \langle \phi, \phi \rangle - \langle \tau(\phi), \tau(\phi) \rangle = \langle \phi - \tau(\phi), \phi - \tau(\phi) \rangle = \langle \phi - \tau(\phi), \phi - \tau(\phi) \rangle \quad (\text{ii})$$

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

$$\deg(\phi) = \langle \phi, \phi \rangle \text{ since } \phi = \phi \text{ in } \mathbb{Z}-\text{linear.}$$

$$6. \log \langle \phi, \phi \rangle = \deg(\phi + \phi) - \deg(\phi) = \langle \phi, \phi \rangle - \deg(\phi)$$

$$\mathbb{Z}[L]/\pi \in E(F_{13}) \Leftarrow \text{tangents } \circ \text{ in } \mathbb{Z}[L]/\pi \Leftarrow 1^n$$

$$\mathbb{Z}[L]/\pi \rightarrow \mathbb{Z}[S]/\pi \times \mathbb{Z}[T]/\pi \in E(F_{13}) \quad \therefore$$

$$|L| = b_1 \times b_2 = (\phi + 1)\deg(\phi - 1) = (\deg(\phi) - 1)\deg(\phi) = b_1 = (\phi + 1)\deg \phi \quad \therefore$$

$$5. \text{ By the parallelism law } \deg(\phi + \phi) = 2 + 2\deg \phi$$

$$\# E_1(F_2) = \# E_2(F_2) \quad \Leftarrow$$

$$\deg \phi \deg(\phi - 1) = \deg(-\phi_1) = \deg(-\phi_2) \quad \Leftarrow$$

$$4(\phi - 1) = 4(\phi_1) \quad \Leftarrow \quad \phi^2 - 4 = \phi_1^2 \quad \therefore$$

$$(h(x_1, y_1), h(x_2, y_2)) = (h(x_1', y_1'), h(x_2', y_2')) \quad \therefore$$

$$\phi^2 \neq (x, y) \text{ with coefficients in } F_2^3$$

$$\text{if different over } F_2 \Leftrightarrow \text{sum two } \mathbb{Z}_n \text{ linear functions in}$$

$$\text{Let } \phi : E_1 \hookrightarrow E_2 : (x, y) \mapsto (h(x), h(y))$$

$$4. \text{ we note that if } f(x) = c_0 + c_1x + \dots + c_nx^n \in F_2[x]^3 \text{ then } f(x) = c_0 + c_1(x) + \dots + c_n(x)^n \in A_1$$

8. For  $\operatorname{Re}(s) \gg 0$  we have

$$\mathcal{Z}_K(s) = Z_E(q^{-s}) \text{ where } Z_E(T) = \frac{1-aT+qT^2}{(1-T)(1-qT)}$$

The RHS is meromorphic on  $\mathbb{C}$ .

$$Z_E\left(\frac{1}{qT}\right) = \frac{1 - \frac{a}{qT} + \frac{1}{qT^2}}{\left(1 - \frac{1}{qT}\right)\left(1 - \frac{1}{T}\right)} = \frac{qT^2 - aT + 1}{(qT-1)(T-1)} = Z_E(T)$$

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

9. (i) Method 1

$$\begin{aligned} E: y^2 &= f(x) \\ E': dy^2 &= f'(x) \end{aligned} \quad \left(\frac{d}{p}\right) = -1$$

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

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

Method 2 let  $\psi: E \xrightarrow{\sim} E'$  (defined over  $\mathbb{F}_{p^2}$ )  
 $(x, y) \mapsto (x, \frac{1}{\sqrt{a}}y)$

Let  $\phi, \phi'$  be the  $p$ -power Frobenius on  $E, E'$

Then  $\phi' \psi = -\psi \phi$

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

Parallelogram law gives

$$\frac{\deg(1-\phi)}{\# E(\mathbb{F}_p)} + \frac{\deg(1+\phi)}{\# E'(\mathbb{F}_p)} = 2 + \frac{2\deg\phi}{p}$$

$$\begin{aligned} \text{(ii)} \quad \# E(\mathbb{F}_p) \# E'(\mathbb{F}_p) &= \deg(1-\phi) \deg(1+\phi) \\ &= \deg(1-\phi^2) \\ &= \# E(\mathbb{F}_{p^2}) \end{aligned}$$

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

$$\begin{aligned} E(\mathbb{F}_p)[2] &\cong (4\mathbb{Z}/2\mathbb{Z})^2 \\ E'(\mathbb{F}_p)[2] &\cong (4\mathbb{Z}/2\mathbb{Z})^2 \\ E(\mathbb{F}_{p^2})[2] &\cong (7\mathbb{Z}/17\mathbb{Z})^2 \end{aligned} \Rightarrow E(\mathbb{F}_{p^2}) \not\cong E(\mathbb{F}_p) \times E'(\mathbb{F}_p)$$

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

$$\begin{aligned} \text{(i) Question 6} \Rightarrow \phi^2 - a\phi + p &= 0 \\ \Rightarrow \phi\psi = \psi\phi &= a\phi - \phi^2 = p \end{aligned}$$

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

(ii)  $\psi$  separable  $\Rightarrow \#\psi^{-1}(Q) = \deg\psi$  for all but finitely many  $Q \in E$

Point  $\psi$  a group homomorphism, so all fibres are cosets of the kernel. Therefore  $\#\ker(\psi) = \deg\psi = p$

If  $O \neq P \in \ker(\phi)$ , say  $P = (x, y)$ , then  $(x^p, y^p) = O$   $\times$   
 $\therefore \ker(\phi) = O$ .

By (i) we have  $E[p] = \ker(\phi\psi) = \ker(\psi)$   
 by structure theorem  $\therefore E[p] \cong \mathbb{Z}/p\mathbb{Z}$

$\therefore E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$  for some  $m \leq r$

Let  $O \neq T \in E[p]$ . 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  $p^r$   $\therefore E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$

$$\begin{aligned} \text{(iii)} \quad E[p] &= 0 \Rightarrow \psi \text{ inseparable} \\ &\Rightarrow 0 = \psi^* \omega = (a-\phi)^* \omega = a\omega \\ &\Rightarrow a \equiv 0 \pmod{p} \end{aligned}$$

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

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

11. Existence we construct a sequence of polynomials  $g_n(x)$ ,  $n \geq 1$  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  $g_1(X) = -X$

$$\text{Then } F(X, Y) = X + Y + XY \dots$$

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

$\forall n \in \mathbb{N}$

Since  $a_i \in \mathbb{R}^x$  and  $a_i \in \mathbb{R}$  it follows by induction that

$a_i \cdot b_n = \text{an integer without remainder in}$

$b_n$  at each  $b_{1,2}, \dots, b_{n-1}$

Putting  $T=0$  we have

The induction step works by differentiating each side  $\square$

This proves the case  $n=1$ .

$$\begin{aligned} &= f(g(T)) g'(T) = 1 \\ &\text{Hence } f(g(T)) = T \end{aligned}$$

$(T, g_1(T), \dots, g_n(T))$

in  $f^{(n)}(g(T))$  and

12. Lemma for each  $n \geq 1$ ,  $f(g(T)) g_n(T) = \text{an integer without remainder}$

$$\text{we have } L(x) = \frac{1+x}{1-x} = 1 - x + x^2 - x^3 + \dots$$

$$G_n : F(x, T) = 1 - (T+1)(x+1)$$

$$= F(f(g(x)), x, h(x)) = F(O, h(x))$$

$$\text{Therefore } g(x) = F(g(x), 0) = F(g(x), F(x, h(x)))$$

$$\text{Therefore } F(x, g(x)) = F(x, h(x)) = 0.$$

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

Therefore  $L = -C$  completes the induction step.

$$\equiv (L+C) X^{n+1} \pmod{X^{n+2}}$$

$$\text{Let } g_{n+1}(x) = g_n(x) + L \cdot X^{n+1} \text{ where } L \in \mathbb{R} \text{ to be chosen later.}$$

$$\text{Now suppose } F(x, g_n(x)) \equiv C X^{n+1} \pmod{X^{n+2}} \text{ some } C \in \mathbb{R}$$