Elliptic Curves – Example Sheet 2.

1. (i)

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 $1, 3, 4, 9, 10, 12$.
$\therefore \quad \# E(\mathbb{F}_{13}) = 9.$

Let $P = (3,3)$. Tangent line has slope $\left.\frac{3x^2+1}{2y}\right|_{(3,3)} = 9$

$$\left.\begin{aligned} \Rightarrow \quad x(2P) &= 9^2 - 2.3 = 10 \\ -y(2P) &= 9(10-3)+3 = 1 \end{aligned}\right\} \Rightarrow 2P = (10,12)$$

Chord joining $P=(3,3)$ & $2P=(10,12)$ has slope $\frac{12-3}{10-3} = 5$

$$\left.\begin{aligned} \Rightarrow \quad x(3P) &= 5^2 - 3 - 10 = 12 \\ -y(3P) &= 5(12-3)+3 = 9 \end{aligned}\right\} \Rightarrow 3P = (12,4)$$

Since $3P \neq O$ we have $E(\mathbb{F}_{13}) \cong \mathbb{Z}/9\mathbb{Z}$ (ie. 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 $E(\mathbb{F}_{13}) \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_t\mathbb{Z} \quad d_1 | d_2 | \dots | d_t$
Pick a prime $p | d_1$
Then $E(\mathbb{F}_{13})[p] \cong (\mathbb{Z}/p\mathbb{Z})^t$
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.

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

□

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

$$\langle x+y, z\rangle = \langle x, z\rangle + \langle y, z\rangle$$
$$\Leftrightarrow \quad q(x+y+z) - q(x+y) - q(z) = q(x+z) - q(x) - q(z) + q(y+z) - q(y) - q$$
$$\Leftrightarrow \quad q(x+y+z) + q(x) + q(y) + q(z) = q(x+y) + q(y+z) + q(x+z)$$

By the parallelogram laws we have

$$q(x+y+z) + q(x+y-z) = 2q(x+y) + 2q(z) \quad \text{—①}$$
$$q(x-y-z) + q(x+y-z) = 2q(x-z) + 2q(y) \quad \text{—②}$$
$$q(x-y-z) + q(x+y+z) = 2q(y+z) + 2q(x) \quad \text{—③}$$

$\frac{① - ② + ③}{2}$ gives $\quad q(x+y+z) - q(x+y) - q(y+z)$

$$\begin{aligned} &= q(x) + q(z) - q(y) - q(x-z) \\ &= q(x+z) - q(x) - q(y) - q(z). \end{aligned}$$

3. Let $\omega = \frac{dx}{x}$.
If $\lambda : x \mapsto ax$ then $\lambda^*(\omega) = \frac{d(ax)}{ax} = \frac{a\,dx}{ax} = \omega$
If $\phi : x \mapsto x^n$ then $\phi^*(\omega) = \frac{d(x^n)}{x^n} = \frac{nx^{n-1}dx}{x^n} = n\omega$

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

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

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

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

Let $\psi : E_1 \longrightarrow E_2 \ ; \ (x,y) \longmapsto \left(\xi(x,y), \eta(x,y)\right)$

ψ defined over $\mathbb{F}_q \Rightarrow$ can take ξ, η rational functions in x,y with coefficients in $\mathbb{F}_q$

$$\therefore \quad \phi_2 \psi(x,y) = \left(\xi(x,y)^q, \eta(x,y)^q\right) = \left(\xi(x^q,y^q), \eta(x^q,y^q)\right) = \psi\,\phi_1\,(x,y)$$

$$\therefore \quad \phi_2 \psi = \psi \phi_1 \Rightarrow \psi(1-\phi_1) = (1-\phi_2)\psi \Rightarrow \deg\psi \deg(1-\phi_1) = \deg(1-\phi_2) \deg\psi \Rightarrow \#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$$

5. By the parallelogram law $\deg(1+\phi) + \underbrace{\deg(1-\phi)}_{=9} = 2 + \underbrace{2\deg\phi}_{=18}$

$\therefore \deg(1+\phi) = 19$

$\therefore \deg(1-\phi^2) = \deg(1-\phi)\deg(1+\phi) = 9 \times 19 = 171$

$\therefore E(\mathbb{F}_{13^2}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/57\mathbb{Z}$ or $\mathbb{Z}/171\mathbb{Z}$

Ex 1 $\Rightarrow \mathbb{Z}/9\mathbb{Z}$ is a subgroup $\Rightarrow E(\mathbb{F}_{13^2}) \cong \mathbb{Z}/171\mathbb{Z}$

6. Let $\langle \phi, \psi \rangle = \deg(\phi+\psi) - \deg(\phi) - \deg(\psi)$
We know $\langle , \rangle$ is $\mathbb{Z}$-bilinear.
Taking $\phi = \psi$ shows $\langle \phi, \phi \rangle = 2\deg(\phi)$

$$\deg(n+\phi) = \tfrac{1}{2}\langle n+\phi, n+\phi\rangle = n^2 + n\underbrace{\langle 1, \phi\rangle}_{=\mathrm{tr}(\phi) \text{ (definition)}} + \deg\phi$$

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

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

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

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

(iii) **Lemma** Let $\phi \in \mathrm{End}(E)$, $n \in \mathbb{Z}$

$$\left.\begin{aligned}\mathrm{tr}(\phi) &= 2n \\ \deg(\phi) &= n^2\end{aligned}\right\} \iff \phi = [n]$$

Proof "$\Leftarrow$" clear

"$\Rightarrow$" $\deg(n-\phi) = n^2 - n\,\mathrm{tr}(\phi) + \deg\phi = n^2 - n(2n) + n^2 = 0$

$\Rightarrow \phi = [n]$ □

Let $\phi \in \mathrm{End}(E)$, $a = \mathrm{tr}(\phi)$, $n = \deg(\phi)$
We claim that $\phi^2 - a\phi = -n$
By the lemma it suffices to compute the trace & degree of LHS.

$\mathrm{tr}(\phi^2 - a\phi) = (a^2 - 2n) - a^2 = -2n$ (using (ii))

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

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

(i) Tangent line at T has equation $y = \sqrt{d}$
Putting $y = \sqrt{d}$ in equation for E gives $x^3 = 0$
$\therefore \ell \cap E = 3(T)$, ie. T has order 3.

$$x(P+T) = \left(\frac{y-\sqrt{d}}{x}\right)^2 - x = \frac{y^2 - 2\sqrt{d}y + d - x^3}{x^2} = \frac{-2\sqrt{d}y + 2d}{x^2}$$

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

$$\therefore \quad x(P) + x(P+T) + x(P-T) = \frac{x^3 + 4d}{x^2} = \xi$$

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

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

$$= \frac{(x^3+4d)^3 - 27dx^6}{x^6} = \xi^3 - 27d$$

$$\boxed{D = -27d}$$

(iii) $$\phi^*\left(\frac{dx}{y}\right) = \frac{\left(1 - \frac{8d}{x^3}\right)dx}{y\left(1 - \frac{8d}{x^3}\right)} = \frac{dx}{y}$$

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

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

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

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

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

$$\therefore \quad \zeta_K(1-s) = Z_E\left(\frac{1}{q^{1-s}}\right) = Z_E(q^{-s}) = \zeta_K(s)$$

9. (i) Method 1

$$E: y^2 = f(x) \qquad E': dy^2 = f(x) \qquad \left(\frac{d}{p}\right) = -1$$

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

Method 2 Let $\psi : E \xrightarrow{\sim} E'$ $\quad (x,y) \longmapsto \left(x, \frac{1}{\sqrt{d}} y\right)$ $\quad$ (defined over $\mathbb{F}_{p^2}$)

Let ϕ, ϕ' be the p-power Frobenius on E, E'

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

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

Parallelogram law gives

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

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

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

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

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

(i) Question 6 $\Rightarrow \quad \phi^2 - a\phi + p = 0$

$$\Rightarrow \quad \phi\psi = \psi\phi = a\phi - \phi^2 = p$$

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

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

But ψ 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 $(x^p, y^p) = O$ ⚡

So $\ker(\phi) = O$.

By (i) we have $E[p] = \ker(\phi\psi) = \ker(\psi)$

by structure theorem ↘ $\quad \therefore E[p] \cong \mathbb{Z}/p\mathbb{Z}$

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

Let $O \neq T \in E[p]$. Since $[p^{r-1}] : E \to E$ is surjective we have $p^{r-1} S = T$ for some $S \in E$.

Then S has order p^r $\quad \therefore E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$

(iii) $E[p] = O \Rightarrow \psi$ inseparable

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

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

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

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 $g_1(X) = -X$

Then $\quad F(X,Y) = X + Y + XY(\cdots)$

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

Now suppose $F(X, g_n(X)) \equiv cX^{n+1} \pmod{X^{n+2}}$ some $c \in R$

Let $g_{n+1}(X) = g_n(X) + bX^{n+1}$ where $b \in R$ to be chosen later.

Then $F(X, g_{n+1}(X)) = F(X, g_n(X) + bX^{n+1})$

$\equiv (b+c)X^{n+1} \pmod{X^{n+2}}$

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

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

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

Then $g(X) = F(g(X), 0) = F(g(X), F(X, h(X))$

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

$\hat{G}_m$: $F(X, Y) = (1+X)(1+Y) - 1$

we take $L(X) = \frac{1}{1+X} - 1 = -X + X^2 - X^3 + \dots$

12. Lemma For each $n \geq 1$,

$f'(g(T))\, g^{(n)}(T) =$ an integer coefficient polynomial in $f^{(i)}(g(T))$ and $g'(T), \dots, g^{(n-1)}(T)$

Proof $f(g(T)) = T$

$\Rightarrow f'(g(T))\, g'(T) = 1$

This proves the case $n = 1$.

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

Putting $T = 0$ we deduce

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

Since $a_1 \in R^\times$ and $a_i \in R$ it follows by induction that all $b_n \in R$.