MATHEMATICAL TRIPOS PART III (2023–24)

Elliptic Curves - Example Sheet 2 of 4 **T.A. Fisher**

1. Find all points defined over the field $\mathbb{F}_{13}$ of 13 elements on the elliptic curve
$$y^2 = x^3 + x + 5,$$
and show that they form a cyclic group. Find an example of an elliptic curve over $\mathbb{F}_{13}$ for which this group is not cyclic. Are there any examples where the group requires more than two generators?

2. Let A be an abelian group. Let $q : A \to \mathbb{Z}$ be a map satisfying
$$q(x+y) + q(x-y) = 2q(x) + 2q(y)$$
for all $x, y \in A$. Show that q is a quadratic form.

3. Find a translation-invariant differential ω on the multiplicative group $\mathbb{G}_m$. Show that if $[n] : \mathbb{G}_m \to \mathbb{G}_m$ is the endomorphism $x \mapsto x^n$ then $[n]^*\omega = n\omega$.

4. Let E_1 and E_2 be elliptic curves over $\mathbb{F}_q$, and let $\psi : E_1 \to E_2$ be an isogeny defined over $\mathbb{F}_q$. Let ϕ_i be the q-power Frobenius on E_i for $i = 1, 2$. Show that $\psi \circ \phi_1 = \phi_2 \circ \psi$ and deduce that $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.

5. Let $E/\mathbb{F}_{13}$ be the elliptic curve in Question 1. Without listing its elements, find the order of $E(\mathbb{F}_{13^2})$ and determine whether this group is cyclic.

6. Show that if $\phi \in \mathrm{End}(E)$ then there exists $\mathrm{tr}(\phi) \in \mathbb{Z}$ such that
$$\deg([n] + \phi) = n^2 + n\ \mathrm{tr}(\phi) + \deg(\phi)$$
for all $n \in \mathbb{Z}$. Establish the following properties:
(i) $\mathrm{tr}(\phi + \psi) = \mathrm{tr}(\phi) + \mathrm{tr}(\psi)$,
(ii) $\mathrm{tr}(\phi^2) = \mathrm{tr}(\phi)^2 - 2\deg(\phi)$,
(iii) $\phi^2 - [\mathrm{tr}(\phi)]\phi + [\deg(\phi)] = 0$.

7. Let E be the elliptic curve $y^2 = x^3 + d$. We put
$$\xi = \frac{x^3 + 4d}{x^2}, \qquad \eta = \frac{y(x^3 - 8d)}{x^3}.$$
(i) Show that $T = (0, \sqrt{d})$ is a point of order 3, and that if $P = (x, y)$ then
$$\xi = x(P) + x(P+T) + x(P+2T).$$
(ii) Verify that $\eta^2 = \xi^3 + D$ for some constant D (which you should find).
(iii) Let E' be the elliptic curve $y^2 = x^3 + D$, and $\phi : E \to E'$ the isogeny given by $(x, y) \mapsto (\xi, \eta)$. Compute $\phi^*(dx/y)$.

8. Let $E/\mathbb{F}_q$ be an elliptic curve and $K = \mathbb{F}_q(E)$. Show that ζ_K is meromorphic on $\mathbb{C}$ and satisfies the functional equation $\zeta_K(1-s) = \zeta_K(s)$.

9. Let $E/\mathbb{F}_p$ be an elliptic curve with p an odd prime. Show that there exists an elliptic curve $E'/\mathbb{F}_p$ with

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

Show further that the groups $E(\mathbb{F}_p) \times E'(\mathbb{F}_p)$ and $E(\mathbb{F}_{p^2})$ have the same order, but need not be isomorphic.

10. Let E be an elliptic curve over $\mathbb{F}_p$ (p a prime) with $\#E(\mathbb{F}_p) = p + 1 - a$, and let $\phi : E \to E$ be the p-power Frobenius, i.e. $\phi : (x, y) \mapsto (x^p, y^p)$. Let $\psi = [a] - \phi$.
(i) Show that $\phi \circ \psi = \psi \circ \phi = [p]$.
(ii) Show that if ψ is separable then $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$.
(iii) Show that if $p \geqslant 5$ and $E[p] = 0$ then $\#E(\mathbb{F}_p) = p + 1$.

11. Let $F \in R[[X, Y]]$ be a formal group over a ring R. Show that there is a unique power series $\iota(T)$ in $R[[T]]$ with $\iota(0) = 0$ and $F(T, \iota(T)) = 0$. Find $\iota(T)$ for the multiplicative formal group $\widehat{\mathbb{G}}_m$.

12. Let R be an integral domain of characteristic zero, with field of fractions K. Suppose that $f(T) = \sum_{n=1}^{\infty}(a_n/n!)T^n$ and $g(T) = \sum_{n=1}^{\infty}(b_n/n!)T^n$ are power series in $K[[T]]$ satisfying $f(g(T)) = g(f(T)) = T$. Show that if $a_1 \in R^\times$ and $a_n \in R$ for all n, then $b_n \in R$ for all n. [*Hint: You should repeatedly differentiate* $f(g(T)) = T$ *and then put* $T = 0$.]