UNIVERSITY OF CAMBRIDGE

MAMA/125, NST3AS/125, MAAS/125

MAT3

MATHEMATICAL TRIPOS Part III

Monday 10 June 2024 9:00 am to 12:00 pm

PAPER 125

ELLIPTIC CURVES

Before you begin please read these instructions carefully

Candidates have THREE HOURS to complete the written examination.

Attempt no more than **FOUR** questions.
There are **FIVE** questions in total.
The questions carry equal weight.

STATIONERY REQUIREMENTS
Cover sheet
Treasury tag
Script paper
Rough paper

SPECIAL REQUIREMENTS
None

You may not start to read the questions printed on the subsequent pages until instructed to do so by the Invigilator.

1

(a) Define the group law on an elliptic curve in terms of the chord and tangent process, and verify that it satisfies the group axioms.

(b) Let $E/\mathbb{Q}$ be the elliptic curve $y^2 + y = x^3 - 4x + 2$ with discriminant $\Delta = 1909 = 23 \cdot 83$.

(i) Let $P = (0, 1)$ and $Q = (-2, 1)$. Compute $2P$ and $P + Q$.

(ii) Compute $\#\widetilde{E}(\mathbb{F}_p)$ for $p = 3, 5, 7$.

(iii) Prove that the torsion subgroup of $E(\mathbb{Q})$ is trivial.

(iv) Find a prime p of good reduction with $\widetilde{E}(\mathbb{F}_p)$ non-cyclic, and use this to show that P and Q (as defined in (i)) are independent points of infinite order, i.e. $mP + nQ = 0$ if and only if $m = n = 0$.

2

(a) State and prove Hasse's theorem.

(b) Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 + 3$. Show that $\widetilde{E}(\mathbb{F}_p)$ has no point of order 17 for $p = 17$ and $p = 31$. In each case decide whether $\widetilde{E}(\mathbb{F}_{p^n})$ has a point of order 17 for some $n \geqslant 2$.

3

Let K be a finite extension of $\mathbb{Q}_p$ with valuation ring $\mathcal{O}_K$, uniformiser π, and residue field k. Let $n \geqslant 2$ be an integer with $p \nmid n$.

(a) What is a formal group $\mathcal{F}$ over $\mathcal{O}_K$? What is a morphism of formal groups? State and prove a condition for a morphism of formal groups to be an isomorphism. Deduce that $\mathcal{F}(\pi\mathcal{O}_K)$ has no n-torsion.

(b) Let E/K be an elliptic curve. Define the groups $E_0(K)$, $E_1(K)$ and $\widetilde{E}_{\mathrm{ns}}(k)$. Briefly outline how it follows from part (a) that there is an injective group homomorphism

$$E_0(K)[n] \to \widetilde{E}_{\mathrm{ns}}(k).$$

(c) Let $E/\mathbb{Q}$ be an elliptic curve. Prove that the set of primes of bad reduction for E and the torsion subgroup of $E(\mathbb{Q})$ are both finite. Compute these for the elliptic curve $y^2 = x^3 + 30x + 30$.

4

(a) Let L/K be a finite Galois extension, $n \geqslant 2$ an integer, and E/K an elliptic curve. Prove that if $E(L)/nE(L)$ is finite then $E(K)/nE(K)$ is finite.

(b) Let A be an abelian group, $n \geqslant 2$ an integer, and $h : A \to \mathbb{R}$ a function satisfying

(i) For any $B \in \mathbb{R}$ the set $\{P \in A : h(P) \leqslant B\}$ is finite.

(ii) There exists $c_1 \in \mathbb{R}$ such that $|h(2P) - 4h(P)| \leqslant c_1$ for all $P \in A$.

(iii) There exists $c_2 \in \mathbb{R}$ such that

$$h(P+Q) + h(P-Q) \leqslant 2h(P) + 2h(Q) + c_2$$

for all $P, Q \in A$.

Show that

$$A \text{ is finitely generated } \iff |A/nA| < \infty.$$

(c) Define the height $H(x)$ of a rational number x. Which of the conditions in (b) are satisfied if $A = (\mathbb{Q}, +)$ and $h(x) = \log H(x)$? Justify your answer.

5

Let $d \geqslant 1$ be an integer. Let E be the elliptic curve $\{u^3 + dv^3 = w^3\} \subset \mathbb{P}^2$ with $0_E = (1:0:1)$ and E' the elliptic curve $y^2 + dy = x^3$ with $0_{E'}$ the point at infinity.

(a) What is an isogeny of elliptic curves? Show that $\phi : E \to E'$; $(u, v, w) \mapsto (\frac{uw}{v^2}, \frac{u^3}{v^3})$ is an isogeny of degree 3.

(b) When is a divisor on an elliptic curve principal? Find $0 \neq T \in E'(\mathbb{Q})$, and $f \in \mathbb{Q}(E')$, $g \in \mathbb{Q}(E)$ such that $\operatorname{div}(f) = 3(T) - 3(0)$ and $\phi^* f = g^3$. Deduce that T is in the kernel of the dual isogeny $\widehat{\phi} : E' \to E$.

(c) Show that there is a group homomorphism $\alpha : E'(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^3$ with kernel $\phi E(\mathbb{Q})$. Give an explicit formula for α and use it to show that $\operatorname{Im}(\alpha) \subset \mathbb{Q}(S, 3)$ where S is the set of primes dividing d. Deduce that if $d = 1$ then $\phi : E(\mathbb{Q}) \to E'(\mathbb{Q})$ is surjective.

[*The long exact sequence of Galois cohomology, properties of the Weil pairing, and Hilbert's theorem 90 may be assumed without proof. It may help to note that* $\alpha(T) = \alpha(-T)^{-1}$.]

END OF PAPER