UNIVERSITY OF CAMBRIDGE

MAMA/125, NST3AS/125, MAAS/125

MAT3

MATHEMATICAL TRIPOS Part III

Wednesday 11 June 2025 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) State and prove Hasse's theorem for an elliptic curve $E/\mathbb{F}_p$. [Any general results about isogenies or quadratic forms may be quoted without proof provided you state them clearly.]

(b) Define the zeta function $Z_E(T)$ as a power series. Explain how your answer to (a) can be used to compute it as a rational function.

(c) Find all primes p for which there exists an elliptic curve $E/\mathbb{F}_p$ with $E(\mathbb{F}_p) = E(\mathbb{F}_{p^2})$.

2 (a) Define a *formal group* and an *isomorphism of formal groups*. State and prove a result classifying formal groups up to isomorphism over a field of characteristic zero.

(b) Let $E/\mathbb{Q}$ be the elliptic curve with equation $y^2 = x^3 + x + 1$. Show that if $P = (0, 1)$ then $v_2(x(2^m P)) = -2m$ for all integers $m \geqslant 1$.

Define the subgroups $E_r(\mathbb{Q}_p) \subset E(\mathbb{Q}_p)$ for all $r \geqslant 1$. Then show for this specific elliptic curve that $E_1(\mathbb{Q}_p) \cong (\mathbb{Z}_p, +)$ for all primes p. [Hint: When $p = 2$ it may help to compute the kernel and image of the multiplication-by-2 map on $E_1(\mathbb{Q}_2)$.]

[Any results you need about formal groups, additional to those in (a), should be clearly stated.]

3 (a) Let E be an elliptic curve. Prove that E is isomorphic to a curve in Weierstrass form via an isomorphism taking O_E to $(0 : 1 : 0)$.

(b) Let $C = \{u^3 + v^3 + w^3 = 0\} \subset \mathbb{P}^2$ and $O_C = (1 : -1 : 0)$. Find the points of inflection on C and hence find a quadratic field K such that $C(K)[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$.

(c) Explain by quoting properties of the Weil pairing why the quadratic field K you found in (b) is the only one that could possibly have worked. Show also that if p and ℓ are primes and $E/\mathbb{F}_p$ is an elliptic curve with $E(\mathbb{F}_p)[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ then $\#E(\mathbb{F}_p) = 1 + p - a$ with $a \equiv 2 \pmod{\ell}$.

(d) Put the elliptic curve $C/\mathbb{Q}$ in (b) in Weierstrass form. Let $p \neq 3$ be a prime. Show that C has good reduction at p and that $\widetilde{C}(\mathbb{F}_p)$ is cyclic if and only if $p \equiv 2 \pmod{3}$.

4 Let K be a number field and $n \geqslant 2$ an integer.

(a) Suppose that $\mu_n \subset K$. Let $\Delta \subset K^*/(K^*)^n$ be a finite subgroup and let L be the composite of all fields $K(\sqrt[n]{x})$ for $x(K^*)^n \in \Delta$. Define a pairing

$$\mathrm{Gal}(L/K) \times \Delta \to \mu_n.$$

Show that your pairing is well defined, bilinear and non-degenerate.

(b) Suppose that E/K is an elliptic curve with $E[n] \subset E(K)$. Let $\Gamma \subset E(K)/nE(K)$ be a finite subgroup and let L be the composite of all fields $K([n]^{-1}P)$ for $P+nE(K) \in \Gamma$. Define a pairing

$$\mathrm{Gal}(L/K) \times \Gamma \to E[n].$$

Show that your pairing is well defined, bilinear and non-degenerate.

(c) Let S be a finite set of primes of K. Define the group $K(S,n)$ and prove that $|K(S,n)| \leqslant n^{|S|+c}$ where c is a constant depending only on K.

(d) Show that in (b) we have $|\Gamma| \leqslant |K(S,n)|^2$ where S is a finite set of primes you should specify. [Results from Kummer theory, or about elliptic curves over local fields, may be quoted without proof provided that you state them clearly.]

5 (a) Describe the method of descent by 2-isogeny for computing the rank of an elliptic curve. Briefly discuss the limitations of the method.

(b) Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 + 13x^2 + 11x$.

(i) Let $P = (1,5)$ and $Q = (-1,1)$. Compute the points $2P$ and $P+Q$. Show that if $(x,y) \in E(\mathbb{Q})_{\mathrm{tors}}$ with $x \neq 0$ then $(11/x, -11y/x^2) \in E(\mathbb{Q})_{\mathrm{tors}}$.

(ii) Find integers $d_1, d_2 \geqslant 1$ and $r \geqslant 0$ such that $E(\mathbb{Q}) \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \mathbb{Z}^r$.

END OF PAPER