UNIVERSITY OF CAMBRIDGE

MAMA/125, NST3AS/125, MAAS/125

MAT3

MATHEMATICAL TRIPOS Part III

Thursday 11 June 09.00am to 12.00pm

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) What is a formal group law over a ring R? Let $\mathcal{F}/R$ and $\mathcal{G}/R$ be formal groups over R, with formal group laws F and G respectively. What is a homomorphism $\theta : \mathcal{F} \to \mathcal{G}$? Show that if $\theta : \mathcal{F} \to \mathcal{G}$ is a homomorphism satisfying $\theta'(0) \in R^\times$ then θ is an isomorphism.

(b) Let p be a prime and let $E/\mathbb{Q}_p$ be an elliptic curve. What is a minimal Weierstrass equation for E? Define the reduction map $E(\mathbb{Q}_p) \to \overline{E}(\mathbb{F}_p)$.

(c) Define subgroups $E_r(\mathbb{Q}_p)$ of $E(\mathbb{Q}_p)$ for all $r \geqslant 0$ and describe (without proof) each of the quotients $E_r(\mathbb{Q}_p)/E_{r+1}(\mathbb{Q}_p)$. [*You do not need to prove that the* $E_r(\mathbb{Q}_p)$ *you define are subgroups.*]

(d) Let $E/\mathbb{Q}$ be an elliptic curve and let $n \geqslant 1$ be an integer. Show that

$$\frac{\#E(\mathbb{R})/nE(\mathbb{R})}{\#E(\mathbb{R})[n]} \cdot \prod_{p \text{ prime}} \frac{\#E(\mathbb{Q}_p)/nE(\mathbb{Q}_p)}{\#E(\mathbb{Q}_p)[n]} = 1.$$

2 Let $E/\mathbb{F}_p$ be an elliptic curve.

(a) Define the trace of an endomorphism ϕ of E. Show that $\operatorname{tr}(\phi^2) = \operatorname{tr}(\phi)^2 - 2\deg(\phi)$. Show further that $\phi^2 - [\operatorname{tr}(\phi)]\phi + [\deg(\phi)] = 0$. [*You may assume that* $\deg : \operatorname{End}(E) \to \mathbb{Z}$ *is a quadratic form.*]

(b) State and prove a formula for the number of points on E over finite extensions of $\mathbb{F}_p$.

(c) Let $E/\mathbb{F}_3$ be the elliptic curve $y^2 = x^3 - x$.

(i) Let $i \in \overline{\mathbb{F}}_3$ be a square root of -1 and let α be the automorphism of E sending (x, y) to $(-x, iy)$, which is defined over $\mathbb{F}_9$ and satisfies $\alpha^2 = [-1]$. Let ℓ be a prime with $\ell \equiv 3 \pmod 4$. Show that if $P \in E$ is a point of order ℓ, then P and $\alpha(P)$ are $\mathbb{F}_\ell$-linearly independent.

(ii) Determine the degree of the field extension $\mathbb{F}_3(E[11])/\mathbb{F}_3$.

3 (a) Define the height $H(P)$ of a point $P \in \mathbb{P}^1(\mathbb{Q})$. Show that if $\Phi : \mathbb{P}^1 \to \mathbb{P}^1$ is a morphism of degree d, defined over $\mathbb{Q}$, then there exist constants $c_1, c_2 > 0$ such that

$$c_1 H(P)^d \leqslant H(\Phi(P)) \leqslant c_2 H(P)^d.$$

(b) Let $E/\mathbb{Q} : y^2 = x^3 + ax + b$ be an elliptic curve. Define the canonical height $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$, checking carefully that any limits involved exist.

[*You may assume that there is a morphism* $\Phi : \mathbb{P}^1 \to \mathbb{P}^1$ *of degree* 4*, defined over* $\mathbb{Q}$*, such that the diagram*

$$\begin{tikzcd} E \arrow[r, "{[2]}"] \arrow[d, "x"] & E \arrow[d, "x"] \\ \mathbb{P}^1 \arrow[r, "\Phi"] & \mathbb{P}^1 \end{tikzcd}$$

commutes.]

(c) The *regulator* $\mathrm{Reg}(E/\mathbb{Q})$ of $E/\mathbb{Q}$ is defined as follows. Let $P_1, ..., P_n \in E(\mathbb{Q})$ be points whose images (under the quotient map) give a $\mathbb{Z}$-basis for $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$. Then $\mathrm{Reg}(E/\mathbb{Q})$ is the determinant of the $n \times n$ matrix with (i, j) entry

$$\langle P_i, P_j \rangle := \hat{h}(P_i + P_j) - \hat{h}(P_i) - \hat{h}(P_j).$$

Show that $\mathrm{Reg}(E/\mathbb{Q})$ is independent of the choice of $P_1, ..., P_n$. Show further that if E' is an elliptic curve over $\mathbb{Q}$, and if $\phi : E \to E'$ is an isogeny defined over $\mathbb{Q}$, then there exists $d \in \mathbb{Q}^\times$ such that

$$\mathrm{Reg}(E'/\mathbb{Q}) = d^2 \deg(\phi)^{\mathrm{rk}(E/\mathbb{Q})} \mathrm{Reg}(E/\mathbb{Q}).$$

[*You may assume that* $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ *is a quadratic form and that* $\hat{h}(\phi(P)) = \deg(\phi)\hat{h}(P)$ *for all* $P \in E(\mathbb{Q})$*.*]

4 (a) Let K be a number field, let E/K be an elliptic curve and let $n \geqslant 2$. Suppose that $\mu_n \subseteq K$ and $E[n] \subseteq E(K)$. Show that $E(K)/nE(K)$ is finite.

[*Any results about elliptic curves over local fields may be quoted without proof. You may also assume a result concerning the finiteness of the number of extensions of* K *with specified properties, provided that you state it clearly.*]

(b) Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 + x^2 + 7x$. Show that $E(\mathbb{Q})$ is finite and determine its elements.

[*Hint: while you may not use this fact without proof, it may be helpful to know in advance that* $\#E(\mathbb{Q}) = 6$*.*]

5 Let K be an algebraically closed field of characteristic 0. Let E and E' be elliptic curves over K and let $\phi : E \to E'$ be an isogeny.

(a) Show that the associated field extension $K(E)/K(E')$ is Galois with

$$\mathrm{Gal}(K(E)/K(E')) \cong E[\phi].$$

[*Facts from algebraic geometry may be assumed without proof, provided they are stated clearly. You may assume that ϕ is a homomorphism.*]

(b) Let $n = \deg(\phi)$ and denote by $\hat{\phi} : E' \to E$ the dual isogeny. Define a map

$$E'[\hat{\phi}] \longrightarrow \frac{K(E')^{\times} \cap K(E)^{\times n}}{K(E')^{\times n}}$$

and prove that it is a well-defined, injective homomorphism. Define the Weil pairing $e_\phi : E[\phi] \times E'[\hat{\phi}] \to \mu_n$ and give an explicit formula for it.

[*Denote by $\eta : E \to \mathrm{cl}^0(E)$ the map given by $P \mapsto [(P) - (0)]$ and denote by η' the corresponding map for E'. You may assume that η and η' are isomorphisms of abelian groups and that the diagram*

$$\begin{tikzcd} E' \arrow[r, "\hat{\phi}"] \arrow[d, "\eta'"] & E \arrow[d, "\eta"] \\ \mathrm{cl}^0(E') \arrow[r, "\phi^*"] & \mathrm{cl}^0(E) \end{tikzcd}$$

is commutative.]

(c) Let $m \geqslant 2$ be a positive integer, possibly distinct from $n = \deg(\phi)$. Show that, for all $P \in E[m]$ and $Q \in E'[m]$, we have

$$e_m(\phi(P), Q) = e_m(P, \hat{\phi}(Q)).$$

[*Hint: when applying the explicit formula for e_m to the right hand side, note that by commutativity of the diagram in* (b) *there exists $h \in K(E)^\times$ with $\hat{\phi}(Q) - (0) = \phi^*((Q) - (0)) + \mathrm{div}(h)$.*]

END OF PAPER