UNIVERSITY OF CAMBRIDGE

MAMA/125, NST3AS/125, MAAS/125

MAT3

MATHEMATICAL TRIPOS Part III

Friday, 9 June, 2023 1:30pm to 4:30pm

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 the Riemann-Roch theorem for a smooth projective curve of genus 1. For E an elliptic curve, define the group $\mathrm{Pic}^0(E)$ and prove that the map $E \to \mathrm{Pic}^0(E)$ given by $P \mapsto [(P) - (O_E)]$ is a bijection.

(b) Define the group law on an elliptic curve in terms of the chord and tangent process, and prove that it defines an abelian group.

(c) Let $\phi : E_1 \to E_2$ be a separable isogeny of degree d with $\#(E_1[\phi] \cap E_1[2]) =$ 1 or 4. Show that there is a rational function g on E_1 satisfying

$$\mathrm{div}(g) = \phi^*(O_{E_2}) - d\,(O_{E_1}) \quad \text{and} \quad [-1]^*g = \pm g.$$

Show that both signs $\pm$ can occur by computing explicit formulae for g in the cases where ϕ is multiplication by 2 or 3 on an elliptic curve in shorter Weierstrass form.

2 State and prove Hasse's theorem for elliptic curves over finite fields, clearly stating any general facts about isogenies or differentials that you use.

Give an example of a pair of elliptic curves over $\mathbb{F}_p$ that are isogenous over $\mathbb{F}_p$ but for which $E_1(\mathbb{F}_p) \not\cong E_2(\mathbb{F}_p)$. Prove that there are no such examples if $p < 43$ and the isogeny has degree 7. [*Properties of the Weil pairing may be quoted without proof.*]

3 Let K be a finite extension of $\mathbb{Q}_p$ with valuation ring $\mathcal{O}_K$, uniformiser π, and residue field k. Let E/K be an elliptic curve with good reduction.

(a) Explain what is meant by saying E/K has good reduction. Define the reduction map $E(K) \to \widetilde{E}(k)$ and prove that it is a group homomorphism.

(b) State a version of Hensel's lemma for polynomials in $\mathcal{O}_K[X]$. Use it to show that the reduction map is surjective, and that for each $0 \neq t \in \pi\mathcal{O}_K$ there is a unique point $\theta(t) = (x, y)$ in the kernel of reduction with $t = -x/y$. We set $\theta(0) = O_E$.

For the final part of this question you may assume that there is a formal group $F \in \mathcal{O}_K[[X, Y]]$ with $\theta(F(t_1, t_2)) = \theta(t_1) + \theta(t_2)$ for all $t_1, t_2 \in \pi\mathcal{O}_K$. Any other results you need about formal groups should be carefully stated.

(c) Show that if $P \in E(K)$ and $p \nmid n$ then $K([n]^{-1}P)/K$ is unramified. Deduce that for some finite unramified extension L/K the natural map $E(K)/nE(K) \to E(L)/nE(L)$ is the zero map.

4 Let $E/\mathbb{Q}$ be an elliptic curve with equation $y^2 = x^3 + ax + b$ where $a, b \in \mathbb{Z}$.

(a) Define the height $H(x)$ of a rational number x. Show that if $\xi(X) = r(X)/s(X)$ with $r, s \in \mathbb{Q}[X]$ coprime and $\max(\deg(r), \deg(s)) = d$ then there exist constants $c_1, c_2 > 0$ such that

$$c_1 H(x)^d \leqslant H(\xi(x)) \leqslant c_2 H(x)^d$$

for all $x \in \mathbb{Q}$ with $s(x) \neq 0$. Following this proof, or otherwise, show that for $(x, y) \in E(\mathbb{Q})$ we have

$$\gamma^{-2} H(x)^3 \leqslant H(y)^2 \leqslant \gamma H(x)^3$$

where $\gamma = 1 + |a| + |b|$.

(b) Define the logarithmic height $h : E(\mathbb{Q}) \to \mathbb{R}$ and the canonical height $\widehat{h} : E(\mathbb{Q}) \to \mathbb{R}$. Show that the latter is well defined and satisfies $\widehat{h}(nP) = n^2 \widehat{h}(P)$ for all $n \in \mathbb{Z}$ and $P \in E(\mathbb{Q})$.

(c) Explain, with brief justification, how the canonical height $\widehat{h}$ would change if

(i) we changed to a different Weierstrass equation for E,

(ii) we changed the definition of $\widehat{h}$ replacing the constants 2 and 4 by 3 and 9.

(iii) we changed the definition of h replacing the x-coordinate by the y-coordinate.

[*You may wish to use the identity* $(X^2 - a)(X^3 + aX + b) - (bX^2 - a^2 X - ab) = X^5$.]

5 (a) Let $E/\mathbb{Q}$ be an elliptic curve with equation $y^2 = x^3 + ax^2 + bx + c$ where $a, b, c \in \mathbb{Z}$. Quoting suitable results from the theory of formal groups show that if $0_E \neq T = (x, y) \in E(\mathbb{Q})$ is a point of finite order then $x, y \in \mathbb{Z}$.

(b) Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 - x^2 + 25x$. Let $T = (0, 0)$, $P = (1, 5)$ and $Q = (5, 15)$. Compute $P + T$, $Q + T$ and $P + Q$. Describe the method of descent by 2-isogeny. Use this and your previous calculations to compute integers $d_1 | d_2 | \cdots | d_t$ and r such that $E(\mathbb{Q}) \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z} \times \mathbb{Z}^r$.

END OF PAPER