UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Monday, 7 June, 2021 12:00 pm to 3:00 pm

PAPER 125

ELLIPTIC CURVES

Before you begin please read these instructions carefully

Candidates have THREE HOURS to complete the written examination.

*Attempt **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) Write down the general form of a Weierstrass equation. When do two such equations define isomorphic elliptic curves? How do your answers simplify over fields of characteristic not 2 or 3?

(b) Let $E/\mathbb{Q}$ be an elliptic curve with $j(E) \neq 0, 1728$. Define a twist of E, and prove that the twists of E (up to isomorphism over $\mathbb{Q}$) are parametrised by the square-free integers.

(c) For which integers $n \geqslant 2$ is it possible that all n-torsion points of E are defined over $\mathbb{Q}$? Briefly justify your answer.

(d) Prove that at most two of the twists of the elliptic curve in part (b) have a 3-torsion point defined over $\mathbb{Q}$.

(e) Prove that if $[K : \mathbb{Q}] = 2$ then $\operatorname{rank} E(K) = \operatorname{rank} E(\mathbb{Q}) + \operatorname{rank} E'(\mathbb{Q})$ where E' is a suitable twist of E.

2

(a) Let K be a finite extension of $\mathbb{Q}_p$ with valuation ring $\mathcal{O}_K$ and uniformiser π. What is a formal group $\mathcal{F}$ over $\mathcal{O}_K$? Define the group $\mathcal{F}(\pi^r\mathcal{O}_K)$ for $r \geqslant 1$. Prove that if r is sufficiently large then $\mathcal{F}(\pi^r\mathcal{O}_K) \cong (\mathcal{O}_K, +)$. [*You may quote a condition for a morphism of formal groups to be an isomorphism.*]

(b) Let $E/\mathbb{Q}$ be the elliptic curve given by the equation

$$y^2 + xy + y = x^3 - x^2$$

for which the discriminant Δ is -53. Compute the cardinality of $\widetilde{E}(\mathbb{F}_p)$ for $p = 2, 3$. Carefully stating any further facts you need about formal groups, prove the following statements.

(i) The torsion subgroup of $E(\mathbb{Q})$ is trivial.

(ii) The torsion subgroup of $E(\mathbb{Q}_2)$ has order dividing 8.

(iii) If $P = (0, 0)$ in $E(\mathbb{Q})$ then $7P$ does not have integral coordinates.

3

(a) Derive formulae for the group law for an elliptic curve in the shorter Weierstrass form $y^2 = x^3 + ax + b$. Prove that if $P, Q, P+Q, P-Q$ have x-coordinates $x_1, \ldots, x_4$ then

$$x_3 + x_4 = \frac{2(x_1x_2 + a)(x_1 + x_2) + 4b}{(x_1 - x_2)^2} \quad \text{and} \quad x_3x_4 = \frac{(x_1x_2 - a)^2 - 4b(x_1 + x_2)}{(x_1 - x_2)^2}.$$

Outline how these formulae are used in showing that both the degree map for isogenies, and the canonical height, are quadratic forms.

(b) Let $E/\mathbb{C}$ be the elliptic curve $y^2 = x^3 + 1$. Let $\alpha : E \to E$ be the isogeny given by $(x, y) \mapsto (\zeta x, y)$ where ζ is a primitive cube root of unity. By showing that $\alpha^2 + \alpha + 1 = 0$, or otherwise, compute $\deg(m + n\alpha)$ for all integers m and n.

Explain how isogenies may be characterised in terms of their kernels. Let $\phi : E \to E'$ be a 2-isogeny with $\ker(\phi) = \{0, (-1, 0)\}$. Show that $\phi(\alpha - \alpha^2) = \psi\phi$ where $\psi : E' \to E'$ is an isogeny of degree 3 with $\psi^2 = -3$.

4

Write an essay on

EITHER

Hasse's theorem and zeta functions of elliptic curves over finite fields,

OR

Galois cohomology and its application to the proof of the weak Mordell-Weil theorem.

5

Let $E/\mathbb{Q}$ be an elliptic curve of the form $y^2 = x(x^2 + ax + b)$.

(a) Prove that there is a group homomorphism $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ satisfying $\alpha(x, y) = x(\mathbb{Q}^*)^2$ whenever $(x, y) \in E(\mathbb{Q})$ with $x \neq 0$.

(b) Explain how computing rank $E(\mathbb{Q})$ may be reduced to deciding the solubility of finitely many equations of the form $w^2 = f(u, v)$. [*You may quote a description of* $\ker(\alpha)$, *but any other properties of* α *you need should be proved.*]

(c) Let $p \geqslant 5$ be a prime. Determine the list of equations in part (b) when E is given by $y^2 = x(x^2 + px + p^2)$. Show that if $p \equiv 7 \pmod{12}$ then rank $E(\mathbb{Q}) = 0$ or 1.

END OF PAPER