UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Wednesday, 8 June, 2022 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 $E/\mathbb{Q}$ in terms of the chord and tangent process. Assuming this defines a group, show that $E(\mathbb{Q})$ is a subgroup.

(b) Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 - 9x + 9$. Let $P = (0, 3)$ and $Q = (3, 3)$. Compute $2P$, $2Q$, $P + Q$ and $P - Q$. Show that if $0 \neq (x, y) \in E(\mathbb{Q})$ then $v_3(y) \leqslant 1$.

(c) State and prove the Lutz-Nagell theorem. [Results about formal groups may be stated without proof, but not results about torsion points.]

(d) Show that for the elliptic curve in (b) we have

$$E(\mathbb{Q})_{\text{tors}} \subset \{0, \pm P, \pm Q, \pm(P + Q), \pm(P - Q)\}.$$

Hence or otherwise determine $E(\mathbb{Q})_{\text{tors}}$.

[*You may wish to use the identity*

$$(3x^2 + 4a)(3x^2 + a)^2 - 27(x^3 + ax - b)(x^3 + ax + b) = 4a^3 + 27b^2.\,]$$

2 Define the *degree* of an isogeny, and explain what it means to say the degree map is a quadratic form. Define the *trace* of $\phi \in \mathrm{End}(E)$ and find a formula for $\mathrm{tr}(\phi^2)$ in terms of $\mathrm{tr}(\phi)$ and $\deg(\phi)$.

State and prove Hasse's theorem giving upper and lower bounds on the number of k-points on an elliptic curve defined over a finite field k. Give examples (over a finite field k of your choice) to show that both bounds can be attained.

3 Let $\phi : E \to E'$ be a separable isogeny of elliptic curves defined over a field k. You may assume that $\mathrm{char}(k) \neq 2, 3$ and both curves are in shorter Weierstrass form.

(a) Compute a non-zero regular differential on E.

(b) Show that ϕ is given by

$$(x, y) \mapsto \left(\frac{p(x)}{q(x)}, \frac{p'(x)q(x) - p(x)q'(x)}{cq(x)^2} y \right)$$

where $p, q \in k[x]$ are coprime polynomials and $c \in k^\times$ is a constant.

For the rest of this question you may assume that p and q have degrees d and $d-1$ where $d = \deg \phi$.

(c) Let $K = k((T))$ be the field of fractions of $k[[T]]$. Let $v : K^\times \to \mathbb{Z}$ be the discrete valuation satisfying $v(a) = 0$ for all $a \in k^\times$ and $v(T) = 1$. For $r \geqslant 1$ let

$$E_r(K) = \{(x, y) \in E(K) \mid v(x) \leqslant -2r \text{ and } v(y) \leqslant -3r\} \cup \{0\}.$$

Show that $\phi(E_r(K)) \subset E'_r(K)$.

(d) Explain how, by passing to an alternative affine piece, and defining a suitable power series $w(T)$, we may identify $E_1(K) = \{(t, w(t)) \in E(K) \mid v(t) \geqslant 1\}$.

(e) Define a *formal group* and a *morphism of formal groups*. Show that ϕ determines a morphism of formal groups $\widehat{E} \to \widehat{E'}$.

[*You may assume any form of Hensel's lemma, provided it is stated clearly. You are not required to prove that $\widehat{E}$ is a formal group.*]

4 Let E be an elliptic curve over a number field K, and let $n \geqslant 2$ be an integer.

(a) Show that if L/K is a finite Galois extension then the natural map

$$K^\times/(K^\times)^n \to L^\times/(L^\times)^n$$

has finite kernel.

(b) Show that if $\mu_n \subset K$ and $a \in K^\times$ then $K(\sqrt[n]{a})/K$ is a Galois extension with Galois group isomorphic to a subgroup of μ_n.

(c) State and prove analogues of (a) and (b) for the elliptic curve E.

(d) Complete the proof that $E(K)/nE(K)$ is finite. [Results about elliptic curves over local fields, about class groups and units of number fields, and about Kummer theory may be quoted without proof.]

5 Let $D \geqslant 1$ be a square-free integer. Given a point $P = (x, y)$ on the elliptic curve $E_D : Dy^2 = x^3 - x$, let Δ_P be the triangle with side lengths $\left|\frac{x^2-1}{y}\right|, \left|\frac{2x}{y}\right|, \left|\frac{x^2+1}{y}\right|$.

(a) Show that every right-angled triangle with rational side lengths and area D is of the form Δ_P for some $P \in E_D(\mathbb{Q})$ with $2P \neq 0$.

(b) Compute the rank and torsion subgroup of $E_5(\mathbb{Q})$.

(c) Stating any properties you need of the height $h : E_D(\mathbb{Q}) \to \mathbb{R}$, define the canonical height $\widehat{h}$ and prove that it is a quadratic form.

(d) Show that if $P, Q \in E_5(\mathbb{Q})$ with $\widehat{h}(P) = \widehat{h}(Q) \neq 0$ then the triangles Δ_P and Δ_Q are the same (up to re-ordering the sides).

[*You may assume that if $P = (x, y) \in E_D$ then the points $P + T$ for $T \in E_D[2]$ have x-coordinates* $x, -\frac{1}{x}, \frac{x+1}{x-1}, -\frac{x-1}{x+1}$.]

END OF PAPER