UNIVERSITY OF
CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Tuesday, 3 June, 2014 9:00 am to 12:00 pm

PAPER 22

ELLIPTIC CURVES

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

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

(i) Find rational parametrisations of the plane curves $y^2 = x^2 + 1$ and $y^2 = x^3$.

(ii) Show that if $u, v \in \mathbb{C}[t]$ are coprime polynomials and $\alpha u + \beta v$ is a square for four distinct $(\alpha : \beta) \in \mathbb{P}^1(\mathbb{C})$ then u and v are constant. Deduce that an elliptic curve (given in Weierstrass form) has no rational parametrisations.

(iii) Explain how to construct a group from a (possibly singular) Weierstrass equation, using the chord and tangent process. Prove the associative law in the non-singular case.

2

(i) Let E be an elliptic curve over the field $\mathbb{F}_q$ with q elements. State and prove Hasse's bounds on the order of $E(\mathbb{F}_q)$.

(ii) Let $E/\mathbb{F}_7$ be the elliptic curve $y^2 = x^3 - x + 1$. Compute the orders of $E(\mathbb{F}_7)$ and $E(\mathbb{F}_{49})$, and find an elliptic curve $E'/\mathbb{F}_7$ with $E'(\mathbb{F}_7) \cong \mathbb{Z}/4\mathbb{Z}$.

3

(i) Explain what is meant by a *formal group* over a ring R, and by a *morphism* between two formal groups. If $f \in R[[T]]$ is such a morphism, state and prove a condition in terms of $f'(0)$ for f to be an isomorphism.

(ii) Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 - D^2 x$ where D is a squarefree integer. Carefully stating any results about formal groups that you use, prove that the torsion subgroup of $E(\mathbb{Q})$ has order 4.

(iii) Prove that there are infinitely many right angled triangles with rational side lengths and area 15.

4

EITHER

(i) Write an essay on heights and their role in the proof of the Mordell–Weil Theorem.

OR

(ii) Write an essay on Kummer theory and the proof of the weak Mordell–Weil Theorem.

5

(i) Let E be the elliptic curve $y^2 = x(x^2 + ax + b)$. Let $T = (0, 0)$ and $P = (x, y)$ be points on E. Compute $P' = P + T$, say $P' = (x', y')$. Find a relation satisfied by $\xi = x + x' + a$ and $\eta = y + y'$. Hence write down a degree 2 isogeny $E \to E'$ where E' is a second elliptic curve you should specify.

(ii) Let E be the elliptic curve $y^2 = x(x^2 + i)$ over $K = \mathbb{Q}(i)$ where $i = \sqrt{-1}$. Prove that $E(K) \cong \mathbb{Z}/2\mathbb{Z}$.

[*You may assume that reducing* E *mod* (3) *and mod* $(2 - i)$ *gives groups* $\widetilde{E}(\mathbb{F}_9)$ *and* $\widetilde{E}(\mathbb{F}_5)$ *whose orders are powers of* 2.]

END OF PAPER