UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Tuesday 6 June, 2006 9 to 12

PAPER 29

ELLIPTIC CURVES

*Attempt **ALL** questions.*

*There are **FOUR** 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) Let E be an elliptic curve over the finite field $\mathbb{F}_q$. State and prove Hasse's estimate for the order of $E(\mathbb{F}_q)$.

(ii) Let E_1 and E_2 be elliptic curves over $\mathbb{F}_q$ and let $\pi : E_1 \to E_2$ be an isogeny defined over $\mathbb{F}_{q^2}$. Let ϕ_1 (resp. ϕ_2) be the qth power Frobenius endomorphism on E_1 (resp. E_2). Show that if $\pi\phi_1 = -\phi_2\pi$ then

$$|E_1(\mathbb{F}_q)| + |E_2(\mathbb{F}_q)| = 2(q+1).$$

[Standard facts about isogenies may be quoted without proof provided you state them clearly.]

2 Let E be the elliptic curve over $\mathbb{Q}$ given by

$$y^2 + y = x^3 + 4x^2 - 2x$$

for which you may assume $\Delta = -91$.

(i) Describe the group law on E in terms of the chord and tangent process.

(ii) Let $P_1 = (0,0)$ and $P_2 = (-2,-4)$. Compute $2P_1$, $3P_1$ and $P_1 \oplus P_2$.

(iii) Compute the order of $\widetilde{E}(\mathbb{F}_p)$ for $p = 2, 3, 5$.

(iv) Determine the torsion subgroup of $E(\mathbb{Q})$.

(v) Show that $P_1 + 5P_2$ does not have integral co-ordinates.

3 EITHER

(i) Let K be a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_K$ and maximal ideal $\pi\mathcal{O}_K$. Show that if $\mathcal{F}$ is a formal group over $\mathcal{O}_K$ then $\mathcal{F}(\pi\mathcal{O}_K)$ contains a subgroup of finite index isomorphic to $\mathcal{O}_K$ under addition.

OR

(ii) Write an essay on heights and their application to the proof of the Mordell-Weil theorem.

4 Describe a procedure, that often works in practice, to compute the rank of an elliptic curve over $\mathbb{Q}$ with a rational 2-torsion point. Illustrate by finding the rank of

$$E: \quad y^2 = x^3 + 8x^2 - 7x.$$

END OF PAPER