MATHEMATICAL TRIPOS Part III

Wednesday 4 June 2008 9.00 to 12.00

PAPER 28

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 Let E be an elliptic curve over $\mathbb{F}_q$, the field with q elements.

(i) State and prove Hasse's estimate for the number of rational points on E.

(ii) Given that $\phi^2 - [\mathrm{tr}(\phi)]\phi + [\deg(\phi)] = 0$ for any isogeny $\phi : E \to E$, show there exists $\alpha \in \mathbb{C}$ with $|\alpha| = \sqrt{q}$ such that $\#E(\mathbb{F}_{q^n}) = (1 - \alpha^n)(1 - \alpha^{-n}q^n)$ for all $n \geq 1$.

[Standard facts about isogenies may be quoted without proof.]

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

$$y^2 - 13y = x^3 + x^2 + 13x$$

with discriminant $\Delta = -91^3$. Let E' be the elliptic curve over $\mathbb{Q}$ given by the plane projective curve

$$x^3 + y^3 + 13z^3 - 2xyz = 0$$

with base point $(x : y : z) = (1 : -1 : 0)$. It is known that there is an isogeny $\phi : E' \to E$ of degree 3, defined over $\mathbb{Q}$. (You are not required to find ϕ.)

(i) Find the points of inflection on E' defined over $\overline{\mathbb{Q}}$.

(ii) Compute $2P$ and $2Q$ where $P = (0, 0)$ and $Q = (-2, 3)$ on E.

(iii) Determine the torsion subgroups of $E(\mathbb{Q})$ and $E'(\mathbb{Q})$.

(iv) Prove that the points $P + 4Q$ and $P - 4Q$ do not have integral co-ordinates.

3 Let $n \geq 2$ be an integer and p a prime not dividing n.

(i) What is a formal group $\mathcal{F}$ over $\mathbb{Z}_p$? Prove that the multiplication-by-n map $[n] : \mathcal{F} \to \mathcal{F}$ is an isomorphism of formal groups.

(ii) Show that if E is an elliptic curve over $\mathbb{Q}_p$ with good reduction, and $P \in E(\mathbb{Q}_p)$, then there exists a finite unramified extension $L/\mathbb{Q}_p$ and a point $Q \in E(L)$ with $nQ = P$.

4 EITHER

(a) Write an essay on the congruent number problem, including a proof that 1 and 2 are not congruent numbers.

OR

(b) Write an essay on Galois cohomology and its applications to Kummer theory and the proof of the Weak Mordell-Weil Theorem.

END OF PAPER