UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Monday 9 June 2003 9 to 12

PAPER 21

ELLIPTIC CURVES

Attempt **FOUR** *questions.*

There are **four** *questions in total.*

The questions carry equal weight.

Notation *Throughout,* $\mathbb{Q}$ *will denote the field of rational numbers. For each prime* $p, \mathbb{Q}_p$ *will denote the field of* p*-adic numbers, and* $\mathbb{F}_p$ *will denote the field* $\mathbb{Z}/p\mathbb{Z}$*.*

You may not start to read the questions printed on the subsequent pages until instructed to do so by the Invigilator.

1 (a) Briefly describe how, in practice, one determines the group of rational points on an elliptic curve defined over $\mathbb{Q}$, which possesses a point of order 2 with coordinates in $\mathbb{Q}$.

(b) Briefly explain why the procedure described in (a) cannot always be guarenteed to find the rank of the group of rational points.

(c) Find the rank of the group of rational points on the elliptic curve over $\mathbb{Q}$ given by

$$y^2 = x^3 - 17x\,.$$

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

$$y^2 = x^3 + x^2 + x + 1\,,$$

for which you may assume that $\Delta = -2^8$.

(a) Compute the number of points on the reduction of E modulo p for $p = 3, 5, 7, 11$.

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

(c) Prove that $E(\mathbb{Q})$ is infinite.

(d) If P is any point in $E(\mathbb{Q})$, let P_n denote any point in $E(\bar{\mathbb{Q}})$ such that $2^n P_n = P (n = 1, 2, \ldots)$; here $\bar{\mathbb{Q}}$ denotes a fixed algebraic closure of $\mathbb{Q}$. Which primes of $\mathbb{Q}$ are ramified in the extension obtained by adjoining to $\mathbb{Q}$ the coordinates of P_n?

3 (a) Explain what it means for an elliptic curve E over $\mathbb{Q}$ to have good reduction at the prime p.

(b) Determine the set of primes where the elliptic curve E over $\mathbb{Q}$ given by

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

has good reduction (you may assume that $\Delta = -11$ for this curve).

(c) Assume E is an elliptic curve over $\mathbb{Q}$ which has good reduction at the prime p. Let $\tilde{E}_p$ be the reduction of E modulo p. Define the reduction map from $E(\mathbb{Q}_p)$ to $\tilde{E}_p(\mathbb{F}_p)$, and prove that it is a surjective homomorphism of abelian groups. (You may assume Hensel's lemma, provided you state it clearly.)

4 Write an essay on isogenies between elliptic curves over a field k. In particular, prove that if E_1 and E_2 are any two elliptic curves over a field k, then the degree map defines a positive definite quadratic form with values in $\mathbb{Z}$ on the abelian group Hom (E_1, E_2) consisting of the zero map together with all isogenies from E_1 to E_2.