UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Friday 31 May 2002 9 to 12

PAPER 24

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) Describe geometrically the group law on the set of points of an elliptic curve given by a non-singular generalized Weierstrass equation with coefficients in a field k.

(b) Let E be the elliptic curve over $\mathbb{Q}$ given by

$$y^2 + y = x^3 - 7x + 6.$$

Let $P_0 = (0,2), P_1 = (1,0), P_2 = (2,0)$. Compute $P_0 \oplus P_1, P_0 \ominus P_1$, and $2P_1$.

2 (a) Briefly describe the procedure for determining the rank of $E(\mathbb{Q})$, when E is an elliptic curve over $\mathbb{Q}$ such that $E(\mathbb{Q})$ contains a non-zero point of order 2.

(b) Determine the rank of $E(\mathbb{Q})$ when E is given by

$$y^2 = x^3 - 7x^2 + 12x.$$

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

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

for which the discriminant Δ is equal to 37. For each prime p, let $\widetilde{E}_p$ be the reduction of E modulo p.

(a) Find the singular point on $\widetilde{E}_{37}$.

(b) Compute the cardinalities of $\widetilde{E}_2(\mathbb{F}_2), \widetilde{E}_3(\mathbb{F}_3), \widetilde{E}_{11}(\mathbb{F}_{11})$.

(c) Prove that the torsion subgroup of $E(\mathbb{Q})$ is trivial.

(d) For every odd prime p, determine the p-primary subgroup of the torsion subgroup of $E(\mathbb{Q}_2)$.

(e) If $p \neq 37$, write down Hasse's estimate for the cardinality of $\widetilde{E}_p(\mathbb{F}_p)$.

4 Write an essay on the formal group law which is attached to a generalized Weierstrass equation for an elliptic curve defined over a field k. Your essay should include a discussion of the following points:-

(a) How the formal group law is derived from the algebraic group law on E;

(b) How the formal group law can be used to describe the group $E(\mathbb{Q}_p)$ when $k = \mathbb{Q}_p$;

(c) How the formal group law can be used to determine the torsion subgroup of $E(\mathbb{Q}_p)$ when $k = \mathbb{Q}_p$ and E has good reduction.