UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Monday 13 June, 2005 9 to 12

PAPER 32

ELLIPTIC CURVES

*Attempt **FOUR** questions.*

*There are **FOUR** questions in total.*

The questions carry equal weight.

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

You may also use the following formulae attached to a generalized Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\,.$$

$$b_2 = a_1^2 + 4a_2, b_4 = a_1a_3 + 2a_4, b_6 = a_3^2 + 4a_6,$$
$$c_4 = b_2^2 - 24b_4, c_6 = -b_2^3 + 36b_2b_4 - 216b_6,$$
$$1728\Delta = c_4^3 - c_6^2, j = c_4^3/\Delta\,.$$

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 the elliptic curve over $\mathbb{Q}$

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

Compute the discriminant of E, and find the set of primes where E has bad reduction.

(ii) If $\tilde{E}$ denotes the reduction of E modulo a prime number p, compute the cardinality of $\tilde{E}(\mathbb{F}_p)$ for $p = 2$ and 3.

(iii) Prove that $P = (0, 0)$ has infinite order in $E(\mathbb{Q})$.

(iv) Compute $2P$ and $3P$.

(v) Prove that both the x and y coordinates of $5P$ and $7P$ do not lie in $\mathbb{Z}$, and that the same is true of $7P$..

2 (i) Define an isogeny between two elliptic curves over a field k, and explain briefly why an isogeny induces a homomorphism between their groups of points.

(ii) Let E_1 and E_2 be the elliptic curves over $\mathbb{F}_5$ defined by

$$E_1 : y_1^2 = x_1^3 - x_1 \quad , \quad E_2 : y_2^2 = x_2^3 - x_2 + 1\,.$$

Compute the cardinalities of $E_1(\mathbb{F}_5)$ and $E_2(\mathbb{F}_5)$ and show that these two abelian groups are not isomorphic.

(iii) Show that

$$x_2 = \frac{y_1^2}{(x_1 - 1)^2} - 2, \quad y_2 = \frac{x_1 y_1}{x_1 - 1} - \frac{(x_1 + 1)y_1}{(x_1 - 1)^2}$$

defines an isogeny from E_1 to E_2, and determine its degree.

(iv) Prove that E_1 and E_2 are not isomorphic over the algebraic closure of $\mathbb{F}_5$.

(Hint: compute j-invariants.)

3 Let E be an elliptic curve over the field $\mathbb{Q}_p$ of p-adic numbers, having good reduction. Let $\tilde{E}$ denote the reduction of E modulo p.

(i) Define the reduction map

$$\phi : E(\mathbb{Q}_p) \rightarrow \tilde{E}(\mathbb{F}_p)\,,$$

and prove it is a homomorphism of groups.

(ii) Define the formal group $\hat{E}$ attached to E, and explain why the kernel of ϕ can be identified with the group $\hat{E}(p\mathbb{Z}_p)$.

(iii) If q is any prime different from p, prove that the q-primary subgroup of $E(\mathbb{Q}_p)$ is finite, and its order is equal to the order of the q-primary subgroup of $\tilde{E}(\mathbb{F}_p)$.

4 Let E be an elliptic curve over $\mathbb{Q}$, having a rational point of order 2. Write an essay covering the following material:-

(i) a brief sketch of the proof that $E(\mathbb{Q})$ is finitely generated;

(ii) a sketch of the procedure which usually allows one to compute the rank g_E of $E(\mathbb{Q})$;

(iii) the calculation of g_E for two numerical examples of elliptic curves E, one of which at least has $g_E > 0$.

END OF PAPER