UNIVERSITY COLLEGE LONDON

University of London

EXAMINATION FOR INTERNAL STUDENTS

For The Following Qualifications:-

B.Sc. *M.Sci.*

Mathematics M324: Elliptic Curves

COURSE CODE : **MATHM324**

UNIT VALUE : **0.50**

DATE : **24-MAY-04**

TIME : **14.30**

TIME ALLOWED : **2 Hours**

04-C0971-3-30

TURN OVER

All questions may be attempted but only marks obtained on the best **four** *solutions will count.*
The use of an electronic calculator is **not** *permitted in this examination.*

1. (a) For a point P in the affine plane $\mathbb{A}^2(\mathbb{C})$, define
   (i) the *local ring* $\mathbb{C}[x,y]_P$;
   (ii) the *intersection number* $I(C_1, C_2, P)$ of two curves at P.

   (b) For every complex number λ, calculate the intersection number of the following two curves at the point $(0,0)$:

$$C_1 : y^2 = x^4 + x^2, \qquad C_2 : y = x^2 + \lambda x.$$

   (c) Find all rational points on the following conic:

$$C : x^2 - 3y^2 = 1.$$

2. (a) Define the term *elliptic curve over a field k.*

   For an elliptic curve C over k, <u>not</u> necessarily in Weierstrass form, define with the aid of a diagram the group law on the curve. Explain the role of Bezout's theorem in this construction.

   (b) Find a Weierstrass form of the following elliptic curve over $\mathbb{Q}$, starting from the given point:

$$C : u^3 + v^3 + w^3 = 0, \quad \mathcal{O} = (1 : 1 : 1).$$

3. (a) Define the term *elliptic function.*

(b) Let f be a non-zero elliptic function with respect to a lattice L and let $\mathcal{P}$ be a fundamental cell for L. Prove the following:

(i) The sum of the residues of f at points of $\mathcal{P}$ is 0;

(ii) The number of zeros of f in $\mathcal{P}$ is equal to the number of poles (taking into account the multiplicity).

(c) Give a formula for a group isomorphism

$$\Phi : \mathbb{C}/L \to C(\mathbb{C}),$$

where C is the curve defined by $y^2 = x^3 + g_4(L)x + g_6(L)$. (Do NOT prove that Φ is an isomorphism).

Prove that Φ is bijective.

4. (a) State the Nagell-Lutz Theorem.

Describe an algorithm for calculating the group of rational torsion points on an elliptic curve over $\mathbb{Q}$.

Let P be a point of an elliptic curve C in Weierstrass form. Show that $3P = 0$ if, and only if, P is a point of inflection.

(b) Let C be the elliptic curve with discriminant -3^7, defined over $\mathbb{Q}$ by the equation

$$y^2 = x^3 + 9.$$

Find a point of order 3 on $C(\mathbb{Q})$.

Calculate the group $\tilde{C}(\mathbb{F}_5)$.

Hence determine $C(\mathbb{Q})^{tors}$.

5. (a) State Mordell's Theorem.

Define the *rank* of an elliptic curve over $\mathbb{Q}$.

(b) Calculate the rank of the following elliptic curve:

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