UNIVERSITY COLLEGE LONDON

University of London

EXAMINATION FOR INTERNAL STUDENTS

For The Following Qualification:-

M.Sci.

Mathematics M324: Elliptic Curves

COURSE CODE : **MATHM324**

UNIT VALUE : **0.50**

DATE : **24-MAY-05**

TIME : **10.00**

TIME ALLOWED : **2 Hours**

05-C0974-3-30

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) Consider the following curve over $\mathbb{C}$:

$$C_1 : x^2 - y^4 = 1.$$

Show that there is only one point P at infinity on C_1.

Show that P is a singular point of C_1.

Using Bezout's theorem or otherwise, find the intersection number $I(C_1, L, P)$, where L is the line at infinity in projective space (i.e. $z = 0$).

For all values $\lambda \in \mathbb{C}$, calculate $I(C_1, C_2, Q)$, where $Q = (1, 0)$ and C_2 is given by

$$C_2 : \lambda y^2 = x - 1.$$

(b) Find all rational points on the following conic

$$x^2 + 2xy = 1.$$

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

Let C be an elliptic curve over k and let $\mathcal{O} \in C(k)$. Define, with the aid of a diagram, the group law on $C(k)$ corresponding to the point $\mathcal{O}$. Explain the role of Bezout's theorem in the definition.

Show that $\mathcal{O}$ is the identity element.

Show that every element has an inverse.

(b) Show that $\mathcal{O} = (1 : -1 : 0)$ is a point of inflection of the following elliptic curve over $\mathbb{Q}$:

$$C : u^3 + v^3 + w^3 = 0.$$

Reduce C to Weierstrass form.

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

Let f be a non-zero elliptic function with respect to a lattice L and let $\mathcal{P}$ be a fundamental cell for L. If $P_1, \ldots, P_r$ are the zeroes of f and $Q_1, \ldots, Q_r$ the poles of f in $\mathcal{P}$ (counting multiplicity) show that

$$\sum P_i - \sum Q_i \in L.$$

(b) Define the Weierstrass $\wp$-function with respect to a lattice L generated by $b_1, b_2 \in \mathbb{C}$.

Show that $\wp(-z) = \wp(z)$ and $\wp'(-z) = -\wp'(z)$.

Hence show that $\wp'$ has zeros of multiplicity 1 at $\frac{b_1}{2}$, $\frac{b_2}{2}$ and $\frac{b_1+b_2}{2}$ and no other zeros in the fundamental cell.

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 $P = (a, b)$ be a point on an elliptic curve C in Weierstrass form. Show that $2P = \mathcal{O}$ if, and only if, $b = 0$.

(b) Calculate the rational torsion on the curve

$$y^2 = x^3 + 1.$$

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:

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

END OF PAPER