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	:	**09-MAY-06**
TIME	:	**14.30**
TIME ALLOWED	:	**2 Hours**

06-C1057-3-30

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) Find all *rational* solutions to the equation
$$X^2 + Y^2 = 1$$
(b) Consider the diophantine equation
$$X^2 + Y^2 = Z^2$$
(i). Let (x, y, z) be an integer solution. Show that there is a solution (x', y', z') with x', y', z' pairwise coprime.
(ii). Let (x, y, z) be an integer solution with x, y, z pairwise coprime. Show, possibly after permuting x and y, that one can assume that x is odd and y is even.
(iii). Using the solution to (a) above show that there exist two coprime integers m and n and an integer λ such that
$$\lambda z = n^2 + m^2 \quad \lambda x = n^2 - m^2 \quad \lambda y = 2nm.$$
Show that λ is 1 or 2.
(iv). Show that $\lambda = 1$.
(c) Show that the equation $X^2 + Y^2 = 3Z^2$ has no integer solutions.

2. (a) Let C_1 and C_2 be two projective curves of degrees d_1 and d_2 given by homogeneous polynomials f_1 and f_2 respectively. State Bezout's theorem for C_1 and C_2.
(b) Let C be the algebraic curve in $\mathbb{P}^2$ defined by the polynomial
$$F(X, Y, Z) = X^3 + Y^3 - 2X^2Z + Y^2Z + XZ^2$$
(i) Find the singular points of C, the multiplicities of C at these points and the equations of the tangent lines at these points.
(ii) Let L_1 be the line in $\mathbb{A}^2$ defined by $X = 0$, let L_2 be the line $Y = 0$ and let Let P be the point $(0, 0)$. Compute $I_P(C, L_1)$ and $I_P(C, L_2)$.

3. (a) Say what is meant by Weierstrass normal form of an elliptic curve.
   (b) Let P and Q be points on an elliptic curve C with origin O. Explain the geometric construction of $P+Q$.
   Given the elliptic curve $y^2 = x^3 + 17$, O the point at infinity and rational points $P_1 = (2,5)$ and $P_2 = (4,9)$. Calculate the coordinates of $P_1 * P_2$ and of $P_1 + P_2$.
   (c) Let C have the equation $y^2z = x^3 + ax^2z + bxz^2 + cz^3$ and $O = [0:1:0]$. Show that 0 is a point of inflection. Let $P = (x,y)$ be a point on C. Show that $-P = (x,-y)$ and describe the subgroup $C[2]$ of points P such that $2P = 0$.

4. (a) State the Nagell-Lutz theorem.
   (b) Let $y^2 = f(x)$ where $f(x) = x^3 + ax^2 + bx + c$ be an equation of the elliptic curve C. Let $P = (x_0, y_0)$ be a point on C such that $y_0 \neq 0$. Express the coordinates of $2P$ in terms of $\lambda = \frac{f'(x_0)}{2y_0}$, x_0 and y_0.
   (c) Let $P = (x,y)$ be a point on C such that both P and $2P$ have integer coordinates and $y \neq 0$. Let D be the discriminant of f. Show that y divides D. (You can use without proof the fact that there exist two polynomials r and s with integer coefficients such that $D = r(x)f(x) + s(x)f'(x)$).
   (d) Let $P = (-2,3)$ be a point on the elliptic curve the curve $y^2 = x^3 + 17$. By calculating the coordinates of $2P, 4P, \ldots$ or otherwise, show that P is not a torsion point.

5. (a) Define the height H of a rational point on an elliptic curve. Show that for every real $M \geqslant 0$, the set of rational points P such that $H(P) \leqslant M$ is finite.
   (b) Define the *rank* of an elliptic curve. State the Mordell-Weil theorem.
   (c) Consider the elliptic curve $C\colon y^2 = x^3 - x$.
      (i) Calculate the rank of C.
      (ii) The torsion subgroup $C^{\text{tors}}(\mathbb{Q})$ (You may assume that the discriminant of $x^3 - x$ is 4 and you may use the stronger form of Nagell-Lutz theorem)

END OF PAPER