MA 5260

THE UNIVERSITY OF WARWICK

MSc EXAMINATION: APRIL 2001

ELLIPTIC CURVES

Time Allowed: 3 hours

Read carefully the instructions on the answer book and make sure that the numbers required are entered on it.

Candidates should attempt **all 4** *questions. However more credit will be given for complete answers than for a number of fragments.*

---

1. (a) For a lattice $L \subset \mathbb{C}$ and an integer $k \geq 2$, define the lattice sum $G_{2k}(L)$ and prove its convergence properties.

(b) Define the Weierstrass $\wp$-function and prove that it is an elliptic function for L. Convergence may be stated without proof.

(c) Calculate the Taylor series expansion of $\wp - \frac{1}{z^2}$ about $z = 0$.

(d) Describe briefly what you need to do to establish the Weierstrass equation $(\wp')^2 = 4\wp^3 + g_2\wp + g_3$. (The actual values of g_2 and g_3 are not required.)

---

2. (a) Write E for the elliptic curve with equation

$$y^2 = (x - e_1)(x - e_2)(x - e_3). \tag{1}$$

Suppose that $P_2 = (x_2, y_2) \in E$ for which $x_2 - e_i = f_i^2$, $y_2 = f_1 f_2 f_3$, and set $m = -(f_1 + f_2 + f_3)$. Prove that the line

$$y - y_2 = m(x - x_2)$$

touches E at a point P_1, which is to be determined.

(b) Let K be a field and E be the curve (1). Prove that a point $P_2 = (x_2, y_2) \in E(K)$ with coordinates in K and $y_2 \neq 0$ is the double of a point in $E(K)$ if and only if $x_2 - e_i$ is a perfect square in K. (The construction of the group law on E is assumed known.)

(c) Consider the curve (1) with $e_i \in \mathbb{Z}$. Sketch the proof that the quotient group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

---

3. (a) Explain the action of $\mathrm{SL}(2, \mathbb{Z})$ on the upper half-plane $\mathcal{H}$, and derive the standard fundamental domain D from first principles. Relate the action to the classification of lattices in $\mathbb{C}$ modulo an appropriate equivalence relation.

(b) Define a modular form of weight $2k$ for $\mathrm{SL}(2, \mathbb{Z})$.

(c) Explain how to go from the lattice sum $G_{2k}(L)$ treated in Question 1, (a) to a modular form for $\mathrm{SL}(2, \mathbb{Z})$. (A detailed treatment of the behaviour at the cusp is not required.)

---

4. (a) Set an MSc exam question on the use of elliptic curves in cryptography. **[10]**

(b) Write out a model solution to your question. **[15]**

You may if you prefer write an essay on topics of your choice in elliptic curves and cryptography not restricted by the above framework. Credit will be given for mathematical content rather than discussion of applications in the "popular science" style.
