MA 4260

THE UNIVERSITY OF WARWICK

FOURTH YEAR EXAMINATION: JUNE 2001

ELLIPTIC CURVES

Time Allowed: 3 hours

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

ANSWER 4 QUESTIONS.

If you have answered more than the required 4 questions in this examination, you will only be given credit for your 4 best answers.

---

1. (a) Show how to introduce a coordinate at the point at infinity on the complex plane $\mathbb{C}$ to obtain the projective line $\mathbb{P}^1_{\mathbb{C}}$. If $f(z) = \frac{p(z)}{q(z)} \in \mathbb{C}(z)$ is a rational function, explain how this allows us to view f as a holomorphic map $\varphi\colon \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$. **[8]**

(b) If $P_1, \dots, P_n \in \mathbb{P}^1_{\mathbb{C}}$ are distinct points, state and prove a theorem describing the set of rational functions $f(z) \in \mathbb{C}(z)$ that have at worst a simple pole at each P_i and are regular at every other point of $\mathbb{P}^1_{\mathbb{C}}$. **[8]**

(c) Write down a rational function f that has simple poles at the three cube roots of unity $z = 1, z = \varepsilon, z = \varepsilon^2$ (where $\varepsilon = \exp(2\pi i/3)$), and a zero of order 3 at $z = 0$. Describe geometrically the degree 3 holomorphic map $\varphi\colon \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ defined by f. **[9]**

---

2. (a) Say what is meant by an elliptic function with respect to a lattice $L \subset \mathbb{C}$. Give a clear statement and proof of the result that an elliptic function has as many zeros as poles. **[12]**

(b) If f is an elliptic function with respect to a lattice $L \subset \mathbb{C}$, define the degree d of f, and explain the precise sense in which f represents the quotient $E = \mathbb{C}/L$ as a d-sheeted cover of $\mathbb{P}^1_{\mathbb{C}}$. **[5]**

(c) Let f be an elliptic function of degree 2, and suppose that f has a double pole at $0 \in \mathbb{C}$. Prove that f is an even function. **[8]**

Given information for part (c): it is a result of the course that if an elliptic function f has zeros α_i of order n_i and poles β_j of order m_j then $\sum n_i\alpha_i = \sum m_j\beta_j$ modulo L.

---

3. (a) Describe the geometric construction of the sum of two general points on a non-singular plane cubic curve E. Explain briefly the geometric proof that addition is associative for general points. [You may assume the fact that if two plane cubic curves meet in 9 points, any other cubic through 8 of these points also passes through the 9th. The treatment of special configurations involving tangencies and inflexions is not required.) **[8]**

(b) Suppose that E is given by $y^2 = x(x^2 + b)$ (with the origin at infinity, as usual), and let $P = (0, 0)$. Derive a formula for the translation map $t_P\colon E \to E$ given by $Q \mapsto P + Q$. **[9]**

(c) Using these formulas, calculate the composite map $t_P \circ t_P$. **[4]**

(d) Explain how to determine the 2-torsion of an elliptic curve, and use this to give an alternative proof of the result of (c). **[4]**

---

4. *Given information: Let E be the elliptic curve $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{Z}$. The quotient group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. The duplication formula for the x-coordinate of $2P = (x_2, y_2)$ is*

$$x_2 = \frac{g_1(x)^2 - 8xg(x)}{4g(x)},$$

where $g(x) = x^3 + ax + b$ and $g_1 = 3x^2 + a$. Moreover, there exist polynomials A, A', B, B' of degree ≤ 3 with integer coefficients such that

$$\Delta = A\Big(g_1(x)^2 - 8xg(x)\Big) + Bg(x), \quad \Delta x^7 = A'\Big(g_1(x)^2 - 8xg(x)\Big) + B'g(x)$$

where Δ is the discriminant of E (a nonzero integer).

(a) Define the (logarithmic) height $h(x)$ of a rational number $x \in \mathbb{Q}$ and describe its elementary properties. **[5]**

(b) The height of a point $P = (x, y) \in E(\mathbb{Q})$ is defined to be the height of its x-coordinate. (The point at infinity has height 0.) Deduce from the given information that there exists a constant k_E depending only on E such that

$$4h(Q) - k_E \leq h(2Q) \leq 4h(Q) + k_E$$

for every $Q \in E(\mathbb{Q})$. **[12]**

(c) It is also known that for fixed $P \in E(\mathbb{Q})$, there exists a constant k_P so that $h(P \pm Q) \leq 2h(Q) + k_P$ for every $Q \in E(\mathbb{Q})$. Sketch the proof of the Mordell–Weil theorem using these ideas. **[8]**

---

5. (a) Prove that any lattice $L \subset \mathbb{C}$ is of the form $L = \mathbb{Z} \cdot w_1 + \mathbb{Z} \cdot w_2$ where w_1, w_2 is an oriented basis normalised by the conditions that w_2 is a shortest vector and w_1 is a vector in L shortest among vectors in $L \setminus \mathbb{Z} \cdot w_2$. **[7]**

(b) Draw the standard fundamental domain D for the action of $\mathrm{SL}(2, \mathbb{Z})$ on the upper half-plane $\mathcal{H}$. Explain the notion of similarity of lattices in $\mathbb{C}$, and deduce from (a) that L is similar to $L_\tau = \mathbb{Z} \cdot \tau + \mathbb{Z} \cdot 1$, where τ is in D. **[6]**

(c) Define a modular form of weight $2k$ for $\mathrm{SL}(2, \mathbb{Z})$. **[4]**

(d) For a lattice L and $k \geq 2$, define the lattice sum $G_{2k}(L)$ by

$$G_{2k}(L) = \sum_{w \in L \setminus \{0\}} \frac{1}{w^{2k}}.$$

Explain how to go from this to a modular form for $\mathrm{SL}(2, \mathbb{Z})$. (A detailed treatment of the behaviour at the cusp is not required.) **[8]**

END