MA 4260

THE UNIVERSITY OF WARWICK

FOURTH YEAR EXAMINATION: JUNE 2000

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) Say how the order of zero and poles of a rational function $f(z) = p(z)/q(z)$ at every point of $\mathbb{C}$ is defined; show how to introduce a coordinate at the point at infinity, and define also the order of f there. Justify the equality #zeros = #poles. **[6]**

(b) Explain why a global meromorphic function on $\mathbb{P}^1_{\mathbb{C}}$ is the same thing as a rational function $f \in \mathbb{C}(z)$, and why it defines a holomorphic map $\mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$. (Please give clear statements, but no proofs.) **[6]**

(c) Show that a holomorphic map $\varphi\colon \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ has a well defined degree $d = \deg \varphi$, and that the inverse image $\varphi^{-1}(c)$ of every point $c \in \mathbb{P}^1_{\mathbb{C}}$ consists of d points "with multiplicity" (explain what this means). **[6]**

(d) Describe geometrically the degree 2 holomorphic map $\varphi\colon \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ given by the rational function

$$f(z) = \frac{(z-1)^2}{z} = z - 2 + \frac{1}{z}\,.$$

Which points map to 0 and to ∞, which pairs of points of $\mathbb{P}^1_{\mathbb{C}}$ are identified, where are the two ramification points? **[7]**

---

2. (a) What is meant by an elliptic function with respect to a lattice $L \subset \mathbb{C}$? Prove that an elliptic function is determined up to scalar multiple by its divisor of zeros and poles. **[5]**

(b) Explain briefly what is wrong with defining the Weierstrass $\wp$-function as the sum $\sum_{w\in L} \frac{1}{(z+w)^2}$, and the traditional manoeuvre for getting around the problem. **[10]**

(c) Let $w_i/2$ for $i = 1, 2, 3$ be the 3 half periods of L and write $\wp(w_i/2) = e_i$. Using the fact that $\wp$ is an even function, prove that $\wp(z) - e_i$ has a double zero at e_i, and deduce that $\wp$ satisfies the differential equation

$$(\wp')^2 = 4(\wp - e_1)(\wp - e_2)(\wp - e_3).$$

[10]

---

3. (a) Explain briefly the geometric construction of the group law on a nonsingular plane cubic. Proofs are not required, but you should display awareness of the special cases in the construction. **[6]**

(b) For the standard cubic $C : y^2 = x^3 + ax + b$ (with the point at infinity O as origin), derive in detail the "duplication" formula

$$x_2 = m^2 - 2x_1 \quad \text{with} \quad m = \frac{3x_1^2 + a}{2y_1}$$

for the x-coordinate of $P_2 = 2P_1$, where $P_1 = (x_1, y_1)$. **[8]**

(c) Prove that P_1 is an inflection point of C if and only if its x-coordinate satisfies $3x_1^4 + 6ax_1^2 + 12bx_1 - a^2 = 0$. **[8]**

(d) How many inflection points should we expect to find on C? **[3]**

---

4. (a) Let $C : y^2 = (x - e_1)(x - e_2)(x - e_3)$ with distinct $e_1, e_2, e_3 \in \mathbb{Z}$. Suppose that $P = (x, y) \in C(\mathbb{Q})$ is a point over C with coordinates in $\mathbb{Q}$. Prove that for any prime p not dividing $e_1 - e_2, e_2 - e_3, e_3 - e_1$, the exact power of p contained in the numerator or denominator of each $x - e_i$ is an even power. **[10]**

(b) If $(x, y) \in C(\mathbb{Q})$ is as above, state without proof a necessary and sufficient condition for P to be 2-divisible in $C(\mathbb{Q})$, that is, $P = 2P_1$ with $P_1 \in C(\mathbb{Q})$. **[3]**

(c) Sketch briefly the argument that allows you to deduce that $C(\mathbb{Q})/2C(\mathbb{Q})$ is a finite group from (a) and (b). **[3]**

(d) Consider the elliptic curve $C : y^2 = x(x^2 - a)$ with $a \in \mathbb{Z}$, and let p be a prime not dividing a and with $p \equiv 3$ modulo 4. Prove that the congruence

$$y^2 \equiv x(x^2 - a) \quad \text{modulo } p$$

has exactly p solutions $(x, y) \in \mathbb{F}_p$. [Standard facts on quadratic residues may be used.] **[9]**

---

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, define the lattice sum $G_{2k}(L)$ by $G_{2k}(L) = \sum'_{w \in L \setminus \{0\}} \frac{1}{w^{2k}}$ for $k \geq 2$. 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]**
