MA 4260

THE UNIVERSITY OF WARWICK

FOURTH YEAR EXAMINATION: JUNE 2002

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) Discuss the construction of the Riemann sphere $\mathbb{C} \cup \infty = \mathbb{P}^1_{\mathbb{C}}$ as the union of two copies of $\mathbb{C}$ with coordinates z and $w = 1/z$. Show that the differential $\mathrm{d}z$ on $\mathbb{C}$ has a pole of order 2 when viewed as a rational differential near ∞. **[4]**

(b) Let $p(z)$, $q(z)$ be polynomials having disjoint zeros on $\mathbb{C}$, and consider the rational differential $\omega = \frac{p(z)\,\mathrm{d}z}{q(z)}$ on $\mathbb{C}$. Say how the order of zeros and poles of ω at every point of $\mathbb{P}^1_{\mathbb{C}}$ is defined, and prove the equality

$$\sum \text{order of zeros of } \omega - \sum \text{order of poles of } \omega = -2.$$ **[7]**

(c) Let f be a function that is holomorphic on the whole of $\mathbb{C}$ and bounded, and consider the meromorphic differential $\omega = \frac{f\,\mathrm{d}z}{(z-a)(z-b)}$. By computing the residue of ω at each point of $\mathbb{P}^1_{\mathbb{C}}$ and applying Cauchy's theorem, deduce that f is the constant function (Liouville's theorem). **[7]**

(d) Describe geometrically the degree 2 map $\varphi \colon \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ given on $\mathbb{C}$ by $\varphi(z) = \frac{z^2+bz+c}{z}$. 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) Define an elliptic function with respect to a lattice $L \subset \mathbb{C}$. Given points $\alpha_i \in \mathbb{C}$, distinct mod L, and integer multiplicities $m_i > 0$, prove that the vector space of elliptic functions w.r.t. L with poles of order $\le m_i$ at α_i (and no other poles mod L) has dimension $\le \sum m_i$. **[8]**

(b) The Weierstrass $\wp$ function is defined by

$$\wp(z) := \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Show that the sum has appropriate convergence properties away from lattice points to ensure that $\wp$ is a meromorphic function on $\mathbb{C}$, and prove that it is an elliptic function. **[9]**

(c) For any natural number $m \ge 2$, use $\wp$ and its derivative $\wp'$ to construct elliptic functions having pole at 0 of order exactly m. Deduce from this that elliptic functions with poles at 0 of order $\le m$ form a vector space of dimension m. **[8]**

You may use standard results of complex analysis without comment in this question, together with the fact that the lattice sum $\sum' \frac{1}{\omega^k}$ is absolutely convergent for $k \ge 3$.

---

3. Let $E : (y^2 + ay = x^3 + bx^2 + cx + d) \subset \mathbb{C}^2$ be a nonsingular cubic curve. In this question, take as given the group law on E with the point at infinity O as zero, and

$$P + Q + R = 0 \iff P, Q, R \text{ are collinear.} \qquad (*)$$

(a) Calculate the inverse $-Q$ in the group law of $Q = (x, y) \in E$. **[4]**

(b) Let $E : y^2 + 2y = x^3 + x^2 + 2x$, and $P = (0,0) \in E$. For $Q_0 = (x_0, y_0) \in E$, prove that the third point of intersection of the line PQ_0 with E is the point

$$R = \left(\frac{-2x_0}{x_0 + y_0 + 2}, \frac{-2y_0}{x_0 + y_0 + 2} \right).$$

Deduce that $P + Q_0 = Q_1 = \left(\frac{-2x_0}{x_0+y_0+2}, \frac{-2(x_0+2)}{x_0+y_0+2} \right)$. [Hint: *The equation of E can be rewritten in the form* $\frac{-x}{x+y+2} = \frac{x-y}{x^2}$.] **[7]**

(c) Let E, P be as in (b). Write $s\colon E \to E$ for the map given by $Q \mapsto P + Q$; calculate the composite map $s \circ s$. (In other words, calculate the coordinates of $Q_2 = P + Q_1$.) **[6]**

(d) Explain in geometric terms how the group law $(*)$ handles the special cases when some or all of O, P, Q, R coincide. In particular, say how the 3-torsion of an elliptic curve appears geometrically. **[4]**

(e) Determine $s \circ s \circ s$. **[4]**

---

4. (a) Let $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ with distinct $e_1, e_2, e_3 \in \mathbb{Z}$. Suppose that $P = (x, y) \in E(\mathbb{Q})$ is a point of E 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. **[12]**

(b) State without proof a necessary and sufficient condition for $P = (x, y) \in E(\mathbb{Q})$ to be 2-divisible in $E(\mathbb{Q})$, that is, $P = 2P_1$ with $P_1 \in E(\mathbb{Q})$. **[5]**

(c) Prove that $E(\mathbb{Q})/2E(\mathbb{Q})$ is a finite group. **[8]**

---

5. (a) Prove that any lattice $L \subset \mathbb{C}$ is of the form $L = \mathbb{Z} \cdot \omega_1 + \mathbb{Z} \cdot \omega_2$ where ω_1, ω_2 is an oriented basis normalised by the conditions that ω_2 is a shortest vector and ω_1 is a vector in L shortest among vectors in $L \setminus \mathbb{Z} \cdot \omega_2$. **[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{document} will automatically print END after the last question.`