MATHEMATICAL TRIPOS PART III (2005–06)

Elliptic Curves - Problem Sheet 1 of 4 **T.A. Fisher**

Note: Some standard formulae are recalled at the end of the sheet.

1) Alter building Vadic priests in India know by about 800BC how to construct rational right-angled trianges with areas 6, 15, 21 and 210. Repeat their discovery.

2) Find *two* rational right-angled triangles of area 7. [Hint: Look for rational points on the elliptic curve $y^2 = x^3 - 49x$.]

3) Find rational parametrisations for the plane conic $x^2 + xy + 3y^2 = 1$ and for the singular plane cubic $y^2 = x^2(x + 1)$.

4) Compute the Hessian of the plane cubic

$$a(X^3 + Y^3 + Z^3) + bXYZ = 0$$

and use this to find the points of inflection. Then, working over $\mathbb{Q}$, put the curve $X^3 + Y^3 + Z^3 = 0$ in (shorter) Weierstrass form, and determine its j-invariant.

5) Show that $\wp''(z)$ and $\wp(2z)$ are even elliptic functions, and find their poles. Deduce that $\wp''(z)$ and $\wp'(z)^2\wp(2z)$ are polynomials in $\wp(z)$. By computing series expansions at $z = 0$ or otherwise show that

$$\wp''(z) = 6\wp(z)^2 - \frac{1}{2}g_2 \quad \text{and} \quad \wp(2z) = \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2 - 2\wp(z).$$

6) Compute the j-invariant of $\mathbb{C}/\Lambda$ for $\Lambda = \mathbb{Z}[i]$ and for $\Lambda = \mathbb{Z}[\omega]$ where $\omega = e^{2\pi i/3}$.

7) Show that if p is a prime then $X^3 + pY^3 + p^2Z^3 = 0$ is a smooth plane cubic, defined over $\mathbb{Q}$, but with no $\mathbb{Q}$-rational points.

8) Let K be an algebraically closed field with $\text{char}(K) \neq 2$. Let C be the projective closure of the affine curve with equation $y^2 = f(x)$, where $f(x) \in K[x]$. Show that if $\deg(f) = 3$ then C is smooth if and only if f has distinct roots. What happens if $\deg(f) > 3$?

9) Let E be the elliptic curve over $\mathbb{Q}$ defined by $y^2 + y = x^3 - x$. Compute Δ and j for this curve, and draw a graph of its real points. Let $P = (0, 0)$. Compute nP for $n = 2, 3, 4, 5, 6, 7, 8$.

10) Let E be the elliptic curve over $\mathbb{Q}$ defined by $y^2 + y = x^3 + x^2 - 2x$. Compute Δ and j for this curve, and draw a graph of its real points. Let $P_1 = (0, 0)$ and $P_2 = (1, 0)$. Compute $2P_1$, $2P_2$, $P_1 \oplus P_2$, $P_1 \ominus P_2$, $2P_1 \ominus P_2$.

11) Let E be the elliptic curve over $\mathbb{Q}$ defined by $y^2 + xy = x^3 + 1$. Compute Δ and j for this curve, and draw a graph of its real points. Let $P_1 = (0, 1)$ and $P_2 = (-1, 0)$. Compute $2P_1$, $2P_2$, $3P_1$, $3P_2$, $P_1 \oplus P_2$, $P_1 \ominus P_2$.

12) Find an elliptic curve E defined over a finite field $\mathbb{F}_q$ for which the group $E(\mathbb{F}_q)$ is not cyclic. Can you find an example where more than two generators are required?

13) Let E be an elliptic curve over $\mathbb{Q}$ with Weierstrass equation $y^2 = f(x)$.
(i) Put the curve $E_d : dy^2 = f(x)$ in Weierstrass form. (In particular we require that the coefficients of y^2 and x^3 are 1.)
(ii) Show that if $j(E) \neq 0, 1728$ then every twist of E is isomorphic to E_d for some unique square-free integer d. (A twist of E is an elliptic curve E' defined over $\mathbb{Q}$ that is isomorphic to E over $\overline{\mathbb{Q}}$.)

14) Let K be any field. Show that the projective curve defined by the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_1, a_2, a_3, a_4, a_6 \in K$ is non-singular if and only if $\Delta \neq 0$. [Hint: If $\mathrm{char}(K) \neq 2$ use your answer to Question 8. If $\mathrm{char}(K) = 2$ reduce either to the case $a_1 = 1$, $a_3 = a_4 = 0$ or to the case $a_1 = a_2 = 0$.]

15) (i) Find a formula for doubling a point on the elliptic curve $y^2 = x^3 + ax + b$, and compare your answer with Question 5.
(ii) Find a polynomial in x whose roots are the x-coordinates of the points T with $3T = 0$. [Hint: Write $3T = 0$ as $2T = -T$.]
(iii) What do you notice about the derivative of the polynomial found in (ii)?

Formulae

We associate to a (generalised) Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

the quantities

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$
$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6,$$
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

It may be verified that $c_4^3 - c_6^2 = 1728\Delta$. The j-invariant is $j = c_4^3/\Delta$.