MATHEMATICAL TRIPOS PART III (2023–24)

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

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

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

3. Consider the curve $C_d = \{U^d + V^d = W^d\} \subset \mathbb{P}^2$ defined over $\mathbb{Q}$.
(i) Find the points of inflection on C_3, and then put this curve in Weierstrass form.
(ii) Let $x, y \in \mathbb{Q}(C_4)$ be given by $x = W^2/U^2$ and $y = V^2W/U^3$. Show that $y^2 = x^3 - x$, and hence find all the $\mathbb{Q}$-rational points on C_4.

4. Let K be an algebraically closed field with $\mathrm{char}(K) \neq 2$. 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. [*It's probably simplest to work with the affine equation, and then check the point at infinity separately.*] What happens if $\deg(f) > 3$?

5. Let E be the elliptic curve over $\mathbb{Q}$ defined by $y^2 + y = x^3 - x$. Draw a graph of its real points. Let $P = (0, 0)$. Compute nP for $n = 2, 3, 4, 5, 6, 7, 8$. What do you notice about the denominators? Can you prove anything in this direction?

6. Show that the congruent number elliptic curve $Dy^2 = x^3 - x$ has Weierstrass equation $y^2 = x^3 - D^2x$. Now use the group law to find *two* rational right-angled triangles of area 5.

7. 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.
(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 $\overline{\mathbb{Q}}$.*]

8. The elliptic curve E_λ over $\mathbb{C}$ with equation $y^2 = x(x - 1)(x - \lambda)$ has j-invariant
$$j = \frac{2^8(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$
Find the complex numbers λ' for which $E_\lambda \cong E_{\lambda'}$.

9. (i) Find a formula for doubling a point on the elliptic curve $E : y^2 = x^3 + ax + b$. [*You should fully expand the numerator of each rational function in your answer.*]
(ii) Find a polynomial in x whose roots are the x-coordinates of the points T with $3T = 0_E$. [*Hint: Write $3T = 0_E$ as $2T = -T$.*]
(iii) Show that the polynomial found in (ii) has distinct roots.

10. Let C be the plane cubic $aX^3 + bY^3 + cZ^3 = 0$ with $a, b, c \in \mathbb{Q}^*$. Show that the image of the morphism $C \to \mathbb{P}^3$; $(X : Y : Z) \mapsto (X^3 : Y^3 : Z^3 : XYZ)$ is an elliptic curve E, and put E in Weierstrass form. [*You should try to give an answer that is symmetric under permuting a, b and c.*] What is the degree of the morphism from C to E?

11. Let $E/\mathbb{F}_2$ be the elliptic curve $y^2 + y = x^3$. Show that the group $\mathrm{Aut}(E)$ of automorphisms of E is a non-abelian group of order 24. [*An automorphism of E is an isomorphism from E to itself. In this example all the automorphisms are defined over $\mathbb{F}_4 = \mathbb{F}_2(\omega)$ where $\omega^2 + \omega + 1 = 0$.*]

12. Let $C \subset \mathbb{P}^2$ be a smooth plane cubic defined over $\mathbb{Q}$. Show that if $C(K) \neq \emptyset$ for $K/\mathbb{Q}$ a quadratic field extension then $C(\mathbb{Q}) \neq \emptyset$. Can you generalise this result to field extensions of degree n for other integers n?