MATHEMATICAL TRIPOS PART III (2023–24)

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

1. Let E and E' be the elliptic curves (defined over a number field K) given by
$$E : y^2 = x^3 + ax^2 + bx \qquad E' : y^2 = x^3 + a'x^2 + b'x$$
with $a' = -2a$, $b' = a^2 - 4b$. Let $\phi : E \to E'$ be the 2-isogeny given by $\phi(x, y) = (y^2/x^2, y(x^2 - b)/x^2)$.
(i) Show that $T' = (0, 0)$ belongs to $\phi(E(K))$ if and only if $b' \in (K^\times)^2$.
(ii) Let $P = (x, y)$ in $E'(K)$ with $P \neq 0, T'$. Let $t \in \overline{K}$ be a square root of x. Show that $\phi^{-1}(P) = \{(x_1, y_1), (x_2, y_2)\}$ where
$$x_1 = \tfrac{1}{2}(x - a + y/t), \quad y_1 = x_1 t, \quad x_2 = \tfrac{1}{2}(x - a - y/t), \quad y_2 = -x_2 t.$$
(iii) Define $\alpha : E'(K) \to K^\times/(K^\times)^2$ via $\alpha(0) = 1$, $\alpha(T') = b'$ and $\alpha(x, y) = x$ if $x \neq 0$. Show that $\ker \alpha = \phi(E(K))$.
(iv) Suppose the line $y = \lambda x + \nu$ meets the curve E' in points P_1, P_2, P_3 (counted with multiplicity). Show that if $P_i = (x_i, y_i)$ for $i = 1, 2, 3$ then $x_1 x_2 x_3 = \nu^2$.
(v) Deduce that α is a group homomorphism. [*There will be some special cases you need to check.*]

2. Prove that 2 is not a congruent number.

3. Compute the rank of $E(\mathbb{Q})$ for each of the following elliptic curves $E/\mathbb{Q}$.
(i) $y^2 = x^3 + 6x^2 - 2x$
(ii) $y^2 = x^3 + 8x^2 - 7x$
(iii) $y^2 = x^3 - 3x^2 + 10x$
(iv) $y^2 = x^3 - 377x$.

4. Find the rank of $y^2 = x^3 - p^2 x$ for p a prime with $p \equiv 3 \pmod 8$.

5. Let $\nu(x)$ be the number of distinct prime factors of an integer x. Show that if $E/\mathbb{Q}$ is an elliptic curve with Weierstrass equation $y^2 = x^3 + ax^2 + bx$ with $a, b \in \mathbb{Z}$ then
$$\operatorname{rank} E(\mathbb{Q}) \leqslant \nu(b) + \nu(a^2 - 4b).$$
By considering real solubility, show that the inequality is strict. [*This last part is easier if $a = 0$, so assume that if you like.*]

6. Let E be an elliptic curve over $\mathbb{Q}$ and let $P \in E(\mathbb{Q})$. Show that P is a torsion point if and only if $\widehat{h}(P) = 0$. [*This gives another proof that the torsion subgroup is finite.*]

7. Show that if $\phi : E \to E'$ and $\psi : E' \to E''$ are isogenies defined over a number field K, then there is an exact sequence
$$E'(K)[\psi] \to S^{(\phi)}(E/K) \to S^{(\psi\phi)}(E/K) \to S^{(\psi)}(E'/K).$$
Deduce from results proved in lectures that $S^{(\phi)}(E/K)$ is finite.

8. Let E be an elliptic curve over $\mathbb{Q}$. Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer. The quadratic twist E_d of E by d was defined in Question 7 on Example Sheet 1. Show that there is a group homomorphism $E(\mathbb{Q}) \times E_d(\mathbb{Q}) \to E(K)$ with finite kernel and cokernel. Deduce that

$$\operatorname{rank} E(K) = \operatorname{rank} E(\mathbb{Q}) + \operatorname{rank} E_d(\mathbb{Q}).$$

9. Let E be an elliptic curve over $\mathbb{C}$. Let ω be an invariant differential on E. Show that the map $\operatorname{End}(E) \to \mathbb{C}$; $\phi \mapsto \phi^*\omega/\omega$ is an injective ring homomorphism. Use this to check that the 2-isogenies ϕ and $\widehat{\phi}$ (as defined in Question 1 and in lectures) are indeed dual isogenies.

10. Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x(x+1)(x+4)$.
(i) Compute the rank and torsion subgroup of $E(\mathbb{Q})$. [*For the latter you may quote your answer from Question 2 on Example Sheet 3.*]
(ii) Show that if $r, s, t \in \mathbb{Q}^\times$ with $r^2, s^2, 1, t^2$ in arithmetic progression then

$$(-2s^2, 2rst) \in E(\mathbb{Q}).$$

(iii) Deduce the result of Euler that there are no non-constant four term arithmetic progressions of square numbers.

11. Let E be an elliptic curve defined over a number field K with $E[2] \subset E(K)$, say $y^2 = f(x) = (x - e_1)(x - e_2)(x - e_3)$ with $e_1, e_2, e_3 \in K$.
(i) Define a group homomorphism $\delta : E(K) \to K^\times/(K^\times)^2 \times K^\times/(K^\times)^2$ with kernel $2E(K)$. Using your answer to Question 1, or otherwise, show that it is given by

$$(x, y) \mapsto \begin{cases} (x - e_1, x - e_2) & \text{if } x \neq e_1, e_2 \\ (f'(e_1), e_1 - e_2) & \text{if } x = e_1 \\ (e_2 - e_1, f'(e_2)) & \text{if } x = e_2 \end{cases}$$

(ii) Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 - x$. Compute $\delta(T)$ for each $T \in E(\mathbb{Q})[2]$. Show, by adapting the proof in the first lecture, that these elements generate the image of δ. Deduce that $\operatorname{rank} E(\mathbb{Q}) = 0$.