MATHEMATICAL TRIPOS PART III (2005–06)

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

43) Let E and E' be the elliptic curve over $\mathbb{Q}$ given by

$$E : y^2 = x^3 + ax^2 + bx \qquad E' : y^2 = x^3 + a'x^2 + b'x$$

with $a, b \in \mathbb{Z}$ and $a' = -2a$, $b' = a^2 - 4b$. 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 $\phi(E(\mathbb{Q}))$ if and only if $b' \in (\mathbb{Q}^*)^2$.
(ii) Let $P = (x, y)$ in $E'(\mathbb{Q})$ with $P \neq 0, T'$. Let $t \in \overline{\mathbb{Q}}$ be a square root of x. Show that $\phi^{-1}(P) = \{(x_1, y_1), (x_2, y_2)\}$ where

$$x_1 = \frac{1}{2}(x - a + y/t), \quad y_1 = x_1 t, \quad x_2 = \frac{1}{2}(x - a - y/t), \quad y_2 = -x_2 t.$$

(It may help to notice that $x_1 + x_2 = x - a$ and $x_1 x_2 = b$.)
(iii) Define $\alpha : E'(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ via $\alpha(0) = 1$, $\alpha(T') = b'$ and $\alpha(x, y) = x$ if $x \neq 0$. Show that $\ker(\alpha) = \phi(E(\mathbb{Q}))$.
(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 a number of special cases to consider.)

44) Prove that 2 is not a congruent number.

45) Compute generators for $E(\mathbb{Q})$ where $E : y^2 = x^3 - 7x^2 + 12x$.

46) 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) $y^2 = x^3 - 377x$.

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

48) 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

$$\operatorname{rank} E(\mathbb{Q}) \leq \nu(b) + \nu(a^2 - 4b).$$

By considering real solubility, show that the inequality is strict when $a = 0$.

49) Let E be an elliptic curve over $\mathbb{Q}$ and let $P \in E(\mathbb{Q})$. Show that $\widehat{h}(P) = 0$ if and only if P is a point of finite order. Deduce that the canonical height $\widehat{h}$ defines a positive definite quadratic form on $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$.

50) Let $F, G \in \mathbb{Z}[X, Y]$ be homogeneous polynomials of degree d, with no common root in $\mathbb{P}^1(\overline{\mathbb{Q}})$. Show that there exist polynomials $R_1, R_2, S_1, R_2 \in \mathbb{Z}[X, Y]$ and non-zero integers Δ_1, Δ_2 such that

$$R_1 F + S_1 G = \Delta_1 X^{2d-1}$$

$$R_2 F + S_2 G = \Delta_2 Y^{2d-1}.$$

(One method is to use Euclid's algorithm in $\mathbb{Q}[x]$.)

Further Problems

51) Let E be an elliptic curve over $\mathbb{Q}$, and let $K = \mathbb{Q}(\sqrt{d})$ with d a square-free integer. The quadratic twist E_d of E by d was defined in Problem 13. 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

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

52) 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

$$E'(K)[\psi] \to S^{(\phi)}(E/K) \to S^{(\psi\phi)}(E/K) \to S^{(\psi)}(E'/K).$$

53) Let $\phi, \psi \in \operatorname{Hom}(E_1, E_2)$. Recall that $\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$ is a bilinear form. We write $\widehat{\phi}$ for the dual of ϕ.
(i) By computing the degree of $\phi(\widehat{\phi}+\widehat{\psi})\psi$ in two different ways show that $\deg(\widehat{\phi}+\widehat{\psi}) = \deg(\phi + \psi)$.
(ii) Let $r, s \in \mathbb{Z}$. By computing the degree of $(r\phi + s\psi)(r\widehat{\phi} + s\widehat{\psi})$ in two different ways, show that $\deg(m + n(\phi\widehat{\psi} + \psi\widehat{\phi})) = (m + \langle \phi, \psi \rangle n)^2$ for all $m, n \in \mathbb{Z}$.
(iii) Deduce that $\phi\widehat{\psi} + \psi\widehat{\phi} = \langle \phi, \psi \rangle$.
(iv) Deduce that $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$.
[In Silverman's book, (iv) is established first. It is then used to show that deg : $\operatorname{Hom}(E_1, E_2) \to \mathbb{Z}$ is a quadratic form.]

54) Let E be an elliptic curve over a number field K. Let $m \geq 2$ be an integer. Let $\mathfrak{p}$ be a prime of K with $\mathfrak{p} \nmid m$ and $\gcd(c_{\mathfrak{p}}(E), m) = 1$. Show that the image of the local connecting map

$$\delta_{m,\mathfrak{p}} : E(K_{\mathfrak{p}}) \to H^1(K_{\mathfrak{p}}, E[m])$$

is the unramified subgroup $H^1_{\mathrm{nr}}(K_{\mathfrak{p}}, E[m]) := \ker\big(H^1(K_{\mathfrak{p}}, E[m]) \to H^1(K^{\mathrm{nr}}_{\mathfrak{p}}, E[m])\big)$.
[You should modify the proof sketched in lectures for $\mathfrak{p}$ a prime of good reduction. We have written $c_{\mathfrak{p}}(E)$ for the Tamagawa number of $E/K_{\mathfrak{p}}$.]

A note on the exam. The past exam questions for this course will give you a better idea what to expect in the exam, than do these problem sheets. This year's exam will be similar to previous years in format, mix of problems to bookwork, and style of problems. The bookwork parts will reflect the way I have lectured the course this year. You are expected to know your notes!