MATHEMATICAL TRIPOS PART III (2005–06)

Elliptic Curves - Problem Sheet 3 of 4 **T.A. Fisher**

31) For each of the following elliptic curves over $\mathbb{Q}$, determine the set of primes of bad reduction, and find a globally minimal Weierstrass equation.
(i) $y^2 + 27y = x^3 - 9x^2$
(ii) $y^2 = x^3 - 7x - 6$
(iii) $y^2 = x^3 + 16$.

32) Let E be an elliptic curve over a field $\mathbb{Q}$ given by a Weierstrass equation with integer coefficients. Let $P = (x, y)$ be a non-zero point in $E(\mathbb{Q})$. Show that $x = u/w^2$ and $y = v/w^3$ where $u, v, w \in \mathbb{Z}$ with $(u, w) = (v, w) = 1$.

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

$$y^2 + xy = x^3 - 2x + 1,$$

for which the discriminant Δ is equal to -61.
(i) Find the singular point on the reduction of E modulo 61.
(ii) Compute the cardinality of $\widetilde{E}(\mathbb{F}_p)$ for $p = 2, 3, 5, 7$.
(iii) Prove that the torsion subgroup of $E(\mathbb{Q})$ is trivial.
(iv) Prove that the torsion subgroup of $E(\mathbb{Q}_2)$ has order dividing 8.
(v) If $P = (1, 0)$ in $E(\mathbb{Q})$, prove that $7P$ and $9P$ do not have integral co-ordinates.

34) Find the torsion groups over $\mathbb{Q}$ for the elliptic curves
(i) $y^2 + y = x^3 + x^2 - 2x$
(ii) $y^2 + xy + y = x^3$
(iii) $y^2 - xy - 4y = x^3 - 4x^2$.

35) (i) Prove that the torsion subgroup of the group of $\mathbb{Q}$-points on the elliptic curve $y^2 = x^3 + d$ has order dividing 6. [Hint: Modify the result proved in lectures for the elliptic curves $y^2 = x^3 - D^2x$.]
(ii) Show that the point $P = (-1, 2)$ on $y^2 = x^3 + 5$ has infinite order.

36) Show that if E has Weierstrass equation

$$y^2 = x^3 + ax^2 + bx$$

with $a, b \in \mathbb{Z}$ and $P = (x, y) \in E(\mathbb{Q})$ is a point of finite order, then x divides b and $x + a + b/x$ is a perfect square. Find the torsion subgroup when $a = 0$ and $b = 4$. [Hint: Look at the proof of Lutz-Nagell.]

37) Let E be an elliptic curve over $\mathbb{Q}$, and let p be a prime. Let K be a number field, and $\mathfrak{p}$ a prime of K dividing p.
(i) Show that if $E/\mathbb{Q}$ has good reduction at p, then E/K has good reduction at $\mathfrak{p}$.
(ii) Show that if $E/\mathbb{Q}$ has multiplicative reduction at p, then E/K has multiplicative reduction at $\mathfrak{p}$. [You may assume $p \neq 2, 3$ if you like.]
(iii) Give an example where $E/\mathbb{Q}$ has additive reduction at p, yet E/K has good reduction at $\mathfrak{p}$.

38) Show that the reduction type of an elliptic curve (good, multiplicative or additive) does not change when we make an unramified field extension.

39) (i) Let E be the elliptic curve $y^2 + xy = x^3 + p$ over $\mathbb{Q}_p$. Show that the point $(0,0)$ on the reduction of E mod p does not lift to $E(\mathbb{Q}_p)$.
(ii) Find an example of an elliptic curve E over $\mathbb{Q}_p$ such that the mod p curve has a node which is the reduction of a point on $E(\mathbb{Q}_p)$.

40) Show that $\sqrt{2}$ does not belong to $\mathbb{Q}(\sqrt{-1}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{13})$. [Hint: This is painless if you quote something from lectures.]

41) Find elements of $K^\times$ generating $K(S,2)$ where (i) $K = \mathbb{Q}(\sqrt{-5})$ and (ii) $K = \mathbb{Q}(\sqrt{11})$, in each case taking S to be the set of primes above $2, 3, 5$. [You will need to compute the class groups and unit groups of these fields.]

42) Let K be a number field with $\mu_m \subset K$. Show that if S is a sufficiently large finite set of places of K then $K(S,m)$ has order $m^{|S|}$. (By "sufficiently large" we mean that S contains all infinite places, and a set of generators for the class group.)