MATHEMATICAL TRIPOS PART III (2023–24)

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

1. 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.
For each prime p, let $\widetilde{E}_p$ be the reduction of E modulo p.
(i) Compute the cardinality of $\widetilde{E}_p(\mathbb{F}_p)$ for $p = 2, 3, 5, 7$.
(ii) Prove that the torsion subgroup of $E(\mathbb{Q})$ is trivial.
(iii) Prove that the torsion subgroup of $E(\mathbb{Q}_2)$ has order dividing 8.
(iv) If $P = (1, 0)$ in $E(\mathbb{Q})$, prove that $7P$ and $9P$ do not have integral coordinates.

2. Find the torsion groups over $\mathbb{Q}$ for the elliptic curves
(i) $y^2 + xy + y = x^3$,
(ii) $y^2 - xy - 4y = x^3 - 4x^2$,
(iii) $y^2 = x^3 + 5x^2 + 4x$.

3. Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 + \lambda x$ where λ is an integer. For p a prime not dividing 2λ we write $\#\widetilde{E}(\mathbb{F}_p) = p + 1 - a_p$. Show that if $p = 4k + 1$ then
$$a_p \equiv \lambda^k \binom{2k}{k} \pmod{p}.$$
Deduce that $a_p \equiv 0 \pmod{p}$ if and only if $p \equiv 3 \pmod{4}$.

4. (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.
(ii) Show that the elliptic curve $y^2 = x^3 + 5$ has infinitely many $\mathbb{Q}$-points.

5. 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 either $x = 0$ or x divides b and $x + a + b/x$ is a perfect square. [*Thinking about how the proof of Lutz-Nagell works might help you find a short proof.*]

6. Let $p \geqslant 5$ be a prime, and let K be a finite extension of $\mathbb{Q}_p$. Show that every elliptic curve $E/\mathbb{Q}_p$ has a minimal Weierstrass equation of the form $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}_p$. What are the conditions on $v_p(a)$ and $v_p(b)$ for this to be a minimal Weierstrass equation? Show that if $E/\mathbb{Q}_p$ has good reduction then E/K has good reduction? Is the corresponding statement true if we replace "good" by "multiplicative"? What about the additive case?

7. Let K be a field of characteristic not 2. Let E/K be the curve defined by the singular Weierstrass equation $y^2 = x^2(x+1)$. Find a rational parametrisation $t \mapsto (\phi(t), \psi(t))$ with $t = 0, \infty$ mapping to the singular point and $t = 1$ mapping to the point at infinity. Use this to show that $E_{\mathrm{ns}}(K) \cong K^\times$. [*For the last part, try to find a method similar to the one used in lectures in the additive case.*]

8. Let p be a prime number of the form $u^2 + 64$ for some integer u (e.g. $p = 73, 89, 113, 233, \ldots$). Choose the sign of u so that $u \equiv 1 \pmod 4$. Consider the two elliptic curves
$$E : y^2 = x^3 + ux^2 - 16x$$
$$E' : y^2 = x^3 - 2ux^2 + px$$
Prove that E and E' are isogenous, and that both curves have good reduction at all primes different from p. Can you say anything about the Tamagawa numbers $c_p(E)$ and $c_p(E')$?

9. (i) Let E be an elliptic curve over an algebraically closed field K. Let $\phi : E \to E$ be a morphism of curves (not necessarily an isogeny). Show that if ϕ has no fixed points, then ϕ (and hence also ϕ^n) is a translation map.
(ii) Let $C/\mathbb{F}_q$ be a smooth projective curve of genus one. Show that $C(\mathbb{F}_q) \neq \emptyset$.

10. Let $E/\mathbb{Q}_p$ be as in Question 6, with minimal discriminant Δ_E. Show that $v_p(\Delta_E)$ can take any positive integer value, but that if $v_p(\Delta_E) \geqslant 12$ then either E or its quadratic twist by p has multiplicative reduction.

11. (Some group theory needed for Question 12.) For A an abelian group and $n \geqslant 2$ an integer we define
$$q(A) = \frac{\#\mathrm{coker}([n] : A \to A)}{\#\ker([n] : A \to A)}.$$
(It is undefined if either group is infinite.) Show that if $A \subset B$ is a subgroup of finite index, and either $q(A)$ or $q(B)$ is defined, then they are both defined and $q(A) = q(B)$.

12. Let K be a finite extension of $\mathbb{Q}_p$. Let E/K be an elliptic curve and $n \geqslant 2$ an integer. Use Question 11 and the theory of formal groups to show that
(i) $\#(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n) = \#\mu_n(K) \cdot \#(\mathcal{O}_K/n\mathcal{O}_K)$,
(ii) $\#(E(K)/nE(K)) = \#E(K)[n] \cdot \#(\mathcal{O}_K/n\mathcal{O}_K)$.