Honour School of Mathematics Part C: Paper C3.7
Master of Science in Mathematical Sciences: Paper C3.7

Elliptic Curves
James Newton
Checked by: Alan Lauder

22/2/2025

Do not turn this page until you are told that you may do so

1. (a) [10 marks] Let E be the elliptic curve over $\mathbb{Q}$ with affine equation

$$E : Y^2 - Y = X^3 - X^2$$

and identity element the point at infinity.

(i) Find a birational transformation from E to a curve with equation of the form

$$Y^2 = X^3 + aX + b,$$

with $a, b \in \mathbb{Z}$.

(ii) Find the group of rational torsion points, $E(\mathbb{Q})_{\text{tors}}$. If you find it helpful, you may use without proof the fact that the rank of $E(\mathbb{Q})$ is 0.
[*Your answer should give the structure of* $E(\mathbb{Q})_{\text{tors}}$*, together with explicit rational points of* E *which are generators for this group.*]

(b) [15 marks] Let $\alpha \in \mathbb{Z}_{>0}$ be a positive integer, and consider the elliptic curve E_α over $\mathbb{Q}$ with affine equation

$$E_\alpha : Y^2 = X(X^2 + \alpha)$$

and identity the point at infinity.

(i) For a point P of E_α, explain the definition of the point $2P$, and show that $2P \in E_\alpha(\mathbb{Q})$ if $P \in E_\alpha(\mathbb{Q})$.

(ii) Find a necessary and sufficient condition on α for E_α to have a rational point of order 4.

2. (a) [10 marks] Let F be a formal group defined over a characteristic 0 field K.

(i) Explain what a *normalized invariant differential* for F is, and prove that there is at most one normalized invariant differential.

(ii) Assuming the existence of a normalized invariant differential for F, define the *logarithm* $\log_F \in K[\![X]\!]$ and show that it defines an isomorphism from F to the additive formal group $\widehat{\mathbb{G}}_a$ with group law $X + Y$.

(b) [15 marks] Let R be the ring of integers in a characteristic 0 field K, complete with respect to a non-Archimedean valuation $|\cdot|$. Suppose that the maximal ideal $\{z \in R : |z| < 1\}$ is the principal ideal pR for a prime number p, and that the residue field of R has order $q = p^k$ for a positive integer k.

(i) Consider the polynomial $h(X) = pX + X^q \in R[X]$. Show that for each integer $a \in \mathbb{Z}$ there is a unique power series $g_a(X) \in R[\![X]\!]$ satisfying:

$$h(g_a(X)) = g_a(h(X)) \text{ and } g_a(X) = aX + (\text{terms of degree} \geqslant 2).$$

[*Hint: For each* $r \geqslant 1$*, show that there is a unique polynomial* $g_{a,r}(X) = aX + \cdots \in R[X]$ *of degree* $\leqslant r$ *such that* $h(g_{a,r}(X)) = g_{a,r}(h(X)) + (\text{terms of degree} \geqslant r+1)$*. You may use without proof the fact that* $z^q = z \bmod p$ *for all* $z \in R$*.*]

(ii) Suppose that $F(X, Y) \in R[\![X, Y]\!]$ is a formal group such that the polynomial $h(X)$ from part (i) defines a homomorphism from F to F. Deduce from part (i) that the power series $[p](X)$ giving multiplication by p on the formal group F satisfies $[p](X) = h(X)$.

3. (a) [10 marks] Consider an elliptic curve $C : Y^2 = X(X^2 + aX + b)$, with $a, b \in \mathbb{Z}$ satisfying $b(a^2 - 4b) \neq 0$, together with the curve $D : V^2 = U(U^2 - 2aU + (a^2 - 4b))$. Recall that there is a 2-*isogeny* $\phi : C \to D$ defined by

$$\phi(x, y) = \left(\left(\frac{y}{x} \right)^2, y - \frac{by}{x^2} \right).$$

Define the non-zero map

$$q : D(\mathbb{Q}) \to \mathbb{Q}^\times / \left(\mathbb{Q}^\times \right)^2,$$

and prove that the preimage of the identity coset $1 \cdot (\mathbb{Q}^\times)^2$ is $\phi(C(\mathbb{Q}))$.

(b) [15 marks] Consider the elliptic curve $C : Y^2 = X(X^2 + 5X + 3)$ defined over $\mathbb{Q}$.

(i) Find the group of rational torsion points, $C(\mathbb{Q})_{\text{tors}}$.
[*Your answer should give the structure of this group, together with explicit points of* $C(\mathbb{Q})$ *which are generators.*]

(ii) Find the rank of the group $C(\mathbb{Q})$. If the rank is positive, give an example of a point of infinite order.