

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

10/12/2025

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

[For all elliptic curves in this paper, the identity point O is the point at infinity.]

1. Let p be a prime number and let F be a formal group defined over $\mathbb{Z}_p$.

(a) [10 marks]

(i) Show that the multiplication by p homomorphism on F can be written as

$$[p](T) = pf(T) + g(T^p)$$

for power series $f(T), g(T) \in T\mathbb{Z}_p[[T]]$.

[You may assume existence and uniqueness of a normalized invariant differential for F without proof.]

(ii) Prove that, for every $x \in p\mathbb{Z}_p$,

$$\lim_{n \rightarrow \infty} [p^n](x) = 0.$$

(b) [15 marks]

(i) Suppose that a homomorphism $f : F \rightarrow F$ satisfies $f(T) = 0 \pmod{T^2}$. Show that $f(T) = 0$.

(ii) Show that $[p^n](T) \in (p, T)^{n+1}$ for every $n \geq 1$.

[Here (p, T) denotes the ideal in $\mathbb{Z}_p[[T]]$ generated by p and T .]

(iii) Prove that, for every $a \in \mathbb{Z}_p$, there exists a unique homomorphism $[a] : F \rightarrow F$ satisfying $[a](T) = aT \pmod{T^2}$.

[Hint for uniqueness: to compare two homomorphisms $f(T)$ and $g(T)$, consider the power series $F(f(T), i \circ g(T))$, where $i(T)$ is the inverse for the formal group F .]

2. (a) [7 marks] Consider an elliptic curve over $\mathbb{Q}$ defined by the equation

$$E : y^2 = x^3 + Ax + B,$$

with $A, B \in \mathbb{Z}$.

Show that if a point $P = (x_0, y_0) \neq O$ of $E(\mathbb{Q})$ has finite order, then $x_0, y_0 \in \mathbb{Z}$.

[In this question, results on formal groups from lectures may be assumed, provided they are clearly stated.]

(b) [10 marks] Now suppose that E has equation

$$E : y^2 = x^3 + B,$$

for a non-zero integer B .

(i) For a point $P = (x_0, y_0) \in E(\mathbb{Q})$ with $y_0 \neq 0$, find a formula for the x -coordinate of $2P$ in terms of x_0 . You should write your formula in the form

$$x(2P) = \frac{a(x_0)}{4b(x_0)},$$

with $a(x)$ and $b(x)$ coprime polynomials.

(ii) By considering the polynomial $3x^2a(x) - (3x^3 - 27B)b(x)$, or otherwise, deduce that

$$y_0^2 (12x_0^2x(2P) - (3x_0^3 - 27B)) = 27B^2.$$

(iii) Show that if P has finite order, then the integer y_0 divides $27B^2$.

(c) [8 marks] Let p be a prime number and consider the elliptic curve $E : y^2 = x^3 + p$.

(i) Show that the order of $E(\mathbb{Q})_{\text{tors}}$ is odd and less than or equal to 25.

(ii) Find a specific prime p such that $E(\mathbb{Q})_{\text{tors}}$ is trivial, justifying your answer.

3. (a) [5 marks] Let E be the elliptic curve $y^2 = x^3 + 10x - 2$, and consider the point

$$P = (1, 3) \in E(\mathbb{Q}).$$

Explain how to use the computation of $3P$ to factorize the integer 4331.

[Note that $(13/6)^2 = 125 \pmod{4331}$.]

- (b) [5 marks] Find the torsion subgroup $C(\mathbb{Q})_{\text{tors}}$ for the elliptic curve over $\mathbb{Q}$ defined by

$$C : y^2 = x(x^2 - 25).$$

- (c) [15 marks] Find the rank of $C(\mathbb{Q})$. If the rank is greater than 0, give (with justification) an example of a point of infinite order.

[You might find it helpful to recall the formula $\hat{\phi}(u, v) = \left(\frac{1}{4} \left(\frac{v}{u} \right)^2, \frac{1}{8} \left(v - \frac{100v}{u^2} \right) \right)$ for the 2-isogeny from the curve $D : v^2 = u(u^2 + 100)$ to C .]