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

Elliptic Curves
James Newton
Draft solutions

12/6/2025

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.

Solution 1. (a)(i) [5 marks, S] We have to complete the square on the left hand side, so we write

$$(Y - 1/2)^2 = X^3 - X^2 + 1/4.$$

Completing the cube on the right hand side, gives us

$$(Y-1/2)^2 = (X-1/3)^3-(X-1/3)/3+1/4-1/9+1/27 = (X-1/3)^3-(X-1/3)/3+19/(2^2 3^3).$$

Rescaling to get an integral equation we get:

$$(2^{-6}3^{-6})(2^3 3^3 Y - 2^2 3^3)^2 = (2^{-6}3^{-6})(2^2 3^2 X - 2^2 3)^3 - (2^{-2}3^{-2})(2^2 3^2 X - 2^2 3)/3 + 19/(2^2 3^3)$$

or

$$(2^3 3^3 Y - 2^2 3^3)^2 = (2^2 3^2 X - 2^2 3)^3 - (2^4 3^3)(2^2 3^2 X - 2^2 3) + 2^4 3^3 19.$$

So the birational transformation $X' = 2^2 3^2 X - 2^2 3, Y' = 2^3 3^3 Y - 2^2 3^3$ maps to the curve with equation $(Y')^2 = (X')^3 - 2^4 3^3 X' + 2^4 3^3 19$.

(a)(ii) [5 marks, S] We see from the short Weierstrass equation that 3 is a prime of bad reduction, so we consider the reduction mod 5. The equation is $Y^2 = X^3 - 2X - 2$. Checking the discriminant, we see that 5 is a prime of good reduction, and computing the $\mathbb{F}_5$-points on the curve gives 5 points in total. We deduce that the group $E(\mathbb{Q})_{\text{tors}}$ has order dividing 5. We do have rational points different from the identity, e.g. $(0, 0)$ in the initial coordinates. Since the rank is 0, this point must be a torsion point, which shows that $E(\mathbb{Q})_{\text{tors}}$ is cyclic of order 5, with $(0, 0)$ a generator.

(b)(i)[5 marks, B] We first consider the tangent t_P to E_α at the point P. This intersects E_α with multiplicity three, by Bézout's theorem. Since t_P is a tangent at P, the intersection at P has multiplicity $\geqslant 2$. If the third point of intersection (which could be P itself, if P is an inflexion) is (x, y), then $2P$ is defined to be $(x, -y)$. [The general definition, without assuming that the identity is an inflexion, is also acceptable.]

For the rationality, the tangent t_P has a rational equation, and so it suffices to show that its intersections with E_α have rational X-coordinate. The X-coordinates of the intersection points are roots of the cubic with rational coefficients obtained by substituting the equation for the tangent line into the equation for the curve. Since at least two of these roots have rational X-coordinate, the third will.

(b)(ii)[10 marks, S/N - they have seen plenty of examples of doubling a point] Suppose $P \in E_\alpha(\mathbb{Q})$ has order 4. Then $2P$ has order 2. Therefore we must have $2P = (0,0)$, and P has non-zero X- and Y-coordinate otherwise it would have order 2.

[*3 marks for noticing that we need to solve* $2P = (0,0)$]

Suppose $P = (x, y)$. The tangent at P has equation

$$Y - y = \frac{3x^2 + \alpha}{2y}(X - x).$$

If $2P = (0,0)$, this tangent passes through $(0,0)$, so we have $(3x^2 + \alpha)(-x) + 2y^2 = 0$. Substituting in the equation of the curve gives $(3x^2 + \alpha)(-x) + 2(x^3 + \alpha x) = -x^3 + \alpha x = 0$. Since the X-coordinate of Y is non-zero, we deduce that $x = \pm\sqrt{\alpha}$. This gives a rational point only if α is a perfect square.

[*4 more marks for deducing that* α *must be a square*]

If we consider the Y-coordinate, we find that $Y^2 = \pm 2\alpha\sqrt{\alpha}$.

So we need both α and $2\alpha\sqrt{\alpha}$ to be a perfect square. Thinking about the prime factorization of α, we see that $\alpha = n^2$ for a positive integer n which itself is of the form $n = 2m^2$. We deduce that a necessary and sufficient condition is for $\alpha = 4m^4$ for a positive integer m.

[*Final 3 marks for finishing off problem.*]

Solution 2. (a)(i) [5 marks, B] An invariant differential $\omega(T) = P(T)dT$ satisfies $\omega(F(T,S)) = \omega(T)$, or more explicitly:

$$P(F(T,S))\frac{\partial F}{\partial X}(T,S) = P(T).$$

It is normalized if the constant term of $P(T)$ is 1. Suppose $\omega(T)$ is a normalized invariant differential. Note that, setting $T = 0$, we have $P(S) = P(0)\left(\frac{\partial F}{\partial X}(0,S)\right)^{-1}$. Note that $\frac{\partial F}{\partial X}(0,S) = 1 + S(\cdots)$, so this power series is invertible. Since $\omega(T)$ is normalized, $P(0) = 1$, and we necessarily have $P(T) = \left(\frac{\partial F}{\partial X}(0,T)\right)^{-1}$, hence the uniqueness.

(a)(ii) [5 marks, B] If $\omega(T)$ is the normalized differential $\left(\frac{\partial F}{\partial X}(0,T)\right)^{-1} dT$, we define $\log_F = \int \omega(T)$. In other words we integrate the power series $\left(\frac{\partial F}{\partial X}(0,T)\right)^{-1}$ term by term. To show that it defines an isomorphism to $\widehat{\mathbb{G}}_a$, first we note that it suffices to show that it defines a homomorphism, since $\log_F(T) = T$+higher order terms, so the linear coefficient is invertible. Now we need to check that $\log_F(F(X,Y)) = \log_F(X)+\log_F(Y)$. We know that the derivative $\frac{\partial}{\partial X}(\log_F(F(X,Y)) - \log_F(X))$ is 0, by the invariance of ω. We deduce that $\log_F(F(X,Y)) - \log_F(X) = G(Y)$ for a power series $Y \in K[\![Y]\!]$. Setting $X = 0$, we deduce that $G(Y) = \log_F(Y)$, and we have shown that $\log_F$ is indeed a homomorphism.

(b)(i) [12 marks, N but similar to proofs in the formal power series section of the lecture notes, where power series are defined term by term] We follow the hint. We necessarily have $g_{a,1}(X) = aX$. Suppose we have shown that there is a unique $g_{a,r}$. Then we have $h(g_{a,r}(X)) = g_{a,r}(h(X)) + \delta_{r+1}(X)$+terms of degree $\geqslant r+2$, where $\delta_{r+1}(X)$ is a degree $r+1$ monomial. We are looking for $g_{a,r+1}(X) = g_{a,r}(X) + \alpha_{r+1}X^{r+1}$ for some α_{r+1} in R. Now we have $h(g_{a,r+1}(X)) = h(g_{a,r}(X)) + p\alpha_{r+1}X^{r+1}$+terms of degree $\geqslant r+2$. On the other hand, we have $g_{a,r+1}(h(X)) = g_{a,r}(h(X)) + \alpha_{r+1}p^{r+1}X^{r+1}$+terms of degree $\geqslant r+2$.

We deduce that we must have $0 = \delta_{r+1}(X) + p\alpha_{r+1}X^{r+1} - \alpha_{r+1}p^{r+1}X^{r+1}$, and therefore $\alpha_{r+1}X^{r+1} = \frac{\delta_{r+1}(X)}{p^{r+1}-p}$. This gives the unique polynomial $g_{a,r+1} = g_{a,r} + \frac{\delta_{r+1}(X)}{p^{r+1}-p} \in K[X]$.

[*9 marks for getting this far*]

For this to be an element of $R[X]$, we need p to divide $\delta_{r+1}(X)$ (note that $p^r - 1$ is invertible in R). If we consider the equation $h(g_{a,r}(X)) = g_{a,r}(h(X))+\delta_{r+1}(X)$+terms of degree $\geqslant r+2$ modulo p, we get $g_{a,r}(X)^q = g_{a,r}(X^q) + \delta_{r+1}(X) \bmod p$. Since the residue field of R has size q, we have $z^q = z \bmod p$ for all $z \in R$. We deduce that $g_{a,r}(X)^q = g_{a,r}(X^q) \bmod p$, and therefore $\delta_{r+1}(X) = 0 \bmod p$. [*remaining 3 marks for checking the divisibility by p*]

(b)(ii) [3 marks, N but easy given the previous part] Since $h(X)$ is a homomorphism, we have $h([p](X)) = [p](h(X))$. It follows that $[p](X) = g_p(X)$, the power series from part (i). But $h(x)$ itself also satisfies the property uniquely characterising $g_p(X)$. We deduce that $[p](X) = h(X)$.

Solution 3. (a) [10 marks, B] The definition of the map is that $q(u,v) = u$ if $u \neq 0$, $q(0,0) = a^2 - 4b$, and $q(O) = 1$. [*1 mark for definition.*]

A point (u,v) with $u \neq 0$ maps to the identity coset if and only if u is a square. If $(u,v) = \phi(x,y)$ then $u = (y/x)^2$ is a square. Conversely, if u is a square then we look for a preimage (x,y) with $y = \sqrt{u}x$. We have $v = \sqrt{u}x(1 - b/x^2)$, so $x - b/x = v/\sqrt{u}$. We also have $y^2 = ux^2 = x(x^2 + ax + b)$, so $u = x + a + b/x$. We deduce that $2x + a = u + v/\sqrt{u}$, so $x = 1/2(u - a + v/\sqrt{u})$. That gives a preimage $(1/2(u - a + v/\sqrt{u}), \sqrt{u}/2(u - a + v/\sqrt{u}))$ of (u,v). [*7 marks for this part.*]

It remains to consider when $q(0,0)$ is equal to the identity coset. This happens if and only if $a^2 - 4b$ is a rational square, which happens if and only if all the 2-torsion points of C are rational. This is equivalent to the two preimages of $(0,0)$ being rational points, since these preimages are precisely the order two points other that $(0,0)$.

[*Final 2 marks for handling the case of* $q(0,0)$.]

(b)(i) [5 marks, S] We consider the reduction mod 5, which gives equation $Y^2 = X(X^2 + 3)$. This curve has 10 points over $\mathbb{F}_5$. Reducing mod 7 gives a curve with 10 points over $\mathbb{F}_7$ as well. Persevering, the reduction mod 11 has 16 points. Since $C(\mathbb{Q})_{\text{tors}}$ is isomorphic to a subgroup of both $\widetilde{C}(\mathbb{F}_5)$ and $\widetilde{C}(\mathbb{F}_{11})$, it has size at most two. On the other hand, $(0,0)$ gives a point of order two. So $C(\mathbb{Q})_{\text{tors}}$ is cyclic of order two, generated by $(0,0)$. One can also attempt to use Nagell–Lutz, but there are some infinite order points which satisfy the 'Nagell–Lutz criterion'.

(b)(ii) [10 marks, S although they have seen more rank 0 examples than positive rank.] We follow the usual 2-descent procedure. The group $D(\mathbb{Q})/\phi(C(\mathbb{Q}))$ has image under q given by certain squarefree integers r dividing $a^2 - 4b = 13$. So $r \in \{\pm 1, \pm 13\}$. The integer r is contained in the image if the equation

$$W_r : rl^4 - 2al^2m^2 + \frac{(a^2 - 4b)}{r}m^4 = n^2$$

has non-zero solution (l,m,n) with $\gcd(l,m) = 1$. Considering signs, we have $r \in 1, 13$ and $q(0,0) = 13$, so $D(\mathbb{Q})/\phi(C(\mathbb{Q}))$ is generated by $(0,0)$, which is sent to O by $\hat{\phi}$.

[*3 marks for this part*]

Now we consider $C(\mathbb{Q})/\hat{\phi}(D(\mathbb{Q}))$. The group $D(\mathbb{Q})/\phi(C(\mathbb{Q}))$ has image under $\hat{q}$ given by certain squarefree integers r dividing 3. So $r \in \{\pm 1, \pm 3\}$. We have $\hat{q}(0,0) = 3$. We consider the equation

$$\widehat{W}_{-1} : -l^4 + 5l^2m^2 - 3m^4 = n^2.$$

It has a solution $(l,m,n) = (1,1,1)$. We have $\hat{q}(-1,1) = -1$.

[*5 more marks for this part*]

We deduce that $C(\mathbb{Q})/2C(\mathbb{Q})$ has order 4 and is generated by $(0,0)$ and $(-1,1)$. Since $C(\mathbb{Q})[2] = \langle (0,0) \rangle$, we deduce that $C(\mathbb{Q})$ has rank one and $(-1,1)$ is a point of infinite order.

[*2 marks for final deduction*]