

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)  
Summer 2025

This paper is also taken for the relevant examination for the  
Associateship of the Royal College of Science

## Elliptic Curves

**Date:** Tuesday, May 13, 2025

**Time:** Start time 14:00 – End time 16:30 (BST)

**Time Allowed:** 2.5 hours

**This paper has 5 Questions.**

***Please Answer All Questions in 1 Answer Booklet***

This is a closed book examination.

Candidates should start their solutions to each question on a new sheet of paper.

Supplementary books may only be used after the relevant main book(s) are full.

Any required additional material(s) will be provided.

Credit will be given for all questions attempted.

Allow margins for marking.

**DO NOT OPEN THIS PAPER UNTIL THE INVIGILATOR TELLS YOU TO DO SO**

1. (a) State a version of Hensel's lemma.

(2 marks)

- (b) Find the number of solutions to the equation  $X^3 - 7X + 24 = 0$  in  $\mathbb{Q}_p$  for  $p = 2, 3, 5$ .

(8 marks)

- (c) Let  $s \in \mathbb{Q}$ . Show that if there is one  $k \in \mathbb{Q}$  such that the equation

$$X^3 + sX + k = 0$$

has 3 rational roots, then there are infinitely many.

[Hint. Let  $u$  be a rational root. Find the condition, in terms of  $s, u, k$  that the two remaining roots are rational.]

(10 marks)

(Total: 20 marks)

2. (a) (i) Show that the torsion subgroup  $E(\mathbb{Q})_{tors}$  of the elliptic curve  $E$  over  $\mathbb{Q}$  given by

$$E : Y^2 = X(X + 1)(X + 4)$$

is isomorphic to either  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  or  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ .

(4 marks)

- (ii) Show that  $P = (2, 6) \in E(\mathbb{Q})$  and compute  $2P$ . Deduce that  $E(\mathbb{Q})_{tors}$  is isomorphic to  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ .

(6 marks)

- (b) Let  $E : Y^2 = X(X + r^2)(X + s^2)$  be an elliptic curve over  $\mathbb{Q}$  with  $r, s \in \mathbb{Z}$ . Show that  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$  is a subgroup of  $E(\mathbb{Q})$ .

(10 marks)

(Total: 20 marks)

3. (a) State the Mordell-Weil theorem. Explain why the conclusion of the Mordell-Weil theorem does not hold for the cubic in  $\mathbb{P}_{\mathbb{Q}}^2$  given by the equation  $Y^2Z = X^3 + X^2Z$ .

(2 marks)

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

$$E : Y^2 = X(X + 1)(X + 4)$$

Compute the rank of  $E(\mathbb{Q})$ .

(18 marks)

(Total: 20 marks)

4. (a) Find a birational transformation defined over  $\mathbb{Q}$  taking the intersection of two quadric surfaces in  $\mathbb{P}_{\mathbb{Q}}^3$  given by the equations

$$X_1^2 - 2X_2^2 + X_3^2 = 0, X_2^2 - 2X_3^2 + X_4^2 = 0$$

into the canonical (Weierstrass) form of an elliptic curve in  $\mathbb{P}_{\mathbb{Q}}^2$ , with  $(1, 1, 1, 1)$  going to the point at infinity. (15 marks)

- (b) Deduce that if  $n_1 < n_2 < n_3 < n_4$  are integers in arithmetic progression, they cannot all be perfect squares.

[Hint. The results from Questions (3) and (4a) should be useful here.] (5 marks)

(Total: 20 marks)

5. Consider the family of cubic curves in  $\mathbb{P}_{\mathbb{Q}}^2$  given by

$$E_t : (X + Y + Z)(XY + YZ + ZX) = tXYZ$$

- (a) Find the values of  $t$  for which  $E_t$  is an elliptic curve. (10 marks)

- (b) Show that if  $E_t$  is an elliptic curve, then  $E_t(\mathbb{Q})$  has a subgroup of order 6.

[Hint. Investigate the points  $[1 : 0 : 0], [0 : 1 : 0], [0 : 0 : 1], [0 : 1 : -1], [-1 : 0 : 1], [1 : -1 : 0]$  on  $E_t$ .]

(10 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2025

This paper is also taken for the relevant examination for the Associateship.

MATH70064

Elliptic Curves (Solutions)

Setter's signature

Yankı Lekili

Checker's signature

.....

Editor's signature

.....

1. (a) Let  $f = \sum_{i=0}^n a_i X^i \in \mathbb{Z}_p[x]$ . Suppose that there exists  $x_0 \in \mathbb{Z}_p$  such that

$$|f(x_0)| < |f'(x_0)|^2 \quad (1)$$

where  $f'(X) = \sum_{i=1}^n i a_i X^{i-1}$  is the (formal) derivative. Then, there exists a unique root  $x$  of  $f$  in  $\mathbb{Z}_p$  satisfying  $|x - x_0| < |f'(x_0)|$ .

2, A

- (b) We may suppose  $|X|_p \leq 1$ , as otherwise the norms of  $X^3$ ,  $-7X$  and  $24$  are all different, hence no cancellation can occur.

Let  $f(X) = X^3 - 7X + 24$ . We have  $f'(X) = 3X^2 - 7$ .

Modulo 2, we see that both 0 and 1 are solution to  $f(X) = 0$ , but  $f'(0) \neq 0$ , so by Hensel's lemma we have a unique solution in  $\mathbb{Q}_2$  which lifts  $0 \in \mathbb{F}_2$ . We next show that there is no solution of the form  $1 + 2Y$  modulo 4. As we have  $(1 + 2Y)^3 - 7(1 + 2Y) + 24 = 2(4)$ . Hence, there is no solution lifting 1. Thus, the number of solutions in  $\mathbb{Q}_2$  is 1.

Modulo 3, we see that  $f(X) = X^3 + 2X$  and  $f'(X) = 2$ . Hence,  $X = 0, 1, 2$  are all solution modulo 3 and they can be lifted uniquely to solutions in  $\mathbb{Q}_3$ .

Finally, modulo 5,  $f(X) = X^3 + 3X + 4$ , hence  $X = 3, 4$  are solutions modulo 5. Now  $f'(X) = 3X^2 + 3$ , this is not zero for  $X = 4$ , hence 4 has a unique lift. On the other hand, if we try  $3 + 5Y$ , we see that  $(3 + 5Y)^3 - 7(3 + 5Y) + 24 = 6(25)$  hence the solution  $X = 3$  does not lift. Thus, we have a unique solution in  $\mathbb{Q}_5$ .

8, A

- (c) Suppose  $u$  is a rational root, then we can write

$$X^3 + sX + k = (X - u)(X^2 + uX + u^2 + s)$$

Thus, to have 3 roots, we must have that  $u^2 - 4(u^2 + s) = -3u^2 - 4s$  has a rational square root  $v$ . Conversely, suppose  $v$  is a rational number such that  $v^2 = -3u^2 - 4s$ , then we see that  $X^3 + sX + k = (X - u)(X + (u + v)/2)(X + (u - v)/2)$  where  $s$  and  $k$  are determined by the formula  $s = (-3u^2 - v^2)/4$  and  $k = u(v^2 - u^2)/4 = -u(u^2 + s)$ .

In other words, the cubic polynomial  $X^3 + sX + k$  has 3 rational roots if and only if the conic

$$3U^2 + V^2 + 4s = 0$$

has a rational solution  $(u, v)$ . Now, if there exists such a rational solution determined by a particular value of  $k$ , then we deduce that the conic  $3U^2 + V^2 + 4s = 0$  is birational to a line, hence it must have infinitely many rational points. This, in turn, gives infinitely many  $k$ .

10, A

2. (a) (i) The discriminant is  $(0+1)^2(0+4)^2(3)^2 = 9.16$ . Hence, for  $p = 5$ , we have that the reduction modulo 3 map is injective on torsion points.  $\overline{E}(\mathbb{F}_5)$  is given by

$$Y^2 = X(X+1)(X-1)$$

and the set of points is given by

$$\{(0,0), (1,0), (2, \pm 1), (3, \pm 2), (4,0), \mathcal{O}\}$$

So, this is an abelian group of order 8. On the other hand, we already can see the 2-torsion points of the original equation which are given by

$$\{(0,0), (-1,0), (-4,0), \mathcal{O}\}$$

which we know is the abelian group  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . Therefore,  $E(\mathbb{Q})_{tors}$  can be either  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  or  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ . To see it is the latter, we need to find a point of order 4.

4, A

- (ii)  $6^2 = 2(2+1)(2+4)$  hence  $(2,6) \in E(\mathbb{Q})$ . Let  $F(X,Y) = Y^2 - X(X+1)(X+4)$ , we compute  $\partial F/\partial X = -3X^2 - 10X - 4$  and  $\partial F/\partial Y = 2Y$ . Then, the tangent line at  $(2,6)$  is

$$-36(X-2) + 12(Y-6) = 0$$

or equivalently  $Y = 3X$ . Then, we plug this in the equation of the curve

$$(3X)^2 = X(X+1)(X+4)$$

or equivalently,  $X^3 - 4X^2 + 4X = X(X-2)^2$ . Hence, the third intersection point is  $(0,0)$ . We conclude that  $2(2,6) = (0,0)$ , hence  $(2,6)$  is a point of order 4. As a result we conclude that  $E(\mathbb{Q})_{tors} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ .

6, A

- (b) The order 2 elements are given by  $(0,0)$ ,  $(-r^2,0)$  and  $(-s^2,0)$ . Now, consider the homomorphism

$$\begin{aligned} \delta : E(\mathbb{Q}) &\longrightarrow (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^3 \\ \mathcal{O} &\longmapsto (1,1,1) \\ (0,0) &\longmapsto (r^2s^2, r^2, s^2) = (1,1,1) \\ (-r^2,0) &\longmapsto (-r^2, r^2(r^2-s^2), s^2-r^2) = (-1, r^2-s^2, s^2-r^2) \\ (-s^2,0) &\longmapsto (-s^2, r^2-s^2, s^2(s^2-r^2)) = (-1, r^2-s^2, s^2-r^2) \\ (x,y) &\longmapsto (x-e_1, x-e_2, x-e_3), \quad y \neq 0 \end{aligned}$$

Since we have proved in the lectures that  $\text{Ker}\delta = 2E(\mathbb{Q})$ , and as  $(0,0) \in \text{Ker}\delta$ , it follows that there exists  $Q$  such that  $2Q = (0,0)$ , hence  $Q$  is an order 4 element. The subgroup generated by  $Q$  and the 2-torsion elements then give  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$  as a subgroup of  $E(\mathbb{Q})$ .

10, B

3. (a) Mordell-Weil : Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$ , then  $E(\mathbb{Q})$  is a finitely generated abelian group.

The cubic  $Y^2Z = X^3 + XZ$  is not an elliptic curve as it is not smooth.  $[0 : 0 : 1]$  is a singular point. Indeed, as we saw in the lectures,  $E(\mathbb{Q})$  is isomorphic to  $\mathbb{Q}^\times$ .

2, A

- (b) We consider the 2-descent homomorphism:

$$\begin{aligned} \delta : E(\mathbb{Q})/2E(\mathbb{Q}) &\longrightarrow (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^2 \\ (x, y) &\longmapsto (x, x+1) \\ \mathcal{O} &\longmapsto (1, 1) \\ (0, 0) &\longmapsto (4, 1) = (1, 1) \\ (-1, 0) &\longmapsto (-1, -3) \\ (-4, 0) &\longmapsto (-4, -3) = (-1, -3) \end{aligned}$$

To find  $\text{Im}\delta$ , we need to solve the equations

$$x = au^2, \quad x+1 = bv^2, \quad x+4 = cw^2, \quad u, v, w \in \mathbb{Q}^\times,$$

where  $a, b, c \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$  such that  $abc = 1$ , or equivalently

$$bv^2 - au^2 = 1, \quad abw^2 - au^2 = 4, \quad u, v, w \in \mathbb{Q}^\times.$$

Let  $u = U/Z$ ,  $v = V/Z$ , and  $w = W/Z$  with  $U, V, W, Z \in \mathbb{Z}$ , then we want to solve

$$bV^2 - aU^2 = Z^2, \quad abW^2 - aU^2 = 4Z^2, \quad U, V, W, Z \in \mathbb{Z}^\times.$$

Let  $\checkmark$  be  $(a, b) \in \text{Im}\delta$  and  $\times$  be  $(a, b) \notin \text{Im}\delta$ .

We have  $\delta(0, 0) = (1, 1)$  and  $\delta(-1, 0) = (-1, -3)$ . We also have  $\delta(2, 6) = (2, 3)$ . Hence, we also have  $\delta((-1, 0) + (2, 6)) = (-2, -1)$ .

$a \backslash b$	1	2	3	6	-1	-2	-3	-6
1	$\checkmark$							
2			$\checkmark$					
3								
6								
-1							$\checkmark$	
-2					$\checkmark$			
-3								
-6								

We claim that there are no other solutions. Let's first eliminate  $ab < 0$ . First note that if  $a > 0$  and  $b < 0$  then the equation  $bV^2 - aU^2 = Z^2$  has no solution. Also note that if  $(a, b) \in \text{Im}\delta$  then  $(a, b)(-2, -1) = (-2a, -b)$  is also in  $\text{Im}\delta$ . Hence, there cannot be any solution with  $a < 0, b > 0$  either.

For the same reason, it suffices to determine the number of solutions with  $a, b > 0$ , as multiplication with  $(-2, -1)$  gives a bijection between solution with  $a, b > 0$  and  $a, b < 0$ .

Now, let's investigate  $(a, b) = (1, 2)$ . Then, we have the system  $2V^2 - U^2 = Z^2$  and  $2W^2 - U^2 = 4Z^2$ . From the second equation we see  $2|U$ , hence also  $2|W$  and from the first equation we see  $2|Z$ , hence also  $2|V$ . Hence by descent, this gives no non-trivial solutions.

This argument uses only the fact that  $2|b$  and  $2 \nmid a$ . Hence, it also rules out  $(1, 6)$  and  $(3, 2), (3, 6)$ . Multiplying these with  $(2, 3)$ , we also get  $(2, 3)(1, 2) = (2, 6) \notin \text{Im}\delta$ ,  $(2, 3)(1, 6) = (2, 2) \notin \text{Im}\delta$ ,  $(2, 3)(3, 2) = (6, 6) \notin \text{Im}\delta$ ,  $(2, 3)(3, 6) = (6, 2) \notin \text{Im}\delta$ .

$a \backslash b$	1	2	3	6
1	✓	×		×
2		×	✓	×
3		×		×
6		×		×

Next, let's investigate  $(1, 3)$ . We have the system  $3V^2 - U^2 = Z^2$  and  $3W^2 - U^2 = 4Z^2$ . From the first equation we see that if  $3 \nmid U$  then  $Z^2 = -1 \pmod{3}$  which is impossible, hence  $3|U$  which implies  $3|Z$  and this in turn implies  $3|V$ . Similarly, from the second equation, we see  $3|W$ . Hence, again by descent, there are no non-trivial solutions. From  $(1, 3)(2, 3) = (2, 1)$ , we conclude  $(2, 1) \notin \text{Im}(\delta)$ .

Same argument works but this time using the second equation works for eliminating  $(3, 1)$  and  $(6, 1)$ . Indeed, the second equation for  $(3, 1)$  is  $3W^2 - U^2 = 4Z^2$ , hence by the same argument  $3|U, Z$ , which implies  $3|W$  and now using the first equation  $V^2 - 3U^2 = Z^2$  we see  $3|V$ . Similarly we rule out  $(6, 1)$ .

Now, observe that  $(3, 1)(2, 3) = (6, 3)$  and  $(6, 1)(2, 3) = (3, 3)$ . Hence, we conclude

$a \backslash b$	1	2	3	6
1	✓	×	×	×
2	×	×	✓	×
3	×	×	×	×
6	×	×	×	×

which implies that  $|\text{Im}\delta| = 4$ , hence rank of  $E(\mathbb{Q})$  is zero.

18, C

4. (a) First, we do the change of co-ordinates  $(X_1, X_2, X_3, X_4) \rightarrow (X_1 + X_2, X_2, X_3 + X_2, X_4 + X_2)$  which gives the equations

$$\begin{aligned} X_1^2 + X_3^2 + 2X_2(X_1 + X_3) &= 0 \\ X_4^2 - 2X_3^2 + 2X_2(X_4 - 2X_3) &= 0 \end{aligned}$$

and in the new co-ordinates, we have  $\mathbf{o} = (0, 1, 0, 0)$ . Now, we can eliminate  $X_2$ , relabeling  $X_1 = X, X_3 = Y, X_4 = Z$ , we get

$$F(X, Y, Z) := (X^2 + Y^2)(Z - 2Y) - (X + Y)(Z^2 - 2Y^2) = 0$$

with a rational point given by  $Z - 2Y = X + Y = 0$ , that is,  $\mathbf{o} = (1, -1, -2)$ . We compute the derivatives

$$\begin{aligned} \frac{\partial F}{\partial X} &= 2XZ - 4XY - Z^2 + 2Y^2 \\ \frac{\partial F}{\partial Y} &= -2X^2 + 2YZ + 4XY - Z^2 \\ \frac{\partial F}{\partial Z} &= X^2 + Y^2 - 2XZ - 2YZ \end{aligned}$$

Thus, we see that the tangent line at  $\mathbf{o}$  is  $t(\mathbf{o}) = X + 3Y - Z$ . We easily compute that  $t(\mathbf{o})$  intersects our curve also at  $\mathbf{p} = (1, 0, 1)$ .

Now, in order to apply Nagell's algorithm, we want to move  $\mathbf{o}$  to  $(0, 1, 1)$ , and  $\mathbf{p}$  to  $(0, 0, 1)$  and the tangent line at  $\mathbf{o}$  to  $X = 0$ , we apply the transformation  $(X, Y, Z) \rightarrow (X + Z, -Y, Z - 3Y)$

Now, in order to move  $\mathbf{o}$  to  $(0, 1, 0)$  and the tangent line  $t(\mathbf{o})$  to  $Z = 0$ , we apply the transformation  $(X, Y, Z) \rightarrow (X + Y + Z, -Y, X - 2Y)$ . Then the equation becomes

$$((X + Z)^2 + Y^2)(Z - Y) - ((Z - 3Y)^2 - 2Y^2)(X + Z - Y) = 0$$

Setting  $Z = 1$  and reorganizing according to the degree we get

$$F_3(X, Y) + F_2(X, Y) + F_1(X, Y)$$

with  $F_3(X, Y) = 6Y^3 - 7XY^2 - X^2Y$ ,  $F_2(X, Y) = X^2 + 4XY - 12Y^2$ ,  $F_1(X, Y) = X + 6Y$ . We set  $s = 2F_3(1, t)x + F_2(1, t)$  and  $G(t) = F_2(1, t)^2 - 4F_1(1, t)F_3(1, t)$ . Our curve is now equivalent to  $s^2 = G(t)$ . Expanding out  $G(t)$ , we get the equation

$$s^2 = 48t^3 + 44t^2 + 12t + 1$$

Multiplying by 36 and redefining  $y = 6s$  and  $x = 12t$ , we get

$$y^2 = x^3 + 11x^2 + 36x + 36$$

We notice that  $-2$  is a root of the right hand side, so sending  $x \rightarrow x - 2$  simplifies the equation to

$$y^2 = x(x + 1)(x + 4)$$

By a further change of variables by sending  $x \rightarrow x - (5/3)$  and multiplying both sides with  $3^6$  and rescaling, one can get to the form

$$y^2 = x^3 - 351x + 1890$$

- (b) From Questions (3) and (4) we know that this curve has  $E(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ . In particular, it has  $|E(\mathbb{Q})| = 8$ . On the other hand, we know that the original equations have 8 solutions  $(X_1, X_2, X_3, X_4) = [\pm 1 : \pm 1 : \pm 1 : 1]$ . Hence, (up to overall factor) these are all solutions for the equations:

$$X_1^2 - X_2^2 = X_2^2 - X_3^2 = X_3^2 - X_4^2$$

5, A
------

5. (a) Let  $F = (X+Y+Z)(XY+YZ+ZX)-tXYZ$ . Computing the partial derivatives, we get

$$\begin{aligned}\frac{\partial F}{\partial X} &= (X+Y+Z)^2 - X^2 + (1-t)YZ \\ \frac{\partial F}{\partial Y} &= (X+Y+Z)^2 - Y^2 + (1-t)XZ \\ \frac{\partial F}{\partial Z} &= (X+Y+Z)^2 - Z^2 + (1-t)XY\end{aligned}$$

To find singular points, we set these equal to zero, which in particular implies

$$X^2 + (t-1)YZ = Y^2 + (t-1)XZ = Z^2 + (t-1)XY$$

If  $X, Y, Z$  are mutually distinct, these imply that

$$X+Y = (t-1)ZY + Z = (t-1)XZ + X = (t-1)Y$$

From which, we conclude that, if  $X+Y+Z \neq 0$ , then  $t = 3$ . Then, from the first equation, we have  $X+Y = 2Z$  and from  $F = 0$ , we get  $3Z(XY+3Z^2) - 3XYZ = 0$ , hence  $9Z^3 = 0$ , which implies  $Z = 0$ . By cyclic symmetry, this implies  $X = Y = Z = 0$  which means  $t = 3$  gives an elliptic curve. The remaining exceptional cases are when  $[X : Y : Z] = [X : 1 : 1]$  or  $[1 : Y : 1]$  or  $[1 : 1 : Z]$  or  $X+Y+Z = 0$ . If  $X+Y+Z = 0$ , we get from  $F = 0$ , that  $tXYZ = 0$ . So, either  $t = 0$  (which gives a reducible curve, hence is singular) or we may assume  $X = 0$ . Then,  $Y+Z = 0$ . Hence, we get  $[0 : 1 : -1]$ . Plugging this to  $\frac{\partial F}{\partial Y} = 0$  gives 1, hence this case does not arise. Finally, let us analyze  $[X : 1 : 1]$  (the other cases are symmetric). Then, from partial derivatives we get the equations:

$$\begin{aligned}(X+2)^2 - X^2 + (1-t) &= 0 \\ (X+2)^2 - 1 + (1-t)X &= 0\end{aligned}$$

The first equation gives  $t = 4X + 5$ . Plugging this to the second equation gives  $X^2 = 1$ . Hence  $X = \pm 1$ . The case  $X = 1$ , gives a singular point  $[1 : 1 : 1]$  for  $t = 9$  and the case  $X = -1$  gives a singular point for  $t = 1$ . Hence, we conclude that  $E_t$  is an elliptic curve except for  $t = 0, 1, 9$ .

10, D

- (b) It is easy to see that the given points lie on  $E_t$  for any  $t$ . We compute the tangent lines on these points by evaluating the partial derivatives. We see that tangent lines are given as follows:

$$\begin{aligned}\text{At } [1 : 0 : 0] \text{ tangent line is } Y + Z &= 0 \\ \text{At } [0 : 1 : 0] \text{ tangent line is } X + Z &= 0 \\ \text{At } [0 : 0 : 1] \text{ tangent line is } X + Y &= 0 \\ \text{At } [0 : 1 : -1] \text{ tangent line is } (1-t)X + Y + Z &= 0 \\ \text{At } [-1 : 0 : 1] \text{ tangent line is } X + (1-t)Y + Z &= 0 \\ \text{At } [1 : -1 : 0] \text{ tangent line is } X + Y + (1-t)Z &= 0\end{aligned}$$

We claim that  $[0 : 1 : -1]$ ,  $[-1 : 0 : 1]$ ,  $[1 : -1 : 0]$  are inflection points. By symmetry, it suffices to show the first one. We plug in  $Y + Z = (t - 1)X$  in  $F = 0$ , we get

$$(tX)((t - 1)X^2 + YZ) = tXYZ$$

Hence  $t(t - 1)X^3 = 0$ . As  $t \neq 0, 1$ , this implies  $X = 0$ . Hence, we get that  $[0 : 1 : -1]$  is the only intersection of the tangent line at  $[0 : 1 : -1]$  with  $F = 0$ . Next, we claim that the tangent lines at  $[1 : 0 : 0]$ ,  $[0 : 1 : 0]$ ,  $[0 : 0 : 1]$  intersects the curve at one of these three inflection points. Again by symmetry, let's only consider  $[1 : 0 : 0]$ , then we plug in  $Y + Z = 0$  in  $F = 0$ , we get

$$X(YZ) = tXYZ$$

Hence, we have  $Y + Z = 0$  and  $XYZ = 0$ . The only solutions are  $[1 : 0 : 0]$  or  $[0 : 1 : -1]$ . Thus, we conclude that the given 6 points form a subgroup of order 6.

10, B

**Review of mark distribution:**

Total A marks: 37 of 37 marks

Total B marks: 20 of 20 marks

Total C marks: 18 of 18 marks

Total D marks: 25 of 25 marks

Total marks: 100 of 100 marks

Total Mastery marks: 0 of 0 marks

## MATH70064 Elliptic Curves Markers Comments

- Question 1      1 a and 1 b were generally solved correctly by majority of the students.  
1 c was a difficult part but the solutions were available on the course website as part of the exercises. So, it is disappointing that most students did not know how to do this (I had assumed that they study the solutions that I provided).
- Question 2      This was the easiest problem of the exam, and most students got high marks from it.
- Question 3      We had a lot of practice solving this type of problem. It is lengthy but most students who studied knew how to work this out. There were occasional errors in calculation.
- Question 4      Unfortunately, no one managed to solve this problem fully. This, I believe, is partly due to lack of time as we have seen several similar examples of this type as part of the coursework. Moreover, the solutions to 4a is actually available on the course website as part of the solutions to the exercises that I had provided. It is disappointing to see that students have not studied these solutions.
- Question 5      This was perhaps one of the more original questions. It is not hard but I think most students couldn't get to it as they ran out of time. Some people managed to solve it.