

## Elliptic Curves MT25: Solutions to Sheet 1 sections A and C

- (1) (a). We find rational points on each curve. This tells us that each curve is birational to  $\mathbb{P}^1$ , and hence birational to each other. For the first, we have  $(1, 1)$ . For the second, we have  $(1, 0)$ . So the points of the first conic are parameterised by  $t = \frac{y-1}{x-1} \in \mathbb{P}^1(\mathbb{Q})$ . To find a corresponding point on the second curve, we intersect  $Y = t(X-1)$  with the curve. We get the equation  $X^2 + t^2(X-1)^2 - 6tX(X-1) = 1$ . The coefficient of  $X^2$  is  $1 + t^2 - 6t$  and coefficient of  $X$  is  $-2t^2 + 6t$ . So if the intersection point is  $(x_1, y_1)$ , we have  $x_1 + 1 = \frac{2t^2 - 6t}{t^2 - 6t + 1}$ , and hence  $x_1 = \frac{t^2 - 1}{t^2 - 6t + 1}$ ,  $y_1 = \frac{2t(3t-1)}{t^2 - 6t + 1}$ . Substituting  $t = \frac{y-1}{x-1}$ , we get the rather unpleasant birational transformation from the first curve to the second

$$(x, y) \mapsto \left( \frac{(y-1)^2 - (x-1)^2}{(y-1)^2 - 6(y-1)(x-1) + (x-1)^2}, \frac{2(y-1)(3(y-1) - (x-1))}{(y-1)^2 - 6(y-1)(x-1) + (x-1)^2} \right).$$

- (b). We can rewrite the first equation as  $(\frac{Y}{(X+2)^3})^2 = X^3 + 1$ . So we can take the birational transformation

$$(x, y) \mapsto (x, \frac{y}{(x+2)^3}).$$

- (c). Over  $\mathbb{C}$ , we have the birational transformation  $(x, y) \mapsto (\sqrt{2}x, y)$ . Over  $\mathbb{Q}$ , the second curve is reducible, with irreducible components  $Y = \pm X$ . The first curve is irreducible. So the two curves are not birational over  $\mathbb{Q}$ . Alternatively, the first curve's only rational point is  $(0, 0)$ , whilst the second has infinitely many, so again they cannot be birational over  $\mathbb{Q}$ .

- (2) (a). The only points on  $Y^2 = X^3 + 2X$  over  $\mathbb{F}_5$  are:  $\mathbf{o}, (0, 0)$ . The group table is the same as that of  $C_2$  ("cyclic 2" group; i.e. the integers modulo 2 under addition), with 0, 1 replaced by  $\mathbf{o}, (0, 0)$ , respectively.

- (b). The only points on  $Y^2 = X^3 + 1$  over  $\mathbb{F}_5$  are:  $\mathbf{o}, (0, 1), (0, 4), (4, 0), (2, 2), (2, 3)$ . The point  $(2, 2)$  has order 6, and the group table is the same as that of  $C_6$  ("cyclic 6" group; i.e. the integers modulo 6 under addition), with 0, 1, 2, 3, 4, 5 replaced by  $\mathbf{o}, (2, 2), (0, 4), (4, 0), (0, 1), (2, 3)$ , respectively. Note that it's also correct to say that the group is  $C_2 \times C_3$ , since  $C_2 \times C_3$  is isomorphic to  $C_6$ .

- (3) We have:  $2YY' = 3X^2 + 4$ , and so the slope at the point  $(2, 4)$  is:  $(3 \cdot 2^2 + 4)/(2 \cdot 4) = 2$ . The line tangent to the curve at  $(2, 4)$  is:  $Y = 2X$ . The  $x$ -coordinate of the third point of intersection is therefore:  $2^2 - 2 - 2 = 0$ , with  $y$ -coordinate  $y = 2 \cdot 0 = 0$ . Hence,  $(2, 4) + (2, 4) + (0, 0) = \mathbf{o}$ , and so  $(2, 4) + (2, 4) = (0, -0) = (0, 0)$ . Now, note that we always have  $-(x, y) = (x, -y)$  and so  $-(0, 0) = (0, 0)$ , giving:  $2(0, 0) = \mathbf{o}$ . Hence,  $4(2, 4) = 2(0, 0) = \mathbf{o}$ . Also, check that  $3(2, 4) = 4(2, 4) - (2, 4) = -(2, 4) = (2, -4)$ . Summarising: the first 4 multiples of  $(2, 4)$  are:  $1(2, 4) = (2, 4)$ ,  $2(2, 4) = (0, 0)$ ,  $3(2, 4) = (2, -4)$ ,  $4(2, 4) = \mathbf{o}$ , and so 4 is the smallest positive multiple of  $(2, 4)$  equal to  $\mathbf{o}$ .

(9) (a). Let  $L$  be the tangent line to the curve at  $P$ , and let  $R$  be the third point of intersection; that is, the line and the curve meet at  $P, P, R$ . Then  $P + P + R = \mathbf{o}$ . Then,  $3P = \mathbf{o} \iff R = P \iff L$  intersects  $\mathcal{E}$  only at  $P$  (3 times).

(b). The Hessian matrix is:

$$\begin{pmatrix} -6X_0 & 0 & -2AX_2 \\ 0 & 2X_2 & 2X_1 \\ -2AX_2 & 2X_1 & -2AX_0 - 6BX_2 \end{pmatrix}$$

The determinant is:

$$\begin{aligned} & -6X_0(2X_2(-2AX_0 - 6BX_2) - (2X_1)(2X_1)) - 2AX_2(0 - (2X_2)(-2AX_2)) \\ & = 8(3AX_0^2X_2 + 9BX_0X_2^2 + 3X_0X_1^2 - A^2X_2^3). \end{aligned}$$

The only projective point  $(X_0, X_1, X_2)$  on the curve with  $X_2 = 0$  is  $(0, 1, 0) = \mathbf{o}$ , for which the statement is true, since  $3\mathbf{o} = \mathbf{o}$  and  $(X_0, X_1, X_2) = (0, 1, 0)$  makes the Hessian determinant 0. When  $X_2 \neq 0$ , we can write everything in affine form, with  $x = X_0/X_2$  and  $y = X_1/X_2$ , when we see that the Hessian determinant (after dividing through by  $8X_2^3$ ) is 0 exactly when:

$$3Ax^2 + 9Bx + 3xy^2 - A^2 = 0. \quad (1)$$

Also, the point  $P = (x, y) \neq \mathbf{o}$ , written in affine form, has order 3 exactly when  $2(x, y) = (x, -y)$  which happens if and only if the  $x$ -coordinate of  $2(x, y)$  is  $x$ . But, as usual, the  $x$ -coordinate of  $2(x, y)$  is  $m^2 - 2x$ , where  $m = (3x^2 + A)/(2y)$  (note that  $y \neq 0$  here, since  $y = 0$  would make  $P$  be of order 2). So,  $P$  being of order 3 implies  $((3x^2 + A)/(2y))^2 - 2x = x$ , that is:

$$-9x^4 - 6Ax^2 + 12xy^2 - A^2 = 0. \quad (2)$$

Finally, we use the fact the  $(x, y)$  is a point on the curve, so that  $y^2 = x^3 + Ax + B$ , and so we can replace  $y^2$  by  $x^3 + Ax + B$  in equations (1),(2). This makes both equations become the same equation:  $3x^4 + 6Ax^2 + 12Bx - A^2 = 0$ , as required.

(c). By part (b), the  $x$ -coordinate of any point of order 3 must be a root of the quartic  $3x^4 + 6Ax^2 + 12Bx - A^2$ , which has at most 4 roots  $x_1, \dots, x_4$ . Each  $x_i$  gives rise to at most two points  $(x_i, y_i), (x_i, -y_i)$  on the curve, giving at most 8 points of order 3. Together with  $\mathbf{o}$ , this gives at most 9 points that are 3-torsion.