

Elliptic Curves MT25: Solutions to Sheet 1

- (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 $\mathbf{o}$.

(4) (a). Case 1. m is odd. The birational transformation $(X, Y) \mapsto (X/f_m, Y/f_m^{(m+1)/2})$ [with inverse transformation: $(X, Y) \mapsto (Xf_m, Yf_m^{(m+1)/2})$] maps the given curve to: $f_m^{(m+1)}Y^2 = f_m^{(m+1)}X^m + \dots + f_0$, which is the same as: $Y^2 = X^m + c_{m-1}X^{m-1} + \dots + c_0$, where $c_i = f_i/f_m^{m+1-i} \in \mathbb{Q}$ [N.B. our birational transformation is legitimate, since $(m+1)/2$ is an integer]. So, our new right hand side is monic and is still defined over $\mathbb{Q}$. Now, write each $c_i = n_i/d_i$, where each $n_i, d_i \in \mathbb{Z}$, with each n_i, d_i coprime. Let d be the least common multiple of $d_0, \dots, d_{(m-1)}$; that is to say, d is the smallest integer divisible by all of the denominators of the coefficients c_i . Now, the birational transformation $(X, Y) \mapsto (Xd^2, Yd^m)$ [with inverse transformation: $(X, Y) \mapsto (X/d^2, Y/d^m)$] maps to the curve: $Y^2/d^{2m} = X^m/d^{2m} + c_{m-1}X^{m-1}/d^{2m-2} + \dots + c_0$, which is the same as: $Y^2 = X^m + g_{m-1}X^{m-1} + \dots + g_0$, where $g_i = c_id^{2(m-i)}$. But now, each $d_i|d$ and so each $c_id \in \mathbb{Z}$, giving that each $g_i \in \mathbb{Z}$, as required.

Case 2. f_m is a square. Let w be such that $f_m = w^2$. The birational transformation $(X, Y) \mapsto (X, Y/w)$ [with inverse transformation: $(X, Y) \mapsto (X, Yw)$] maps the given curve to: $f_mY^2 = f_mX^m + \dots + f_0$, which is the same as: $Y^2 = X^m + c_{m-1}X^{m-1} + \dots + c_0$, where $c_i = f_i/f_m \in \mathbb{Q}$. We are again in the situation where our right hand side is monic and is still defined over $\mathbb{Q}$. So now apply the same second birational transformation as in Case 1.

(b). The birational transformation $(X, Y) \mapsto (5X, 5^2Y)$ [with inverse $(X, Y) \mapsto ((1/5)X, (1/5^2)Y)$] maps the given curve to the curve: $Y^2 = X^3 + 75X^2 + 625$. The birational transformation $(X, Y) \mapsto (X + 25, Y)$ [with inverse $(X, Y) \mapsto (X - 25, Y)$] maps this to the curve: $Y^2 = X^3 - 1875X + 31875$, as required.

(5) To compute the group inverse, we need to find the tangent line through $(1, -1, 0)$. Using Lemma 1.40 in lecture notes as suggested, we compute that this tangent is $3X + 3Y = 0$, i.e. $Y = -X$. Substituting this into the equation of the curve gives $aZ^3 = 0$. The only point with $Z = 0$ and $Y = -X$ is $(1, -1, 0)$, so the tangent intersects the curve at $(1, -1, 0)$ with multiplicity three. Moreover, the inverse of a point (x, y, z) is given by the third point of intersection on the line joining (x, y, z) to $(1, -1, 0)$. This line has equation $z(X + Y) - (x + y)Z = 0$. We can check (or deduce from the symmetry in X and Y) that the third point of intersection with the curve is (y, x, z) .

To compute the doubling map, we first note that the tangent line through (x, y, z) has equation

$$x^2X + y^2Y + az^2Z = 0.$$

We need to compute the third point of intersection of this line with the curve $X^3 + Y^3 + aZ^3 = 0$. Substituting $Z = \frac{-x^2X - y^2Y}{az^2}$ gives

$$X^3(1 - \frac{x^6}{a^2z^6}) - X^2Y\frac{3x^4y^2}{a^2z^6} + \dots = 0.$$

This polynomial factorises as

$$(1 - \frac{x^6}{a^2z^6})(X - (x/y)Y)^2(X - (x'/y')Y)$$

and we need to compute x'/y' . We get $2(x/y) + (x'/y') = \frac{3x^4y^2}{a^2z^6x^6} = \frac{3x^4y^2}{(az^3+x^3)(az^3-x^3)} = \frac{3x^4}{y(x^3-az^3)}$. Rearranging gives

$$(x'/y') = \frac{x(x^3 + 2az^3)}{y(x^3 - az^3)} = \frac{x(az^3 - y^3)}{y(x^3 - az^3)}.$$

We deduce from this that the third point of intersection is (x', y', z') with

$$(z'/y') = \frac{-x^2x'/y' - y^2}{az^2} = \frac{z(y^3 - x^3)}{y(x^3 - az^3)}.$$

Rewriting the projective point by rescaling gives

$$(x', y', z') = (x(az^3 - y^3), y(x^3 - az^3), z(y^3 - x^3)).$$

We have $[2](x, y, z) = -(x', y', z') = (y', x', z')$ which gives

$$[2](x, y, z) = (y(x^3 - az^3), x(az^3 - y^3), z(y^3 - x^3))$$

as required.

It is probably easier to establish the formula for points $(x, y, 1)$ and then homogenize to get the general formula.

- (6) (a). Since $p \equiv 2 \pmod{3}$, we have $\gcd(3, p-1) = 1$, and so there exist $\lambda, \mu \in \mathbb{Z}$ such that $3\lambda + (p-1)\mu = 1$. For any $x, y \in \mathbb{F}_p^*$, we have $x^{p-1} = y^{p-1} = 1$ [by Fermat's Little Theorem], and so:

$$\begin{aligned} x^3 = y^3 &\Rightarrow (x^3)^\lambda \cdot 1^\mu = (y^3)^\lambda \cdot 1^\mu \Rightarrow (x^3)^\lambda \cdot (x^{p-1})^\mu = (y^3)^\lambda \cdot (y^{p-1})^\mu \\ &\Rightarrow x^{3\lambda+(p-1)\mu} = y^{3\lambda+(p-1)\mu} \Rightarrow x = y. \end{aligned}$$

Thus the map $x \mapsto x^3$ is injective on $\mathbb{F}_p^*$ and so is a bijection. Since $0^3 = 0$, the map is also a bijection on $\mathbb{F}_p$. Now, rearrange the equation of the curve as: $X^3 = Y^2 - A$. We see that, for each $Y = 0, \dots, p-1$ in $\mathbb{F}_p$, there is precisely one $X \in \mathbb{F}_p$ such that $X^3 = Y^2 - A$, giving rise to a total of precisely p affine points, which becomes $p+1$ points when we include the point at infinity.

(b). Since $p \equiv 3 \pmod{4}$, we have that $\left(\frac{-1}{p}\right) = -1$ [i.e. -1 is not congruent to a square mod p]. First note that $X = 0$ gives rise to precisely one point $(0, 0)$. Now, pair each $X \in \mathbb{F}_p^*$ with its negative $-X$ mod p . If $X(X^2 + B) = 0$ then the pair $X, -X$ gives rise to precisely two points: $(X, 0), (-X, 0)$. If $X(X^2 + B) \neq 0$ then one of $X(X^2 + B)$ and $-X(X^2 + B)$ will be a nonzero quadratic residue mod p and the other will be a quadratic nonresidue mod p [using the fact that -1 is a quadratic nonresidue mod p and the standard property of Legendre symbols that: $\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$]. Whichever one is a nonresidue will contribute no points; which one is a residue will contribute two points: $(X, Y), (X, -Y)$. In all cases, each pair $X, -X$ will contribute two points. This gives rise to a total of precisely p affine points, which becomes $p+1$ points when we include the point at infinity.

(7) (a). $(2, 0) + (-2, 0) = \mathbf{o}$, where $(-2, 0)$ is the inverse of $(2, 0)$; but we know that $(-2, 0) = (2, -0) = (2, 0)$ and so $(2, 0) + (2, 0) = \mathbf{o}$; that is, $(2, 0)$ is of order 2, as required.

(b). In general, a point (x, y) on $Y^2 = X^3 + f_2X^2 + f_1X + f_0$ has inverse: $(x, -y)$ and so (x, y) is of order 2 exactly when $(x, y) + (x, y) = \mathbf{o} \iff (x, y) = (x, -y)$. But $y = -y$ precisely when $y = 0$. So, we see that all points of order 2 are of the form $(x, 0)$ where x is a root of the cubic $X^3 + f_2X^2 + f_1X + f_0$. There are at most 3 such points over any field, since a cubic has at most 3 roots in any field. In the complex numbers, of course, there will always be exactly 3 such points. Applying this to the curve $Y^2 = X(X^2 - 3)$, we see that $X(X^2 - 3)$ has one $\mathbb{Q}$ -rational root $X = 0$, giving $(0, 0)$ as the only $\mathbb{Q}$ -rational point of order 2; the other two roots give the points $(\sqrt{3}, 0)$ and $(-\sqrt{3}, 0)$, which are the remaining two $\mathbb{C}$ -rational points of order 2. The curve $Y^2 = X^3 - 7$ has no $\mathbb{Q}$ -rational point of order 2 (since $X^3 - 7$ has no $\mathbb{Q}$ -rational roots); over $\mathbb{C}$, there are the 3 points of order 2 given by: $(\omega_1, 0), (\omega_2, 0), (\omega_3, 0)$, where $\omega_k = 7^{1/3}e^{2\pi i k/3}$, for $k = 0, 1, 2$. Finally, the curve $Y^2 = X(X - 1)(X - 7)$ has the points of order 2: $(0, 0), (1, 0), (7, 0)$ all of which are both $\mathbb{C}$ -rational and $\mathbb{Q}$ -rational. Group structures of the 2-torsion groups over $\mathbb{Q}$ for the three curves are clearly: C_2, C_1 and $C_2 \times C_2$, respectively (since all members except $\mathbf{o}$ have order 2).

(8) Using $2YY' = 3X^2$, we see that the slope of the curve at $(0, 2)$ is $3 \cdot 0^2 / (2 \cdot 2) = 0$, and so the tangent to the curve at $(0, 2)$ is the line: $Y = 2$. The x -coordinate of the third point of intersection is then: $0^2 - 0 - 0 = 0$, with corresponding y -coordinate 2. In summary: The line $Y = 2$ intersects the curve at $(0, 2)$ with multiplicity 3. Hence: $(0, 2) + (0, 2) + (0, 2) = \mathbf{o}$, and so: $3(0, 2) = \mathbf{o}$. But, $1(0, 2) = (0, 2)$ and $2(0, 2) = (0, -2)$, and so 3 is the smallest $k \geq 1$ such that $k(0, 2) = \mathbf{o}$; that is, $(0, 2)$ has order 3.

(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.