Elliptic Curves - Assignment 5

Matteo Durante, s2303760, Leiden University

9th April 2019

Exercise 2

Proof. (a) Consider an elliptic curve over $\mathbb{Q}$ defined by the equation $Y^2 + Y = X^3$ with a point $Q = (0, 0)$. Let $E \xrightarrow{\tau_Q} E$ be the map s.t. $P \mapsto P + Q$.

Observe that τ_Q is a rational map defined at every point of E, hence it is a morphism. Furthermore, it has an inverse rational map, namely the one given by the traslation by $-Q$, τ_{-Q}.

It follows that τ_Q is a curve automorphism.

Notice that $\tau_Q \neq \mathrm{Id}_E$ and, by applying the algorithm in [1, p. III.2.3], $Q + Q = 2Q = (0, -1)$. Since $2Q + Q = 3Q = O$, we get that $\tau_Q^3(P) = P + Q + Q + Q = P + 3Q = P + O = P$ for any $P \in E$, hence ours is a curve automorphism of order 3.

To show that it is not an elliptic curve automorphism we only have to show that it does not preserve the group structure, which is given by the fact that $\tau_Q(O) = O + Q = Q \neq O$, i.e. it does not preserve the zero-element. □

Proof. (b) Let $(x, y) = P \in E$. Let's start by considering $x \neq 0$. Using the group law algorithm in [1, p. III.2.3], we have $\tau_Q(P) = P + Q = (\frac{y^2}{x^2} - x, -\frac{y^3}{x^3} + y - 1)$. From (a), we have that $2Q = (0, -1)$, hence we get:

$$\tau_Q^2(P) = P + Q + Q = P + 2Q = \left(\frac{9x^4}{(2y+1)^2} - x, -\frac{27x^6}{(2y+1)^3} - \frac{2x^3 + y}{2y+1} - 1 \right)$$

Suppose instead that $x = 0$. From the equation of the curve, we get that $y = 0$ or $y = -1$, thus $P = (0, 0) = Q$ or $= (0, -1) = 2Q$.

If $P = Q$, we have the following:

$$\tau_Q^2(P) = \tau_Q^2(Q) = Q + Q + Q = 3Q = O$$

If $P = 2Q$, we have that:

$$\tau_Q^2(P) = \tau_Q^2(2Q) = 2Q + Q + Q = 4Q = Q$$

□

Proof. (c) We know that H is the subgroup generated by Q and E' is the elliptic curve described by $Y^2 + 3Y = X^3 - 9$. Consider the map $\phi(x, y) = (x + \frac{1}{x^2}, y - 1 - \frac{2y+1}{x^3})$, which we can describe projectively on $F \cap U_2$, the affine patch of the projectification of E corresponding to E itself, by setting $\phi(x : y : 1) = (x + \frac{1}{x^2} : y - 1 - \frac{2y+1}{x^3} : 1)$. Remember that F is described by homogenizing the equation defining E, which gives us $Y^2Z + YZ^2 = X^3$.

We verify that ϕ defines a map $E \to E'$. To do this, we just substitute $X = x + \frac{1}{x},\ Y = y - 1 + \frac{2y+1}{x^3}$ in $Y^2 + 3Y = X^3 - 9$ and check that the equality holds using the relation $y^2 + y = x^3$.

Next we check that ϕ is a morphism through the definition in [1, p. 12].

As required, ϕ is a rational map regular at every point $P \in E$ besides $O,\ Q$ and $2Q$. Multiplying throughout by $x^3 \in K(E)$, we get the map $\phi'(x : y : 1) = (x^4 + x : x^3y - x^3 - 2y - 1 : x^3)$, which is clearly regular at those remaining points of E.

Since E is defined over $\mathbb{Q}$, we see that $x^4 + x = 0$ if and only if $x = 0$ or $x^3 = -1$ and substituting these values in the equation $x^3y - x^3 - 2y - 1 = 0$ we get $y = 0$ and $= -1/2$ respectively. However, the points $(0, 0),\ (\zeta_3^i, -1/2),\ i = 0, 1, 2$ do not lie on E, hence there is no point in E whose image under ϕ' is $(0, 0)$. Using the definition, we can conclude that ϕ is indeed a morphism.

Now, since $F \cap U_2 = E$ and $Z \neq 0$ on U_2, we get $\phi(X : Y : Z) = \phi(x : y : 1) = (x + \frac{1}{x^2} : y - 1 - \frac{2y+1}{x^3} : 1)$, where $x = X/Z,\ y = Y/Z$. Substituting, we get the following:

$$\begin{aligned}
\left(x + \frac{1}{x^2} : y - 1 - \frac{2y+1}{x^3} : 1\right) &= \left(\frac{X}{Z} + \frac{Z^2}{X^2} : \frac{Y}{Z} - 1 - \frac{(2Y+Z)Z^2}{X^3} : 1\right) \\
&= \left(\frac{X}{Z} + \frac{XZ^2}{X^3} : \frac{Y}{Z} - 1 - \frac{(2Y+Z)Z^2}{Y^2Z + YZ^2} : 1\right) \\
&= \left(X + \frac{XZ^3}{Y^2Z + YZ^2} : Y - Z - \frac{(2Y+Z)Z^2}{Y^2 + YZ^2} : Z\right) \\
&= \left(X + \frac{XZ^2}{Y^2 + YZ} : Y - Z - \frac{(2Y+Z)Z^2}{Y^2 + YZ^2} : Z\right)
\end{aligned}$$

Substituting $O = (0 : 1 : 0)$ into the expression, we get $\phi(O) = \phi(0 : 1 : 0) = (0 : 1 : 0) = O$, thus ϕ is an isogeny. Also, from the expression for $\phi(x : y : 1)$ we have that $\phi(x : y : 1) = (x + \frac{1}{x^2} : y - 1 - \frac{2y+1}{x^3} : 1)$, which gives us $\phi(\tilde{Q}) = (0 : -1 : 0) = O$ and $\phi(2\tilde{Q}) = (0 : 1 : 0) = O$, where $\tilde{Q} = (0 : 0 : 1) \in F \cap U_2$ corresponds to $Q \in E$ and $2\tilde{Q} = (0 : -1 : 1) \in F \cap U_2$ to $2Q \in E$. This gives the inclusion $H \subset \ker(\phi)$.

Now, looking at the projective description of ϕ, we see that $\phi(X : Y : Z) = (0 : 1 : 0)$ implies that $X = 0$ or $Z = 0$.

If $Z = 0$, we get that $(X : Y : Z) = O$, while for $X = 0,\ Z \neq 0$, since the only points in E with X-coordinate are Q and $2Q$ and we know that $\phi(Q) = \phi(2Q) = O$, we have that $\ker(\phi) = \{O, Q, 2Q\} = H$. □

Exercise 4

Proof. We will begin by writing down the formulas we will be using.

Since the Weierstrass equation of the elliptic curve is given by $Y^2 + Y = X^3$, we have that $a_1 = a_2 = a_4 = a_6 = 0,\ a_3 = 1$. Now, for any point $(x_P, y_P) = P \in E$, we get $-P = (x_P, -y_P - 1)$. Also, setting $\lambda = \frac{3x_P^2}{2y_P+1}$, we get $x_{2P} = \lambda^2 - 2x_P,\ y_{2P} = -1 - \lambda^3 + 3\lambda x_P - y_P$.

Let's find the torsion points of order 2.

Such points would have to lie on E and have the property that $P = -P$, hence they correspond

to the solutions of the following system of equations:

$$\begin{cases} y_P^2 + y_P = x_P^3 \\ x_P = x_P \\ y_P = -y_P - 1 \end{cases} \quad \begin{cases} x_P^3 = -1/4 \\ y_P = -1/2 \end{cases} \quad \begin{cases} x_P = -\zeta_3^i / \sqrt[3]{4} \text{ for } i=0,1,2 \\ y_P = -1/2 \end{cases}$$

It follows that such points are $(-\frac{\zeta_3^i}{\sqrt[3]{4}}, \frac{1}{2})$ for $i = 0, 1, 2$.

Similarly, torsion points of order 3 would have to lie on E and have the property that $[2]P = -P$, hence they correspond to the solutions of the following system of equations:

$$\begin{cases} y_P^2 + y_P = x_P^3 \\ \lambda = \frac{3x_P^2}{2y_P+1} \\ \lambda^2 - 2x_P = x_P \\ -1 - \lambda^3 + 3\lambda x_P - y_P = -y_P - 1 \end{cases} \quad \begin{cases} y_P^2 + y_P = x_P^3 \\ \lambda = \frac{3x_P^2}{2y_P+1} \\ \lambda^2 = 3x_P \\ 3\lambda x_P = \lambda^3 \end{cases} \quad \begin{cases} y_P^2 + y_P = x_P^3 \\ \lambda = \frac{3x_P^2}{2y_P+1} \\ \lambda^2 = 3x_P \end{cases} \quad \begin{cases} y_P^2 + y_P = x_P^3 \\ 9x_P^4 = 3x_P(2y_P+1)^2 \end{cases}$$

$$\begin{cases} y_P^2 + y_P = x_P^3 \\ 3x_P y_P^2 + 3x_P y_P = 4x_P y_P^2 + 4x_P y_P + x_P \end{cases} \quad \begin{cases} y_P^2 + y_P = x_P^3 \\ x_P(y_P^2 + y_P + 1) = 0 \end{cases} \quad \begin{cases} y_P^2 + y_P = x_P^3 \\ x_P = 0 \ \vee \ y_P = \frac{-1\pm\sqrt{-3}}{2} \end{cases}$$

We will now discuss the solutions for the different values of x_P, y_P we have found.

Clearly, for $x_P = 0$ we get $(0, 0),\ (0, 1)$.

Now, for $y_P = \frac{-1\pm\sqrt{-3}}{2}$, we get $x_P^3 = -1/3$, hence $x_P = -\zeta_3^i / \sqrt[3]{3}$ for $i = 0, 1, 2$. It follows that the remaining solutions are $(-\frac{\zeta_3^i}{\sqrt[3]{3}}, \frac{-1\pm\sqrt{-3}}{2})$ for $i = 0, 1, 2$. □

References

[1] Silverman James Harris. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009.