Exercises PQC sheet 1 – Isogenies

1. This exercise lets you get familiar with isogenies, the main character of isogeny-based crypto. Let

$$E_1/\mathbb{F}_{17} : y^2 = x^3 + 1, \qquad E_2/\mathbb{F}_{17} : y^2 = x^3 - 10.$$

and

$$E_3/\mathbb{F}_{17} : y^2 = x^3 + 2x + 5.$$

   (a) Check that

$$f : (x, y) \mapsto ((x^3 + 4)/x^2, (x^3y - 8y)/x^3)$$

   defines a map $E_1 \to E_2$.

   (b) Determine the kernel of f.

   (c) What is the degree of f?

   (d) Calculate the points in the preimage of $(3, 0)$ under f.

   (e) Compute the number of points on $E_1(\mathbb{F}_{17}), E_2(\mathbb{F}_{17})$, and $E_3(\mathbb{F}_{17})$.

   (f) Compute $j(E_1), j(E_2)$, and $j(E_3)$.

   (g) Show that E_1 and E_2 are not isomorphic over $\mathbb{F}_{17}$ but that they are isomorphic over $\mathbb{F}_{17^2}$.

   (h) Check that

$$g : (x, y) \mapsto ((x^2 + x + 3)/(x + 1), (x^2y + 2xy + 15y)/(x^2 + 2x + 1))$$

   defines a map $E_1 \to E_3$.

   (i) Determine the kernel of g.

   (j) What is the degree of g?

2. Let ℓ be a prime. Show that there are $\ell + 1$ size-ℓ subgroups of $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.

3. Let $p = 419 = 4 \cdot 3 \cdot 5 \cdot 7 - 1$ and let $E_0 : y^2 = x^3 + x$.

   (a) Find a point P of order 105 on E_0. Compute $R = 35P$, a point of order 3.

(b) Compute τ_3, σ_3 and $f_3(x)$ for $\langle R \rangle$ to compute the curve coefficient B of the curve isogenous to E_0 under the 3-isogeny induced by R. You can verify your solution by checking the labeled graph for $p = 419$ in the bonus slides of the slide set.

(c) Compute the image $P' = \varphi_3(P)$ under the 3-isogeny and verify that the resulting point P' has order 35. Why does this happen?

(d) Compute $7P'$ and use it to compute the 5-isogeny, getting the curve parameter and the image $P'' = \varphi_5(P')$. Check that P'' has order 7 and that the curve matches the picture in the slides.

(e) Finally do the same for the 7 isogeny coming from P''.