Exercise week 3 – (C)SIDH

1. This exercise is a recap of isogenies from week one. Check theree for definitions. 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

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

   defines a map $E_1 \to E_2$.

   (b) Detemine 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

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

   defines a map $E_1 \to E_3$.

   (i) Determinne 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. Check that this matches the picture in the slides for part IV.

(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 part IV.

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

4. Let p be a prime with $p \equiv 3 \bmod 4$. Show that $E : y^2 = x^3 + x$ has $p + 1$ points.
Hint: You can argue similar to how I showed that the curve and its quadratic twist together have $2p+2$ points. Remember that in $\mathbb{F}_p^*$ there are exactly $(p-1)/2$ squares and as many non-squares.

5. The slides for part V say that there is a meet-in-the-middle attack on CSIDH. For the CSIDH-512 parameters explain how you would mount such an attack if you can use memory.
This attack and optimizations are the topic of week 6, but you should think through the easier version yourself.

6. Let $p = 431$ and note that $p + 1 = 432 = 2^4 \cdot 3^3$. The curve $E_0 : y^2 = x^3 + x$ is a supersingular curve over $\mathbb{F}_p$ and has $p + 1$ points. Consider the curve over $\mathbb{F}_{p^2}$ where it has $(p + 1)^2$ points. Find a basis of the 2^4 and the 3^3 torsion subgoups, i.e., find points P and Q of order 2^4 so that $\langle P \rangle \cap \langle Q \rangle = \{\infty\}$ and points R and S of order 3^3 so that $\langle R \rangle \cap \langle S \rangle = \{\infty\}$.
Hint: You can check this as $[8]P \neq [8]Q$ and $[9]R \neq \pm[9]S$.
Hint: For the 3^3 torsion points, remember how the negative direction is defined for CSIDH to find the independent points or use the solutions from week 1.

7. Let ℓ be a prime. Show that there exist $\ell + 1$ different isomorphism classes of curves, counted with multipliciy, that are ℓ-isogenous to a given supersingular elliptic curve $E/\mathbb{F}_{p^2}$. Note that the isogenies need not be defined over $\mathbb{F}_{p^2}$ but can be defined over an extension field.