Exercise sheet 5, 10 March 2022

We will work through these exercises on wonder.me; you can find the URL for the room in the Zulip chat. These are exercises to challenge your understanding of the lectures you have watched already, These are not for homework but for working on during the live session, ideally with a group of people..If you need a shared whiteboard I suggest you use https://webwhiteboard.com; one of you opens the board and then shares the url in the chat in your circle.

You can call me over by choosing "invite to circle". Please note, though, that if I am in another circle busy talking I will not come right away and invitations expire quickly. I will be in the bottom right space "Tanja's hideout" when I am not busy.

I expect you to use Sage or Magma for computing multiples of points.
For Sage, the following might be useful:

```
p=17
R.<x,y> = PolynomialRing(GF(p))
E0 = EllipticCurve(y^2-(x^3+x))
P=E0.random_point()
S=3*P
```

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

2. 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''.

3. 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.

4. 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.
   (For the low-memory version see the paper by Delfs and Galbraith, but here you're not supposed to report what that paper said but think through the easier version yourself.)

5. 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 points P and Q of order 2^4 so that $Q \notin \langle P \rangle$ and points R and S of order 3^3 so that $R \notin \langle S \rangle$.
   Hint: Remember how the negative direction is defined for CSIDH to find the independent points.

6. Let ℓ be a prime. Show that there exist $\ell + 1$ different isomorphism classes of curves 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.