**Cryptography, exercise sheet 2 for 14 Sep 2021**

We will work through these exercises on wonder.me; you can find the URL for the room in the Canvas announcement. These are exercises to challenge your understanding of the lectures you have watched already. These are not for homework.

You can call one of us over by choosing "invite to circle". Please note, though, that if we are in another circle busy talking we will not come right away and invitations expire quickly. So pick one of us who is in the TA corner, thus not occupied.

1. Show that
$$(x, y) + (-x, y) = (0, 1)$$
on a twisted Edwards curve $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$.
Note: The video already showed that the $x$ coordinate is 0, you need to show that the resulting $y$-coordinate equals 1.

2. Show that the following correctly computes doubling
$$2(x, y) = \Big(2xy/(ax^2 + y^2), (y^2 - ax^2)/(2 - ax^2 - y^2)\Big)$$
on a twisted Edwards curve $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$.

3. Find all points $(x_1, y_1)$ on the Edwards curve $x^2 + y^2 = 1 - 5x^2y^2$ over $\mathbb{F}_{13}$. Show how you can use symmetries in the curve equation. Do not solve this exercise by brute force over all pairs $x, y$.

4. Use the Jacobi criterion to show hat the Montgomery curve
$$M_{A,B} : Bv^2 = u^3 + Au^2 + u$$
is non-singular if $B \neq 0$ and $A \neq \pm 2$.

5. Let $Bv^2 = u^3 + Au^2 + u$ be a Montgomery curve over $\mathbb{F}_p$ and $(A + 2)/B$ be a square over $\mathbb{F}_p$.
Show that $(1, \pm\sqrt{(A + 2)/B})$ are points on the curve and that they double to $(0, 0)$ and thus have order 4.

6. Write 20210914 in binary and compute the coefficients of the presentation with window width $w = 3$.

7. Take the doubling formulas from exercise 2 and turn them into projective formulas using as few multiplications as possible.

8. Test your understanding of the Montgomery ladder by explaining it to a fellow student or one of the TAs.