Cryptography, exercise sheet 2 for 08 Sep 2026

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: We showed this for Edwards curves, show it for twisted Edwards curves. The main thing you need to show is 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. 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.

5. On twisted Edwards curves, simplify the addition formulas for the special case of doubling, i.e., for $P_1 = P_2$. Use the curve equation to reduce the number of multiplciations and squarings needed.

6. Take the doubling formulas for twisted Edwards curves and turn them into projective formulas using as few multiplications as possible.