Cryptography, exercise sheet 3 for 19 Sep 2023

1. 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.

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

3. Take the doubling formulas for twisted Edwards curves from exercise sheet 2 and turn them into projective formulas using as few multiplications as possible.

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

5. For this exercise you may (and should) use a computer algebra system like sage for doing the elliptic curve computations. You need to hand in your sage code, i.e. anything you typed, as part of your solution.

   The elliptic curve
   $$y^2 = x^3 + x + 3 \text{ over } \mathbb{F}_{43}$$
   has 47 points. The point $P = (19, 42)$ has order 47. The point $P_A = (28, 15)$ is a multiple of P. Use the BSGS method to compute the discrete logarithm $a = \log_P(P_A)$ of P_A with base P.
   Verify your result.
   Each point that you compute should be documented, i.e., all baby steps and all the giant steps until you find a match. You do not need to document the arihmetic steps taken in computing the elliptic-curve additions. $\boxed{\text{5 points}}$