Cryptology, homework sheet 3

Due 26 September 2023, 13:30

Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually.

1. For this exercise you can use your calculator or Pari-GP for basic arithmetic modulo 13 but not for more advanced calculations.

   The points $P = (6, 3)$ and $Q = (3, 7)$ are on the curve $E : x^2 + y^2 = 1 - 5x^2y^2$ over $\mathbb{F}_{13}$. Compute $R = 2P + Q$. Compute the birationally equivalent Montgomery curve $M : Bv^2 = u^3 + Au^2 + u$ and compute the images P', Q' and R' of P, Q and R on M. Compute $2P' + Q'$ on M using the Montgomery-curve addition and verify that the result equals R'. 9 points

2. 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

   $$y^2 = x^3 + x + 20 \text{ over } \mathbb{F}_{41}$$

   has 53 points. The point $P = (3, 38)$ has order 53. The point $P_A = (25, 34)$ 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, but you do need to documnet the verification. 6 points