Cryptology, homework sheet 1
Due 21 September 2021, 13:15

Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually.
For this exercise you can use your calculator or Pari-GP for basic arithmetic modulo 13 but not for more advanced calculations.

1. Verify that $P = (6, 3)$ 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'. 10 points

2. Show that points of the form $(\pm b, \pm b)$ on $x^2 + y^2 = 1 + dx^2y^2$ have order 8 if they exist.
   Hints:
   - Show that they double to a point of order 4, then argue that this implies order 8.
   - Make sure to check that your denominators are nonzero. **Note:** this exercise has been fixed to put $a = 1$.

   5 points