Cryptology, homework sheet 2

Due 22 September 2022, 10:30

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. 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 points