

## Cryptography, homework sheet 6

Due for 2MMC10: 15 October 2020, 10:45

and for Mastermath: 26 November 2020, 10:45

Submission is done by email to `crypto.course@tue.nl`.

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

1. Prove that for  $(x_1, y_1)$  and  $(x_2, y_2)$  on the circle  $x^2 + y^2 = 1$  also their sum  $(x_1, y_1) + (x_2, y_2) = (x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$  is on the circle.
2. Find all points  $(x, y)$  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  $x, y$ .
3. 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  $R'$ .