EINDHOVEN UNIVERSITY OF TECHNOLOGY

Homework #3

Student name: *Chengqi Liu (1954148), Maitraiyi Dandekar (1990136), Zakariae Jabbour (2039702)*

Course: *Cryptology (2MMC10)* – Professor: *Tanja Lange*
Due date: *September 26th, 2023*

1.

The curve E is an Edwards Curve with $d = -5$. The following calculations are on $\mathbb{F}_{13}$: Using the formula $(x_1, y_1) + (x_2, y_2) = (\frac{x_1y_2+x_2y_1}{1-5x_1x_2y_1y_2} \mod 13, \frac{y_1y_2-x_1x_2}{1+5x_1x_2y_1y_2} \mod 13)$,

$$\begin{aligned} R =& 2P + Q \\ =& 2(6,3) + (3,7) \end{aligned}$$

where

$$\begin{aligned} 2(6,3) =& (\frac{2*6*3}{1-5*6^2*3^2} \mod 13, \frac{3^2-6^2}{1+5*6^2*3^2} \mod 13) \\ =& (\frac{36}{-1619} \mod 13, \frac{-27}{1621} \mod 13) \\ =& (\frac{36 \mod 13}{-1619 \mod 13} \mod 13, \frac{-27 \mod 13}{1621 \mod 13} \mod 13) \\ =& (\frac{10}{6} \mod 13, \frac{12}{9} \mod 13) \end{aligned}$$

Because $(2, 13) = 1$, $\frac{10}{6} = \frac{10/2}{6/2} = \frac{5}{3} \mod 13$.
Because $(3, 13) = 1$, $\frac{12}{9} = \frac{12/3}{9/3} = \frac{4}{3} \mod 13$.

$$\begin{aligned} 2(6,3) =& (\frac{5}{3} \mod 13, \frac{4}{3} \mod 13) \\ =& (5*3^{-1} \mod 13, 4*3^{-1} \mod 13) \end{aligned}$$

Because $3 * 9 \mod 13 = 1$, $3^{-1} \mod 13 = 9$.

$$\begin{aligned} 2(6,3) =& (5*9 \mod 13, 4*9 \mod 13) \\ =& (6, 10) \end{aligned}$$