EINDHOVEN UNIVERSITY OF TECHNOLOGY

Homework #4

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

Course: *Cryptology (2MMC10)* – Professor: *Tanja Lange*
Due date: *October 3th, 2023*

1.

First, assume that the slope of the line is l. Calculate the addition and double formula of the elliptic curve.
Addition formula:

$$\begin{aligned} (x_p, y_p) + (x_q, y_q) &= (x_r, y_r) \\ l =& \frac{y_p - y_q}{x_p - x_q} \mod 41 \\ x_r =& l^2 - x_p - x_q \mod 41 \\ y_r =& l(x_p - x_r) - y_p \mod 41 \end{aligned}$$

Double formula:

$$\begin{aligned} 2(x, y) &= (x_r, y_r) \\ l =& \frac{3x^2 + a}{2y} = \frac{3x^2 + 1}{2y} \mod 41 \\ x_r =& l^2 - 2x \mod 41 \\ y_r =& l(x - x_r) - y \mod 41 \end{aligned}$$

Run the code "Get_R0_to_R3.py" to compute $R0 \sim R3$.
(It should be placed in the same directory as file "Pollard_rho.py" when running.)

```python
from Pollard_rho import kP_plus_mPA

if __name__=="__main__":
    p=53
    P_x=3
    P_y=38
    PA_x=25
    PA_y=34
    print("W0: ",kP_plus_mPA(2,3,P_x,P_y,PA_x,PA_y))
    print("R0: ",kP_plus_mPA(23,13,P_x,P_y,PA_x,PA_y))
    print("R1: ",kP_plus_mPA(19,11,P_x,P_y,PA_x,PA_y))
    print("R2: ",kP_plus_mPA(2,41,P_x,P_y,PA_x,PA_y))
    print("R3: ",kP_plus_mPA(25,37,P_x,P_y,PA_x,PA_y))
```

The output is:

```
W0: (20, 39)
R0: (23, 22)
R1: (30, 20)
R2: (0, 26)
R3: (27, 38)
```

So,

$$\begin{aligned} W_0 =& 2P + 3P_A = (20, 39) \\ R_0 =& 23P + 13P_A = (23, 22) \\ R_1 =& 19P + 11P_A = (30, 20) \\ R2 =& 2P + 41P_A = (0, 26) \\ R3 =& 25P + 37P_A = (27, 38) \end{aligned}$$

We define the 4 set S_0, S_1, S_2, S_3 as below:

$$\begin{aligned} S_0 =& \{x \in \mathbb{Z}_{41} : x \equiv 0 \mod 41\} \\ S_1 =& \{x \in \mathbb{Z}_{41} : x \equiv 1 \mod 41\} \\ S_2 =& \{x \in \mathbb{Z}_{41} : x \equiv 2 \mod 41\} \\ S_3 =& \{x \in \mathbb{Z}_{41} : x \equiv 3 \mod 41\} \end{aligned}$$

We define the step function $f(x, y)$ by $(x, y) + R_i$ when $i \equiv x(W) \mod 4$:

$$f(x, y) = \begin{cases} (x, y) + (23, 22), x \equiv 0 \mod 4 \\ (x, y) + (30, 20), x \equiv 1 \mod 4 \\ (x, y) + (0, 26), x \equiv 2 \mod 4 \\ (x, y) + (27, 38), x \equiv 3 \mod 4 \end{cases}$$

(You can find our codes in the file "Pollard_rho.py". The codes are relatively long and is less readable if we paste them here.)

Run the program "Pollard_rho.py" and get the output:

```
S0:(20,39) F0:(20,39)
S1:(21,35) F1:(11,3)
S2:(11,3) F2:(7,1)
```

S3:(23,22) F3:(34,30)

S4:(7,1) F4:(23,19)

S5:(30,20) F5:(3,3)

S6:(34,30) F6:(39,16)

S7:(9,26) F7:(16,14)

S8:(23,19) F8:(13,37)

S9:(11,38) F9:(39,25)

S10:(3,3) F10:(40,10)

S11:(29,24) F11:(23,19)

S12:(39,16) F12:(3,3)

S13:(0,15) F13:(39,16)

S14:(16,14) F14:(16,14)

The answer is: 23

The result is verified to be correct.