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 $(x_1, y_1) + (x_2, y_2) = (\frac{x_1y_2+x_2y_1}{1-5x_1x_2y_1y_2} \mod 13, \frac{y_1y_2-x_1x_2}{1+5x_1x_2y_1y_2} \mod 13)$,

$$\begin{aligned}R =& 2P + Q\\ =& 2(6,3) + (3,7)\\ =& (6,10) + (3,7)\\ =& (12,0)\end{aligned}$$

Edwards Curve is a kind of Twisted Edwards Curve with $a = 1$. In $M : 5v^2 = u^3 + 3u^2 + u$, we have

$$\begin{aligned}A =& 2\frac{a+d}{a-d} = 3 \mod 13\\ B =& \frac{4}{a-d} = 5 \mod 13\end{aligned}$$

So,

$$M : 5v^2 = u^3 + 3u^2 + u$$

The formula of mapping from Edwards Curve E to Montgomery Curve M is $(x, y) \to (u, v) = (\frac{1+y}{1-y} \mod 13, \frac{1+y}{x(1-y)} \mod 13)$. So,

$$\begin{aligned}P =& (6,3) \to P' = (11,4)\\ Q =& (3,7) \to Q' = (3,1)\\ R =& (12,0) \to R' = (1,12)\end{aligned}$$

Suppose the slope of a line through the two points is l. The double formula on M is $2(u, v) = (u', v')$, where

$$\begin{aligned}l =& \frac{3u^2 + 2Au + 1}{2Bv} = \frac{3u^2 + 6u + 1}{10v} \mod 13\\ u' =& Bl^2 - A - 2u = 5l^2 - 3 - 2u \mod 13\\ v' =& l(u - u') - v \mod 13\end{aligned}$$

So,

$$2P' = (6, 1), \text{ with } l = 1$$

The addition formula on M is $(u_1, v_1) + (u_2, v_2) = (u_3, v_3)$, where

$$\begin{aligned} l =& \frac{v_2 - v_1}{u_2 - u_1} \mod 13 \\ u' =& Bl^2 - A - u_1 - u_2 = 5l^2 - 3 - u_1 - u_2 \mod 13 \\ v' =& l(u - u_1) - v_1 \mod 13 \end{aligned}$$

So,

$$2P' + Q' = (6, 1) + (3, 1) = (1, 12) \text{ with } l = 0$$

So we get $2P' + Q' = R'$.

2.

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:

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

You can also find our codes in the file "BSGS.py".

```
import math
from Crypto.Util.number import inverse


a=1
b=20
```

```
def Double(x,y,modn):
  '''Double the point (x,y) modulo modn. Result is (x_r,y_r).'''
  if math.isinf(x) or math.isinf(y):
    return math.inf,math.inf
  l=(3*x*x+a)*inverse(2*y,modn)%modn
  x_r=(l*l-2*x)%modn
  y_r=(l*(x-x_r)-y)%modn
  return x_r,y_r

def Add(x_p,y_p,x_q,y_q,modn):
  '''Add two poins (x_p,y_p) and (x_q,y_q) modulp modn. Result is
     (x_r,y_r).'''
  if math.isinf(x_p):
    return x_q,y_q
  if math.isinf(x_q):
    return x_p,y_p
  if x_p==x_q and y_p!=y_q:
    return math.inf,math.inf
  if x_p==x_q and y_p==y_q:
    return Double(x_p,y_p,modn)
  l=(y_p-y_q)*inverse((x_p-x_q),modn)%modn
  x_r=(l*l-x_p-x_q)%modn
  y_r=(l*(x_p-x_r)-y_p)%modn
  return x_r,y_r

def Power(x,y,exp,modn):
  '''Calculate the exp times of the point (x,y) modulo modn. Result is
     (x_r,y_r).'''
  n=1
  x_r=x
  y_r=y
  while n<exp:
    x_r,y_r=Add(x_r,y_r,x,y,modn)
    n=n+1
  return x_r,y_r

def BSGS(x_A,y_A,x,y,order,modn):
  '''
  Solve DLP using Baby Step Giant Step.
  Return log_{(x,y)}(x_A,x_A) modulo modn.
```

```
    The point (x,y) has order "order".
    '''
    t=math.floor(math.sqrt(order))
    _xt,_yt=Power(x,y,t,modn)
    k=1
    _xkt=_xt
    _ykt=_yt
    g_map=dict()
    g_map[(_xt,_yt)]=k
    while k<math.floor(order/t):
        k=k+1
        _xkt,_ykt=Add(_xkt,_ykt,_xt,_yt,modn)
        g_map[(_xkt,_ykt)]=k
    i=1
    while i<t+1:
        _xi,_yi=Power(x,y,i,modn)
        _xAi,_yAi=Add(x_A,y_A,_xi,_yi,modn)
        if (_xAi,_yAi) in g_map:
            return (g_map[(_xAi,_yAi)]*t-i)%modn
        i=i+1
    return -1

if __name__=="__main__":
    modn=41
    p=53
    P_x=3
    P_y=38
    PA_x=25
    PA_y=34
    print("The answer is:",BSGS(PA_x,PA_y,P_x,P_y,p,modn))
```

Run the program and get the output:
The answer is: 23