EINDHOVEN UNIVERSITY OF TECHNOLOGY

Homework #1

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

Course: *Cryptology (2MMC10)* – Professor: *Tanja Lange*
Due date: *September 12th, 2023*

1.
Use Python programming to solve this problem.

```
Px=1000
Py=2
PAx=837670
PAy=538535
p=1000003
a=1
x=Px
y=Py
while not (x ==PAx and y ==PAy):
    x_2=(x*Py+y*Px)%p
    y_2=(y*Py-x*Px)%p
    a=a+1
    x=x_2
    y=y_2

print("a is: "+str(a))
```

Run the program and it gives the result "a is: 271828".
Therefore, we find the integer $a = 271828$ with $P_A = aP$.
You can find this program in the file "Question1.py".

2.
Show:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1y_1x_2y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1y_1x_2y_2}\right)$$

$\forall P = (x, y) \in x^2 + y^2 = 1 + dx^2y^2$:

$$
\begin{aligned}
P + (0,1) =& (\frac{1x + 0y}{1 + 0dxy}, \frac{y - 0x}{1 - 0dxy}) = (x, y) = P \\
(0,1) + P =& (\frac{0y + 1x}{1 + 0dxy}, \frac{y - 0x}{1 - 0dxy}) = (x, y) = P
\end{aligned}
$$

So. $P + (0,1) = (0,1) + P = P$. $(0,1)$ is the neutral element with respect to the addition law on an Edwards curve.
$\forall P = (x, y) \in x^2 + y^2 = 1 + dx^2y^2$:

$$
2P = (\frac{2xy}{1 + dx^2y^2}, \frac{y^2 - x^2}{1 - dx^2y^2})
$$

So,

$$
\begin{aligned}
2(0,-1) =& (\frac{0}{1+0}, \frac{1-0}{1-0}) = (0,1) \\
4(\pm 1, 0) =& 2(\frac{0}{1+0}, \frac{0-1}{1-0}) = 2(0,-1) = (0,1)
\end{aligned}
$$

So, $(0,-1)$ has order 2 and $(\pm 1, 0)$ have order 4.

3.

Show:

First check the existence of the points $(\pm b, \pm b), b \in \mathbb{R}$.

$$
\begin{aligned}
&\exists (\pm b, \pm b) \in x^2 + y^2 = 1 + dx^2y^2 \\
\Leftrightarrow & 2b^2 = 1 + db^4 \text{ has a solution} \\
\Leftrightarrow & db^4 - 2b^2 + 1 = 0 \text{ has a solution}
\end{aligned}
$$

Let $x = b^2 \geq 0$, $f(x) = dx^2 - 2x + 1$. So $f(x)$ is a quadratic function. It equals $f(x) = 0$ having a solution. By the definition of Edwards curve, $d \notin \{0, 1\}$.
When $d < 0$, according to the properties of quadratic functions, $\lim_{x \to +\infty} f(x) = -\infty$, $f(0) = 1 > 0$. So, there must be a solution in $(0, +\infty)$.
When $d > 0$, $f_{min}(x) = f(\frac{1}{d}) = \frac{d-1}{d}$. Because $f_{min}(x) \leq 0$ and $d \notin \{0, 1\}$, we get $d \in (0, 1)$.
So, when $d \in (-\infty, 0) \cup (0, 1)$, the points $(\pm b, \pm b), b \in \mathbb{R}$ exist.

Second, show they have order 8:
Because $(\pm b, \pm b) \in x^2 + y^2 = 1 + dx^2y^2$, $2b^2 = 1 + db^4$.

If $1 - db^4 = 0$, $d = \frac{1}{b^4}$.

$$\begin{aligned} & 2b^2 = 1 + db^4 \\ \Rightarrow & 2b^2 = 2 \\ \Rightarrow & b = \pm 1 \\ \Rightarrow & d = 1 \end{aligned}$$

But we have $d \notin \{0, 1\}$. It's a contradiction. So, $1 - db^4 \neq 0$.

$$\begin{aligned} 2(\pm b, \pm b) = & \left(\frac{2b^2}{1 + db^4}, \frac{0}{1 - db^4}\right) \\ = & \left(\frac{2b^2}{1 + db^4}, 0\right) \\ = & \left(\frac{2b^2}{2b^2}, 0\right) \\ = & (1, 0) \end{aligned}$$

From the question 2, we have shown that $(1, 0)$ has order 4. $4(1, 0) = (0, 1)$. So,

$$\begin{aligned} 8(\pm b, \pm b) = & 4(2(\pm b, \pm b)) \\ = & 4(1, 0) \\ = & (0, 1) \end{aligned}$$

In all, when $d \in (-\infty, 0) \cup (0, 1)$, the points $(\pm b, \pm b), b \in \mathbb{R}$ exist, and have order 8.