MA 4100 - CS 4710: Elliptical Curve Worksheet

1 Introduction

We will consider the Elliptical Curve given by

$$y^2 \equiv x^3 + ax + b \mod p \tag{1}$$

where p is prime and $4a^3 + 27b^2 \not\equiv 0 \mod p$. We will use the following addition equations below.

Given $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ in $EC_p(a, b) \setminus \{O\}$

$$\lambda = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} \mod p: & \text{if } P \neq Q \\ \frac{3x_P^2 + a}{2y_P} \mod p: & \text{if } P = Q \end{cases}$$

$$\begin{aligned} x_R &= (\lambda^2 - x_P - x_Q) \mod p \\ y_R &= \lambda(x_P - x_R) - y_P \mod p \end{aligned} \tag{2}$$

where $P + Q = R = (x_R, y_R)$.

Note:

1. $O \in EC_p(a, b)$.
2. For any $P \in EC_p(a, b)$ we have $P + O = O + P = P$.
3. For any $P = (x_P, y_P) \in EC_p(a, b)$ we have $-P = (x_P, -y_P)$. That is,

$$(x_P, y_P) + (x_P, -y_P) = O.$$

EXAMPLE: For $EC_7(1, 1)$ we consider the equation

$$y^2 \equiv x^3 + x + 1 \mod 7.$$

- Note $(0, 1) \in EC_7(1, 1)$ by noting the follwing equation holds:

$$y^2 \equiv x^3 + x + 1 \mod 7$$
$$(1)^2 \equiv 0^3 + 0 + 1 \mod 7.$$

PROBLEM: Verify $(2, 2) \in EC_7(1, 1)$.

- We will find all points $P = (2, y_P) \in EC_7(1, 1)$. Note if $x_p = 2$ we have that $y^2 \equiv 2^3 + 2 + 1 \equiv 4 \mod 7$. So we need to find all elements in $y_P \in \mathbb{Z}_7$ where $y_P^2 \equiv 4 \mod 7$. I will simply test each element to find there are only two such elements: $y_P = 2$ and $y_P = 5$. So all such points are: $(2, 2)$ and $(2, 5)$.

PROBLEM: Find all points $P = (0, y_P) \in EC_7(1, 1)$.
PROBLEM: Find all points $P = (3, y_P) \in EC_7(1, 1)$.

We will compute $(2,2)+(0,1)$. Let $P=(2,2)$ and $Q=(0,1)$. Thus

$$\lambda \equiv \frac{1-2}{0-2} \equiv \frac{1}{2} \equiv 4 \mod 7 \text{ since } 2\cdot 4 \equiv 1 \mod 7.$$

$$\begin{aligned} x_R &\equiv \lambda^2 - x_P - x_Q \mod 7 \equiv 4^2 - 2 - 0 \equiv 0 \mod 7 \\ y_R &\equiv 4(2-0) - 2 \equiv 6 \mod 7. \end{aligned} \tag{3}$$

Thus $P+Q=R=(0,6)$.
PROBLEM: Compute $(2,2)+(2,2)$ and $(2,2)+(0,6)$.

Note $EC_7(1,1)=\{(0,1),(0,6),(2,2),(2,5),O\}$. Also note for our above calculations we see that

$$\begin{aligned} 1\cdot(2,2) &= (2,2) \\ 2\cdot(2,2) &= (2,2)+(2,2)=(0,1) \\ 3\cdot(2,2) &= (2,2)+(2,2)+(2,2)=(0,6) \\ 4\cdot(2,2) &= (2,2)+(2,2)+(2,2)+(2,2)=(2,5) \\ 5\cdot(2,2) &= (2,2)+(2,2)+(2,2)+(2,2)+(2,2)=O \end{aligned} \tag{4}$$

Definition: We say $n \in \mathbb{N}$ is the order of some $G \in EC_p(a,b)$ if n is the smallest number so that $n\cdot G = O$.

So the order of $(2,2)$ in $EC_7(1,1)$ is 5.
PROBLEM: Compute the order of $(0,1)$ in $EC_7(1,1)$.

2 Encipering and Deciphering

How do we use elliptical curves to encipher messages?

1. Publicly agree on some G an element of some $EC_p(a,b)$.

2. Person A selects some $n_A < n$ where n is the order of G. And publishes $P_A = n \cdot G$ (note P_A is a point in $EC_p(a,b)$).

3. Person B selects some $n_B < n$ where n is the order of G. And publishes $P_B = n \cdot G$ (note P_A is a point in $EC_p(a,b)$).

SUMMARY	
Public	G, $EC_p(a,b)$, P_A and P_B
Private (for Person A)	n_A
Private (for Person B)	n_B

TO ENCIPHER: Let P_m be a plaintext block represented by a point in $EC_p(a,b)$ that Person A is sending to Person B. Person A chooses, at random, some $k \in \mathbb{N}$. Then Person A computes the pair $C_m = \{k\cdot G, P_m + kP_B\}$ of points in $EC_p(a,b)$. And sends C_m to Person B.

TO DECIPHER: Person B simply computes $P_m + kP_B - n_Bk\cdot G = P_m + kn_B \cdot G - n_Bk \cdot G = P_m$.

EXAMPLE:

We will use $EC_{23}(1,1)$ and $G = (0,1)$ which has order 28 (see calculation worksheet). We will use the follwing equivalence to the alphabet:

a	b	c	d	e	f	g
(0,1)	(0,22)	(1,7)	(1,16)	(3,10)	(3,13)	(4,0)
h	i	j	k	l	m	n
(5,4)	(5,19)	(6,4)	(6,19)	(7,11)	(7,12)	(9,7)
o	p	q	r	s	t	u
(9,16)	(11,3)	(11,20)	(12,4)	(12,19)	(13,7)	(13,16)
v	w	x	y	z	unused	unused
(17,3)	(17,20)	(18,3)	(18,20)	(19,5)	(19,18)	O

- Person A will select privately $n_A = 7$ and publish $P_A = 7 \cdot (0,1) = (11,3)$.
- Person B will select privately $n_B = 11$ and publish $P_B = 11 \cdot (0,1) = (1,16)$.

Mission is for Person A to encipher P = "Cake". So

P_1	P_2	P_3	P_4
C	A	K	E
$(1,7)$	$(0,1)$	$(6,19)$	$(3,10)$

(5)

Person A selects $k = 3$ at random. So

$$\begin{aligned} C_1 &= \{k \cdot G, P_1 + k \cdot P_B\} \\ &= \{3 \cdot (0,1), (1,7) + 3 \cdot (1,16)\} \\ &= \{(3,13), (1,7) + (18,3)\} \\ &= \{(3,13), (7,12)\} \end{aligned} \tag{6}$$

And C_2, C_3 and C_4 are computed similarly.
Person A receives C_1, C_2, C_3 and C_4 and deciphers as follows:

$$\begin{aligned} P_1 &= (P_1 + k \cdot P_B) - n_B k \cdot G \\ &= (7,12) - 11 \cdot (3,13) \\ &= (7,12) - (18,3) \\ &= (7,12) + (18,20) \\ &= (1,7) = c \end{aligned} \tag{7}$$

PROBLEM: Compute C_2, C_3 and C_4.