BRAC UNIVERSITY

Inspiring Excellence

CSE-447
Assignment - 03

Submitted By:
Mohammad Shafkat Hasan
Section: 01
ID: 19101077

Date of Submission:
13th August 2023

ID : 19101077

Ans. To The Q. (a)

Given,

Elliptic Curve E : $y^2 = x^3 - 2x + 2 \pmod{23}$

and Point $P = (4, 9)$

We need to determinate 2P and 3P

Evaluating 2P:

We know, $2P = P + P \rightarrow$ Doubling

For doubling, $s = \dfrac{3x_1^2 + a}{2y_1} \bmod P$

$x_3 = s^2 - x_1 - x_2 \bmod P$

Here,

$p = (x_1, y_1) = (4, 9)$

$\therefore x_1 = 4$ & $y_1 = 9$

comparing, $y^2 = x^3 - 2x + 2 \bmod 23$

with $y^2 = x^3 + ax + b \bmod P$

So, $a = -2$ $\quad P = 23$

$b = 2$

$\therefore s = \dfrac{3(4)^2 + (-2)}{2(9)} \bmod 23$

$= \dfrac{23}{9} \bmod 23$

$= 23 * 9^{-1} \quad mod \quad 23$

~~$\therefore 5 = 414$~~

$= 23 * 18 \quad mod \quad 23$

$= 414 \quad mod \quad 23$

$\therefore 5 = 0$

$9^{-1} \; mod \; 23 = -5 + 23 = 18$

q	r1	r2	r	t1	t2	t
2	23	9	5	0	1	-2
1	9	5	4	1	-2	3
1	5	4	1	-2	3	-5
4	4	1	0	3	$\boxed{-5}$	23

$t = t_1 - q t_2$

$= 0 - 2 \times 1 = -2$

$= 1 - 1 \times (-2)$

$= 1 + 2 = 3$

$= -2 - 1 \times (3) = -5$

$= 3 - 4 \times (-5) = 23$

$2P = (4, 9) + (4, 9)$

$x_3 = 5^{r} - x_1 - x_2 \; mod \; P$

~~171388~~

$= (\cancel{41}0)^{r} - 8 \; mod \; 23$

~~$= 171388 \; mod \; 23$~~

$= 15$

$$\begin{array}{r} 23 \\ -\ 8 \\ \hline 15 \end{array}$$

$y_3 = 5 \, (x_1 - x_3) - y_1 \; mod \; 23$

$= \cancel{44}0 \, (4 - 15) - 9 \; mod \, 23$

~~$= -4563 \; mod \; 23$~~

$$\begin{array}{r} 23 \\ -\ 9 \\ \hline 14 \end{array}$$

~~4563 mod 23 = 9~~

$= \cancel{21} - 9 \; mod \; 23$

$= 14$

$\therefore 2P \, (x_3, y_3) = (15, 14)$

(Ans)

ID : 19101077

Evaluating 3P:

We know, $3P = \cancel{2}P + 2P$ → Addition

$= (4, 9) + (15, 14)$

For Addition, $s = \dfrac{y_2 - y_1}{x_2 - \cancel{y_1}} \bmod p$

Here,

$(x_1, y_1) = (4, 9)$ and $(x_2, y_2) = (15, 14)$

$a = -2$ $\qquad p = 23$

$b = 2$

$\therefore s = \dfrac{14 - 9}{15 - 4} \bmod 23$

$= \dfrac{5}{11} \bmod 23$

$= 5 * 11^{-1} \bmod 23$

$= 5 * 21 \bmod 23$

$= 105 \bmod 23$

$\therefore s = 13$

$11^{-1} \bmod 23 = (-2 + 23) = 21$

q	r_1	r_2	r	t_1	t_2	t
2	23	11	1	0	1	-2
11	11	1	0	1	$\boxed{-2}$	23

$t = t_1 - q t_2$

$= 0 - 2(1) = -2$

$= 1 - 11(-2) = 23$

$x_3 = s^2 - x_1 - x_2 \mod p$

$= (13)^2 - 4 - 15 \mod 23$

$= 150$~~00~~ $\mod 23$

$= 12$

$y_3 = s(x_1 - x_3) - y_1 \mod p$

$= 13(4 - 12) - 9 \mod 23$

$= $ ~~-849~~ $-113 \mod 23$

$\boxed{\begin{array}{c} 113 \\ \text{mod} \\ 23 \\ = 21 \end{array}}$ $= -21 \mod 23$

$\boxed{\begin{array}{r} 23 \\ -21 \\ \hline 2 \end{array}}$ $= 2$

~~$\therefore 3P = (x_3, y_3) = (102, 2)$~~

$= 3P = (x_3, y_3) = (12, 2)$

(Ans)

ID: 19101077

Ans. To The Q. ~~No~~(b)

Here,

$y^2 = x^3 - 2x + 2 \mod 23$

$P = (4, 9)$ $\quad a = 3, b = 6$

Alice

$a = 3$

$a \cdot P$

$= 3(4, 9)$

$= (12, 2)$

Bob

$b = 6$

$b \cdot P$

$= 6(4, 9)$

$= (15, 9)$

$\xrightarrow{a \cdot P}$

$\xleftarrow[b \cdot P]{}$

$6 \cdot (12, 2)$

$= (15, 14)$

$3 \cdot (15, 9)$

~~$= (15, 9)$~~

$= (15, 14)$

Shared key $= 15$