Muhammad Izham Bin Norhamadi
B032020039

# Tutorial 5.1: ECC over prime field P

**Instruction: Take your *i* = 10 + (ID mod 100 or nearest assigned number).**

Step 0: My sample number is ***i*=10+39=49**. I am taking $P_1(x_1, y_1)$ = **(22,95)**.

Table 5: A list of points on a curve E: $y^2 = x^3 - 4x + 7 \pmod{257}$

| $i$ | $x_i$ | $y_i$ | $i$ | $x_i$ | $y_i$ | $i$ | $x_i$ | $y_i$ |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 21 | 161 | 136 | 41 | 34 | 232 |
| 2 | 239 | 186 | 22 | 193 | 197 | 42 | 57 | 184 |
| 3 | 46 | 28 | 23 | 72 | 211 | 43 | 65 | 47 |
| 4 | 97 | 131 | 24 | 114 | 2 | 44 | 209 | 173 |
| 5 | 18 | 192 | 25 | 142 | 255 | 45 | 96 | 104 |
| 6 | 49 | 36 | 26 | 103 | 154 | 46 | 147 | 128 |
| 7 | 50 | 231 | 27 | 16 | 21 | 47 | 130 | 200 |
| 8 | 28 | 197 | 28 | 44 | 132 | 48 | 172 | 130 |
| 9 | 112 | 53 | 29 | 36 | 197 | 49 | 22 | 95 |
| 10 | 22 | 162 | 30 | 36 | 60 | 50 | 112 | 204 |
| 11 | 172 | 127 | 31 | 44 | 125 | 51 | 28 | 60 |
| 12 | 130 | 57 | 32 | 16 | 236 | 52 | 50 | 26 |
| 13 | 147 | 129 | 33 | 103 | 103 | 53 | 49 | 221 |
| 14 | 96 | 153 | 34 | 142 | 2 | 54 | 18 | 65 |
| 15 | 209 | 84 | 35 | 114 | 255 | 55 | 97 | 126 |
| 16 | 65 | 210 | 36 | 72 | 46 | 56 | 46 | 229 |
| 17 | 57 | 73 | 37 | 193 | 60 | 57 | 239 | 71 |
| 18 | 34 | 25 | 38 | 161 | 121 | 58 | 1 | 255 |
| 19 | 79 | 224 | 39 | 141 | 183 | 59 | -1 | -1 |
| 20 | 141 | 74 | 40 | 79 | 33 | 60 | 1 | 2 |

Choose a prime number as a maximum. Let ***p*=257**.

1. Choose a random sample $a = -4$ and $b = 7$ for the curve

$$E: y^2 = x^3 + ax + b$$

such that $4a^3 + 27b^2 \neq 0 \pmod{p}$.

Muhammad Izham Bin Norhamadi
B032020039

2. Choose a base Point $P_1(x_1, y_1) = (x_i, y_i)$. Compute $P_2(x_2, y_2) = 2 \otimes P_1(x_1, y_1)$
   **Double Point**
   Let $(x_1, y_1)$ be a point on an elliptic curve $E(F_p)$, and $(x_1, y_1) \neq (x_2, -y_2)$
   then let $(x_2, y_2) = 2 \otimes (x_1, y_1)$ such that

$$x_2 = \left( \frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1 \quad \text{and} \quad y_2 = \frac{3x_1^2 + a}{2y_1} \cdot (x_1 - x_2) - y_1$$

Let slope of the tangent line

$$c = \frac{3x_1^2 + a}{2y_1},$$

then

$$x_2 = c^2 - 2x_1 \text{ and } y_2 = c\,(x_1 - x_2) - y_1.$$

**Take $2y_1 = 2 \cdot 95 = 190$ (mod 257).**

First, we need to compute an inverse of denominator $(2y_1)^{-1} \equiv (190)^{-1} = 23$ **(mod 257)** using Extended Euclidean Algorithm in excel.

Extended Euclidean Algorithm

| *i* | *b* = | *a* * | *q* | + | *r* | *u* | *v* | *w* = *u* - *vq* |
|---|---|---|---|---|---|---|---|---|
| 0 | 257 | 190 | 1 | | 67 | 0 | 1 | -1 |
| 1 | 190 | 67 | 2 | | 56 | 1 | -1 | 3 |
| 2 | 67 | 56 | 1 | | 11 | -1 | 3 | -4 |
| 3 | 56 | 11 | 5 | | 1 | 3 | -4 | 23 |

If w is in negative add 257

**The answer is $190^{-1} \equiv 23$**

Second, we compute the slope of the tangent line

$$c = \frac{3x_1^2 + a}{2y_1} = [3(22)^2 - 4](23) = [3 \cdot 484 - 4](23)$$

$$= 1448(23) = 33304 = 151 \pmod{257}$$

Third, we can start compute the

$x_2 = c^2 - 2x_1 = 151^2 - 2 \cdot 22 = 22801 - 44 = 141$ **(mod 257)**

Muhammad Izham Bin Norhamadi
B032020039

Fourth, we can compute

$$
\begin{aligned}
y_2 &= c(x_1 - x_2) - y_1 \\
&= 151 \cdot (22 - 141) - 95 \\
&= 151 \cdot (-119) - 95 \\
&= -17969 - 95 \\
&= -18{,}064 \\
&= 183 \pmod{257}
\end{aligned}
$$

A double point here is $\mathbf{P_2(x_2, y_2) = (141, 183)}$

**3. Add Point**

To compute $P_3(x_3, y_3) = P_1(x_1, y_1) \oplus P_2(x_2, y_2) = (103, 103) \oplus (50, 231)$.

Let $(x_1, y_1)$ and $(x_2, y_2)$ are two points on an elliptic curve $E(F_p)$, and $(x_1, y_1) \neq (x_2, \pm y_2)$

then let $(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2)$ such that

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - (x_1 + x_2) \quad \text{and} \quad y_3 = \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3) - y_1$$

Let the slope

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$ of the line connecting $(x_1, y_1)$ and $(x_2, y_2)$

then

$$x_3 = m^2 - (x_1 + x_2) \text{ and } y_3 = m \cdot (x_1 - x_3) - y_1.$$

Let us add 2 points, namely, $P_1(x_1, y_1) + P_2(x_2, y_2) = (22, 95) \oplus (141, 183)$.

First, we compute denominator of the slope of secant line,

$$\mathbf{x_2 - x_1 = 141 - 22 = 119 \pmod{257}}$$

Extended Euclidean Algorithm

| $i$ | $b =$ | $a$ * | $q$ | + | $r$ | $u$ | $v$ | $w = u - vq$ |
|---|---|---|---|---|---|---|---|---|
| 0 | 257 | 119 | 2 | | 19 | 0 | 1 | -2 |
| 1 | 119 | 19 | 6 | | 5 | 1 | -2 | 13 |
| 2 | 19 | 5 | 3 | | 4 | -2 | 13 | -41 |
| 3 | 5 | 4 | 1 | | 1 | 13 | -41 | 54 |

Second, we need to compute an inverse of the denominator,

$$\mathbf{(x_2 - x_1)^{-1} = 119^{-1} \equiv 54 \pmod{257}}$$

Let us compute the numerator $= \mathbf{y_2 - y_1 = 183 - 95 = 88 \pmod{257}}$

Muhammad Izham Bin Norhamadi
B032020039

Third, the slope of secant line shall be

$$m = \frac{y_2 - y_1}{x_2 - x_1} = 88 \cdot 54 = 4752 \equiv 126 \pmod{257}$$

Finally, we can compute the add point,

$$\begin{aligned} x_3 &= m^2 - (x_1 + x_2) \\ &= 126^2 - (22 + 141) \\ &= 15{,}876 - (163) \\ &= 36 \pmod{257} \end{aligned}$$

and

$$\begin{aligned} y_3 &= m(x_1 - x_3) - y_1 \\ &= 126 \cdot (22 - 36) - 95 \\ &= 126 \cdot (-14) - 95 \\ &= -1{,}764 - 103 \\ &= 197 \pmod{257} \end{aligned}$$

$P_3(x_3, y_3) = (36,197)$

Final answer $3 \otimes (22,95) = (36,197)$

$$\begin{aligned} 3\otimes(22, 95) &= 3\otimes 49\otimes(1, 2) \\ &= 147\otimes(1, 2) \end{aligned}$$

Let us check $2\otimes(141, 183) = 2\otimes 39\otimes (1, 2) = 78\otimes(1,2)$