16-124-836
Marcel Matti ZAUDER

3.4 Question 4

3.4.A Consider the elliptic curve: $y^2 = x^3 + 4x + 6 \ mod \ 11$, $E_{11}(4,6)$. Let $P = (4,3)$ and $Q = (6,9)$. Find:

Calculation Rules

$$x_R = (\lambda - x_P - x_Q) \ mod \ p$$
$$x_Y = (\lambda(x_P - x_R) - y_P) \ mod \ p$$

$$\lambda = \begin{cases} \left(\frac{y_q - y_P}{x_Q - x_P}\right) \ mod \ p & , if \ P \neq Q \\ \left(\frac{3x_P^2 + a}{2y_P}\right) \ mod \ p & , if \ P = Q \end{cases}$$

(I) $P + Q$

First compute λ:

$$\lambda = \left(\frac{9-3}{6-4}\right) \ mod \ 11 = \left(\frac{6}{2}\right) \ mod \ 11 = 3$$

Next Compute x_R and y_R:

$$x_R = (3^2 - 4 - 6) \ mod \ 11 = -1 \ mod \ 11 = 10$$
$$y_R = (3(4-10) - 3) \ mod \ 11 = (-18 - 3) \ mod \ 11 = (-21) \ mod \ 11 = 1$$
$$\Rightarrow \ P + Q = (10, 1)$$

Check if $(10, 1)$ is part of elliptic curve:

$$1^2 \stackrel{?}{=} (10)^3 + 4 * 10 + 6 \ mod \ 11$$
$$1 = 1000 + 40 + 6 \ mod \ 11 = 1046 \ mod \ 11 = 1 \qquad qed.$$

(II) $2P = P + P$

First compute λ:

$$\lambda = \left(\frac{3 * 4^2 + 4}{2 * 3}\right) \ mod \ 11 = \left(\frac{8}{6}\right) \ mod \ 11 = 8 * 6^{-1} \ mod \ 11 = 5$$

Next Compute x_R and y_R:

$$x_R = (5^2 - 4 - 4) \ mod \ 11 = 17 \ mod \ 11 = 6$$
$$y_R = (5(4-6) - 3) \ mod \ 11 = (-10 - 3) \ mod \ 11 = -13 \ mod \ 11 = 9$$
$$\Rightarrow \ 2P = (6, 9)$$

Check if $(6, 9)$ is part of elliptic curve:

$$9^2 \ mod \ 11 \stackrel{?}{=} 6^3 + 4 * 6 + 6$$
$$81 \ mod \ 11 = 216 + 24 + 6 \ mod \ 11 = 246 \ mod \ 114 \qquad = 4 \qquad qed.$$

(III) $2P + 2Q = (P + P) + (Q + Q)$

From **(II)** we know that $2P = (6, 9)$, therefore we calculate now the result of $2Q$:

First compute λ:

$$\lambda = \left(\frac{3 * 6^2 + 4}{2 * 9}\right) \; mod \; 11 = \left(\frac{112}{18}\right) \; mod \; 11 = 2 * 7^{-1} \; mod \; 11 = 5$$

Next Compute x_R and y_R:

$$x_R = (5^2 - 6 - 6) \; mod \; 11 = 13 \; mod \; 11 = 2$$
$$y_R = (5(6 - 2) - 9) \; mod \; 11 = (20 - 9) \; mod \; 11 = 11 \; mod \; 11 = 0$$
$$\Rightarrow \; 2Q = (2, 0)$$

Check if $(2, 0)$ is part of elliptic curve:

$$0^2 \stackrel{?}{=} 2^3 + 4 * 2 + 6$$
$$0 = 8 + 8 + 6 \; mod \; 11 = 22 \; mod \; 11 = 0 \qquad qed.$$

Now we can compute $2P + 2Q$, with $2P = (6, 9)$ and $2Q = (2, 0)$:

First compute λ:

$$\lambda = \left(\frac{0 - 9}{2 - 6}\right) \; mod \; 11 = \left(\frac{9}{4}\right) \; mod \; 11 = 5$$

Next Compute x_R and y_R:

$$x_R = (5^2 - 6 - 2) \; mod \; 11 = 17 \; mod \; 11 = 6$$
$$y_R = (5(6 - 6) - 9) \; mod \; 11 = (0 - 9) \; mod \; 11 = -9 \; mod \; 11 = 2$$
$$\Rightarrow \; 2P + 2Q = (6, 2)$$

Check if $(6, 2)$ is part of elliptic curve:

$$2^2 \stackrel{?}{=} 6^3 + 4 * 6 + 6$$
$$4 = 216 + 24 + 6 \; mod \; 11 = 246 \; mod \; 11 = 4 \qquad qed.$$