Criptografía y Seguridad - Tarea 3

Rivera González Damián
Tadeo Guillén Diana G

November 25, 2019

Ejercicio 1

Sea la curva $y^2 = x^3 + 7x + 2$ en Z_{11}

a) Mostrar que el punto P =(7, 3) $\in E(Z_{11})$ dada por la ecuación y $y^2 = x^3 + 7x + 2$
Como $y^2 = x^3 + 7x + 2$ entonces siendo x = 7 tenemos

$$y^2 = (7)^3 + 7(7) + 2 = 343 + 49 + 2 = 394 mod 11 = 9$$

Así

$$y^2 = 9 \Rightarrow y = 3$$

Por lo tanto (7,3) $\in E(Z_{11})$

b) dar el orden de (7, 3).
Su orden es de 7, puesto que 7(7, 3) = ∞

c) Usar el teorema de Hasse y el orden de (7, 3) para encontrar el orden de $E(Z_{11})$.
El teorema dice que

$$q + 1 - 2\sqrt{q} \leq \#E(F_q) \leq q + 1 + 2\sqrt{q}$$

Entonces

$$11 + 1 - 2\sqrt{11} \leq \#E(Z_{11}) \leq 11 + 1 + 2\sqrt{1}$$

Así

$$5 \leq \#E(Z_{11}) \leq 18$$

Como debe ser un múltiplo del orden del punto (7, 3), entonces este puede ser 7 o 14.

d) Verificar que la cardinalidad de E es igual a $q + 1 + \sum_{x \in Z_{11}} (\frac{x^3+7x+2}{11})$ donde $\frac{x^3+7x+2}{11}$ es el símbolo de Lengendre y q = 11.
Tenemos que

$$q + 1 + \sum_{x \in Z_{11}} (\frac{x^3 + 7x + 2}{11})$$

y así

$$
\begin{aligned}
\#E(Z_{11}) &= 11+1 \\
&\quad + \left(\frac{2}{11}\right) + \left(\frac{10}{11}\right) + \left(\frac{24}{11}\right) + \left(\frac{50}{11}\right) + \left(\frac{94}{11}\right) + \left(\frac{162}{11}\right) \\
&\quad + \left(\frac{260}{11}\right) + \left(\frac{394}{11}\right) + \left(\frac{570}{11}\right) + \left(\frac{794}{11}\right) + \left(\frac{1072}{11}\right) \\
&= 12 + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + 1 + 1 + (-1) + 1 \\
&= 12 + (-5) \\
&= 7
\end{aligned}
$$

Ejercicio 2

Sea la ecuación $y^2 = x^3 + x + 1$ en Z_{77} y sea el punto P = (0, 1) que satisface la ecuación anterior, calcule 5P sumando de P en P y así encontrar un factor de 77.

$$2P = P + P = (0,1) + (0,1)$$

$$\Rightarrow \lambda = \frac{3(0)^2+1}{2(1)} = \frac{1}{2} mod 77 = 39$$

$$\Rightarrow (x_3, y_3) = ((39)^2 - 2(0) mod 77, 39(0-58) - 1 mod 77)$$

$$2P = (58, 47)$$

$$3P = 2P + P = (58,47) + (0,1)$$

$$\Rightarrow \lambda = \frac{1-47}{0-58} = \frac{23}{29} mod 77 = 30$$

$$\Rightarrow (x_3, y_3) = ((30)^2 - 58 - 0 mod 77, 30(58-72) - 47 mod 77)$$

$$3P = (72, 72)$$

$$4P = 3P + P = (72,72) + (0,1)$$

$$\Rightarrow \lambda = \frac{1-72}{0-72} = \frac{71}{72} mod 77 = 32$$

$$\Rightarrow (x_3, y_3) = ((32)^2 - 72 - 0 mod 77, 32(72-28) - 72 mod 77)$$

$$4P = (28, 27)$$

$$5P = 4P + P = (28,27) + (0,1)$$

$$\Rightarrow \lambda = \frac{1-27}{0-28} \Rightarrow ...$$

Como necesitamos calcular el inverso de 28, no existe en Z_{77}, puesto que mcd(28, 77) = 7, no son primos entre si, además $1 < 7 < 77$, por lo cual 28, es un factor de 77.

Ejercicio 4

Sea E la curva elíptica dada por los puntos que satisfacen la ecuación $y^2 = x^3 + 7x + 19$ en Z_{31} y P = (18, 26) un punto en E de orden 39, el ECIES simplificado definido sobre Z_{31}^* como espacio de texto plano, supongamos que la clave privada es m = 8

a) Calcula Q = mP .

b) Descifra la siguiente cadena de texto cifrado
((4, 1), 1); ((11, 0), 18); ((27, 1), 17); ((28, 1), 29); ((23, 0), 26).

c) Supongamos que cada texto plano representa un carácter alfabético, convierte el texto plano en una palabra. Usa la asociación (A $\rightarrow$ 1, . . . , z $\rightarrow$ 26) en este caso 0 no es considerado como un texto plano o un par ordenado.