



# Universidad Nacional Autónoma de México

## Facultad de Ciencias

**Leyva Castillo Luis Angel 314050577**  
**Rosado Cabrera Diego Rosado Cabrera 314293804**

1. Sea  $E: y^2 + 20x = x^3 + 21 \pmod{35}$  y sea  $Q = (15, -4) \in E$ .

A Factoriza 35 tratando de calcular  $3Q$ .

Primero para poder realizar esta operación tenemos que encontrar  $2Q$ , para ello tenemos que sumar los puntos  $(15, 4) + (15, 4)$  Recordando que la suma se define de la siguiente forma

$P+Q=$

$$\begin{cases} \text{Infinito} & \text{SI } x_1 = x_2 \text{ \& } -y_1 = y_2; \\ (x_3, y_3) & x_3 = (\lambda - x_1 - x_2) \pmod{p} \text{ y } y_3 = (\lambda(x_1 - x_3) - x_1) \pmod{p} \end{cases}$$

Pero para esto necesitamos sacar primero a  $\lambda$  que recordemos que se define de la siguiente manera

$\lambda=$

$$\begin{cases} ((3x_1^2 + A) * 2(y_1)^{-1}) \pmod{p} & \text{si } P = Q; \\ ((y_1 - y_2) * (x_1 - x_2)) \pmod{p} & \text{si } P \neq Q; \end{cases}$$

Para esto entonces simplemente sustituimos los valores, en lambda debido a que  $P=Q$  entonces usamos el primer caso de la lambda lo cual nos dice que  $\lambda = (((3(15)^2) + -20) * 2(-4)^{-1}) \pmod{35}$

$$\rightarrow (((3*225)-20*(-8)^{-1}) \pmod{35}$$

$$\rightarrow ((675-20)*13) \pmod{35}$$

$$\rightarrow (655 * 13) \pmod{35}$$

$$\rightarrow 8515 \pmod{35}$$

$$\therefore \lambda = 10$$

Ahora ya podemos sumar, primero sacaremos  $x_3 = 10^2 - 15 - 15 \pmod{35}$

$$\rightarrow 100 - 30 \pmod{35}$$

$$\rightarrow 70 \pmod{35}$$

$$\therefore x_3 = 0$$

Ahora debemos sacar a  $y_3 = (10(15-0) - -4) \pmod{35}$

$$\rightarrow 150 + 4 \pmod{35}$$

$$\rightarrow 154 \pmod{35}$$

$$\therefore y_3 = 14$$

Entonces ya sabemos el valor del punto  $2Q$ , ahora debemos sumar  $Q+2Q$  para tener  $3Q$ , para eso debemos calcular de nuevo  $\lambda$  por lo que haremos  $\lambda = \frac{-4-14}{15-0}$

Aquí encontramos un error debido a que 15 no tiene inverso multiplicativo en el grupo 35 así que eso implica que tenemos que sacar el  $\text{MCD}(35, 15) = 5$   $\therefore 5$  es factor de 35.

2 Factoriza 35 tratando de calcular 4Q duplicándolo.

Ahora no calcularemos 2Q debido a que ya lo calculamos anteriormente en el ejercicio 1 por lo cual pasaremos a calcular  $\lambda$  bajo la definición del ejercicio 1

$$\lambda = \frac{3(0)^2}{2(14)} \bmod 35$$

Encontramos de nuevo el mismo problema que en el ejercicio anterior debido a que  $28 \bmod 35$  no tiene inverso, por lo cual debemos sacar su MCD( $28, 35$ ) = 7  $\therefore$  7 es un factor de 35

3 Calcula 3Q y 4Q sobre E (mod 5) y sobre E (mod 7) explica por que el factor 5 se obtiene calculando 3Q y por que el factor 7 se obtiene calculando 4Q.

Debido a que cuando calculas 3Q, intentamos sacar el inverso de 15 en el grupo 35, esto conflictuó ya que como 15 y 35 no son primos  $\rightarrow$  que son números compuesto por primos esto nos lo sabemos por el teorema fundamental de la aritmética, ahora al sacar su MCD descubrimos que 5 es ese número  $\therefore$  por esa razón 3Q, nos dio el valor 5 por compartir ese primo con 15 y análogamente pasa lo mismo con 28 y 35

Ahora el valor de 3Q con 5 = No se puede calcular debido a que tenemos que cuando intentamos sumar  $Q = (15, -4)$  con  $2Q = (0, 4)$  (Los calculos de como se llego a 2Q se dejan como ejercicio para el lector) e intentamos sacar  $\alpha = (-4-4) \cdot (0-15)^{-1}$

$\rightarrow 8 \cdot (-15)^{-1}$  y como -15 no esta en el campo de 5 entonces lo que hacemos es devolverlo con la operación modulo  $\rightarrow -15 \bmod 5 = 0$  y 0 no tiene inverso multiplicativo en 5 y no existe MCD(0,5) por lo que nuestro proceso termina aquí

2. Sea E la curva elíptica  $y^2 = x^3 + x + 28$  definida sobre  $\mathbb{Z}_{71}$

a) Calcula y muestra el número de puntos de E.

Puntos:

O, (1,32), (1,39), (2,31), (2,40), (3,22), (3,49), (4,5), (4,66), (5,4), (5,67), (6,26), (6,45), (12,8), (12,63), (13,26), (13,45), (15,9), (15,62), (19,27), (19,44), (20,5), (20,66), (21,3), (21,68), (22,30), (22,41), (23,19), (23,52), (25,22), (25,49), (27,0), (31,32), (31,39), (33,1), (33,70), (34,23), (34,48), (35,14), (35,57), (36,12), (36,59), (37,33), (37,38), (39,32), (39,39), (41,7), (41,64), (43,22), (43,49), (47,5), (47,66), (48,11), (48,60), (49,24), (49,47), (52,26), (52,45), (53,0), (58,27), (58,44), (61,15), (61,56), (62,0), (63,17), (63,54), (65,27), (65,44), (66,18), (66,53), (69,35), (69,36).

b) Muestra que E no es un grupo cíclico.

c) ¿Cuál es el máximo orden de un elemento en E? Encuentra un elemento que tenga ese orden.

3. Sea E :  $y^2 - 2 = x^3 + 333x$  sobre  $\mathbb{F}_{347}$  y sea P = (110,136).

a) ¿Es Q=(81,-176) un punto de E?

Para verificar esto hay que sustituir en E:  $x = 81$ ,  $y = -176$ .

b) si sabemos que  $|E| = 358$  ¿Podemos decir E es criptográficamente útil? ¿Cuál es el orden de P? ¿Entre que valores se puede escoger la clave privada?

c) si tu clave privada es  $k=101$  y algún conocido te ha enviado el mensaje cifrado ( $M_1=(232,278)$  y  $M_2=(135,214)$ ) ¿Cuál era el mensaje original?

4. Sea  $\mathbb{E} : F(x,y)=y^2 - x^3 - 2x - 7$  sobre  $\mathbb{Z}_{31}$  con  $\# \mathbb{E} = 39$  y P = (2,9) es un punto de orden 39 sobre  $\mathbb{E}$ , el ECIES simplificado definido sobre  $\mathbb{E}$  tiene  $\mathbb{Z}_{31}^*$  como espacio de texto plano, supongamos que la clave privada es  $m = 8$ .

a) Calcula Q=mP

Hay que calcular  $Q = 8P$

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

Como son los mismos puntos tenemos  $\lambda = (3x_1^2 + A) (2y_1)^{-1} = (3(2)^2 + 2)(2(9))^{-1}$  hay que encontrar

el inverso de 9 mod 31 usando el algoritmo extendido de euclides,  $2(9)^{-1} \equiv 18^{-1} \equiv 19 \pmod{31}$ .

Entonces  $\lambda = (12+2) \times 19 = 266$ .

Queda calcular  $x_3 = \lambda^2 - x_1 - x_2$ ,  $y_3 = \lambda(x_1 - x_3) - y_1$ .

$x_3 = (266)^2 - 2 - 2 = 70,756 - 4 = 70,752 \equiv 10 \pmod{31}$ .

$y_3 = 266(2 - 70,752) - 9 = -18,819,509 \equiv 2 \pmod{31}$ .

Entonces  $2P = (10, 2)$ .

$4P = 2P + 2P = (10, 2) + (10, 2)$ .

Entonces  $\lambda = (3(10^2) + 2)(2(2))^{-1} = 2,416$ .

$x_3 = (2,416)^2 - 10 - 10 = 5,837,036 \equiv 15 \pmod{31}$ .

$y_3 = 2,416(10 - 5,837,036) - 2 = -14,102,254,818 \equiv 8 \pmod{31}$ .

Por lo que  $4P = (15, 8)$ , solo falta calcular  $8P = 4P + 4P = (15, 8) + (15, 8)$ .

Ahora  $\lambda = (3(15)^2 + 2)(2(8)^{-1})$ ;  $2(8)^{-1} \equiv 2 \pmod{31}$ .

entonces  $\lambda = 677 \times 2 = 1354$ .

$x_3 = 1,354^2 - 15 - 15 = 1,833,286 \equiv 8 \pmod{31}$ .

$y_3 = 1354(15 - 1,833,286) - 8 = -24,82,248,942 \equiv 15 \pmod{31}$ .

Entonces  $8P = (8, 15)$ .

b) Descifra la siguiente cadena de texto cifrado:

$((18, 1), 21), ((3, 1), 18), ((17, 0), 19), ((28, 0), 8)$

E :  $y^2 = x^3 + 2x + 7 \pmod{31}$

1)  $((18, 1), 21)$

Evaluamos 18 en E:

Entonces  $18^3 + 2(18) + 7 = 5875 \equiv 16 \pmod{31}$ .

$y = \pm 4$ , ahora hay que fijarnos en la segunda entrada la cual nos dice que  $y \equiv 1 \pmod{2}$ , entonces  $y = 27$ .

El punto de descompresión es  $(18, 27)$ , entonces  $8(18, 27) = (15, 8)$

Ahora hay que encontrar  $15^{-1} \equiv 29 \pmod{31}$ , y con esto hay que calcular  $29(21) \pmod{31}$  que nos da: 20.

2)  $((3, 1), 18)$

Evaluamos 3 en E :

Entonces  $3^3 + 2(3) + 7 = 40 \equiv 9 \pmod{31}$

$y = \pm 3$ , ahora hay que fijarnos en la segunda entrada la cual nos dice que  $y \equiv 1 \pmod{2}$ , entonces  $y = 28$

El punto de descompresión es  $(3, 28)$ , entonces  $8(3, 28) = (2, 22)$

Ahora hay que encontrar  $2^{-1} \equiv 16 \pmod{31}$ , y con esto hay que calcular  $16(18) \pmod{31}$  que nos da: 9.

3)  $((17, 0), 19)$

Evaluamos 17 en E:

Entonces  $17^3 + 2(17) + 7 = 4954 \equiv 25 \pmod{31}$

$y = \pm 5$ , ahora hay que fijarnos en la segunda entrada la cual nos dice que  $y \equiv 0 \pmod{2}$ , entonces  $y = 26$

El Punto de descompresión es  $(17, 26)$ , entonces  $8(17, 26) = (29, 29)$

Ahora hay que encontrar  $29^{-1} \equiv 15 \pmod{31}$ , y con esto hay que calcular  $15(19) \pmod{31}$  que nos da: 6

4)  $((28, 0), 8)$

Evaluamos 28 en E:

Entonces  $28^3 + 2(28) + 7 = 22015 \equiv 5 \pmod{31}$  Hay que sumarle a 5, 31 tantas veces como sea necesario para que nos genere un cuadrado perfecto. En este caso  $5 + 31 = 36$ .

Entonces  $y = \pm 6$ , ahora nos fijamos en la segunda entrada la cual nos dice que  $y \equiv 0 \pmod{2}$ , entonces  $y = 26$

El punto de descompresión es  $(28, 26)$ , entonces  $8(28, 26) = (5, 10)$

Ahora hay que encontrar  $5^{-1} \equiv 25 \pmod{31}$ , y con esto hay que calcular  $25(8) \pmod{31}$  que nos da:

14.

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

Del ejercicio anterior obtuvimos los valores  $\{20, 9, 6, 14\}$

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Y con los valores obtenemos **TIFN** y si buscamos por acronimo,  
obtenemos **That's it for now**