

Facultad de Ciencias, UNAM
Criptografía y Seguridad
Tarea 3

Altamirano Vázquez Jesús Fernando
Rubí Rojas Tania Michelle

23 de junio de 2020

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

a) Factoriza 35 tratando de calcular $3Q$.

SOLUCIÓN:

b) Factoriza 35 tratando de calcular $4Q$ duplicándolo.

SOLUCIÓN:

c) Calcula $3Q$ y $4Q$ sobre E (mód 5) y sobre E (mód 7). Explica por qué el factor 5 se obtiene calculando $3Q$ y por qué el factor 7 se obtiene calculando $4Q$.

SOLUCIÓN:

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 .

SOLUCIÓN: Sabemos que los puntos en una curva elíptica

$$E : y^2 = x^3 + Ax + B \quad (\text{mód } n)$$

son los pares (x, y) (mód n) con $x, y \in K$ tales que satisfacen la ecuación anterior, junto con el punto en el infinito.

Dada la siguiente implementación

```
1      '''
2      Regresa los puntos que pertenecen a la curva eliptica
3      E: y^2 = x^3 + Ax + B (mod n)
4      '''
5      def encontrar_puntos(A, B, n):
6          puntos = []
7          # Sabemos que x pertenece al conjunto [0, 70].
8          for i in range(0, n):
9              # Sabemos que y pertenece al conjunto [0, 70].
10             for j in range(0, n):
11                 # Encontramos el valor de x^3 + Ax + B (mod n)
12                 valor = (pow(i, 3, n) + ((A * i) % n) + B) % n
13                 # Encontramos los posibles valores para y.
14                 y2 = pow(j, 2)
15                 # Verificamos que el par satisface la ecuacion.
16                 if ((y2 - valor) % n) == 0:
17                     puntos.append((i, j))
18
19         print("La curva eliptica E tiene " + str(len(puntos) + 1) +
```

```

20         " puntos.")
21     return puntos
22
23     if __name__ == "__main__":
24         print(encontrar_puntos(1, 28, 71))
25

```

obtenemos que, junto con el punto en el infinito, hay 72 puntos en la curva elíptica, los cuales son:

(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.

Demostración. Sabemos que un elemento $P \in E$ es un punto primitivo si genera a todo el conjunto de puntos que pertenecen a E , es decir, todos los elementos del grupo pueden ser expresados de la forma

$$P + P + \cdots + P (k \text{ veces}) \quad \text{para alguna } k \in \{1, 2, \dots, \#E(\mathbb{F}_q)\}$$

Por un corolario del teorema de *Lagrange* sabemos que el orden de un subgrupo generado por un elemento en E necesariamente divide a $\#E(\mathbb{F}_q) = 72$, por lo que

$$D = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36\}$$

son los posibles valores para el orden de cada uno de los puntos en $E(\mathbb{F}_{71})$, ya que son justamente todos los divisores de 72.

Por el ejercicio 2.c sabemos que el orden de cada uno de los elementos en E se encuentra dentro del conjunto

$$O = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$

Entonces, como

$$\#E(\mathbb{F}_{71}) = n = 72 = 2^3 \cdot 3^2$$

no es primo, podemos buscar al punto primitivo P de la siguiente forma: para cada primo p que divide a 72, calculamos $\left(\frac{n}{p}\right)P$. Si ninguno de estos puntos es el punto en el infinito, entonces P genera a E . Por ejemplo, si $P = (1, 32)$ tenemos que

$$\begin{aligned} \left(\frac{72}{2}\right)P &= 36(1, 32) = \infty \\ \left(\frac{72}{3}\right)P &= 24(1, 32) = (20, 5) \end{aligned}$$

Como $36P = \infty$, entonces no genera a E .

Ahora bien, podemos seguir el siguiente camino: el orden de un elemento en E siempre será múltiplo de 36 o 24, y eso implica que kP , con $k = |P| \cdot i = 36$ o 24, genera el punto en el infinito. Tomando un elemento P cuyo orden pertenezca al conjunto O , tenemos que

$$|P = (1, 32)| = 18 \Rightarrow 18 \cdot 2 = 36 \Rightarrow 36P = \infty$$

$$\begin{aligned}
|P = (2, 31)| &= 6 \Rightarrow 6 \cdot 4 = 24 \Rightarrow 24P = \infty \\
|P = (3, 22)| &= 12 \Rightarrow 12 \cdot 2 = 24 \Rightarrow 24P = \infty \\
|P = (4, 5)| &= 36 \Rightarrow 36 \cdot 1 = 36 \Rightarrow 36P = \infty \\
|P = (5, 4)| &= 4 \Rightarrow 4 \cdot 6 = 24 \Rightarrow 24P = \infty \\
|P = (20, 5)| &= 3 \Rightarrow 3 \cdot 8 = 24 \Rightarrow 24P = \infty \\
|P = (27, 0)| &= 2 \Rightarrow 2 \cdot 12 = 24 \Rightarrow 24P = \infty \\
|P = (31, 32)| &= 9 \Rightarrow 9 \cdot 4 = 36 \Rightarrow 36P = \infty
\end{aligned}$$

Notemos que todas las operaciones fueron verificadas con la función `suma_puntos()`, implementada en el ejercicio 2.c.

Como $|\infty| = 1$ no puede ser el generador del grupo, y el orden del resto de los puntos en E oscila entre los valores del conjunto O , eso quiere decir que todos los puntos generan el punto en el infinito, lo que implica que E no es generado por ninguno de sus elementos. Por lo tanto, E no es cíclico. □

- c) ¿Cuál es el máximo orden de un elemento en E ? Encuentra un elemento que tenga este orden.
 SOLUCIÓN: Por un corolario del teorema de *Lagrange* sabemos que el orden de un punto siempre divide el orden del grupo $E(\mathbb{F}_{71})$.

Dada la siguiente implementación

```

1      # Regresa los divisores de un numero n.
2      def divisores(n):
3          div = []
4          for i in range(1, n):
5              if ((n % i) == 0):
6                  div.append(i)
7
8          return div
9
10     if __name__ == "__main__":
11         print(divisores(72))
12

```

sabemos que

$$D = [1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36]$$

son los posibles valores para el orden de cada uno de los puntos en $E(\mathbb{F}_{71})$. En particular, por el teorema de *Lagrange* tenemos que $\#E(\mathbb{F}_{71})P = 72P = \infty$, con $P \in E(\mathbb{F}_{71})$.

Ahora bien, el orden de un punto en $E(\mathbb{F}_{71})$ será el mínimo entero $k \in D$ tal que $kP = \infty$.

Dada la siguiente implementación

```

1      '''
2      Regresa una tupla (mcd, s, t) que obtenemos al aplicar el algoritmo
3      extendido de Euclides, donde as + bt = mcd(a, b) son los elementos
4      que conforman la tupla.
5      '''
6      def aee(a, b):
7          s = 0; s_i = 1
8          t = 1; t_i = 0
9          g = b; g_i = a
10

```

```

11         while g != 0:
12             cociente = g_i // g
13             g_i, g = g, g_i - cociente * g
14             s_i, s = s, s_i - cociente * s
15             t_i, t = t, t_i - cociente * t
16         return (g_i, s_i, t_i)
17
18     # Regresa el inverso multiplicativo de a modulo m.
19     def inverso(a, m):
20         g, s, t = aee(a, m)
21         # El inverso de a modulo m existe si y solo si (a, m) = 1.
22         if g != 1:
23             print("No tiene inverso multiplicativo.")
24         else:
25             inverso = s % m
26
27         return inverso
28
29     # Regresa la suma de dos puntos P y Q en E.
30     def suma_puntos(P, Q, A, p):
31         # Casos especiales.
32         if (P == None):
33             return Q
34         if (Q == None):
35             return P
36
37         x1, y1 = P
38         x2, y2 = Q
39
40         if (x1 == x2):
41             m = (3 * x1 * x1 + A) * inverso(2 * y1, p)
42         else:
43             m = (y1 - y2) * inverso(x1 - x2, p)
44
45         x3 = m * m - x1 - x2
46         y3 = m * (x1 - x3) - y1
47         suma = (x3 % p, y3 % p)
48         return suma
49
50     # Regresa el orden de un elemento en E.
51     def orden(P, a, p):
52         # Como P = P y y_1 = 0 entonces P+P = infinito.
53         if (P[1] == 0):
54             return 2
55
56         # Calculamos 2P.
57         P2 = suma_puntos(P, P, a, p)
58         aux = P2
59
60         orden = 3
61         for i in range(0, p):
62             # Calculamos P + kP
63             aux = suma_puntos(P, aux, a, p)
64             # Si encontramos a 2P, entonces hemos encontrado el orden.
65             if (aux == P2):
66                 break
67             orden += 1
68         return orden
69
70     # Regresa el orden de cada uno de los elementos en la lista puntos.
71     def get_ordenes(puntos, a, p):

```

```

72         ordenes = []
73         for punto in puntos:
74             o = orden(punto, a, p)
75             ordenes.append(o)
76
77         return ordenes
78
79     if __name__ == "__main__":
80         print(get_ordenes(encontrar_puntos(1, 28, 71), 1, 71))
81

```

obtenemos la siguiente tabla, la cual indica el orden de cada uno de los elementos que pertenecen a E .

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

Por lo tanto, el punto $P = (4, 5)$ con $|P| = 36$ es un elemento en E con el máximo orden.

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

a) ¿Es $Q = (81, -176)$ un punto de \mathbb{E} ?

SOLUCIÓN: Para saber si Q es un punto en E simplemente debemos comprobar que con los valores $x = 81$ y $y = -176$ se cumple la congruencia

$$y^2 - 2 \equiv x^3 + 333x \pmod{347}$$

Entonces

$$\begin{aligned}
 y^2 - 2 &\equiv x^3 + 333x \pmod{347} \\
 (-176)^2 - 2 &\equiv (81)^3 + 333(81) \pmod{347} \\
 30974 &\equiv 558414 \pmod{347}
 \end{aligned}$$

Como $p = 347 \mid 558414 - 30974 = 527440$ ya que $347(1520) = 527440$, entonces podemos concluir que $Q = (81, -176) \in E(F_{347})$.

b) Si sabemos que $|\mathbb{E}| = 358$. ¿Podemos decir que \mathbb{E} es criptográficamente útil? ¿Cuál es el orden de P ? ¿Entre qué valores se puede escoger la clave privada?

SOLUCIÓN: Como $|E| = 358 = 2 \cdot 179$ entonces se puede decir que E no es criptográficamente útil ya que una *curva fuerte* busca que

- El orden de E sea divisible por un primo grande (2 no lo es), ó
- El orden de E sea un primo grande (tenemos que 358 es par).

Utilizando la función `orden()`, definida en el ejercicio 2.c, obtenemos que el orden del elemento $P = (110, 136)$ es 179.

Los valores de la clave privada se pueden escoger entre los enteros del intervalo $[1, 179]$, el cual está acotado por el orden del punto P (ya que es el punto primitivo).

- c) Si tu clave privada es $k = 101$ y algún conocido te ha enviado el mensaje cifrado

$$(M_1 = (232, 278), M_2 = (135, 214))$$

¿Cuál era el mensaje original?

SOLUCIÓN: El mensaje está cifrado usando *ElGamal elíptico*, por lo que simplemente hay que seguir su algoritmo para descifrar.

- Calculamos $M = M_2 - kM_1$, donde k es nuestra llave privada.
Usando la función `suma_puntos()`, implementada en el ejercicio 2.c obtenemos que

$$\begin{aligned} M &= (135, 214) - 101(232, 278) \\ &= (135, 214) - (275, 176) \\ &= (135, 214) + (275, -176) && \text{por definición de } -P \\ &= (74, 87) \end{aligned}$$

Por lo tanto, el mensaje original es $M = (74, 87)$.

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 $Q = mP$.

SOLUCIÓN: Usando la función `suma_puntos()`, implementada en el ejercicio 2.c, obtenemos que

$$Q = 8(2, 9) = (8, 15)$$

- b) Descifra la siguiente cadena de texto cifrado

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

SOLUCIÓN:

- c) Supongamos que cada texto plano representa un carácter alfabético, convierte el texto plano en una palabra en Inglés. Usa la asociación ($A \rightarrow 1, \dots, Z \rightarrow 26$).

SOLUCIÓN: