# Tarea 3.

Profesor: Manuel Díaz Díaz
Ayudante:Gerardo Rubén López Hernández
Alumnos: César Eduardo Jardines Mendoza,
Emiliano Galeana Araujo

26 de junio de 2020

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

   *a*) Factoriza 35 tratando de calcular $3\mathbb{Q}$.
   Sea E la curva eliptica de la forma $y^2 = x^3 - 20x + 21$ mod 35 y considerando que P = (15,-4). Como primer paso debemos calcular la linea tangente pendiente del punto P y dado que solo se contempla un punto tenemos que usar la siguente formula:

   $$\text{m} = \frac{dy}{dx} = \frac{3x_1^2+A}{2y_1}$$

   y contemplando que debemos de encontrar en P el punto m y aplicando la formula mencionada con anterioridad tendríamos que:

   $$\text{m} = \frac{3x_1^2+A}{2y_1} = \frac{3(15)^2-(20)}{2(-4)} = -\frac{25}{8} \text{ mod } 35$$

   Con lo que se obtendrá el máximo común divisor del denominador m y teniendo el módulo p, gcd(8,35) = 1. Dado que es 1 se calculará el inverso módulo p del denominador de la pendiente m el cual tenemos que $8^-1 \equiv 22$ mód 35. Con esto tendremos el inverso y la pendiente queda como:

   $$-\frac{25}{8} \cdot (8^-1) = -\frac{25}{8} \cdot (22) \equiv 10 \text{ mód } 35$$

   teniendo todo esto y para encontrar 2p con P y utilizando la pendiente tenemos que considerar lo siguente:

   $$\text{Si } P_1 = P_2 \wedge y1 \sqsupset 0x3 = m^2 - 2x1, y3 = m(x1 - x3) - y1 \text{ donde tenemos que } m = \frac{3x_1^2+A}{2y_1}$$

   Y sustituyendo en nuestra fórmula previa para calcular 2P = (x,y) con m = 10 se tiene que:

   $$x \equiv (10)^2 - 2(15) \equiv 0, y \equiv (10)((15) - (0)) - (-4) \equiv 14$$

   teniendo todo esto con 2P = (0,14) y desarrollando esto para calcular 3P debemos de sumar bajo la opearación del grupo a P y 2P con la formula:

   $$\text{Si } x1 \neq x2 \text{ entonces } x_3 = m^2 - x1 - x_2, y_3 = m(x1 - x3) - y1 \text{ donde m} = \frac{y_2-y_1}{x_2-x_1}$$

   con lo que tendríamos que:

   $$\frac{14-(-4)}{0-15} = -\frac{19}{15}$$

Y teniendo el denominador de m previo y con p (el primo) tendremos que gcd(15,35) = 5 $\sqsupset$ 1 por lo que $15^{-}1$ mod 35 y no se puede evaluar la tangente que se tiene por lo que hemos encontrado un factor de 35 que es 5 por lo que tenemos que:

$$35 = 5 \cdot 7$$

*b*) Factoriza 35 tratando de calcular $4\mathbb{Q}$ duplicándolo.
Recordemos que podemos ver a $4\mathbb{Q}$ como $2\mathbb{Q} + 2\mathbb{Q}$.
Calculamos

$$2\mathbb{Q} = (0, 14)$$

Recordando que

$$m = \frac{3x_1^2 + A}{2y_1}$$

Calculamos la pendiente:

$$m = \frac{3(0)^2 + (-20)}{2(14)} = -\frac{20}{28}(mod 35)$$

Calculamos el $GCD(35, 28) = 7 \neq 1$. Por lo que la factorización queda de la siguiente manera.

$$35 = 7 \cdot 5$$

*c*) Calcula $3\mathbb{Q}$ y $4\mathbb{Q}$ sobre $\mathbb{E}(mod 5)$ y sobre $\mathbb{E}(mod 7)$ explica por qué el factor 5 se obtiene calculando $3\mathbb{Q}$ y por qué el factor 7 se obtiene calculando $4\mathbb{Q}$.

| | $3\mathbb{Q}$ | $4\mathbb{Q}$ |
|---|---|---|
| $mod 5$ | (0,0) | (0,1) |
| $mod 7$ | (1,4) | (0,0) |

Para $3\mathbb{Q}$ obtuvimos una pendiente que tenía un 5 en el denominador, por lo tanto fue infinito modulo5. Por otro lado el orden de $\mathbb{Q}(mod 7)$ es 4.

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

*a*) Calcula y muestra el número de puntos de $\mathbb{E}$.
Los 71 puntos (Sin contar el infinito) calculados son [1]:

| | | | | | | |
|---|---|---|---|---|---|---|
| (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) | | | | | | |

[1] Usamos un programa, si se requiere, podemos brindarlo.

*b*) Muestra que $\mathbb{E}$ no es un grupo cíclico.
Podemos ver de manera rapida que E al ser un grupo finito se cumple que para cualquier P ∈ E con x ∈ $\mathbb{Z}$ y xP = (x mod n)P donde n = $|E - \{O\}|$. Con esto podemos observar que si tenemos k-racionales puntos (los 3 puntos) de $E$ tales que su orden 2 lo que vendrían siendo:

- (27,0)
- (53,0)
- (62,0)

lo antes mencionado nos da a entender que al ser 2 el minimo entero que cumple para los tres puntos anteriores que 2P = $O$, donde $O$ al ser el punto al infinito el cual es el elemento neutro del grupo. Con esto tenemos que los dons puntos distinto $P_1 y P_2$ tales que $P_1 \neq P_2$ y $2P_1 = 2P_2 = O$. Supongamos que $E$ es un grupo cíclico, por definición tendría que existir un elemento generador y sea $P_G$ con $\forall P \in E x \in \mathbb{Z}$ tal que x$P_G = P$, en especial x$P_G \neq O$ para cualquier 0 ¡x ¡n.

$$2P_1 = O \rightarrow 2(x_1)P_G = O \rightarrow (2x_1)P_g = (2x_1 mod n)P_G = O$$

Esto nos lleva a que

$$x_1 = n \times 2^{-1} mod n$$

Análogamente a lo que hicimos anteriormente, tenemos:

$$2P_2 = 2(x_2 P_G) = O \rightarrow (2x_2)P_G = (2x_2 mod n)P_G = O$$

Por lo anterior, vemos que:

$$x_2 = n \times 2^{-1} mod n$$

Por lo que $2P_1 = 2x_1 P_G = O = 2x_2 P_G = 2P_2 \rightarrow P_1 = P_2$.
Y por ($P_1 \neq P_2$), llegamos a una contradicción.
Por lo que $\mathbb{E}$ no es un grupo cíclico.

*c*) ¿Cuál es el máximo orden de un elemento en $\mathbb{E}$?, encuentra un elemento que tenga este orden.
Haciendo uso del programa del inciso *a)*, y modificando un poco, tenemos que el orden de cada punto es el siguiente:

| | | | | | | |
|---|---|---|---|---|---|---|
| (1, 32), 18 | (1, 39), 19 | (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), 33 | (20, 5), 11 |
| (20, 66), 3 | (21, 3), 36 | (21, 68), 72 | (22, 30), 51 | (22, 41), 18 | (23, 19), 40 | (23, 52), 36 |
| (25, 22), 18 | (25, 49), 39 | (27, 0), 2 | (31, 32), 9 | (31, 39), 48 | (33, 1), 62 | (33, 70), 62 |
| (34, 23), 33 | (34, 48), 72 | (35, 14), 72 | (35, 57), 72 | (36, 12), 9 | (36, 59), 12 | (37, 33), 72 |
| (37, 38), 72 | (39, 32), 6 | (39, 39), 49 | (41, 7), 22 | (41, 64), 36 | (43, 22), 49 | (43, 49), 22 |
| (47, 5), 72 | (47, 66), 61 | (48, 11), 46 | (48, 60), 35 | (49, 24), 72 | (49, 47), 72 | (52, 26), 26 |
| (52, 45), 72 | (53, 0), 2 | (58, 27), 57 | (58, 44), 57 | (61, 15), 72 | (61, 56), 60 | (62, 0), 2 |
| (63, 17), 24 | (63, 54), 55 | (65, 27), 72 | (65, 44), 72 | (66, 18), 12 | (66, 53), 8 | (69, 35), 33 |
| (69, 36), 18 | | | | | | |

Por que el orden máximo es el 72, así que cualquier punto con este orden funciona, nosotros daremos el punto `(21, 68)`.

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

   *a*) ¿Es $\mathbb{Q} = (81, -176)$ un punto de $\mathbb{E}$?
   No, pero $(81, 176)$ sí lo es.
   Recordemos [2] la siguiente definición:

   $$E(K) = \{(x,y) \in K^2 | y^2 = x^3 + ax + b\} \cup \{\infty\}$$

   Esto nos dice que $E(K)$ son todos los puntos $K-$racionales de la curva. Por lo que bastaría con listarlos y posteriormente verificar si $\mathbb{P}$ existe en el conjunto.

   *b*) Si sabemos que $|\mathbb{E}| = 358$. ¿Podemos decir que $\mathbb{E}$ es criptográficamente útil?, ¿Cuál es el orden de $\mathbb{P}$? ¿Entre qué valores se puede escoger la clave privada? Considerando que la curva elíptica $y^2 = x^3 + ax + b$ definen un grupo abeliano en $F_q$ si

   $$(4a^3 + 27b^2) mod p \neq 0 mod p$$

   donde podemos observar que $4 * 33^3 + 27 * 2^2 = 236$ mod 347 po lo que podemos deducir que en la curva se puede usar para encriptirar, ahora tenemos que $|E|$ = 358 =179*2, en la práctica no sería usada pues su tamaño es muy pequeño.

   En pocas palabras lo que el algoritmo se enfoca en hacer los pasos:

   - Calcula nuestro Q
   - Toma un entero m que cumpla la m $> q^1/4$
   - Calcula y guarda los puntos (j=0,1,2,3,4,..,m)
   - Calcula Q+k(2mP) para un K=m donde m1,m2,...,m. Esto hasta que se cumpla Q + k(2mP) = $\pm$ jP para algunto punto que se presente negativo de los que se estan obteniendo.
   - Teniendo a M = q + 1 2mk $\pm$ j, se factoriza M con factores que van desde $p_1, p_2, ..., p_r$ (factores primos)
   - Calculamos (M/$p_i$)P para cada i = 1,....,r. Si (M/$p_i$)P cumple entonces se reemplaza, se factoriza con una nueva M y entra en un loop hasta que se cumpla que (M/$p_i$)P sea distinto en toda i
   - Comprueba si M es el orden de P

   Teniendo en consideración los pasos del algoritmo [3] , nosotros tendríamos que M = 2 * 179, sabemos que (M/2)P = ínf y (M/179)P $\neq$ ínf por lo que concluimos que es el orden de P. Y considerando los valores en los que se puede escoger la llave privada, estos están acotados por el orden P = 179 y obtendr íamos que d $\in [1, 179 - 1]$

   *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?

   Calculamos $M = M_2 - dM_1 = M_2 - (101)M_1$[4]: Obteniendo a $M = (74, 87)$, siendo el mensaje original: $m = 74$.

   Para encontrar el número aleatorio, usamos el algoritmo de `Paso grande, paso chico`. El cuál nos da como resultado $k = 7$.

[2] Definición
[3] Con el uso del programa nos basamos para resolver de manera más optima el ejercicio
[4] Con el uso de un programa, nos ayudamos para resolver el ejercicio.

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

$$E : y^2 = x^3 + 2x + 7$$

*a*) Calcula $\mathbb{Q} = m\mathbb{P}$.

2(2,9) = (10,2) $\rightarrow$ 2(10,2) = (15,8)
$\rightarrow$ 2(15,8) = 8(2,9) = (8,15) [5]

*b*) Descifra la siguiente cadena de texto cifrado $((18,1),21),((3,1),18)),((17,0),19),((28,0),8)$
Siguendo los siguentes pasos y tomando en cuenta que se debe de descomprimir cada tupla en la forma $D_k : ((\mathbb{Z}_{31}^* x \mathbb{Z}_2) x \mathbb{Z}_{31}^*)$. Teniendo esto en cuenta y considerandolo, sea P = $((x_1,y_1)y_2)$ tenemos que se ejecutarán los pasos:

- Se evaluará en $x_1$, dando un residuó cuadrático con mod 31, con esto se obtendrán dos raíces $(z_1,z_2)$
  P=((18,1)21)
  $y_2 = 18^3 + 2(18) + 7 mod 31 = 16 \rightarrow y = \pm 4$
  $y_1$ nos indicará que se tendrá que obtener una z tal que z $\equiv$ 1 mod 2, con lo que se tiene qie observar que -4 $\equiv$ 27 mod 31, 27 $\equiv$ 1 mod 2 y mod 4 $\equiv$ 0 mod 2 con lo que obtendríamos que nuestro punto de comprensión -como se mencionó anteriormente- tenemos que es (18,27).
  Entonces tendríamos que:
  8(18,27) = (15,8)
  $\rightarrow$ el inverso de 15 es 29 ya que 15 x 29 $\equiv$ 1 mod 31 $\rightarrow$ n = 29. Con esto se obtendría que:
  29 x 21 mod 31 = 20.

- Se tendrá que determinar cual será la raíz cuadrada la que el cual mediante el calculo se tendrá que cumplir que $z_1 \equiv y_1$ mod 2. obteniendo los puntos de descomprensión $(x_1,z_1)$. P=((3,1)18)
  $y_2 = 3^3$ + 2(3)+ 7 mod 31 = 9 $\rightarrow$y = $\pm$ 3, despues de tener esto se tendrá que calcular un z tal que z $\equiv$ 1 mod 2, el cual se observa que -3 $\equiv$ 28 mod 31, 20 $\equiv$ 0 mod 2 y 3 $\equiv$ 1 mod 2, con lo que nuestro punto de descomprensión es de (3,3).
  Se calcula a 8(3,3) = (2,9) $\rightarrow$ 2 x 16 $\equiv$ 1 mod 31 $\equiv$ n = 16, lo que vendría siendo 18 ya que 16 x 18 mod 31 = 9.

- Despues se tendrá que multiplicar el punto de descomprensión hacia la llave privada por lo que se tendrá que multiplicar por ocho lo que se vendría obtendría $x_0, y_0$
  P=((17,0)19)
  $y^2$ = $17^3$ + 2(17) + 7 mod 31 = 25 $\rightarrow$y = $\pm$ 5 donde se calcula también a z -como se ha estado haciendo en los otros pasos- el cual queda que -5 $\equiv$ 26 mod 31, 26 $\equiv$ 0 mod 2 y 5 $\equiv$1 mod 2 con lo que nuestro punto de descomprensión es (17,26), teniendo esto ahora calculamos 8(17,26)=(30,29).
  Ahora el inverso vendría siendo 30 ya que 30 x 30 $\equiv$ 1 mod 31 $\rightarrow$ n = 30, con lo que se obtiene que 30 x 19 mod 31 = 12,

[5] Con el uso de los programas se pudo obtener los calculos mencionados

- Se calculará el inverso de $x_0$ con mod 31 y este multiplicandolo por $y_2$ mod 31 de igual forma. Esto nos arroja finalmente el número original que se tiene que devolver.
  P=((28,0)8)
  $y^2 = 28^3 + 2(28) + 7 \bmod 31 = 25 \rightarrow y = \pm 5$, $5 \equiv 26 \bmod 31 \equiv y = \pm 6$, y determinando a z se tiene que si $-6 \equiv 25 \bmod 31$, $25 \equiv 1 \bmod 2$ y $6 \equiv 0 \bmod 2$ con lo que obtendremos que nuestro punto de descomprensión es el (28,6).
  Ahora calculamos a 8(28,6) = (14,19) y encontrando el inverso que es 20 ya que $14 \times 20 \equiv 1 \bmod 31 \rightarrow n = 20$, por lo que obtendríamos que $20 \times 8 \bmod 31 = 5$.

*c*) Supongamos que cada texto plano representa un caracter alfabético, convierte el texto plano en una palabra en inglés. Usa la asociación (A $\rightarrow$ 1, ..., Z $\rightarrow$ 26) en este caso 0 no es considerado como un texto plano o un par ordenado.
Con los dicho anteriormente y considerandolo tendremos un esquema de codificación de la forma:

$$20 \rightarrow \text{T}$$
$$9 \rightarrow \text{I}$$
$$12 \rightarrow \text{L}$$
$$5 \rightarrow \text{E}$$