Facultad de Ciencias de la Universidad Nacional Autónoma de México

Tarea 3 de Criptografía y Seguridad

Parcial 3: Curvas elípticas

Oscar Andrés Rosas Hernandez
Jorge Luís García De Santiago

26 de noviembre de 2019

Índice general

Capítulo 1

Primera sección

Sea la curva $y^2 = x^3 + 7x + 2$ en $\mathbb{Z}_{11}$

- **Mostrar que el punto** $P = (7, 3) \in \mathbb{Z}_{11}$

  Esto es muy sencillo, basta con sustituir y suponer que $(x, y) = (7, 3)$:

$$
\begin{aligned}
y^2 &= x^3 + 7x + 2 \mod 11\\
3^2 &= 7^3 + 7(7) + 2 \mod 11\\
9 &= 7^3 + 7(7) + 2 \mod 11\\
9 &= 343 + 49 + 2 \mod 11\\
9 &= 343 + 49 + 2 \mod 11\\
9 &= 394 \mod 11\\
9 &= 394 \mod 11\\
9 &= 9 \mod 11
\end{aligned}
$$

  Pues recuerda que $394 = 11(35) + 9$.

O podemos mostrarlo de otra manera diciendo que:

$$\begin{aligned}
y^2 &= x^3 + 7x + 2 \mod 11 \\
y^2 &= 7^3 + 7(7) + 2 \mod 11 \\
y^2 &= 7^3 + 7(7) + 2 \mod 11 \\
y^2 &= 343 + 49 + 2 \mod 11 \\
y^2 &= 343 + 49 + 2 \mod 11 \\
y^2 &= 394 \mod 11 \\
y^2 &= 394 \mod 11 \\
y^2 &= 9 \mod 11
\end{aligned}$$

Y también que $y^2 = 9 \to y = 3$.

Por lo tanto $(7, 3) \in \mathbb{Z}_{11}$

- **Dar el orden de $P = (7, 3)$**

  El orden de un punto es un k tal que $kP = \mathbb{O}$, y por lo tanto $(k-1)P = -P$.

  Recordemos tambien que si $P = (x, y)$ entonces $-P = (x, -y)$.

  Ahora veamos que:

  - $P + P = (8, 8)$
  - $2P + P = (10, 4)$
  - $3P + 3P = (7, 8)$

  Por lo tanto $6P = (7, 8) = -P$, por lo tanto el orden es 7.

- **Usar el teorema de Hasse y el orden de $(7, 3)$ para encontrar el orden de $\mathbb{Z}_{11}$**

  El teorema dice que:

$$\begin{aligned}
q + 1 - 2\sqrt{q} \leq \#E(F_q) &\leq q + 1 + 2\sqrt{q} \\
11 + 1 - 2\sqrt{11} \leq \#E(F_q) &\leq 11 + 1 + 2\sqrt{11} \\
5 \leq \#E(F_q) &\leq 19
\end{aligned}$$

- **Verificar que la cardinalidad de E es igual a** $q+1+\sum_{x\in\mathbb{Z}_{11}} \frac{x^3+7x+2}{11}$ **donde** $\frac{x^3+7x+2}{11}$ **es el símbolo de Lengendre y** $q = 11$**.**

  Tenemos que:

$$\begin{aligned}
\#E(\mathbb{Z}_{11}) &= q + 1 + \sum_{x\in\mathbb{Z}_{11}} \frac{x^3+7x+2}{11} \\
&= 11 + 1 + \sum_{x\in\mathbb{Z}_{11}} \frac{x^3+7x+2}{11} \\
&= 11 + 1 + \frac{2+10+24+50+94+162+260+394+570+794+1072}{11} \\
&= 11 + 1 + \frac{3432}{11} \\
&= 11 + 1 + (312 \mod 11) \\
&= 11 + 1 + 4 \\
&= 16
\end{aligned}$$

Capítulo 2

Segunda sección

Sea la ecuacion $y^2 = x^3 + x + 1$ en $\mathbb{Z}_{77}$ y sea el punto $P = (0, 1)$ que satisface la ecuacion anterior, calcule 5P sumando de P en P y asi encontrar un factor de 77.

Recordemos que:

- If $P_1 \neq P_2$ and $x_1 = x_2$, then $P_1 + P_2 = \mathcal{O}$.
- If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = 2P_1 = \mathcal{O}$.
- If $P_1 \neq P_2$ (and $x_1 \neq x_2$),
$$\text{let } \lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ and } \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$
- If $P_1 = P_2$ (and $y_1 \neq 0$),
$$\text{let } \lambda = \frac{3x_1^2 + A}{2y_1} \text{ and } \nu = \frac{-x^3 + Ax + 2B}{2y}.$$

Then

$$P_1 + P_2 = (\lambda^2 - x_1 - x_2, -\lambda^3 + \lambda(x_1 + x_2) - \nu).$$

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

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

$$x = (39)^2 - 2(0) \mod 77 = 58$$

$$y = 39(0 - 58) - 1 \mod 77 = 47$$

Por lo tanto es $(58, 47)$

- $2P + P$

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

$$x = (30)^2 - 58 \mod 77 = 72$$

$$y = 30(58 - 72) - 47 \mod 77 = 72$$

Por lo tanto es $(72, 72)$

- $2P + 2P$

$$\lambda = \frac{3(58)^2 + 1}{2(47)} = \frac{10093}{94} \mod 77 = 68 * 10093 \mod 77 = 23$$

$$x = (23)^2 - 2(58) \mod 77 = 28$$

$$y = 23 + 23(58 * 2) - 47 \mod 77 = 27$$

Por lo tanto es $(28, 27)$

- $4P + P$

$$\lambda = \frac{1-27}{0-28} = \frac{26}{28} \mod 77$$

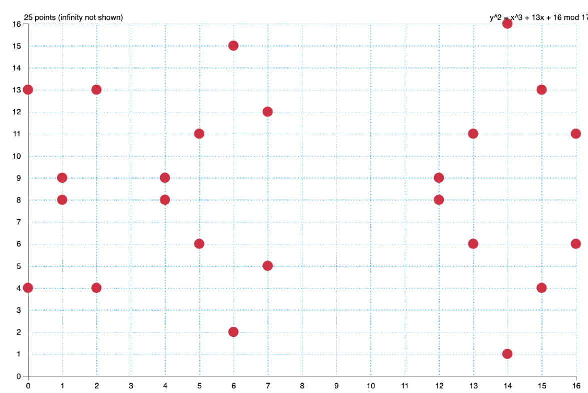
Ahora encontramos un problema porque el $gcd(28, 77) \neq 1$, sino es 7, y por lo mismo no podemos sumar hasta llegar a $5P$, pero mas importante, ya encontramos un factor de 77, el 7.

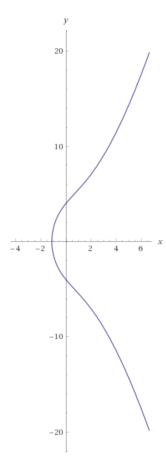
Capítulo 3

Tercera sección

Sea la curva $y^2 = x^3 + 13x + 16$ en $\mathbb{Z}_{17}$

- Mostremos todos los puntos de E.





Para empezar podemos hacer un programa que los calcule a todos por fuerza bruta, comprobando la ecuacion, con ello obtenemos 24 puntos.

```
from typing import *
point = Tuple[int, int]


def get_points(A: int, B: int, p: int) -> List[point]:
    '''y^2 = x^3 + Ax + B'''

    points: List[point] = []

    for x in range(p):
        lhs = (pow(x, 3, p) + (A * x) + B) % p

        for y in range(p):
            rhs = pow(y, 2, p)

            if lhs == rhs:
                points.append((x, y))

    return points


points = get_points(A=13, B=16, p=17)
print(points)
print(len(points))
```

Con los puntos:

```
[
  (0, 4), (0, 13), (1, 8), (1, 9), (2, 4),
  (2, 13), (4, 8), (4, 9), (5, 6), (5, 11),
  (6, 2), (6, 15), (7, 5), (7, 12), (12, 8),
  (12, 9), (13, 6), (13, 11), (14, 1), (14, 16),
  (15, 4), (15, 13), (16, 6), (16, 11)
]
```

Siendo mas formales por definicion se consideran los puntos como:

$E(L) = \{\ \infty\ \}\, u \left\{\ (x, y) \in L \times L | y^2 = x^3 + 13x + 16\ \right\}$

Es decir los puntos del programa mas el infinito.

- Alicia desea enviar el siguiente mensaje $C = (a, b) = ((6, 2), (14, 1))$ a Bob, los parametros publicos de Bob son $\alpha = (0, 13) \in E$ una raiz primitiva y $\beta = (15, 13)$, donde $beta = s\alpha$ y s su llave privada.

Usa cualquier algoritmo mencionado en la seccion 5.2 del libro Elliptic Curves Number Theory and Cryptography de Lawrence C. Washington Para resolver logaritmo.

Vamos a hacer el algoritmo de Paso chico, paso grande.

Ya sabemos el orden del grupo (25), lo que podemos seleccionar a $m = 6$, pues $m \geq \sqrt{N}$.

Ahora podemos computar $mP = 6(0, 13)$, esto va vimos como hacerlo a mano, así que solo mostraremos el resultado final:

- $2(0, 13) = (13, 6)$
- $3(0, 13) = (6, 2)$
- $4(0, 13) = (12, 9)$
- $5(0, 13) = (7, 12)$
- $6(0, 13) = (1, 9)$

Ahora tenemos que hacer lo siquiente:

- $Q - jmP = (15, 13) - 1(1, 9) = (15, 13) + (1, 8) = (0, 13)$
- $Q - jmP = (15, 13) - 2(1, 9) = (15, 13) - (16, 6) = (15, 13) + (16, 11) = (7, 5)$
- $Q - jmP = (15, 13) - 3(1, 9) = (15, 13) - (15, 14) = (15, 13) + (15, 3) = (0, 0)$
- $Q - jmP = (15, 13) - 4(1, 9) = (15, 13) - (0, 4) = (15, 13) + (0, 13) = (2, 4)$
- $Q - jmP = (15, 13) - 5(1, 9) = (15, 13) - (7, 12) = (15, 13) + (7, 5) = (13, 6)$
- $Q - jmP = (15, 13) - 6(1, 9) = (15, 13) - (5, 6) = (15, 13) + (5, 11) = (12, 8)$

Y es aqui cuando me di por vencido, luchando, hasta que me di cuenta que se me habia olvidado lo mas obvio: $1(0, 13) = (0, 13)$.

Y mira que: $Q - jmP = (15, 13) - 1(1, 9) = (15, 13) + (1, 8) = (0, 13)$

Por lo tanto podemos ver que: $iP = Q - jmP$, por lo tanto la respuesta es $i + jm \mod N$, es decir $1 + 1(6) \mod N = 7$.

Y mira que estuve muy cerca de calcularla.

Por lo tanto $7(0, 13) = (15, 13)$

- A partir de la informacion encontrada antes descifra el mensaje enviado a Bob

  Solucion: Usando ElGamal (pagina 188 del libro) siguiendo la formula de: $M = M2 - sM1$

Se tiene que:

$$
\begin{aligned}
M &= (14,1) - s(6,2) \\
&= (14,1) - 7(6,2) \\
&= (14,1) - (12,8) \\
&= (14,1) + (12,9) \\
&= (7,5)
\end{aligned}
$$

Donde el mensaje original es $M = (7,5)$.

Capítulo 4

Cuarta sección

Sea la curva $y^2 = x^3 + 7x + 19$ en $\mathbb{Z}_{31}$ y $P = (18, 26)$ un punto en E de orden 39, el ECIES simplificado definido sobre $\mathbb{Z}_{31}$ como espacio de texto plano, supongamos que la clave privada es $m = 8$.

- Usando lo que vimos antes podemos solo mostrar el resultado:

  $Q = mP = 8(18, 26) = (10, 2)$

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

  Sabemos que en el criptosistem ECIES simplificado, el mensaje cifrado es de la forma $((Zp \times Z_2) \times Zp^*) = (y_1, y_2)$

  Como el orden de P es el mismo que E, P es un generador y puede ser usado en la encriptacion de ECIES simplificado.

  Los puntos de compresion recibidos son: $(4, 1), (11, 0), (27, 1), (28, 1), (23, 0)$

  Debemos calcular sus respectivos puntos de descompresion. Sabemos que:

  $z \leftarrow (x^3 + 7x + 19) \mod 31$

  - $$\begin{aligned} z &\leftarrow (x^3 + 7x + 19) \mod 31 \\ &\leftarrow (4^3 + 7(4) + 19) \mod 31 \\ &\leftarrow 111 \mod 31 \\ &\leftarrow 18 \mod 31 \end{aligned}$$

Por lo que $y = \pm 7$, por la segunda componentes es $y = 7$. por lo tanto el punto es $8 * (4, 7) = (2, 17)$.
$d = 1 * 2^{-1} \mod 31 = 16 = 16 \mod 31$, es decir P.

- $$\begin{aligned} z &\leftarrow (x^3 + 7x + 19) \mod 31 \\ &\leftarrow (11^3 + 7(11) + 19) \mod 31 \\ &\leftarrow 1427 \mod 31 \\ &\leftarrow 1 \mod 31 \end{aligned}$$

  Por lo que $y = \pm 1$, por la segunda componentes es $y = 30$. por lo tanto el punto es $8 * (11, 30) = (23, 3)$.
  $d = 18 * 23^{-1} \mod 31 = 18 * 27 = 21 \mod 31$, es decir U.

- $$\begin{aligned} z &\leftarrow (x^3 + 7x + 19) \mod 31 \\ &\leftarrow (27^3 + 7(27) + 19) \mod 31 \\ &\leftarrow 19891 \mod 31 \\ &\leftarrow 20 \mod 31 \end{aligned}$$

  Por lo que $y = \pm 12$, por la segunda componentes es $y = 19$. por lo tanto el punto es $8 * (27, 19) = (18, 26)$.
  $d = 17 * 18^{-1} \mod 31 = 17 * 19 = 13 \mod 31$, es decir M.

- $$\begin{aligned} z &\leftarrow (x^3 + 7x + 19) \mod 31 \\ &\leftarrow (28^3 + 7(28) + 19) \mod 31 \\ &\leftarrow 22167 \mod 31 \\ &\leftarrow 2 \mod 31 \end{aligned}$$

  Por lo que $y = \pm 2$, por la segunda componentes es $y = 23$. por lo tanto el punto es $8 * (28, 23) = (29, 20)$.
  $d = 29 * 29^{-1} \mod 31 = 1 \mod 31$, es decir B.

- $$\begin{aligned} z &\leftarrow (x^3 + 7x + 19) \mod 31 \\ &\leftarrow (23^3 + 7(23) + 19) \mod 31 \\ &\leftarrow 12347 \mod 31 \\ &\leftarrow 9 \mod 31 \end{aligned}$$

  Por lo que $y = \pm 3$, por la segunda componentes es $y = 28$. por lo tanto el punto es $8 * (23, 28) = (3, 25)$.
  $d = 26 * 3^{-1} \mod 31 = 26 * 21 = 19 \mod 31$, es decir S.
  pumbs

Bibliografía

[1] Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. 1996. Handbook of Applied Cryptography (1st ed.). CRC Press, Inc., Boca Raton, FL, USA.