Breve documento sobre Curvas elípticas.

Jesús Martín Ovejero.

En el presente documento se resolverán algunos problemas relativos a curvas elípticas. También se verá la aplicación de las curvas elípticas a la criptografía asimétrica.

Problema 1. Considérese la curva elíptica $y^2 = x^3 + x + 1$ sobre $\mathbb{F}_5$. Calcular todos los puntos racionales de la curva y probar que el conjunto de puntos racionales de la curva es un grupo de orden 9.

Solución 1. El procedimiento para calcular los puntos racionales de una curva definida sobre un cuerpo finito es sencillo. En primer lugar estudiaremos cuáles son los posibles valores de x, y de la expresión x^3+x+1. En función de esta última expresión calcularemos los valores de y.

Para empezar supongamos que $x = 0$. En este caso se tiene que la expresión $x^3 + x + 1$ es 1 y por tanto $y^2 = 1$. Los puntos $y \in \mathbb{F}_5$ que verifican que $y^2 = 1$ son $y = \pm 1$ mód. 5, es decir $y = 1$ e $y = 4$. Por tanto las parejas $(0, 1)$ y $(0, 4)$ son puntos de la curva.
Consideremos ahora $x = 1$. En este caso se tiene que la expresión $x^3 + x + 1$ toma el valor 3. Una comprobación elemental demuestra que la expresión $y^2 = 3$ no tiene solución en $\mathbb{F}_5$.

Procediendo del mismo modo llegamos a la siguiente tabla:

Curva $y^2 = x^3 + x + 1$ sobre $\mathbb{F}_5$			
x	$x^3 + x + 1$	y	Puntos
0	1	± 1	$(0, 1), (0, 4)$
1	3	-	-
2	1	± 1	$(2, 1), (2, 4)$
3	1	± 1	$(3, 1), (3, 4)$
4	4	± 2	$(4, 2), (4, 3)$

Al conjunto de puntos racionales hay que añadirle el punto del infinito ∞. La tabla queda por tanto del siguiente modo:

Curva $y^2 = x^3 + x + 1$ sobre $\mathbb{F}_5$			
x	$x^3 + x + 1$	y	Puntos
0	1	± 1	$(0, 1), (0, 4)$
1	3	-	-
2	1	± 1	$(2, 1), (2, 4)$
3	1	± 1	$(3, 1), (3, 4)$
4	4	± 2	$(4, 2), (4, 3)$
∞		∞	∞

Concluimos que el conjunto de puntos racionales es un grupo de orden 9.

Problema 2. Encriptar el mensaje $(13, 10, 5)$ utilizando una curva elíptica cualquiera.

Solución 2. Antes de proceder a la resolución del problema vamos a recordar cual es el el sistema criptográfico. En primer lugar ha de fijarse un número primo p y considerar una curva elíptica E sobre $\mathbb{F}_p$. Se ha de considerar un punto racional $P \in E(\mathbb{F}_p)$ de orden n, siendo n el orden del grupo que genera el punto. Cada usuario de la comunicación tiene una clave privada que es un entero entre 1 y $n-1$ y una clave pública que es el punto racional $Q = d \cdot P$. El usuario da a conocer la clave pública y mantiene en secreto la clave privada. Los algoritmos de cifrado y descifrado son los siguientes:

Cifrado

- Sea m el mensaje que se va a enviar, y $M \in E$ el punto de la curva que le asociamos a m.
- Tomamos k al azar con $1 \leq k \leq n-1$.
- Calculamos la pareja de puntos $C_1 = k \cdot P$, $C_2 = M + k \cdot Q$, siendo Q la clave pública del destinatario.
- Se envía (C_1, C_2).

Descifrado

- Recibimos los datos (C_1, C_2) que representan dos puntos de E.
- Siendo d nuestra clave privada, recuperamos el punto M mediante el cálculo $M = C_2 - d \cdot C_1$, ya que
$$(M + k \cdot Q) - d \cdot k \cdot P = (M + k \cdot d \cdot P) - d \cdot k \cdot P = M$$
- recuperamos el mensaje m como el texto asociado al punto M

Observación 0.1. Si quisiéramos implementar enviar cualquier texto escrito en formato ASCII, deberíamos encontrar una curva elíptica con al menos 257 puntos racionales (contando con el infinito). Utilizando el teorema de Hasse-Weil sabemos que se ha de verificar que

$$2\sqrt{p} \geq 257 - (p+1) \Rightarrow 2\sqrt{p} + p \geq 256 \Leftrightarrow p \geq 226.$$

Se tiene por tanto que para poder cifrar a través de una curva elíptica todos los caracteres del alfabeto ASCII, necesitamos considerar un número primo mayor que 226. Por ejemplo, la curva elíptica utilizada para cifrar y descrifrar en WhatsApp se conoce como curva 25519, y el número primo que se toma es $p = 2^{555} - 19$.

Vamos a implementar el sistema de cifrado y descifrado en Mathematica. Las curvas elípticas que consideraremos son de la forma:

$$y^2 = x^3 + ax + b$$

y el número primo p será mayor o igual que 5. Vamos a recordar lo siguiente (TEORÍA): dados dos puntos (x_1, y_1) y (x_2, y_2) distintos de la curva elíptica $y^2 = x^3 + ax + b$, su suma es el punto (x, y) donde:

- $x = \lambda^2 - x_1 - x_2$,
- $y = -y_1 + \lambda(x_1 - x)$
- $\lambda = (y_2 - y_1)/(x_2 - x_1)$.

En el caso de considerar dos puntos iguales, se tiene que $2(x_1, x_2) = (x, y)$ con:

- $x = \lambda^2 - 2x_1$,
- $y = -y_1 + \lambda(x_1 - x)$,
- $\lambda = (3x_1^2 + a)/(2y_1)$.

A continuación vamos a implementar la función SumaCurvaElipticaCompleto[p,a,b,P,Q] que va a sumar los puntos P y Q de la curva elíptica $y^2 = x^3 + ax + b$. Para ello vamos a considerar dos casos, cuando los puntos que se suman son distintos o iguales. Además, en la implementación

final se ha de tener en cuenta el caso en el que el punto resultante o alguno de los datos de entrada es el punto del infinito, siendo éste denotado por O.

```
SumaCurvaElipticaDistintos[p_, a_, b_, P_List, Q_List] := Module[{l1, x3, y3, P3},
                                                          módulo

  l1 = Mod[(Q[[2]] - P[[2]]) * PowerMod[(Q[[1]] - P[[1]]), -1, p], p];
       operación módulo              potencia modular
  x3 = Mod[l1^2 - P[[1]] - Q[[1]], p];
       operación módulo
  y3 = Mod[-P[[2]] + l1 (P[[1]] - x3), p];
       operación módulo
  P3 = {x3, y3}
 ]

   SumaCurvaElipticaIguales[p_, a_, b_, P_List] := Module[{l2, x4, y4, P3},
                                                   módulo

      l2 = Mod[(3 (P[[1]]^2) + a) * PowerMod[2 P[[2]], -1, p], p];
           operación módulo          potencia modular
      x4 = Mod[l2^2 - 2 P[[1]], p];
           operación módulo
      y4 = Mod[-P[[2]] + l2 (P[[1]] - x4), p];
           operación módulo
      P3 = {x4, y4}];

SumaCurvaElipticaCompleto[p_, a_, b_, P_List, Q_List] := Module[{P3, R, S},
                                                         módulo

  If[And[P == {0}, Q ≠ {0}], P3 = Q];
  si  operación y notación O notación O
  If[And[P == {0}, Q == {0}], P3 = {0}];
  si  operación y notación O notación O    notación O
  If[And[P ≠ {0}, Q == {0}], P3 = P];
  si  operación y notación O notación O
  If[And[And[P ≠ {0}, Q ≠ {0}], And[P[[1]] == Q[[1]], P[[2]] == Q[[2]]]],
  si  op··· operación y notación O nota·· operación y
   P3 = SumaCurvaElipticaIguales[p, a, b, P]];
  If[And[And[P ≠ {0}, Q ≠ {0}], And[P[[1]] == Q[[1]], P[[2]] == Q[[2]]]],
  si  op··· operación y notación O nota·· operación y
   P3 = SumaCurvaElipticaIguales[p, a, b, P]];
  If[And[And[P ≠ {0}, Q ≠ {0}], And[P[[1]] ≠ Q[[1]], P[[2]] ≠ Q[[2]]]],
  si  op··· operación y notación O nota·· operación y
   P3 = SumaCurvaElipticaDistintos[p, a, b, P, Q]];
  If[And[And[P ≠ {0}, Q ≠ {0}], And[P[[1]] == Q[[1]], P[[2]] ≠ Q[[2]]]], P3 = {0}];
  si  op··· operación y notación O nota·· operación y                    notació


  P3];
```

A continuación vamos a implementar la función que calcula el múltiplo de un punto P de la curva. Será una función que llame a la función SumaCurvaElipticaCompleto n-veces.

```
Mult[n_, P_, q_, a_, b_] := Module[{x, A, B}, x = n; A = P; B = {0};
                            módulo                  notación O

While[x > 1, If[OddQ[x], B = SumaCurvaElipticaCompleto[q, a, b, A, B];
mientras     si  ¿impar?
x = x - 1, A = SumaCurvaElipticaCompleto[q, a, b, A, A];
x = x / 2;
];
];
A = SumaCurvaElipticaCompleto[q, a, b, A, B];
A]
```

En nuestro caso vamos a considerar la curva elíptica del primer ejercicio que es: $y^2 = x^3 + x + 1$ sobre $\mathbb{F}_5$. El punto que vamos a considerar es $P = (0, 4)$. Para saber el orden del punto vamos a crear una tabla con sus múltiplos, $P, 2P, 3P...$:

```
DeleteDuplicates[Table[Mult[i, {0, 4}, 5, 1, 1], {i, 1, 9}]]
elimina repeticiones    tabla

{{0, 4}, {4, 3}, {2, 4}, {3, 1}, {3, 4}, {2, 1}, {4, 2}, {0, 1}, {0}}
```

El punto P considerado tiene orden 9 y genera al grupo de puntos racionales de la curva. Supongamos que el Usuario A y el Usuario B eligen enteros al azar (claves privadas) que van a ser 2 y 4 respectivamente. Las claves públicas de ambos usuarios serán:

$$Q_1 = 2P = (4, 3), \quad Q_2 = 4P = (3, 1),$$

respectivamente. El usuario A quiere enviar el mensaje (13,10,5). Empecemos por el 10. El convenio a seguir será la siguiente correspondencia entre puntos de la curva:

$$13 - - > (0, 1), \quad 10 - -- > (2, 1), \quad 5 - -- > (4, 2).$$

El usuario A codifica el 10 del modo que sigue. Considera un entero k al azar entre $1 \leq k \leq 8$, por ejemplo $k = 3$. El usuario A calcula

$$C_1 = k \cdot P, \quad C_2 = M + kQ_2$$

siendo M el punto $(0, 1)$ (el que le corresponde a 13). Utilizando las funciones implementadas en Mathematica:

$$C_1 = (2, 4), \quad C_2 = (2, 4).$$

Procediendo análogamente se cifran 10 y 5.