Curvas Elípticas

Este documento no pretende ser un curso exhaustivo, en el mejor de los casos, únicamente puede considerarse como un conjunto de notas complementarias en alguna asignatura. Por supuesto, todo documento es susceptible de mejora, cualquier sugerencia o comunicación de error u omisión será bienvenida.

Formalmente, una curva elíptica es el conjunto de puntos definido por una ecuación de la forma $y^2 = x^3 + ax + b$ para determinados valores a y b. Intuitivamente, una curva elíptica tiene una forma similar a las mostradas en la Figura 1.

En el contexto de aplicaciones criptográficas que se tratan aquí, es interesante que la curva no tenga discontinuidades como las de las curvas de la fila inferior de la Figura 1, para ello los valores de a y b deben cumplir la ecuación:

$$4a^3 + 27b^2 \neq 0.$$

Si a la definición de curva elíptica se le añade un punto en el infinito, que denotaremos como 0, se obtiene que cualquier recta no tangente que corte la curva lo haga en tres puntos. En el caso que la recta sea tangente a la curva, el número de puntos comunes a la recta y la curva es dos (pudiendo ser uno de ellos el infinito). Esto será clave en la definición de las operaciones criptográficas sobre curvas elípticas.

Definición de grupo basado en CE

En criptografía basada en curvas elípticas se considera una de estas curvas para definir un grupo sobre el que realizar transformaciones. Recordamos que un grupo $\langle C, \oplus \rangle$ es una estructura algebraica que cumple las propiedades:

- La operación $\oplus$ es de composición interna y asociativa.
- Existe un (único) elemento neutro.
- Todo elemento del grupo tiene inverso respecto $\oplus$.

Considerando una curva elíptica, puede definirse un grupo donde el conjunto viene dado por los puntos de la curva elíptica al que se añade el punto en el infinito 0, el punto en el infinito es el elemento neutro, y el inverso de P, que denotaremos con $-P$, como el punto simétrico a P respecto el eje X.

Obviamente falta definir la operación $\oplus$ a la que nos referiremos como *suma* en lo que sigue (de ahí que se denote como 0 el elemento neutro). La definición de la operación se

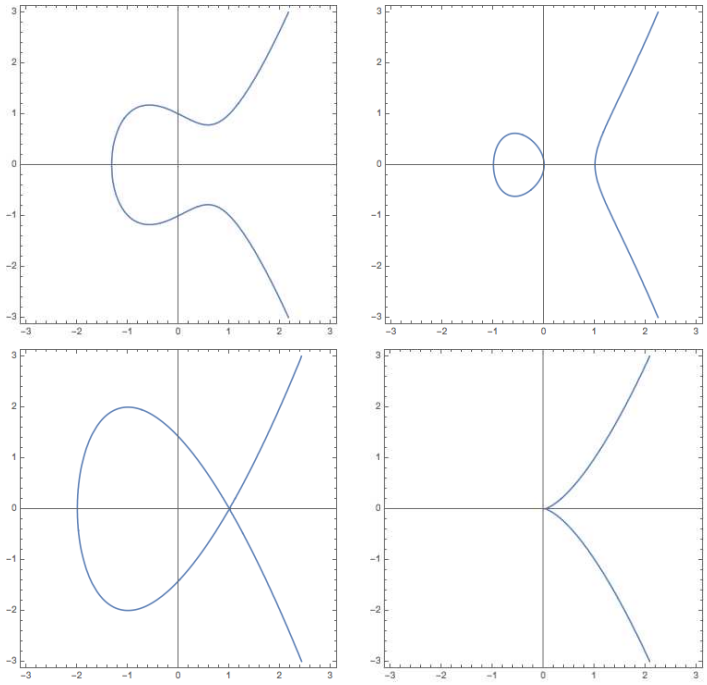

Figura 1: Curvas elípticas.

basa en que la suma de tres puntos alineados P, Q y R da como resultado el elemento neutro, esto es:

$$P \oplus Q \oplus R = 0.$$

Aunque un poco más adelante definiremos formalmente esta operación de suma de puntos, utilizando una representación gráfica de la curva es fácil entender intuitivamente la operación $P \oplus Q$ para dos puntos P y Q cualesquiera de una curva elíptica C. El primer paso es trazar la recta secante a la curva y que pase por P y Q.

Caso i

Si la recta que pasa por los puntos P y Q corta a la curva en un tercer punto, ese punto es el inverso de $P \oplus Q$ que buscamos obtener.

En terminos gráficos, el tercer punto de la recta que corta la curva es $-(P \oplus Q)$, y, como hemos definido un poco más arriba, $P \oplus Q$ es el simétrico respecto el eje X. La Figura 2 ilustra este proceso.

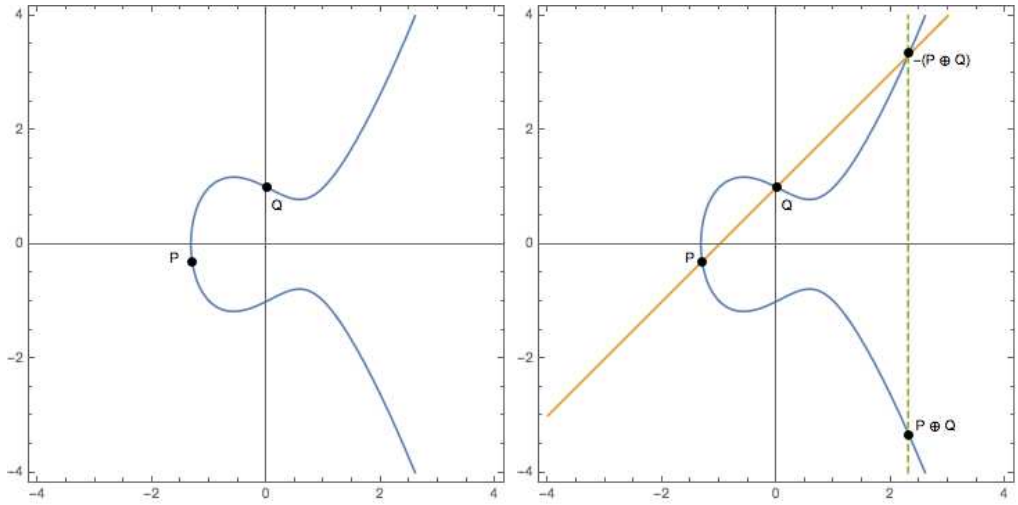

Figura 2: Definición gráfica de suma de puntos en una curva elíptica.

Caso ii

La definición de la operación $\oplus$ es consistente con la de elemento neutro, esto es, $0 \oplus P = P \oplus 0 = P$. Sirva como explicación gráfica la mostrada en la Figura 3.

Incluímos en este caso la suma de un punto y su inverso. Obviamente, $P \oplus (-P)$ debe dar como resultado el elemento neutro 0. La misma Figura 3 ilustra gráficamente este caso.

Caso iii

Tratamos en este caso la suma de un valor consigo mismo. En este caso la operación considera un único punto de la curva elíptica, por lo que la recta secante considerada en la suma de dos puntos se sustituye por una tangente sobre la curva (forzando un poco el argumento, una secante que pasa dos veces por el punto que se suma). La Figura 4 ilustra gráficamente la operación.

Caso iv

Por último, consideramos el caso particular cuando la recta que pasa por los puntos P y Q a sumar no corta a la curva en un tercer punto. En este caso, la recta es tangente a la curva en el punto P o en el punto Q.

Considerando que P es el punto en el cual la recta es tangente a la curva, $P \oplus Q = -P$. Sirva como explicación intuitiva que en este caso, puede verse el tercer punto de la recta que corta a la curva como una copia de P. La Figura 5 ilustra este caso.

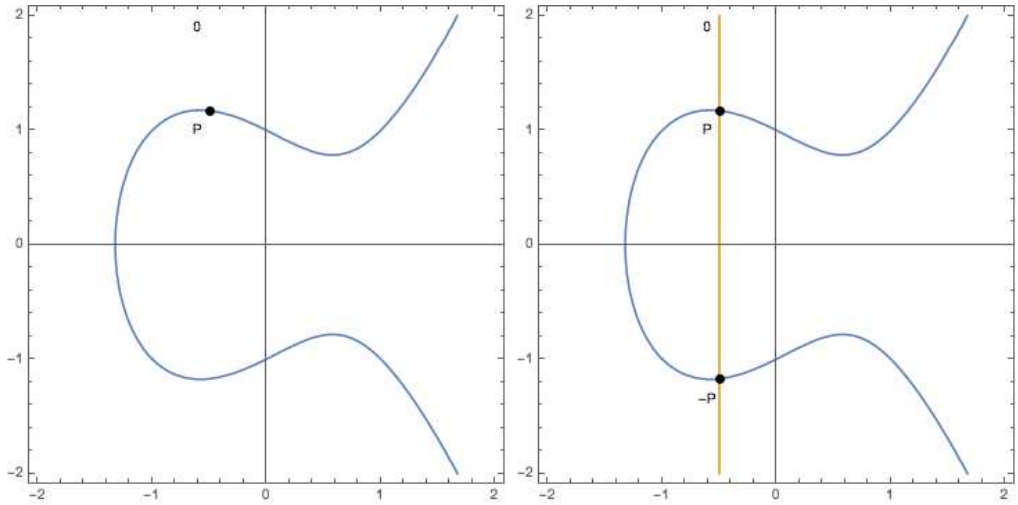

Figura 3: Prueba gráfica del 0 como elemento neutro.

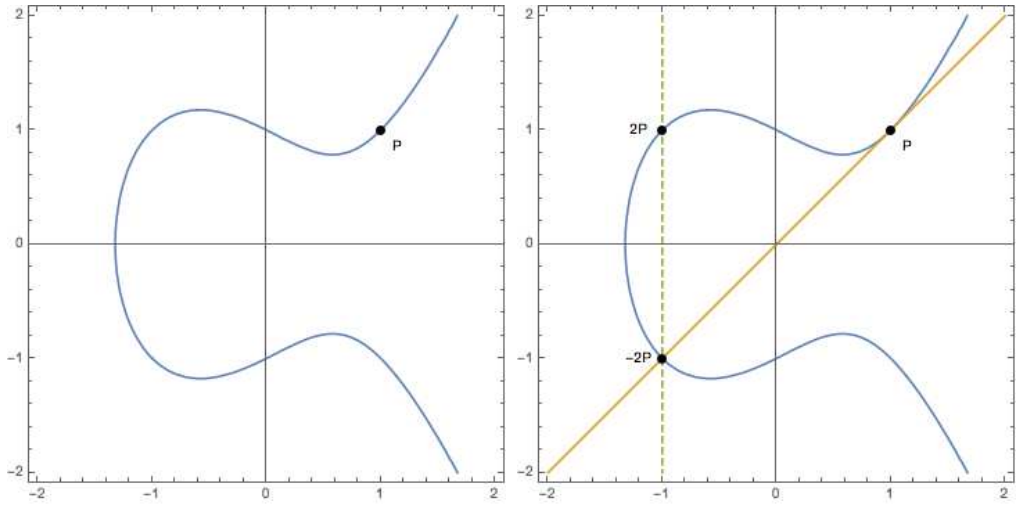

Figura 4: Cálculo de $P \oplus P$.

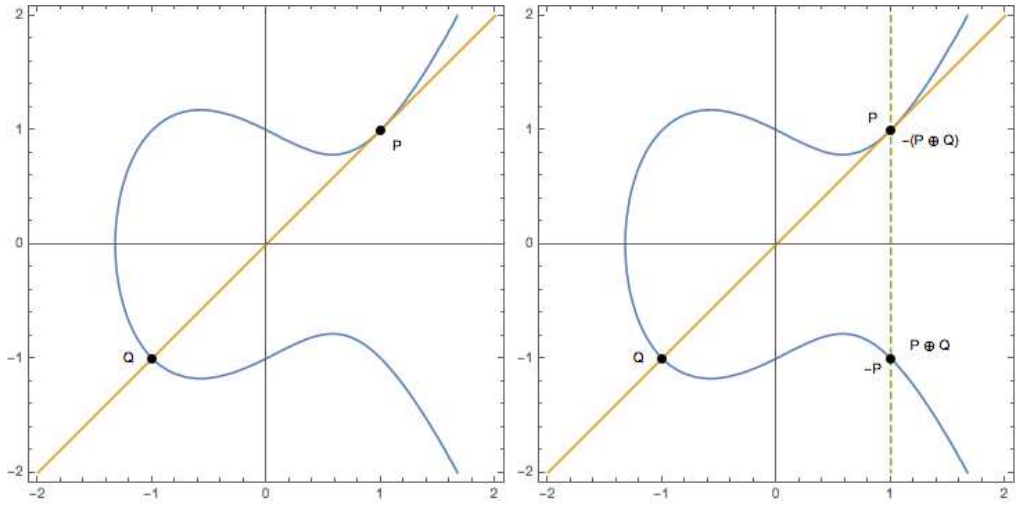

Figura 5: Si $P \oplus P = -Q$, entonces $P \oplus Q = -P$.

Cálculo de $P \oplus Q$

Para el cálculo efectivo de la suma de dos puntos en una curva elíptica se necesita formular las operaciones gráficas expuestas anteriormente.

En esta sección se exponen sin demostración las operaciones necesarias para llevarlas a cabo. Se intentará, sin embargo, relacionar las distintas formulas con las ideas intuitivas expuestas hasta el momento.

Dados dos puntos P y Q sobre una curva elíptica, en la suma $P \oplus Q$ se descartan como casos particulares:

- Cuando $P = 0$ (o bien $Q = 0$), en cuyo caso $P \oplus Q = Q$ (respectivamente $P \oplus Q = P$).
- La suma $P \oplus (-P) = 0$, por ser aplicación de la definición.

proporcionamos por lo tanto el procedimiento para el calculo de $P \oplus Q$ cuando los puntos P y Q no son uno inverso del otro y ninguno es el elemento neutro.

En todos los casos, consideraremos la curva $y^2 = x^3 + ax + b$ y las coordenadas de los puntos $P = (x_P, y_P)$ y $Q = (x_Q, y_Q)$.

Caso i: $P \neq Q$

En el caso de que $P \neq Q$, el primer paso para trasladar la idea gráfica expuesta sería calcular la pendiente de la recta que pasa por P y Q:

$$m = \frac{y_P - y_Q}{x_P - x_Q}$$

para posteriormente obtener las coordenadas del tercer punto R en el que intersectan la recta y la curva:

$$\begin{aligned} x_R &= m^2 - x_P - x_Q \\ y_R &= y_P + m(x_R - x_P) \end{aligned} \tag{1}$$

$$(\text{alternativamente, } y_R = y_Q + m(x_R - x_Q))$$

Por lo tanto, para obtener las coordenadas de $P \oplus Q$, basta considerar $(x_R, -y_R)$.

Ejemplo 1. *Consideremos la curva elíptica $y^2 = x^3 - x + 1$ y los puntos $P = (1, 1)$ y $Q = (-1, -1)$.*

Al ser $P \neq Q$ y $P \neq -Q$, el primer paso es calcular la pendiente de la recta $\overline{PQ}$:

$$m = \frac{y_P - y_Q}{x_P - x_Q} = \frac{1 - (-1)}{1 - (-1)} = 1.$$

Una vez calculada la pendiente se obtienen las coordenadas del tercer punto que corta a la curva:

$$\begin{aligned} x_R &= m^2 - x_P - x_Q = 1 - 1 - (-1) = 1 \\ y_R &= y_P + m(x_R - x_P) = 1 + (1 - 1) = 1 \end{aligned}$$

por lo que $P \oplus Q = (1, -1)$.

Caso ii: $P = Q$

En el caso de que $P = Q$, el cálculo de la pendiente de la recta tangente es distinto:

$$m = \frac{3x_P^2 + a}{2y_P}$$

una vez calculada la pendiente de la recta tangente a la curva en P, las coordenadas de R se obtienen con las mismas ecuaciones descritas en 1.

Ejemplo 2. *Consideremos la curva elíptica* $y^2 = x^3 - x + 1$ *y el punto* $P = (-1, -1)$. *En el cálculo de* $P \oplus P$ *el primer paso es calcular la pendiente de la recta tangente a la curva en* P*:*

$$m = \frac{3x_P^2 + a}{2y_P} = \frac{3(-1)^2 - 1}{2(-1)} = -1.$$

Una vez calculada la pendiente se obtienen las coordenadas del tercer punto que corta a la curva:

$$x_R = m^2 - x_P - x_Q = 1 - (-1) - (-1) = 3$$
$$y_R = y_P + m(x_R - x_P) = -1 - (3 - (-1)) = -5$$

por lo que $P \oplus P = (3, 5)$.

Cálculo de kP

Del mismo modo que se define la potencia en un grupo módulo n como composición de la operación producto, puede definirse el producto por un escalar en un grupo definido sobre una curva elíptica.

$$kP = \underbrace{P \oplus P \oplus P \oplus \ldots \oplus P}_{k \text{ veces}}$$

Ejemplo 3. *Consideremos la curva elíptica* $y^2 = x^3 - x + 1$ *y el punto* $P = (-1, -1)$.

El cálculo de $4P$ *supone, inicialmente, realizar el cálculo:*

$$4P = P \oplus P \oplus P \oplus P$$

concretamente:

$$(-1, 1) \oplus (-1, 1) = (3, -5)$$

$$(3, -5) \oplus (-1, 1) = (\tfrac{1}{4}, \tfrac{7}{8})$$

$$(\tfrac{1}{4}, \tfrac{7}{8}) \oplus (-1, 1) = (\tfrac{19}{25}, \tfrac{103}{125})$$

Para el cálculo eficiente del producto por un escalar en el grupo definido por una curva elíptica puede utilizarse el hecho:

$$\begin{cases}(2k)P = kP \oplus kP \\ (2k+1)P = kP \oplus kP \oplus P\end{cases}$$

que permite utilizar una aproximación equivalente a la utilizada para el cálculo de la exponenciación modular por cuadrados sucesivos, considerando la codificación binaria de k y procesando los bits hacia el menos significativo. El Algoritmo 1 resume el proceso.

Algoritmo 1 Producto en una curva elíptica de un punto por un escalar

Entrada: Una curva elíptica $y^2 = x^3 + ax + b$
Entrada: Un punto P de la curva
Entrada: Un número entero k
Salida: El punto kP
  Método
  $b_1 b_2 \dots bm$ = representación binaria de k
  $sol = 0$ //sol = elemento neutro
  for $i = 1$ **to** m **hacer**
    $sol = sol \oplus sol$
    Si $b_i == 1$ **entonces**
      $sol = sol \oplus P$
    FinSi
  FinPara
  Devolver sol
  FinMétodo.

Ejemplo 4. *Consideremos la curva elíptica* $y^2 = x^3 - x + 1$ *y el punto* $P = (-1, -1)$.

Para el cálculo de $10P$ *consideramos la codificación binaria de* $20 = 1010_2$ *y aplicamos el Algoritmo 1:*

i	b_i	$sol = sol \oplus sol$	$sol = sol \oplus P$
1	1		$(-1,-1) = 0 \oplus (-1,-1)$
2	0	$(3,5) = (-1,-1) \oplus (-1,-1)$	
3	1	$(\frac{19}{25}, \frac{103}{125}) = (3,5) \oplus (3,5)$	$(\frac{159}{121}, -\frac{1861}{1331}) = (\frac{19}{25}, \frac{103}{125}) \oplus (-1,-1)$
4	0	$sol = (\frac{159}{121}, -\frac{1861}{1331}) \oplus (\frac{159}{121}, -\frac{1861}{1331})$	

Se deja el cálculo de la solución final como ejercicio.

El Algoritmo 1 realiza la operacion con complejidad $\mathcal{O}(n)$ donde n denota la talla de k (número de bits para codificar k).

Grupo definido por una CE en un cuerpo finito

Para un uso criptográfico de el grupo definido por una CE debe cambiarse el dominio y codominio de la operación $\oplus$ de $\mathbb{R}$ a $\mathbb{Z}_n$. Para esto, la definición de la curva se modifica ligeramente para considerar el conjunto de puntos que cumplen:

$$y^2 \equiv x^3 + ax + b \pmod{n}$$

para determinados valores enteros a y b que deben cumplir:

$$4a^3 \not\equiv 27b^2 \pmod{n}.$$

La consideración de $\mathbb{Z}_n$ en lugar de $\mathbb{R}$ es directa ya que, por una parte, la idea que subyace en la definición de la operación $\oplus$ (la suma de tres puntos alineados es igual al elemento neutro) puede trasladarse directamente al conjunto $\mathbb{Z}_n$. Por otra parte, los cálculos para obtener la suma de dos puntos necesita exclusivamente considerar el algoritmo extendido de Euclides para obtener los inversos del producto módulo n cuando sea necesario, concretamente, para la suma de P y Q donde $P \neq Q$:

$$m = (y_P - y_Q)(x_P - x_Q)^{-1} \text{ mód } n$$

y en el caso de que $P = Q$:

$$m = (3x_P^2 + a)(2y_P)^{-1} \text{ mód } n$$

para posteriormente obtener las coordenadas del punto $P \oplus Q$ mód n como:

$$x_{P\oplus Q} = m^2 - x_P - x_Q \text{ mód } n$$
$$y_{P\oplus Q} = -(y_P + m(x_{P\oplus Q} - x_P)) \text{ mód } n$$

Ejemplo 5. *Consideremos la curva elíptica* $y^2 \equiv x^3 - x + 1 \pmod{13}$ *y los puntos* $P = (4, 10)$ *y* $Q = (7, 5)$.

El primer paso es calcular m *(tenemos en cuenta que* $P \neq Q$ *y* $P \neq -Q$*):*

$$m = (y_P - y_Q)(x_P - x_Q)^{-1} \text{ mód } 13$$

aplicamos el algoritmo extendido de euclides y obtenemos que:

$$(4-7)^{-1} \text{ mód } 13 = 4$$

por lo que:

$$m = (10-5)4 \text{ mód } 13 = 7$$

Una vez calculada la pendiente se obtienen las coordenadas de $P \oplus Q$ mód n*:*

$$x_{P\oplus Q} = 12$$
$$y_{P\oplus Q} = 12$$

Para el cálculo de $P \oplus P$ mód n*, el cálculo de* m *cambia:*

$$(2y_p)^{-1} \text{ mód } 13 = 2$$

$$m = (3x_P^2 + a)(2y_P)^{-1} \text{ mód } 13 = 3$$

y las coordenadas del punto $P \oplus P$ mód n*:*

$$x_{P\oplus P} = m^2 - x_P - x_P \text{ mód } 13 = 1$$
$$y_{P\oplus P} = -(y_P + m(x_{P\oplus P} - x_P)) \text{ mód } 13 = 12$$

Orden del grupo

Una cuestión interesante es el número de puntos que pertenecen a la curva elíptica módulo n, o en otras palabras, ¿cuál es el orden del grupo?

Es interesante señalar que el orden del grupo puede calcularse de forma eficiente, sin embargo, no se conoce algoritmo polinómico para obtener el orden del grupo generado por un determinado punto de la curva. Obviamente, los resultados básicos sobre Teoría de Grupos (Teoremas de Lagrange, Euler, Fermat...) son aplicables en los grupos definidos por curvas elípticas.

Ejemplo 6. *Consideremos la curva elíptica* $y^2 \equiv x^3 - x + 3 \pmod{37}$ *y el punto* $P = (6, 18)$.

El conjunto de puntos de la curva puede generarse a partir de P *y, manteniendo el orden de generación, son los siguientes:*

$$\begin{aligned}\{\ & \{6,18\},\{4,27\},\{1,15\},\{20,18\},\{11,19\},\{23,23\},\\ & \{15,12\},\{0,15\},\{22,11\},\{5,7\},\{36,22\},\{21,17\},\\ & \{35,16\},\{3,29\},\{25,27\},\{34,33\},\{8,10\},\{2,3\},\\ & \{13,2\},\{27,30\},\{30,37\},\{27,7\},\{13,35\},\{2,34\},\\ & \{8,27\},\{34,4\},\{25,10\},\{3,8\},\{35,21\},\{21,20\},\\ & \{36,15\},\{5,30\},\{22,26\},\{0,22\},\{15,25\},\{23,14\},\\ & \{11,18\},\{20,19\},\{1,22\},\{4,10\},\{6,19\},0 \qquad\qquad \}\end{aligned}$$

El grupo tiene 42 puntos, por lo que se muestra que no hay relación directa entre el valor modular utilizado y el tamaño del grupo.

De acuerdo con los resultados en Teoría de Grupos, todo subgrupo tendrá un número de elementos divisor de 42. Como ejemplo, el subgrupo generado por $(1, 15)$ *tiene 14 elementos.*

Ejercicios

Ejercicio 1.

Mostrar gráficamente como $2P - P = P$.

Recuérdese que $-P$ *es el simétrico de* P *respecto el eje* X.

Ejercicio 2.

Mostrar gráficamente que, dada una curva elíptica y una recta secante que corta a la curva en tres puntos P, Q *y* R, *se cumple que* $P \oplus Q \oplus R = 0$.

Ejercicio 3.

Dada la curva $y^2 \equiv x^3 - x + 1 \pmod{23}$ *y los puntos* $P = (3, 18)$ *y* $Q = (11, 5)$, *calcular:*

1. $P \oplus Q$ mód 21
2. $Q \oplus Q$ mód 21

3. $19Q$ mód 21

Ejercicio 4.

Dada la curva $y^2 \equiv x^3 - x + 1 \pmod{29}$*, ¿cuál es el orden del subgrupo generado por el punto* $(2, 6)$*?*
