e-math | 2018

Universidad Politécnica de Cartagena

Las matemáticas de las criptodivisas

Juan Medina Molina
Departamento de Matemática Aplicada y Estadística
Universidad Politénica de Cartagena

Matemáticas y Estadística en Economía

- La estadística y las matemáticas están muy presentes en Economía.

Matemáticas y Estadística en Economía

- Bitcoin y blockchain.
- Estimación del valor de mercado de futbolistas de élite.

Bitcoin y blockchain

El bitcoin roza los 10000 dólares y dobla su cotización desde octubre.

La moneda virtual protagoniza la mayor burbuja financiera de la historia.

El periódico, web, 28/11/2017

Bitcoin y blockchain

El BCE advierte de que el bitcoin “no es una moneda”, sino “un instrumento de especulación”.

Expansión, web, 22/09/2017

Bitcoin y blockchain

El precio del bitcoin es cercano a cero. (Kenneth Rogoff, profesor en la Universidad de Harvard y economista jefe del FMI entre 2001 y 2003)

Su voz anticipa el “colapso” del precio del bitcoin, la estrella de las ciberdivisas, que estos días se cotiza a más de 8000 dólares por unidad.

El País, 16/11/2017

Bitcoin y blockchain

En 2020 el consumo eléctrico del Bitcoin igualaría al de todos los países del planeta.

Cinco días, web, 24/11/2017

Bitcoin y blockchain

Bitcoin es una moneda electrónica creada en 2009 por un programador cuyo pseudonimo es Sathosi Nakamoto.

Las operaciones con esta moneda se realizan entre usuarios, sin que exista la intermediación de ningún organismo o banco.

El valor del bitcoin se determina por la oferta y la demanda.

Bitcoin y blockchain

¿Cómo funciona?

Para usar bitcoins debes instalar un monedero en un ordenador, teléfono móvil o Tablet.

Entonces se genera tu primera dirección bitcoin con la que podrás pagar o recibir bitcoins.

Cada dirección bitcoin solo deberá ser usada en una transacción.

Bitcoin y blockchain

- Si quieres pagar o realizar un traspaso de bitcoins, deberás utilizar tu dirección.
- Si quieres recibir un pago o traspaso, deberás darles tu dirección bitcoin.

Bitcoin y blockchain

El monedero bitcoin cuenta con una contraseña que será utilizada cuando se realice una transacción.

Bitcoin y blockchain

Todas las transacciones que se realizan son verificadas por la comunidad en unos 10 minutos.

Se puede pagar una comisión para reducir el tiempo de espera.

Estas comisiones también permiten evitar que usuarios malintencionados bloqueen el sistema con la realización masiva de transacciones.

Bitcoin y blockchain

Las cadenas de bloques son un registro público de todas las operaciones en bitcoins.

Todo el mundo puede ver las transacciones, conocer la dirección bitcoin de la operación pero no las identidades de los intervinientes, que vienen protegidas por la contraseña.

Bitcoin y blockchain

Una vez realizadas las comprobaciones, las operaciones son incluidas como bloques en unas bases de datos (sellado), las conocidas como cadenas de bloques (blockchain)

Bitcoin y blockchain

El proceso anterior requiere de la realización de una serie cálculos matemáticos que permitan:

1. Verificar que la operación es correcta.

2. Añadir de forma correcta el nuevo bloque a la cadena de bloques para que ningún bloque incorporado a esta pueda ser modificado.

Para lo anterior se utilizan herramientas criptográficas.

Bitcoin y blockchain

El proceso anterior se conoce como minería, los mineros (sus ordenadores) se encargan de realizar todo el proceso anterior a cambio de comisiones en bitcoins.

Sin embargo, existe una competencia a la hora de realizar los cálculos, el que primero lo logra recibe la comisión.

Bitcoin y blockchain

Cualquiera puede ser minero, simplemente instalamos un programa y tu ordenador empieza a realizar todos los cálculos sin que tengas que hacer nada, solo dejarlo enchufado.

Bitcoin y blockchain

Sin embargo, actualmente esto no es rentable, solo reporta pequeñas cantidades de beneficio, ya que existen empresas dedicadas a ello, con miles de ordenadores dedicados a este trabajo.

Competir con esto es imposible.

Bitcoin y blockchain

El blockchain surgió como parte del Bitcoin.

Esta es una tecnología que aporta muchas ventajas relativas a seguridad, autenticidad, etcétera, lo que está haciendo que el Blockchain empiece a utilizarse fuera del bitcoin.

¿Sobrevivirán los notarios al desarrollo del Blockchain?

El notariado europeo ha iniciado una discusión pública sobre los efectos de la aplicación de la cada de bloques a su actividad. El colectivo cree que, a corto plazo, esta tecnología no cambiará su modelo.

Diario Expansión, 21/11/2017

Bitcoin y blockchain

Las matemáticas son claves en el Blockchain.

Bitcoin y blockchain

Las entradas de la base de datos pueden verse como matrices.

Bitcoin y blockchain

El blockchain utiliza herramientas criptográficas, que son matemáticas.

Criptografía: Arte de escribir con clave secreta o de un modo enigmático. (RAE)

CIFRADO CESAR

FM UFTPSP FTUB EFCBKP EF MB DBNB

EL TESORO ESTÁ DEBAJO DE LA CAMA

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

Bitcoin y blockchain

MÁQUINA ENIGMA, usada por los alemanes en la segunda guerra mundial.

Se dice que el descifrado de la máquina ENIGMA por el ejercito aliado adelantó dos años el fin de la guerra.

Bitcoin y blockchain

La criptografía se basa en problemas matemáticos fáciles de resolver en un sentido, pero difíciles en el otro.

Bitcoin y blockchain

p, q números primos grandes con ciertas propiedades.

Fácil calcular p*q.

Difícil calcular p y q a partir de p*q.

Base del algoritmo criptográfico RSA.

Bitcoin y blockchain

RSA es uno de los algoritmos criptográficos más importantes.

Fue desarrollado por Ron River, Adi Shamir y Leonard Adleman.

Bitcoin y blockchain

Logaritmo discreto:

En un cuerpo finito GF(q), si a, b\in GF(q)* tal que a^n=b, entonces:

$$Log\_a(b)=n$$

Bitcoin y blockchain

El logaritmo discreto puede introducirse en cualquier grupo.

Bitcoin y blockchain

El logaritmo discreto se usa en criptografía:

- Algoritmo de Diffie-Hellman para intercambio de claves privadas.
- Cifrado Elgammal. (libre, sin patente)

Bitcoin y blockchain

Blockchain utiliza un algoritmo basado en curvas elípticas.

La ventaja sobre el logaritmo discreto es que las claves pueden ser más cortas obteniendo el mismo nivel de seguridad.

- Una curva elíptica es conjunto de puntos (x,y) que satisfacen la ecuación:

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

para ciertos valores constantes a y b, junto con un punto O que se llama punto del infinito.

- Una curva elíptica es conjunto de puntos (x,y) que satisfacen la ecuación:

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

para ciertos valores constantes a y b, junto con un punto O que se llama punto del infinito.

- La curva elíptica usada para blockchain es aquella que se obtiene para $a = 0$ y $b = 7$:

- Una curva elíptica es conjunto de puntos (x,y) que satisfacen la ecuación:

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

para ciertos valores constantes a y b, junto con un punto O que se llama punto del infinito.

- La curva elíptica usada para blockchain es aquella que se obtiene para $a = 0$ y $b = 7$:

$$y^2 = x^3 + 7.$$

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

- Podemos obtener puntos de esta curva dando valores a x, calculando los valores de y correspondientes.

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

- Podemos obtener puntos de esta curva dando valores a x, calculando los valores de y correspondientes.

$x = 0$

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

- Podemos obtener puntos de esta curva dando valores a x, calculando los valores de y correspondientes.

$x = 0$ ➡ $y^2 = 0 + 7$

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

- Podemos obtener puntos de esta curva dando valores a x, calculando los valores de y correspondientes.

$$x = 0 \Rightarrow y^2 = 0 + 7 \Rightarrow y^2 = 7$$

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

- Podemos obtener puntos de esta curva dando valores a x, calculando los valores de y correspondientes.

$$x = 0 \Rightarrow y^2 = 0 + 7 \Rightarrow y^2 = 7 \Rightarrow y = \pm\sqrt{7}.$$

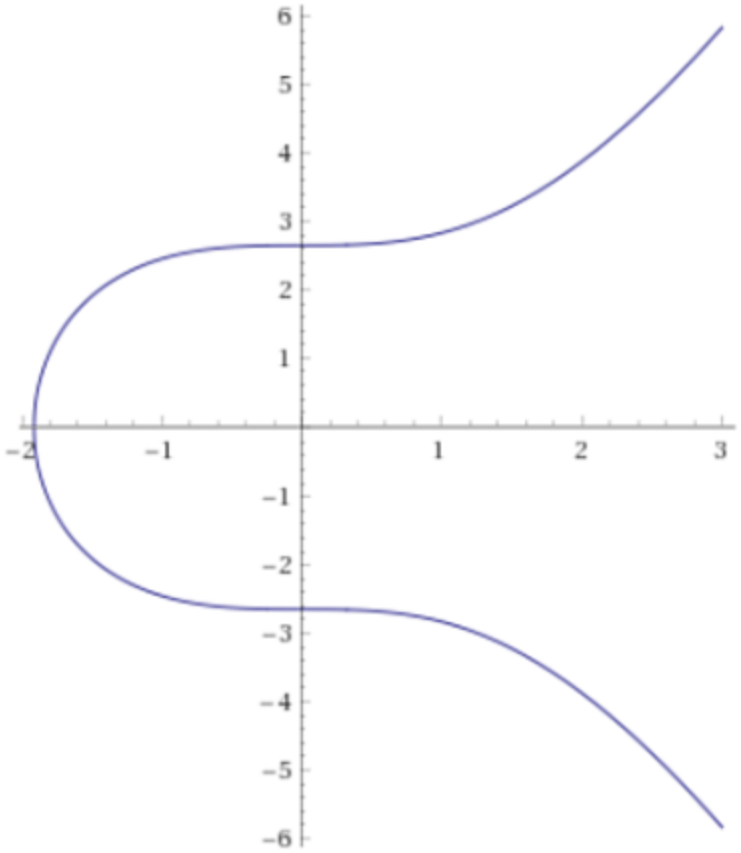
$$y^2 = x^3 + 7$$

- Podemos obtener puntos de esta curva dando valores a x, calculando los valores de y correspondientes.

$x = 0$ ➡ $y^2 = 0 + 7$ ➡ $y^2 = 7$ ➡ $y = \pm\sqrt{7}$.

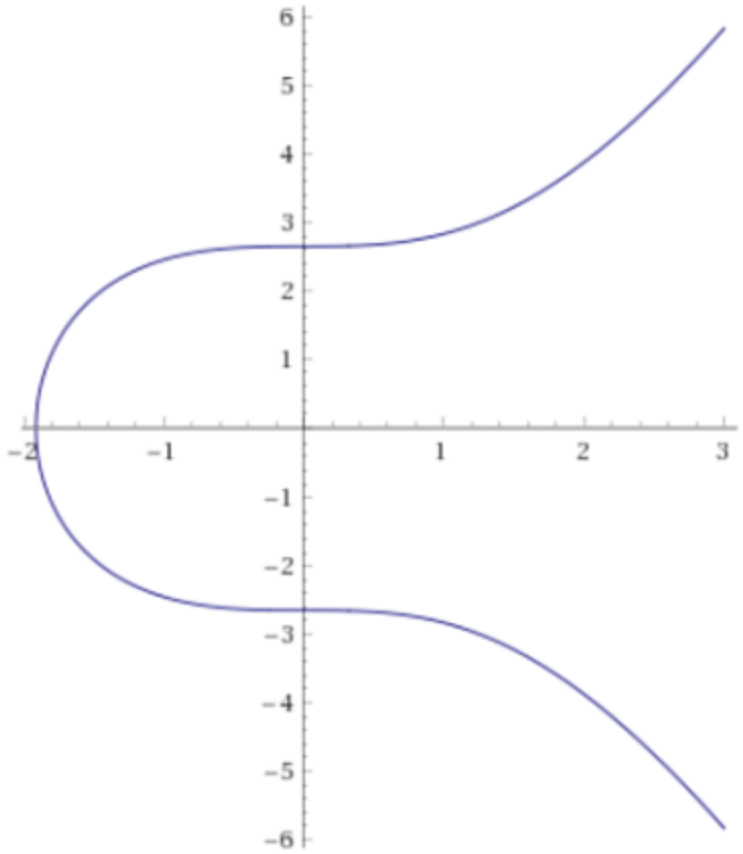
Obtenemos los puntos $(0, \sqrt{7})$ y $(0, -\sqrt{7})$.

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



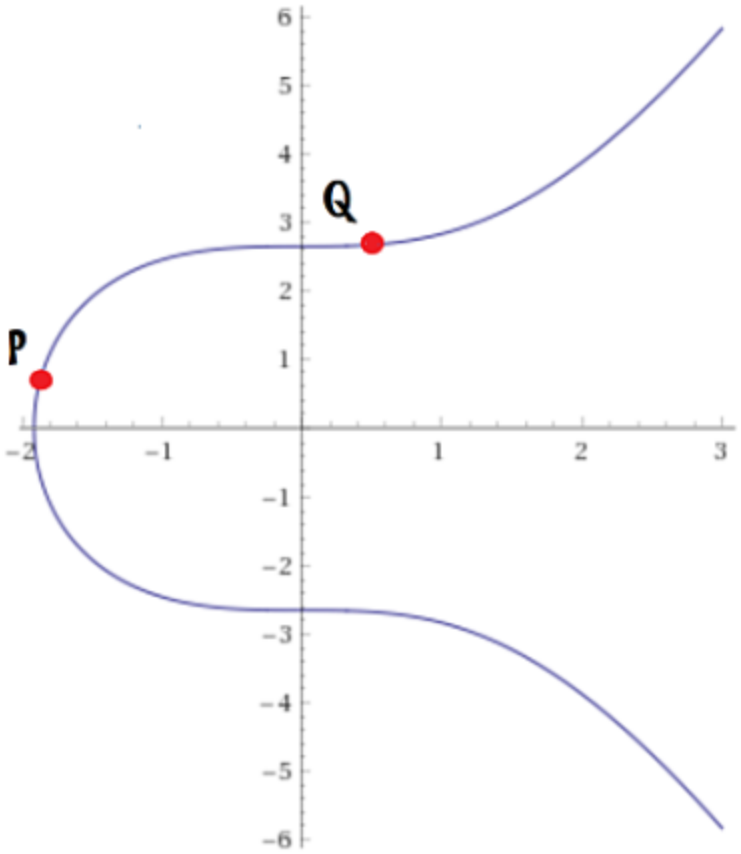
$$y^2 = x^3 + 7$$

- Suma en una curva elíptica:



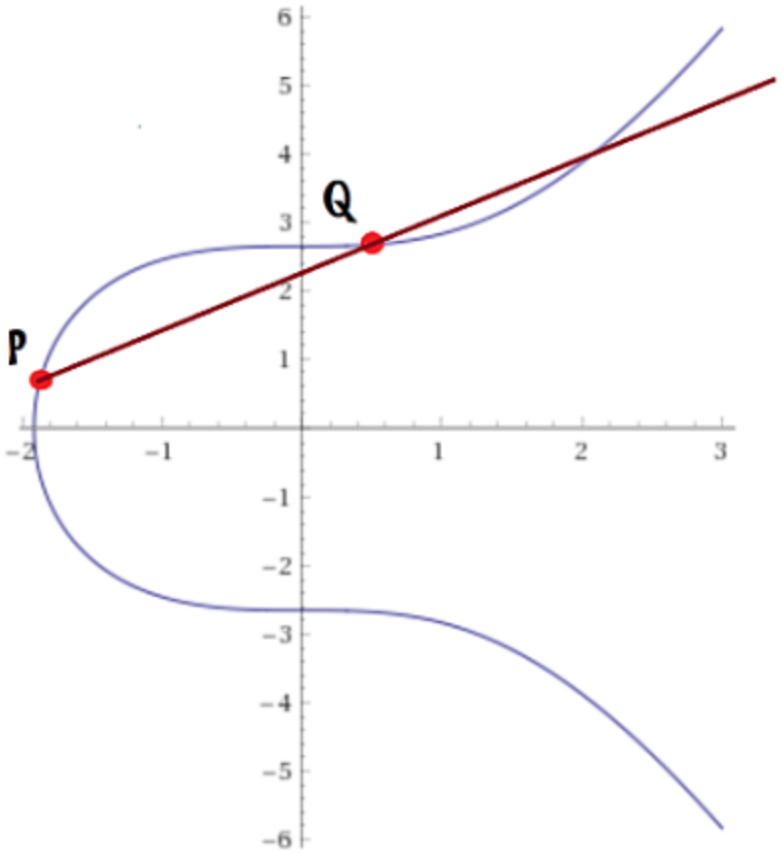
$$y^2 = x^3 + 7$$

- Suma en una curva elíptica:



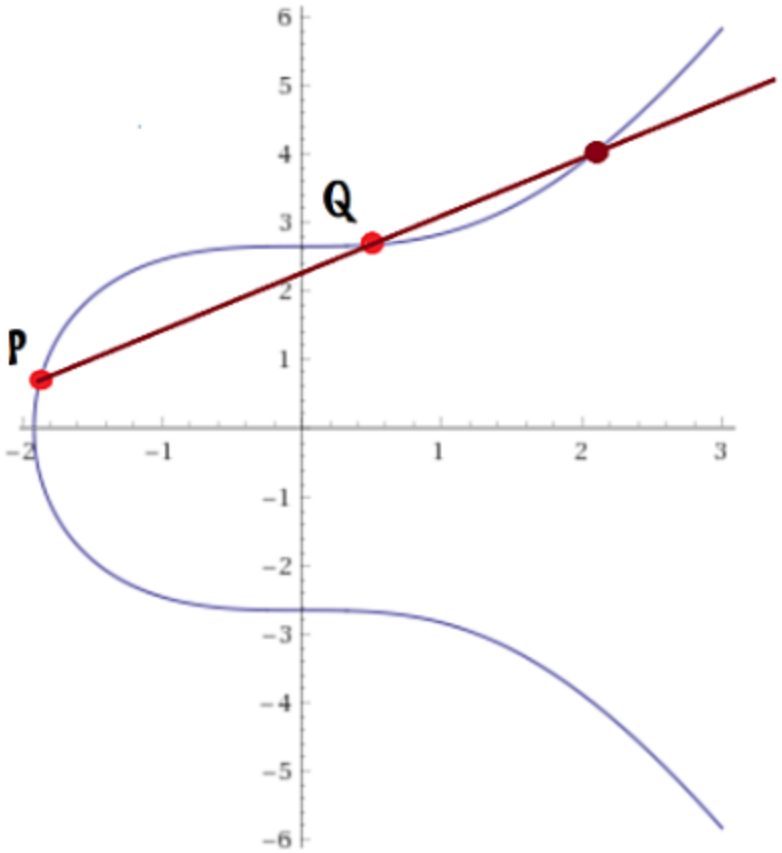
$$y^2 = x^3 + 7$$

- Suma en una curva elíptica:



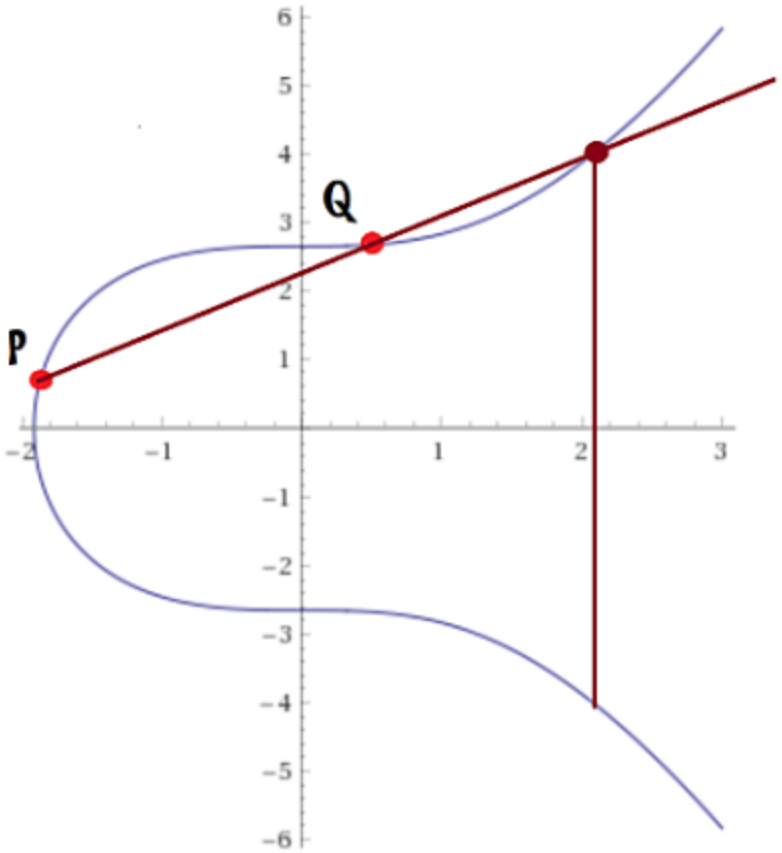
$$y^2 = x^3 + 7$$

- Suma en una curva elíptica:



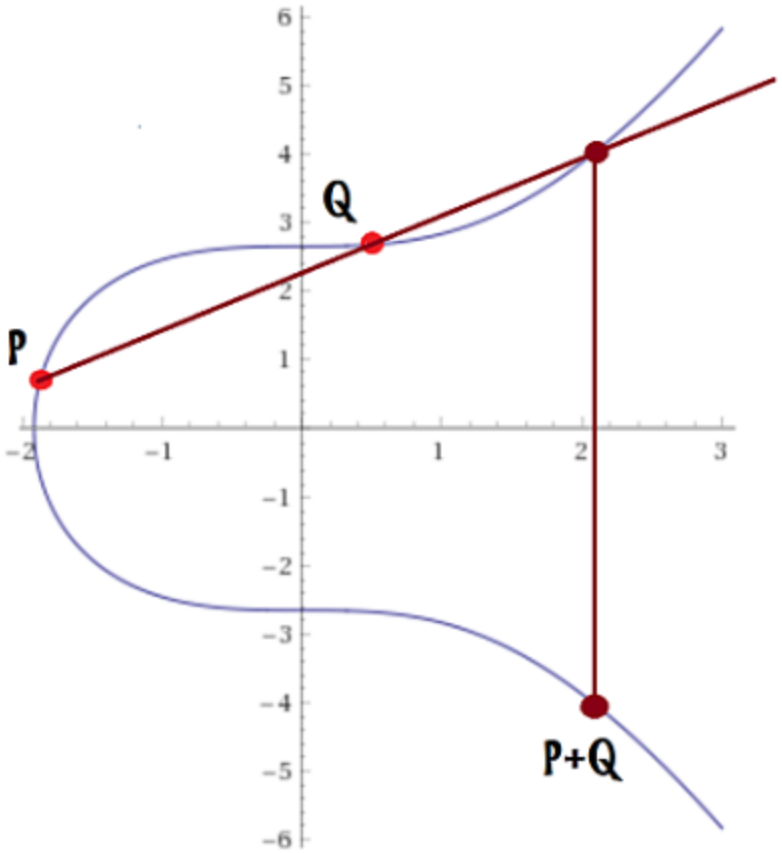
$$y^2 = x^3 + 7$$

- Suma en una curva elíptica:



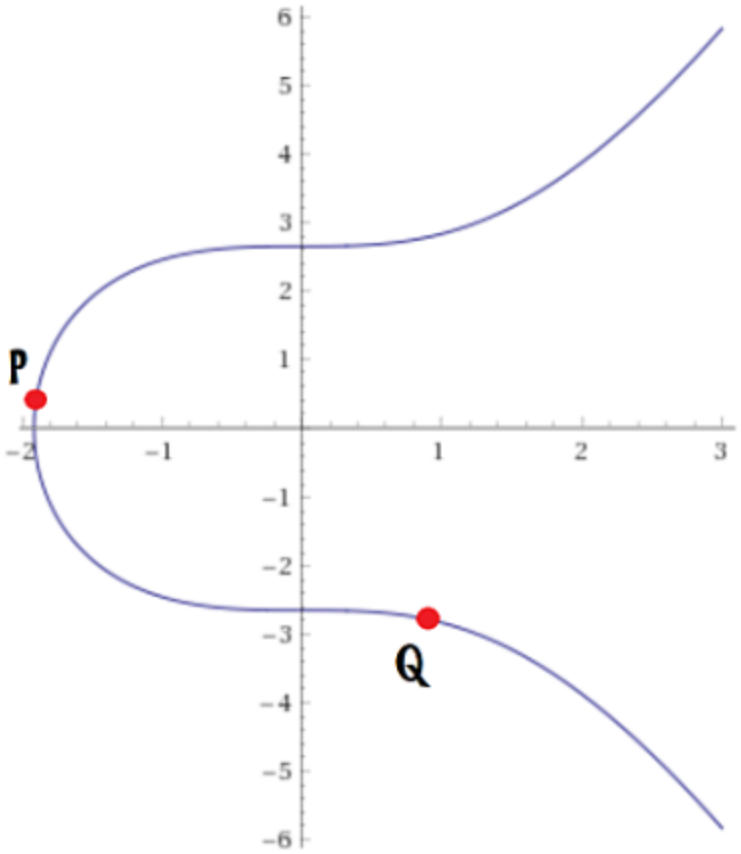
$$y^2 = x^3 + 7$$

- Suma en una curva elíptica:



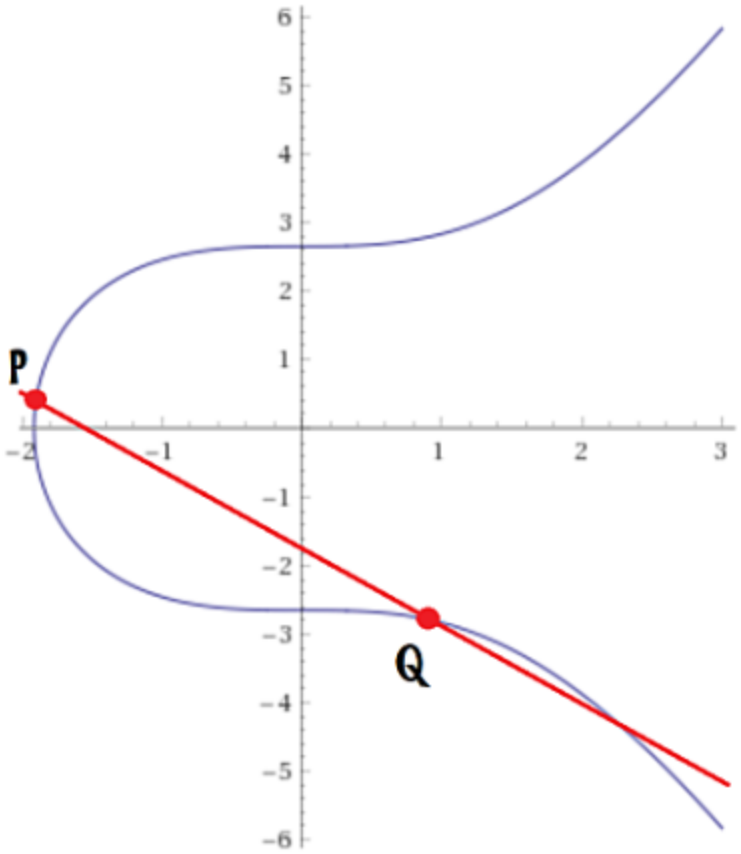
$$y^2 = x^3 + 7$$

- Suma en una curva elíptica:



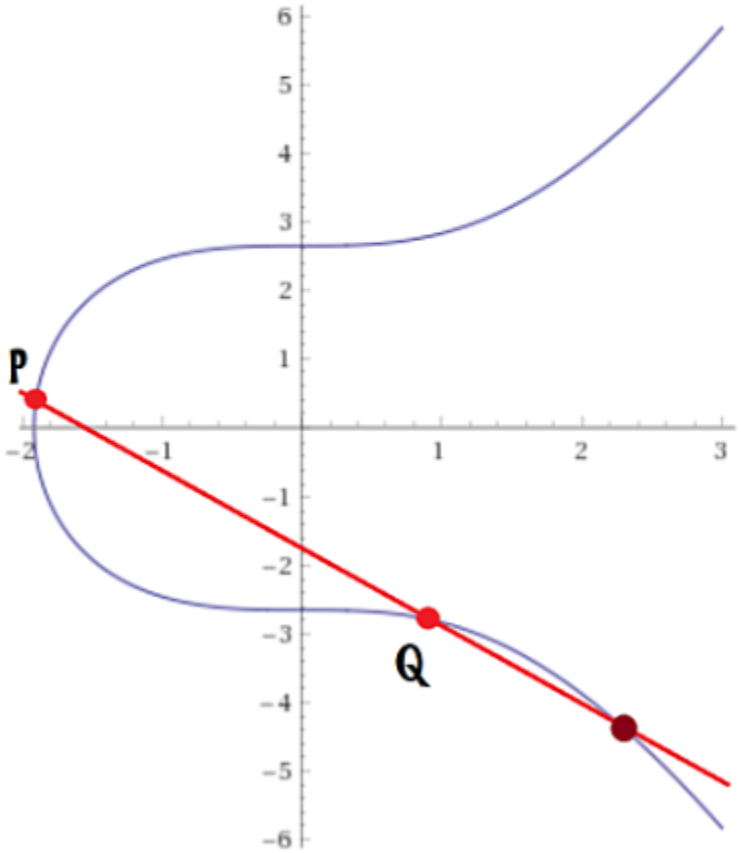
$$y^2 = x^3 + 7$$

- Suma en una curva elíptica:



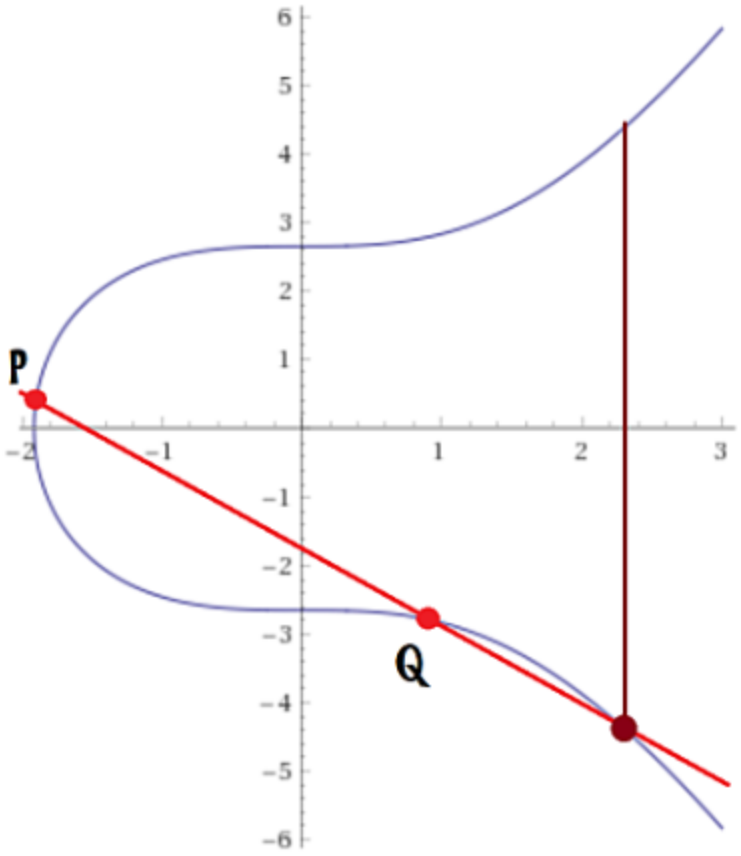
$$y^2 = x^3 + 7$$

- Suma en una curva elíptica:



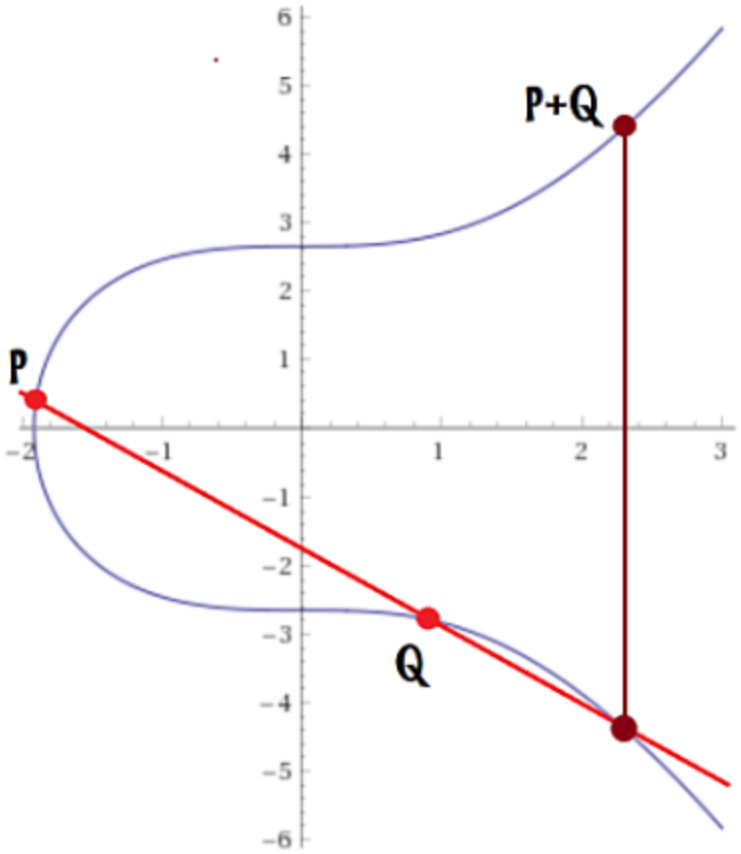
$$y^2 = x^3 + 7$$

- Suma en una curva elíptica:



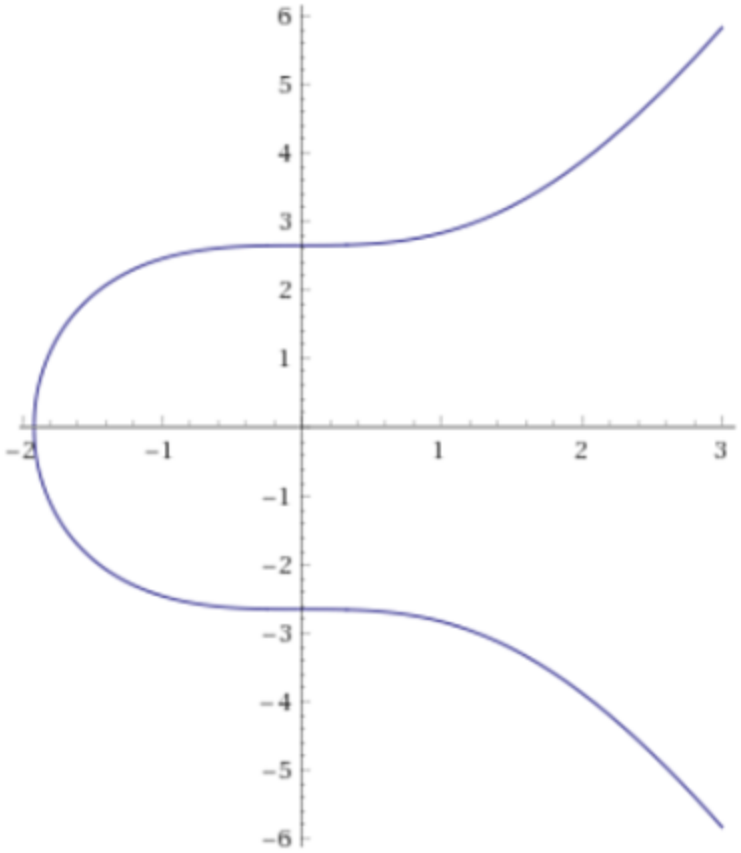
$$y^2 = x^3 + 7$$

- Suma en una curva elíptica:



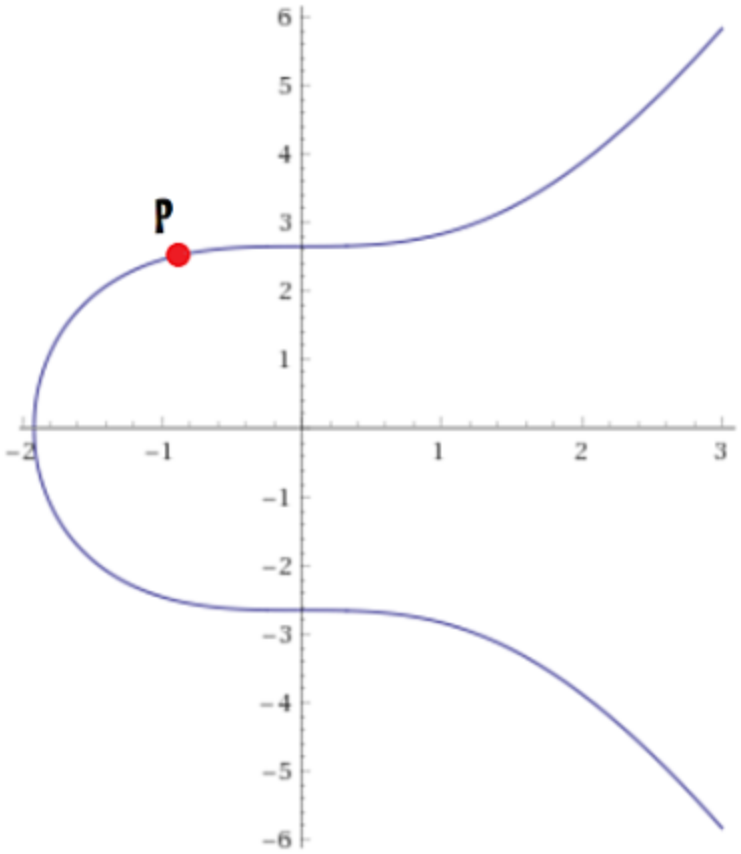
$$y^2 = x^3 + 7$$

- Doble de un punto en una curva elíptica:



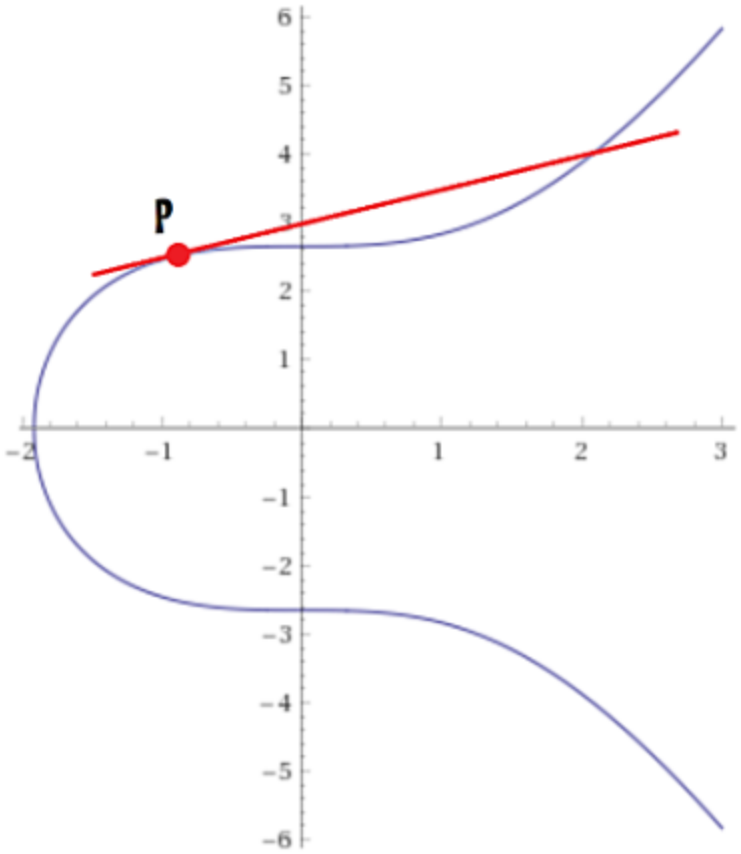
$$y^2 = x^3 + 7$$

- Doble de un punto en una curva elíptica:



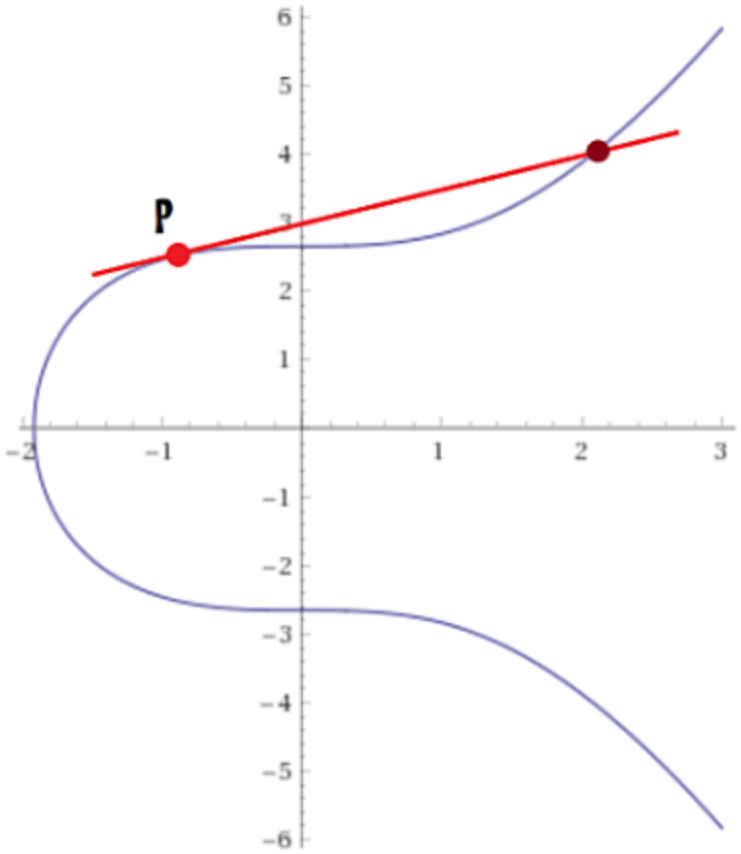
$$y^2 = x^3 + 7$$

- Doble de un punto en una curva elíptica:



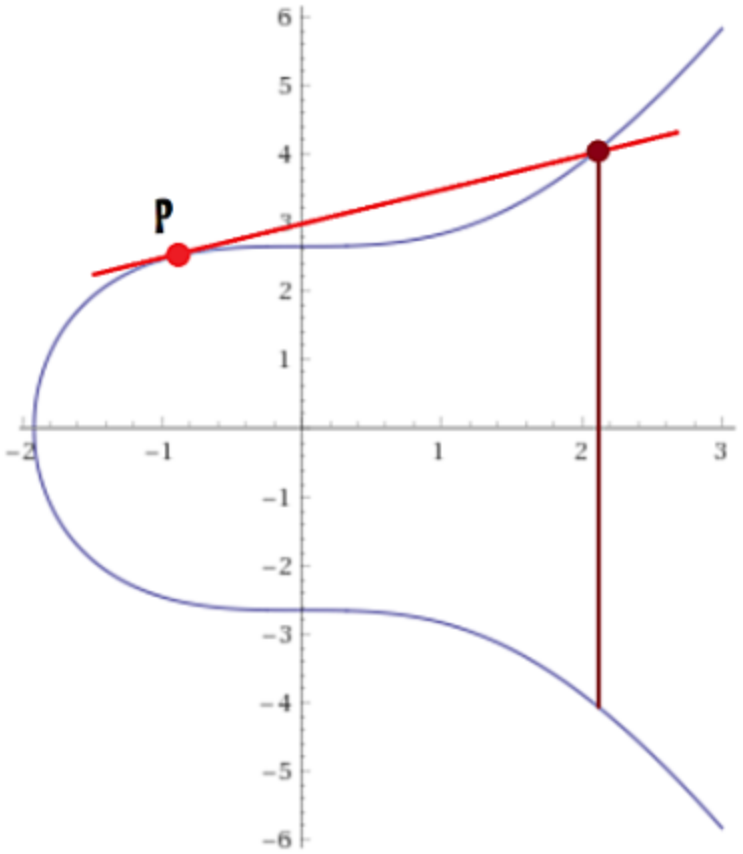
$$y^2 = x^3 + 7$$

- Doble de un punto en una curva elíptica:



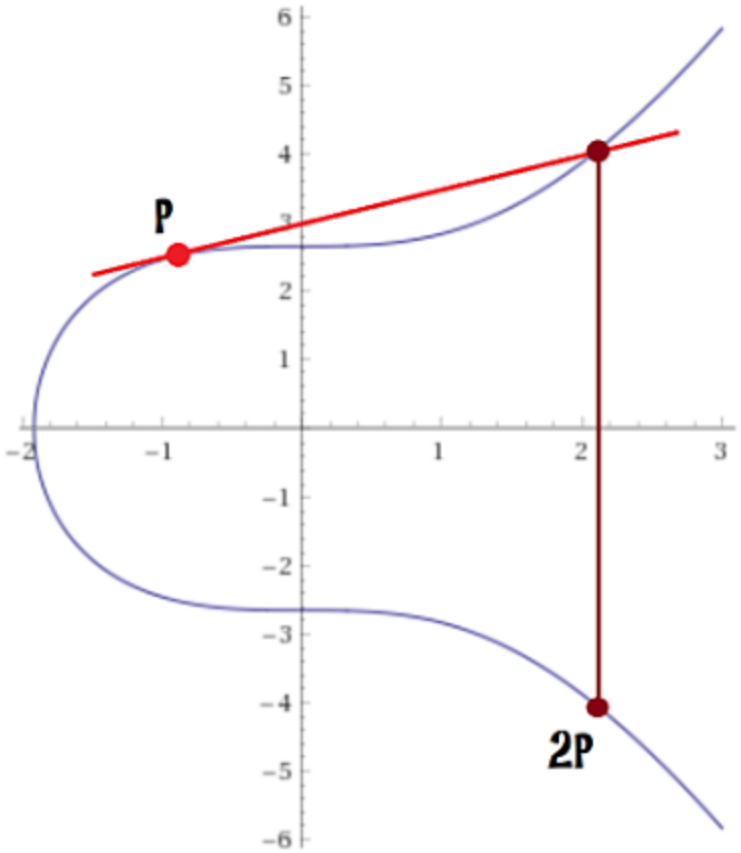
$$y^2 = x^3 + 7$$

- Doble de un punto en una curva elíptica:

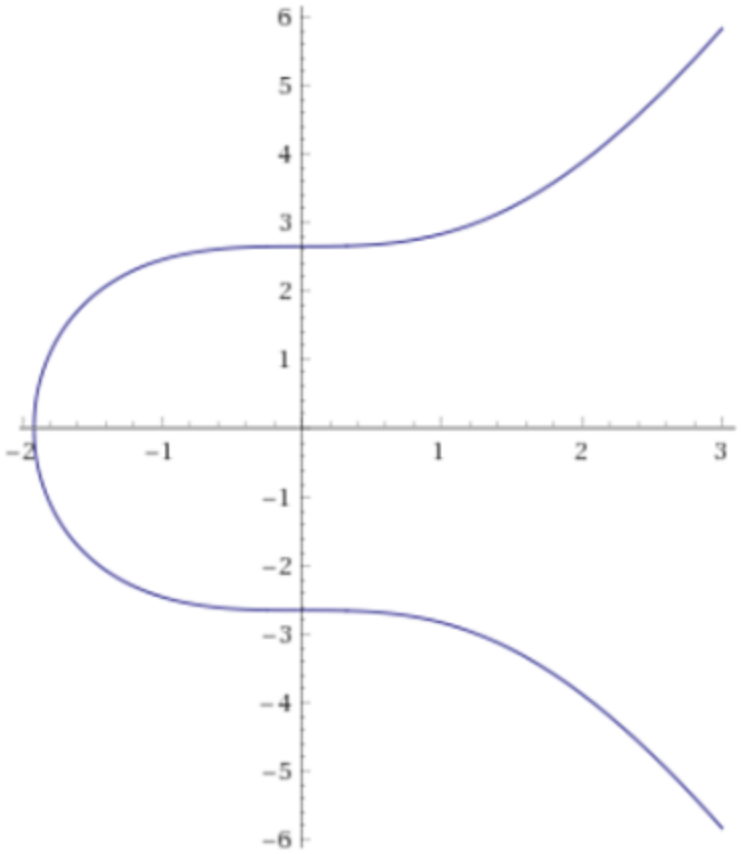


$$y^2 = x^3 + 7$$

- Doble de un punto en una curva elíptica:



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



- Se cumple el conjunto de puntos de una curva elíptica con la suma satisface la propiedad conmutativa, asociativa, existencia de elemento neutro, que es O, y existencia de elemento simétrico, luego estamos ante un grupo abeliano.

Bitcoin y blockchain

Se obtienen expresiones para la operación suma y múltiplo de un punto.

En el caso de una curva elíptica sobre un cuerpo finito, se utilizan estas expresiones para definir las operaciones en esta.

Bitcoin y blockchain

La criptografía en una curva elíptica se basa en el uso del logaritmo discreto en el grupo de los puntos de esta.

Bitcoin y blockchain

La ventaja principal de la criptografía sobre curvas elípticas frente a otras, es que se pueden utilizar claves de menor longitud obteniendo los mismo niveles de seguridad.

En criptografía para curvas elípticas trabajamos en un cuerpo finito $\mathbb{F}_p$.

En el caso del Blockchain:

$$y^2 = x^3 + 7 \quad \text{mod.} p$$

para $p = 115792089210356248762697446949407573530086143415290314195533631308867097853951$.

Se toma este número primo por varias razones:

1. Tiene un tamaño adecuado, 256 bits.
2. Se facilitan los cálculos con este dado que tiene 127 ceros y 129 unos.

Conocimiento previos

Conocimientos básicos para llegar a la criptografía del Blockchain.

1. Repaso de divisibilidad.

2. Algoritmo euclídeo para el cálculo del **mcd**.

Si a, b son enteros positivos con $a > b$, entonces $\mathbf{mcd}(a, b) = \mathbf{mcd}(b, r)$ donde r es el resto de $a : b$.

3. Identidad de Bezout. (Para el cálculo del inverso)

Si $d = \mathbf{mcd}(a, b)$, existen enteros x e y tales que $d = ax + by$.

Algoritmo euclídeo para el cálculo de x e y.

4. Aritmética modular.

5. Repaso de los conceptos de grupo, anillo y cuerpo.

6. El cuerpo $\mathbb{F}_p$. Operaciones e inverso.

7. Potencias. Pequeño teorema de Fermat.

8. Criptosistemas básicos: Traslaciones, funciones afines y matrices.

9. RSA. (Opcional)

10. Logaritmo discreto.

11. Curvas elípticas sobre cuerpos finitos: Cálculo de puntos, subgrupos cíclicos, logaritmo discreto en curvas elípiticas.

Bibliografía

1. Koblitz, Neal: A Course in Number Theory and Cryptography, Springer.

2. Silverman, Joseph H.: A Friendly Introduction to Number Theory, Pearson Education, Inc.

¡¡GRACIAS POR VUESTRA ATENCIÓN!!