Seminario

Elliptic Curve Cryptography -ECC

MM3023 Teoría de Números

Criptografía moderna

Criptografía moderna

La criptografía moderna se basa en la idea de que la clave que se utiliza para cifrar los datos puede hacerse pública, mientras que la clave que se utiliza para descifrar los datos puede mantenerse en privado. Por ello, estos sistemas se conocen como **sistemas criptográficos de clave pública**.

Lo que se necesita para que un sistema criptográfico de clave pública funcione es un conjunto de algoritmos que sea fácil de procesar en una dirección, pero difícil de deshacer.

Criptografía moderna

El sistema criptográfico RSA basa su seguridad en que la factorización es lenta y la multiplicación rápida.

A medida que aumentan los recursos computacionales disponibles, el tamaño de las claves tiene que crecer aún más rápido.

Esta no es una situación sostenible para los dispositivos móviles y de baja potencia que tienen una capacidad de cálculo limitada; la diferencia entre factorizar y multiplicar no es sostenible a largo plazo.

Curvas elípticas

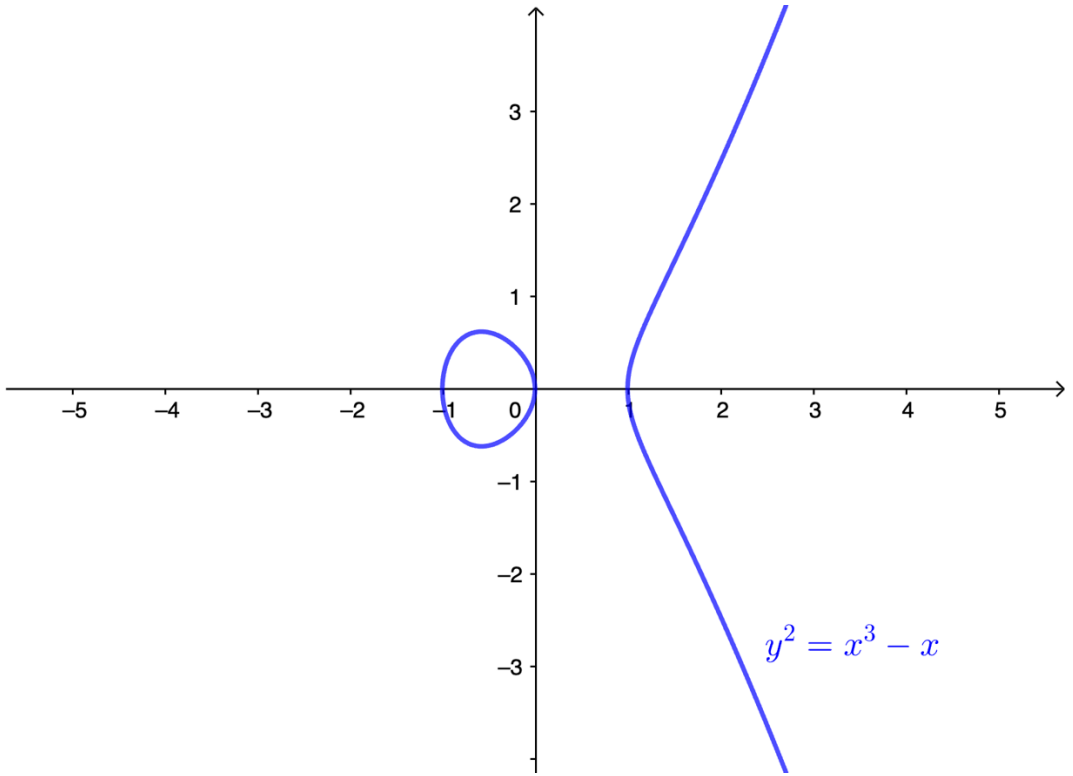
Curva elíptica

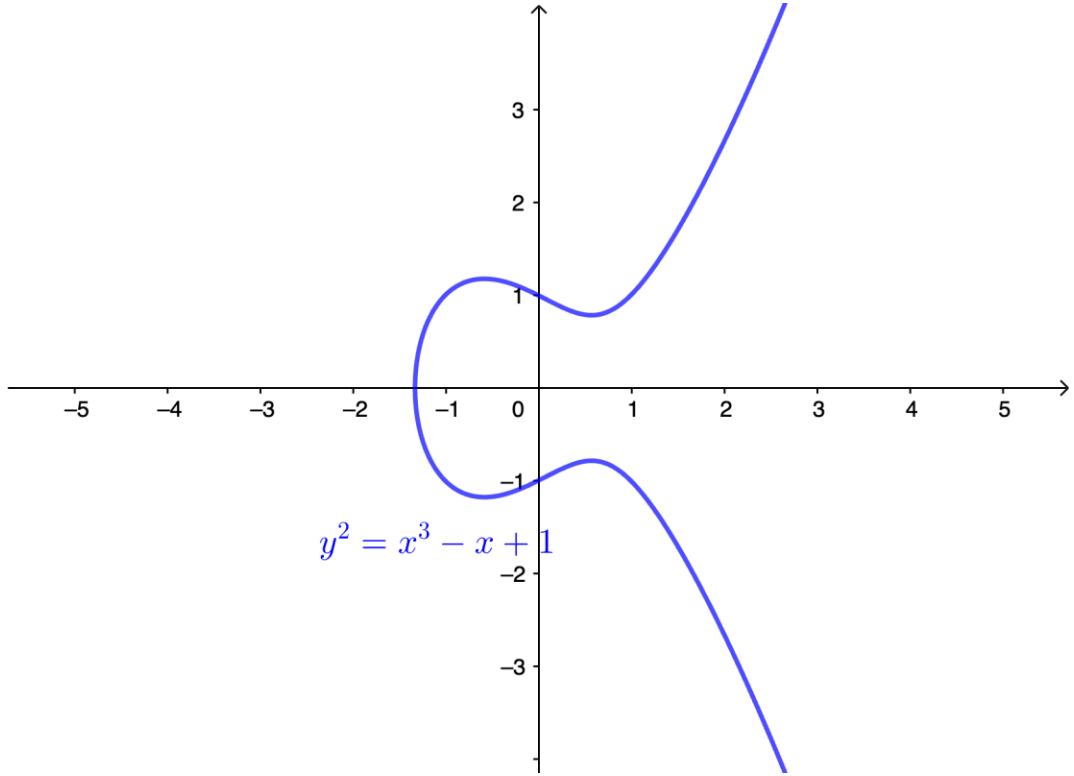
Una curva elíptica sobre un campo K es el conjunto de todos los pares (x, y) que satisfacen una ecuación de la forma:

$$y^2 = x^3 + ax + b, \text{ con } a, b \in K$$

Nota: Se requiere que la curva no sea singular, i.e. que la curva no tenga picos ni se corte a sí misma (esto se consigue si $4a^3 + 27b^2 \neq 0$).

Ejemplo 1

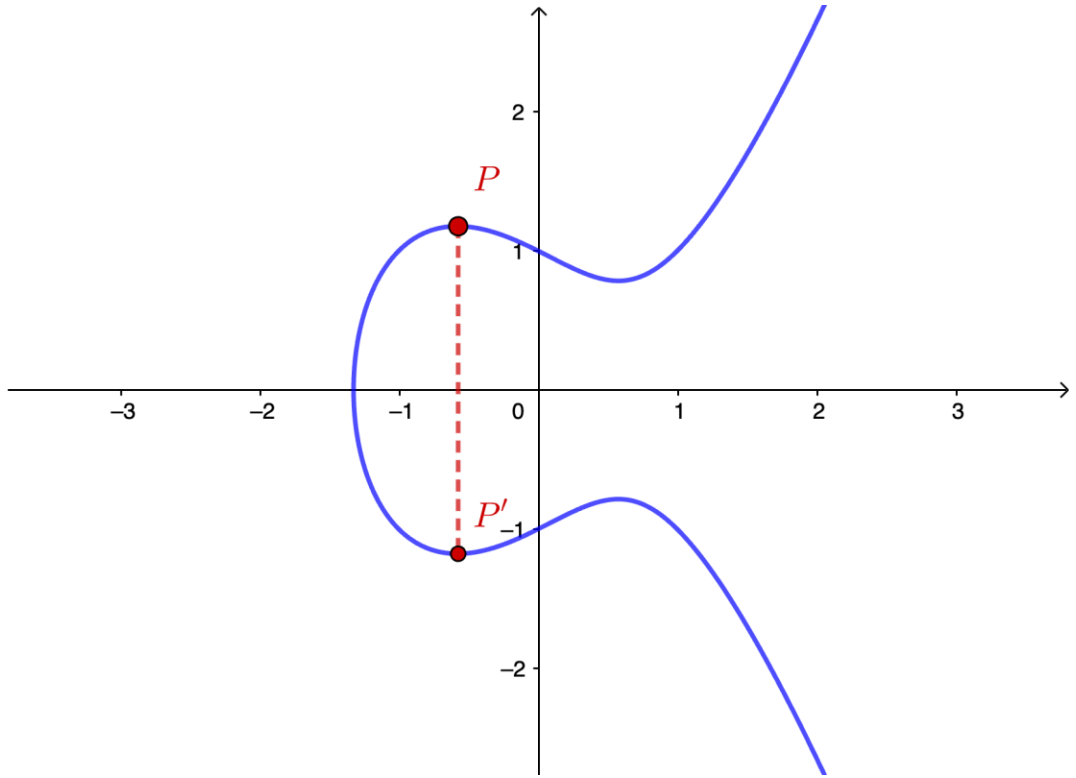




Curvas elípticas

Propiedad 1

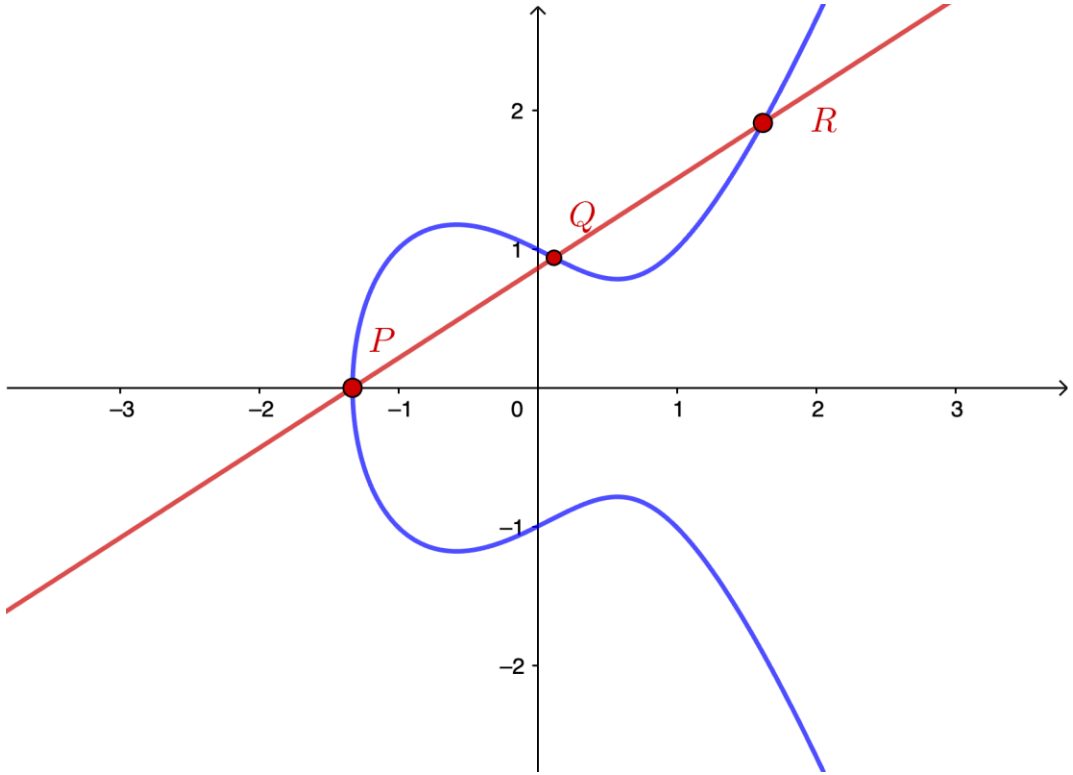
Las curvas elípticas tienen simetría respecto del eje x, es decir, que cualquier punto P sobre la curva se puede reflejar sobre el eje x y sigue estando sobre la curva (punto P').



Curvas elípticas

Propiedad 2

Cualquier línea no vertical intersecará la curva en máximo tres puntos.

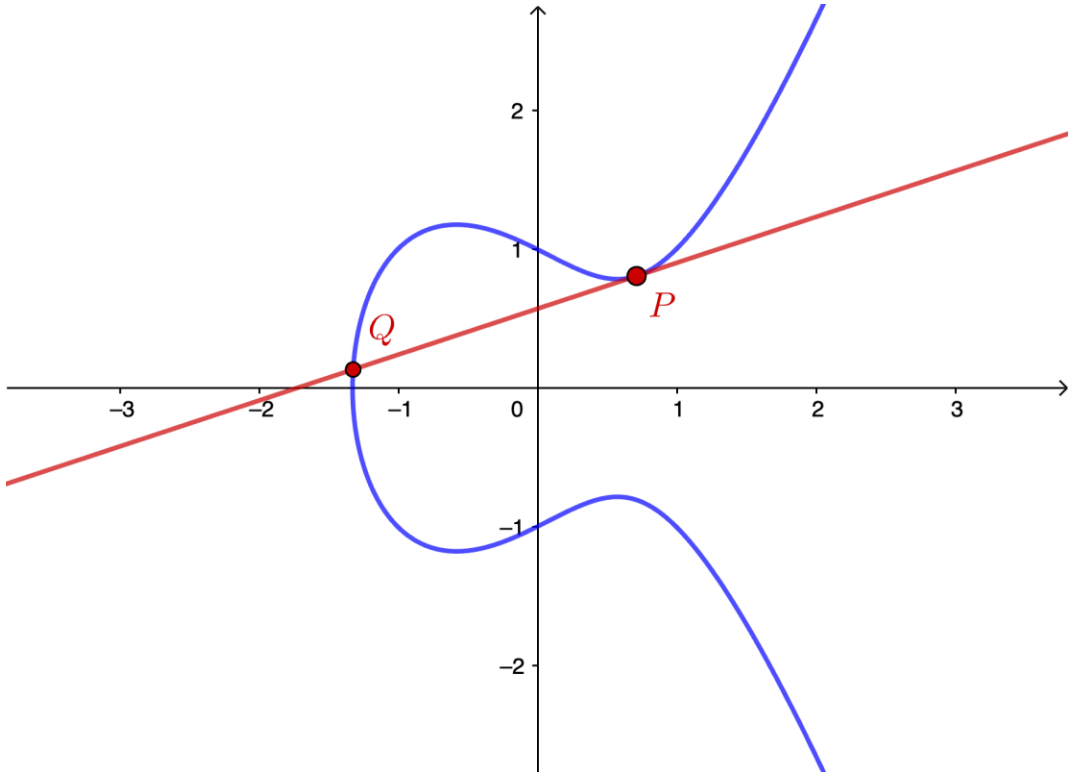


Curvas elípticas

Propiedad 2

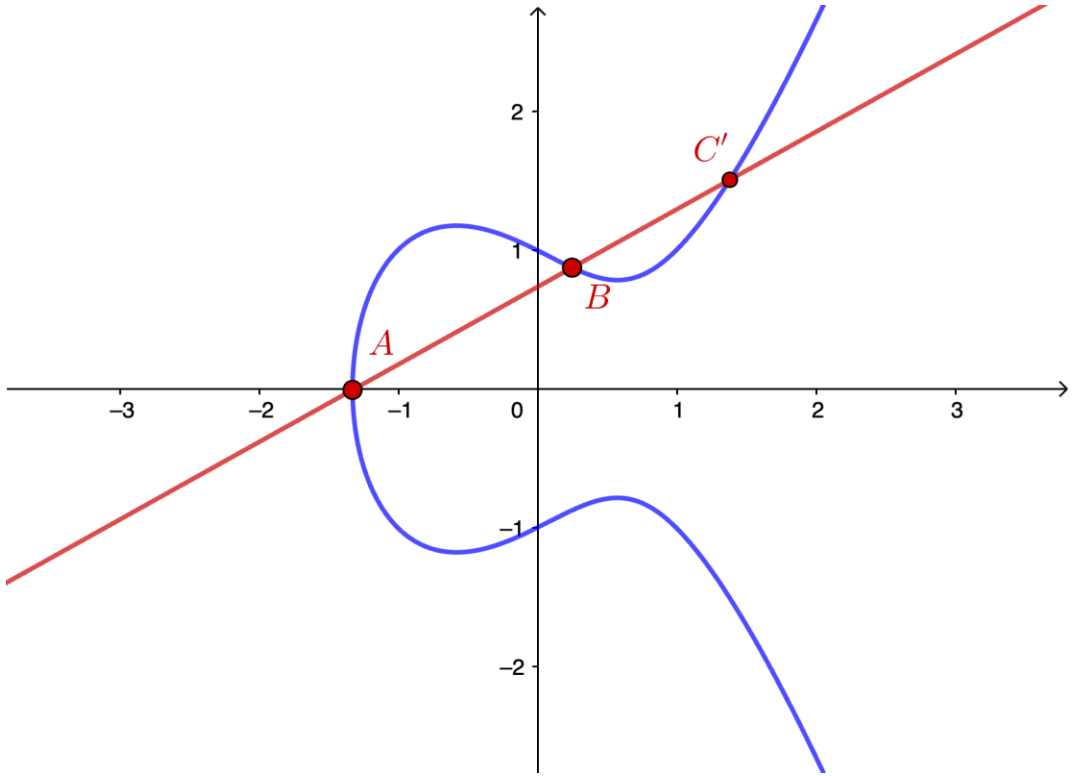
Cualquier línea no vertical intersecará la curva en máximo tres puntos.

En la figura, un ejemplo de un caso en que la intersección se da sólo en dos puntos.



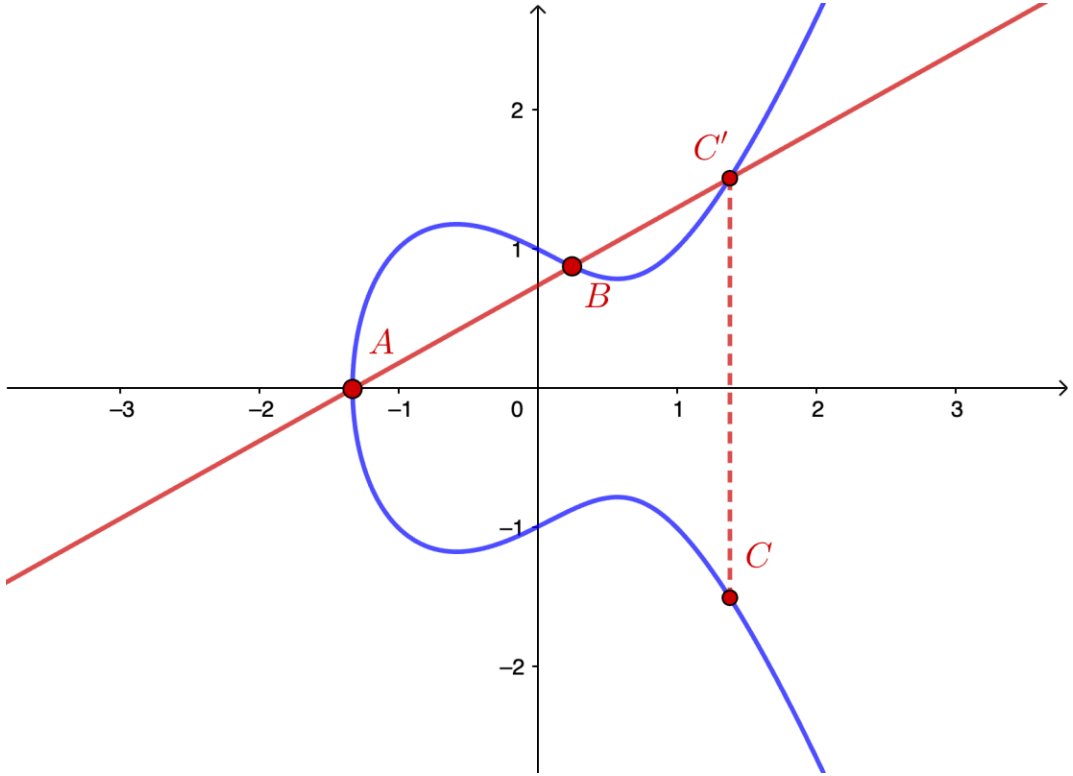
Curvas elípticas

Entonces, dados dos puntos distintos A y B (y con coordenadas x distintas) sobre una curva elíptica, por la Propiedad 2 la recta que une dichos puntos interseca la curva en un tercer punto, a saber, C'.



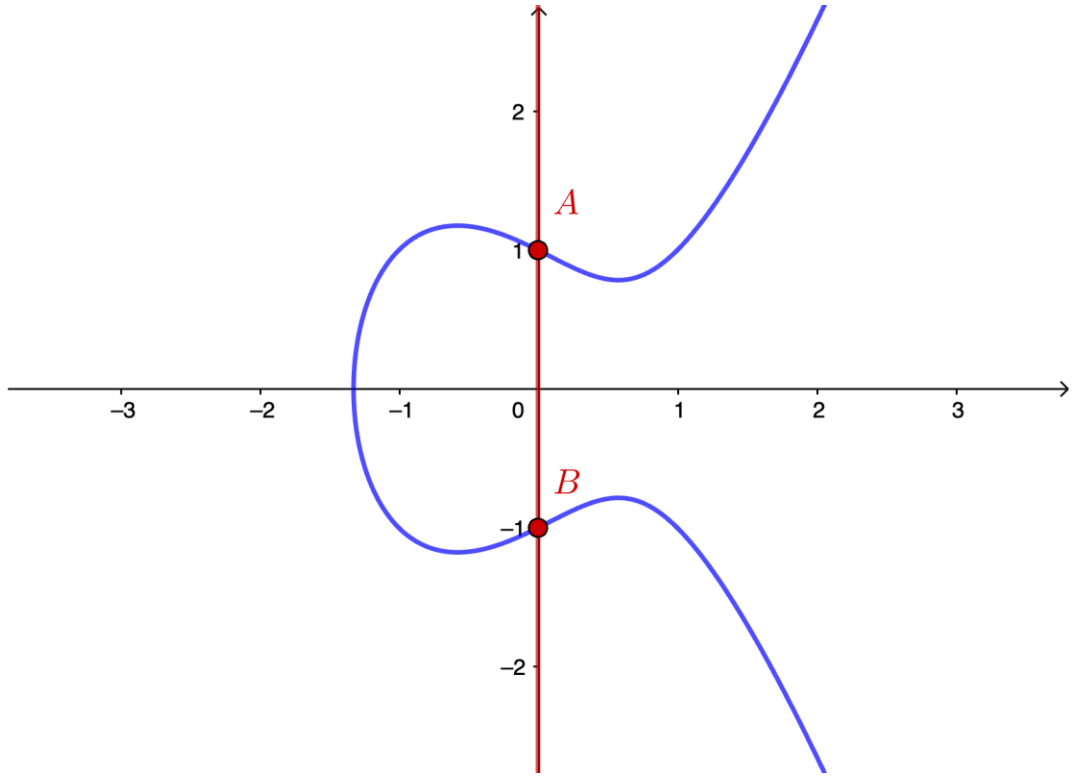
Curvas elípticas

Además, por la Propiedad 1, el punto C, el reflejo sobre el eje x de C', también está sobre la curva.



Curvas elípticas

Si los puntos A y B coinciden en sus coordenadas x, se dice que la recta que los une interseca a la curva en el punto en el infinito O.



Observación

Entonces, dada una curva elíptica:

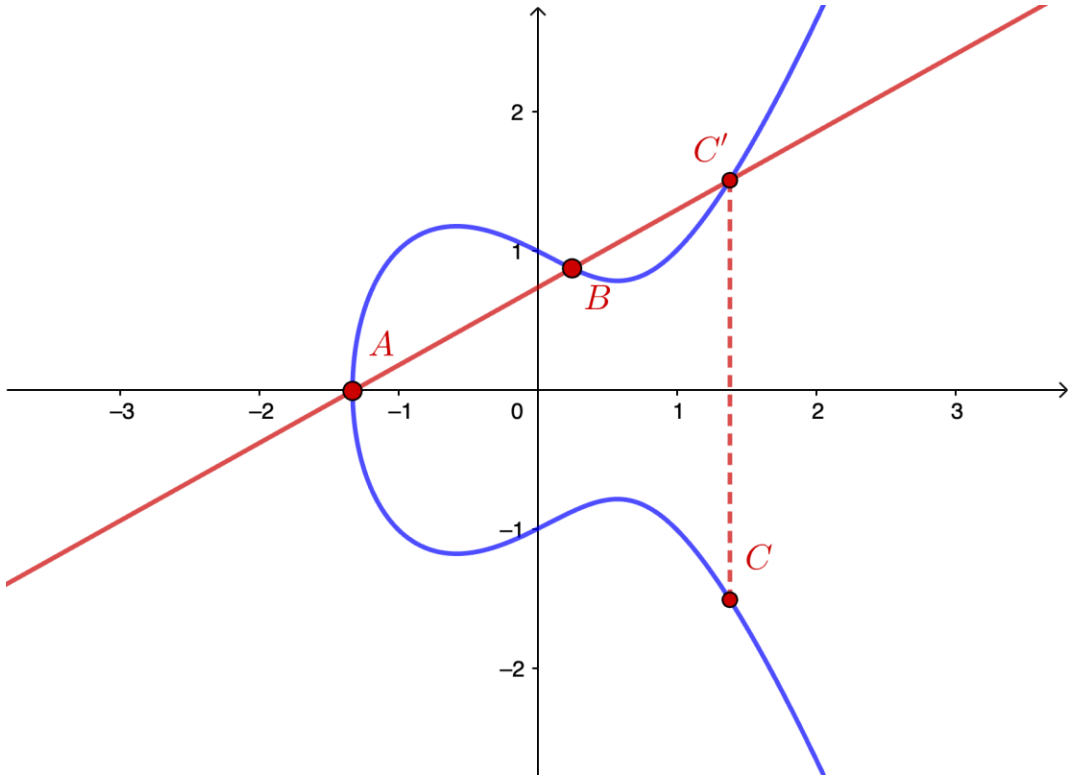
$$\varepsilon: y^2 = x^3 + ax + b$$

se puede definir sobre el conjunto:

$$G = \{(x, y) \in \varepsilon\} \cup \{O\}$$

una operación binaria $\cdot$ como:

$$A \cdot B = C$$



Observación

Entonces, dada una curva elíptica:

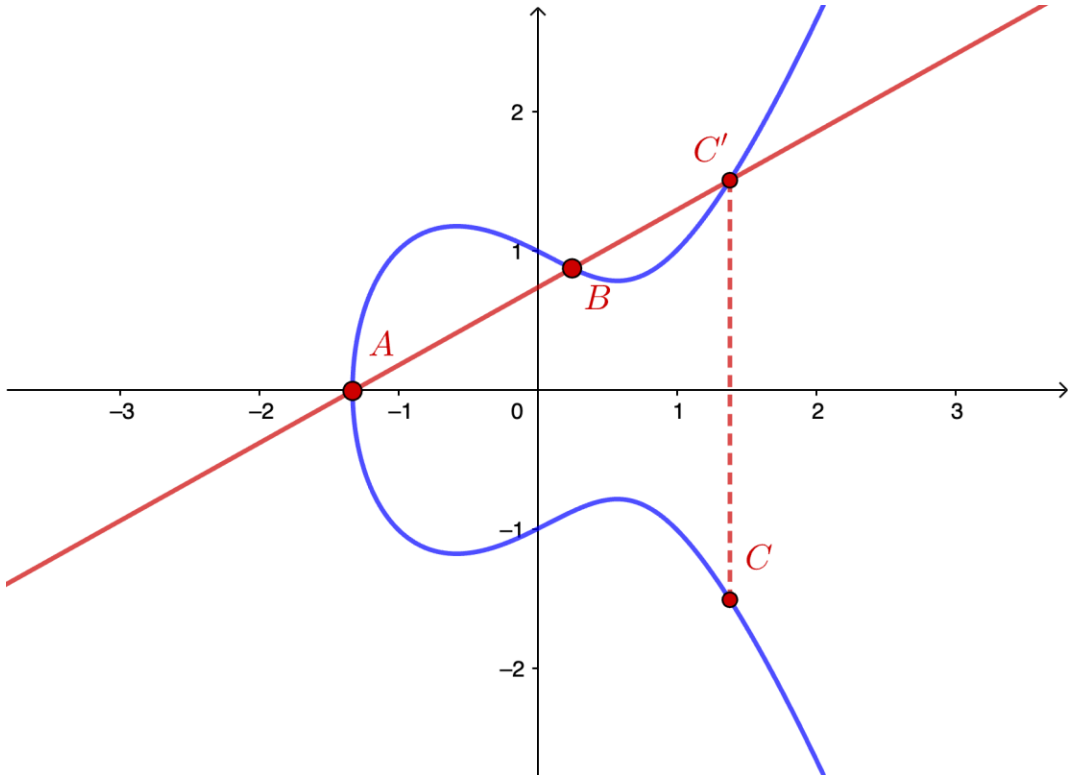
$$E: y^2 = x^3 + ax + b$$

se puede definir sobre el conjunto:

$$G = \{(x, y) \in E\} \cup \{O\}$$

una operación binaria $\cdot: G \times G \to G$ como:

$$A \cdot B = C$$

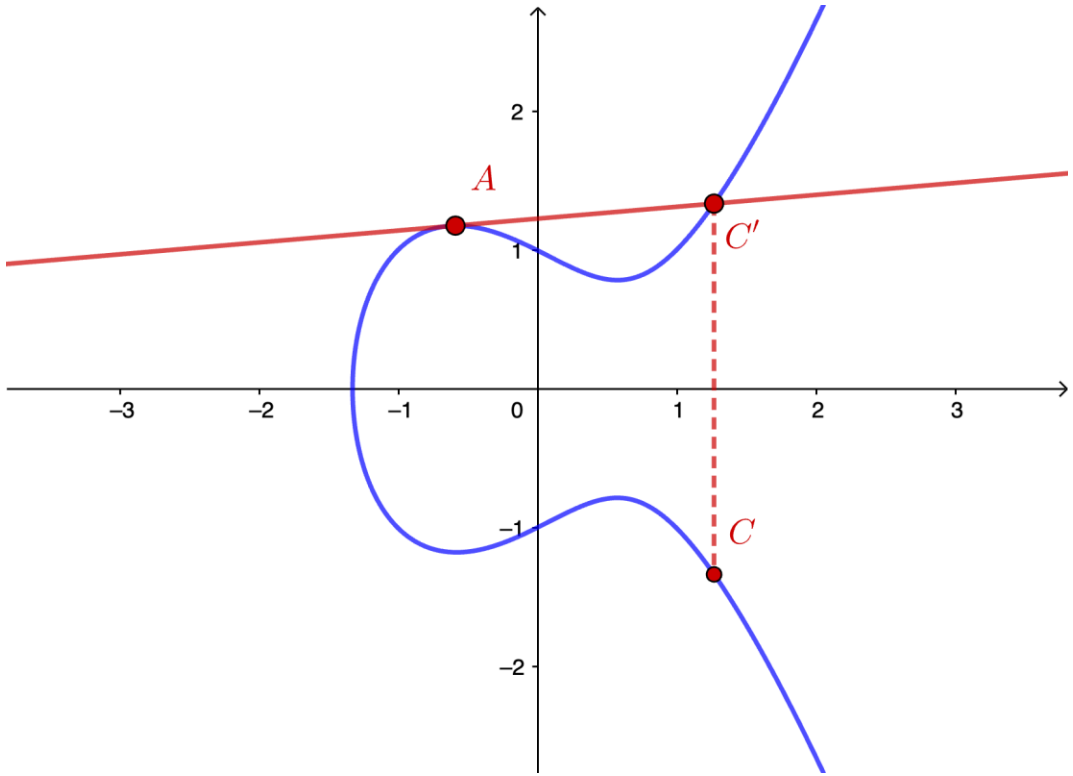


Observación

Si $A = B$, entonces la recta es una recta tangente a la curva y se tiene:

$$A \cdot A = A^2 = C$$

Se puede demostrar que $(G, \cdot)$ es un grupo abeliano.



Campos finitos

Campo finito

Un campo finito (también llamado campo de Galois) es un campo con un orden finito.

Teorema 1 (clasificación de campos finitos)

Para cada primo p y cada entero positivo n, existe un único campo de orden p^n, salvo isomorfismo.

Notas:

- Como sólo hay un campo de orden p^n, éste se representa como:

  $\mathrm{GF}(p^n)$ (o bien $\mathbb{F}_{p^n}$) y se le llama campo de Galois de orden p^n

- Si $n = 1$, $\mathrm{GF}(p) = \mathbb{F}_p = \mathbb{Z}_p$.

Teorema 2 (estructura de $\mathbb{F}_{p^n}$)

Como grupo aditivo, $\mathbb{F}_{p^n} \cong \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n \text{ veces}}$ con la operación en $\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$.

Como grupo multiplicativo, $\mathbb{F}_{p^n}^* \cong \mathbb{Z}_{p^n-1}$ con la suma en $\mathbb{Z}_{p^n-1}$ (y, por lo tanto, es cíclico).

Curvas elípticas sobre campos finitos

Curva elíptica sobre $\mathbb{Z}_p$

Sea $p > 3$. La curva elíptica sobre $\mathbb{Z}_p$, $E: y^2 = x^3 + ax + b$, es el conjunto de soluciones (x, y) de la congruencia:

$$y^2 = x^3 + ax + b \pmod{p},$$

en donde $a, b \in \mathbb{Z}_p$ y $4a^3 + 27b^2 \neq 0 \pmod{p}$.

Curva elíptica sobre $\mathbb{Z}_p$

Sean $E: y^2 = x^3 + ax + b$ una curva elíptica sobre $\mathbb{Z}_p$ y $G = \{(x, y) \in E\} \cup \{O\}$, en donde O es el punto en el infinito.

Si $P = (x_1, y_1), Q = (x_2, y_2) \in E$, se define una operación binaria $\cdot$ sobre G:

- $P \cdot O = O \cdot P = P, \forall P \in E$
- si $x_1 = x_2$ y $y_1 = -y_2$, entonces $P \cdot Q = O$
- de lo contrario, $P \cdot Q = (x_3, y_3)$ en donde:

$$x_3 = \lambda^2 - x_1 - x_2,\ y_3 = \lambda(x_1 - x_3) - y_1 \ \&\ \lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}, & P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1}, & P = Q \end{cases}$$

Curva elíptica sobre $\mathbb{Z}_p$

Sean $E: y^2 = x^3 + ax + b$ una curva elíptica sobre $\mathbb{Z}_p$ y $G = \{(x, y) \in E\} \cup \{O\}$, en donde O es el punto en el infinito.

Si $P = (x_1, y_1), Q = (x_2, y_2) \in E$, se define una operación binaria $\cdot$ sobre G:

- $P \cdot O = O \cdot P = P, \forall P \in E$
- si $x_1 = x_2$ y $y_1 = -y_2$ entonces $P \cdot Q = O$
- de lo contrario, $P \cdot Q = (x_3, y_3)$ en donde:

$$x_3 = \lambda^2 - x_1 - x_2,\ y_3 = \lambda(x_1 - x_3) - y_1 \ \&\ \lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}, & P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1}, & P = Q \end{cases}$$

Se puede demostrar que $(G, \cdot)$ es un grupo abeliano finito.

Ejemplo 2

Sea $E: y^2 = x^3 + x + 6$ sobre $\mathbb{Z}_{11}$. Se calculan los puntos sobre E verificando si para cada $x \in \mathbb{Z}_{11}, x^3 + x + 6$ es residuo cuadrático. Entonces:

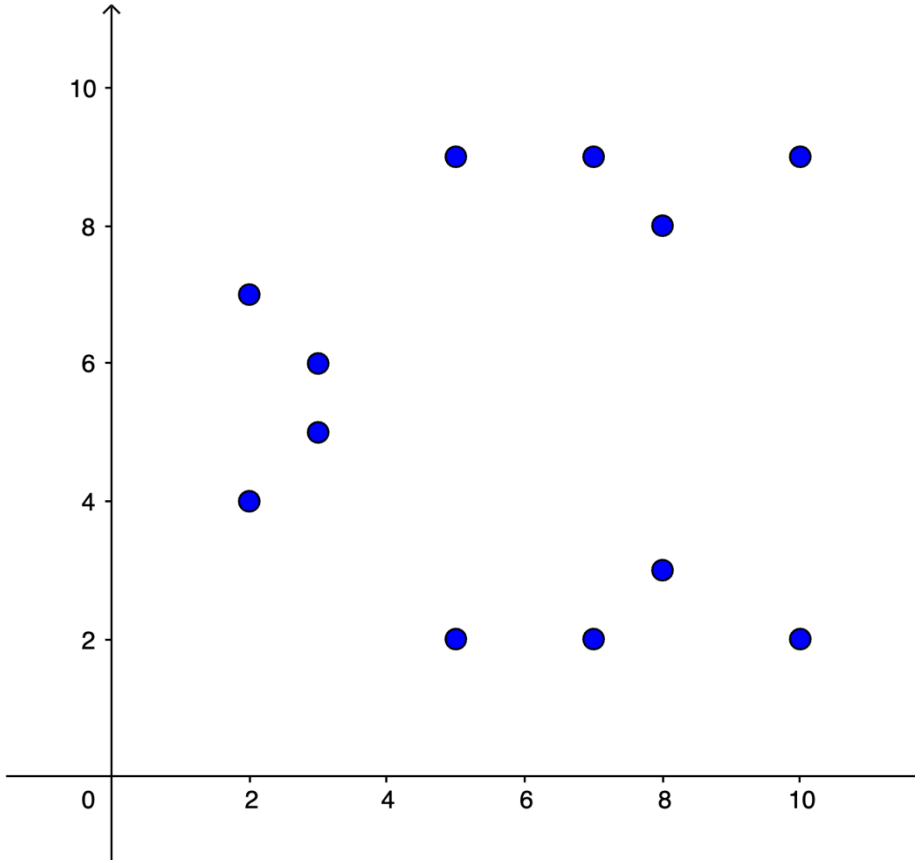
$$G = \{O, (2,4), (2,7), (3,5), (3,6), (5,2), (5,9), (7,2), (7,9), (8,3), (8,8), (10,2), (10,9)\}$$

Además, como $|G| = 13 \Rightarrow (G, \cdot) \cong (\mathbb{Z}_{13}, +)$.

Ejemplo 2

En la figura se muestra la representación gráfica de la curva elíptica E sobre $\mathbb{Z}_{11}$.

Nótese la simetría horizontal.



Ejemplo 2

Para calcular $(2,7) \cdot (5,2)$ se tiene $\lambda = (2-7)(5-2)^{-1} = 6 \cdot 4 = 2 \pmod{11}$.

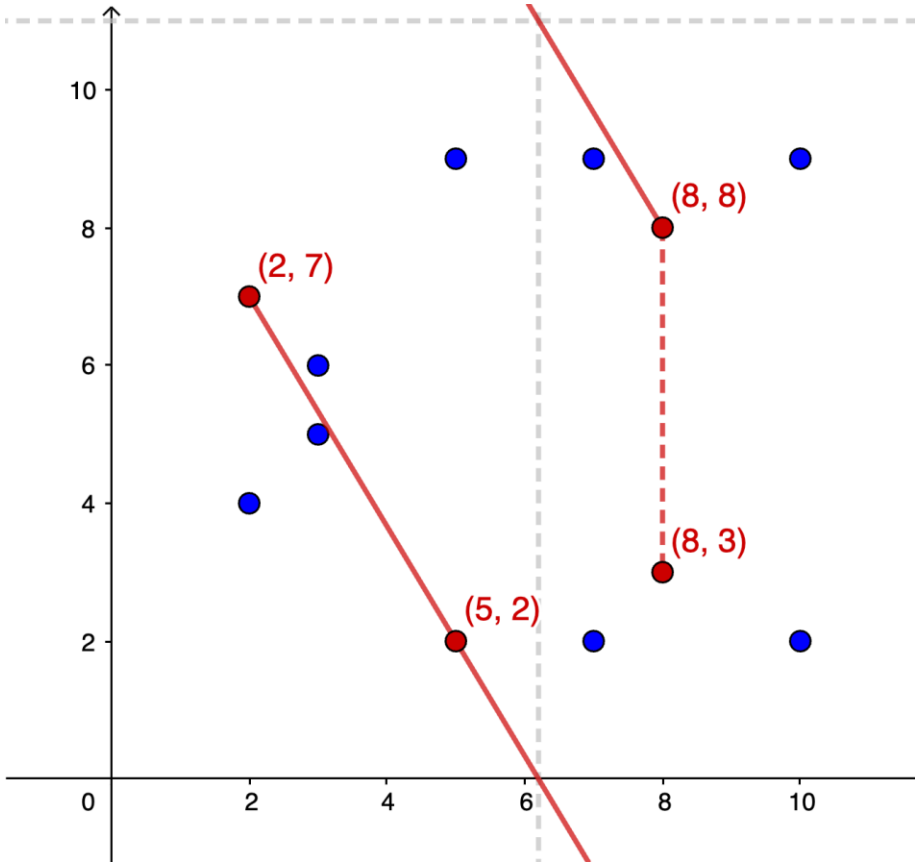
Entonces, $x_3 = 2^2 - 2 - 5 = -3 = 8$ & $y_3 = 2(2-8) - 7 = -19 = 3 \pmod{11}$.

Por lo tanto, $(2,7) \cdot (5,2) = (8,3)$.

Ejemplo 2

La representación gráfica de la operación $(2,7) \cdot (5,2) = (8,3)$ se muestra en la figura.

Nótese que se puede visualizar la línea entre dos puntos como una línea que se “envuelve” al salir de los bordes.



Ejemplo 2

Para calcular $(2,7)^2$ se tiene $\lambda = (3(2)^2 + 1)\big(2(7)\big)^{-1} = 13 \cdot 4 = 8 \pmod{11}$.

Entonces, $x_3 = 8^2 - 2 - 2 = 60 = 5$ & $y_3 = 8(2-5) - 7 = -31 = 2 \pmod{11}$.

Por lo tanto, $(2,7)^2 = (5,2)$.

Curva elíptica sobre $\mathbb{Z}_p$

El teorema de Hasse sobre curvas elípticas proporciona una estimación del número de puntos de una curva elíptica sobre un campo finito. Éste afirma que:

Si N es el número de puntos de la curva elíptica E sobre un campo finito con p elementos, entonces:

$$p + 1 - 2\sqrt{p} \leq N \leq p + 1 - 2\sqrt{p}$$

En general, se requiere encontrar un subgrupo H de G de orden primo q, lo cual implica que $H \cong \mathbb{Z}_q$.

Elliptic Curve Cryptography - ECC

Problema de logaritmo discreto de la curva elíptica

Se conocen algoritmos eficientes para hacer la operación A^n en $(G,\cdot)$, pero no se conocen métodos eficientes para calcular n dados A y A^n.

El problema de invertir la operación se conoce como Problema del Logaritmo Discreto de la Curva Elíptica (ECDLP).

La Criptografía de Curva Elíptica se basa en la exponenciación de puntos de curva elíptica y su seguridad viene dada por la dificultad de resolver el ECDLP.

ECC

Los métodos utilizados en la práctica para cifrar mensajes son adaptaciones de antiguos criptosistemas de logaritmos discretos; entre los que se podrían incluir Diffie-Hellman, ElGamal y DSA.

Suponga que se desea encriptar un mensaje M usando el sistema ElGamal.

Primero, se genera un par de claves:

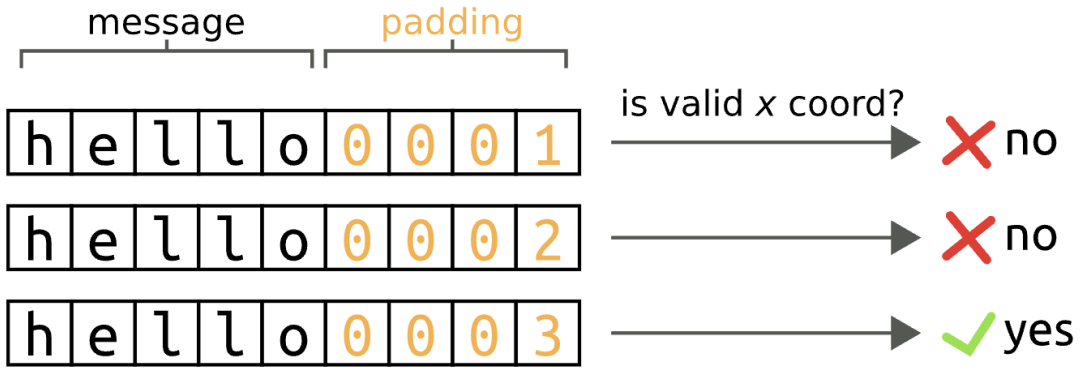
- se escoge un entero n (clave privada)
- se escoge un generador G del grupo cíclico de la curva elíptica y se calcula

$$P = G^n \text{ (clave pública)}$$

Segundo, se mapea M a un punto Q en la curva elíptica.

Nota: Para una computadora, las cadenas de bytes y los números enteros tienen la misma naturaleza: no son más que secuencias de bits, por lo que existe una correspondencia natural entre ambos.

Si M no se mapea a una coordenada x válida, se puede añadir un byte aleatorio (o varios bytes) al mensaje hasta conseguir una coordenada x válida y luego se calcula la coordenada y correspondiente, de modo que $M = (x, y) = Q$.



Tercero, se escoge un entero aleatorio k y se calculan $C_1 = G^k$ y $C_2 = P^k Q$. Finalmente, el par (C_1, C_2) es el mensaje cifrado.

Para recuperar el mensaje usando la clave privada n, se calcula $C_2 C_1^{-n}$. Esto pues:

$$C_2 C_1^{-n} = \left(P^k Q\right)\left(G^k\right)^{-n} = P^k Q (G^n)^{-k} = P^k Q (P)^{-k} = Q,$$

y como se mostró anteriormente, $M = Q$.

Conclusión

Conclusión

Se han creado algoritmos especializados como el *Quadratic Sieve* y el *General Number Field Sieve* para abordar el problema de la factorización de primos y han tenido un éxito moderado.

Estos algoritmos de factorización son más eficientes a medida que aumenta el tamaño de los números a factorizar, que es la manera de incrementar la seguridad en sistemas como RSA.

Aunque es probable que se pueda mantener la seguridad de RSA aumentando la longitud de las claves, esto tiene el costo de un rendimiento criptográfico más lento para el usuario.

Conclusión

A pesar de casi tres décadas de investigación, aún no se ha encontrado un algoritmo que resuelva el PLDCE que mejore el enfoque exhaustivo.

Esto significa que, para números del mismo tamaño, resolver logaritmos discretos de curva elíptica es significativamente más difícil que factorizar.

Puesto que un problema difícil más intensivo computacionalmente significa un sistema criptográfico más fuerte, se deduce que los criptosistemas de curva elíptica son más difíciles de romper que RSA y Diffie-Hellman.

Conclusión

Con ECC es posible utilizar claves más pequeñas para obtener los mismos niveles de seguridad.

Las claves pequeñas son importantes, sobre todo en un mundo en el que la criptografía se realiza cada vez más en dispositivos menos potentes, como los teléfonos móviles.

ECC parece ofrecer una mejor compensación: alta seguridad con claves cortas.

Conclusión

ECC parece ofrecer una mejor compensación: alta seguridad con claves cortas.

Tamaño de la clave	Tamaño del módulo	Tamaño de curva elíptica
80 bits	1024 bits	160 bits
128 bits	3072 bits	256 bits
256 bits	15360 bits	512 bits

¿Preguntas?