Curvas Elípticas

José Eduardo López Gómez

Universidad Del Valle de Guatemala

noviembre 23, 2021

1. Son objetos de teoría de números que se encuentran entre la aplicación y la teoría.
2. Sus estructuras de grupo son ideales para construir criptosistemas.
3. Proveen buena seguridad de incriptación.
4. Están ligadas al sistema de criptografía RSA.
5. Pueden utilizarse para resolver problemas teóricos como el último Teorema de Fermat o factorización de enteros sobre campos finitos.

Definition

Se denomina como curva elíptica sobre un campo K a la curva definida por una ecuación de la forma:

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

donde $a, b \in K$ y $-16(4a^3 + 27b^2) \neq 0$. Esta condición implica que la curva no tiene puntos singulares.

Definition

Forma de Weierstrass
Esta es una forma más general de curva elíptica sobre el campo K y se denomina de la siguiente manera:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$$

donde $a_1, a_2, a_3, a_4, a_5 \in K$

Definition

Punto Singular

Se denomina como punto singular a un punto p tal que la curva definida por $f(x, y) = 0$ cumple con que el gradiente se indefine en dicho punto p. Es decir, una curva tiene un punto singular si:

$$\nabla f(p) = 0$$

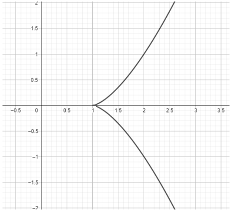


Figure: La imagen corresponde a $y^2 = (x-1)^3$ sobre $\mathbb{R}$ con un punto singular en $(1, 0)$

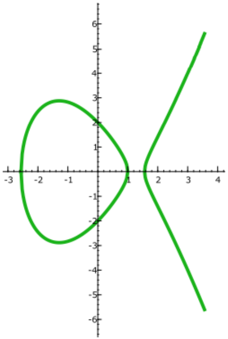


Figure: La imagen corresponde a $y^2 = x^3 - 5x + 4$ sobre $\mathbb{R}$

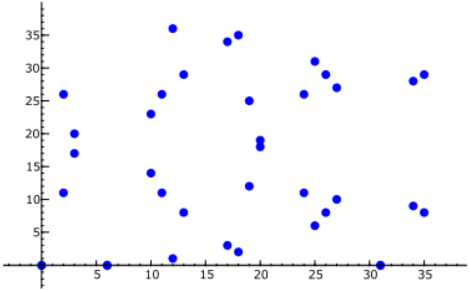


Figure: La imagen corresponde a $y^2 = x^3 + x$ sobre $\mathbb{Z}/37\mathbb{Z}$

Definition

La estructura de grupo abeliano sobre el conjunto $K-$ racional de puntos en una curva E sobre K.

$$E(K) = \{(x, y) \in K \times K : y^2 = x^3 + ax + b\} \cup \{\mathbb{O}\}$$

Nota: el punto $\mathbb{O}$ puede ser interpretado como un punto en el infinito de E.

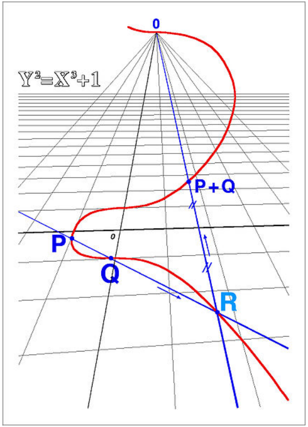


Figure: Punto al "infinito" perspectiva de plano

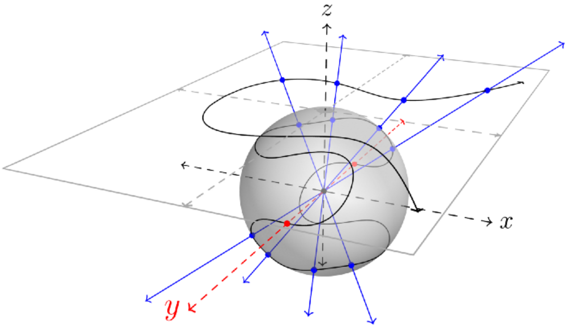
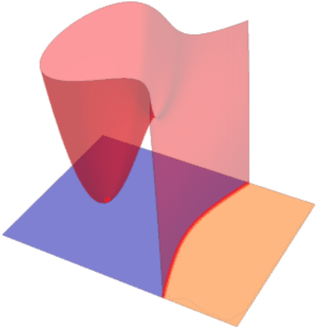
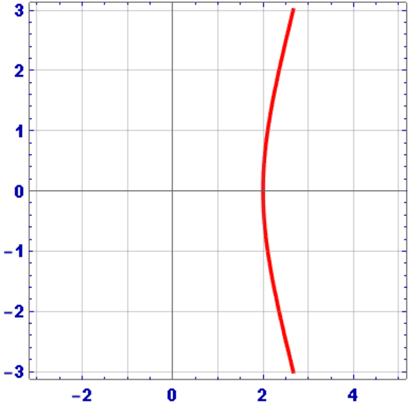


Figure: Punto al infinito perspectiva de 2 - esfera




3
2
1
0
-1
-2
-3
-2
0
2
4

Sea E una curva elíptica sobre el campo K, dada la ecuación $y^2 = x^3 + ax + b$. Se define la operación binaria $+$ en $E(K)$.

Definition

Dados dos puntos $P_1, P_2 \in E(K)$ este algoritmo computa un tercer punto:

$$R = P_1 + P_2 \in E(k)$$

- Identidad: si $P_1 = \mathbb{O}$ entonces $R = P_2$. En el caso contrario, si $P_2 = \mathbb{O}$ entonces $R = P_1$.
- Negativos: si $x_1 = x_2$ y $y_1 = -y_2$ entonces $R = \mathbb{O}$

Definition

Dados dos puntos $P_1, P_2 \in E(K)$ este algoritmo computa un tercer punto:

$$R = P_1 + P_2 \in E(k)$$

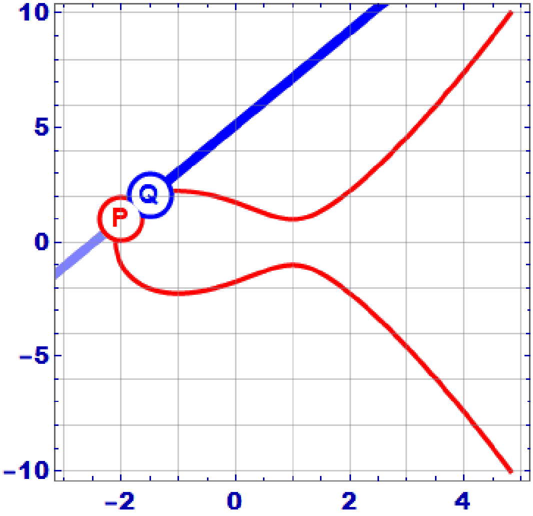
- Computar

$$\lambda = \begin{cases} (3x_1^2 + a)/2y_1 & , \quad \text{si } P_1 = P_2 \\ (y_1 - y_2)/(x_1 - x_2) & , \quad \text{en cualquier otro caso} \end{cases}$$

- Computar la suma:

$$R = (\lambda^2 - x_1 - x_2, -\lambda x_3 - v)$$

donde: $v = y_1 - \lambda x_1$ y $x_3 = \lambda^2 - x_1 - x_2$


10
5
0
−5
−10
−2
0
2
4
P
Q

Considere la curva elíptica sobre $\mathbb{R}$:

$$y^2 = x^3 - 5x + 4$$

y los puntos: $P_1 = (0,2), P_2 = (1,0)$ entonces al aplicar el algoritmo tenemos que:

$$\boxed{\lambda = \frac{2-0}{0-1} = -2} \qquad \boxed{x_3 = 4 - 0 - 1 = 3} \qquad \boxed{v = 2}$$

Por lo tanto el punto $R = P_1 + P_2$ es:

$$\boxed{R = (3, 6-2) = (3,4)}$$

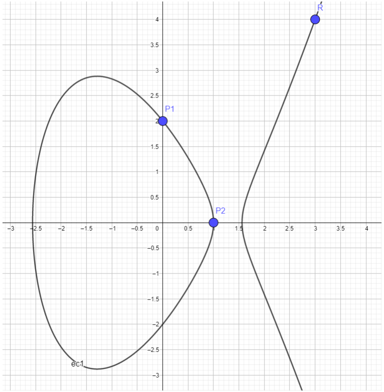


Figure: Resultado de $(0, 2) + (1, 0) = (3, 4)$ en $y^2 = x^3 - 5x + 4$ sobre $\mathbb{R}$

Theorem

La operación binaria + dota al conjunto $E(K)$ de una estructura abeliana de grupo con identidad $\mathbb{O}$

Lema

Suponga $P_i = (x_i, y_i), \quad i = 1, 2$ son puntos distintos sobre una curva elíptica de la forma $E : y^2 = x^3 + ax + b$ y además, $x_1 \neq x_2$. Sea L la única linea que pasa por P_1 y P_2, entonces L intersecta a la curva E en exactamente otro punto con coordenadas:

$$R = (\lambda^2 - x_1 - x_2, \lambda x_3 + v)$$

donde $\lambda = (y_1 - y_2)/(x_1 - x_2)$ y $v = y_1 - \lambda x_1$

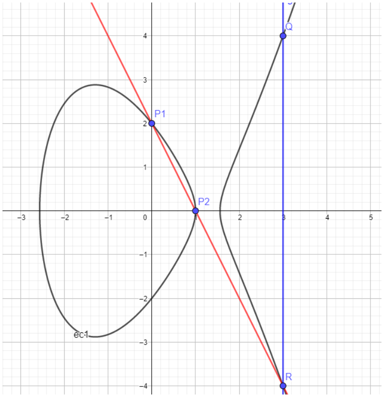


Figure: Visualización del Lema sobre la curva: $y^2 = x^3 - 5x + 4$

Definition

(Potencia Suave) Sea B un entero poistivo. Si n es un entero positivo con factorización prima:

$$n = \prod p_i^{a_i}$$

entonces n es de potencia B- suave si se cumple que:

$$p_i^{ai} \leq B \quad \forall i$$

Ejemplos

$30 = 2 \cdot 3 \cdot 5$ es potencia 5 - suave.
$150 = 2 \cdot 3 \cdot 5^2$ no es potencia 5 - suave pero es potencia 25 - suave.

Mínimo múltiplo común de los primeros B enteros

Dado un entero positivo B, este algoritmo computa el mínimo común múltiplo de los enteros positivos hasta B.

- Filtar: usando un algoritmo de filtro, computar la lista P de todos los primos $p \leq B$.
- Multiplicar: computar lo siguiente

$$a = \prod_{p \in P} p^{\lfloor log_p(B) \rfloor}$$

Algoritmo de filtrado

Dado un entero positivo n:

- Iniciar: sea $X = [3, 5, ...]$ sea la lista de números impares entre 3 y n. Sea $P = [2]$, la lista de primos encontrados hasta ahora.
- ¿Terminó?: sea p el primer elemento de X. Si $p \geq \sqrt{n}$ agregue ese p a P y termina. En otro caso, añadimos p a P.
- Tachado: actualice la lista X a la sublista de elementos de X que no son divisibles dentro de p. Volver al paso anterior.

Trabajeremos un ejemplo con pocos primos porque el algoritmo crece bastante rápido, entonces considere $n = 10$, el cual tiene la siguiente lista de primos:

$$P = [2, 3, 5, 7]$$

por lo que:

$$a = 2^{\lfloor log_2(10) \rfloor} \cdot 3^{\lfloor log_3(10) \rfloor} \cdot 5^{\lfloor log_5(10) \rfloor} \cdot 7^{\lfloor log_7(10) \rfloor}$$

$$a = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^1 = 8 \cdot 9 \cdot 5 \cdot 7$$

$$\boxed{a = 2520}$$

Algoritmo (No es el método ρ)

Dado un entero positivo n:

1. Computar MCM: usando el algoritmo de los primeros B enteros computamos m.
2. Iniciar: $a = 2$.
3. Potencia y MCD: computamos $x = a^n - 1 \pmod N$ y $g = MCD(x, N)$.
4. ¿Terminó?: si $g \neq 1$ o N, devuelva g y termina.
5. Intentar de nuevo: si $a < 10$, actualizamos $a = a + 1$ y regresamos al paso 3. De otra forma, el algoritmo termina.

Si fijamos un entero B. Si $N = pq$ donde p y q son primos, y suponemos que $p-1$ y $q-1$ no son potencia $B-$suave, entonces el método de Pollard no funciona bien.

Algoritmo

Dado un entero positivo N y una cota superior B, este algoritmo intenta encontrar un factor no trivial g de N o falla:

1. Computar MCM: usando el algoritmo de los primeros B enteros computamos m.
2. Escoger una curva E: escoger un valor aleatorio $a \in \mathbb{Z}/N\mathbb{Z}$ tal que: $a^3 + 27 \in (\mathbb{Z}/N\mathbb{Z})^*$. Entonces $P = (0, 1)$ es un punto en la curva elíptica $y^2 = x^3 + ax + 1$ sobre $\mathbb{Z}/N\mathbb{Z}$
3. Computar: se intenta computar mP usando el algoritmo análogo a las curvas elípticas. Si en algún punto no se puede computar la suma dado que un denominador no es coprimo a N, computamos el máximo comun divisor g de este denominador con N. Si g es un divisor no trivial, se saca. Si todos los denominadores son coprimos a N se muestra que el algoritmo falla.

El Caso donde falla Pollard

Considere $N = 5959 = 59 \cdot 101$, tome $B = 20$ y notemos que:

$$p - 1 = 58 = 2 \cdot 29 \qquad q - 1 = 100 = \cdot 4 \cdot 25$$

ninguno de los dos números es potencia 20 - suave. Además tenemos que:

$$m = lcm(1, 2, 3, ..., 20) = 232792560$$

lo cual es:

$$2^m - 1 \equiv 5944 \pmod{5959}$$

y finalmente:

$$gcd(2^m - 1, 5959) = 1$$

por lo que no se encuentra un factor de N

Diffie - Hellman

1. Nikita y Michael escogen un número de 200 dígitos p que es probable que sea primo, y escogen un número g tal que $1 \leq g \leq p$.
2. Nikita es coge un número entero n
3. Michael escoge un número entero m
4. Nikita le dice a Miuchael el resultado de computar $g^n \pmod p$
5. Michael le dice a Nikita el resultado de computar $g^m \pmod p$
6. Comparten una clave secreta de la siguiente forma:

$$s \equiv (g^n)^m \equiv (g^m)^n \equiv g^{nm} \pmod p$$

Curva Elíptica análoga a Diffie - Hellman

Suponga que Michael y Nikita concuerdan en una llave secreta de la siguiente manera:

1. Michael y Nikita concuerdan en un primo p, una curva elíptica E sobre el campo $\mathbb{Z}/p\mathbb{Z}$ y un punto $P \in (\mathbb{Z}/p\mathbb{Z})$
2. Michael escoge un número aleatorio y secreto m y computa mP.
3. Nikita escoge un número aleatorio y secreto n y computa nP.
4. la clave secreta es entonces nmP que ambos pueden computar.

- Stein, W (2011) Elementary Numer Theory: Primes, Congruences and Secrets
- Silverman, J; Tate, J. (2015). Rational Points on Elliptic Curves, Estados Unidos, Springer
- Mars, A. (2006) Elliptic Curves. Extraído de: https://www.maths.tcd.ie/pub/Maths/Courseware/499/2006/Mars/ellcurves.pdf
- Donald, N. (2021) Elliptic Curves. Extraído de: https://www.math.uci.edu/ ndonalds/math180b/7elliptic.pdf
- Stein, W. (2006) Diffie - Hellman - a way to create a shared secret. Extraído de: https://wstein.org/simuw06/notes/notes/node15.html
- Oza, J.; Singh, N. (2015) Algorithms for factoring. Extraído de: https://www.csa.iisc.ac.in/ arpita/Cryptography15/CT9.pdf