Curvas elípticas:

¡No son elipses!

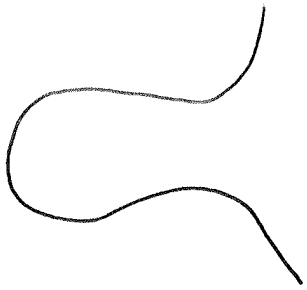
Una CE es el conjunto de soluciones a una ecuación de la forma

$$Y^2 = X^3 + AX + B$$

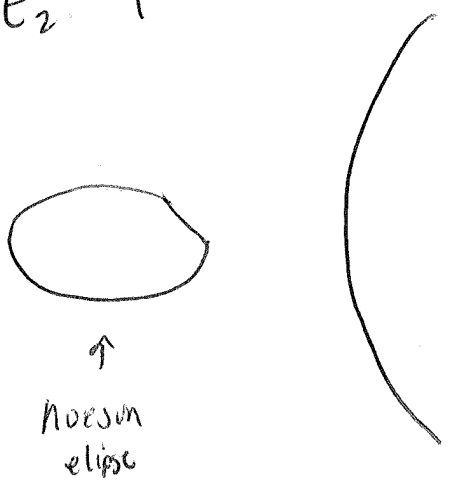
ec. de Weierstrass

Ej:

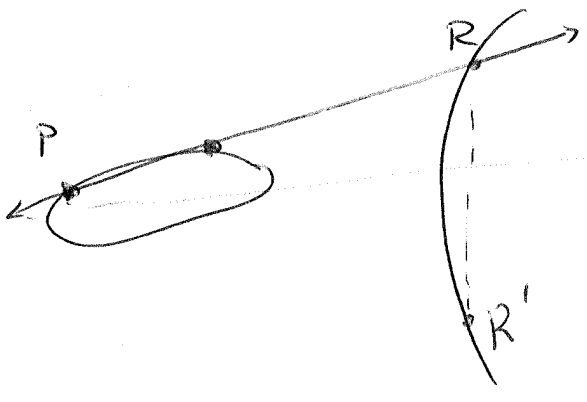
E_1: $Y^2 = X^3 - 3X + 3$



E_2: $Y^2 = X^3 - 6X + 5$



Se puede sumar dos puntos cualesquiera en E tal que en cierta manera para que el ~~resultado~~ B es otro punto en la curva:



$P \oplus Q = R'$

4: $E: Y^2 = X^3 - 15X + 18$

$P(7,16); Q = (1,2)$ están en E ✓

$(4 = 1 - 15 + 18)$

La recta L entre P y Q es

$L: Y = \frac{7}{3}X - \frac{1}{3}$ $\left[Y - 2 = \left(\frac{16-2}{7-1}\right)(X-1)\right]$

Ahora tomamos L y lo sustituimos en E:

$$\left(\frac{7}{3}x - \frac{1}{3}\right)^2 = X^3 - 15X + 18$$

$$0 = x^3 - \frac{49}{9}x^2 - \frac{121}{9}X + \frac{161}{9}$$

Para encontrar el tercer punto, tenemos que resolver para X

Hay 3 soluciones, pero ya sabemos 2: $X = 1, 7$.

$$X^3 - \frac{49}{9}x^2 - \frac{121}{9}X + \frac{161}{9} = (X-1)(X-7)\left(X + \frac{23}{9}\right)$$

Para encontrar la coordenada de Y:

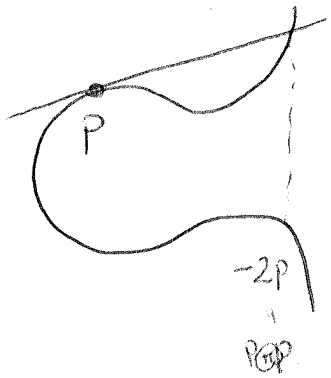
$$Y = \frac{7}{3}\left(-\frac{23}{9}\right) - \frac{1}{3} = \pm\frac{170}{27}$$

y la reflejamos:

$$P \oplus Q = \left(-\frac{23}{9}, -\frac{170}{27}\right).$$

R'

¿P⊕P que es!



Ej Encuentre la recta tangente a la curva $y^2 = x^3 - 15$, en el punto $P = (7, 16)$

$$2y\frac{dy}{dx} = 3x^2 - 15$$

$$\Rightarrow \frac{dy}{dx} = \frac{3x^2 - 15}{2y}$$

$$\Rightarrow \left.\frac{dy}{dx}\right|_{(7,16)} = \frac{33}{8}$$

La tangente es dada por

$$L: \quad y = \frac{33}{8}x - \frac{103}{8}$$

El mismo procedimiento...

$$0 = x^3 - \frac{1089}{64}x^2 + \frac{2419}{32}x - \frac{9457}{64} = 0$$

$$= (x-7)^2\left(x - \frac{193}{64}\right)$$

↑ 7 es un doble cero

Y como antes L @ $x = \frac{193}{64} \Rightarrow y = \frac{223}{54}$ $\xrightarrow{\text{reflejo}}$ $P \oplus P = \left(\frac{193}{64}, \frac{-223}{54}\right)$

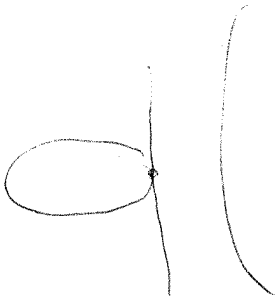
$P = (a, b)$ $P' = (a, -b)$ ¿$P \oplus P'$ que es?

Definimos un punto $\mathcal{O}$ en el infinito: es un punto que vive fuera de $\mathbb{R}^2$ pero vive en toda recta vertical.

Entonces se define que $P \oplus P' = \mathcal{O}$.

¿Ahora $P \oplus \mathcal{O}$ que es? o:

$P \oplus \mathcal{O} = P$



Ej: $T = (3, 0)$ es un punto en E.

$$T \oplus T = \mathcal{O}.$$

Def. Una curva elíptica E es el conjunto de soluciones de una ecuación de Weierstrass dada por

$$E: Y^2 = X^3 + AX + B$$

junto con un punto "distinguido" $\mathcal{O}$ donde las constantes complejas

$$4A^3 + 27B^2 \neq 0$$

discriminante no cero ⇒ ~~curva lisa~~ el cubico tiene tres raíces

~~E toma~~ Entonces la curva E con la ~~suma~~ suma definida

anda es un grupo:

$\mathcal{O}$: elemento nulo

$P + Q = R$

$-P$ con $P = (a, b)$ es el opuesto

La ley es bastante difícil de probar geométricamente

En particular $nP = \underbrace{P + P + \cdots + P}_{n \text{ veces}}$

$E: y^2 = f(x)$

Obs: $\Delta_E = 4A^3 + 27B^2$ y $\Delta_E \neq 0 \iff f(x)$ tiene 3 raíces distintas

$\Delta_E = 0 \Rightarrow E$ tiene puntos singulares

Veamos fórmulas para poder implementar la suma

$E: Y^2 = X^3 + AX + B$

entrada P_1, P_2

salida $P_1 + P_2$

(a) $P_1 = \mathcal{O}$ return P_2

(b) $P_2 = \mathcal{O}$ return P_1

(c) $P_1 = (x_1, y_1)$ $P_2 = (x_2, y_2)$

(d) si $x_1 = x_2$ y $y_1 = -y_2$ return $\mathcal{O}$

(e) en otro caso

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{si } P_1 \neq P_2 \\ \dfrac{3x_1^2 + A}{2y_1} & \text{si } P_1 = P_2 \end{cases}$$

y sea

$x_3 = \lambda^2 - x_1 - x_2$ $y_3 = \lambda(x_1 - x_3) - y_1$

return (x_3, y_3)

Dem (parte c).

λ es el pendiente de la recta o la tangente.

$$L: Y = \lambda X + \nu \quad \text{con} \quad \nu = y_1 - \lambda x_1$$

Sustituyendo L en E $\Rightarrow$

$$(\lambda X + \nu)^2 = X^3 + AX + B$$

$\Rightarrow$

$$X^3 - \lambda^2 X^2 + (A - 2\lambda\nu)X + (B - \nu^2) = 0$$

Como x_1, x_2, x_3 son raíces de este polinomio

$$\underbrace{X^3 - \lambda^2 X^2 + (A - 2\lambda\nu)X + (B - \nu^2)}_{\text{coef. de } X^2 \text{ es } -\lambda^2} = \underbrace{(X - x_1)(X - x_2)(X - x_3)}_{\text{coef de } X^2 \text{ es } -x_1 - x_2 - x_3}$$

Entonces $x_3 = \lambda^2 - \underbrace{x_1 - x_2}_{\text{conocidos}}$ y $y_3 = \lambda x_3 + \nu$. □

¿Aplicaciones criptográficas: hay que considerar la curva sobre $\mathbb{F}_p$

Y acá la intuición/definición geométrica de la suma no existe pero las fórmulas sí!

E sobre $\mathbb{F}_p$:

$$E: \quad y^2 = x^3 + Ax + B \qquad A, B \in \mathbb{F}_p \text{ tq } 4A^3 + 27B^2 \neq 0$$

y ambos

$$E(\mathbb{F}_p) = \{(x,y): \ x, y \in \mathbb{F}_p \text{ verifican } y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}.$$

Por ahora suponemos $p \geq 3$.

Ej: $E: y^2 = x^3 + 3x + 8$ sobre $\mathbb{F}_{13}$.

x^2	x
0	0
1	1
4	2
9	3
3	
12	
10	
10	
12	
3	
9	
4	12
1	

1) $x = 0 \Rightarrow$ $y^2 = 8$ no hay solución

2) $x = 1 \Rightarrow$ $y^2 = 12 \Rightarrow x = 5, \ x = 8$
$\Rightarrow (1,5), (1,8) \in E(\mathbb{F}_{13})$

Resulta que hay nueve ptos en $E(\mathbb{F}_{13})$.

¿Cómo se suman?

Tma. $E \setminus \mathbb{F}_p$ $P, Q \in E(\mathbb{F}_p)$

(a) $P+Q \in E(\mathbb{F}_p)$ usando el algoritmo de antes.

(b) $E(\mathbb{F}_p)$ es un grupo.

El grupo $E(\mathbb{F}_p)$ es finito, ¿pero qué grande es?

Para cada X hay p posibilidades y para cada X particular hay a lo sumo 2 soluciones en

$$Y^2 \equiv X^3 + AX + B$$

Agregando el punto θ hay a lo máximo $2p+1$ en $E(\mathbb{F}_p)$

De hecho, este corte no es muy bueno. Para un X fijo

$$X^3 + AX + B$$

es un RC o no. Si es un RC, tenemos dos de dos puntos en $E(\mathbb{F}_p)$

y esto pasa más o menos 50% de las veces. Entonces

$$\# E(\mathbb{F}_p) \approx 50\% \cdot 2 \cdot p + 1 = p+1$$

Tma (Hasse) $E \setminus \mathbb{F}_p$

$$\# E(\mathbb{F}_p) = p+1-t_p \quad \text{con } |t_p| \leq 2\sqrt{p}$$

Def. El número $p+1-t_p$ se llama la traza de Frobenius

El ECDLP

Def: $E \setminus \mathbb{F}_p$; $P, Q \in E(\mathbb{F}_p)$

El ECDLP es el problema de hallar el entero n tq $Q = nP$. Se denota

$$n = \log_P(Q)$$

Obs:
- Es posible que no exista el $n \Rightarrow \log_P(Q)$ es no definido
- En la práctica uno elige un n y P secreto y calcula $Q = nP$
- n es definido módulo el orden de P

  $P, 2P, \ldots$ son todos distintos y como hay una cantidad finita, $\exists k, j$ tq $kP = jP$

  $\Rightarrow (k-j)P = \mathcal{O}$.

  $\Rightarrow s$ el mínimo de los enteros k tq $kP = \mathcal{O}$.

- Si n_0 es un entero tq $n_0 P = \mathcal{O}$, entonces todos los n tq $nP = \mathcal{O}$ son de la forma $n = n_0 + is$ con $i \in \mathbb{Z}$ y s el orden

- $\log_P(Q_1 + Q_2) = \log_P(Q_1) + \log_P(Q_2)$ $\forall Q_1, Q_2 \in E(\mathbb{F}_p)$

- O sea $\log_P : E(\mathbb{F}_p) \to \mathbb{Z}/s\mathbb{Z}$ es un homomorfismo.

El algoritmo doblar y sumar (potenciación rápida)

Entrada Punto $P \in E(\mathbb{F}_p)$ entero $n \geq 1$

1. $Q \leftarrow P$ y $R \leftarrow \mathcal{O}$
2. while $n > 0$
3. si $n \equiv 1 \bmod 2$, entonces $R \leftarrow R + Q$
4. $Q \leftarrow 2Q$, $n \leftarrow \lfloor n/2 \rfloor$
5. devolver R $(= nP)$

Idea

$n = n_0 + n_1 2 + n_2 4 + \cdots + n_r 2^r$, $n_i \in \{0,1\}$

$$\left.\begin{array}{l} Q_0 = P \\ Q_1 = 2Q_0 \\ Q_2 = 2Q_1 \\ \vdots \\ Q_r = 2Q_{r-1} \end{array}\right\} \Rightarrow nP = n_0 Q_0 + n_1 Q_1 + \cdots + n_r Q_r$$

Obs: si la suma de dos puntos es una operación $\mathcal{A}$, este procedimiento tiene $2r$ operaciones (r para las sumas y r para los dobles)

Expansiones ternarias

En vez de descomponer n como una suma de potencias de dos, es más eficiente descomponerlo como una suma y resta de potencias de dos

Ej $947 = 1 + 2 + 2^4 + 2^5 + 2^7 + 2^8 + 2^9 \Rightarrow$ 15 operaciones

$947 = 1 + 2 - 2^4 - 2^6 + 2^{10} \Rightarrow$ 9 operaciones

(sumar $P = (x,y)$ es tan fácil que sumar restar $-P = (x,-y)$)

~~Conjet.~~

¿Cuán mejor es este método?

Peor de los casos.

$n = 2^k - 1$ { Solo sumas requiere $2k$ operaciones
sumas y restas requiere $k+1$ sumas y $\frac{3}{2}k$ dobles

En el promedio { Solo sumas $\frac{3}{2}k+1$
restas y sumas $\frac{4}{3}k+1$.

Prop. $n \in \mathbb{Z}_{>0}$, $k = \lfloor \log_2 n \rfloor + 1$. Entonces se puede escribir

$$n = u_0 + u_1 2 + u_2 2^2 + \cdots + u_k 2^k$$

con $u_i \in \{\pm 1, 0\}$ y a lo sumo $\frac{1}{2}k$ de los u_i distintos de cero.

Dem: (un algoritmo):

$n = n_0 + n_1 2 \cdots + n_{k-1} 2^{k-1}$ en binario

Buscamos la primera aparición de dos ni distintos de cero:

$n_s = n_{s+1} = \cdots = n_{s+t-1} = 1$ pero $n_{s+t} = 0$. Osea,

en $2^s + 2^{s+1} + \cdots + 2^{s+t-1} + 0 \cdot 2^{s+t}$
$= 2^s (1 + 2 + \cdots + 2^{t-1}) = 2^s (2^t - 1)$

Ocurre en la expansión binaria de n. Cambiamos la suma larga en

$-2^s + 2^{s+t}$

Al final tenemos una expansión donde no hay ± 1 consecutivos.

$\Rightarrow \frac{k}{2}$ dígitos binarios son no cero. □

Obs Aunque $n \approx 2^{k-1}$ la expansión del k prop puede llegar hasta 2^k.