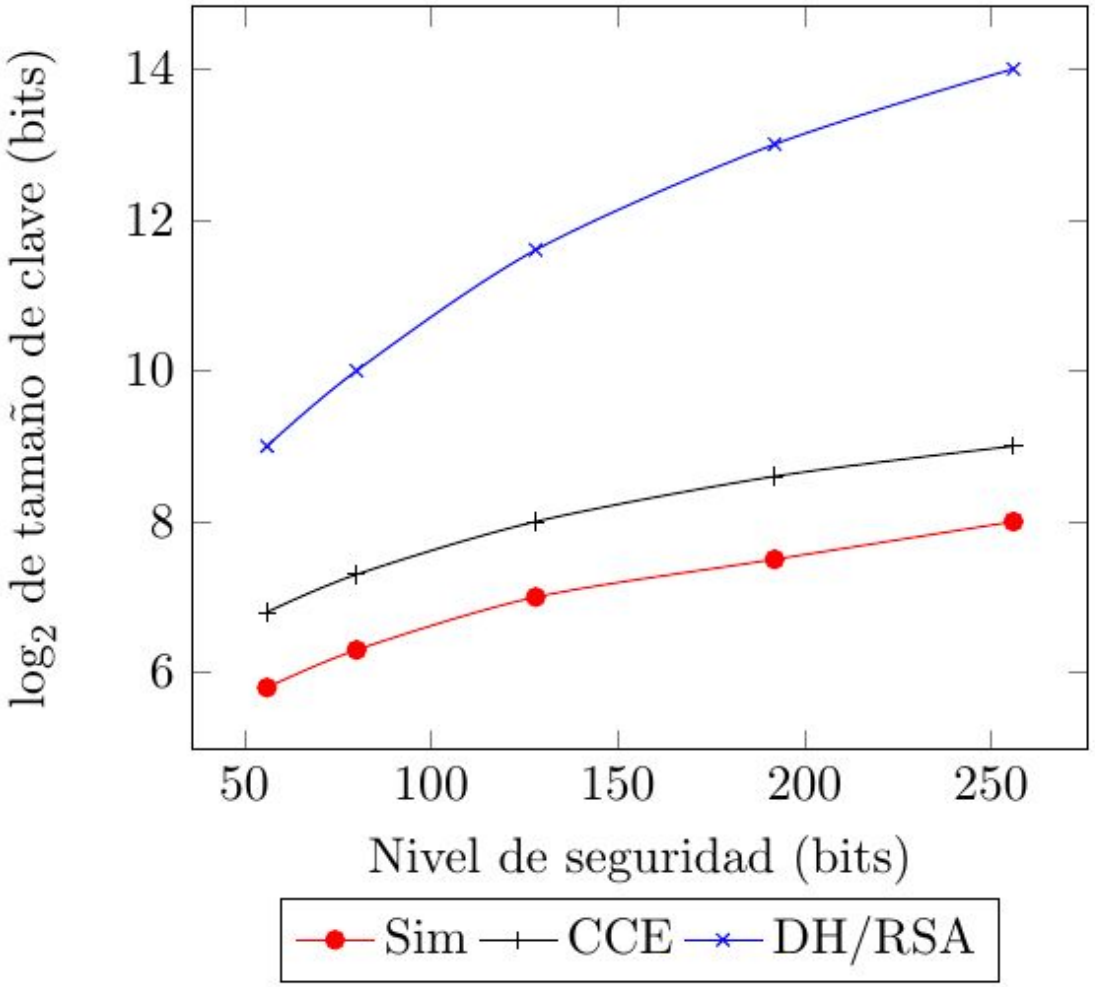
Criptografía sobre curvas elípticas

José Galaviz

Motivación

1985, Neal Koblitz y Victor Miller proponen simultánea e independientemente que es posible montar sistemas criptográficos de clave pública usando curvas elípticas.

La exploración



Datos

Simétricos	DH/RSA	CCE
80	1024	163
128	3072	283
192	7680	409
256	15360	571

Definición

Una curva elíptica es una curva algebraica plana definida por una ecuación de la forma:

$$E: \ y^2 = x^3 + ax + b \tag{2.1}$$

siempre y cuando no sea *singular*, esto es, la curva no se cruza a sí misma ni tiene *cúspides*[1]. Estas restricciones se pueden establecer formalmente diciendo:

$$4a^3 + 27b^2 > 0 \tag{2.2}$$

Ejemplos

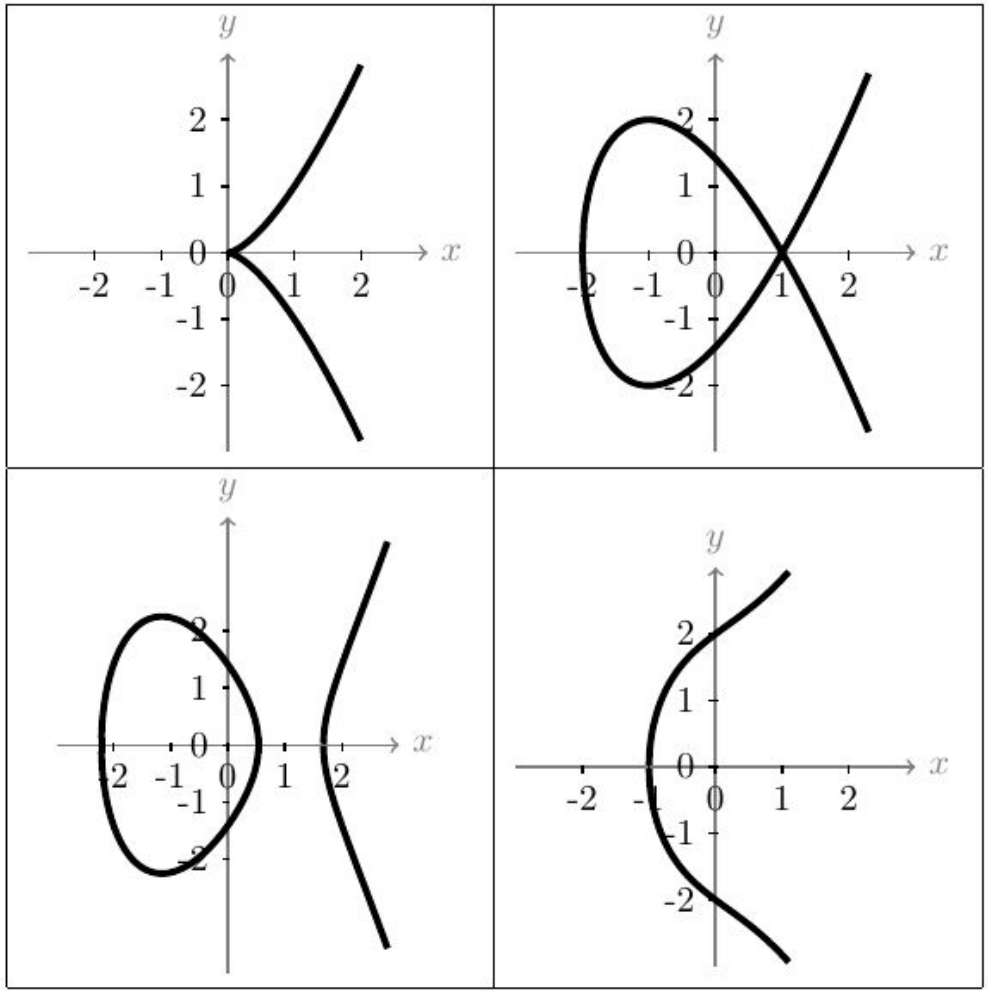


Figura 2.1: Algunos tipos de curvas elípticas: (arriba, izquierda) $y^2 = x^3$ es singular, tiene cúspide; (arriba, derecha) $y^2 = x^3 - 3x + 2$ es singular, exhibe un punto de cruce; (abajo, izquierda) $y^2 = x^3 - 4x + 2$ tiene dos componentes y (abajo, derecha) $y^2 = x^3 + 3x + 4$.

¿Qué hacemos?

- Tomar un conjunto finito de puntos sobre la curva.
- Definir una operación entre ellos.
- Darle estructura algebraica (grupo cíclico).
- Definir sobre ella una función de un sentido.

Nuestra curva de ejemplo

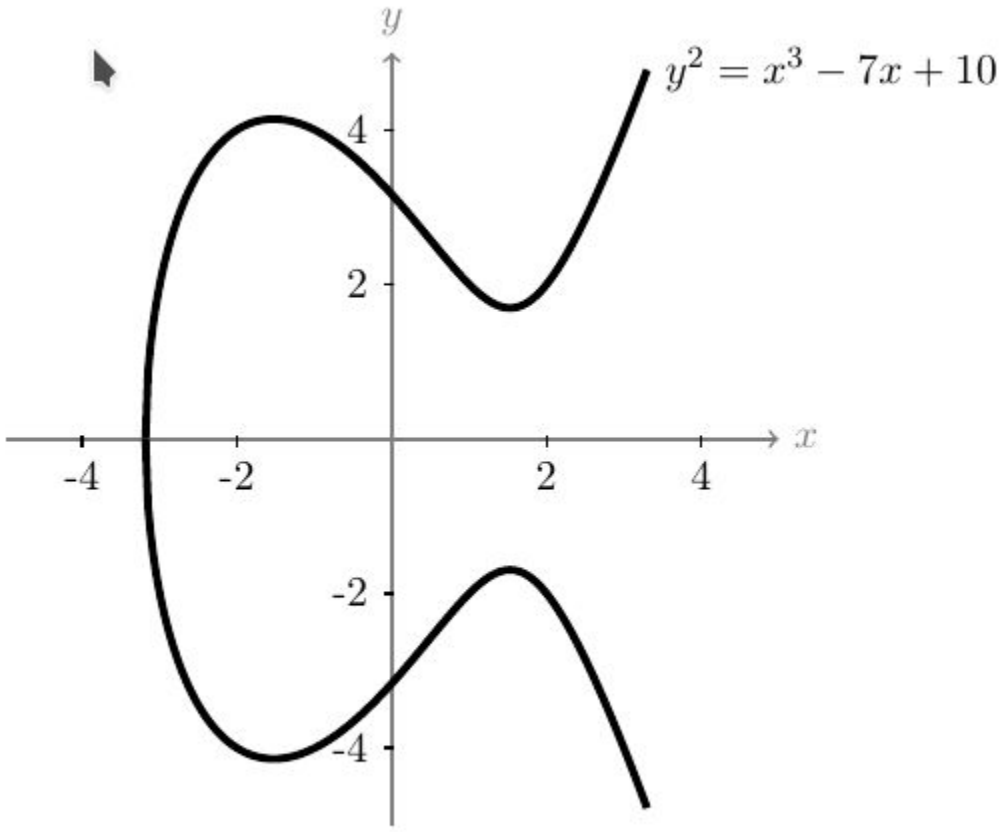


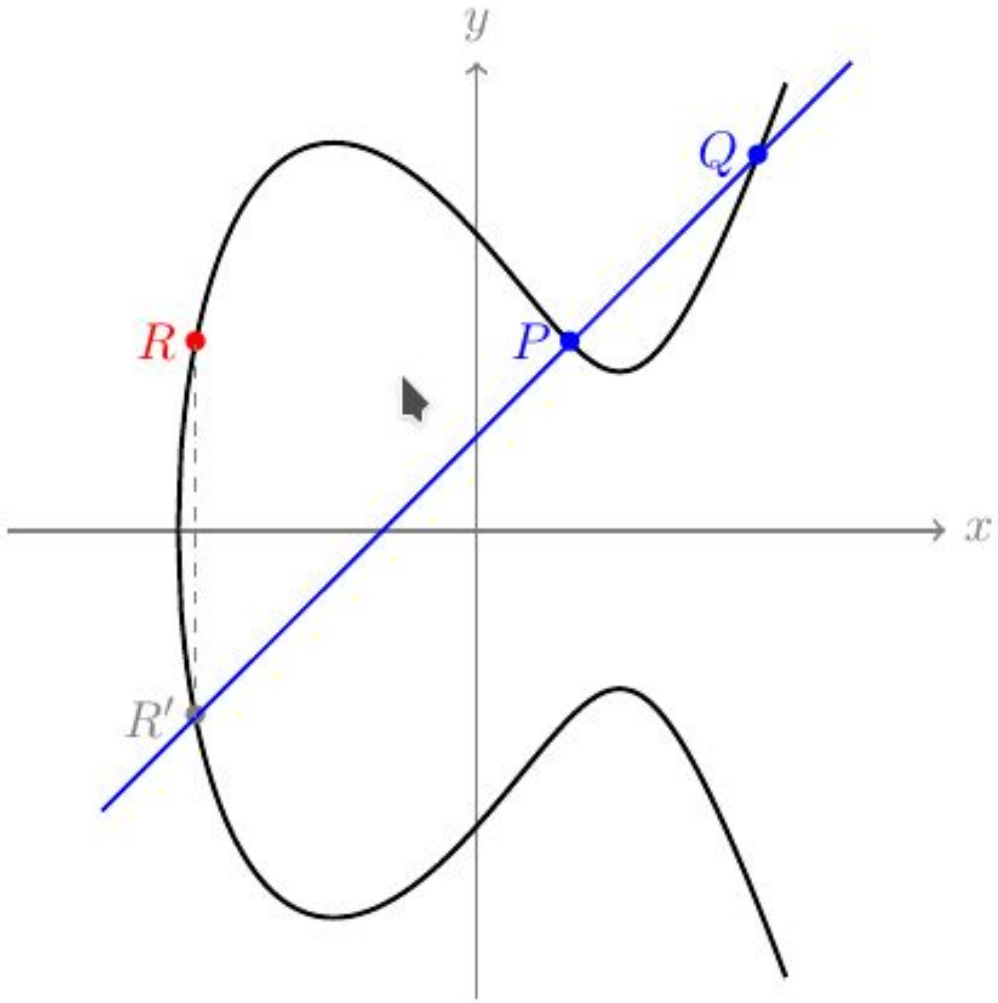
Figura 2.2: Gráfica de la curva $y^2 = x^3 - 7x + 10$ en $\mathbb{R}^2$.

Suma de puntos

Dados dos puntos P y Q sobre la curva definiremos la suma R=P+Q mediante un procedimiento geométrico:

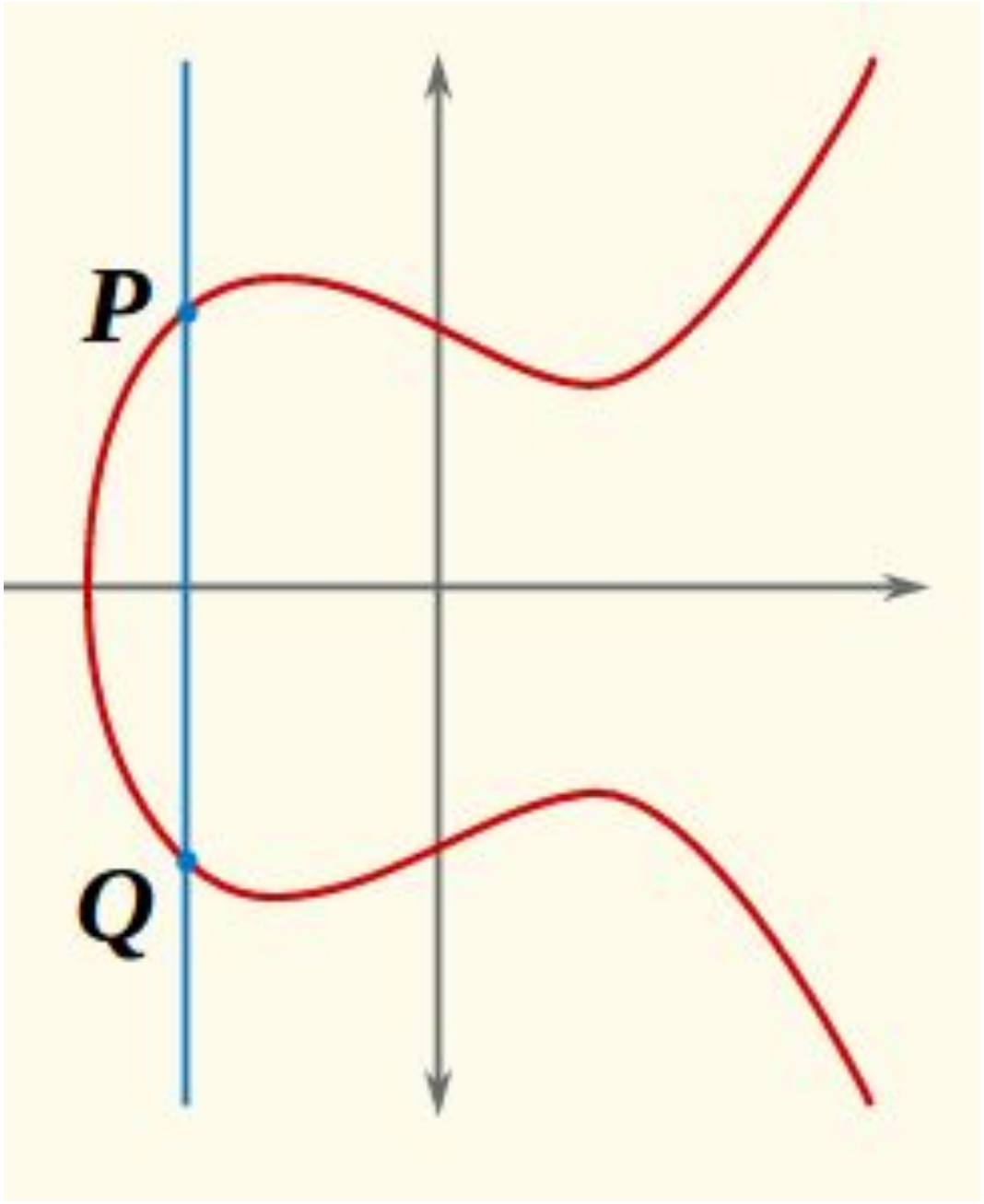
1. Se traza la línea recta que une P con Q.
2. Esta recta debe intersectar a la curva en otro punto al que llamaremos R'.
3. Reflejando R' en el eje horizontal se obtiene R, al que asociaremos con la suma de P y Q.

Ejemplo



Casos particulares que resolver

1. P y Q sobre la misma vertical ¿Cuál otro punto sobre la curva?
2. Si P y Q son el mismo punto, entonces P + Q = P + P = 2P ¿cómo lo encontramos?
    - Peor aún son el mismo y son el vértice de la curva (el punto en que cruza el eje horizontal)


P
Q

P y Q en la vertical

Tenemos que añadir a alguien. No es realmente un punto, es un concepto.

El punto al infinito

- P y Q están en la misma vertical, entonces la recta cruza a la “curva” en el punto al infinito $\mathcal{O}$, y lo reflejamos y

- ¿Y si sumamos P y $\mathcal{O}$?

P y Q en la vertical

Tenemos que añadir a alguien. No es realmente un punto, es un concepto.

El punto al infinito

- P y Q están en la misma vertical, entonces la recta cruza a la “curva” en el punto al infinito $\mathcal{O}$, y lo reflejamos y nos da… el mismo punto al infinito.
- ¿Y si sumamos P y $\mathcal{O}$?

P y Q en la vertical

Tenemos que añadir a alguien. No es realmente un punto, es un concepto.

El punto al infinito

- P y Q están en la misma vertical, entonces la recta cruza a la “curva” en el punto al infinito $\mathcal{O}$, y lo reflejamos y nos da… el mismo punto al infinito.
- ¿Y si sumamos P y $\mathcal{O}$? La vertical que pasa por P y el punto al inifinito cruza la curva en el simétrico de P y al reflejarlo nos da… pues P.

¿Quien es el punto al infinito $\mathcal{O}$?

$\mathcal{O}$

Resulta que:

- P + P’ = $\mathcal{O}$.
- P + $\mathcal{O}$ = P.

$\mathcal{O}$

Resulta que:

- $P + P' = \mathcal{O}$.
- $P + \mathcal{O} = P$.

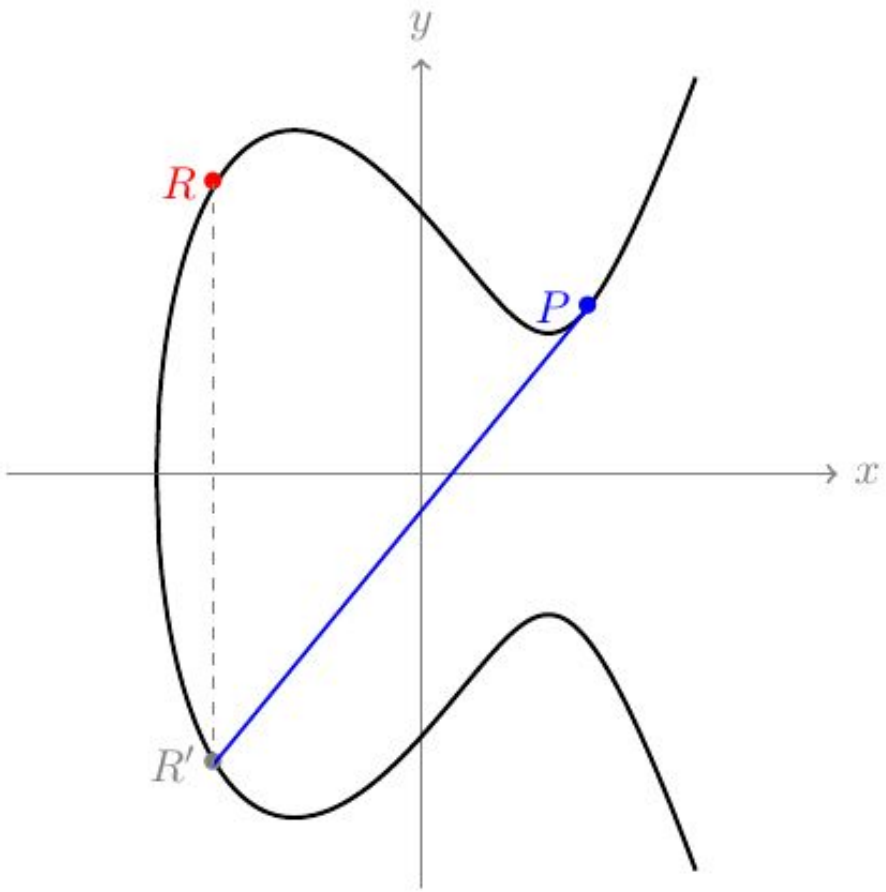
Es el neutro aditivo

P y Q son el mismo punto

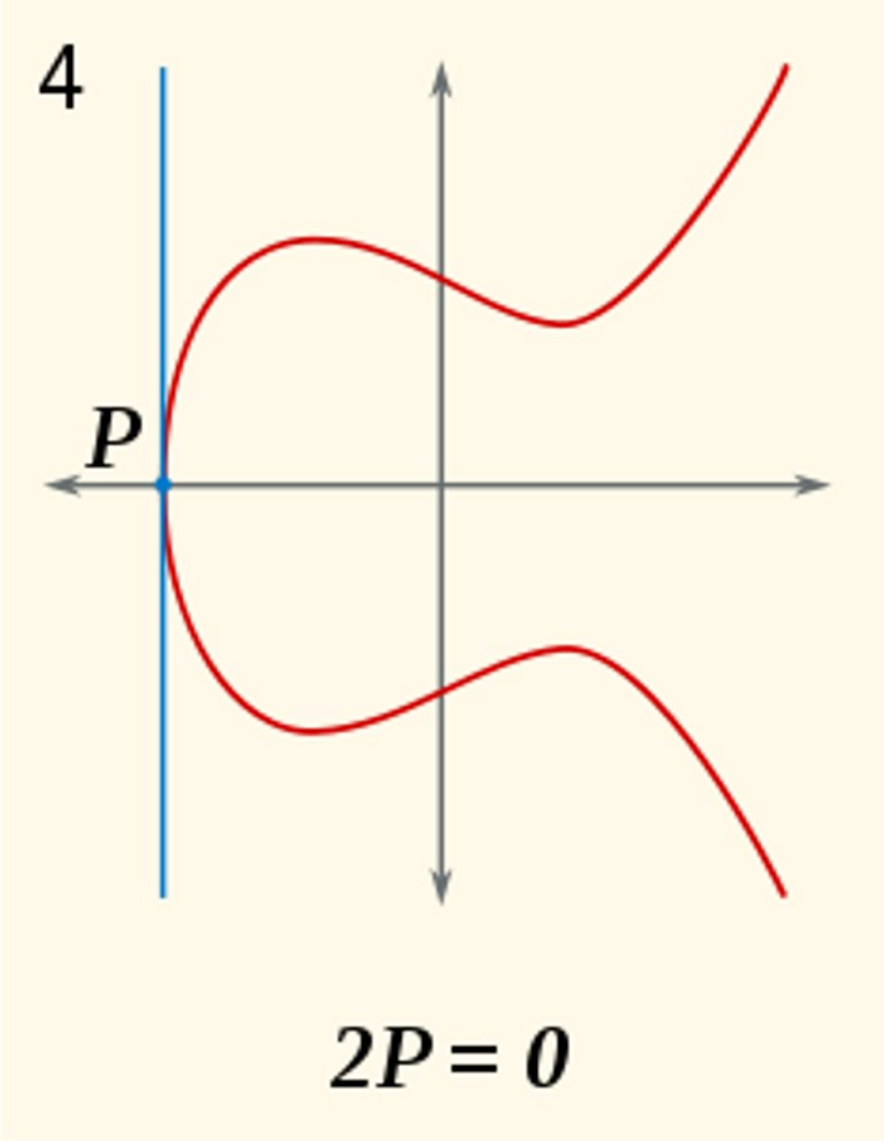
Si P y Q se van
acercando

P y Q son el mismo punto

La secante es una tangente.



Y sí P y Q son el mismo y son el vértice



En ese caso

- O = 2P

En ese caso

- O = 2P = 4P = 6P = …

En ese caso

- O = 2P = 4P = 6P = …
- P = 3P = 5P = 7P = ...

Ya sólo falta algo...

- No podemos trabajar sobre los reales.
- Definamos puntos con coordenadas enteras.
- En un campo.

Curva elíptica como la queremos

Definición 1. Una curva elíptica sobre $\mathbb{Z}_p$ ($p > 3$ primo) es el conjunto de parejas $(x, y) \in \mathbb{Z}_p^2$ que satisfacen:

$$E: \; y^2 \equiv x^3 + ax + b \pmod{p} \tag{2.3}$$

con $a, b \in \mathbb{Z}_p$, sujetas a la restricción:

$$4a^3 + 27b^2 \not\equiv 0 \pmod{p} \tag{2.4}$$

junto con un punto imaginario llamado *punto al infinito* denotado con $\mathcal{O}$.

Y la operación:

Definición 2. Sean $P = (x_1, y_1)$, $Q = (x_2, y_2)$ dos puntos sobre una curva elíptica de acuerdo a la definición 1 y $R = (x_3, y_3)$ el punto sobre la curva que corresponde a la suma de P y Q, entonces:

- Si $P \neq Q$ pero $x_1 = x_2$, entonces $R = P + Q = \mathcal{O}$.
- Si $P = Q$ y $y_1 = y_2 = 0$, entonces $R = P + Q = 2P = \mathcal{O}$.
- En otro caso:

$$x_3 \equiv s^2 - x_1 - x_2 \pmod{p} \tag{2.5}$$
$$y_3 \equiv s(x_1 - x_3) - y_1 \pmod{p} \tag{2.6}$$

donde:

$$s \equiv \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \pmod{p} & \text{si } P \neq Q \\ \\ \frac{3x_1^2 + a}{2y_1} \pmod{p} & \text{si } P = Q \end{cases} \tag{2.7}$$

El punto que corresponde con el inverso aditivo de P, denotado como $-P$ es:

$$-P \equiv (x_1, -y_1) \pmod{p} = (x_1, p - y_1)$$

Ejemplo

Ejemplo 2.3.1. Haremos algunas operaciones con la curva elíptica que está ilustrada en la figura 2.2.

Sea

$$E : y^2 \equiv x^3 - 7x + 10 \pmod{19} \tag{2.8}$$

recordemos que todas las operaciones deben hacerse módulo 19.

- Sea $P_1 = (9, 7)$, si duplicamos este punto obtendremos $2P_1$, para hacerlo, de la expresión 2.7:

$$\begin{aligned} s &\equiv \frac{3 \cdot 9^2 - 7}{2 \cdot 7} \pmod{19} \\ &\equiv (3 \cdot 9^2 - 7) \cdot 14^{-1} \pmod{19} \\ &\equiv (3 \cdot 81 - 7) \cdot 15 \pmod{19} \\ &= 6 \end{aligned}$$

Substituyendo en 2.5:

$$x_3 \equiv (6^2 - 9 - 9) \pmod{19} = 18$$

y en 2.6:

$$y_3 \equiv 6 \cdot (9 - 18) - 7 \pmod{19} = -4 \pmod{19} = 15$$

Así que $2P = (18, 15)$

- Supongamos ahora que tenemos $P_2 = (5, 9)$, si sumamos este punto con P_1 tenemos que:

$$\begin{aligned} s &\equiv \frac{9-7}{5-9} \pmod{19} \\ &\equiv (2) \cdot -4^{-1} \pmod{19} \\ &\equiv (2) \cdot 15^{-1} \pmod{19} \\ &\equiv 2 \cdot 14 \pmod{19} \\ &= 9 \end{aligned}$$

De donde:

$$\begin{aligned} x_3 &\equiv 9^2 - 9 - 5 \pmod{19} = 10 \\ y_3 &\equiv 9 \cdot (9 - 10) - 7 \pmod{19} \equiv -16 \pmod{19} = 3 \end{aligned}$$

¿Qué construimos?

El conjunto de puntos sobre E módulo p con la operación “+” definida es un grupo abeliano finito, cíclico.

Existe una k, escalar, tal que kP = P.

Todos los elementos tienen un periodo.

Hay algunos cuyo periodo es el tamaño del grupo: Generadores.

El ejemplo

Sea

$$E : y^2 \equiv x^3 - 7x + 10 \pmod{19}$$

El punto $P_1 = (9, 7)$ usado en el ejemplo previo genera los siguientes elementos de E:

$$\{P_1 = (9,7), 2P_1 = (18,15), 3P_1 = (1,17), 4P_1 = (7,0),$$
$$5P_1 = (1,2), 6P_1 = (18,4), 7P_1 = (9,12), 8P_1 = \mathcal{O}\}$$

Así que es un generador de un subgrupo cíclico de orden 8. El grupo completo asociado con la curva que nos ocupa es el mostrado en la tabla 2.1. Como puede observarse hay varios elementos que generan todo el grupo asociado a E módulo 19.

x	y	Orden	x	y	Orden
1	2	8	1	17	8
2	2	24	2	17	24
3	4	24	3	15	24
5	9	12	5	10	12
7	0	2	9	7	8
9	12	8	10	3	24
10	16	24	12	1	3
12	18	3	13	8	12
13	11	12	16	2	6
16	17	6	17	4	24
17	15	24	18	4	4
18	15	4	$\mathcal{O}$		0

El problema del “logaritmo” discreto

Definición 4. Dada una curva elíptica módulo un número primo p, sean G un elemento generador y P otro punto cualquiera, con $G, P \in < E, p, + >$, el *Problema del Logaritmo Discreto* consiste en encontrar un número $k \in \mathbb{N}$ tal que:

$$kG \equiv P \pmod{p}$$

Diffie-Hellman

1. Elegir un primo p grande y los valores de a y b en la expresión
$$E : y^2 \equiv x^3 + a \cdot x + b \pmod{p}$$
2. Elegir un elemento G, generador de los puntos de E.
3. A elige $k_A <| E |$ (el orden de $< E, p, + >$).
4. A calcula $Q_A = k_A \cdot G$. Nótese que este no es un escalar, es un punto de E.
5. B elige $k_B <| E |$.
6. B calcula $Q_B = k_B \cdot G$.
7. A envía a B el punto Q_A.
8. B envía a A el punto Q_B.
9. A calcula $R_A = k_A \cdot Q_B$
10. B calcula $R_B = k_B \cdot Q_A$

El secreto común

Por supuesto, tanto A como B llegan al mismo punto, dado que:

$$\begin{aligned} R_B &= k_B \cdot Q_A = k_B \cdot (k_A \cdot G) \\ &= (k_B \cdot k_A) \cdot G = (k_A \cdot k_B) \cdot G \\ &= k_A \cdot (k_B \cdot G) = k_A \cdot Q_B \\ &= R_A \end{aligned}$$

Suponiendo que es difícil calcular el valor del múltiplo escalar que produce los resultados parciales y que

No hay otra manera de obtener R