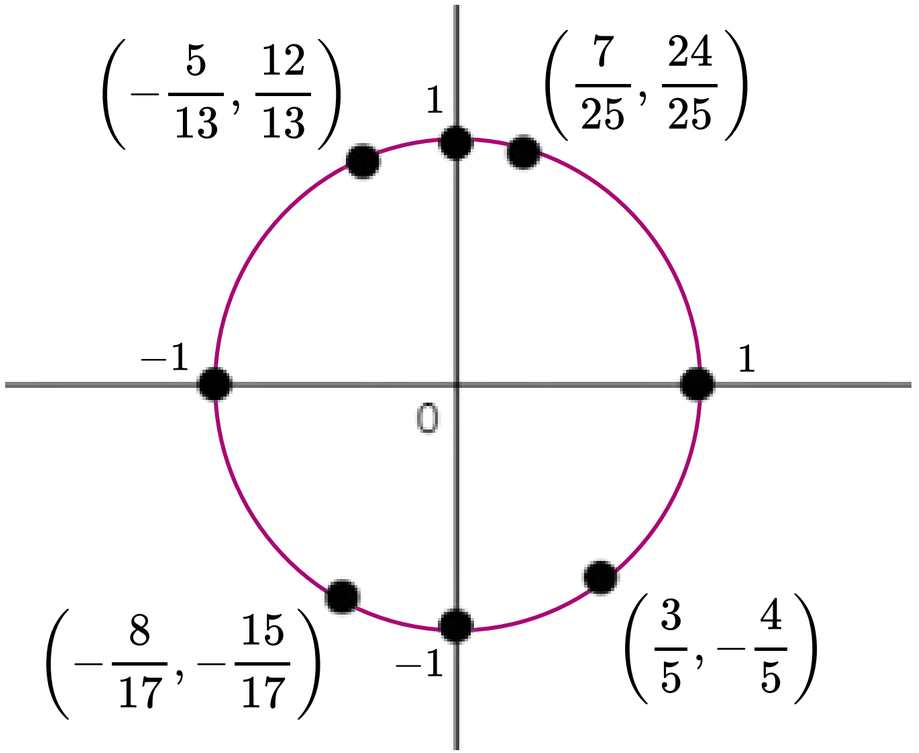
CURVAS ELÍPTICAS

JUAN PABLO CORDÓN COTERO || *cor21458@uvg.edu.gt* || **5to año**
Matemática Aplicada || *Seminario 1: Teoría de Números*

Consideremos el círculo unitario:

$$x^2 + y^2 = 1$$

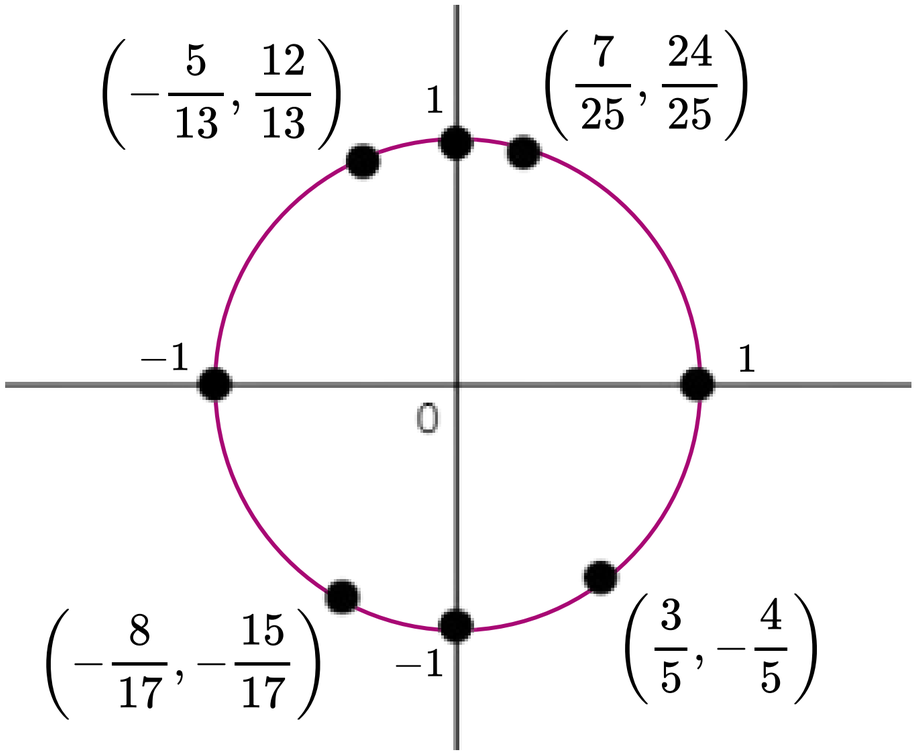
y supongamos que buscamos determinar ¿cuáles son los ***puntos racionales*** sobre el círculo?



Consideremos el círculo unitario:

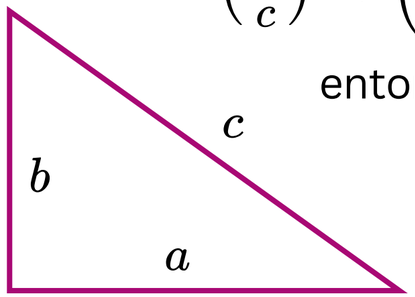
$$x^2 + y^2 = 1$$

y supongamos que buscamos determinar ¿cuáles son los ***puntos racionales*** sobre el círculo?



Existe un truco simple:

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1 \quad \Leftrightarrow \quad a^2 + b^2 = c^2$$



entonces, a, b, c forman una **terna pitagórica!!**
(si a, b, c son coprimos, una terna pitagórica primitiva)

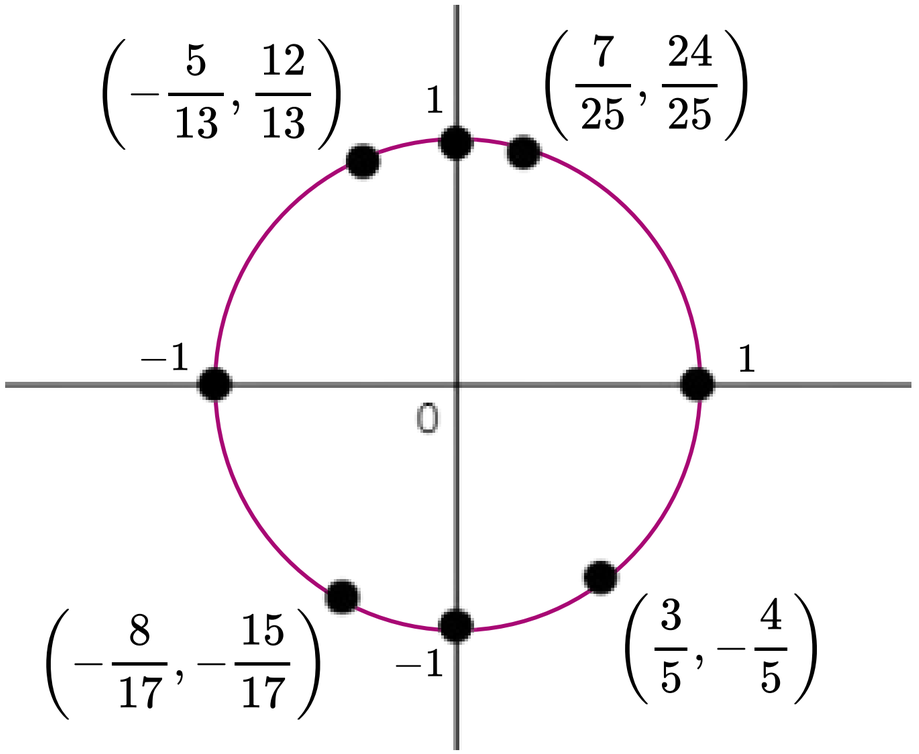
$$\left\{\begin{array}{c}\text{puntos}\\ \text{racionales}\\ \text{en el círculo}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{ternas}\\ \text{pitagóricas}\\ \text{(primitivas)}\end{array}\right\}$$

Conocemos todas las ternas pitagóricas, entonces ¡también todos los **puntos racionales del círculo!**

Consideremos el círculo unitario:

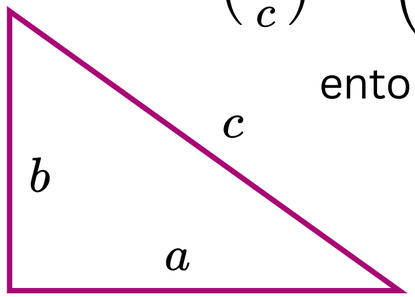
$$x^2 + y^2 = 1$$

y supongamos que buscamos determinar ¿cuáles son los ***puntos racionales*** sobre el círculo?



Existe un truco simple:

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1 \quad \Leftrightarrow \quad a^2 + b^2 = c^2$$



entonces, a, b, c forman una **terna pitagórica!!**
(si a, b, c son coprimos, una terna pitagórica primitiva)

$$\left\{\begin{array}{c}\text{puntos}\\ \text{racionales}\\ \text{en el círculo}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{ternas}\\ \text{pitagóricas}\\ \text{(primitivas)}\end{array}\right\}$$

Conocemos todas las ternas pitagóricas, entonces ¡también todos los **puntos racionales del círculo!**

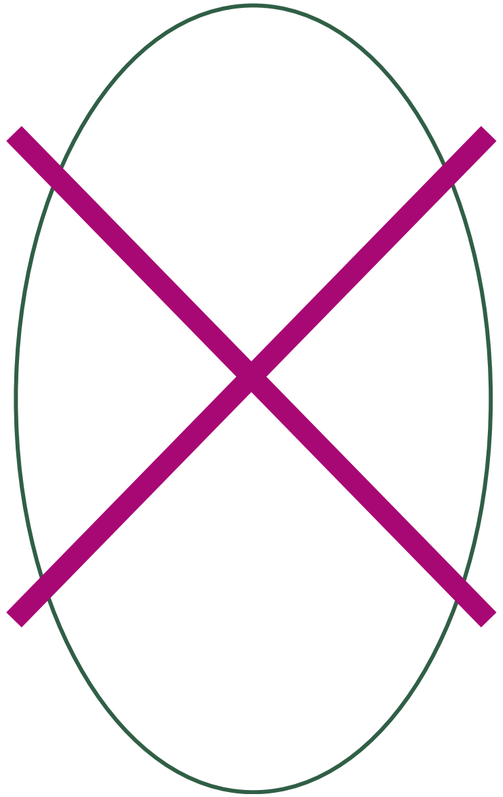
Pero... ¿qué pasa si cambiamos la ecuación ligeramente?

$$x^3 + y^2 = 1$$

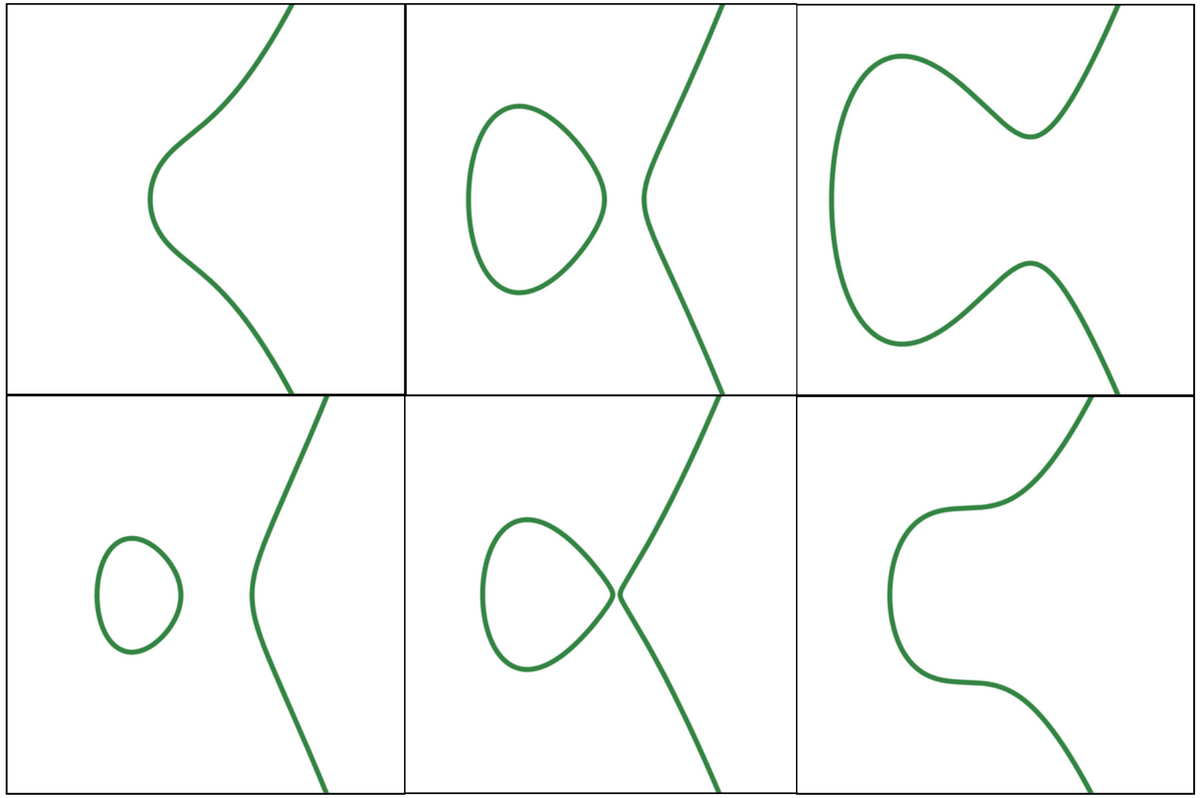
encontrar los **puntos racionales** se vuelve... ***complicado***

¿QUÉ ES UNA **CURVA ELÍPTICA**?

NO ES una elipse



Son *curvas elípticas*



¿QUÉ ES UNA **CURVA ELÍPTICA**?

Una **Curva Elíptica** E sobre un campo K es el conjunto de todos los pares (x, y) que satisfacen la ecuación:

$$y^2 = x^3 + Ax + B$$

con $A, B \in K$

Se requiere que la curva no sea *singular* es decir, que no tenga picos ni autointersecciones (es se cumple si $4A^3 + 27B^2 \neq 0$)

¿QUÉ ES UNA **CURVA ELÍPTICA**?

Una **Curva Elíptica** E sobre un campo K es el conjunto de todos los pares (x, y) que satisfacen la ecuación:

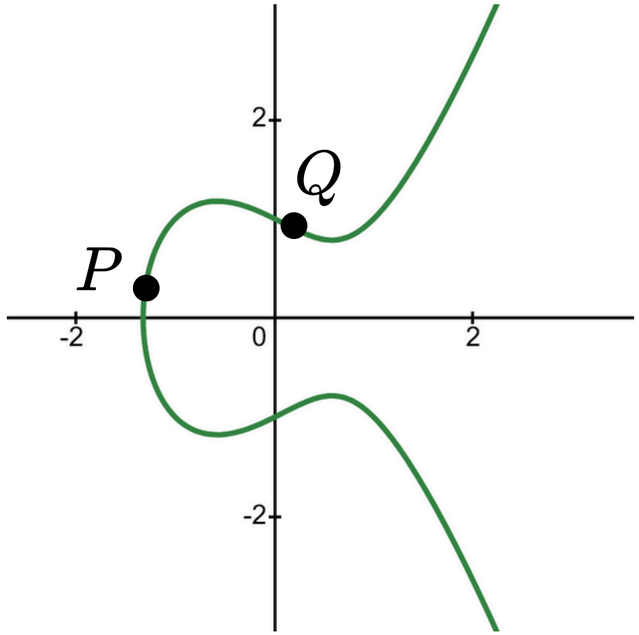
$$y^2 = x^3 + Ax + B$$

con $A, B \in K$

Se requiere que la curva no sea *singular* es decir, que no tenga picos ni autointersecciones (es se cumple si $4A^3 + 27B^2 \neq 0$)

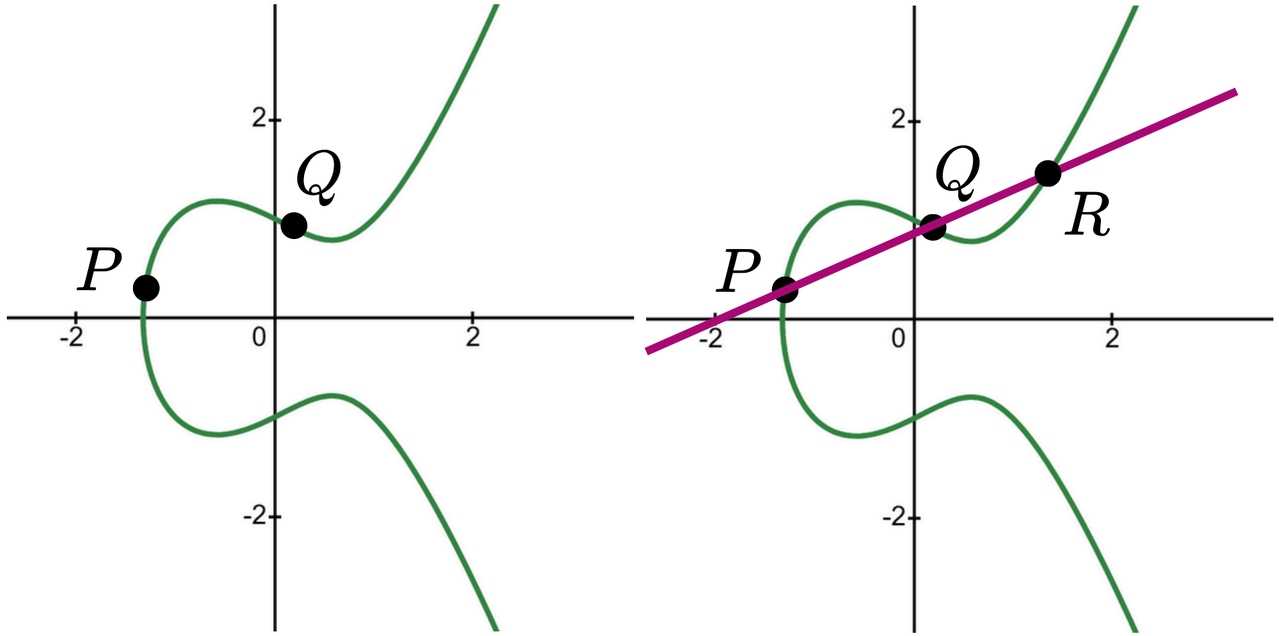
GEOMETRÍA DE **CURVAS ELÍPTICAS**

Consideremos dos puntos P y Q sobre la curva, y luego trazamos la recta a través de los puntos:



GEOMETRÍA DE **CURVAS ELÍPTICAS**

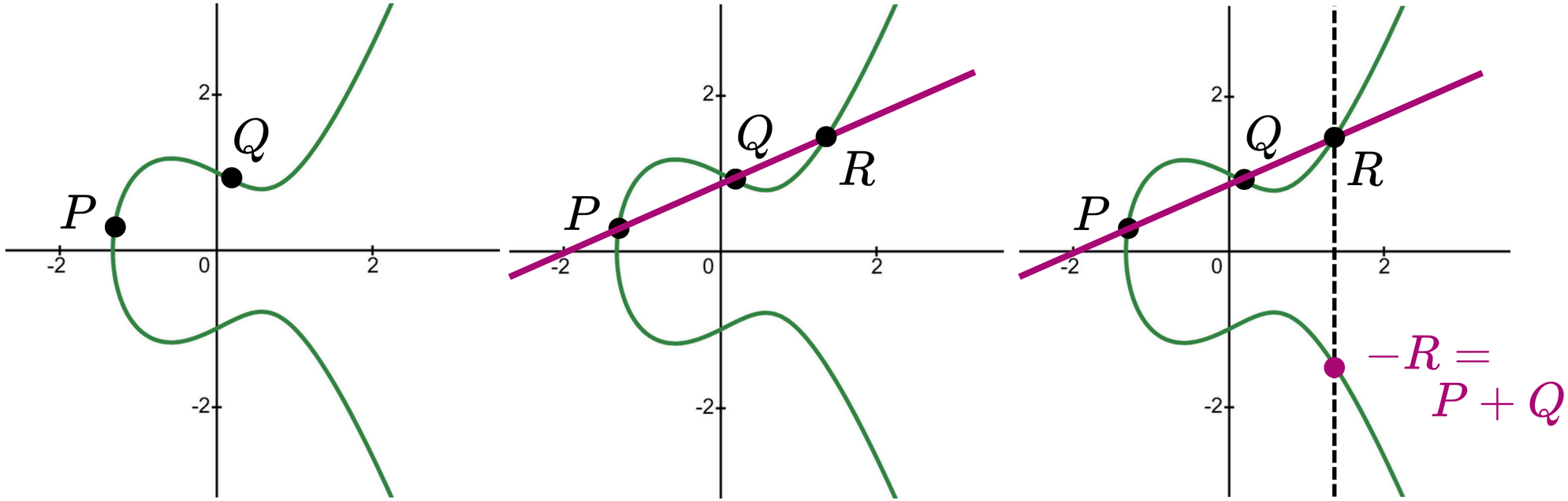
Consideremos dos puntos P y Q sobre la curva, y luego trazamos la recta a través de los puntos:



A la intersección de esta recta con la curva le llamamos R .

GEOMETRÍA DE **CURVAS ELÍPTICAS**

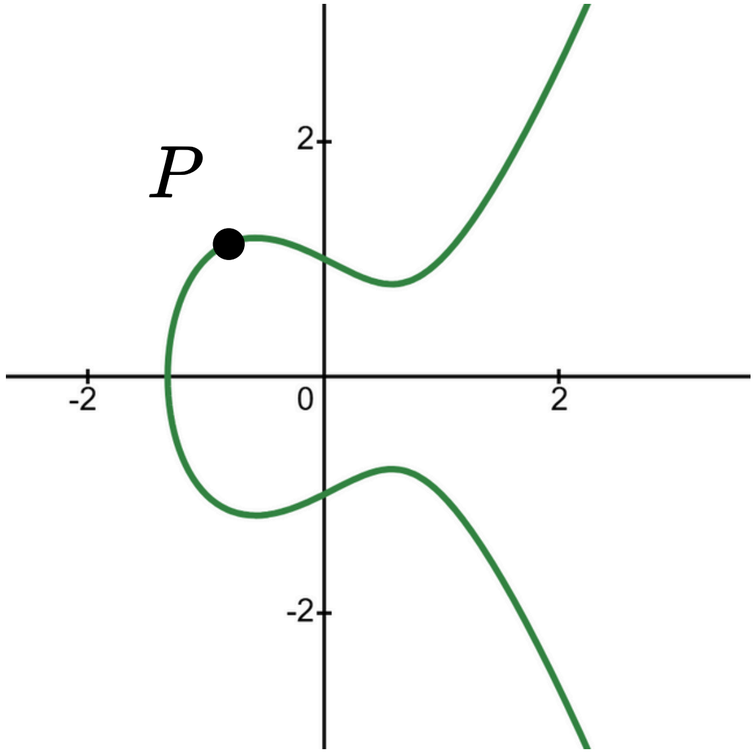
Consideremos dos puntos P y Q sobre la curva, y luego trazamos la recta a través de los puntos:



Reflejamos R horizontalmente, y a este nuevo punto $-R$ le llamamos $P + Q$. Así definimos la **suma de puntos.**

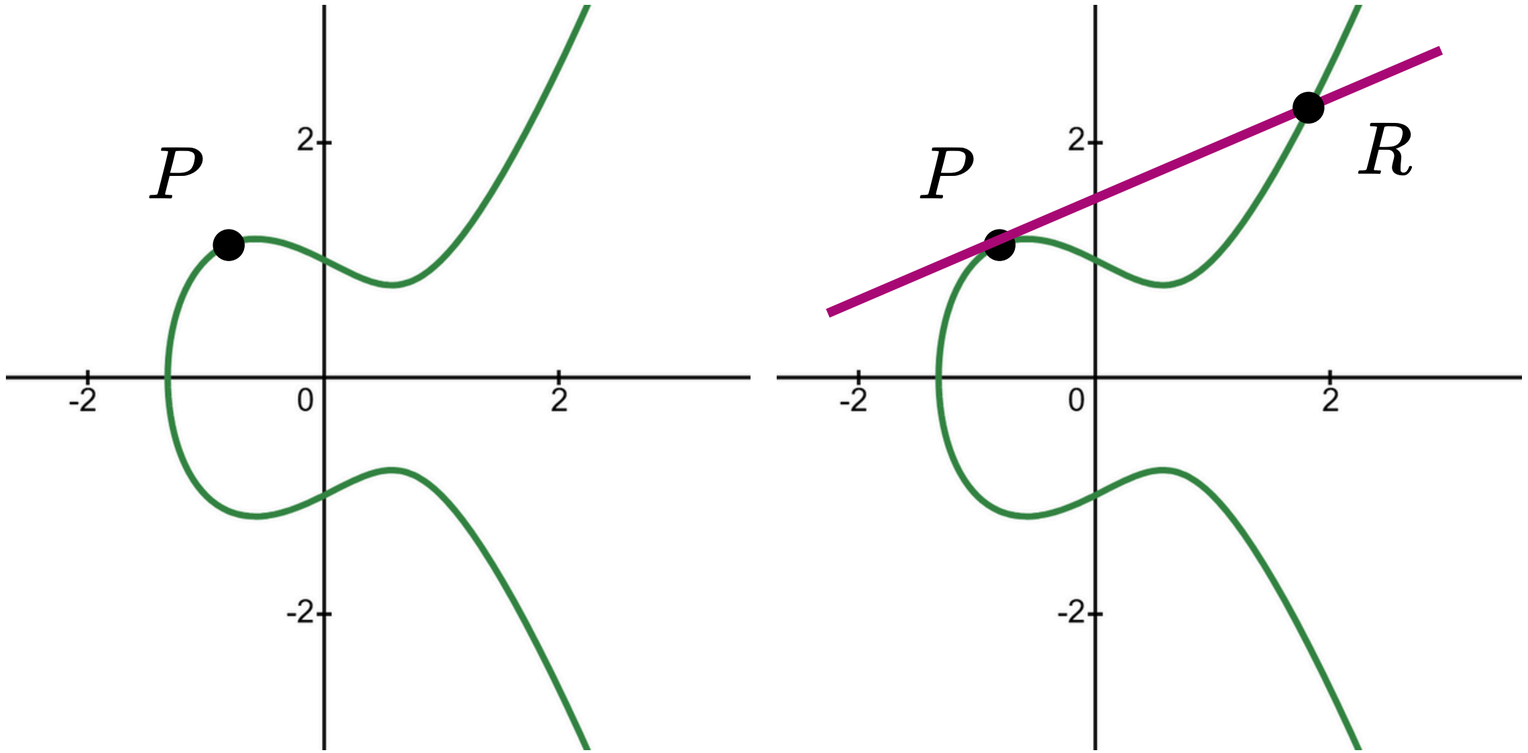
GEOMETRÍA DE **CURVAS ELÍPTICAS**

Si tenemos un solo punto, podemos sumarlo a sí mismo realizando la misma construcción, pero con la recta **tangente.**



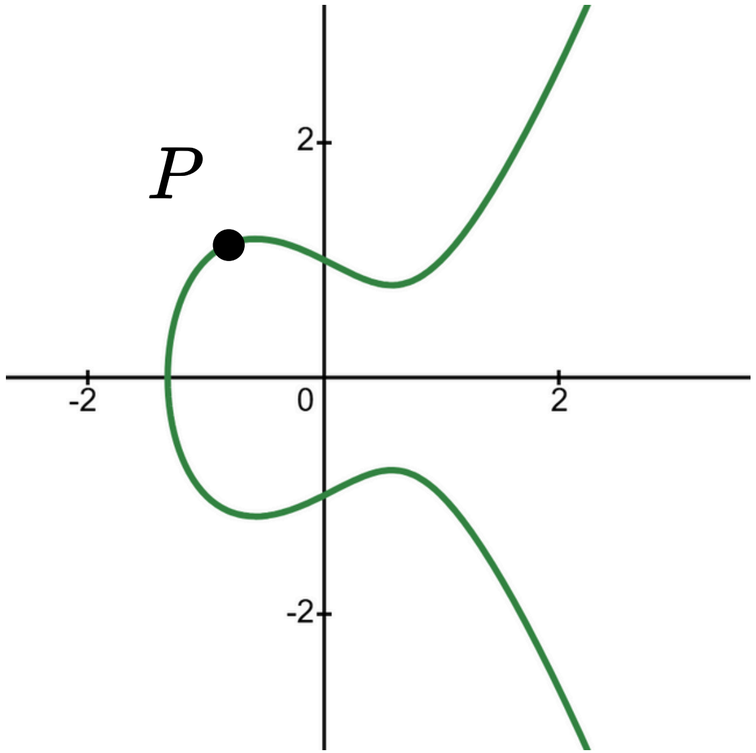
GEOMETRÍA DE **CURVAS ELÍPTICAS**

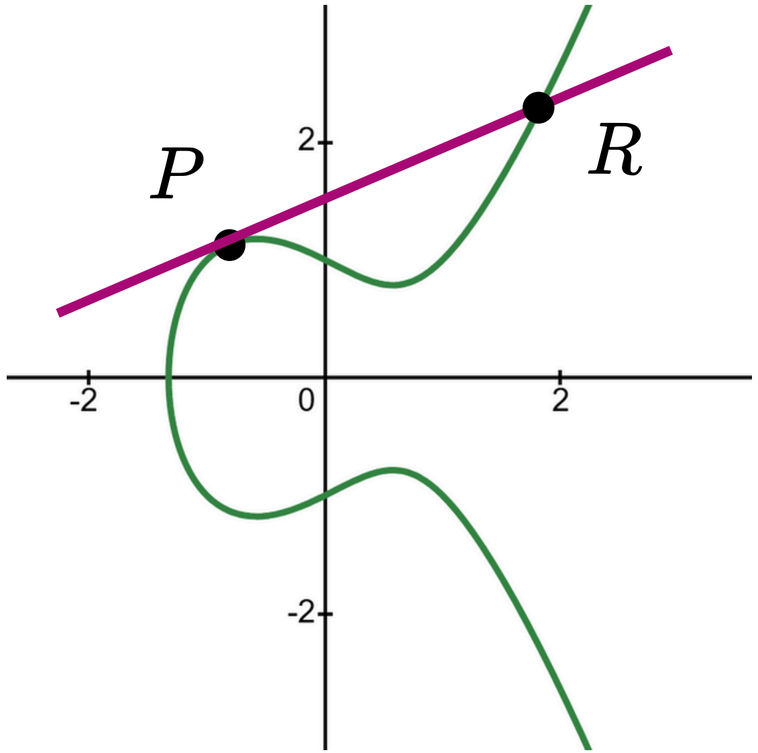
Si tenemos un solo punto, podemos sumarlo a sí mismo realizando la misma construcción, pero con la recta **tangente.**

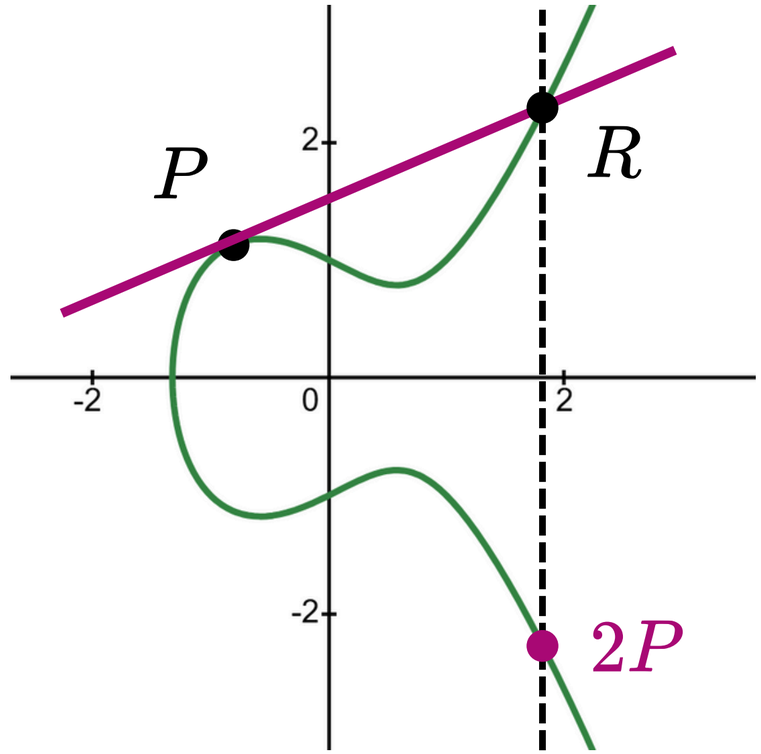


GEOMETRÍA DE **CURVAS ELÍPTICAS**

Si tenemos un solo punto, podemos sumarlo a sí mismo realizando la misma construcción, pero con la recta **tangente.**

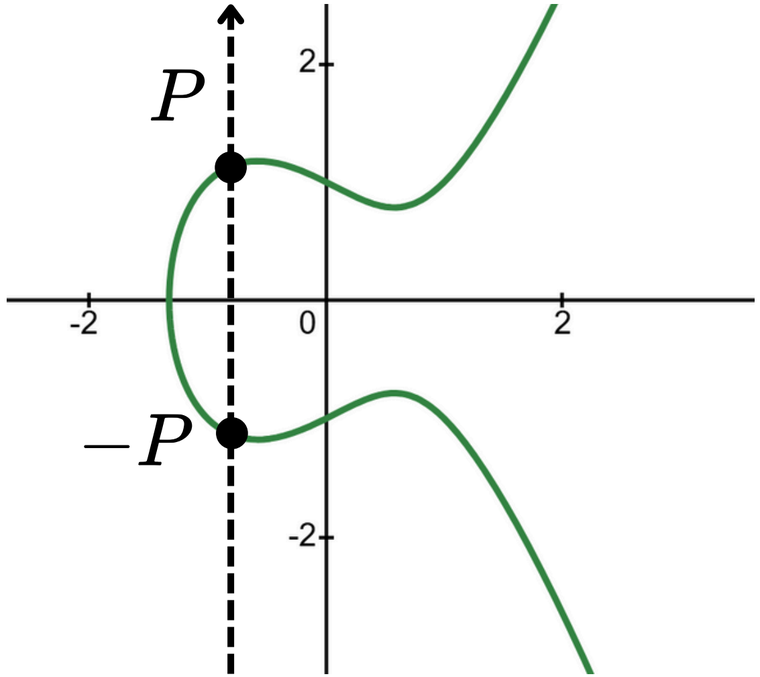






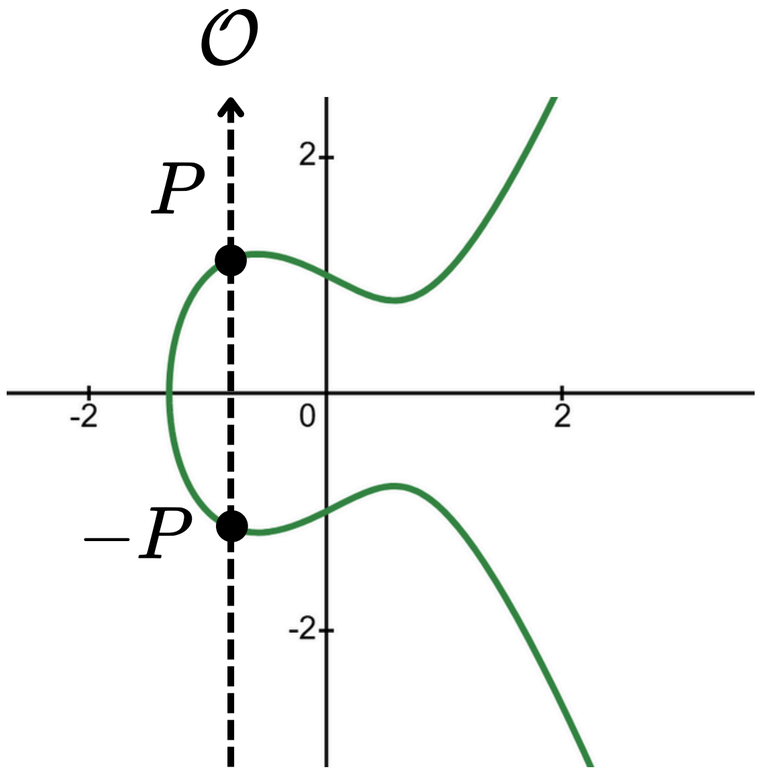
GEOMETRÍA DE **CURVAS ELÍPTICAS**

Un *gran problema* es que la línea vertical entre P y $-P$ **no intersecta la curva...** necesitamos un tercer punto para definir $P + (-P)$ ...



GEOMETRÍA DE **CURVAS ELÍPTICAS**

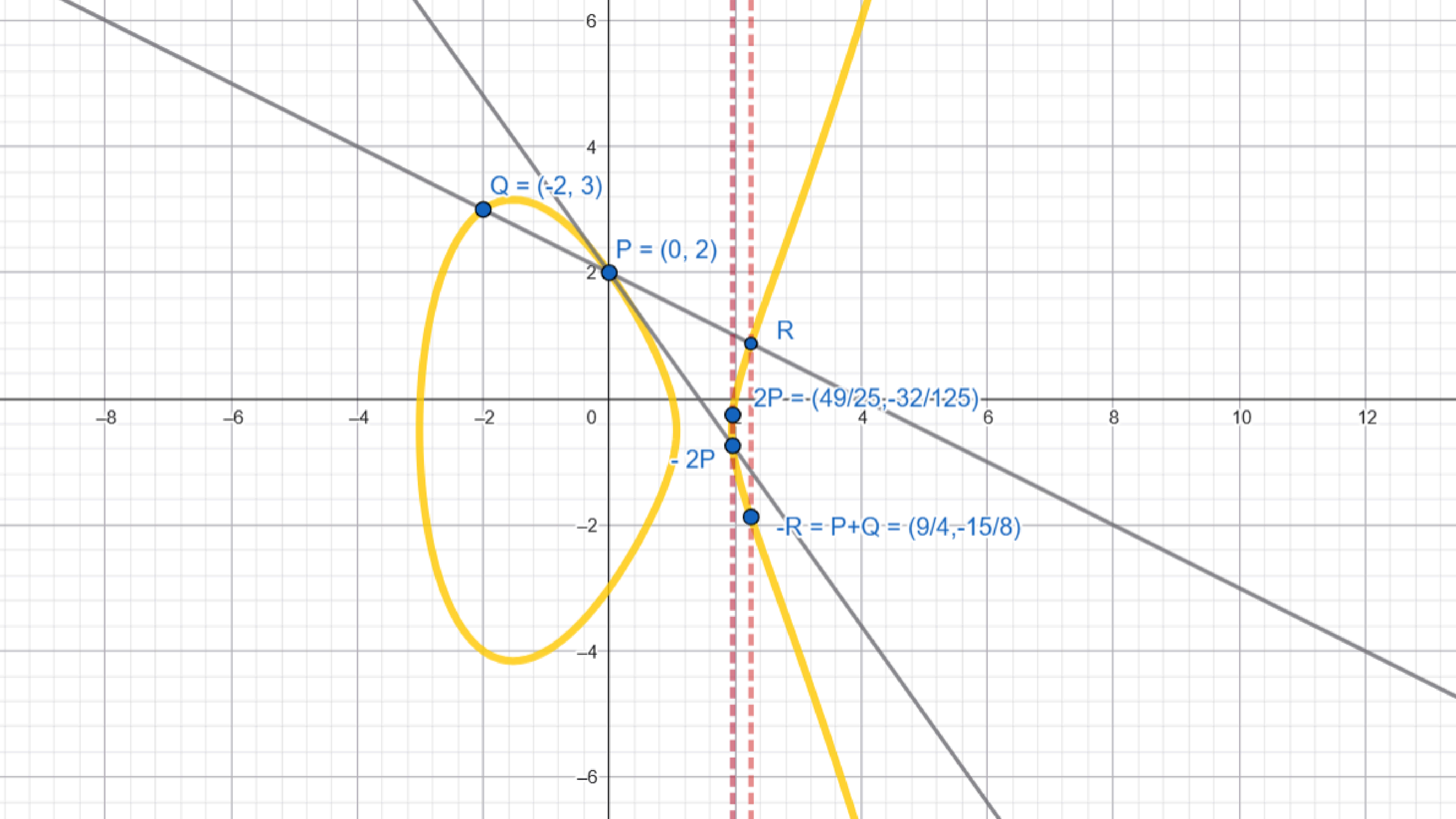
Un *gran problema* es que la línea vertical entre P y $-P$ **no intersecta la curva...** necesitamos un tercer punto para definir $P + (-P)$ ...

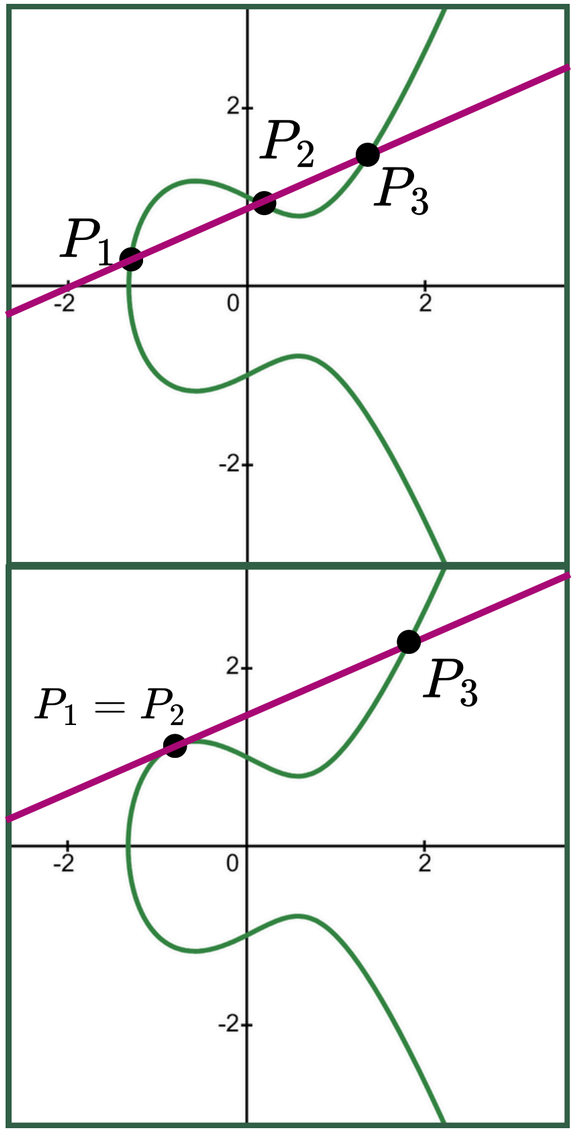


Así, definimos el **punto al infinito**

$$\mathcal{O} = P + (-P)$$

(!) Como regla, $\mathcal{O}$ es un punto en todas las líneas verticales.


Q = (-2, 3)
P = (0, 2)
R
2P = -(49/25, -32/125)
- 2P
-R = P+Q = (9/4, -15/8)
6
4
2
0
−2
−4
−6
−8
−6
−4
−2
4
6
8
10
12



FÓRMULAS DE ADICIÓN

Queremos sumar los puntos

$$P_1 = (x_1, y_1) \quad , \quad P_2 = (x_2, y_2)$$

Sobre:

$$E : y^2 = x^3 + Ax + B$$

Sea la linea que conecta a los puntos:

$$L : y = \lambda x + \nu$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{para } P_1 \neq P_2 \\ \frac{3x_1^2 + A}{2y_1} & \text{para } P_1 = P_2 \end{cases} \quad \text{y} \quad \nu = y_1 - \lambda x_1.$$

FÓRMULAS DE ADICIÓN

Encontramos la intersección de

$$E : y^2 = x^3 + Ax + B \qquad\qquad L : y = \lambda x + \nu$$

Resolviendo:

$$(\lambda x + \nu)^2 = x^3 + Ax + B$$

FÓRMULAS DE ADICIÓN

Encontramos la intersección de

$$E : y^2 = x^3 + Ax + B \qquad\qquad L : y = \lambda x + \nu$$

Resolviendo:

$$(\lambda x + \nu)^2 = x^3 + Ax + B$$

Sabemos que x_1, x_2 son soluciones, por lo que podemos computar x_3

$$\begin{aligned} x^3 + Ax + B - (\lambda x + \nu)^2 &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3. \end{aligned}$$

FÓRMULAS DE ADICIÓN

Encontramos la intersección de

$$E : y^2 = x^3 + Ax + B \qquad\qquad L : y = \lambda x + \nu$$

Resolviendo:

$$(\lambda x + \nu)^2 = x^3 + Ax + B$$

Sabemos que x_1, x_2 son soluciones, por lo que podemos computar x_3

$$\begin{aligned} x^3 + Ax + B - (\lambda x + \nu)^2 &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3. \end{aligned}$$

Igualando los coeficientes de x^2 obtenemos

$$-\lambda^2 = -x_1 - x_2 - x_3 \Rightarrow \boxed{x_3 = \lambda^2 - x_1 - x_2}$$

FÓRMULAS DE ADICIÓN

Encontramos la intersección de

$$E : y^2 = x^3 + Ax + B \qquad\qquad L : y = \lambda x + \nu$$

Resolviendo:

$$(\lambda x + \nu)^2 = x^3 + Ax + B$$

Sabemos que x_1, x_2 son soluciones, por lo que podemos computar x_3

$$\begin{aligned} x^3 + Ax + B - (\lambda x + \nu)^2 &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3. \end{aligned}$$

Igualando los coeficientes de x^2 obtenemos

$$-\lambda^2 = -x_1 - x_2 - x_3 \Rightarrow \boxed{x_3 = \lambda^2 - x_1 - x_2} \quad \text{y} \quad \boxed{y_3 = \lambda x_3 + \nu}$$

y finalmente: $\boxed{P_1 + P_2 = (x_3, -y_3)}$

FÓRMULAS DE ADICIÓN

Algoritmo de adición en curvas elípticas:

- Si $P_1 \neq P_2$ y $x_1 = x_2$, entonces $P_1 + P_2 = \mathbb{O}$.
- Si $P_1 = P_2$ y $y_1 = 0$, entonces $P_1 + P_2 = 2P_1 = \mathbb{O}$.
- Si $P_1 \neq P_2$ (y $x_1 \neq x_2$),

  entonces $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ y $\nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$.
- Si $P_1 = P_2$ (y $y_1 \neq 0$),

  entonces $\lambda = \frac{3x_1^2 + A}{2y_1}$ y $\nu = \frac{-x^3 + Ax + 2B}{2y}$.

Luego,

$$P_1 + P_2 = \left(\lambda^2 - x_1 - x_2 - \lambda^3 + \lambda(x_1 + x_2) - \nu\right).$$

ÁLGEBRA DE **CURVAS ELÍPTICAS**

La suma de puntos en una curva elíptica E sobre un campo K cumple las siguientes propiedades:

- $P + \mathcal{O} = \mathcal{O} + P = P$
- $P + (-P) = \mathcal{O}$
- $P + Q = Q + P$
- $P + (Q + R) = (P + Q) + R$

$\forall P, Q, R \in E$

Es decir, es un **grupo abeliano.** (Poincaré, 1901)

ÁLGEBRA DE **CURVAS ELÍPTICAS**

La suma de puntos en una curva elíptica E sobre un campo K cumple las siguientes propiedades:

- $P + \mathcal{O} = \mathcal{O} + P = P$
- $P + (-P) = \mathcal{O}$
- $P + Q = Q + P$
- $P + (Q + R) = (P + Q) + R$ $\quad \forall P, Q, R \in E$

Es decir, es un **grupo abeliano.** (Poincaré, 1901)

Teorema: (Mordell, 1922) Los puntos racionales sobre una curva elíptica forman un **grupo abeliano finitamente generado.**

Es decir, existen finitos $P_1, P_2, \ldots, P_n \in E(\mathbb{Q})$ tal que $P \in E(\mathbb{Q})$ puede ser expresado:

$$P = k_1P_1 + k_2P_2 + \ldots + k_nP_n \qquad k_1, k_2, \ldots, k_n \in \mathbb{Z}$$

A estos $P_1, P_2, \ldots, P_n$ les llamamos **generadores,** y con ellos puedo encontrar **todos los puntos racionales!!**

ÁLGEBRA DE **CURVAS ELÍPTICAS**

Teorema: (Mordell, 1922) Los puntos racionales sobre una curva elíptica forman un **grupo abeliano finitamente generado.**

Es decir, existen finitos $P_1, P_2, \ldots, P_n \in E(\mathbb{Q})$ tal que $P \in E(\mathbb{Q})$ puede ser expresado:

$$P = k_1P_1 + k_2P_2 + \ldots + k_nP_n \qquad k_1, k_2, \ldots, k_n \in \mathbb{Z}$$

A estos $P_1, P_2, \ldots, P_n$ les llamamos **generadores,** y con ellos puedo encontrar **todos los puntos racionales!!**

El teorema fundamental de grupos abelianos finitamente generados nos dice entonces que:

$$E(Q) \cong (\text{Grupo finito}) \times \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{\textbf{r} \text{ veces}}$$

ÁLGEBRA DE **CURVAS ELÍPTICAS**

$$E(Q) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

$E(\mathbb{Q})_{tors}$ es el grupo finito, conocido como **grupo de torsión de** $E(\mathbb{Q})$

r es un entero conocido como **rango de** $E(\mathbb{Q})$

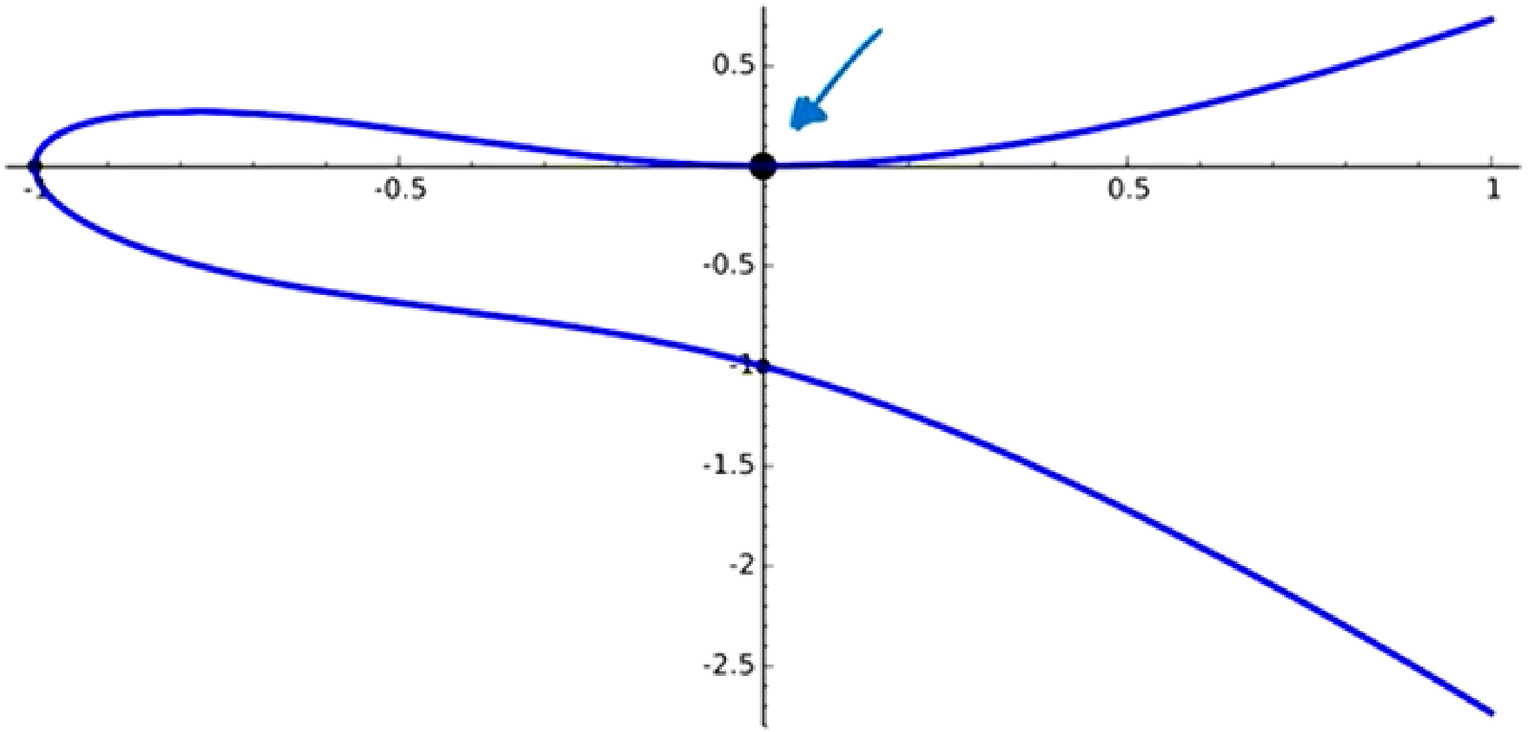
ÁLGEBRA DE **CURVAS ELÍPTICAS**

$$E(Q) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

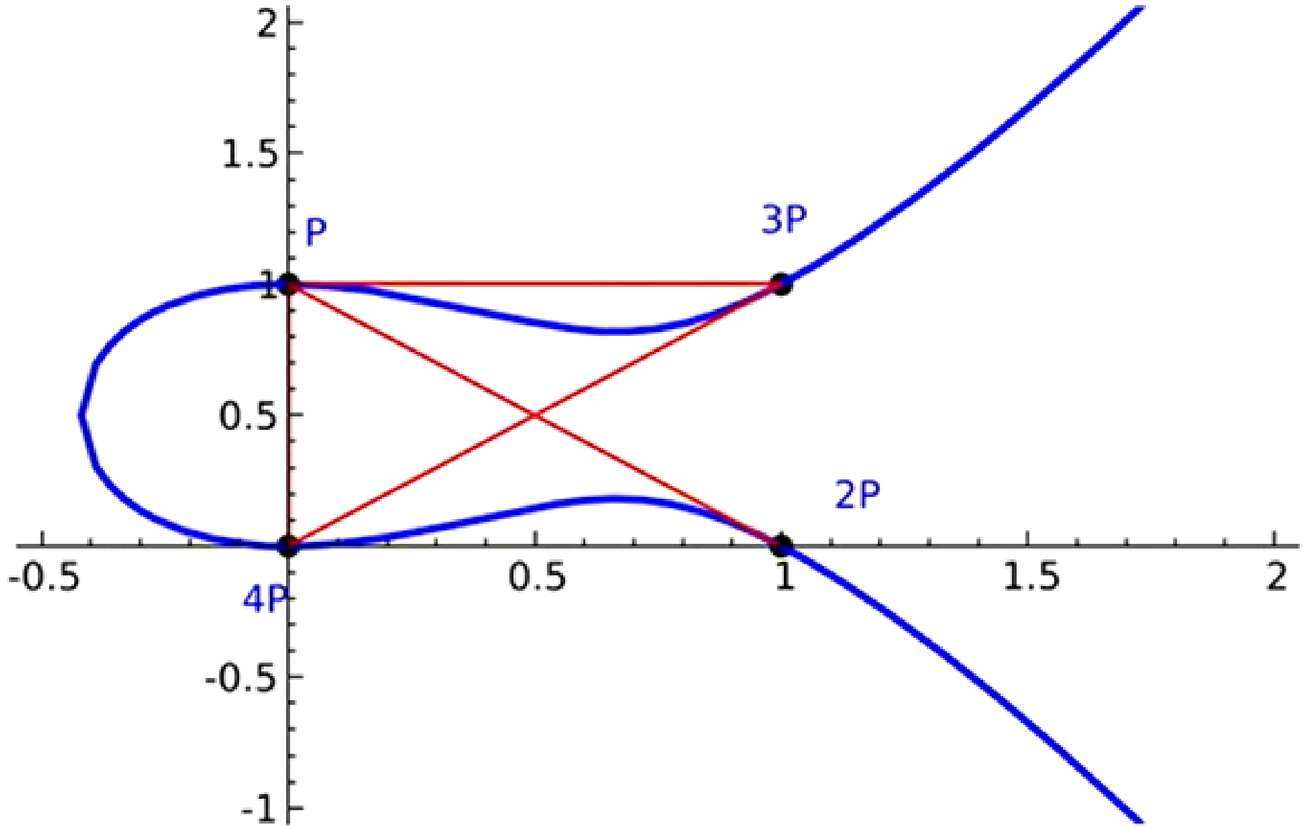
¿Qué grupos de torsión $E(\mathbb{Q})_{tors}$ son posibles?

Teorema: (Mazur, 1977) El subgrupo de torsión del grupo de puntos racionales $E(\mathbb{Q})_{tors}$ sobre una curva elíptica debe ser uno de los siguientes 15 grupos:

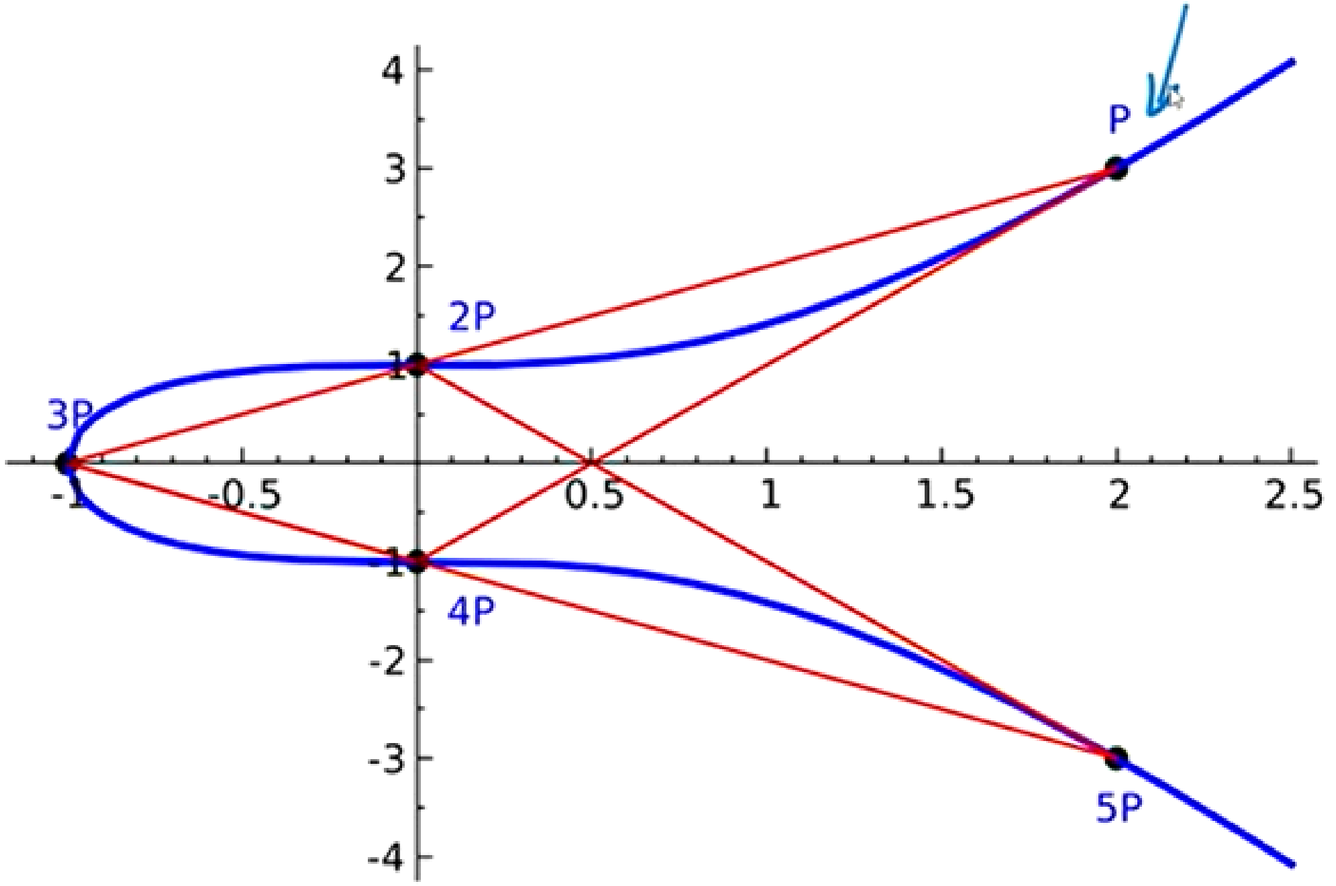
- C_N con $1 \leq N \leq 10$ o $N = 12$,
- $C_2 \times C_{2N}$ con $1 \leq N \leq 4$.



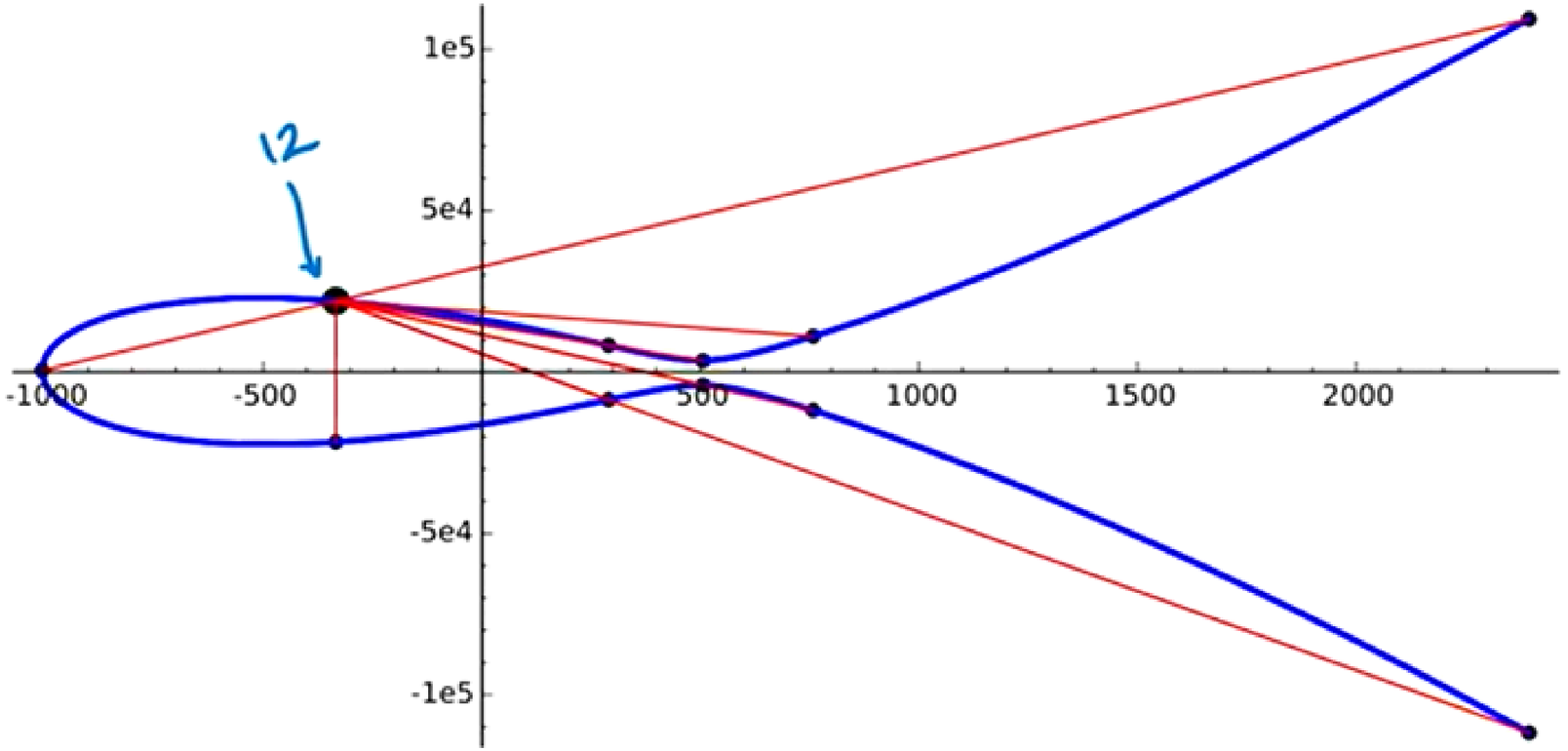
The elliptic curve $E/\mathbb{Q} : y^2 + xy + y = x^3 + x^2$
has a point $P = (0, 0)$ of order 4.



The curve $E/\mathbb{Q} : y^2 - y = x^3 - x^2$ has a point $P = (0, 1)$ of order 5.



The elliptic curve $E/\mathbb{Q} : y^2 = x^3 + 1$ has a point $P = (2, 3)$ of order 6.



The elliptic curve `30030bt1` has a point of order 12.

$$y^2 + xy = x^3 - 749461x + 263897441$$

ÁLGEBRA DE **CURVAS ELÍPTICAS**

$$E(Q) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

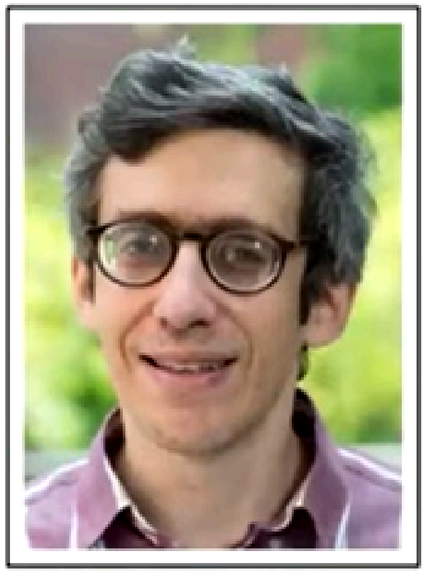
¿Qué rangos r son posibles?

PROBLEMA ABIERTO:
¿Qué valores puede tomar r ? ¿Puede tomar valores arbitrariamente grandes o está acotado?

CONJETURA Park, Poonen, Voight, Wood (2016):
Los rangos r están acotados, existen solo finitos valores de rangos mayores a 21

Example (2006): Elkies' elliptic curve of rank ≥ 28 ($= 28$ under GRH!)

$$y^2 + xy + y = x^3 - x^2 - (20067762415575526585033208209338542750930230312178956502)x + (3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9)$$



Noam Elkies

Independent points of infinite order:

$$P_1 = [-212415009125438107329213746 3, 259854492051899599030515511070780628911531]$$

$$P_2 = [233450986603470175688475453 7, 188720041954944691808683165528036279315 31]$$

$$P_3 = [-167173605406236906387903866 3, 251709377261144287808506947241319126049131]$$

$$\vdots$$

REFERENCIAS

- H. Silverman, J. (2006). An Introduction to the Theory of Elliptic Curves [Diapositivas]. Summer School On Computational Number Theory And Applications To Cryptography University Of Wyoming, Estados Unidos. *https://www.math.brown.edu/johsilve/Presentations/WyomingEllipticCurve.pdf*
- Aleph 0. (2025, 9 marzo). Math isn’t ready to solve this problem [Vídeo]. YouTube. *https://www.youtube.com/watch?v=6gCaEeBNlnk*
- Alvaro Lozano-Robledo. (2021, 14 enero). What is. . . an elliptic curve? [Vídeo]. YouTube. *https://www.youtube.com/watch?v=A2KNrgiWquU*

REFERENCIAS