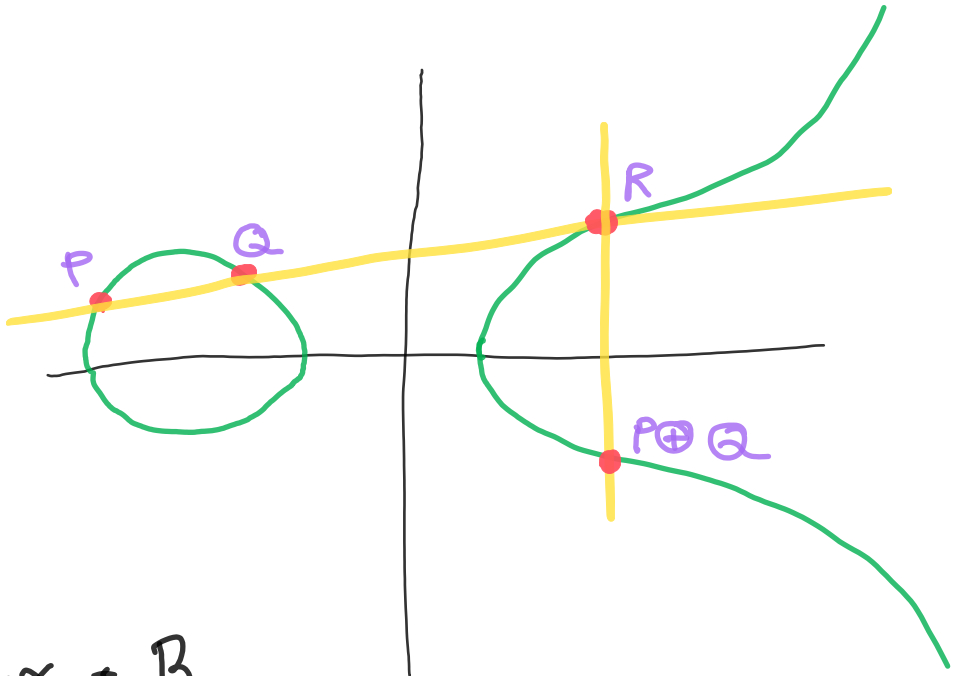
Introducción a las Curvas Elípticas



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

95% of people cannot solve this!



Can you find positive whole values

for 🍎, 🍌, and 🍍?

Here is the simplest solution:

apple = 154476802108746166441951315019919837485664325669565431700026634898253202035277999

banana = 368751317941299998271978115652254748254929799689719709962831374716372246340555 79

pineapple = 437361267792869725786125260237139015281653755816161361862143799337842346777 2036

Ej Hay tres números enteros consecutivos cuyo producto sea un cuadrado?

$$0 \cdot 1 \cdot 2 = 0 = 0^2$$

$$(-1) \cdot 0 \cdot 1 = 0 = 0^2$$

$$(-2)(-1) \cdot 0 = 0 = 0^2$$

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

e)

$$x(x+5)(x+10) = y^2$$

$$0 \cdot 5 \cdot 10 = 0^2$$

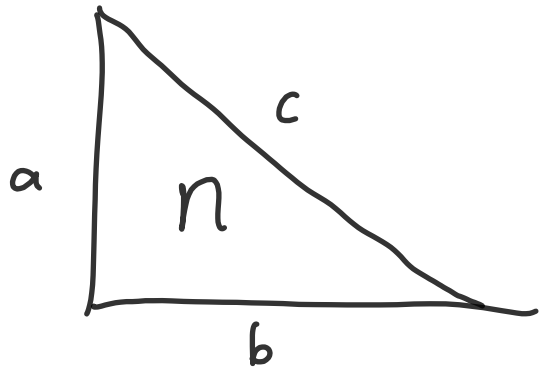
$$(-9)(-9+5)(-9+10) = 36 = 6^2$$

$$40 \cdot 45 \cdot 50 = 300^2$$

$$\left(\tfrac{5}{4}\right) \cdot \left(\tfrac{5}{4}+5\right)\left(\tfrac{5}{4}+10\right) = \left(\frac{75}{8}\right)^2$$

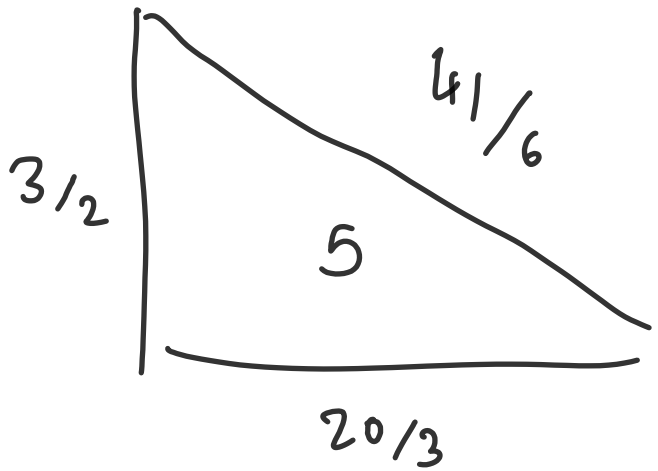
$$x = -9, 40, \tfrac{5}{4}, \frac{-50}{9}, \frac{961}{144}, \frac{7700}{96}, \ldots$$

Ej ¿Qué números $n \geq 1$ son el área de un triángulo recto con lados de long. racional?



$a, b, c \in \mathbb{Q}$

$n = 5$



n es "congruente" si y solo si: la curva

$$y^2 = x^3 - n^2 x$$

tiene un punto (x,y) con $y \neq 0$. $\longrightarrow \in \mathbb{Q} \times \mathbb{Q}$

$C_n = \{(a,b,c) : a^2+b^2=c^2,\ \frac{ab}{2} = n\}$

$E_n = \{(x,y) : y^2 = x^3 - n^2 x,\ y \neq 0\}$

$f : C_n \longrightarrow E_n$

$(a,b,c) \longmapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right)$

$(x,y) \longmapsto \left(\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y}\right)$

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

$\Updownarrow$

$y^2 = (x-1)x(x+1) = x^3 - x$

Ej $x^n + y^n = z^n \quad n > 2$

y con $x \cdot y \cdot z \neq 0$

no tiene soluciones enteras.

(El último teorema de Fermat)

$p > 2$

$a^p + b^p = c^p$

$n = 2 \quad x^2 + y^2 = z^2 \quad (m^2 - n^2, 2mn, m^2 + n^2)$

$m, n \in \mathbb{Z}$

$E: y^2 = x(x - a^p)(x + b^p)$

Ecuaciones Diofánticas

$$C: f(x_1, x_2, \dots, x_n) = 0$$

f un polinomio en n variables y coeficientes enteros

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

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

$$x^2 - 2y^2 = 1$$

$$3x + 5y = 7$$

$f(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$

Encontrar todas las soluciones de $f = 0$ con coordenadas en

- $\mathbb{N} = \{1, 2, 3, \dots\}$
- $\mathbb{Z} = \{\dots -2, -1, 0, 1, \dots\}$
- $\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z},\ n \neq 0 \right\}$

- $n = 1$ $\quad f(x) = 0$, $a_k \in \mathbb{Z}$.

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$$

THM $\quad \frac{m}{n} \in \mathbb{Q}$, $f\left(\frac{m}{n}\right) = 0 \Longrightarrow m \mid a_0$, $n \mid a_n$

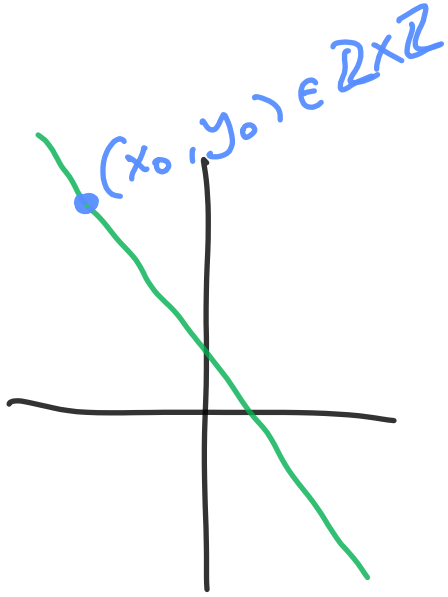
$\gcd(m, n) = 1$

↑

a_0 es múltiplo de m ó m es un divisor de a_0.

- $n = 2$ $\quad gr(f) = 1$

$L: ax + by = c$, $a, b, c \in \mathbb{Z}$.



THM L tiene puntos enteros si y solo si

$$\gcd(a, b) \mid c.$$

$L \quad ax + by$

THM L tiene puntos enteros si y solo si

$$\gcd(a,b) \mid c.$$

Ej $L: 3x + 6y = 1 \qquad L(\mathbb{Z}) = \emptyset$

$L': 3x + 5y = 1 \qquad L'(\mathbb{Z}) \neq \emptyset$

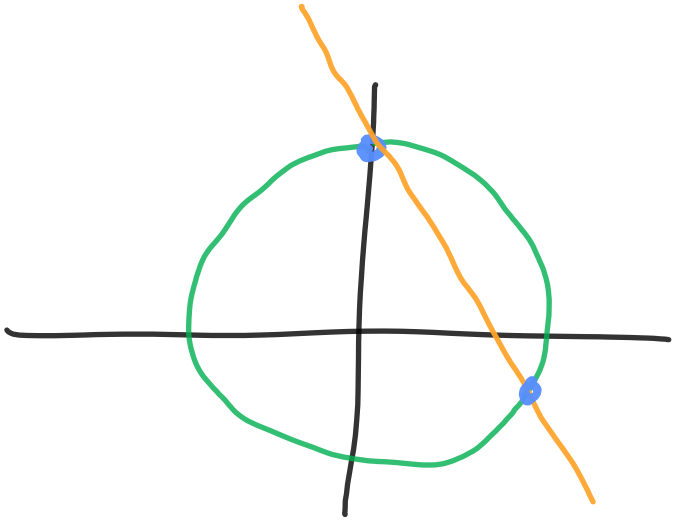
$(2,-1) \in L'(\mathbb{Z}) \qquad \# L'(\mathbb{Z}) = \infty$

- $n = 2$ $\quad \deg(f) = 2$

$a, b, c \ldots \in \mathbb{Z}$.

$$ax^2 + by^2 + cxy + ex + fy + g = 0$$





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

- $n=2$ $\quad \deg(f) = 3$ $\quad \not\exists$
- $E: ax^3 + bxy^2 + cx^2y + dy^3 + \cdots = 0$
- non-singular
- un punto $O \in E(\mathbb{Q})$.

$$3x^3 + 4y^3 + 5 = 0$$

Hasse-Minkowski

C conica $/\mathbb{Q}$

$C(\mathbb{R}) \neq \emptyset$

$C(\mathbb{Q}_p) \neq \emptyset \quad \forall p$

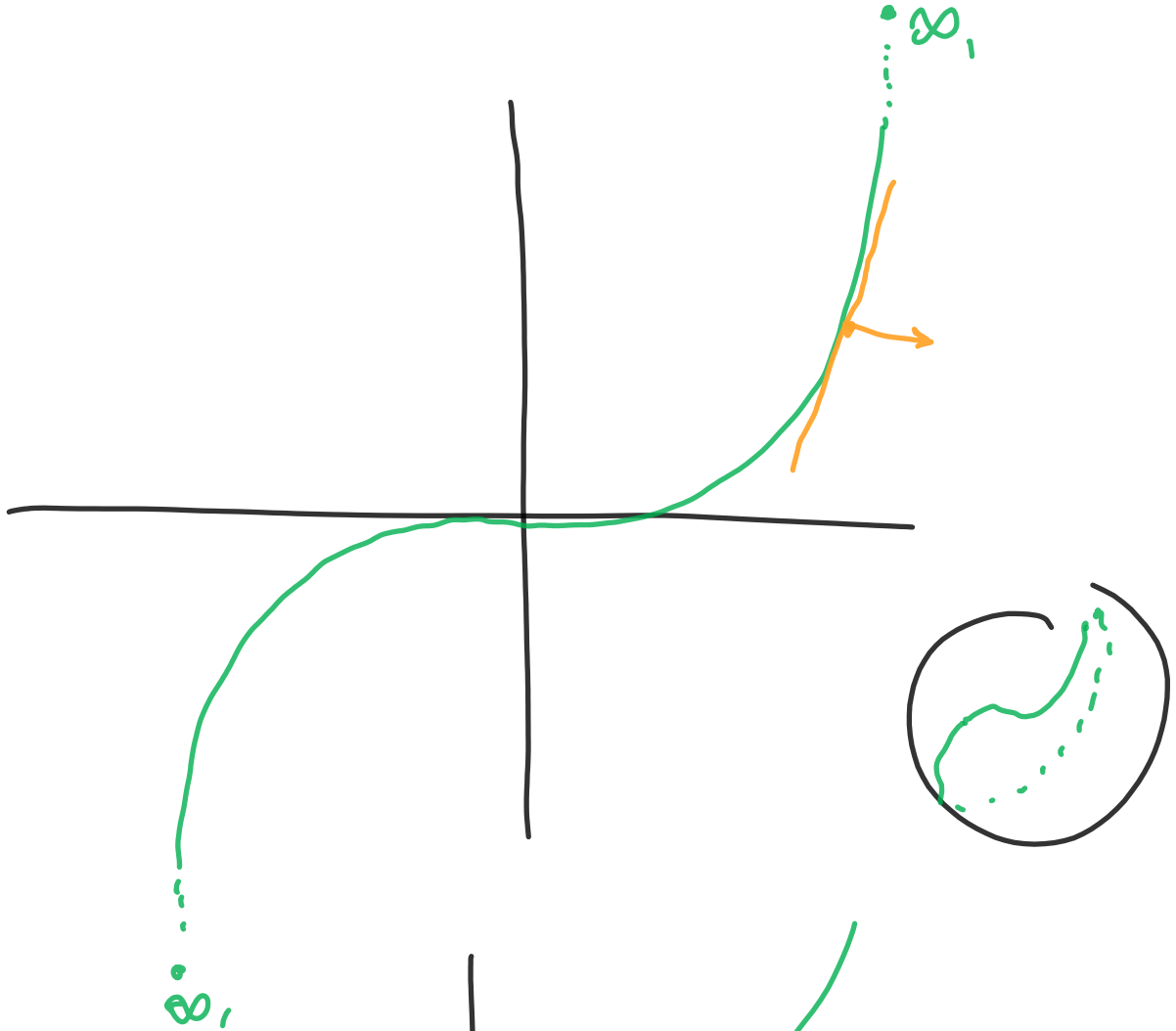
$\longrightarrow C(\mathbb{Q}) \neq \emptyset.$

Ej $y = x^3$

$f = x^3 - y = 0$

$\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right)$

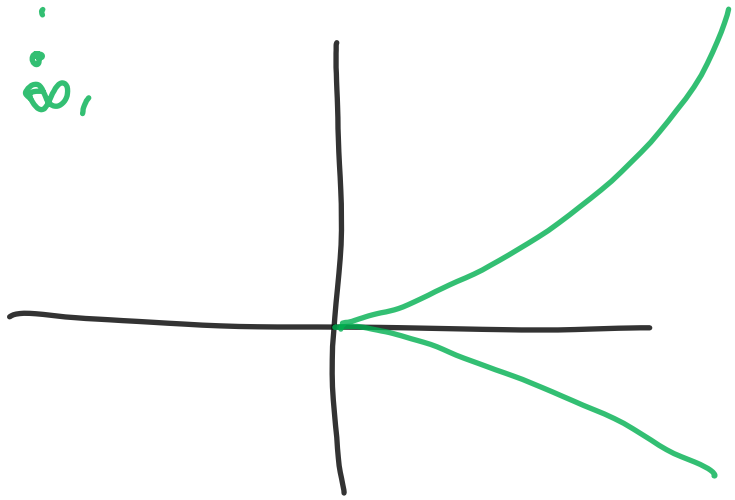
$= (3x^2, -1)$



$x^3 - y^2 = 0$ $\quad y^2 = x^3$

$(3x^2, -2y)\Big|_{(0,0)} = (0,0)$

$\Rightarrow$



Ej $C: y = x^3$ $\quad x^3 - y = 0$ (afín)

$\hat{C}: z^2 y = x^3$ $\quad x^3 - y z^2 = 0$ (proy)

$$\hat{C}(\mathbb{Q}) = \{ [x,y,z] : x^3 - y z^2 = 0 \}$$

$$[3,27,1] = [6,54,2] \quad \text{(afín)}$$

$$C(\mathbb{Q}) = \{ [x,y,1] : x^3 - y \cdot 1 = 0 \}$$

$z^2 y = x^3$ $\qquad z = 0 \implies x = 0$

$\searrow [0, 1, 0] = \infty.$

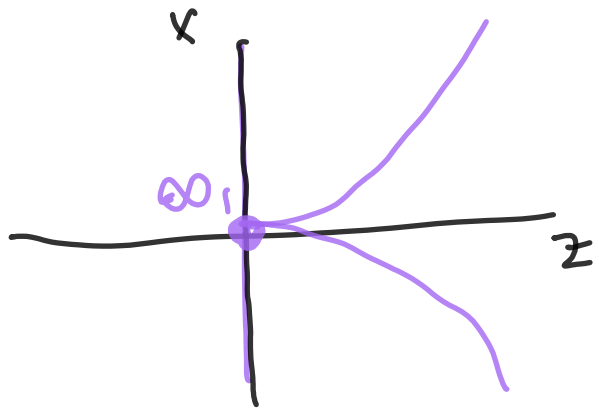


$\hat{\mathbb{C}}(\mathbb{R}) = \mathbb{C}(\mathbb{R}) \cup \infty,$

Carta $\{z = 1\}$

Carta $\{y = 1\}$

$\{[x, 1, z] : z^2 = x^3\}$



$F = x^3 - z^2 y = 0$

$\left(\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}, \frac{\partial F}{\partial z}\right) = (3x^2, -z^2, -2yz)$

$= (0, 0, 0) \Rightarrow x = 0, z = 0$

$\Rightarrow [0, 1, 0]$ es singular

$\in C$

Ej $y^2 = x^3 - x \rightsquigarrow zy^2 = x^3 - z^2x$

$F = 0, \quad x^3 - xz^2 - y^2z = 0$

$$\begin{cases} \frac{\partial F}{\partial x} = 3x^2 - z^2 \\ \frac{\partial F}{\partial y} = -2yz \\ \frac{\partial F}{\partial z} = -y^2 - 2xz \end{cases}$$

Def Una curva elíptica sobre $\mathbb{Q}$, $E/\mathbb{Q}$, es una curva cubica proyectiva suave, con por lo menos un punto racional $\mathcal{O} \in E(\mathbb{Q})$, que llamamos el origen, o el zero de E.

$$F(x, y, z) = 0$$

(proj) $ax^3 + by^3 + cz^3 + \cdots = 0$

$z y^2 = x^3 - xz^2$

Ej $y^2 = x^3 - x$

$\mathcal{O} = [0, 1, 0]$

(afín) $\downarrow$

$ax^3 + by^3 + c + \cdots$

Prop Sea $(E, \mathcal{O})$ una curva elíptica / $\mathbb{Q}$ (cuerpo de característica $\neq 2, 3$)

Entonces existe otra curva el. $\hat{E}$

$$\hat{E}: zy^2 = x^3 + Axz^2 + Bz^3 \quad , A, B \in \mathbb{Q}$$

$$(\text{afín}: \quad y^2 = x^3 + Ax + B) \qquad 4A^3 + 27B^2 \neq 0$$

y una función invertible $\psi: E \longrightarrow \hat{E}$ ← un modelo de Weierstrass.

$$\psi([x,y,z]) = \left[\frac{f_1}{g_1}, \frac{f_2}{g_2}, \frac{f_3}{g_3}\right]$$

f_i, g_i son polinomios con coeff. en $\mathbb{Q}$

y tal que $\psi(\mathcal{O}) = [0,1,0]$

Ej $E: x^3 + y^3 = d$

$\hookrightarrow x^3 + y^3 = d z^3$

$\theta = [1, -1, 0]$

$E': y^2 + 9dy = x^3 - 27d^2$

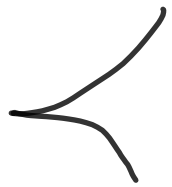
$E'': y^2 = x^3 - 432d^2$

$$y^2 = x^3 + Ax + B \quad , A, B \in \mathbb{Q}$$

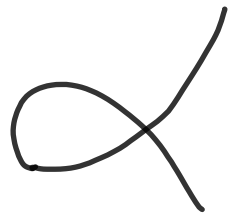
$$(4A^3 + 27B^2 \neq 0.)$$

Suave

$y^2 = x^3$



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



$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad , a_i \in \mathbb{Q}$$

$(x, y) \mapsto \left(\frac{x}{u^2}, \frac{y}{u^3}\right)$

$u \in \mathbb{Q}$

$$y^2 + a_1uxy + a_3u^3y = x^3 + a_2u^2x^2 + a_4u^4x + a_6u^6$$

Ej $y^2 = x^3 + \frac{x}{2} + \frac{5}{3}$

$(x,y) \longmapsto \left(\frac{x}{6^2}, \frac{y}{6^3}\right)$

$y^2 = x^3 + 648x + 77760$

$y^2 = x^3 + Ax + B \quad , \quad A, B \in \mathbb{Z}$

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

Puntos Integrales

Teorema (Siegel)

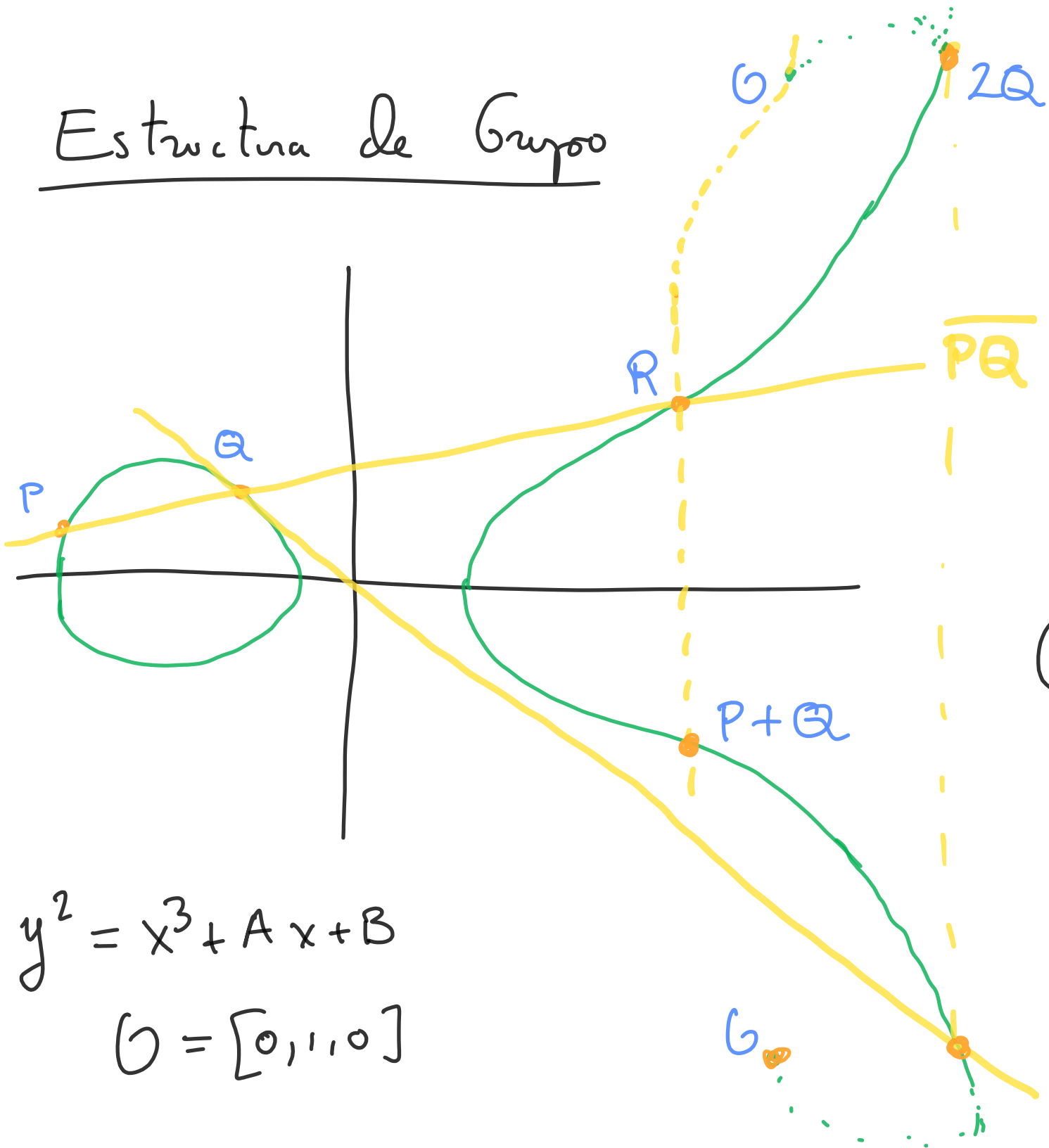
Sea $E/\mathbb{Q}$ una curva elíptica

$$y^2 = x^3 + Ax + B \quad , \quad A, B \in \mathbb{Z}.$$

Entonces $E(\mathbb{Z})$ es finito.

(Baker) $\max(|x|, |y|) < e^{10^6 \max(|A|, |B|)^{10^6}}$

Estructura de Grupo



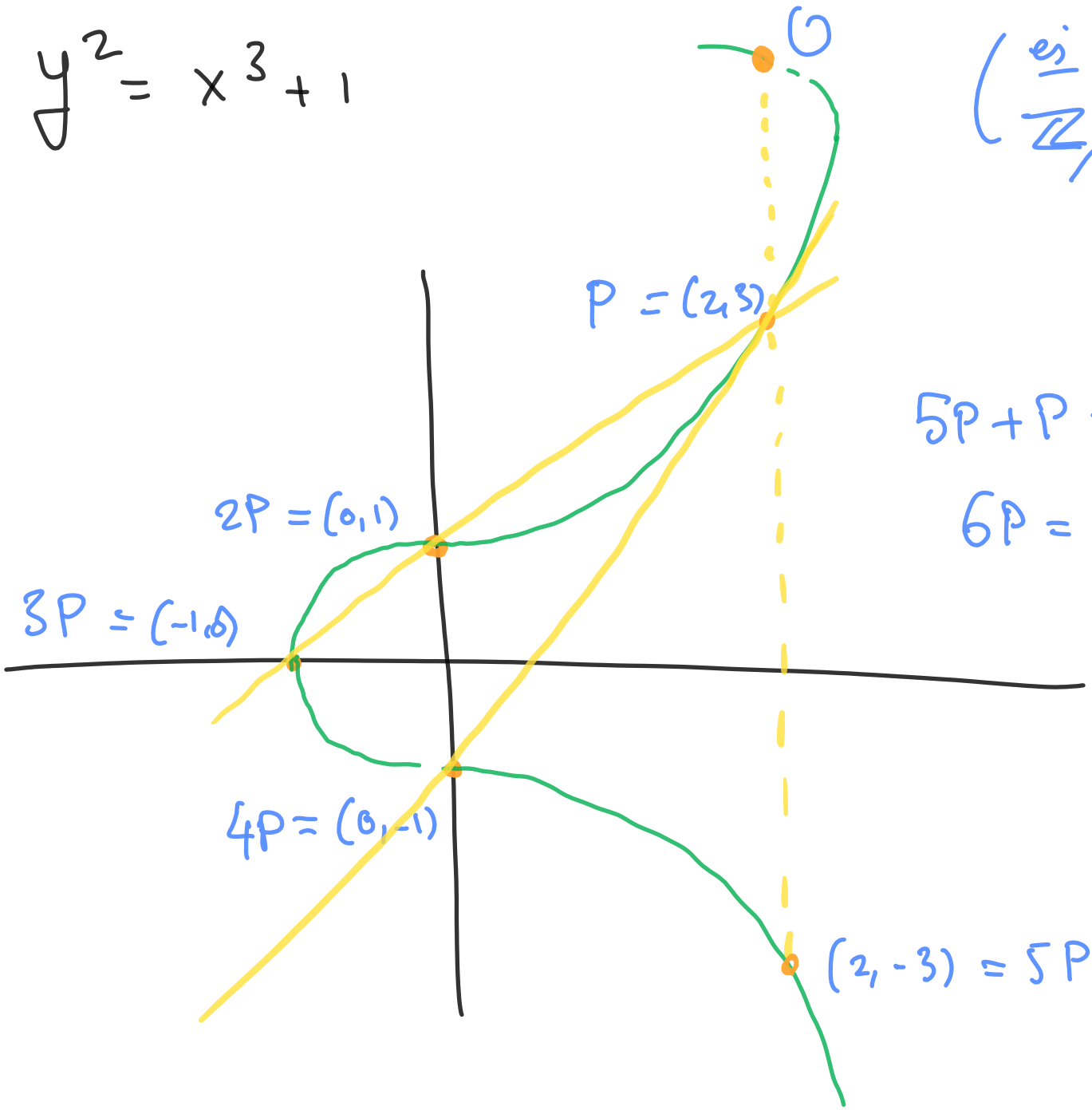
$$y^2 = x^3 + Ax + B$$

$$O = [0,1,0]$$

Nota:

$$(P+Q)+R=O$$

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



$5P + P = O$

$6P = O$

(ej $\mathbb{Z}/6\mathbb{Z}$)

$$\begin{cases} y^2 = x^3 + 1 \\ x = c \end{cases} \Rightarrow y^2 = c^3 + 1$$

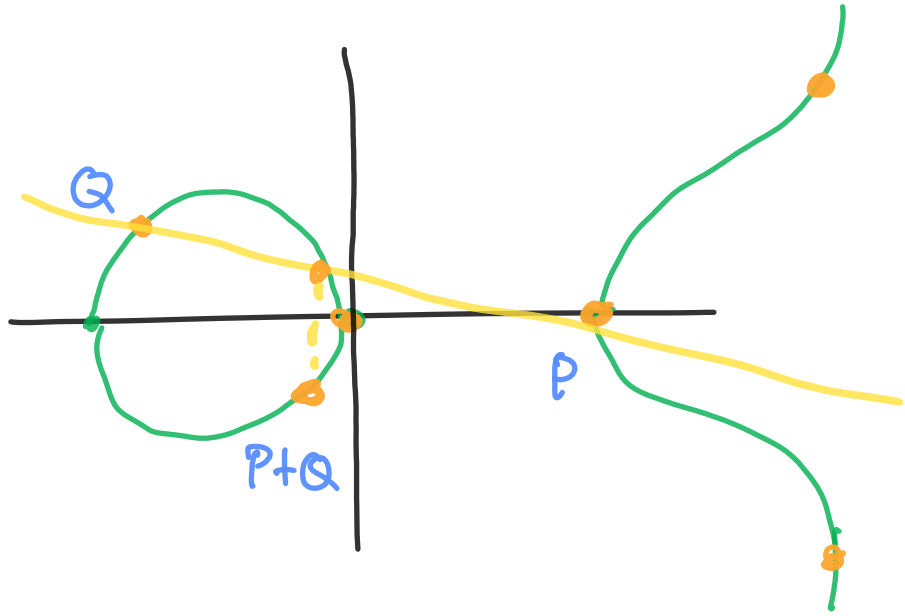
$$y = \pm\sqrt{c^3+1}$$

Ej $y^2 = x^3 - 25x$ $(0,0)$, $(5,0)$, $(-5,0)$

P

$Q = (-4, 6)$

Q Calcular $P+Q$



(1) $L = \overline{PQ}$

$$m = \frac{0-6}{5-(-4)} = -\frac{2}{3}$$

$$L: \; y = -\frac{2}{3}(x-5)$$

(2) $\begin{cases} y = -\frac{2}{3}(x-5) \\ y^2 = x^3 - 25x \end{cases}$ $\Longrightarrow$ $\left(-\frac{2}{3}(x-5)\right)^2 = x^3 - 25x$

$$\left(-\frac{2}{3}(x-5)\right)^2 = x^3 - 25x \qquad \text{“}f(x)\text{”}$$

$$\Rightarrow \quad x^3 - \frac{4}{9}x^2 - \frac{185}{9}x - \frac{100}{9} = 0$$

$x = -4$, $x = 5$ son soluciones!

$$\Rightarrow (x+4)(x-5) \mid f(x)$$

$$\ldots \Rightarrow \quad x = -5/9 \quad \Rightarrow \quad y = \frac{100}{27}$$

$$f(x) = (x-5)(x+4)(x+5/9)$$

$$\Rightarrow P+Q = \left(-\frac{5}{9}, -\frac{100}{27}\right)$$

2Q $\quad Q=(-4,6) \quad y^2=x^3-25x \quad \frac{dy}{dx}?$

(1) $L=\overline{QQ}$ $\qquad 2y\frac{dy}{dx}=3x^2-25$

$L: y-6=\frac{23}{12}(x+4)$ $\qquad \left.\frac{dy}{dx}\right|_Q=\left.\frac{3x^2-75}{2y}\right|_Q=\frac{23}{12}$

$y=\frac{23}{12}(x+4)+6$

(2) $\begin{cases} y=\frac{23}{12}(x+4)+6 \\ y^2=x^3-25x \end{cases}$ $\Rightarrow x^3-\frac{529}{144}x^2-\frac{1393}{18}x-\frac{1681}{9}=0$

$f(x)=0$

$\Rightarrow x=\frac{1681}{144}$ $\qquad (x+4)^2 \mid f(x)$

$y=\frac{62279}{1728} \Rightarrow 2Q=\left(\frac{1681}{144},-\frac{62279}{1728}\right)$