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

$4A^3 + 27B^2$

$$E(\mathbb{Q}) = \{(x_0, y_0) : x_0, y_0 \in \mathbb{Q} \quad y_0^2 = x_0^3 + Ax_0 + B\} \cup \{O\}$$

"
$[0,1,0]$

Teorema $(E(\mathbb{Q}), +)$ es un grupo abeliano.

↑ suma geométrica

(0) $P+Q \in E(\mathbb{Q})$ para todo $P, Q \in E(\mathbb{Q})$

(1) $+$ es asociativa $((P+Q)+S) = (P+(Q+S))$

(2) $+$ es conmutativa

(3) hay $O \in E(\mathbb{Q})$ tal que $O+P = P = P+O$ para todo $P \in E(\mathbb{Q})$

(4) $\forall P \in E$, $-P = (x_0, -y_0)$ tal que $P + (-P) = O$

"(x_0, y_0)

Teorema (Mordell - Weil)

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

Entonces $E(\mathbb{Q})$ es un grupo abeliano finitamente generado.

$$\Longrightarrow \boxed{E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^{R_{E/\mathbb{Q}}}}$$

$E(\mathbb{Q})_{tors}$ es el subgrupo de todos los puntos de orden finito.

$R_{E/\mathbb{Q}}$ = rango de la curva = # generadores de orden infinito.

Ej $E_1 : y^2 = x^3 + 6$ $\quad E_1(\mathbb{Q}) \cong \{0\}$

$E_2 : y^2 = x^3 + 1$ $\quad E_2(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$

$E_3 : y^2 = x^3 - 2$ $\quad E_3(\mathbb{Q}) \cong \mathbb{Z}$

$E_4 : y^2 = x^3 + 7105x^2 + 1327104x$

$E_4(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}^3$

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

$$E(\mathbb{Q})_{tors} = \{ (x_0, y_0) \in E : \; x_0, y_0 \in \mathbb{Q} \text{ existe un } n \in \mathbb{Z} \text{ con } n \cdot P = \mathcal{O} \}$$

"P

$$\underbrace{P + P + \cdots + P}_{n \text{ veces}} = \mathcal{O}$$

↑

n mínimo con esta propiedad

$\Rightarrow n =$ orden de P.

Ejemplo

Ejemplo

$m \in \mathbb{Z}$, $m \neq 0$

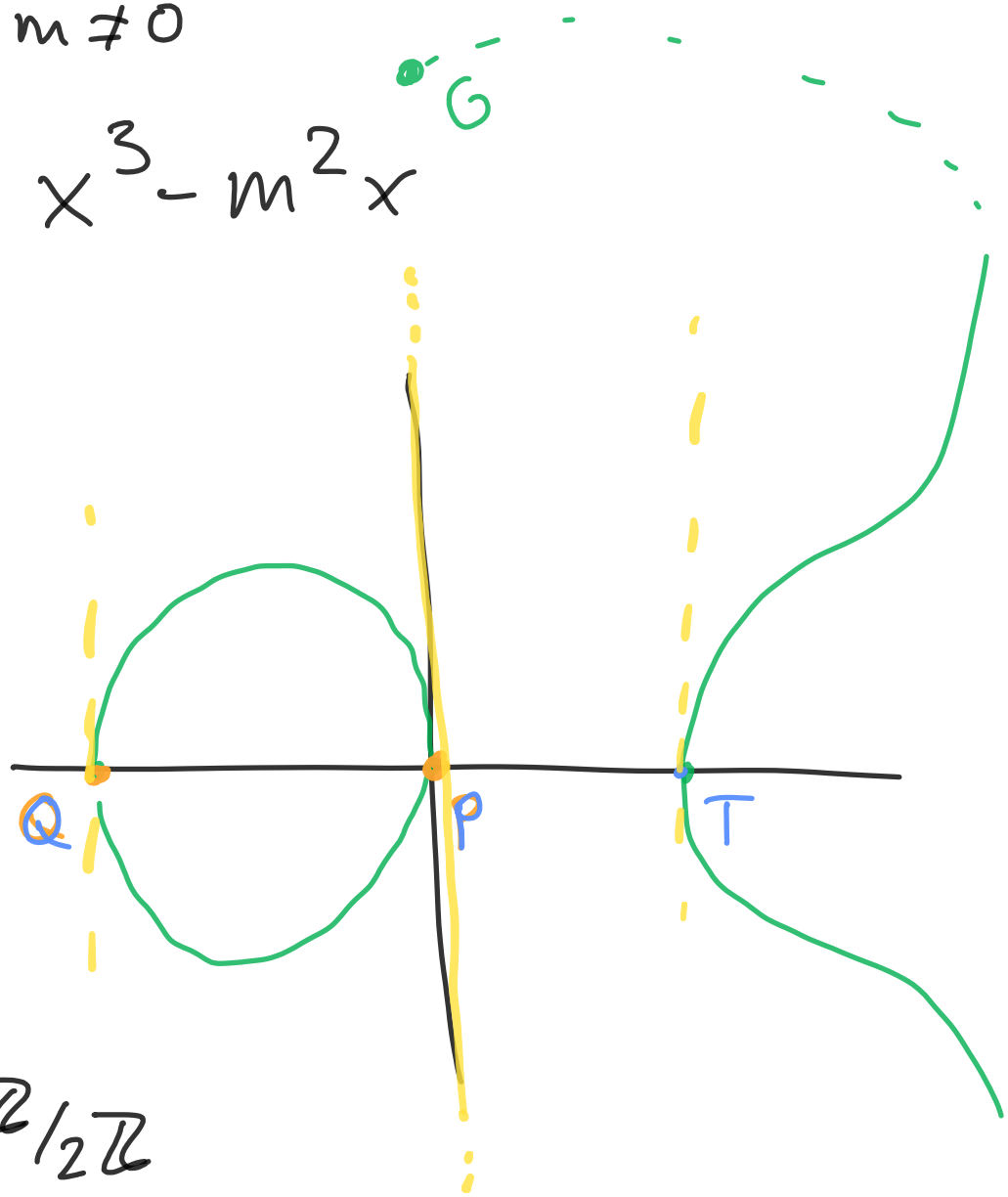
$$E_m : y^2 = x^3 - m^2 x$$

$P = (0,0) \Rightarrow 2P = \mathcal{O}$

$Q = (-m, 0) \quad 2Q = 0$

$T = (m, 0) \quad 2T = 0$

$P + Q = T$



$$E(\mathbb{Q}) \supseteq \langle P, Q \rangle$$

$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

$=$

Teorema (Levi, Ogg, Mazur, 1977)

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

Entonces

$$E(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/N\mathbb{Z} & N = 1,2,3,4,5,6,7,8,9,10, \text{ ó } 12. \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & 1 \leq M \leq 4 \end{cases}$$

Cada posibilidad existe para un número infinito de curvas elípticas no isomorfas sobre $\overline{\mathbb{Q}}$.

Ej $E: y^2 + 17xy - 120y = x^3 - 60x^2$ /$\mathbb{Q}$

$$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$$

$$\cong \langle (-40, 400), (30, -90) \rangle$$

Ej $E: y^2 + 43xy - 210y = x^3 - 210x^2$

$$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/12\mathbb{Z}$$

$$\cong \langle (0, 210) \rangle$$

$t \in \mathbb{Q} \quad t \neq 0$

Ej

$$E_t : y^2 + (1-t)xy - ty = x^3 - tx^2$$

$$E(\mathbb{Q})_{tors} \supseteq \mathbb{Z}/5\mathbb{Z}$$

$$\| \\ \langle (0,0) \rangle$$

Teorema (Nagell - Lutz)

Sea $E/\mathbb{Q}$ una curva elíptica

$$y^2 = x^3 + Ax + B \quad , \quad A, B \in \mathbb{Z} \quad (4A^3 + 27B^2 \neq 0)$$

Entonces si $P \neq \mathcal{O}$ es un punto de torsión

$$(x(P), y(P))$$

(1) $x(P), y(P) \in \mathbb{Z}$

(2) Si P es de orden 2, entonces $y(P) = 0$

y $x(P)^3 + A\,x(P) + B = 0$

(3) Si P es de orden ≥ 3

entonces $y(P)^2$ es un divisor de $4A^3 + 27B^2$.

Ej $E: y^2 = x^3 - 2$ $\quad A = 0,\ B = -2$

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

- $P = \mathcal{O}$
- orden 2? $y = 0,\ x^3 - 2 = 0$

  $x^3 = 2 \Rightarrow x \notin \mathbb{Q}$.

  No hay puntos de orden 2.
- orden ≥ 3: $y(P)^2 \mid 4 \cdot 27 \Rightarrow y(P) = \pm 1, \pm 2, \pm 3, \pm 6$

  $\Rightarrow x^3 = y^2 + 2 = 3, 6, 11, 38$

  $\Rightarrow x \notin \mathbb{Q}$.

No hay puntos de orden ≥ 3

$\Rightarrow E(\mathbb{Q})_{tors} \simeq \{\mathcal{O}\}$

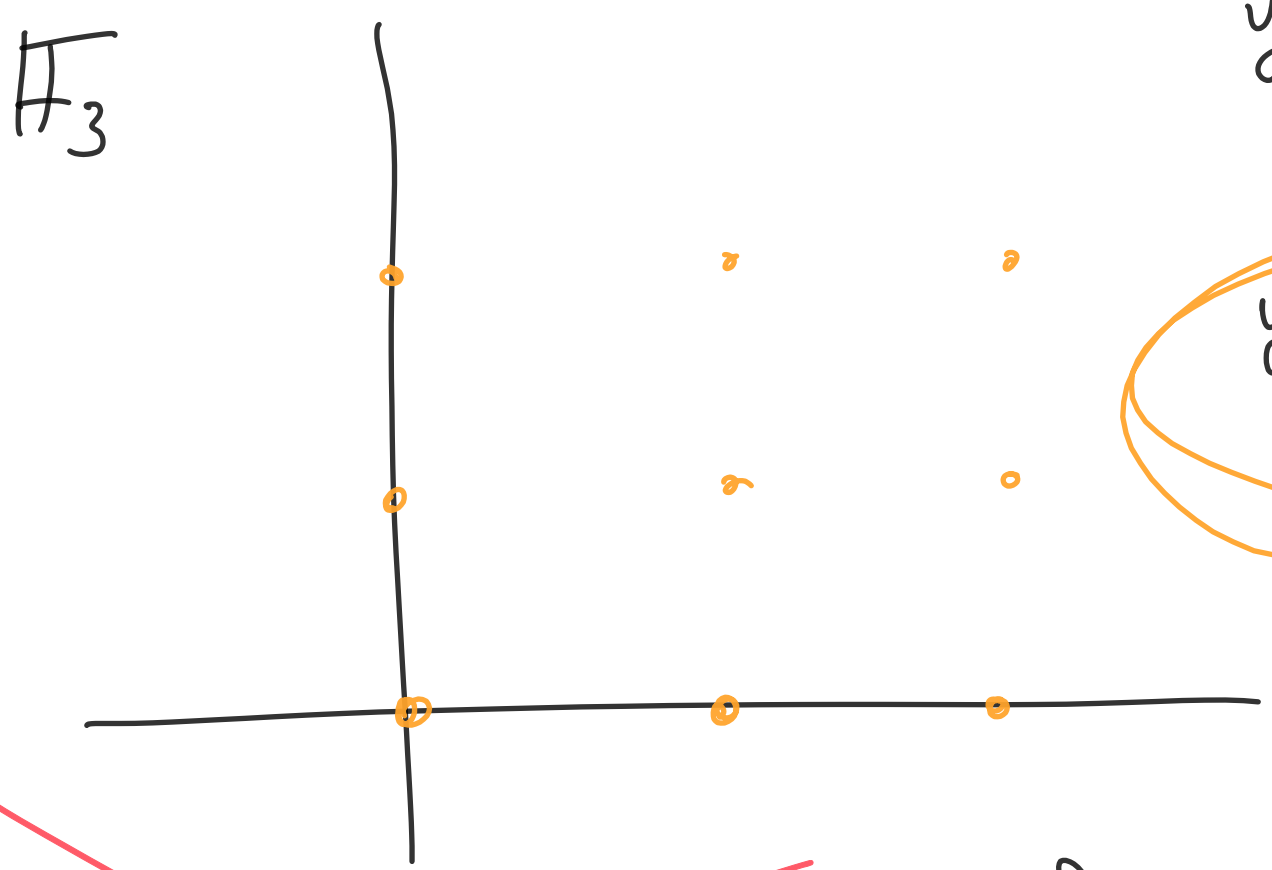
Ej: $y^2 = x^3 + p^2 \Rightarrow E(\mathbb{Q})_{tors} \cong \mathbb{Z}/3\mathbb{Z}$

Curvas elípticas sobre cuerpos finitos

$E : y^2 = x^3 + 1 \quad / \mathbb{F}_p$

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

$= \{0, 1, 2, \ldots, p-1 \bmod p\}$



$y^2 = x^3 + 1 \,/\, \mathbb{Q}$

$y^2 \equiv x^3 + 1 \,/\, \mathbb{F}_p$

para todo p.

$E: y^2 = x^3 + 1 \,/\, \mathbb{F}_3$

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

$\frac{\partial f}{\partial x} = 3x^2 \equiv 0 \bmod 3$

$\frac{\partial f}{\partial y} = -2y \Rightarrow y = 0$

$(2,0) \in E$ es singular!

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

Discriminante de $E/\mathbb{Q}$

$$\Delta_E = -16 \cdot (4A^3 + 27B^2)$$

Ej $E: y^2 = x^3 + 5^6$ $\xleftrightarrow{\left(\frac{x}{5^2}, \frac{y}{5^3}\right)}$ $y^2 = x^3 + 1$

$$\Delta_E = -2^4 \cdot 3^3 \cdot 5^{12} \qquad \Delta_{E'} = -2^4 \cdot 3^3$$

$E \rightsquigarrow \tilde{E}$ mod p es una curva elíptica $\iff p \nmid \Delta_E$.

$$\circledast \begin{cases} zy^2 = x^3 + Axz^2 + Bz^3 \quad (F(x,y,z)=0) \\ \partial F/\partial x = 0 \\ \partial F/\partial y = 0 \\ \partial F/\partial z = 0 \end{cases}$$

$P \in E$ es singular $\Leftrightarrow$ solución de $\circledast$

Ej $y^2 = x^3 + 1 \quad / \mathbb{F}_5$ $\qquad x^3 + z^3 - y^2 z = 0$

"$F(x,y,z)$"

$$\begin{cases} x^3 + z^3 - y^2 z \equiv 0 \mod 5 \\ 3x^2 \equiv 0 \implies x \equiv 0 \\ -2yz \equiv 0 \implies y \equiv 0 \text{ o } z \equiv 0 \implies x \equiv y \equiv z \equiv 0 \mod 5 \\ -3z^2 - y^2 \equiv 0 \end{cases}$$

No es singular!

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

$$\Delta_E = -16 \cdot (4A^3 + 27B^2)$$

- $p \mid \Delta_E \Rightarrow$ mala reducción
- $p \nmid \Delta_E \Rightarrow$ buena reducción.

mala reducción $\begin{cases} p \mid \Delta_E \text{ , la reducción es de tipo cúspide} \Rightarrow \text{decimos reducción aditiva} \\ p \mid \Delta_E \text{ , la reducción tiene un nodo} \Rightarrow \text{decimos reducción es multiplicativa.} \end{cases}$



Ej $E: y^2 = x^3 + 35x + 5 \quad /\mathbb{Q}$

- $p=7 \Rightarrow \tilde{E}: y^2 = x^3 + 5 \quad /\mathbb{F}_7$

  no es singular $\Rightarrow$ c. ell. sobre $/\mathbb{F}_7$.

- $p=5 \Rightarrow \tilde{E}: y^2 = x^3 \quad /\mathbb{F}_5$

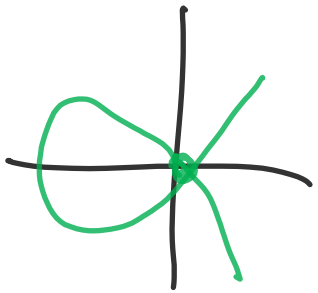
  mala reducción aditiva en $p=5$.

Ej $E: y^2 = x^3 - x^2 + 35 \quad /\mathbb{Q}$

- $p=5 \longrightarrow \tilde{E}: y^2 = x^3 - x^2 \quad /\mathbb{F}_5$

  $= x^2(x-1)$

  mala reducción multiplicativa.



$$E : y^2 = x^3 + Ax + B \quad , \quad A, B \in \overline{\mathbb{F}_p}$$

$$x_0 \in \overline{\mathbb{F}_p} \rightsquigarrow x_0^3 + Ax_0 + B \overset{?}{\equiv} y_0^2 \mod p \,?$$

$$\hookrightarrow (x_0, y_0), (x_0, -y_0)$$

$$\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-1\}$$

$$\left((\mathbb{Z}/p\mathbb{Z})^\times\right)^2 = \{ \text{mitad} \} \Longrightarrow \frac{p-1}{2} \text{ cuadrados.}$$

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

Teorema (Hasse)

Sea $\tilde{E}$ una curva elíptica sobre $\mathbb{F}_p$.

Entonces

$$p+1-2\sqrt{p} < \#E(\mathbb{F}_p) < p+1+2\sqrt{p}$$

ó

$$\left|\#E(\mathbb{F}_p) - (p+1)\right| < 2\sqrt{p}$$

Ej $E/\mathbb{Q} : y^2 = x^3 + 3$

$$\Delta_E = -3888 = -2^4 \cdot 3^5$$

$p = 5$

$$E(\mathbb{F}_5) = \{ O, (1,2), (1,3), (2,1), (2,4), (3,0) \}$$

$$\# E(\mathbb{F}_5) = 6$$

(Hasse: $1.52\ldots < \# E(\mathbb{F}_5) < 10.47\ldots$)

$y^2 = x^3 + Ax + B / \mathbb{Z}$

Prop Sea $E/\mathbb{Q}$ curva elíptica, p primo, $p \nmid \Delta_E$

m natural no divisible por p.

Entonces:

reducción modulo p.

$$E(\mathbb{Q})[m] \longrightarrow \tilde{E}(\mathbb{F}_p)$$

subgrupo de torsión de puntos de orden que dividen m

es un homomorfismo inyectivo de grupos.

En particular $\#E(\mathbb{Q})[m] \mid \#\tilde{E}(\mathbb{F}_p)$

Ej $E: y^2 = x^3 + 3 / \mathbb{Q}$ buena reducción $p \neq 2, 3$.

- $p = 5$ $\quad \widetilde{E}: y^2 = x^3 + 3 / \mathbb{F}_5$

$$\# \widetilde{E}(\mathbb{F}_5) = 6$$

$$E(\mathbb{Q})[q] \hookrightarrow \widetilde{E}(\mathbb{F}_5)$$

No hay torsión.

q primo, $q \neq 5$

$\# E(\mathbb{Q})[q] \mid 6 \Rightarrow q = 2, 3, 5$ ↯

$\# E(\mathbb{Q})[q]$ tiene orden $1, q, q^2, \ldots$

$q = 13, 17$

- $p = 7$, $\# \widetilde{E}(\mathbb{F}_7) = 13 \Rightarrow \# E(\mathbb{Q})[q] \mid 13$