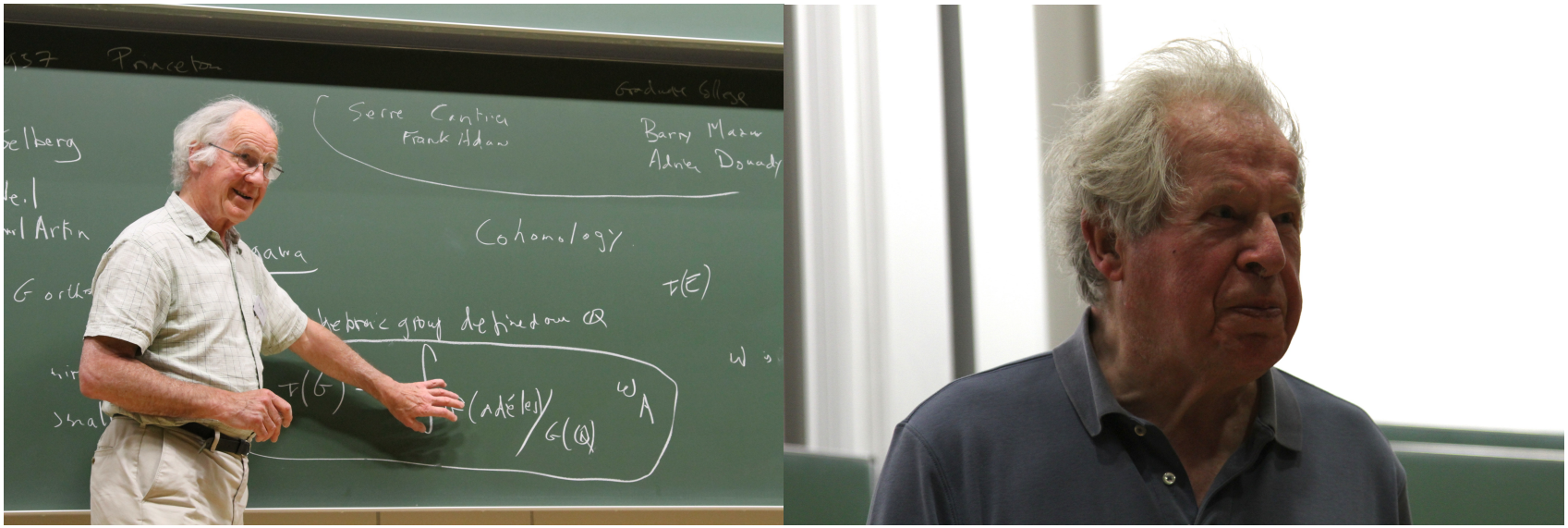
La conjetura de Birch y Swinnerton-Dyer

Victor Rotger (UPC)

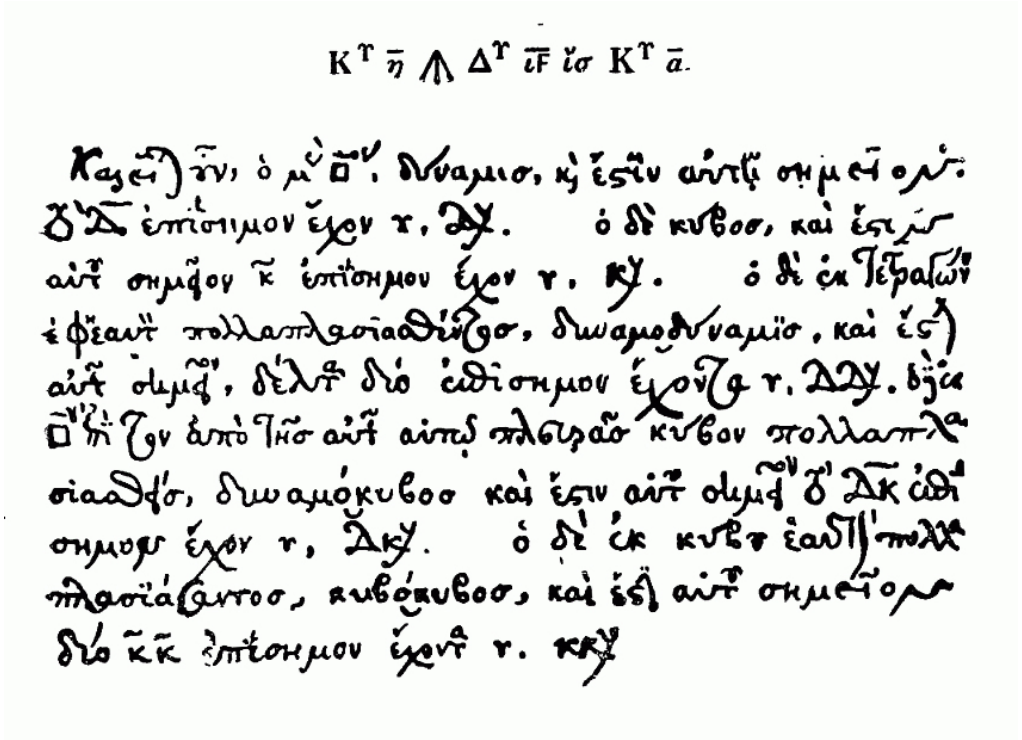
7 de junio de 2011

La conjetura de Birch y Swinnerton-Dyer



Bryan Birch y Peter Swinnerton-Dyer, mayo de 2011

Ecuaciones diofánticas



$$K^{\upsilon}\ \bar{\eta} \wedge \Delta^{\upsilon}\ \bar{\imath}\digamma\ \check{\imath}\sigma\ K^{\upsilon}\ \bar{a}.$$

La *Arimética* de Diofanto de Alejandría.

Ecuaciones diofánticas

- $x + 4 = 10$,

Ecuaciones diofánticas

- $x + 4 = 10$, $\quad x = 6 \in \mathbb{N}$.

Ecuaciones diofánticas

- $x + 4 = 10$, $\qquad x = 6 \in \mathbb{N}$.
- $x + 10 = 4$,

Ecuaciones diofánticas

- $x + 4 = 10$, $\quad x = 6 \in \mathbb{N}$.
- $x + 10 = 4$, $\quad x = -6 \in \mathbb{Z}$.

Ecuaciones diofánticas

- $x + 4 = 10$, $\quad x = 6 \in \mathbb{N}$.
- $x + 10 = 4$, $\quad x = -6 \in \mathbb{Z}$.
- $4x = 10$,

Ecuaciones diofánticas

- $x + 4 = 10$, $\quad x = 6 \in \mathbb{N}$.
- $x + 10 = 4$, $\quad x = -6 \in \mathbb{Z}$.
- $4x = 10$, $\quad x = \frac{10}{4} = \frac{5}{2} \in \mathbb{Q}$.

Ecuaciones diofánticas

- $x + 4 = 10$, $\quad x = 6 \in \mathbb{N}$.
- $x + 10 = 4$, $\quad x = -6 \in \mathbb{Z}$.
- $4x = 10$, $\quad x = \frac{10}{4} = \frac{5}{2} \in \mathbb{Q}$.
- $x^4 = 10$,

Ecuaciones diofánticas

- $x + 4 = 10$, $\quad x = 6 \in \mathbb{N}$.
- $x + 10 = 4$, $\quad x = -6 \in \mathbb{Z}$.
- $4x = 10$, $\quad x = \frac{10}{4} = \frac{5}{2} \in \mathbb{Q}$.
- $x^4 = 10$, $\quad x = \sqrt[4]{10} \in \mathbb{R}$.

Ecuaciones diofánticas

- $x + 4 = 10$, $\quad x = 6 \in \mathbb{N}$.
- $x + 10 = 4$, $\quad x = -6 \in \mathbb{Z}$.
- $4x = 10$, $\quad x = \frac{10}{4} = \frac{5}{2} \in \mathbb{Q}$.
- $x^4 = 10$, $\quad x = \sqrt[4]{10} \in \mathbb{R}$.

De hecho la última ecuación tiene 4 soluciones:

$$\pm\sqrt[4]{10} \in \mathbb{R}, \quad \pm i\sqrt[4]{10} \in \mathbb{C}.$$

Cuáles son las soluciones en $\mathbb{Z}$ o $\mathbb{Q}$ de:

Ecuación	Origen	Solución
$X^2 + Y^2 = Z^2$	Teorema Pitágoras	Babilonia (s. XIX a. C.)
$aX^2 + bY^2 = cZ^2$	Cónica racional	Legendre (1780)
$X^2 - aY^2 = 1$	Ecuación de Pell	Brahmagupta (s. VII)
$X^3 - a^2X = Y^2$	Al Kazin (s. X)	Tunnell (1983)
$X^n + Y^n = Z^n$	Fermat (1620)	Wiles (1995)
$X^4 + Y^4 + Z^4 = W^4$	Euler (1720)	Elkies (1988)
$X^n + 1 = Y^m$	Catalan (1856)	Mihailescu (2003)

Último teorema de Fermat

Pierre de Fermat

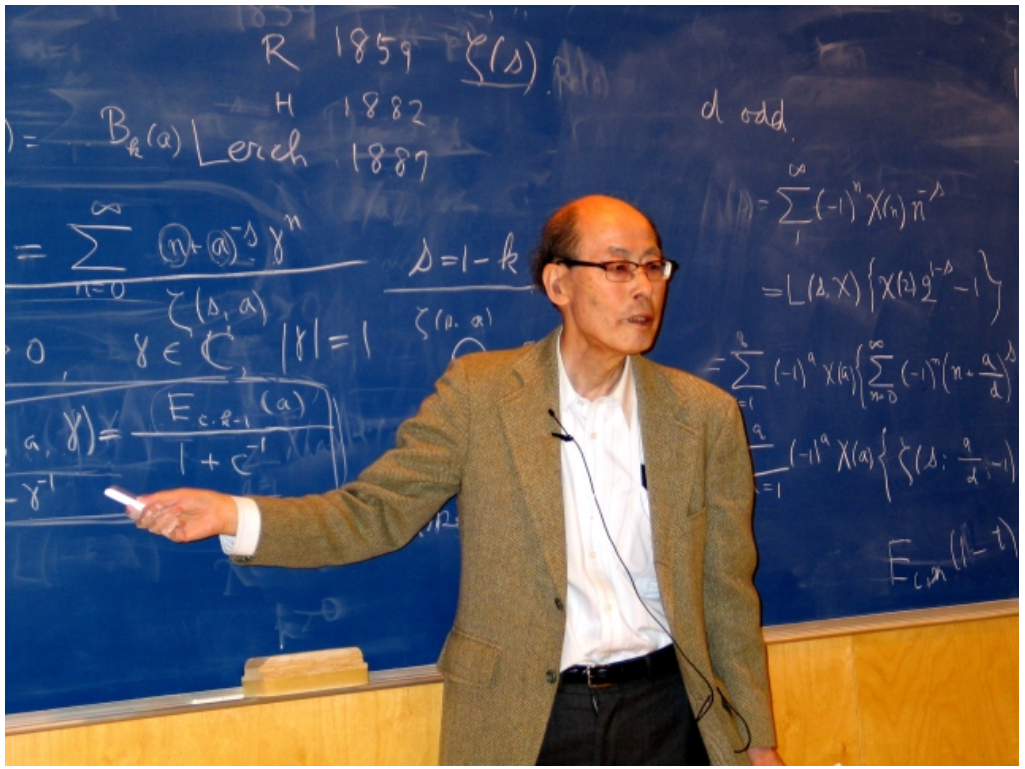
En 1620 Fermat escribió en el margen de su ejemplar de la *Aritmética* de Diofanto que la ecuación

$$X^n + Y^n = Z^n, \quad n \geq 3$$

no tiene soluciones *enteras* aparte de las *triviales*, como $(1, 0, 1)$, $(-1, 0, -1)$...

Último teorema de Fermat

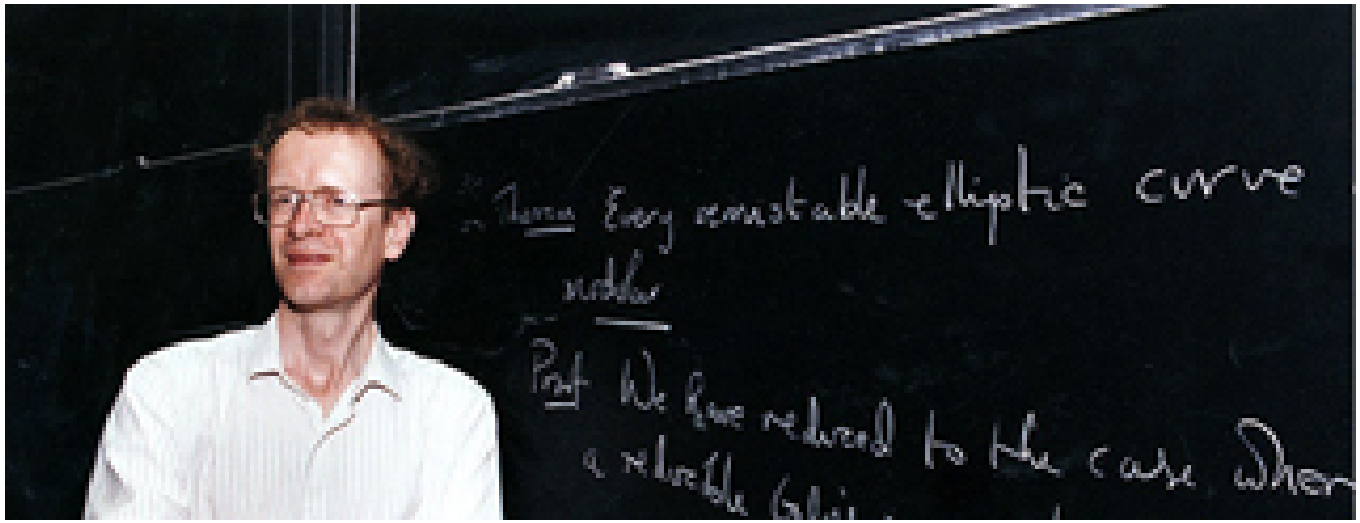
En los años ochenta, Frey, Serre, Ribet y otros vislumbraron un camino para llegar a demostrar el teorema de Fermat, observando que es consecuencia de la *modularidad* de las curvas elípticas, conjeturada por Shimura y Taniyama hacia 1955.



Goro Shimura en Barcelona, abril de 2010

Último teorema de Fermat

Después de tres siglos y medio, en 1993 Andrew Wiles encontró una demostración de la conjeturada *modularidad* de las curvas elípticas, probando así el último teorema de Fermat.



Andrew Wiles

Números congruentes

Sea $a \in \mathbb{N}$.

Números congruentes

Sea $a \in \mathbb{N}$. Existe algún triángulo rectángulo, de lados

$$x, y, z \in \mathbb{Q},$$

cuya área es a? (Al Kazin (s. X))

Números congruentes

Sea $a \in \mathbb{N}$. Existe algún triángulo rectángulo, de lados

$$x, y, z \in \mathbb{Q},$$

cuya área es a? (Al Kazin (s. X))

Si existe, se dice que a es un *número congruente*.

Números congruentes

Sea $a \in \mathbb{N}$. Existe algún triángulo rectángulo, de lados

$$x, y, z \in \mathbb{Q},$$

cuya área es a? (Al Kazin (s. X))

Si existe, se dice que a es un *número congruente*.

Fibonacci encontró un tal triángulo de área $a = 5$.

Números congruentes

Sea $a \in \mathbb{N}$. Existe algún triángulo rectángulo, de lados

$$x, y, z \in \mathbb{Q},$$

cuya área es a? (Al Kazin (s. X))

Si existe, se dice que a es un *número congruente*.

Fibonacci encontró un tal triángulo de área $a = 5$.

Fermat demostró que no hay ninguno de área $a = 1$.

Números congruentes

Sea $a \in \mathbb{N}$. Existe algún triángulo rectángulo, de lados

$$x, y, z \in \mathbb{Q},$$

cuya área es a? (Al Kazin (s. X))

Si existe, se dice que a es un *número congruente*.

Fibonacci encontró un tal triángulo de área $a = 5$.

Fermat demostró que no hay ninguno de área $a = 1$.

Sea $E_a : y^2 = x^3 - a^2 x$.

Números congruentes

Sea $a \in \mathbb{N}$. Existe algún triángulo rectángulo, de lados

$$x, y, z \in \mathbb{Q},$$

cuya área es a? (Al Kazin (s. X))

Si existe, se dice que a es un *número congruente*.

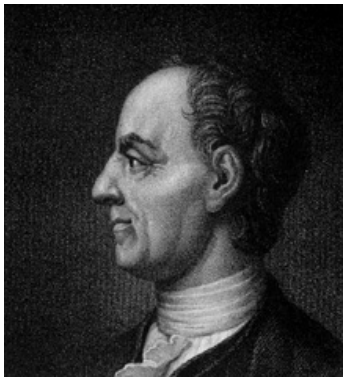
Fibonacci encontró un tal triángulo de área $a = 5$.

Fermat demostró que no hay ninguno de área $a = 1$.

Sea $E_a : y^2 = x^3 - a^2 x$. Se tiene que a es congruente si y sólo si

$$E_a \text{ tiene infinitas soluciones racionales.}$$

La cuártica de Euler



Leonard Euler (1707–1783)

Euler conjeturó que la ecuación

$$X^4 + Y^4 + Z^4 = W^4$$

no tiene soluciones *enteras* no triviales.

La cuártica de Euler

En 1988 Noam Elkies encontró la solución

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4$$

y demostró que la ecuación tiene, de hecho, infinitas soluciones no triviales.

La conjetura de Catalan

En 1844, el matemático belga Eugène Catalan conjeturó que los únicos enteros consecutivos que son potencias no triviales de un entero son

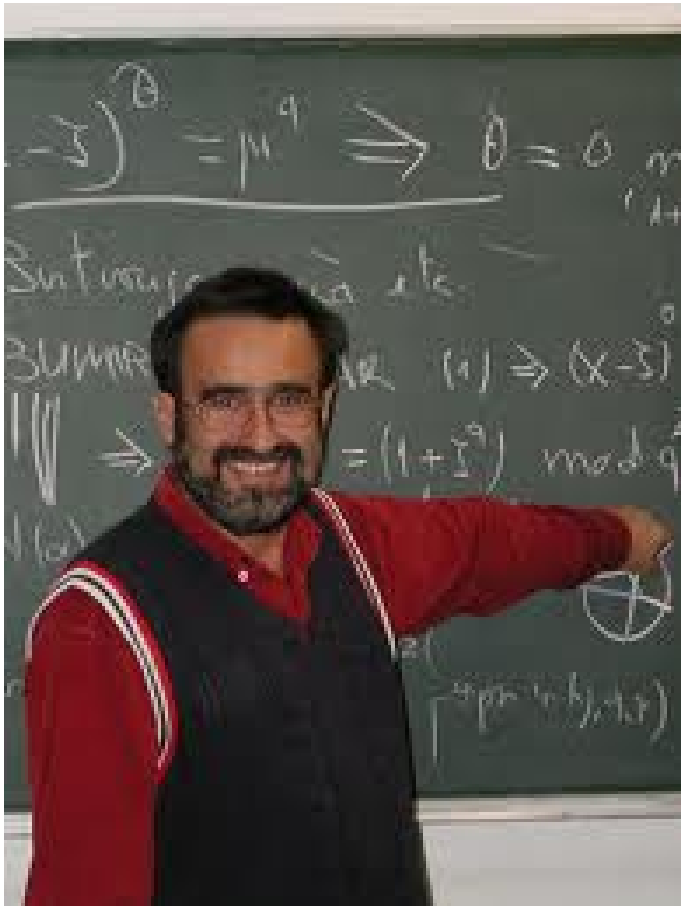
$$8 = 2^3 \quad \text{i} \quad 9 = 3^2.$$

Es decir, que ésta es la única solución no trivial de la ecuación diofántica

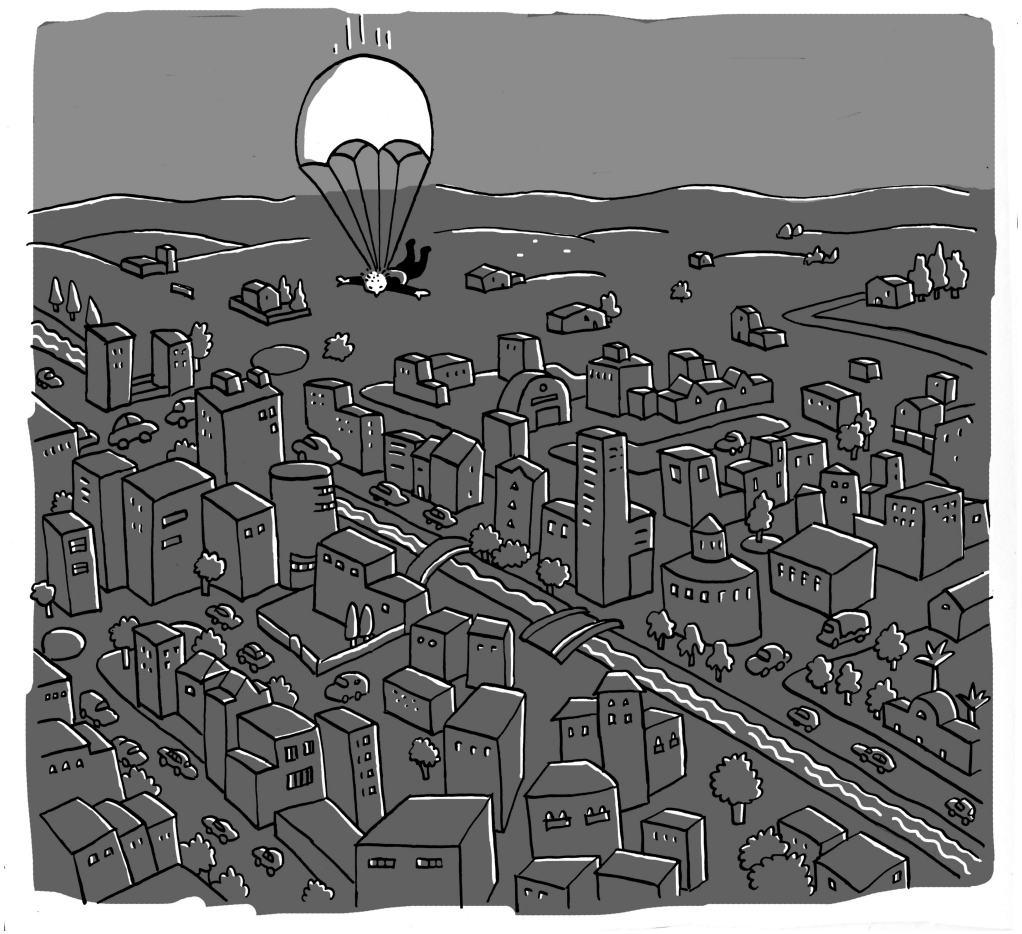
$$X^n + 1 = Y^m, \qquad n, m > 1.$$

La conjetura de Catalan

Esta conjetura fue demostrada el 2002 por el matemático rumano Preda Mihailescu.



Preda Mihailescu



Para encontrar las soluciones de cada una de las ecuaciones que hemos considerado se han necesitado décadas de estudio. Y en cada caso la respuesta se ha obtenido mediante técnicas difíciles, muy diferentes unas de otras.

Organicémonos

Convengamos, para centrar un poco la discusión, que una ecuación diofántica es para nosotros una ecuación

$$E : f = 0$$

donde f es un *polinomio* de una o más variables (x, y, z, ...) con *coeficientes* en un conjunto de números dado.

$E : f = 0$	Variables	Grado	Coeficientes
$x^3 - 11x + 4 = 0$	x	3	$\mathbb{Z}$
$x^7 - \frac{1}{2}x = 0$	x	7	$\mathbb{Q}$
$x^2 + y^2 + 1 = 0$	x, y	2	$\mathbb{Z}$
$y^2 - x^3 - x - 1 = 0$	x, y	3	$\mathbb{Z}$
$3x^{13} + 4\sqrt{2} \cdot y^{12} - 5e^{\frac{2\pi i}{5}} \cdot z^{11} = 0$	x, y, z	13	$\mathbb{C}$

Organicémonos

Dada una ecuación diofántica $E : f(x, y...) = 0$ de grado d y coeficientes en $\mathbb{Z}$:

(1) Tiene alguna solución en $\mathbb{Z}$? En $\mathbb{Q}$? En $\mathbb{R}$? En $\mathbb{C}$?

(2) Si tiene alguna, cuántas hay? cómo están organizadas?

Organicémonos

Dada una ecuación diofántica $E : f(x, y...) = 0$ de grado d y coeficientes en $\mathbb{Z}$:

(1) Tiene alguna solución en $\mathbb{Z}$? En $\mathbb{Q}$? En $\mathbb{R}$? En $\mathbb{C}$?

(2) Si tiene alguna, cuántas hay? cómo están organizadas?

Las respuestas son relativamente sencillas...

- ... si el grado es $d = 1$.
  Ej: $-5x + 2y + 7z - t = 11$.

Organicémonos

Dada una ecuación diofántica $E : f(x, y...) = 0$ de grado d y coeficientes en $\mathbb{Z}$:

(1) Tiene alguna solución en $\mathbb{Z}$? En $\mathbb{Q}$? En $\mathbb{R}$? En $\mathbb{C}$?

(2) Si tiene alguna, cuántas hay? cómo están organizadas?

Las respuestas son relativamente sencillas...

- ... si el grado es $d = 1$.
  Ej: $-5x + 2y + 7z - t = 11$.
- ... si el número de variables es 1.
  Ej: $x^7 - 5x^4 + 10x^3 - 5x^2 + x + 9 = 0$.

Organicémonos

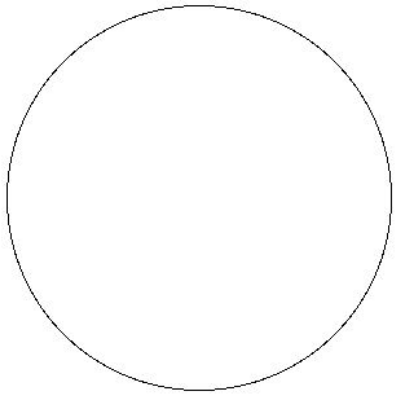
Dada una ecuación diofántica $E : f(x, y...) = 0$ de grado d y coeficientes en $\mathbb{Z}$:

(1) Tiene alguna solución en $\mathbb{Z}$? En $\mathbb{Q}$? En $\mathbb{R}$? En $\mathbb{C}$?

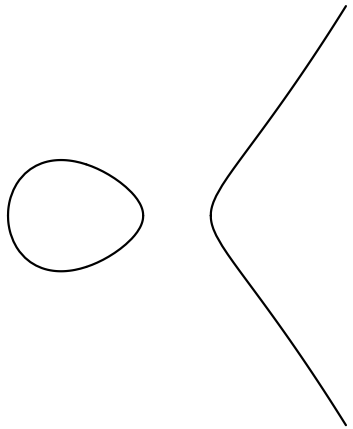
(2) Si tiene alguna, cuántas hay? cómo están organizadas?

Las respuestas son relativamente sencillas...

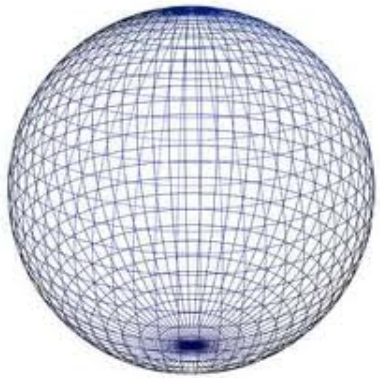
- ... si el grado es $d = 1$.
  Ej: $-5x + 2y + 7z - t = 11$.
- ... si el número de variables es 1.
  Ej: $x^7 - 5x^4 + 10x^3 - 5x^2 + x + 9 = 0$.
- ... en $\mathbb{R}$ o en $\mathbb{C}$.



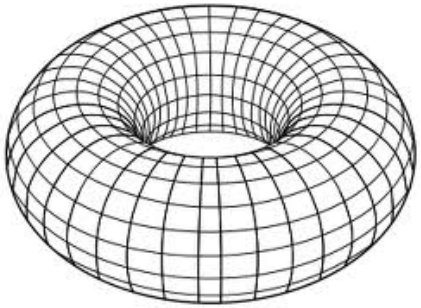
Las soluciones reales de $x^2 + y^2 = 1$.



Las soluciones reales de $y^2 = x^3 - x$.



Las soluciones complejas de $x^2 + y^2 = 1$.



Las soluciones complejas de $y^2 = x^3 - x$.

Ternas pitagóricas

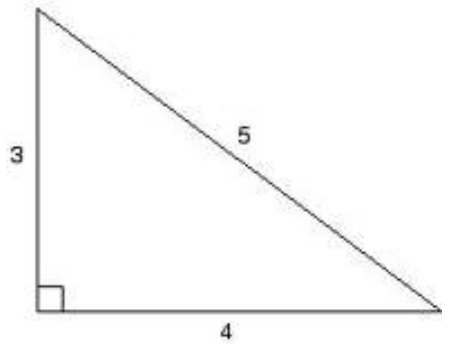
Una de las ecuaciones diofánticas más sencillas es

$$X^2 + Y^2 = Z^2.$$

Sus soluciones enteras positivas, como por ejemplo

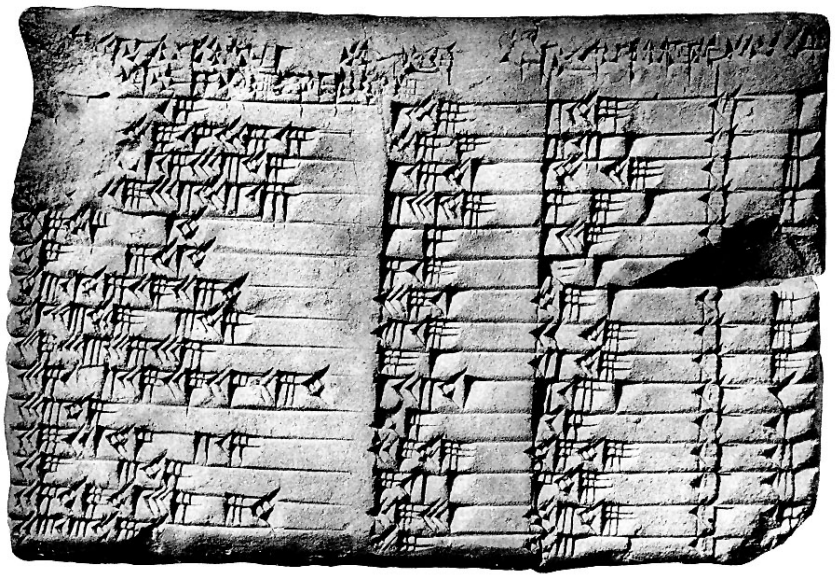
$$(x, y, z) = (3, 4, 5)$$

se llaman ternas pitagóricas, ya que corresponden a los tres lados de un triángulo rectángulo.



Ternas pitagóricas

La tabla babilónica Plimpton 322 (1800-1900 a. C.)



contiene las soluciones $(119, 120, 169)$, $(3367, 3456, 4825)$, $(4601, 4800, 6649)$, $(12709, 13500, 18641)$...

Ternas pitagóricas

Si (X, Y, Z) es una solución de

$$X^2 + Y^2 = Z^2$$

entonces (dX, dY, dZ) también lo es para todo entero d.

Ternas pitagóricas

Si (X, Y, Z) es una solución de

$$X^2 + Y^2 = Z^2$$

entonces (dX, dY, dZ) también lo es para todo entero d.

Basta pues con encontrar las soluciones **primitivas**: ternas $(X, Y, Z) \neq (0, 0, 0)$ sin factores en común.

Ternas pitagóricas

Si (X, Y, Z) es una solución de

$$X^2 + Y^2 = Z^2$$

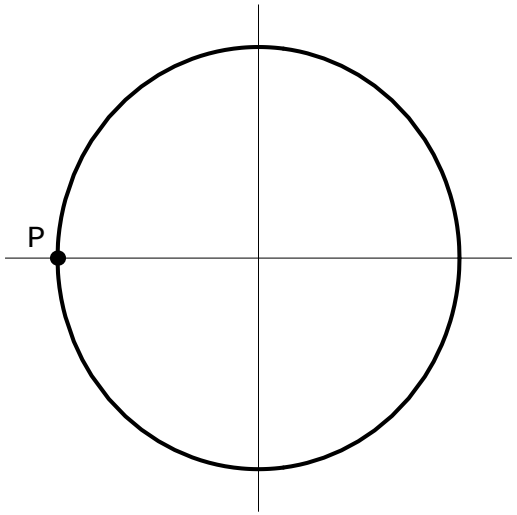
entonces (dX, dY, dZ) también lo es para todo entero d.

Basta pues con encontrar las soluciones **primitivas**: ternas $(X, Y, Z) \neq (0, 0, 0)$ sin factores en común.

Dividiendo por Z se obtiene una correspondencia entre

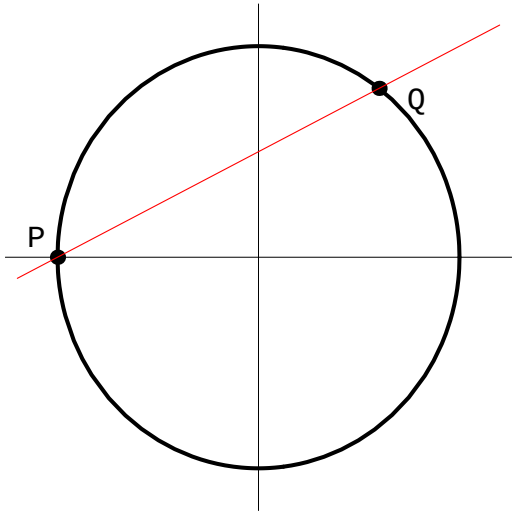
- soluciones **enteras primitivas** de $X^2 + Y^2 = Z^2$, y
- soluciones **racionales** de $x^2 + y^2 = 1$.

Puntos racionales en $C : x^2 + y^2 = 1$



Se escoge un punto racional base P, por ejemplo $P = (-1, 0)$.

Puntos racionales en $C : x^2 + y^2 = 1$



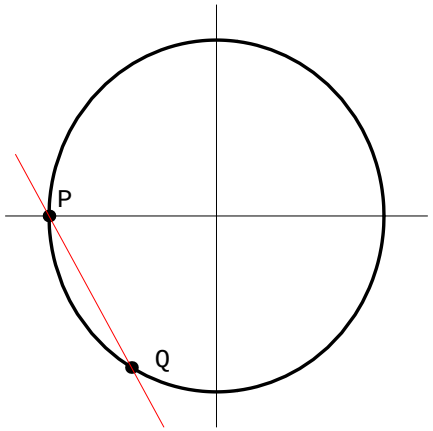
Toda recta que pasa por P corta C en otro punto Q.
Si el pendiente de la recta es t, el punto Q_t tiene coordenadas

$$Q_t = (x, y) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right).$$

La terna $(3, 4, 5)$ corresponde al punto racional

$$Q = (3/5, 4/5) \in C(\mathbb{Q}).$$

Puntos racionales en $C : x^2 + y^2 = 1$

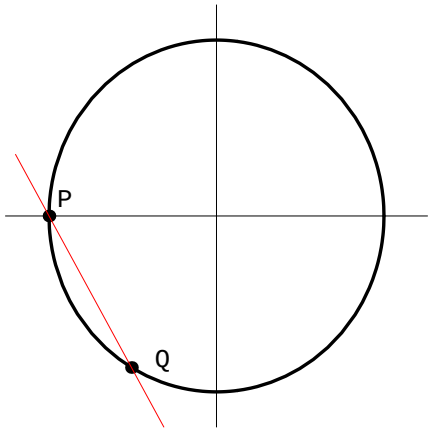


Para $t = -7/4$, da

$$Q = \left(\frac{1 - 49/16}{1 + 49/16}, \frac{-14/4}{1 + 49/16} \right) = \left(\frac{-33}{65}, \frac{-56}{65} \right),$$

que corresponde a la terna $(-33, -56, 65)$.

Puntos racionales en $C : x^2 + y^2 = 1$



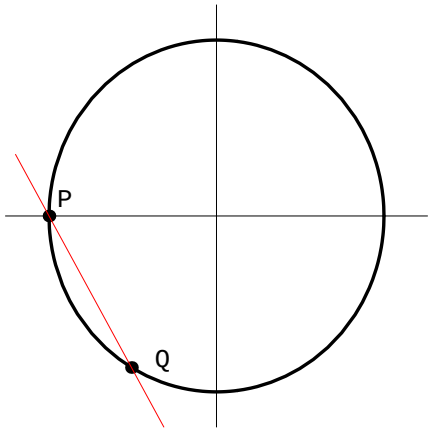
Para $t = -7/4$, da

$$Q = \left(\frac{1 - 49/16}{1 + 49/16}, \frac{-14/4}{1 + 49/16} \right) = \left(\frac{-33}{65}, \frac{-56}{65} \right),$$

que corresponde a la terna $(-33, -56, 65)$.

Hay una biyección de conjuntos entre $\mathbb{Q}$ y $C(\mathbb{Q}) \setminus \{P\}$.

Puntos racionales en $C : x^2 + y^2 = 1$



Para $t = -7/4$, da

$$Q = \left(\frac{1 - 49/16}{1 + 49/16}, \frac{-14/4}{1 + 49/16} \right) = \left(\frac{-33}{65}, \frac{-56}{65} \right),$$

que corresponde a la terna $(-33, -56, 65)$.

Hay una biyección de conjuntos entre $\mathbb{Q}$ y $C(\mathbb{Q}) \setminus \{P\}$.

Si admitimos el pendiente ∞, obtenemos una biyección de conjuntos entre $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ y $C(\mathbb{Q})$.

Puntos racionales en cónicas $C : aX^2 + bY^2 = c$

Si $a = b = c = 1$, encontramos de nuevo $x^2 + y^2 = 1$.

Puntos racionales en cónicas $C : aX^2 + bY^2 = c$

Si $a = b = c = 1$, encontramos de nuevo $x^2 + y^2 = 1$.

Cuáles son las soluciones con coordenadas x, y racionales de la ecuación C? Es decir, cómo podemos calcular $C(\mathbb{Q})$?

Puntos racionales en cónicas $C : aX^2 + bY^2 = c$

Si $a = b = c = 1$, encontramos de nuevo $x^2 + y^2 = 1$.

Cuáles son las soluciones con coordenadas x, y racionales de la ecuación C? Es decir, cómo podemos calcular $C(\mathbb{Q})$?

El método de la recta funciona exactamente igual que antes... si existe una solución racional base $P = (x, y) \in C(\mathbb{Q})$.

Puntos racionales en cónicas $C : aX^2 + bY^2 = c$

Si $a = b = c = 1$, encontramos de nuevo $x^2 + y^2 = 1$.

Cuáles son las soluciones con coordenadas x, y racionales de la ecuación C? Es decir, cómo podemos calcular $C(\mathbb{Q})$?

El método de la recta funciona exactamente igual que antes... si existe una solución racional base $P = (x, y) \in C(\mathbb{Q})$.

Y a veces no existe: es el caso de $x^2 + y^2 = -1$.

Puntos racionales en cónicas $C : aX^2 + bY^2 = c$

Si $a = b = c = 1$, encontramos de nuevo $x^2 + y^2 = 1$.

Cuáles son las soluciones con coordenadas x, y racionales de la ecuación C? Es decir, cómo podemos calcular $C(\mathbb{Q})$?

El método de la recta funciona exactamente igual que antes... si existe una solución racional base $P = (x, y) \in C(\mathbb{Q})$.

Y a veces no existe: es el caso de $x^2 + y^2 = -1$.

Si existe una solución $P = (x, y) \in C(\mathbb{Q})$, entonces existen infinitas, "tantas como $\mathbb{P}^1(\mathbb{Q})$".

Puntos racionales en cónicas $C : aX^2 + bY^2 = c$

Si $a = b = c = 1$, encontramos de nuevo $x^2 + y^2 = 1$.

Cuáles son las soluciones con coordenadas x, y racionales de la ecuación C? Es decir, cómo podemos calcular $C(\mathbb{Q})$?

El método de la recta funciona exactamente igual que antes... si existe una solución racional base $P = (x, y) \in C(\mathbb{Q})$.

Y a veces no existe: es el caso de $x^2 + y^2 = -1$.

Si existe una solución $P = (x, y) \in C(\mathbb{Q})$, entonces existen infinitas, "tantas como $\mathbb{P}^1(\mathbb{Q})$".

Puntos racionales en cónicas $C : ax^2 + by^2 = c$

$X^2 + Y^2 = 3Z^2$ no tiene soluciones enteras primitivas: no las hay ni siquiera módulo 4.

Puntos racionales en cónicas $C : ax^2 + by^2 = c$

$X^2 + Y^2 = 3Z^2$ no tiene soluciones enteras primitivas: no las hay ni siquiera módulo 4.

Adrien-Marie Legendre (1752–1833)

Teorema (Legendre). La cónica $C : aX^2 + bY^2 = cZ^2$ tiene soluciones enteras primitivas si y sólo si tiene soluciones reales y soluciones enteras primitivas módulo n para todo $n \geq 2$.

El principio de Hasse

Las ecuaciones que tienen este comportamiento se dice que satisfacen el *principio de Hasse*.

El principio de Hasse

Las ecuaciones que tienen este comportamiento se dice que satisfacen el *principio de Hasse*.

Un ejemplo de ecuación que no lo satisface fue encontrado por Ernst Selmer: la cúbica

$$C : 3X^3 + 4Y^3 = 5Z^3$$

satisface:

- $C(\mathbb{R}) \neq \emptyset$.
- $C(\mathbb{Z}/n\mathbb{Z}) \neq \emptyset$ para todo $n \geq 2$.
- $C(\mathbb{Z}) = \emptyset$ (y por tanto tampoco hay soluciones racionales de la ecuación $3x^3 + 4y^3 = 5$).

Ecuaciones $E : f(x, y) = 0$ de grado $d \geq 3$

Supongamos que E admite al menos una solución racional.

Ecuaciones $E : f(x, y) = 0$ de grado $d \geq 3$

Supongamos que E admite al menos una solución racional.

(a) Si $d \leq 2$, entonces E tiene infinitas soluciones racionales.

(b) Si $d = 3$, E puede tener un número finito o infinito de soluciones racionales.

(c) Si $d \geq 4$, E tiene sólo un número finito de soluciones racionales.

Puntos racionales en cúbicas.

Sea $E : f(x, y, z) = 0$ una ecuación de grado homogéneo 3 con coeficientes en $\mathbb{Z}$.

Puntos racionales en cúbicas.

Sea $E : f(x, y, z) = 0$ una ecuación de grado homogéneo 3 con coeficientes en $\mathbb{Z}$.

A veces $E(\mathbb{Z}) = \emptyset$, por ejemplo para $E : 3X^3 + 4Y^3 - 5Z^3 = 0$.

Puntos racionales en cúbicas.

Sea $E : f(x, y, z) = 0$ una ecuación de grado homogéneo 3 con coeficientes en $\mathbb{Z}$.

A veces $E(\mathbb{Z}) = \emptyset$, por ejemplo para $E : 3X^3 + 4Y^3 - 5Z^3 = 0$.

No se conoce ningún algoritmo que permita decidir **si** $E(\mathbb{Z})$ **es vacío o no** en un número finito de pasos.

Puntos racionales en cúbicas.

Sea $E : f(x, y, z) = 0$ una ecuación de grado homogéneo 3 con coeficientes en $\mathbb{Z}$.

A veces $E(\mathbb{Z}) = \emptyset$, por ejemplo para $E : 3X^3 + 4Y^3 - 5Z^3 = 0$.

No se conoce ningún algoritmo que permita decidir **si** $E(\mathbb{Z})$ **es vacío o no** en un número finito de pasos.

Si existe un punto $O \in E(\mathbb{Z})$, entonces se puede efectuar un cambio de variables de manera que

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3,$$

$$\Delta(E) := -16(4A^3 + 27B^2) \neq 0$$

Puntos racionales en cúbicas.

Sea $E : f(x, y, z) = 0$ una ecuación de grado homogéneo 3 con coeficientes en $\mathbb{Z}$.

A veces $E(\mathbb{Z}) = \emptyset$, por ejemplo para $E : 3X^3 + 4Y^3 - 5Z^3 = 0$.

No se conoce ningún algoritmo que permita decidir **si** $E(\mathbb{Z})$ **es vacío o no** en un número finito de pasos.

Si existe un punto $O \in E(\mathbb{Z})$, entonces se puede efectuar un cambio de variables de manera que

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3,$$

$$\Delta(E) := -16(4A^3 + 27B^2) \neq 0 \quad \text{y} \quad O = (0, 1, 0).$$

Puntos racionales en cúbicas.

Sea $E : f(x, y, z) = 0$ una ecuación de grado homogéneo 3 con coeficientes en $\mathbb{Z}$.

A veces $E(\mathbb{Z}) = \emptyset$, por ejemplo para $E : 3X^3 + 4Y^3 - 5Z^3 = 0$.

No se conoce ningún algoritmo que permita decidir **si** $E(\mathbb{Z})$ **es vacío o no** en un número finito de pasos.

Si existe un punto $O \in E(\mathbb{Z})$, entonces se puede efectuar un cambio de variables de manera que

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3,$$

$$\Delta(E) := -16(4A^3 + 27B^2) \neq 0 \quad \text{y} \quad O = (0, 1, 0).$$

Estas ecuaciones diofánticas se llaman **curvas elípticas**.

Curvas elípticas

La aplicación $(X, Y, Z) \mapsto (\frac{x}{z}, \frac{y}{z})$ da una biyección entre

- el conjunto $E(\mathbb{Z})$ de soluciones enteras primitivas de

$$Y^2Z = X^3 + AXZ^2 + BZ^3,$$

- el conjunto

$$E(\mathbb{Q}) := \{(x, y) \in \mathbb{Q} \times \mathbb{Q},\ y^2 = x^3 + Ax + B\} \cup \{O\}.$$

Curvas elípticas

Ejemplo: $E : y^2 = x^3 - x$.

Curvas elípticas

Ejemplo: $E : y^2 = x^3 - x$.

$E(\mathbb{Q}) = \{O, (-1, 0), (0, 0), (1, 0)...\}$.

Curvas elípticas

Ejemplo: $E : y^2 = x^3 - x$.

$E(\mathbb{Q}) = \{O, (-1, 0), (0, 0), (1, 0)...\}$.

Ejemplo: $E : y^2 = x^3 + 17$.

Ejemplo: $E : y^2 = x^3 - x$.

$E(\mathbb{Q}) = \{O, (-1, 0), (0, 0), (1, 0)...\}$.

Ejemplo: $E : y^2 = x^3 + 17$.

$$E(\mathbb{Q}) = \{O, (-1, \pm 4), (-2, \pm 3), (2, \pm 5), (4, \pm 9), (8, \pm 23),$$
$$(\frac{137}{64}, \frac{2651}{512}), (\frac{298927}{40401}, \frac{166830380}{8120601})...\}$$

Ejemplo: $E : y^2 = x^3 - x$.

$E(\mathbb{Q}) = \{O, (-1, 0), (0, 0), (1, 0)...\}$.

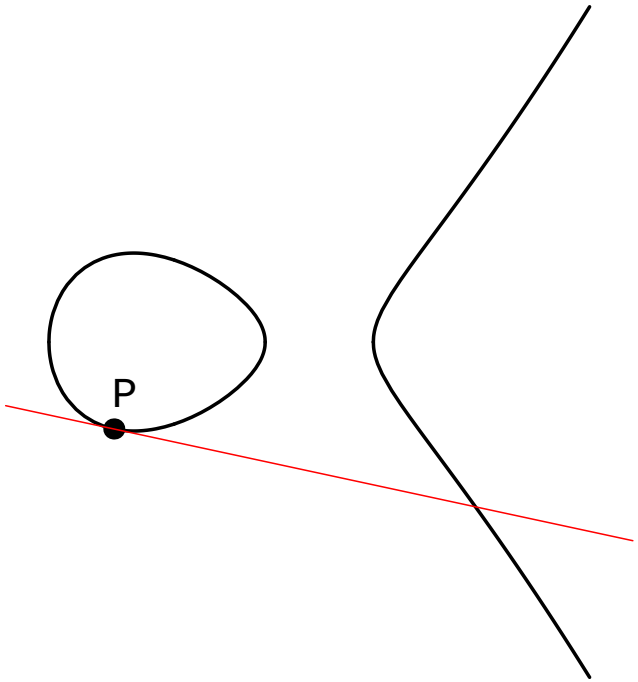
Ejemplo: $E : y^2 = x^3 + 17$.

$$E(\mathbb{Q}) = \{O, (-1, \pm 4), (-2, \pm 3), (2, \pm 5), (4, \pm 9), (8, \pm 23),$$
$$(\frac{137}{64}, \frac{2651}{512}), (\frac{298927}{40401}, \frac{166830380}{8120601})...\}$$

Cómo hemos podido calcular esos puntos?

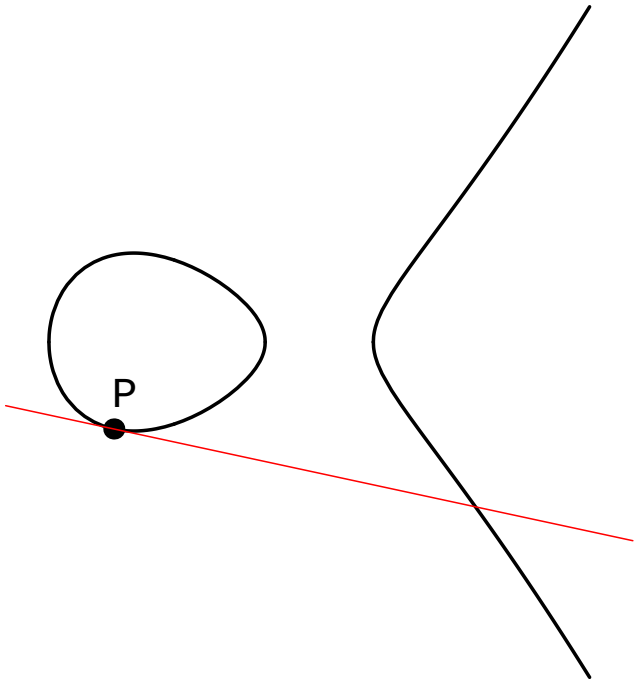
Tomamos como punto base $P = (-1, 4)$.

Tomamos como punto base $P = (-1, 4)$.



Encontramos $(\frac{137}{64}, \frac{2651}{512})$ como el *tercer* punto de intersección de la recta tangente en P con la curva E.

Tomamos como punto base $P = (-1, 4)$.



Encontramos $(\frac{137}{64}, \frac{2651}{512})$ como el *tercer* punto de intersección de la recta tangente en P con la curva E.

Ahora tomamos $P = (\frac{137}{64}, \frac{2651}{512})$ como punto base y repetimos el mismo proceso.

Curvas elípticas

Dada una curva elíptica $E : y^2 = x^3 + Ax + B$:

Curvas elípticas

Dada una curva elíptica $E : y^2 = x^3 + Ax + B$:

Cómo podemos encontrar todas sus soluciones racionales?

Curvas elípticas

Dada una curva elíptica $E : y^2 = x^3 + Ax + B$:

Cómo podemos encontrar todas sus soluciones racionales?

Cuándo es $E(\mathbb{Q})$ un conjunto finito y cuándo infinito?

Curvas elípticas

Dada una curva elíptica $E : y^2 = x^3 + Ax + B$:

Cómo podemos encontrar todas sus soluciones racionales?

Cuándo es $E(\mathbb{Q})$ un conjunto finito y cuándo infinito?

Recordad que un número a es congruente si y sólo si $\sharp E_a(\mathbb{Q}) = \infty$ donde

$$E_a : y^2 = x^3 - a^2 x.$$

Curvas elípticas

Dada una curva elíptica $E : y^2 = x^3 + Ax + B$:

Cómo podemos encontrar todas sus soluciones racionales?

Cuándo es $E(\mathbb{Q})$ un conjunto finito y cuándo infinito?

Recordad que un número a es congruente si y sólo si $\sharp E_a(\mathbb{Q}) = \infty$ donde

$$E_a : y^2 = x^3 - a^2 x.$$

Cómo es $E(\mathbb{Q})$? Tiene alguna estructura interna?

La conjetura de Birch y Swinnerton-Dyer

La conjetura de Birch y Swinnerton-Dyer da una descripción de la *estructura algebraica* del conjunto $E(\mathbb{Q})$

La conjetura de Birch y Swinnerton-Dyer

La conjetura de Birch y Swinnerton-Dyer da una descripción de la *estructura algebraica* del conjunto $E(\mathbb{Q})$ a partir del *orden de anulación* en el punto $s = 1$ de una función analítica

$$\zeta_E(s) : \mathbb{C} \longrightarrow \mathbb{C},$$

la *función zeta* o *función L* de E.

La conjetura de Birch y Swinnerton-Dyer

La conjetura de Birch y Swinnerton-Dyer da una descripción de la *estructura algebraica* del conjunto $E(\mathbb{Q})$ a partir del *orden de anulación* en el punto $s = 1$ de una función analítica

$$\zeta_E(s) : \mathbb{C} \longrightarrow \mathbb{C},$$

la *función zeta* o *función L* de E.

Existe una versión más refinada de la conjetura que predice cuál es el valor del primer coeficiente no nulo en el desarrollo de Taylor de la función $L_E(s)$ en $s = 1$ a partir del comportamiento aritmético de E.

La estructura algebraica de $E(\mathbb{Q})$

Si un polinomio $p(x) \in \mathbb{Q}[x]$ de grado 2 tiene 1 raíz racional, entonces la segunda raíz también debe ser racional.

La estructura algebraica de $E(\mathbb{Q})$

Si un polinomio $p(x) \in \mathbb{Q}[x]$ de grado 2 tiene 1 raíz racional, entonces la segunda raíz también debe ser racional.

$\Rightarrow$ Si una cónica tiene un punto racional, tiene infinitos.

La estructura algebraica de $E(\mathbb{Q})$

Si un polinomio $p(x) \in \mathbb{Q}[x]$ de grado 2 tiene 1 raíz racional, entonces la segunda raíz también debe ser racional.

$\Rightarrow$ Si una cónica tiene un punto racional, tiene infinitos.

Si un polinomio $p(x) \in \mathbb{Q}[x]$ de grado 3 tiene 2 raíces racionales, entonces la tercera raíz también debe ser racional.

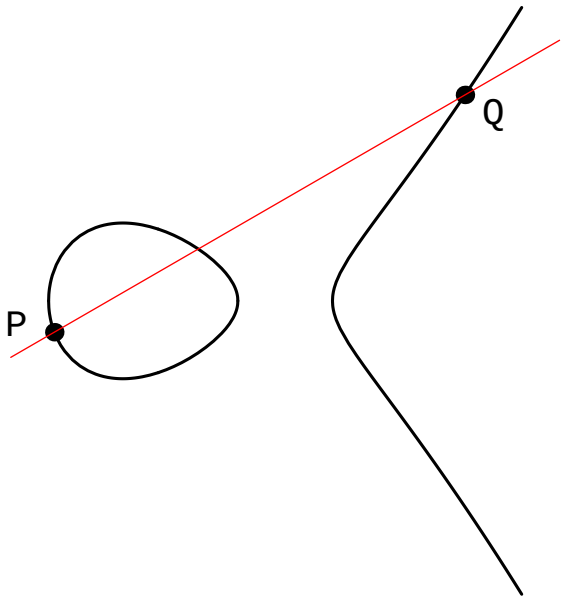
La estructura algebraica de $E(\mathbb{Q})$

Si un polinomio $p(x) \in \mathbb{Q}[x]$ de grado 2 tiene 1 raíz racional, entonces la segunda raíz también debe ser racional.

$\Rightarrow$ Si una cónica tiene un punto racional, tiene infinitos.

Si un polinomio $p(x) \in \mathbb{Q}[x]$ de grado 3 tiene 2 raíces racionales, entonces la tercera raíz también debe ser racional.

En una curva elíptica E: $P_1, P_2 \in E(\mathbb{Q}) \Rightarrow P_3 \in E(\mathbb{Q})$.



La estructura algebraica de $E(\mathbb{Q})$

Cuando los dos puntos P_1 y P_2 están alineados verticalmente,

La estructura algebraica de $E(\mathbb{Q})$

Cuando los dos puntos P_1 y P_2 están alineados verticalmente, el tercer punto de intersección es

$$P_3 = O.$$

La estructura algebraica de $E(\mathbb{Q})$

Cuando los dos puntos P_1 y P_2 están alineados verticalmente, el tercer punto de intersección es

$$P_3 = O.$$

Si tomamos $P_1 = O$, la recta que *une* O con $P_2 = (x_2, y_2)$ es

La estructura algebraica de $E(\mathbb{Q})$

Cuando los dos puntos P_1 y P_2 están alineados verticalmente, el tercer punto de intersección es

$$P_3 = O.$$

Si tomamos $P_1 = O$, la recta que *une* O con $P_2 = (x_2, y_2)$ es la recta vertical

$$x = x_2$$

La estructura algebraica de $E(\mathbb{Q})$

Cuando los dos puntos P_1 y P_2 están alineados verticalmente, el tercer punto de intersección es

$$P_3 = O.$$

Si tomamos $P_1 = O$, la recta que *une* O con $P_2 = (x_2, y_2)$ es la recta vertical

$$x = x_2$$

y el tercer punto de intersección es

$$P_3 = (x_2, -y_2).$$

La estructura algebraica de $E(\mathbb{Q})$

Cuando los dos puntos P_1 y P_2 están alineados verticalmente, el tercer punto de intersección es

$$P_3 = O.$$

Si tomamos $P_1 = O$, la recta que *une* O con $P_2 = (x_2, y_2)$ es la recta vertical

$$x = x_2$$

y el tercer punto de intersección es

$$P_3 = (x_2, -y_2).$$

Si $P_1 = P_2 = O$, decretamos que $P_3 = O$.

Tenemos así una *operación* $'\oplus'$ en el conjunto $E(\mathbb{Q})$.

$$E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow E(\mathbb{Q}), \quad (P_1, P_2) \mapsto P_3 := P_1 \oplus P_2.$$

Tenemos así una *operación* $'\oplus'$ en el conjunto $E(\mathbb{Q})$.

$$E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow E(\mathbb{Q}), \quad (P_1, P_2) \mapsto P_3 := P_1 \oplus P_2.$$

Si $P = (x, y) \in E(\mathbb{Q})$, definimos $-P := (x, -y) \in E(\mathbb{Q})$.

Tenemos así una *operación* $'\oplus'$ en el conjunto $E(\mathbb{Q})$.

$$E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow E(\mathbb{Q}), \quad (P_1, P_2) \mapsto P_3 := P_1 \oplus P_2.$$

Si $P = (x, y) \in E(\mathbb{Q})$, definimos $-P := (x, -y) \in E(\mathbb{Q})$.

Se satisface

$$P \oplus O = -P, \quad P \oplus (-P) = O, \quad O \oplus O = O.$$

Tenemos así una *operación* $'\oplus'$ en el conjunto $E(\mathbb{Q})$.

$$E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow E(\mathbb{Q}), \quad (P_1, P_2) \mapsto P_3 := P_1 \oplus P_2.$$

Si $P = (x, y) \in E(\mathbb{Q})$, definimos $-P := (x, -y) \in E(\mathbb{Q})$.

Se satisface

$$P \oplus O = -P, \quad P \oplus (-P) = O, \quad O \oplus O = O.$$

La operación $\oplus$ es *conmutativa*

Tenemos así una *operación* $'\oplus'$ en el conjunto $E(\mathbb{Q})$.

$$E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow E(\mathbb{Q}), \quad (P_1, P_2) \mapsto P_3 := P_1 \oplus P_2.$$

Si $P = (x, y) \in E(\mathbb{Q})$, definimos $-P := (x, -y) \in E(\mathbb{Q})$.

Se satisface

$$P \oplus O = -P, \quad P \oplus (-P) = O, \quad O \oplus O = O.$$

La operación $\oplus$ es *conmutativa* pero carece de elemento neutro.

La estructura algebraica de $E(\mathbb{Q})$

El candidato natural para elemento neutro sería el punto O,

La estructura algebraica de $E(\mathbb{Q})$

El candidato natural para elemento neutro sería el punto O, pero no es verdad que

$$P \oplus O = P.$$

La estructura algebraica de $E(\mathbb{Q})$

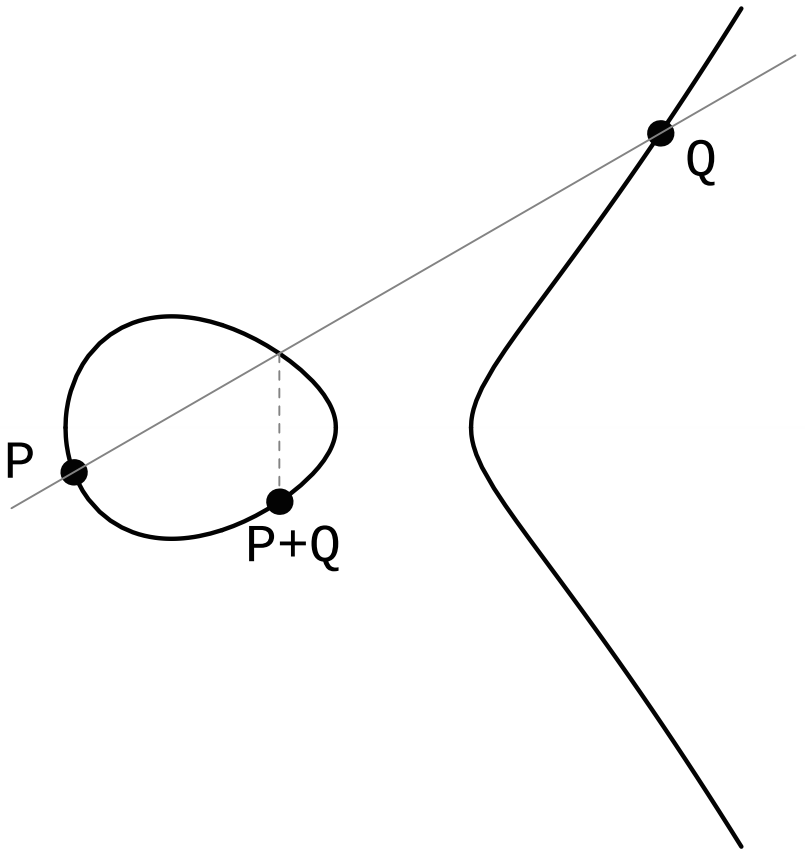
El candidato natural para elemento neutro sería el punto O, pero no es verdad que

$$P \oplus O = P.$$

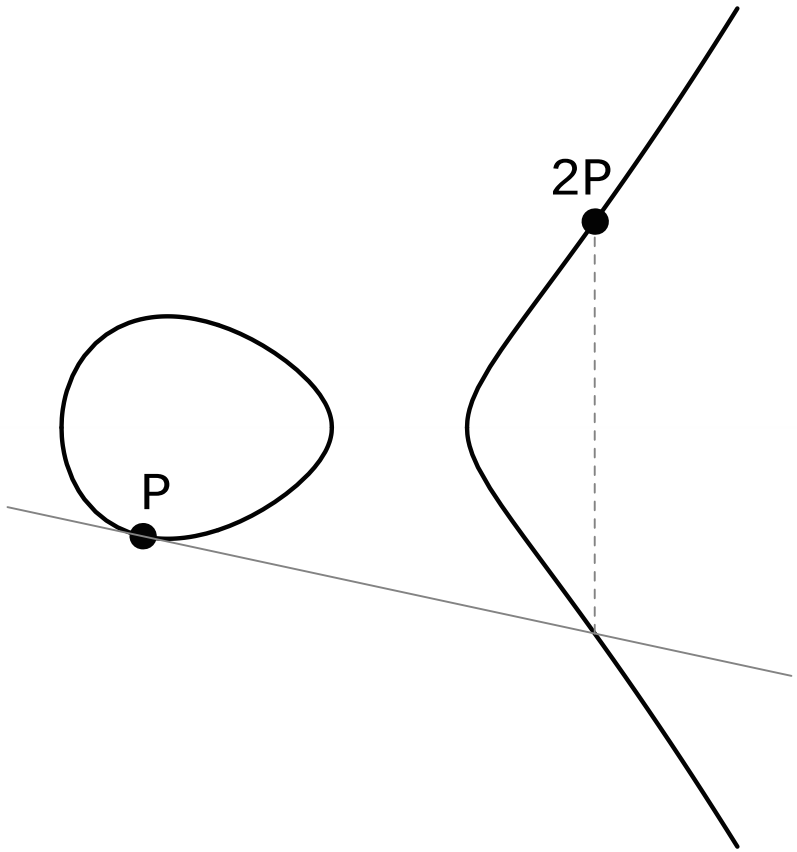
Lo arreglamos definiendo la operación modificada:

$$E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow E(\mathbb{Q}), \quad P_1 + P_2 := -(P_1 \oplus P_2).$$

La estructura algebraica de $E(\mathbb{Q})$



El resultado de operar P y Q con la operación $+$.



El resultado de la operación $P + P$, que simplemente denotamos $2P$.

La estructura algebraica de $E(\mathbb{Q})$

El conjunto $E(\mathbb{Q})$ con la operación $+$ es un **grupo abeliano** con elemento neutro O.

La estructura algebraica de $E(\mathbb{Q})$

El conjunto $E(\mathbb{Q})$ con la operación $+$ es un **grupo abeliano** con elemento neutro O.

Ejemplos más básicos de grupos abelianos son $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$, con la operación $+$ usual y el número 0 como elemento neutro.

La estructura algebraica de $E(\mathbb{Q})$

El conjunto $E(\mathbb{Q})$ con la operación $+$ es un **grupo abeliano** con elemento neutro O.

Ejemplos más básicos de grupos abelianos son $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$, con la operación $+$ usual y el número 0 como elemento neutro.

Dados $P \in E(\mathbb{Q})$ y $n > 0$,

$$n \cdot P = P + \overset{n}{\ldots} + P,$$

La estructura algebraica de $E(\mathbb{Q})$

El conjunto $E(\mathbb{Q})$ con la operación $+$ es un **grupo abeliano** con elemento neutro O.

Ejemplos más básicos de grupos abelianos son $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$, con la operación $+$ usual y el número 0 como elemento neutro.

Dados $P \in E(\mathbb{Q})$ y $n > 0$,

$$n \cdot P = P + \overset{n}{\ldots} + P,$$

$$-n \cdot P = (-P) + \overset{n}{\ldots} + (-P),$$

La estructura algebraica de $E(\mathbb{Q})$

El conjunto $E(\mathbb{Q})$ con la operación $+$ es un **grupo abeliano** con elemento neutro O.

Ejemplos más básicos de grupos abelianos son $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$, con la operación $+$ usual y el número 0 como elemento neutro.

Dados $P \in E(\mathbb{Q})$ y $n > 0$,

$$n \cdot P = P + \overset{n}{\ldots} + P,$$

$$-n \cdot P = (-P) + \overset{n}{\ldots} + (-P),$$

$$0 \cdot P = O.$$

La estructura algebraica de $E(\mathbb{Q})$

El orden de un punto $P \in E(\mathbb{Q})$ es el menor $n > 0$ tal que $n \cdot P = O$.

La estructura algebraica de $E(\mathbb{Q})$

El orden de un punto $P \in E(\mathbb{Q})$ es el menor $n > 0$ tal que $n \cdot P = O$.

Por ejemplo, $\mathrm{ord}(O) = 1$.

La estructura algebraica de $E(\mathbb{Q})$

El orden de un punto $P \in E(\mathbb{Q})$ es el menor $n > 0$ tal que $n \cdot P = O$.

Por ejemplo, $\mathrm{ord}(O) = 1$.

Si no existe ningún $n > 0$ tal que $n \cdot P = O$, $\mathrm{ord}(P) = \infty$.

La estructura algebraica de $E(\mathbb{Q})$

El orden de un punto $P \in E(\mathbb{Q})$ es el menor $n > 0$ tal que $n \cdot P = O$.

Por ejemplo, $\mathrm{ord}(O) = 1$.

Si no existe ningún $n > 0$ tal que $n \cdot P = O$, $\mathrm{ord}(P) = \infty$.

El conjunto de puntos de torsión de $E(\mathbb{Q})$ es

$$E(\mathbb{Q})_{tors} := \{\, P \in E(\mathbb{Q}),\ \mathrm{ord}(P) \text{ es finito} \,\}.$$

La estructura algebraica de $E(\mathbb{Q})$

$$E : y^2 = x^3 - x$$

La estructura algebraica de $E(\mathbb{Q})$

$$E : y^2 = x^3 - x$$

$$E(\mathbb{Q}) = \{O, P = (-1, 0), Q = (0, 0), R = (1, 0)\}$$

La estructura algebraica de $E(\mathbb{Q})$

$$E : y^2 = x^3 - x$$

$$E(\mathbb{Q}) = \{O, P = (-1, 0), Q = (0, 0), R = (1, 0)\}$$

$$\begin{array}{ccc} E(\mathbb{Q}) = \{O, (-1,0), (0,0), (1,0)\} & \xrightarrow{\sim} & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ O & \mapsto & (\bar{0}, \bar{0}) \\ P & \mapsto & (\bar{0}, \bar{1}) \\ Q & \mapsto & (\bar{1}, \bar{0}) \\ R & \mapsto & (\bar{1}, \bar{1}) \end{array}$$

La estructura algebraica de $E(\mathbb{Q})$

$$E : y^2 = x^3 + 17$$

La estructura algebraica de $E(\mathbb{Q})$

$$E : y^2 = x^3 + 17$$

$$E(\mathbb{Q}) = \{O, P_1 = (-1, 4), P_2 = (\frac{137}{64}, -\frac{2651}{512}),$$

$$P_3 = (\frac{298927}{40401}, \frac{166830380}{8120601}),$$

$$P_4 = (-\frac{4531991647}{1799117056}, -\frac{76914444719857}{76311349047296})...\}$$

La estructura algebraica de $E(\mathbb{Q})$

$$E : y^2 = x^3 + 17$$

$$E(\mathbb{Q}) = \{O, P_1 = (-1, 4), P_2 = (\frac{137}{64}, -\frac{2651}{512}),$$

$$P_3 = (\frac{298927}{40401}, \frac{166830380}{8120601}),$$

$$P_4 = (-\frac{4531991647}{1799117056}, -\frac{76914444719857}{76311349047296})...\}$$

$$P_2 = 2P_1, \quad P_3 = 3P_1 \quad \text{y} \quad P_4 = 4P_1$$

La estructura algebraica de $E(\mathbb{Q})$

$$E : y^2 = x^3 + 17$$

$$E(\mathbb{Q}) = \{O, P_1 = (-1, 4), P_2 = (\frac{137}{64}, -\frac{2651}{512}),$$

$$P_3 = (\frac{298927}{40401}, \frac{166830380}{8120601}),$$

$$P_4 = (-\frac{4531991647}{1799117056}, -\frac{76914444719857}{76311349047296})...\}$$

$$P_2 = 2P_1, \quad P_3 = 3P_1 \quad \text{y} \quad P_4 = 4P_1$$

La sucesión de puntos racionales que se obtiene al iterar indefinidamente el algoritmo de la recta tangente es $P_1, -2P_1, 4P_1, -8P_1, 16P_1, -32P_1...$

La estructura algebraica de $E(\mathbb{Q})$

Teorema. (Mordell)

(a) $E(\mathbb{Q})_{tors}$ es un subgrupo *finito* de $E(\mathbb{Q})$ de tamaño menor o igual que 16.

(b) Existen un número $r \geq 0$ y puntos $Q_1, ..., Q_r \in E(\mathbb{Q})$ de orden infinito tales que todo punto $Q \in E(\mathbb{Q})$ puede expresarse de manera única como

$$Q = n_1 Q_1 + ... + n_r Q_r + T$$

donde $n_1, ..., n_r \in \mathbb{Z}$ son números enteros y $T \in E(\mathbb{Q})_{tors}$ es un punto de torsión.

La estructura algebraica de $E(\mathbb{Q})$

Teorema. (Mordell)

(a) $E(\mathbb{Q})_{tors}$ es un subgrupo *finito* de $E(\mathbb{Q})$ de tamaño menor o igual que 16.

(b) Existen un número $r \geq 0$ y puntos $Q_1, ..., Q_r \in E(\mathbb{Q})$ de orden infinito tales que todo punto $Q \in E(\mathbb{Q})$ puede expresarse de manera única como

$$Q = n_1 Q_1 + ... + n_r Q_r + T$$

donde $n_1, ..., n_r \in \mathbb{Z}$ son números enteros y $T \in E(\mathbb{Q})_{tors}$ es un punto de torsión.

Es decir, el grupo abeliano $E(\mathbb{Q})$ está *finitamente generado*.

La estructura algebraica de $E(\mathbb{Q})$

Teorema. (Mordell)

(a) $E(\mathbb{Q})_{tors}$ es un subgrupo *finito* de $E(\mathbb{Q})$ de tamaño menor o igual que 16.

(b) Existen un número $r \geq 0$ y puntos $Q_1, ..., Q_r \in E(\mathbb{Q})$ de orden infinito tales que todo punto $Q \in E(\mathbb{Q})$ puede expresarse de manera única como

$$Q = n_1 Q_1 + ... + n_r Q_r + T$$

donde $n_1, ..., n_r \in \mathbb{Z}$ son números enteros y $T \in E(\mathbb{Q})_{tors}$ es un punto de torsión.

Es decir, el grupo abeliano $E(\mathbb{Q})$ está *finitamente generado*.
El número r que aparece en el enunciado del teorema de Mordell se llama el **rango** de $E(\mathbb{Q})$.

La estructura algebraica de $E(\mathbb{Q})$

$$E : y^2 = x^3 - x,$$

La estructura algebraica de $E(\mathbb{Q})$

$$E : y^2 = x^3 - x, \quad E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

La estructura algebraica de $E(\mathbb{Q})$

$$E : y^2 = x^3 - x, \quad E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad r = 0.$$

La estructura algebraica de $E(\mathbb{Q})$

$$E : y^2 = x^3 - x, \quad E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad r = 0.$$

$$E : y^2 = x^3 + 17,$$

La estructura algebraica de $E(\mathbb{Q})$

$$E : y^2 = x^3 - x, \quad E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad r = 0.$$

$$E : y^2 = x^3 + 17, \quad E(\mathbb{Q}) = \mathbb{Z} \cdot (-1, 4) \oplus \mathbb{Z} \cdot (-2, 3),$$

La estructura algebraica de $E(\mathbb{Q})$

$$E : y^2 = x^3 - x, \quad E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad r = 0.$$

$$E : y^2 = x^3 + 17, \quad E(\mathbb{Q}) = \mathbb{Z} \cdot (-1, 4) \oplus \mathbb{Z} \cdot (-2, 3), \quad r = 2.$$

La estructura algebraica de $E(\mathbb{Q})$

$$E : y^2 = x^3 - x, \quad E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad r = 0.$$

$$E : y^2 = x^3 + 17, \quad E(\mathbb{Q}) = \mathbb{Z} \cdot (-1, 4) \oplus \mathbb{Z} \cdot (-2, 3), \quad r = 2.$$

Conjetura. Existen curvas elípticas con rango r arbitrariamente grande.

La estructura algebraica de $E(\mathbb{Q})$

$$E : y^2 = x^3 - x, \quad E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad r = 0.$$

$$E : y^2 = x^3 + 17, \quad E(\mathbb{Q}) = \mathbb{Z} \cdot (-1, 4) \oplus \mathbb{Z} \cdot (-2, 3), \quad r = 2.$$

Conjetura. Existen curvas elípticas con rango r arbitrariamente grande.

La curva elíptica de mayor rango conocido tiene $r = 28$. (Elkies 2006).

La estructura algebraica de $E(\mathbb{Q})$

$$E : y^2 = x^3 - x, \quad E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad r = 0.$$

$$E : y^2 = x^3 + 17, \quad E(\mathbb{Q}) = \mathbb{Z} \cdot (-1, 4) \oplus \mathbb{Z} \cdot (-2, 3), \quad r = 2.$$

Conjetura. Existen curvas elípticas con rango r arbitrariamente grande.

La curva elíptica de mayor rango conocido tiene $r = 28$. (Elkies 2006).

Conjetura. El 50 % de las curvas elípticas tiene $r = 0$ y el otro 50 % tiene $r = 1$.

La función zeta de E

La función zeta de Riemann

$$\zeta : \{s \in \mathbb{C},\ \mathrm{Re}(s) > 1\} \longrightarrow \mathbb{C}, \quad \zeta(s) := \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p} \frac{1}{(1 - p^{-s})}$$

es la función zeta de $\mathbb{Z}$.

La función zeta de E

La función zeta de Riemann

$$\zeta : \{s \in \mathbb{C},\ \mathrm{Re}(s) > 1\} \longrightarrow \mathbb{C}, \quad \zeta(s) := \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p} \frac{1}{(1 - p^{-s})}$$

es la función zeta de $\mathbb{Z}$.

Se extiende a todo $\mathbb{C}$ con un polo en $s = 1$

La función zeta de E

La función zeta de Riemann

$$\zeta : \{s \in \mathbb{C},\ \mathrm{Re}(s) > 1\} \longrightarrow \mathbb{C}, \quad \zeta(s) := \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p} \frac{1}{(1 - p^{-s})}$$

es la función zeta de $\mathbb{Z}$.

Se extiende a todo $\mathbb{C}$ con un polo en $s = 1$ y $\zeta(s) \leftrightarrow \zeta(1 - s)$.

La función zeta de E

La función zeta de Riemann

$$\zeta : \{s \in \mathbb{C},\, \mathrm{Re}(s) > 1\} \longrightarrow \mathbb{C}, \quad \zeta(s) := \sum_{n \geq 1} \frac{1}{n^s} = \prod_p \frac{1}{(1 - p^{-s})}$$

es la función zeta de $\mathbb{Z}$.

Se extiende a todo $\mathbb{C}$ con un polo en $s = 1$ y $\zeta(s) \leftrightarrow \zeta(1 - s)$.

A muchos objetos o *motivos* aritméticos M se sabe asociar

$$L_M(s) := \prod_{p \nmid \Delta(M)} \frac{1}{L_p(p^{-s})}$$

La función zeta de E

La función zeta de Riemann

$$\zeta : \{s \in \mathbb{C},\ \mathrm{Re}(s) > 1\} \longrightarrow \mathbb{C}, \quad \zeta(s) := \sum_{n \geq 1} \frac{1}{n^s} = \prod_p \frac{1}{(1 - p^{-s})}$$

es la función zeta de $\mathbb{Z}$.

Se extiende a todo $\mathbb{C}$ con un polo en $s = 1$ y $\zeta(s) \leftrightarrow \zeta(1 - s)$.

A muchos objetos o *motivos* aritméticos M se sabe asociar

$$L_M(s) := \prod_{p \nmid \Delta(M)} \frac{1}{L_p(p^{-s})}$$

$\Delta(M) \in \mathbb{Z}$ se llama el *discriminante* de M.

La función zeta de E

La función zeta de Riemann

$$\zeta : \{s \in \mathbb{C},\ \mathrm{Re}(s) > 1\} \longrightarrow \mathbb{C}, \quad \zeta(s) := \sum_{n \geq 1} \frac{1}{n^s} = \prod_p \frac{1}{(1 - p^{-s})}$$

es la función zeta de $\mathbb{Z}$.

Se extiende a todo $\mathbb{C}$ con un polo en $s = 1$ y $\zeta(s) \leftrightarrow \zeta(1 - s)$.

A muchos objetos o *motivos* aritméticos M se sabe asociar

$$L_M(s) := \prod_{p \nmid \Delta(M)} \frac{1}{L_p(p^{-s})}$$

$\Delta(M) \in \mathbb{Z}$ se llama el *discriminante* de M.

$L_p(T) \in \mathbb{Z}[T]$ es un polinomio de grado $d \geq 1$ fijo.

La función zeta de E

Sea $E: \ y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}, \quad \Delta(E) \neq 0.$

La función zeta de E

Sea $E: \ y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}, \quad \Delta(E) \neq 0.$

Dado $p \nmid \Delta(E)$, sea $\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, ..., \overline{p-1}\}$.

La función zeta de E

Sea $E: \ y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}, \quad \Delta(E) \neq 0.$

Dado $p \nmid \Delta(E)$, sea $\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, ..., \overline{p-1}\}$.

$E(\mathbb{Z}/p\mathbb{Z}) = \{O\} \cup \{(\bar{x}, \bar{y}) : \ \bar{y}^2 \equiv \bar{x}^3 + \bar{A} \cdot \bar{x} + \bar{B} \bmod p\}.$

La función zeta de E

Sea $E:\ y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}, \quad \Delta(E) \neq 0.$

Dado $p \nmid \Delta(E)$, sea $\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, ..., \overline{p-1}\}$.

$$E(\mathbb{Z}/p\mathbb{Z}) = \{O\} \cup \{(\bar{x}, \bar{y}) :\ \bar{y}^2 \equiv \bar{x}^3 + \bar{A} \cdot \bar{x} + \bar{B} \bmod p\}.$$

$$\sharp E(\mathbb{Z}/p\mathbb{Z}) = p + 1 - a_p \text{ con } a_p \in \mathbb{Z},\ |a_p| \leq 2\sqrt{p}. \text{ (Hasse)}$$

La función zeta de E

Sea $E:\ y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}, \quad \Delta(E) \neq 0.$

Dado $p \nmid \Delta(E)$, sea $\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, ..., \overline{p-1}\}$.

$$E(\mathbb{Z}/p\mathbb{Z}) = \{O\} \cup \{(\bar{x}, \bar{y}) :\ \bar{y}^2 \equiv \bar{x}^3 + \bar{A} \cdot \bar{x} + \bar{B} \bmod p\}.$$

$$\sharp E(\mathbb{Z}/p\mathbb{Z}) = p + 1 - a_p \text{ con } a_p \in \mathbb{Z},\ |a_p| \leq 2\sqrt{p}. \text{ (Hasse)}$$

La función zeta de E

La función zeta de E es

$$\zeta_E(s) = \prod_{p \nmid \Delta(E)} \frac{1}{1 - a_p \cdot p^{-s} + p \cdot p^{-2s}}.$$

La función zeta de E

La función zeta de E es

$$\zeta_E(s) = \prod_{p \nmid \Delta(E)} \frac{1}{1 - a_p \cdot p^{-s} + p \cdot p^{-2s}}.$$

Converge para $\mathrm{Re}(s) > \frac{3}{2}$.

La función zeta de E

La función zeta de E es

$$\zeta_E(s) = \prod_{p \nmid \Delta(E)} \frac{1}{1 - a_p \cdot p^{-s} + p \cdot p^{-2s}}.$$

Converge para $\mathrm{Re}(s) > \frac{3}{2}$.

Teorema de Wiles. ζ_E extiende a una función entera en $\mathbb{C}$

La función zeta de E

La función zeta de E es

$$\zeta_E(s) = \prod_{p \nmid \Delta(E)} \frac{1}{1 - a_p \cdot p^{-s} + p \cdot p^{-2s}}.$$

Converge para $\mathrm{Re}(s) > \frac{3}{2}$.

Teorema de Wiles. ζ_E extiende a una función entera en $\mathbb{C}$ y

$$\zeta(s) \leftrightarrow \zeta(2 - s).$$

La función zeta de E

La función zeta de E es

$$\zeta_E(s) = \prod_{p \nmid \Delta(E)} \frac{1}{1 - a_p \cdot p^{-s} + p \cdot p^{-2s}}.$$

Converge para $\mathrm{Re}(s) > \frac{3}{2}$.

Teorema de Wiles. ζ_E extiende a una función entera en $\mathbb{C}$ y

$$\zeta(s) \leftrightarrow \zeta(2 - s).$$

El punto $s = 1$ es el centro de simetría.

La función zeta de E

La función zeta de E es

$$\zeta_E(s) = \prod_{p \nmid \Delta(E)} \frac{1}{1 - a_p \cdot p^{-s} + p \cdot p^{-2s}}.$$

Converge para $\mathrm{Re}(s) > \frac{3}{2}$.

Teorema de Wiles. ζ_E extiende a una función entera en $\mathbb{C}$ y

$$\zeta(s) \leftrightarrow \zeta(2 - s).$$

El punto $s = 1$ es el centro de simetría.

La conjetura de Birch y Swinnerton-Dyer

Qué relación guarda la función $\zeta_E(s)$ con el rango r?

La conjetura de Birch y Swinnerton-Dyer

Qué relación guarda la función $\zeta_E(s)$ con el rango r?

B. Birch y P. Swinnerton-Dyer se dejaron llevar por

$$\text{"}L_E(1)\text{"} := \prod_{p \nmid \Delta(E)} \frac{1}{1 - a_p \cdot p^{-1} + p \cdot p^{-2}} =$$

$$= \prod_{p \nmid \Delta(E)} \frac{p}{p - a_p + 1} = \prod_{p \nmid \Delta(E)} \frac{p}{\sharp E(\mathbb{Z}/p\mathbb{Z})}$$

La conjetura de Birch y Swinnerton-Dyer

Qué relación guarda la función $\zeta_E(s)$ con el rango r?

B. Birch y P. Swinnerton-Dyer se dejaron llevar por

$$\text{"}L_E(1)\text{"} := \prod_{p \nmid \Delta(E)} \frac{1}{1 - a_p \cdot p^{-1} + p \cdot p^{-2}} =$$

$$= \prod_{p \nmid \Delta(E)} \frac{p}{p - a_p + 1} = \prod_{p \nmid \Delta(E)} \frac{p}{\sharp E(\mathbb{Z}/p\mathbb{Z})}$$

Inviertiendo, nos conduce a estudiar el comportamiento asintótico de:

$$\mathrm{BSD}_E : \mathbb{N} \longrightarrow \mathbb{R}, \quad \mathrm{BSD}_E(x) = \prod_{p<x} \frac{\sharp E(\mathbb{Z}/p\mathbb{Z})}{p}$$

cuando $x \longrightarrow \infty$.

Inviertiendo, nos conduce a estudiar el comportamiento asintótico de:

$$\mathrm{BSD}_E : \mathbb{N} \longrightarrow \mathbb{R}, \quad \mathrm{BSD}_E(x) = \prod_{p<x} \frac{\sharp E(\mathbb{Z}/p\mathbb{Z})}{p}$$

cuando $x \longrightarrow \infty$.

Cuanto mayor es r,

La conjetura de Birch y Swinnerton-Dyer

Inviertiendo, nos conduce a estudiar el comportamiento asintótico de:

$$\mathrm{BSD}_E : \mathbb{N} \longrightarrow \mathbb{R}, \quad \mathrm{BSD}_E(x) = \prod_{p<x} \frac{\sharp E(\mathbb{Z}/p\mathbb{Z})}{p}$$

cuando $x \longrightarrow \infty$.

Cuanto mayor es r, más puntos debe haber en $E(\mathbb{Z}/p\mathbb{Z})$ al variar p

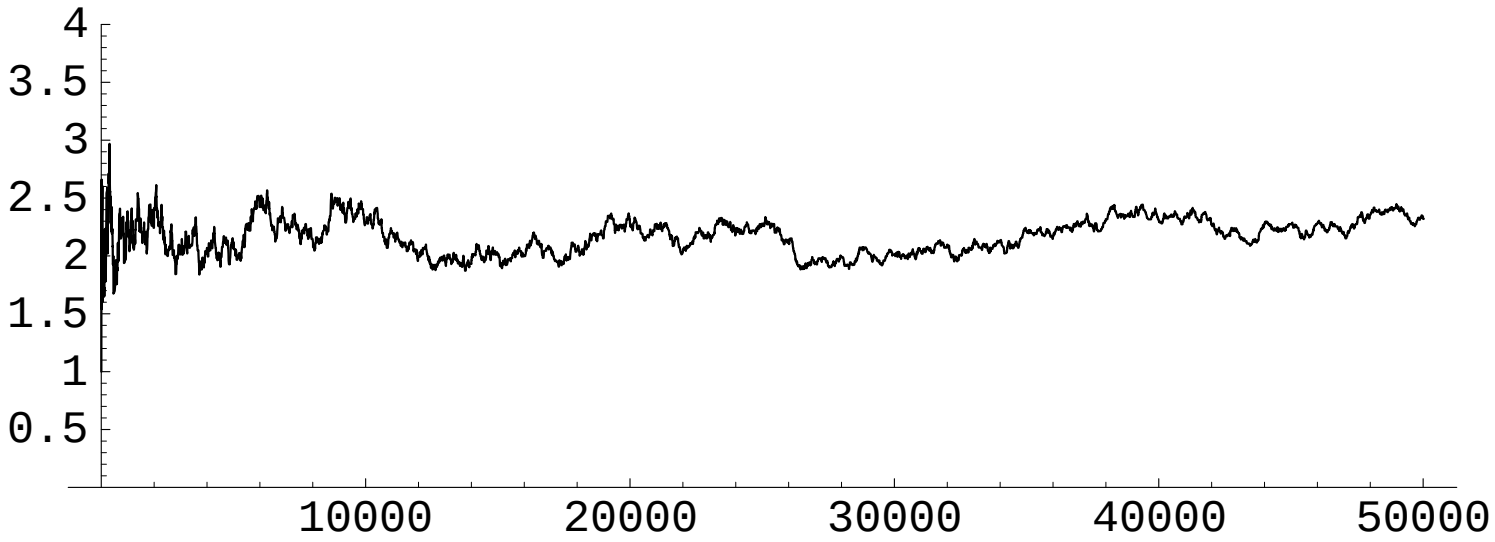
Inviertiendo, nos conduce a estudiar el comportamiento asintótico de:

$$\mathrm{BSD}_E : \mathbb{N} \longrightarrow \mathbb{R}, \quad \mathrm{BSD}_E(x) = \prod_{p<x} \frac{\sharp E(\mathbb{Z}/p\mathbb{Z})}{p}$$

cuando $x \longrightarrow \infty$.

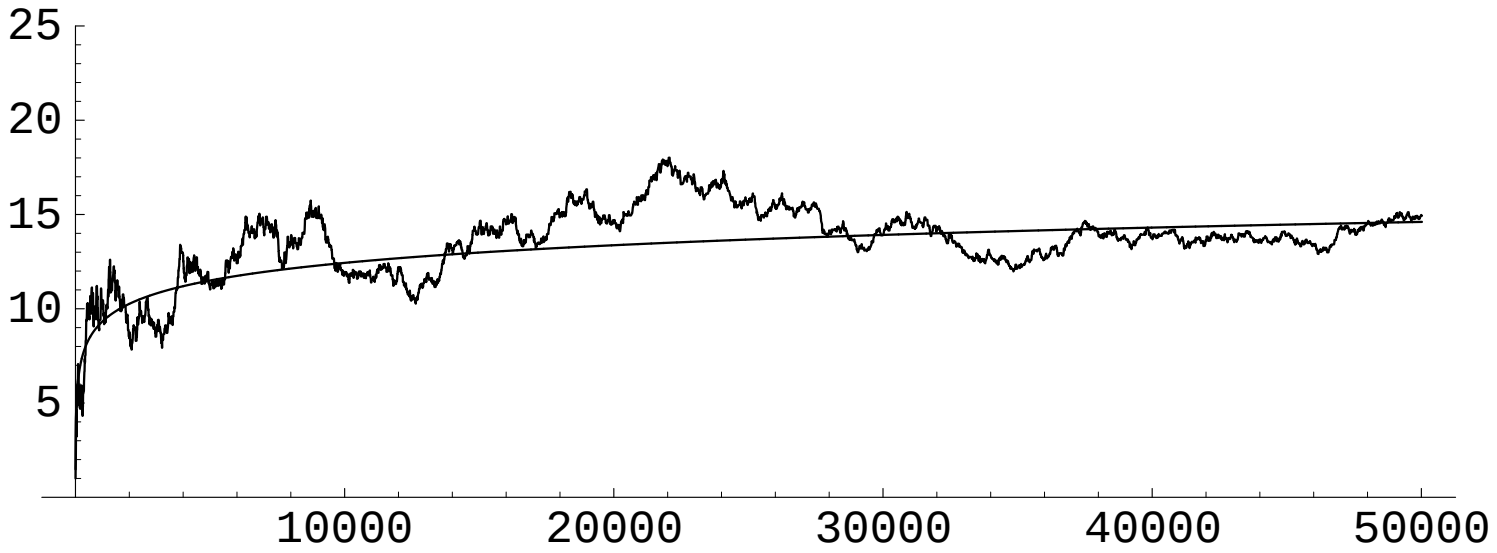
Cuanto mayor es r, más puntos debe haber en $E(\mathbb{Z}/p\mathbb{Z})$ al variar p y "por tanto" BSD_E crece más rápido.

La conjetura de Birch y Swinnerton-Dyer



La función BSD_E para la curva elíptica $E : y^2 = x^3 - x$ de rango $r = 0$. Su comportamiento asintótico es comparable al de una función constante $f(x) = A$, donde $A \sim 2$.

La conjetura de Birch y Swinnerton-Dyer



La función BSD_E para la curva elíptica $E : y^2 = x^3 - 5x$ de rango $r = 1$. Su comportamiento asintótico es comparable al de la función $f(x) = A \cdot \log(x)$ para un valor adecuado de la constante A.

La conjetura de Birch y Swinnerton-Dyer

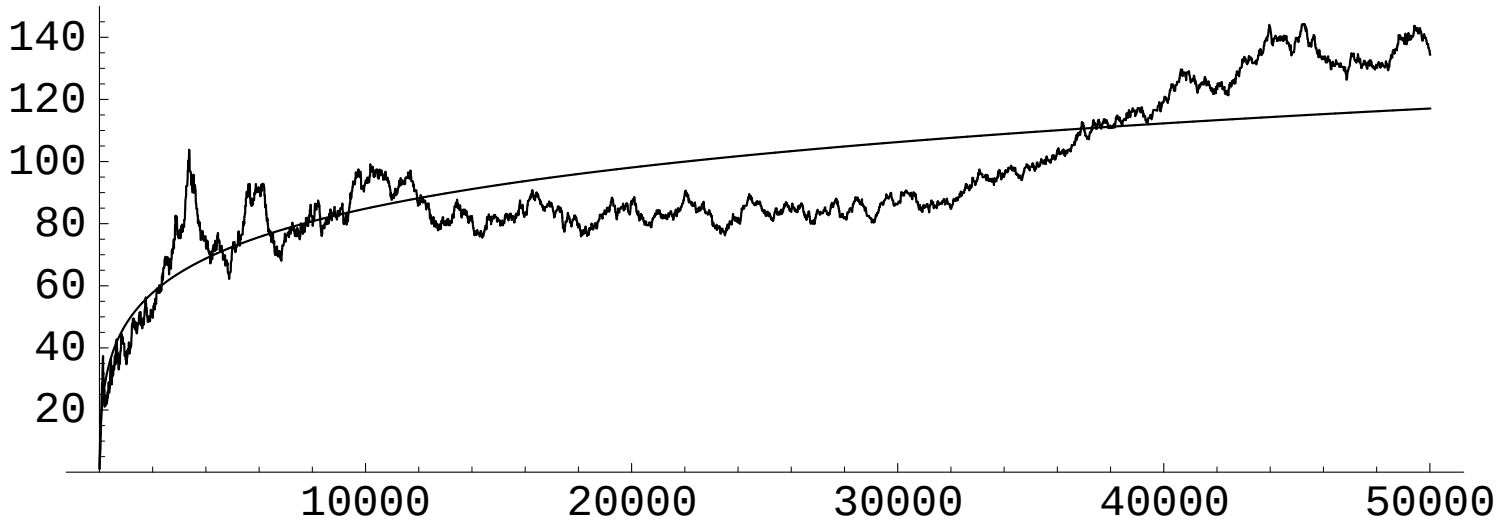


Figura: La función BSD_E para la curva elíptica $E : y^2 = x^3 - 17x$ de rango $r = 2$. Su comportamiento asintótico es comparable al de la función $f(x) = A \cdot \log^2(x)$ para un valor adecuado de la constante A.

La conjetura de Birch y Swinnerton-Dyer

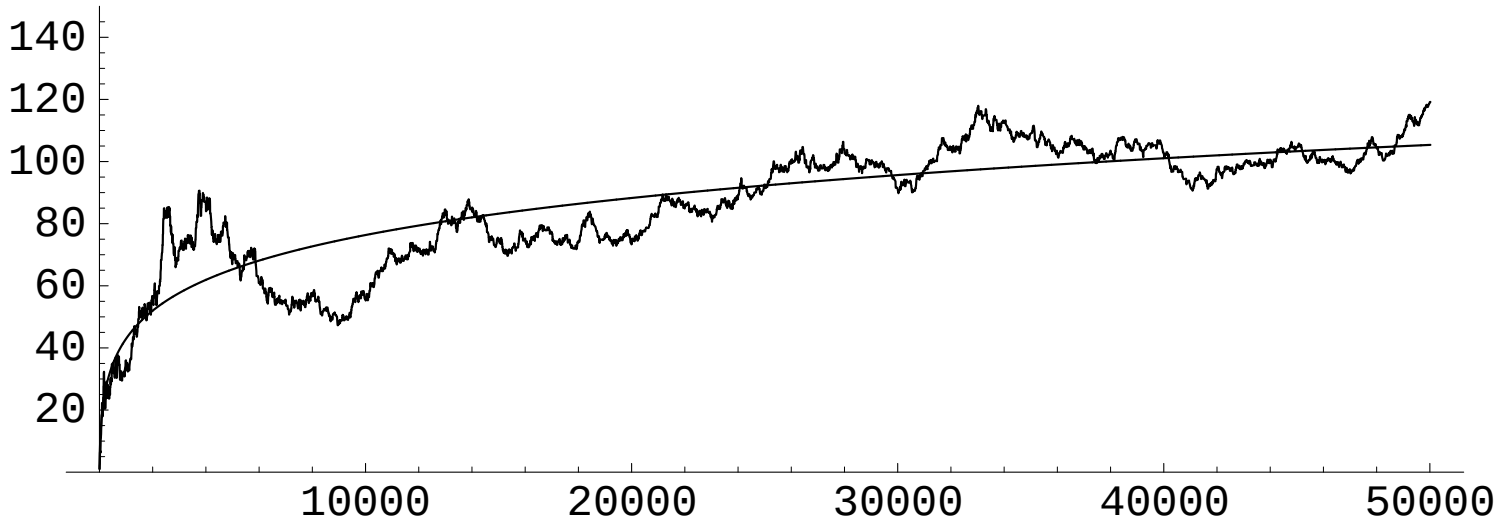


Figura: La función BSD_E para la curva elíptica $E : y^2 = x^3 - 56x$ de rango $r = 3$. Su comportamiento asintótico es comparable al de la función $f(x) = A \cdot \log^3(x)$ para un valor adecuado de la constante A.

La conjetura de Birch y Swinnerton-Dyer

Conjetura. [Birch y Swinnerton-Dyer] Sea E una curva elíptica y sea r su rango. Entonces

$$\mathrm{BSD}_E(x) \sim A \cdot \log^r(x).$$

La conjetura de Birch y Swinnerton-Dyer

Conjetura. [Birch y Swinnerton-Dyer] Sea E una curva elíptica y sea r su rango. Entonces

$$\mathrm{BSD}_E(x) \sim A \cdot \log^r(x).$$

Equivalentemente:

Conjetura. [Birch y Swinnerton-Dyer] El desarrollo de Taylor de la función $\zeta_E(s)$ en $s = 1$ es

$$c(s-1)^r + \text{ términos de orden superior.}$$

La conjetura de Birch y Swinnerton-Dyer

Conjetura. [Birch y Swinnerton-Dyer] Sea E una curva elíptica y sea r su rango. Entonces

$$\mathrm{BSD}_E(x) \sim A \cdot \log^r(x).$$

Equivalentemente:

Conjetura. [Birch y Swinnerton-Dyer] El desarrollo de Taylor de la función $\zeta_E(s)$ en $s = 1$ es

$$c(s-1)^r + \text{ términos de orden superior.}$$

Lo abreviamos: $r(E) \stackrel{?}{=} r_{an}(E)$.

La conjetura de Birch y Swinnerton-Dyer

Generalizaciones naturales

Se puede formular en contextos más generales como:

Generalizaciones naturales

Se puede formular en contextos más generales como:

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

$$A, B \in K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(e^{2\pi i 7}), \mathbb{Q}(\sqrt[5]{2})...$$

Generalizaciones naturales

Se puede formular en contextos más generales como:

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

$$A, B \in K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(e^{2\pi i 7}), \mathbb{Q}(\sqrt[5]{2})...$$

- Variedades abelianas: curvas elípticas de dimensión superior.

Generalizaciones naturales

Se puede formular en contextos más generales como:

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

$$A, B \in K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(e^{2\pi i 7}), \mathbb{Q}(\sqrt[5]{2})...$$

- Variedades abelianas: curvas elípticas de dimensión superior.

- Motivos: subcocientes de la cohomología de una variedad algebraica.

Resultados

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

Resultados

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

Teorema. [Coates, Wiles, V. Kolyvagin, B. H. Gross, D. Zagier, S. Zhang] Sea $K = \mathbb{Q}(\sqrt{-d})$.

Resultados

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

Teorema. [Coates, Wiles, V. Kolyvagin, B. H. Gross, D. Zagier, S. Zhang] Sea $K = \mathbb{Q}(\sqrt{-d})$.

- Si $\zeta_{E/K}(1) \neq 0 \quad \Rightarrow \quad r(E(K)) = 0$.

Resultados

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

Teorema. [Coates, Wiles, V. Kolyvagin, B. H. Gross, D. Zagier, S. Zhang] Sea $K = \mathbb{Q}(\sqrt{-d})$.

- Si $\zeta_{E/K}(1) \neq 0 \quad \Rightarrow \quad r(E(K)) = 0.$
- Si $\zeta_{E/K}(1) = 0, \zeta'_{E/K}(1) \neq 0 \quad \Rightarrow \quad r(E(K)) = 1.$

Resultados

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

Teorema. [Coates, Wiles, V. Kolyvagin, B. H. Gross, D. Zagier, S. Zhang] Sea $K = \mathbb{Q}(\sqrt{-d})$.

- Si $\zeta_{E/K}(1) \neq 0 \quad \Rightarrow \quad r(E(K)) = 0$.
- Si $\zeta_{E/K}(1) = 0, \zeta'_{E/K}(1) \neq 0 \quad \Rightarrow \quad r(E(K)) = 1$.

Corolario. Si $r_{an}(E/\mathbb{Q}) \leq 1 \quad \Rightarrow \quad r(E(\mathbb{Q})) = r_{an}(E/\mathbb{Q})$.