

# DE FIBONACCI Y FERMAT HASTA...

Fermat no se hacía preguntas tontas

29 de Julio de 2015

J. SOTO

Made with ❤️ for ENEM



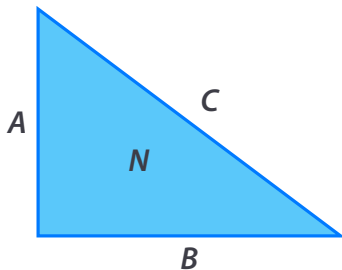
# **ACTO I: LA PREGUNTA**

# FERMAT, 1640

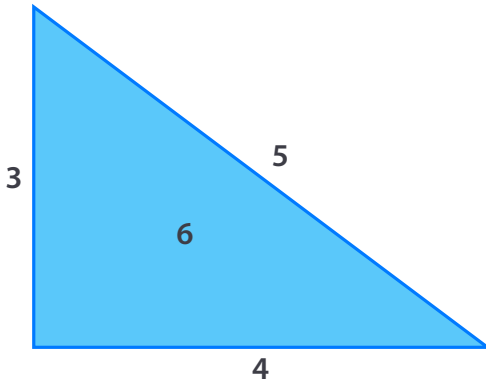


Wikipedia: Pierre de Fermat

¿Qué números enteros  $N \geq 1$  son el área de un triángulo rectángulo de lados racionales?



# EJEMPLO



Por tanto, 6 es “especial”.

# WHAT'S IN A NAME? (SHAKESPEARE, 1597)

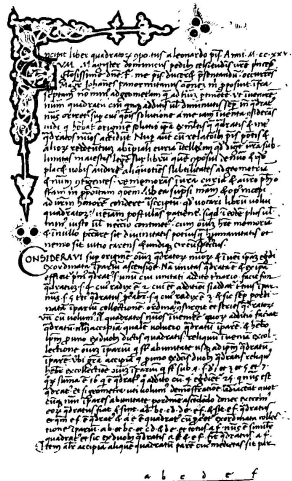
## Definición

Los  $N \in \mathbb{Z}, N \geq 1$  tales que

$$N = \frac{1}{2}AB, \quad A^2 + B^2 = C^2, \quad A, B, C \in \mathbb{Q},$$

se llaman *números congruentes*.

# FIBONACCI, 1225



Beginning of *Liber quadratorum* by Leonardo Pisano. From "Il Libro dei Quadrati di Leonardo Pisano" in *Physis: Rivista Internazionale di Storia della Scienza*, 1979, p. 197. Reprinted with permission of the author, Ettore Picutti.

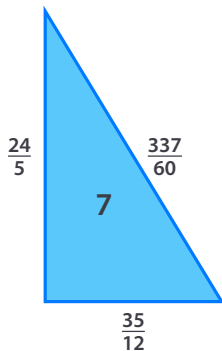
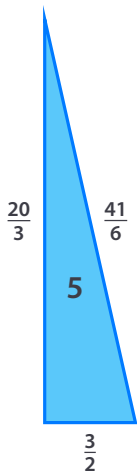
## Definición

Un *congruum* es un entero  $N$  tal que existe otro entero  $x$  con  $x^2 \pm N$  también cuadrados.

## Teorema (Fibonacci)

5 y 7 son *congrua* (y por tanto congruentes).

# DEMOSTRACIÓN





# MÁS PREGUNTAS

1. ¿Es 1 un número congruente? (Fermat: **No.**)
2. ¿Es 157 un número congruente? (Zagier: **Sí.**)
3. ¿Cuáles son los números enteros congruentes? (5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28,... )
4. ¿Cómo abordar este problema?

A scene from the animated series Futurama. Professor Farnsworth, a small, balding man with a large nose and a red topknot, is shown from the chest up, sitting inside the body of Bender, a blue robot. Bender's head is visible on the right, with its eyes closed and a grid-like mouth. The background shows a bathroom with green cabinets and a white toilet with a purple seat. The text "I am afraid we need to use..." is written in orange, and "MATH!" is written in a larger, bold orange font.

I am afraid we need to use...  
**MATH!**

—Professor Farnsworth (in Bender's Body)  
*Futurama, The Prisoner of Benda, Season 6,  
Episode 7*

## **ACTO II: ÁLGEBRA, ARITMÉTICA**

# ÁLGEBRA FTW!

Queremos resolver las ecuaciones

$$N = \frac{1}{2}AB,$$
$$A^2 + B^2 = C^2,$$

con  $A, B, C \in \mathbb{Q}, N \geq 1, N \in \mathbb{Z}$ .

Se trata de calcular la intersección de dos cuádricas.

$$N = \frac{1}{2}AB,$$
$$A^2 + B^2 = C^2,$$

Ponemos

$$x = \left(\frac{C}{2}\right)^2$$
$$y = \frac{(B^2 - A^2)C}{8},$$

y comprobamos que

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

# Teorema

Existe una biyección entre los conjuntos

$$\left\{ (A, B, C) \in \mathbb{Q}^3 \mid \frac{1}{2}AB = N \in \mathbb{N}, N \neq 0, A^2 + B^2 = C^2 \right\}$$

y

$$\{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 - N^2x, y \neq 0\}$$

dada por

$$(A, B, C) \mapsto \left( \frac{NB}{C-A}, \frac{2N^2}{C-A} \right),$$
$$(x, y) \mapsto \left( \frac{x^2 - N^2}{y}, \frac{2Nx}{y}, \frac{x^2 + N^2}{y} \right).$$

# OBJETIVO

Entender los puntos racionales de las curvas de la forma  $y^2 = x^3 - N^2x$ :

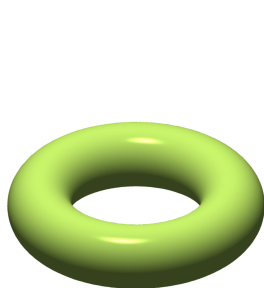
$$E_N(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 - N^2x\}.$$

# INTERMEDIO: EXCURSIÓN TOPOLÓGICA



# GÉNERO

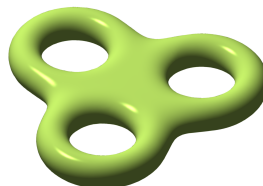
$C$  una curva dada por un polinomio  $f(x, y) \in \mathbb{Q}[x, y]$ , *lisa*.  
Existe un invariante geométrico de  $C$  que se llama género  $g$ .



Género 1



Género 2



Género 3

## Teorema (Faltings '83, Conjetura de Mordell)

Si  $g > 1$ , entonces  $C(\mathbb{Q})$  es finito.

## Ejemplo

La curva  $x^n + y^n = z^n$  no tiene soluciones enteras para  $n \geq 3$ .

## Teorema

Si  $g = 0$ ,  $C(\mathbb{Q})$  es infinito.

## Ejemplo

Existen infinitas soluciones a  $x^2 + y^2 = z^2$ . (Las ternas pitagóricas)

# GÉNERO Y PUNTOS (CASO MÁS INTERESANTE)

## No-Teorema

Si  $g = 1$ , puede pasar de todo.

1.  $y^2 = x^3 - 36x$  tiene infinitos puntos *racionales*.
2.  $y^2 = x^3 - x$  tiene tres puntos *racionales* (y otro punto racional “especial”).
3.  $y^2 = x^3 + 17^2 5x + 17^3$  no tiene puntos racionales (más que el “especial”).

## Objetivo

Entender los puntos racionales de las curvas

$$E_N(\mathbb{Q}) = \{ (x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 - N^2x \}.$$

Si tiene muchos, pocos o ninguno, cómo son, etc.

Pero esta curva no es “cualquier” curva; es una curva elíptica, ( $g = 1$ ).

# **ACTO III: CURVAS ELÍPTICAS**

## Definición

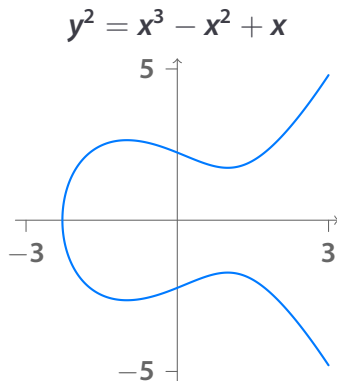
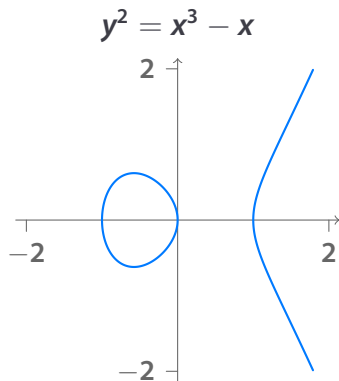
Una curva elíptica es (casi siempre) una curva lisa de la forma

$$y^2 = x^3 + ax + b.$$

(Más generalmente, una curva elíptica siempre se puede escribir en la forma

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.)$$

# UN PAR DE CURVAS ELÍPTICAS



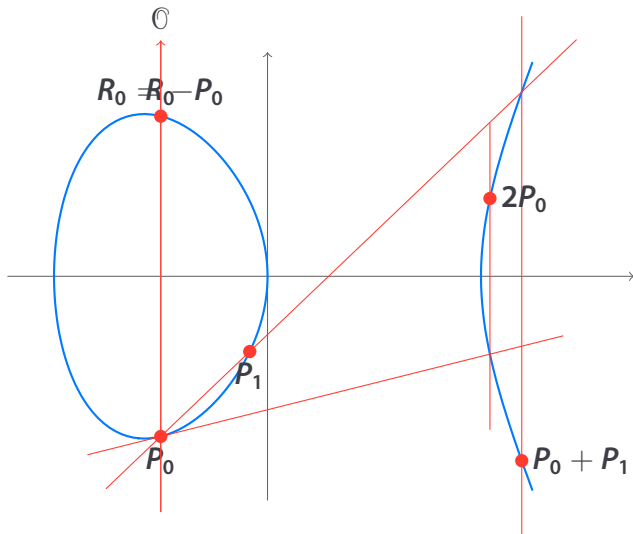


# ALGUNOS USOS DE LAS CURVAS ELÍPTICAS

1. Análisis complejo.
2. Teoría de números.
3. Criptografía.
4. Física Clásica.
5. Topología.
6. Física Moderna
7. Ganar un millón de dólares.

¿Qué tienen de especial las curvas elípticas?

# SUMA DE PUNTOS REALES



# SUMA DE PUNTOS RACIONALES

## Magia Teorema de Mordell

$E_N(\mathbb{Q})$  tiene estructura de grupo abeliano finitamente generado.

## Corolario

Por el Teorema de Estructura de Grupos Abelianos Finitamente Generados (TEGAFG),

$$E_N(\mathbb{Q}) = E_N(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r, \quad r \geq 0.$$

$r$  se llama el *rango* de la curva.

## Conjetura

Existen curvas elípticas de rango arbitrariamente grande.

**Récord de rango, Elkies (2006),  $\text{rango} \geq 28$**

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x \\ + 34481611795030556467032985690390720374855944359319180361266008296291939448732243429.$$

# EJEMPLO

Nuestra curva

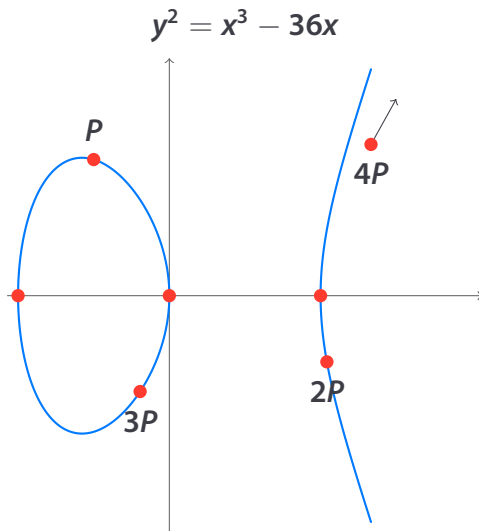
$$y^2 = x^3 - 36x$$

tiene los siguientes puntos racionales:

$$\begin{aligned} E_6(\mathbb{Q}) &= \{O, (0, 0), (\pm 6, 0)\} \times (-3, 9) \cdot \mathbb{Z} \\ &\simeq C_2 \times C_2 \times \mathbb{Z}, \end{aligned}$$

y por tanto, tiene rango 1.

# EJEMPLO



## Teorema

Sea  $E_N(\mathbb{Q})$  una de nuestras curvas elípticas especiales. Entonces

$$\begin{aligned} E_N(\mathbb{Q}) &= \{O, (0, 0), (\pm N, 0)\} \times \mathbb{Z}^r \\ &\simeq C_2 \times C_2 \times \mathbb{Z}^r. \end{aligned}$$

## Corolario

$E_N(\mathbb{Q})$  es infinito si y sólo si  $r \geq 1$ .

# EL GRAN TEOREMA

## Teorema

El entero  $N > 1$  es congruente si y sólo si  $E_N(\mathbb{Q})$  es infinito.

## Demostración

Ejercicio



## Teorema

$$\begin{aligned} N \text{ es un entero congruente} &\iff E_N(\mathbb{Q}) \text{ es infinito} \\ &\iff r \geq 1. \end{aligned}$$

Por tanto, hemos reducido el problema de saber cuándo un entero es congruente a calcular el rango de una curva elíptica.

Lo malo es que no siempre se sabe calcular el rango.

## **ACTO IV: ANÁLISIS**

Vamos a usar algo llamado la  $L$ -función de una curva elíptica, también llamada función zeta de Hasse-Weil, que “no es más” que una variante de las funciones zeta de Riemann y la  $L$ -función de Dirichlet, y que se define como un producto de Euler.

# L-FUNCIÓN

Sea  $p$  un primo (mejor si  $p \nmid 2N$ ), y consideramos el cuerpo finito  $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ . Miramos los puntos de la curva  $y^2 = x^3 - N^2x \pmod{p}$  en  $\mathbb{F}_p^2$ , y definimos

$$a_p = p + 1 - \#E_N(\mathbb{F}_p).$$

## Definición

$$L(s, E_N) = \prod_{p \nmid 2N} \frac{1}{1 - \frac{a_p}{p^s} + p^{1-2s}} \prod_{p \mid 2N} \frac{1}{1 - \frac{a_p}{p^s}}$$

## Teorema

$L(s, E_N)$  converge absolutamente para  $\Re(s) > 3/2$  (Hasse) y tiene una continuación analítica a todo  $\mathbb{C}$  (Weil).

Podemos entonces escribir el desarrollo de Taylor en  $s = 1$ ,

$$L(s, E_N) = b_0 + b_1(s - 1) + \frac{b_2}{2}(s - 1)^2 + \dots$$

Sea  $R$  el primer índice tal que  $b_R \neq 0$ .

# LA CONJETURA DE UN MILLÓN DE DÓLARES

## Conjetura de Birch y Swinnerton-Dyer (BSD)

$$R = r.$$

## Corolario

Si BSD,

$$\begin{aligned} L(1, E_N) = 0 &\iff E_N(\mathbb{Q}) \text{ es infinito} \\ &\iff N \text{ es congruente.} \end{aligned}$$

# ¿QUÉ SABEMOS SIN BSD?

## Teorema (Coates, Wiles, Kolyvagin, Kato)

Si  $R = 0$ , entonces  $r = 0$ .

## Corolario

Si  $L(1, E_N) \neq 0$  entonces  $E_N(\mathbb{Q})$  es finito y  $N$  no es congruente.

## Teorema (Gross-Zagier; Kolyvagin)

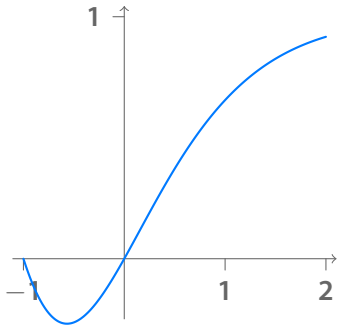
Si  $R$  es exactamente 1, entonces  $E_N(\mathbb{Q})$  es infinito.

## Teorema

1.  $L(1, E_N) \neq 0 \implies N$  no es congruente.
2.  $N$  congruente  $\implies L(1, E_N) = 0$ .
3.  $L(1, E_N) = 0$  y  $L'(1, E_N) \neq 0 \implies N$  es congruente.



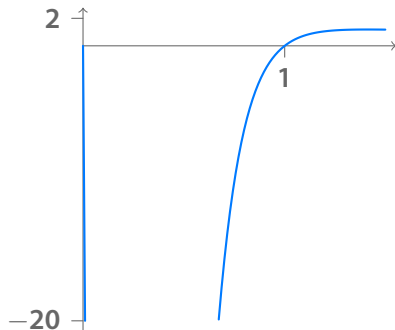
$L$ -función de  $y^2 = x^3 - x$



## Corolario

Como  $L(1, E_1) \neq 0$ , el entero 1 no es congruente.

$L$ -función de  $y^2 = x^3 - 157^2x$



Como  $F(1, E_{157}) = 0$  y  $F'(1, E_{157}) \neq 0$ , se tiene que 157 es congruente...

Podemos encontrar

$$\left( \frac{69648970982596494254458225}{166136231668185267540804}, \frac{538962435089604615078004307258785218335}{67716816556077455999228495435742408} \right) \in y^2 = x^3 - 157^2 x,$$

y encontrar  $157 = \frac{1}{2}AB$ , con  $A^2 + B^2 = C^2$ , y

$$\begin{aligned} A &= \frac{411340519227716149383203}{21666555693714761309610} \\ B &= \frac{6803298487826435051217540}{411340519227716149383203} \\ C &= \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}. \end{aligned}$$

**ONE LAST THING**

## FROM THE DOCTOR

The least important things, sometimes,  
my dear boy, lead to the greatest discoveries.

— The Doctor  
Doctor Who, S2E7,  
*The space museum.*