30 aniversario de la demostración del último teorema de Fermat I

Iván Blanco-Chacón

Universidad Complutense de Madrid

05/11/2025

Resumen

- Pitágoras de Samos (570-490 a.C.)
- Pierre de Fermat (1607-1665)
- Leonhard Euler (1707-1783)
- Sophie Germain (1773-1831) y Gabriel Lamé (1795-1870)
- Anillos de enteros algebraicos
- Ernst Kummer (1803-1893)
- De Kummer a Wiles: el premio Wolfskehl
- De Kummer a Wiles: Poincaré, Mordell y Faltings

Pitágoras de Samos (570-490 a.C.)

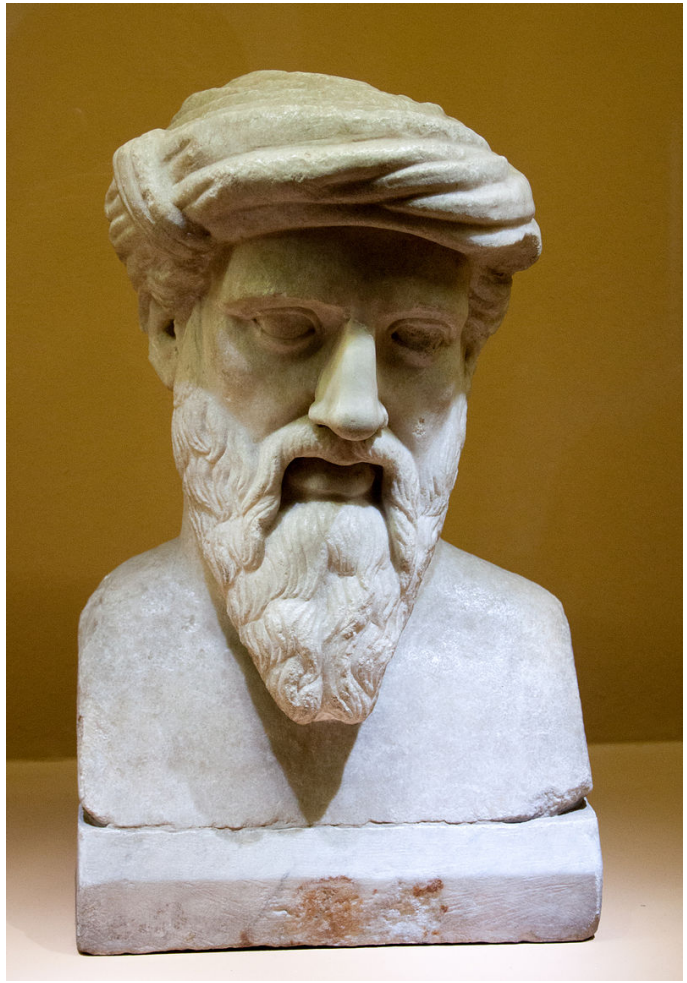


Figure: Pitágoras de Samos. Museo capitolino

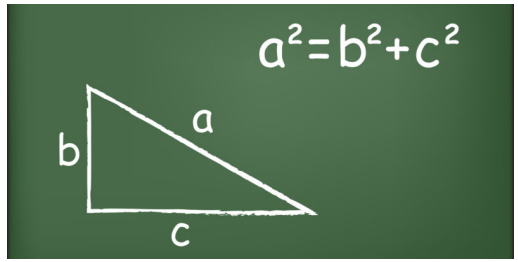
Pitágoras de Samos (570-490 a.C.)

Filósofo y matemático.
Según Diógenes Laercio habría viajado a Egipto y a Tiro, entrando en contacto con las matemáticas locales.

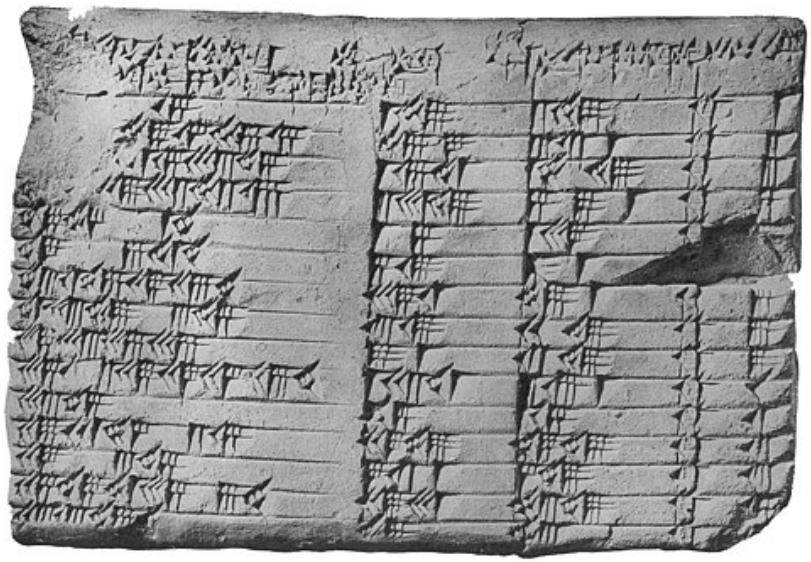
- Como filósofo influyó en Platón (inmortalidad del alma).
- Como matemático se le atribuyen: el teorema de Pitágoras, la teoría de las proporciones y la esfericidad de la tierra.
- Construyó la escala musical basada en la quinta justa.
- Fundó la escuela pitagórica (*matematikói*) en Crotona.
- No comía legumbres.
- Murió frente a un campo de habas.

Pitágoras de Samos (570-490 a.C.)

El teorema de Pitágoras:



A una terna $(a, b, c) \in \mathbb{Z}^3$ se le llama **terna pitagórica**. Si a, b y c son coprimos se llama **terna reducida**.
En la tablilla mesopotámica Plimpton 322 (1800 a.C.) se encuentra una lista de 15 ternas pitagóricas.



Pitágoras de Samos (570-490 a.C.)

Theorem

Las soluciones primitivas de la ecuación $x^2 + y^2 = z^2$ *son:*

$$\pm x = 2rs, \pm y = r^2 - s^2, \pm z = r^2 + s^2,$$

donde r *y* s *son coprimos y exactamente uno de ambos es impar.*

Proof.

Dada x, y, z solución primitiva, debe haber exactamente uno par y dos impares. Además, z no puede ser par (tomar módulo 4), luego x es par.
Ponemos:

$$x^2 = (z + y)(z - y).$$

Observamos que x, $z + y$, $z - y$ son pares y positivos. □

Pitágoras de Samos (570-490 a.C.)

Proof.

(Continuación):
Escribamos

$$x = 2u, z + y = 2v, z - y = 2w.$$

Por tanto $u^2 = vw$, con v y w coprimos.
Así pues $v = r^2$, $w = s^2$, con r y s coprimos. Finalmente:

$$z = v + w = r^2 + s^2; y = v - w = r^2 - s^2,$$

de donde $x = \pm 2rs$. Por último, como y, z impares, exactamente uno de los números r o s es impar. □

Pitágoras de Samos (570-490 a.C.)

Como consecuencia de lo anterior y del llamado método de descenso de Fermat, se deduce:

Corollary

La ecuación $x^4 + y^4 = z^4$ no tiene soluciones enteras no triviales.

Por tanto, para demostrar el último teorema de Fermat basta demostrar:

Theorem

Dado $p \geq 3$ primo, la ecuación

$$x^p + y^p = z^p$$

no tiene soluciones no triviales.

Pierre de Fermat (1607-1665)

- Graduado en leyes por la Universidad de Orleáns.
- Hablaba con soltura latín, griego, italiano y español.
- Se traslada a Burdeos en 1629, donde investiga los extremos de una función (en sus ratos libres).
- En 1636 comienza a cartearse con Marin Mersenne.
- Atacado por Descartes, quien termina reconociendo el valor de su método para calcular máximos y mínimos, que dará origen a la idea de diferencial.

Pierre de Fermat (1607-1665)

- Influenciado por el trabajo de Viéte.
- Exploró ideas fundamentales del cálculo antes que Newton o Leibniz.
- Importantes aportaciones a la geometría analítica, la probabilidad, la teoría de números.
- *...Me resulta tan difícil escribir mis demostraciones que me conformo con haber descubierto la verdad y conocer los medios para probarla cuando tengo tiempo para hacerlo.*(Carta de Fermat a Mersene)
- *...No dudo que la cosa podría haberse pulido más, pero soy el más perezoso de todos los hombres.*(Carta de Fermat a Roverbal)

Pierre de Fermat (1607-1665)

Theorem

(Pequeño teorema de Fermat) Si p es primo y $p \nmid a$, entonces

$$a^{p-1} \equiv 1 \pmod{p}.$$

Demostrado por Leibniz (inédito) y posteriormente, de manera distinta por Euler.

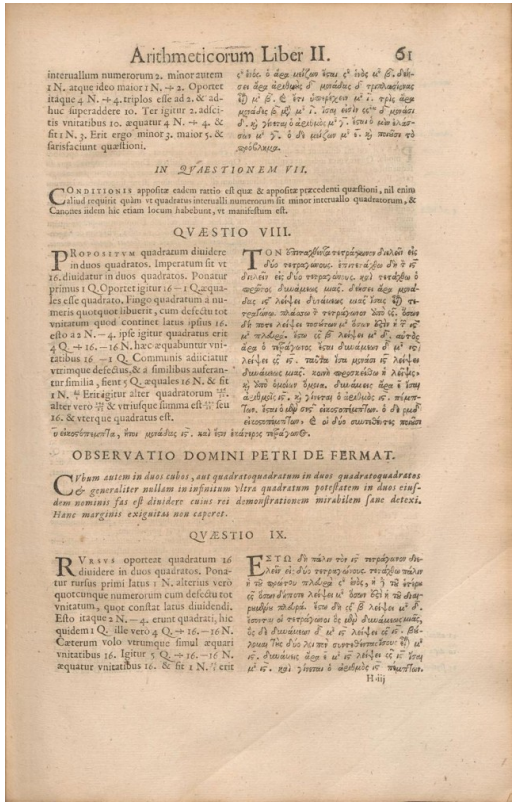
Theorem

(Teorema de Navidad/Lema de Thue) Sea p primo. Entonces p se puede escribir como suma de dos cuadrados perfectos si y sólo si $p = 2$ o $p \equiv 1 \pmod{4}$.

Demostrado por Euler.

Pierre de Fermat (1607-1665)

Cubum autem in duos cubos, aut quadratoquadratos, et generilater nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividire cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exigüitas non caperet.



Arithmeticorum Liber II. 61

IN QVÆSTIONEM VII.

QVÆSTIO VIII.

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

Figure: Diophanti arithmetica cum observationibus de Fermat

Leonhard Euler (1707-1783)

- Doesn't need introduction...
- Demostró FLT para $n = 3$ en 1770:
- Si $x^3 - y^3 = z^3$, con $xyz \neq 0$, factorizamos

$$(x - y)(x - \zeta_3 y)(x - \zeta_3^2 y) = z^3, \text{ con } \zeta_3^3 = 1.$$

Esto es una factorización en el anillo $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. Euler asumió que este anillo satisface el Teorema Fundamental de la Aritmética. Y es cierto, pero no lo demostró. Se tiene pues:

$$x + \zeta_3 y = \pm \left(\frac{2a + b}{2} + \frac{b\sqrt{-3}}{2} \right)^3 .$$

De ahí se obtiene una contradicción.

Sophie Germain (1773-1831) y Gabriel Lamé (1795-1870)

Sophie Germain: no pudo atender a la Escuela Politécnica de París, abierta en 1794.
Animada por Lagrange, dintingue dos casos $p \nmid xyz$ o p divide exactamente uno de los tres. Teorema de Sophie Germain:

Theorem

Si p es primo tal que $x^p + y^p = z^p$ tiene solución no trivial y $q = 2p + 1$ es primo, entonces $p \mid xyz$.

Dirichlet y Legendre prueban FLT para $n = 5$.
Gabriel Lamé: prueba FLT para $n = 7$. trata de generalizar el argumento de Euler, con una modificación debida a Liouville.
Pero $\mathbb{Z}[\zeta]$ no satisface el Teorema Fundamental de la Aritmética, en general!! ($p = 3, 5, 7$ lo satisfacen).

Anillos de enteros algebraicos

Sea R un anillo. Recordemos que:

- Un ideal es $I \subseteq R$ cerrado para la suma tal que para todo $a \in I$, $b \in R$ se tiene que $ab \in I$.
- Un ideal $I \in R$ es primo si dados $a, b \in R$ tales que $ab \in I$ entonces $a \in I$ o $b \in I$.
- Un ideal I es principal si $I = (a) = \{ax, x \in R\}$.
- Un dominio de ideales principales es un anillo en que todo ideal es principal, como en $\mathbb{Z}$.
- Dados I, J ideales, $I + J = \{i + j, i \in I, j \in J\}$, $IJ = \{\sum ij, i \in I, j \in J\}$ son ideales.

Teorema Fundamental de la Aritmética (TFA): Dado $n \in \mathbb{Z}$, podemos descomponer

$$n = \pm p_1^{k_1} \cdots p_r^{k_r}, \text{ con } p_i \text{ primo},$$

de manera única salvo el orden en la descomposición.

Anillos de enteros algebraicos

Sea p primo y $\zeta := \zeta_p \neq 1$ una raíz p-ésima de la unidad. El p-ésimo polinomio ciclotómico es:

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + 1.$$

El p-ésimo cuerpo ciclotómico es

$$K_p := \mathbb{Q}(\zeta) = \left\{ \frac{p(\zeta)}{q(\zeta)} : p(x), q(x) \in \mathbb{Z}[x] \right\}.$$

El anillo de enteros p-ciclotómicos es:

$$\mathbb{Z}(\zeta) = \{p(\zeta) : p(x) \in \mathbb{Z}[x]\} =$$

$$\{a_0 + a_1\zeta + a_2\zeta_2 + \ldots + a_{p-2}\zeta^{p-2}, a_i \in \mathbb{Z}\}.$$

Anillos de enteros algebraicos

Satisface $\mathbb{Z}[\zeta]$ el TFA? En primer lugar, ¿cómo deberíamos definir un elemento primo en un anillo que no sea $\mathbb{Z}$? Un dominio que satisface el TFA se llama dominio de factorización única (DFU).
Sea R un dominio.

- $\alpha \in R$ no nulo es una unidad si existe $\beta \in R$ tal que $\alpha\beta = 1$.
- $\alpha \in R$ es irreducible si $\alpha = \beta\gamma$ implica que β es unidad o γ es unidad.
- $\pi \in R$ es primo si $\pi \mid \alpha\beta$, entonces $\pi \mid \alpha$ o $\pi \mid \beta$.

Todo elemento primo en cualquier anillo es irreducible. El recíproco no es cierto en general, aunque sí lo es en $\mathbb{Z}$ o en un dominio de ideales principales.

- $\mathbb{Z}[\zeta_3]$ es DFU.
- Lamé creía que $\mathbb{Z}[\zeta]$ también lo era, para todo p.

Anillos de enteros algebraicos

En general, $\mathbb{Z}[\zeta]$ no es DFU. Sin embargo satisface la siguiente propiedad, crucial para la demostración del Último Teorema de Fermat dada por Kummer y Dedekind:

Theorem

Sea I un ideal de $\mathbb{Z}[\zeta]$. Entonces, existen unos únicos ideales primos $P_1,\ldots,P_r$ y exponentes $e_1,\ldots,e_r$ tales que

$$I = P_1^{e_1} \cdots P_r^{e_r}.$$

Un dominio que satisface esta propiedad se llama dominio de Dedekind.

Anillos de enteros algebraicos

Definimos las siguiente relación de equivalencia en los ideales de $\mathbb{Z}[\zeta]$: dos ideales $I, J \in \mathbb{Z}[\zeta]$ están relacionados si existen $\alpha, \beta \in \mathbb{Z}[\zeta]$ tales que

$$(\alpha)I = (\beta)J.$$

Esto es una relación de equivalencia y en el conjunto cociente definimos la operación

$$[I][J] = [IJ].$$

Esta operación está bien definida y convierte al conjunto cociente en un grupo $Cl(\mathbb{Z}[\zeta])$. Este grupo es finito (no trivial!!), además el neutro es la clase de los ideales principales. Denotemos por h_p su orden.

Definition

Decimos que p es un primo regular si $(p, h_p) = 1$.

Ernst Kummer (1803-1893)

Sea $p \geq 3$ primo. Supongamos que existen $x, y, z \in \mathbb{Z}$ tales que

$$x^p + y^p = z^p.$$

Podemos suponer que x, y, z son coprimos dos a dos. Supondremos además que $p \nmid xyz$. Reescribimos la ecuación como

$$x^p + y^p + z^p = 0.$$

Factoricemos como:

$$\prod_{j=0}^{p-1}(x - \zeta^j y) = -z^p,$$

donde ζ es una raíz p-ésima primitiva de la unidad. Pasando a ideales, se tiene:

$$\prod_{j=0}^{p-1}\langle x - \zeta^j y\rangle = \langle z\rangle^p.$$

Ernst Kummer (1803-1893)

A continuación se demuestra que los ideales $\langle x - \zeta^j y \rangle$ son coprimos 2 a 2. Para ello se usa la hipótesis de que $p \nmid xyz$.
Factoricemos ahora

$$\langle z \rangle = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r},$$

con los ideales $\mathfrak{p}_i$ primos. Como $\mathbb{Z}[\zeta]$ es un dominio de Dedekind, debe ser

$$\langle x - \zeta^j y \rangle = \mathfrak{a}_j^p,$$

para algún ideal $\mathfrak{a}_j$.
Pero entonces, el orden de $\mathfrak{a}_j$ en $Cl(\mathbb{Z}[\zeta])$ debe dividir a p (y por supuesto a h). Por tanto, dividirá al $mcd(p, h) = 1$, pues p es regular. Por lo tanto

$$\mathfrak{a}_j = \langle \delta \rangle,$$

así pues

$$\langle x - \zeta y \rangle = \langle \delta^p \rangle.$$

Ernst Kummer (1803-1893)

Como

$$\langle x - \zeta y \rangle = \langle \delta^p \rangle,$$

llegamos a que

$$x - \zeta y = \epsilon \delta^p,$$

donde ϵ es una unidad en $\mathbb{Z}[\zeta]$.
A continuación se demuestra que existe $r \in \mathbb{R}$ y $0 \leq g \leq p-1$ tales que

$$x - \zeta y = r\zeta^g \delta^p \longleftarrow \text{LEMA DE KUMMER.}$$

Con algo más de trabajo se llega a:

$$\zeta^{-g}(x - \zeta y) = ra \pmod{\langle p \rangle},$$

Ernst Kummer (1803-1893)

Tomando conjugados y eliminando *ra* llegamos a:

$$x\zeta^{-g} - y\zeta^{1-g} - x\zeta^{g} + y\zeta^{g-1} = \alpha p, \alpha \in \mathbb{Z}[\zeta]$$

Se sigue que $p \nmid g, g-1$. Escribamos:

$$\alpha = \frac{x}{p}\zeta^{-g} - \frac{y}{p}\zeta^{1-g} - \frac{x}{p}\zeta^{g} + \frac{y}{p}\zeta^{g-1},$$

Si los cuatro exponentes fuesen incongruentes módulo p tendríamos que $\frac{x}{p} \in \mathbb{Z}$. Contradicción.
Por tanto $2g = 1 \pmod{p}$, lo que nos lleva a:

$$x \equiv y \equiv z \pmod{p},$$

por tanto

$$p \mid 3x^{p},$$

lo que lleva a $p \mid x$ (imposible) o $p = 3$. lo que es también imposible (ejercicio).

De Kummer a Wiles: el premio Wolfskehl

- En 1905, Mirimanoff prueba FLT para $n \leq 257$ mediante el método de Kummer-Dedekind. La prueba de casos particulares se hace cada vez más técnica y complicada.
- En 1908, Paul Friedrich Wolfskehl instituye un premio de 100000 marcos (aprox. 1,7 millones de dólares actuales) a quien primero diese una prueba o contraejemplo de FLT. Tras su muerte, el premio es anunciado por la Real Sociedad Científica de Göttingen. El premio se podría cobrar hasta 2007.
- En total, la Academia de Göttingen recibió unas 5000 "demostraciones" del FLT. Otras universidades comienzan a recibir "demostraciones" del FLT. Destaca la figura de Albert Fleck (Real Sociedad Científica de Berlín).
- Fleck se encargó de revisar las "demostraciones" de FLT hasta su muerte en 1943, víctima de la persecución Nazi. Obtiene la Medalla Leibniz en 1915.

De Kummer a Wiles: el premio Wolfskehl

- Harry Schulz Vandiver (1882-1973). Avance computacional en el método de Kummer. Premio Cole de la American Mathematical Society en 1931. En 1952 prueba FLT con la ayuda de un ordenador para $n \leq 2000$.
- En 1976, se prueba FLT para $n \leq 125000$. En 1993 para $n \leq 4000000$.
- *"Meanwhile, mathematics was continuing to grow in other directions, which seemed at the time to have nothing whatsoever to do with FLT. However, history is littered with cases where mathematicians attempting to solve one problem ended up by formulating and proving something quite different."* (I. Stewart-D. Tall Algebraic Number Theory and Fermat's Last Theorem)

De Kummer a Wiles: Poincaré, Mordell y Faltings

- Poincaré había desarrollado la topología algebraica. Clasifica las superficies en función de su grupo fundamental y su género (número de *agujeros*).
- Había investigado también las funciones modulares, es decir, $f : \mathcal{H} \to \mathbb{C}$ holomorfas invariantes por $\mathrm{SL}_2(\mathbb{Z})$.
- Una curva algebraica lisa de grado n tiene género $(n-1)(n-2)/2$.
- FLT es equivalente a decir que $x^n + y^n = 1$ no tiene soluciones racionales no triviales.
- Louis Mordell (1922): Una curva de género $g \geq 2$ tiene una cantidad finita de puntos racionales. Teorema probado en 1984 por Gerd Faltings.
- La situación para $g = 1$ es completamete distinta. Mordelll prueba que si $E/\mathbb{Q}$ tiene género 1 y $E(\mathbb{Q}) \neq \emptyset$ entonces $E(\mathbb{Q}) = \mathbb{Z}^r \oplus E_{tors}$, con E_{tors} finito.

Bibliografía

- I. Stewart, D. Tall. Algebraic Number Theory and Fermat's Last Theorem (3rd Edition).
- D. Cox. Primes of the form $x^2 + ny^2$.

Figure: Sir Andrew Wiles en Cambridge, 2015

MUCHAS GRACIAS!