El análisis matemático y los números primos

José Bonet

Instituto Universitario de Matemática Pura y Aplicada

Universitat Politècnica de València

Valencia, 27 de marzo de 2014

- Malas y buenas noticias: Vamos a hablar de Matemáticas y no voy a mencionar para nada mi propio trabajo.

- Hablaremos del análisis matemático y de su relación con los números primos.

- **Advertencia:** No se presenta ninguna novedad para expertos.

- Finalidad de la conferencia: Que ustedes aprendan algo y lo pasen bien. Como dice Gian-Carlo Rota (Notices AMS 1997) "Give the audience something to take home".

“Lo que es imposible, es poco probable que ocurra”

(atribuido a un Premio Nobel de Física).

El análisis matemático

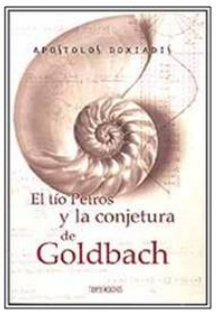
Análisis matemático es la parte de las matemáticas que se ocupa de las desigualdades, la aproximación y de las funciones y su comportamiento.

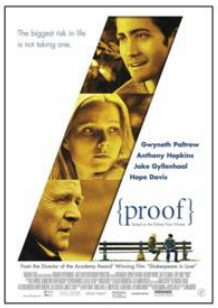
- $e^{\pi i} = -1$, $\sqrt{xy} \leq (x+y)/2$, $\log x = \int_1^x \frac{1}{t} dt$, $\lim_{n\to\infty} (1+\frac{1}{n})^n = e$.
- $1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + ... = \pi^2/6$.
- $\lim_{n\to\infty} \frac{1+\frac{1}{2}+...\frac{1}{n}}{\log n} = 1$.
- $\lim_{n\to\infty}(1 + \frac{1}{2} + ...\frac{1}{n} - \log n) = \gamma = 0,577216...$
- Aplicaciones: Ecuaciones en derivadas parciales (ondas, calor, fluidos, turbulencia, crecimiento de poblaciones,...) y tratamiento de señales (ondículas, análisis tiempo frecuencia,...)

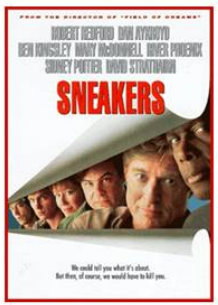
¿POR QUÉ LOS NÚMEROS PRIMOS?

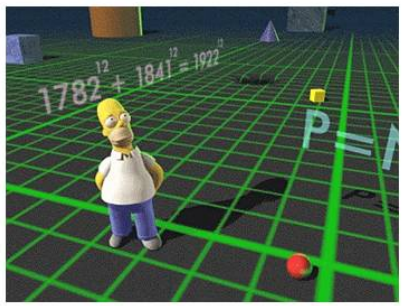
Los números primos son mediáticos

- **Libros:** Simon Singh (El enigma de Fermat), Apostolos Doxiadis (El tío Petros y...), M. Haddon (El curioso incidente del perro...), A.C. Clarke y F. Pohl (The Last Theorem, ciencia ficción)
- **Teatro:** Proof (La prueba, David Auburn), The five hysterical girls theorem (Less Gutman).
- **Musical:** Fermat's Last Tango (J. Rosenblum).
- **Cine:** Proof (2005, con Gwyneth Paltrow), Sneakers (1992, con Robert Redford), Contact (1997, con Jodie Foster), La habitación de Fermat (2007).
- **Televisión:** Los Simpson y el último Teorema de Fermat









Los números primos

Un número **primo** p es un número entero estrictamente mayor que 1 que sólo es divisible por 1 y por sí mismo.

Los números no primos se llaman **compuestos**. Ejemplo $91 = 7 \times 13$.

- **Números primos menores que 150**:
  2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149.

- **¿Por qué** 1 **no se considera primo?**
  Es una convención para que sólo exista una forma de factorizar los números compuestos.

  Henri Lebesgue consideraba 1 como un número primo.

Patrones

Búsqueda de patrones. Se trata de buscar el siguiente número:

- 3, 8, 13, 18, 23, 28,...
- 4, 12, 36, 108,...
- 1, 3, 6, 10, 15, 21,...
- 1, 1, 2, 3, 5, 8, 13, 21,...

Estaría muy bien disponer de una "fórmula" que nos diera el número primo n-ésimo. En su defecto, **conocer aproximadamente la proporción de primos menores que un número n dado.**

Resultados conocidos en Grecia 300 años a.C.

Escuela de Pitágoras (500 a.C.-300 a.C.). Elementos de Euclides, Libro IX (300 a.C.).

El teorema fundamental de la aritmética

Todo número entero $a > 1$ se puede escribir como un producto de potencias de números primos. O sea,

$$a = p_1^{e_1} \ldots p_k^{e_k},$$

donde $p_1, \ldots p_k$ son primos distintos entre sí y cada exponente e_i es positivo. La descomposición es única salvo en el orden de los números primos.

Ejemplos: $23244 = 2^2 \times 3 \times 13 \times 149$

Pregunta: ¿Es sencillo hacer descomposiciones en primos como la anterior, especialmente si el número es grande?

Resultados conocidos en Grecia 300 años a.C.

El teorema de Euclides

Existen infinitos números primos.

Demostración.
Consideremos los k primeros números primos $p_1, ..., p_k$ y calculemos el número natural $m = p_1 \times ... \times p_k + 1$.

- Si m es un número primo, ya hemos terminado la demostración.
- En caso contrario, por el teorema fundamental de la aritmética, debe tener un divisor primo p. No es posible que $p = p_j$ para algún $j = 1, ..., k$, porque el resto de dividir m por p daría 1. Luego p es un primo mayor que los k primeros.

Cuidado!: $(2 \times 3 \times 5 \times 7 \times 11 \times 13) + 1 = 30031 = 59 \times 509$.

Resultados conocidos en Grecia 300 años a.C.

La criba de Eratóstenes: Calcular todos los números primos entre 2 y n

- Se ponen todo en una lista.
- Se suprimen los múltiplos de 2 mayores que 2, luego los múltiplos de 3 mayores que 3.
- Repetimos con el primo 5.
- Nos detenemos cuando lleguemos a un número primo p que sea mayor que $\sqrt{n}$.

Algunas preguntas

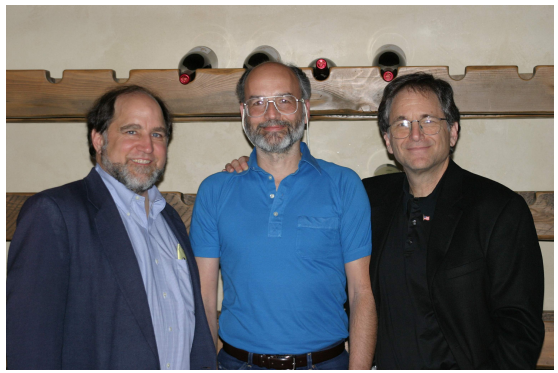
- **¿Qué tiene que ver esto con el análisis matemático?**
- **¿Qué tiene que ver esto con el siglo XXI?**
- **¿Y todo esto para qué puede servir?**

Daré primero la respuesta usual a la tercera pregunta.

El sistema criptográfico con clave pública RSA

Ron Rivest, Adi Shamir y Len Adleman, MIT, 1977.

Algoritmo (=procedimiento) asimétrico cifrador de bloques, que utiliza una clave pública, que se distribuye, y otra privada, que se guarda en secreto por su propietario.



Clave pública quiere decir que cualquiera conoce cómo se ha codificado el mensaje, pero desconoce algún dato de la clave de codificación.

Asimétrico significa que no se usa la misma función para cifrar y descifrar. La seguridad del código radica en que las claves que se publican sirven para enviar mensajes pero no para descifrarlos.

Su funcionamiento se basa en el producto de dos números primos grandes, de más de 100 cifras, y emplea aritmética modular.

El sistema criptográfico con clave pública RSA

El siguiente resultado está en la base del sistema criptográfico RSA.

$\Phi(n)$ es el número de enteros positivos m menores o iguales a n tales que m y n son primos entre sí.

Teorema de Euler (1707-1783)

Si m y n son primos entre sí, entonces $m^{\phi(n)} \mod n = 1$, o sea n divide a $m^{\phi(n)} - 1$.

Euler fue el primero en utilizar herramientas del análisis matemático en el estudio de los números primos.

El sistema criptográfico con clave pública RSA

Los dos problemas prácticos más importantes sobre los primos son:

- Encontrar un método eficaz para determinar si un número grande es primo. Un algoritmo determinista fue presentado por Agrawal, Kayal y Saxena en 2002, pero aún no es eficiente en la práctica.
- Hallar un procedimiento eficiente para descomponer un número dado en factores primos.

El propósito del resto de la charla **NO** es hablar de estos problemas, sino de la **distribución de los números primos.**

A modo de explicación

Tim Gowers, Medalla Fields 1998 en el ICM de Berlín, en su artículo "*La importancia de las Matemáticas*", impartido en el Instituto Clay, en la presentación de los siete problemas del milenio en 2000, decía:

"La mayor parte de los matemáticos, incluyéndome a mí, nos encontramos en mitad del espectro, cuando se trata de actitudes acerca de las aplicaciones. Estaríamos encantados de probar un teorema que resultara útil fuera de las matemáticas, pero no lo buscamos activamente. Ante la elección entre un problema interesante, pero puramente matemático y un problema poco interesante con posible beneficio para ingenieros, físicos o informáticos, optaríamos por el primero; aunque nos sentiríamos mal si nadie trabajara en problemas prácticos."

El teorema de los números primos

Propósito

Estimar la función $\pi(n)$ definida para un natural n como el número de primos menores o iguales a n.

- Los primos se comportan con gran irregularidad. Hay 9 primos entre los 100 números anteriores a 10000000 y sólo 2 entre los 100 posteriores.
- Los números primos grandes aparecen menos a menudo que los pequeños, porque tienen más posibilidades de descomponerse en factores primos.
- Podría pensarse que 10001 es primo porque no se puede dividir por $2, 3, 5, 7, 11, 13, 17$ o 19, pero $10001 = 73 \times 137$.
- Hay huecos entre los números primos tan grandes como queramos.

El teorema de los números primos

Observación

Hay huecos entre los números primos tan grandes como queramos.

En un artículo publicado por la American Mathematical Society en 1999, acerca de como dar un buen Coloquio, John E. McCarthy recomienda **"Prueba solo tautologías"**. Aquí tenemos una:

Dado el número natural n, los números

$$n! + 2, n! + 3, ..., n! + n$$

no son primos.

El teorema de los números primos

Legendre (1752-1833) y **Gauss** (1777-1855) realizaron cálculos aproximados de $\pi(n)$

(antes de los ordenadores!!).

Conjeturaron, respectivamente, que $\pi(n)$ se comportaba como

$$L(n) := \frac{n}{\log n - 1} \qquad \text{ó} \qquad \mathrm{li}(n) := \int_2^n \frac{1}{\log t}\, dt.$$

$n = 50000$	$\pi(n) = 5133$	$L(n) = 5092$	$\mathrm{li}(n) = 5166$
$n = 500000$	$\pi(n) = 41538$	$L(n) = 41246$	$\mathrm{li}(n) = 41607$
$n = 10000000$	$\pi(n) = 664579$	$L(n) = 661459$	$\mathrm{li}(n) = 664918$

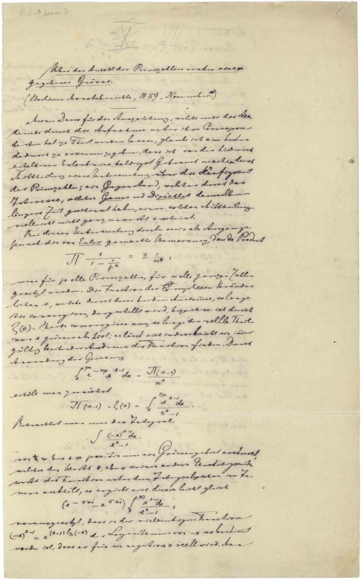
El teorema de los números primos

(Hadamard (1865-1963), de la Vallée Poussin (1867-1962), 1896 independientemente)

$$\lim_{n\to\infty} \frac{\pi(n)\log n}{n} = \lim_{n\to\infty} \frac{\pi(n)}{\mathrm{li}(n)} = 1$$

En otras palabras,

La probabilidad de que un número elegido al azar entre 1 y n sea primo es aproximadamente $1/\log n$.



Paso fundamental: Riemann (1826-1866) en su memoria de 1859 “Sobre el número de primos menores que una cantidad dada”, en la que apareció formulada por primera vez la **Hipótesis de Riemann**, considerado como el problema abierto más importante de las Matemáticas.

El teorema de los números primos

Punto de partida: La función definida para un número complejo s

$$\zeta(s) := 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Euler:

- En 1737, la consideró para s real.
- La serie diverge para $s = 1$ y calcula $\zeta(2) = \pi^2/6$.
- Mostró la relación de los números primos con la función

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1},$$

el producto extendido a los números primos p. De alguna forma esta es una expresión analítica del teorema fundamental de la aritmética.

El teorema de los números primos

Riemann mostró:

- La serie converge si la parte real de s es mayor que 1.
- $\zeta(s)$ tiene una extensión analítica a todo el plano complejo menos $s = 1$, donde tiene un polo simple.
- Obtuvo una ecuación funcional sorprendente (Γ es la función gamma de Euler).

$$\zeta(s) = 2^s \pi^{s-1} \mathrm{sen}(\pi s/2) \Gamma(1-s) \zeta(1-s), \quad s \in \mathbb{C}.$$

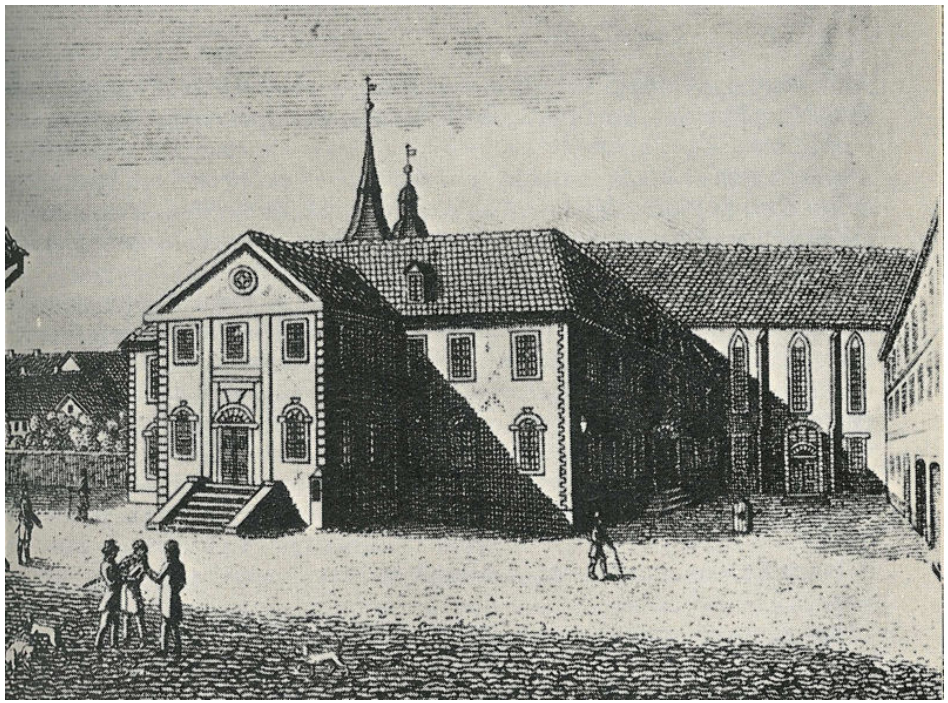
- Probó que no hay ceros de $\zeta(s)$ fuera de la banda $0 \leq \Re(s) \leq 1$, salvo los ceros triviales $s = -2, -4, -6, \ldots$

Una demostración del teorema de los primos sin análisis complejo fue obtenida independientemente por **A. Selberg** y **P. Erdös** en 1949.

A. Selberg

P. Erdös

El centro mundial de las Matemáticas entre 1800 y 1933 fue **Göttingen (Alemania)**.



Allí estuvieron Gauss, Dirichlet, Riemann, Hilbert y Klein.

Después de 1945, el centro mundial de la investigación matemática es el Instituto de Estudios Avanzados de **Princeton (USA)**, donde estuvieron Einstein, Gödel, Selberg y von Neumann, entre muchos otros.

ADVERTENCIA

Las siguientes TRES páginas explican los pasos principales de una demostración con análisis complejo del teorema de los números primos y tienen "mayor contenido matemático".

El trabajo de Chebyshev (1850)

- La función "theta": $\theta(x) := \sum_{p \leq x} \log p$, la suma extendida a todos los primos menores o iguales que $x \geq 1$.
- La función "psi": $\psi(x) = \sum_{n \leq x} \Lambda(n)$, donde $\Lambda(n) = \log p$ si $n = p^m$ para cierto primo p y natural m, $\Lambda(n) = 0$ en otro caso.
- Obtuvo cotas superiores e inferiores para estas funciones. Por ejemplo $\psi(x) \leq 2x$ si $x > 1$.
- Probó el postulado de Bertrand: Para todo natural $n > 1$ existe un primo p tal que $n < p < 2n$.
- Demostró que

$$\lim_{x \to \infty} \frac{\pi(x) \log x}{x} = 1 \Leftrightarrow \lim_{x \to \infty} \frac{\psi(x)}{x} = 1 \Leftrightarrow \lim_{x \to \infty} \frac{\theta(x)}{x} = 1.$$

Pasos principales de una demostración del teorema de los números primos

- Se trata de deducir propiedades de $\psi(x)$ a partir de propiedades de $\zeta'(s)/\zeta(s) = -\sum_{n=1}^{\infty} \Lambda(n) n^{-s}$.
- $\zeta(s)$ puede extenderse a una función holomorfa para $\mathrm{Re} s > 0, s \neq 1$, tal que, cera de $s = 1$,

$$\zeta'(s)/\zeta(s) = -\frac{1}{s-1} + \gamma + a_1(s-1) + ...$$

Hecho crucial

$\zeta(s) \neq 0$ si $\mathrm{Re} s = 1$.

- Luego $\zeta'(s)/\zeta(s)$ existe en y cerca de $\mathrm{Re} s = 1$.

La demostración de Newman 1980 y Korevar 1982

- $f(s) := -\zeta'(s)/\zeta(s)$ es holomorfa en una región que contiene a $\mathrm{Re} s \geq 1$,
- $f(s) = \frac{1}{s-1} - \gamma + (s-1)h(s)$, $h(s)$ holomorfa cerca de $s = 1$,
- $f(s) = \sum_{n=1}^{\infty} \Lambda(n) n^{-s}$ si $\mathrm{Re} s > 1$ y
- $\psi(x) := \sum_{n \leq x} \Lambda(n) \leq 2x$ si $x \geq 1$.

La conclusión se sigue aplicando un teorema Tauberiano.

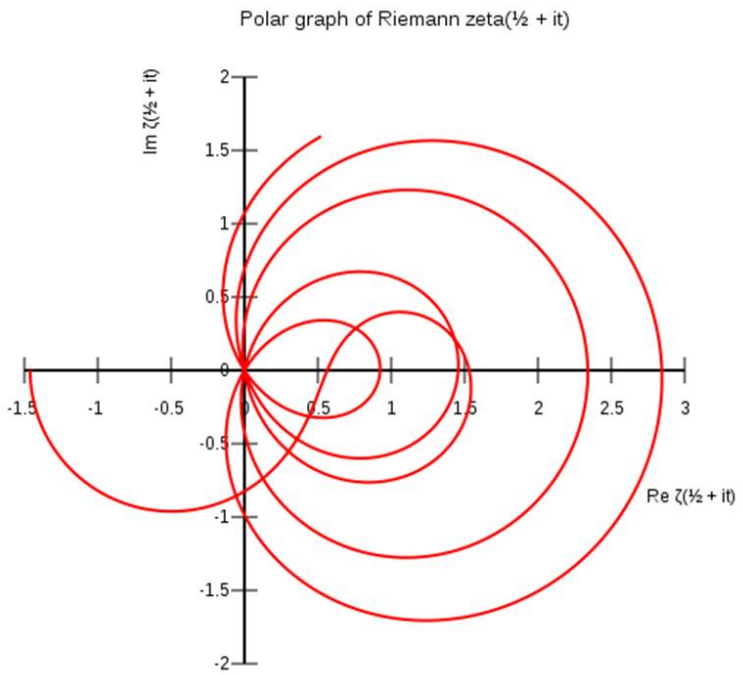
Theorem. Ingham-Newman.

Si una función compleja $f(s)$ satisface las hipótesis mencionadas arriba, entonces

$$\lim_{x \to \infty} \frac{\psi(x)}{x} = 1.$$

La Hipótesis de Riemann

Riemann conjeturó que todos los ceros no triviales de la función $\zeta(s)$ se encuentran en la recta $\Re(s) = 1/2$.



La Hipótesis de Riemann es equivalente a que la diferencia $|\pi(n) - \mathrm{li}(n)|$ es menor o igual que una constante por $\sqrt{n}\log n$.

La Hipótesis de Riemann

- Para valores de n pequeños se había demostrado que $\pi(n) < \mathrm{li}(n)$, de hecho se cumple para $n < 10^{23}$. Ello que llevó a conjeturar a varios matemáticos en la época de Gauss que esto sucedería para todo valor de n, o equivalentemente, que la ecuación

$$\pi(n) - \mathrm{li}(n) = 0$$

  no tenía soluciones reales.

- En 1914 **J. E. Littlewood** demostró que $\pi(n) > \mathrm{li}(n)$ para infinitos valores de n. El primero de ellos se conoce como **primer número de Skewes**, y actualmente se sabe que es inferior a 10^{317}.

Hardy and Littlewood

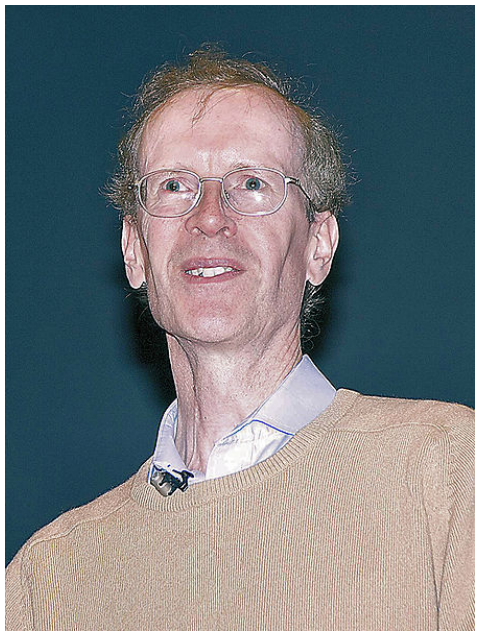
Hardy

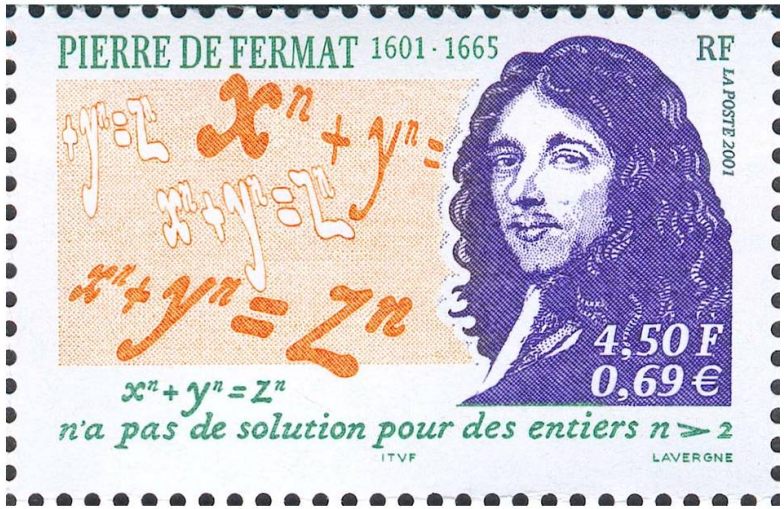
Littlewood

La Hipótesis de Riemann

- Es uno de los problemas del milenio del **Instituto Clay**. Su solución está valorada en un millón de dólares.
- Ya fue incluida por **Hilbert** en su famosa lista de 23 problemas planteados en el ICM de París en 1900,
- **Hardy** y **Littlewood** trabajaron en ella intensamente en la primera parte del siglo XX.
- **Andrew Wiles, 2000:** "Los números primos aparecen como si ocurrieran al azar, pero no sabemos si es exactamente así. La Hipótesis de Riemann da una manera precisa de expresar que esto ocurre. Además, casi cualquier problema que trata de los números primos sería influenciado por la Hipótesis de Riemann."

Andrew Wiles demostró el gran teorema de Fermat en 1993-95.





La Hipótesis de Riemann

Evidencias en favor de la Hipótesis de Riemann:

- **Van de Lune** en 2000 mostró que los primeros 10.000 millones de ceros no triviales están en la línea crítica.
- Mejorado en 2004 por **Gourdon** y **Demichel** pasando a 10 billones.
- El 99 % de los ceros no triviales están cerca de la línea.
- **Selberg** en 1942 demostró que una proporción estrictamente positiva de los ceros están en la línea crítica. **N. Levinsón** en 1974 probó que están, al menos, la tercera parte.
- La simetría de los primos. La Hipótesis de Riemann nos dice que los primos se distribuyen de la manera más regular posible.

?Y EL SIGLO XXI?

Progresiones aritméticas en los primos

- 2
- 2,3
- 3,5,7
- 5,11,17,23
- 11,41,71,101,131
- 7,37,67,97,127,157
- 7,157,307,457,607,757
- $11410337850553 + 4609098694200 \times d;\ d = 0, ..., 21$
  (**Moran, Pritchard, Thyssen, 1995**)
- $56211383760397 + 44546738095860 \times d;\ d = 0, ..., 22$
  (**Frind, Underwood, Jobling, 2004**)

Progresiones aritméticas en los primos

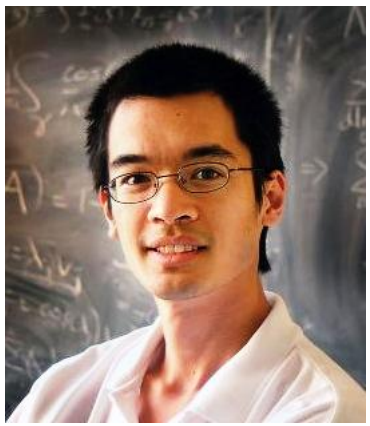
Teorema de Green y Tao, 2004

Los números primos contienen progresiones aritméticas arbitrariamente largas.

Es obvio que no puede haber progresiones aritméticas infinitas de números primos.

Green

Madrid 2006



Tao

Tao fue medalla Fields en el Congreso Internacional de Matemáticos ICM celebrado en Madrid en 2006.

Otros problemas acerca de los números primos

Conjetura de Goldbach impar

Todo número impar mayor que 7 es la suma de tres primos impares.
Ejemplos:

$$9 = 3 + 3 + 3, \quad 11 = 3 + 3 + 5, \ldots$$

Conjetura de Goldbach par. Euler, 1742

Todo número par mayor que 4 es la suma de dos primos impares.
Ejemplos:

$$14 = 7 + 7, \quad 16 = 3 + 13, \quad 18 = 7 + 11 \ldots$$

Conjetura de los primos gemelos

Existen infinitos pares de números primos de la forma $p, p + 2$.
Ejemplos:

$$5, 7 \quad \text{o} \quad 17, 19 \quad \text{o} \quad 59, 61 \quad \text{o} \quad 137, 139.$$

Dos resultados importantes

Teorema de Dirichlet de progresiones aritméticas

Toda progresión aritmética

$$a, a+q,\ a+2q,\ a+3q,\ \ldots,$$

con enteros a y q primos entre sí, contiene infinitos números primos.

Teorema de Chen, 1966

Existen infinitos números primos p tales que $p+2$ es el producto de dos números primos.

Algunos resultados recientes

Harald Helfgott, 2013.

Todo número impar $N > 7$ es la suma de tres primos impares.

- Esto mejora un resultado de Tao de 2012, que demostraba que era N era la suma de 5 números primos.
- En 1937 Vinogradov había demostrado que el resultado se cumplía para N suficientemente grande.

Algunos resultados recientes

Denotamos por p_n el primo n-ésimo.

Zhang. 2013.

Existe una constante $C \leq 70,000,000$ tal que $p_{n+1} - p_n < C$ para infinitos valores de n.

- Goldston, Yildirim, Pintz probaron en 2005 que la diferencia $p_{n+1} - p_n$ entre dos primos consecutivos es menor que $(\log p_n)^{8/9}$ para infinitos valores de n.
- Tao y otros están trabajando en un proyecto "Polymath" (ver blog de Tao) para mejorar la constante C.
- La conjetura de los primos gemelos asegura que $p_{n+1} - p_n = 2$ infinitas veces.

Colaboración en Matemáticas

- ¿Qué es Polymath Project?
- Colaboración online entre matemáticos para resolver problemas importantes y difíciles, coordinandose para comunicar sus ideas y encontrar las mejores vías a su solución. El proyecto comenzó en 2009 en el blog de Tim Gowers.

- Blog de Tao: http://terrytao.wordpress.com/
- Blog de Gowers: http://gowers.wordpress.com/

¿Hay que ser un genio para hacer Matemáticas?

Atribuido a Einstein:

La diferencia entre la genialidad y la estupidez es que un genio conoce sus limitaciones.

P.G. Casazza:

"Hay un número muy pequeño de grandes matemáticos. Afortunadamente, un ejército no puede estar formado solo por generales. Hace falta un gran espectro de matemáticos con toda clase de talentos diferentes para impulsar nuestra ciencia. Además, la más crítica necesidad en matemáticas son las nuevas idea creativas, y estas pueden proceder de cualquiera."

¿Hay que ser un genio para hacer Matemáticas?

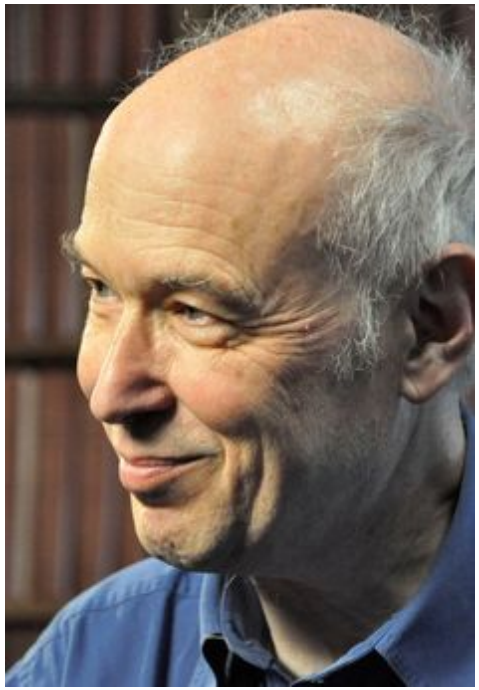
Tao:

"La imagen popular de un genio solitario, que ignora la literatura y el conocimiento actual, y consigue mediante una inspiración inexplicable, obtener una solución original a un problema que ha confundido a todos los expertos, es atractiva y romántica, pero totalmente falsa. Yo encuentro la realidad matemática actual, en la que el progreso se obtiene natural y acumulativamente como consecuencia de trabajo duro, dirigido por la intuición, literatura y algo de suerte, mucho más satisfactoria."

¿Hay que ser un genio para hacer Matemáticas?

Deligne, Premio Abel 2013:

"Grothendieck una vez me dijo que las Matemáticas no eran para él un deporte competitivo. Son diferentes, aunque algunos quieren ser los primeros, especialmente si trabajan en problemas específicos y difícles. Para mí es más importante crear herramientas para entendeer el cuadro general. Pienso que las Matemáticas son una empresa colectiva de larga duración. "



¿Hay que ser un genio para hacer Matemáticas?

Tao:

"Si usted tiene una buena formación, interés y una talento razonable, seguro que hay una parte de las Matemáticas donde pueda hacer una contribución sólida y útil."

"Es también importante recordar que la Matemática profesional no es un deporte, al contrario que las competiciones matemáticas. El objetivo de los matemáticos no es obtener la mejor posición o más premios, sino aumentar nuestra comprensión de las Matemáticas, tanto para uno mismo, como para sus colegas y estudiantes, y contribuir a su desarrollo y sus aplicaciones. Para esas tareas las Matemáticas necesitan tanta gente inteligente como sea posible atraer."

T. Gowers, 2000:

"Podemos estar agradecidos de que sea posible usar modelos matemáticos simples para describir, o incluso explicar, fenómenos complejos de la física y de otras ciencias. Gracias a este afortunado hecho, podemos confiar que los matemáticos, si se les da la libertad de seguir trabajando en el objeto de estudio que les da tanto placer, continuarán produciendo un cuerpo de doctrina que será importante en cualquier sentido del término, tanto en la utilidad práctica de las matemáticas, como en su valor cultural."

Créditos

- **J. Cilleruelo, A. Córdoba**, Los Números, CSIC, 2010.
- **A. Doxiadis**, El tío Petros y la conjetura de Goldbach, *Zeta* 1992.
- **T. Gowers**, Mathematics. A very short introduction, *Oxford University Press* 2002.
- **G.J.O. Jameson**, The Prime Number Theorem, London Math. Soc., 2003.
- **G. Navarro**, Un curso de números, *Publicacions Universitat de València* 2007.
- **M. du Sautoy**, La Música de los Números Primos, *Acantilado* 2007.
- **S. Singh**, El enigma de Fermat, *Planeta* 1997.