Aspectos del análisis matemático para el siglo XXI

José Bonet

Instituto Universitario de Matemática Pura y Aplicada

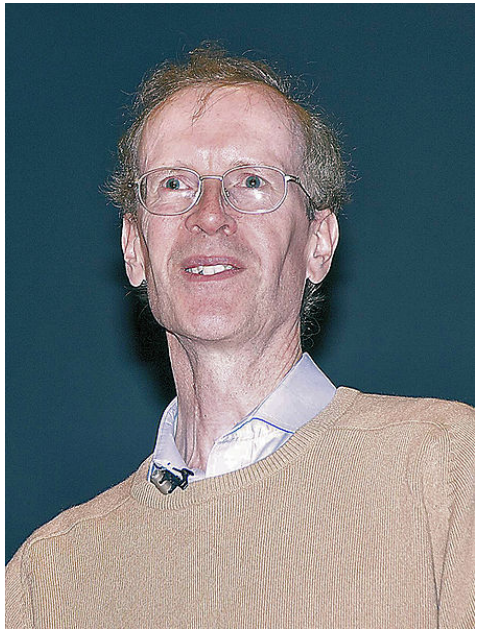
Universidad Politécnica de Valencia

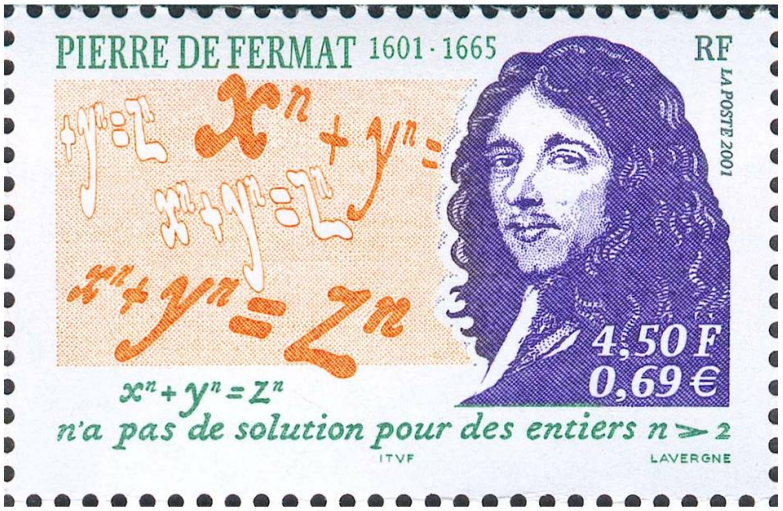
El Legado de Prometeo. Científicos Valencianos de Excelencia.
28 de mayo de 2009

- Buenas y malas noticias.

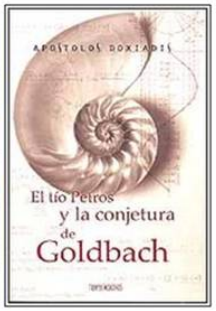
- ¿Cuántos teoremas de matemáticas demostrados en los últimos 50 años conocen?

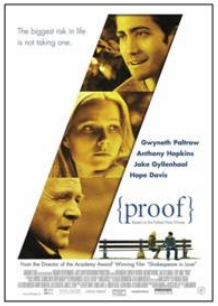
  ¿Y si les pido que me digan uno distinto del gran teorema de Fermat demostrado por Andrew Wiles en 1993-95?

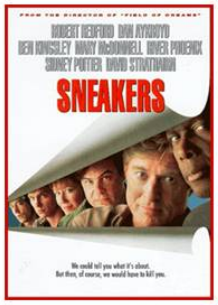


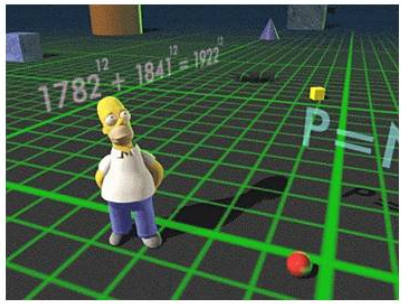


- **Libros:** Simon Singh (El enigma de Fermat), Apostolos Doxiadis (El tío Petros y...), M. Haddon (El curioso incidente del perro...), A.C. Clarke y F. Pohl (The Last Theorem, ciencia ficción)
- **Teatro:** Proof (La prueba, David Auburn), The five hysterical girls theorem (Less Gutman).
- **Musical:** 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









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

(atribuido a un Premio Nobel de Física).

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,...
- 1, 2, 3, 5, 7, 11, 15, 22, 30,...

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,

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

donde $p_1, \dots p_k$ 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.

El algoritmo de Euclides

Es un algoritmo para calcular el máximo común divisor de dos números enteros a, b, $\mathrm{mcd}(a, b)$.

Ejemplo: Nos piden $\mathrm{mcd}(741, 663)$. Se usa reiteradamente el algoritmo de la división.

$$\begin{aligned} 741 &= 663 \times 1 + 78 \\ 663 &= 78 \times 8 + 39 \\ 78 &= 39 \times 2. \end{aligned}$$

Entonces $\mathrm{mcd}(741, 663) = 39$.

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 sirve?**

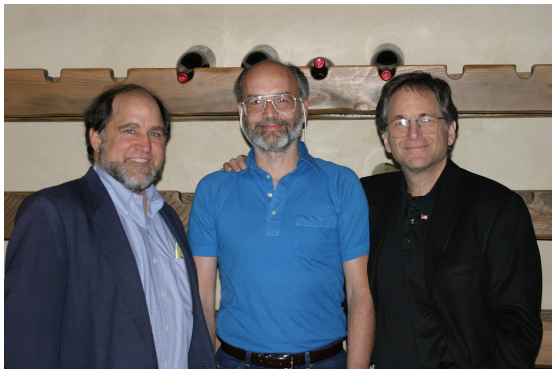
El sistema criptográfico con clave pública RSA

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.



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

Aritmética modular.

Fijamos un número n. Escribimos

$$a \bmod n = s$$

para indicar que el resto de a al dividirlo por n da s.

Ejemplos:
$14 \bmod 12 = 2$ (como todo el mundo sabe del reloj!),
$15 \bmod 7 = 1$.

Como $3 \times 5 \bmod 7 = 1$, decimos que 3 y 5 son inversos módulo 7.

El inverso de 2 módulo 7 es 4.

El sistema criptográfico con clave pública RSA

Dado n, $\phi(n)$ indica el número de enteros s tales que $\mathrm{mcd}(s, n) = 1$, o también cuántos números menores que n tienen inverso módulo n.

Ejemplos:

$$\phi(1) = 1, \quad \phi(2) = 1, \quad \phi(3) = 2,$$
$$\phi(6) = 2, \quad \phi(10) = 4, \quad \phi(15) = 8 \ (1, 2, 4, 7, 8, 11, 13, 14).$$

En general,

- $\phi(p) = p - 1$ si p es primo
- $\phi(pq) = (p - 1)(q - 1)$ si p y q son primos distintos.

El sistema criptográfico con clave pública RSA

Algoritmo RSA.

1. Elegimos al azar dos primos grandes p y q, que NO se hacen públicos.
Ejemplo: $p = 3$, $q = 11$.

2. Hacemos $n = p \times q$
Ejemplo: $n = 3 \times 11 = 33$.

3. Calculamos $\phi(n) = (p-1)(q-1)$.
Ejemplo: $\phi(33) = 2 \times 10 = 20$.

4. Elegimos e tal que $\mathrm{mcd}(e, \phi(n)) = 1$. Buscamos un número impar que al dividir $\phi(n)$ por él no dé 0.
Ejemplo: $e = 3$.

El sistema criptográfico con clave pública RSA

5. Calculamos d el inverso de e módulo $\phi(n)$. O sea,

$$ed \bmod \phi(n) = 1.$$

Ejemplo: $d = 7$, ya que $d \times e = 21$ y $21 \bmod 20 = 1$.

6. Clave pública: (e, n). Clave privada: (d, n).
Ejemplo. $(3, 33)$ (pública) y $(7, 33)$ (privada).

7. Queremos transmitir el número M. Cifrado: $C := M^e \bmod n$.
Ejemplo: $M = 5$. Calculamos $C = 5^3 \bmod 33 = 125 \bmod 33 = 26$.

8. Descifrado: $M = C^d \bmod n$.
Ejemplo: $26^7 \bmod 33 = 8031810176 \bmod 33 = 5$!!!!

El sistema criptográfico con clave pública RSA

Otro ejemplo:

$p = 61,\ q = 53$

$n = pq = 3233,\ \phi(n) = 3120$

$e = 17,\ d = 2753$

$M = 123,\ C = 123^{17} \bmod 3233 = 855$

$855^{2753} \bmod 3233 = 123.$

¿Por qué funciona?

El sistema criptográfico con clave pública RSA

Teorema pequeño de Fermat (siglo XVII)

Si p es primo, entonces $m^{p-1} \bmod p = 1$ para cada número natural m.

Este resultado permite probar que el descifrado de C realmente produce el mensaje M.

Consecuencia. Si p es primo, entonces p divide a $2^p - 2$.

Ejemplo: $2^{341} - 2$ es divisible por 341, aunque $341 = 31 \times 11$.

La "hipótesis china" es falsa.

El sistema criptográfico con clave pública RSA

Teorema de Euler (1707-1783)

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

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

Fortaleza del algoritmo RSA

El problema de calcular la clave privada d a partir de la clave pública (n, e) es equivalente al problema de factorizar $n = p \times q$

Los primos p y q deben ser grandes y no deben ser próximos entre sí. Además $p - 1$ y $q - 1$ deben tener factores primos grandes. Finalmente, la clave secreta d debe ser también grande.

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

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

- $\mathrm{e}^{\pi i} = -1$, $\sqrt{xy} \leq (x+y)/2$.
- $\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + ... = 1$.
- $\lim_{n\to\infty} (1 + \frac{1}{n})^n = e$.
- $f(x) = \log x$, $f(x) = e^x$, $f(x) = \mathrm{sen} x$, $\log x = \int_1^x \frac{1}{t} dt$,...
- Aplicaciones: Ecuaciones en derivadas parciales (ondas, calor, fluidos, turbulencia, crecimiento de poblaciones,...) y tratamiento de imágenes (ondículas, análisis tiempo frecuencia,...)

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

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

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

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

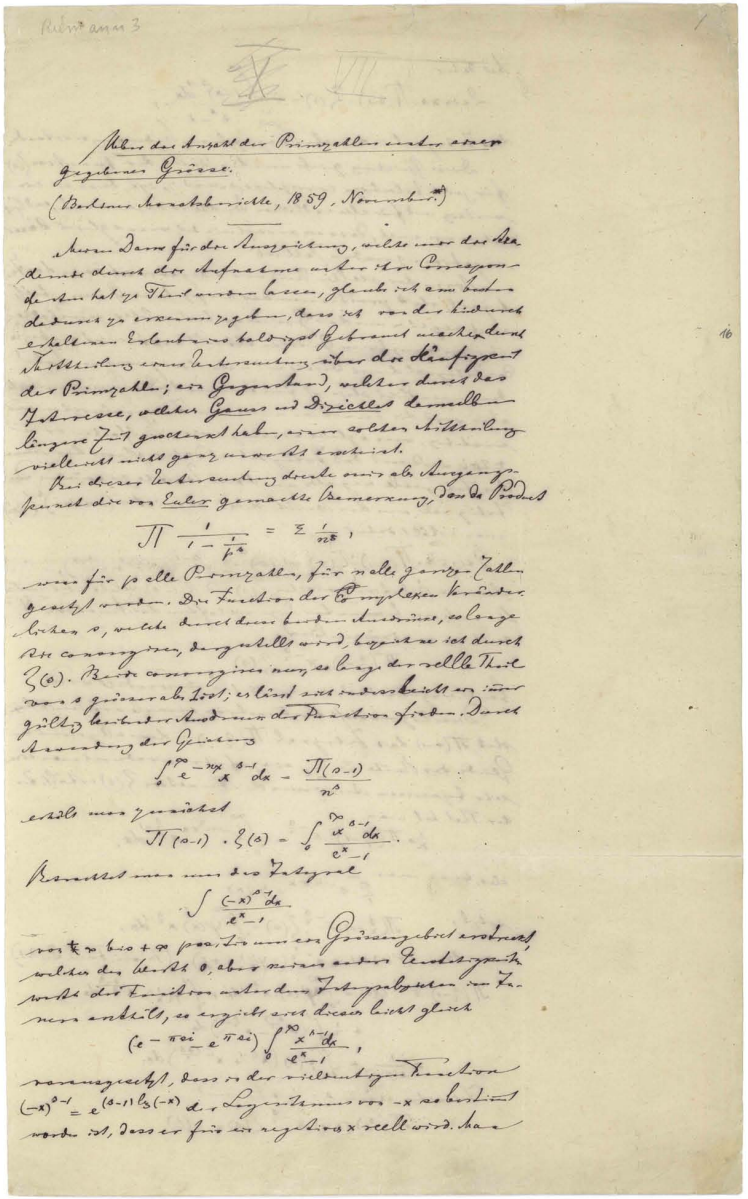
El teorema de los números primos

(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 $\zeta(2) = \pi^2/6$.
- La serie de los inversos de los primos diverge.
- 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.

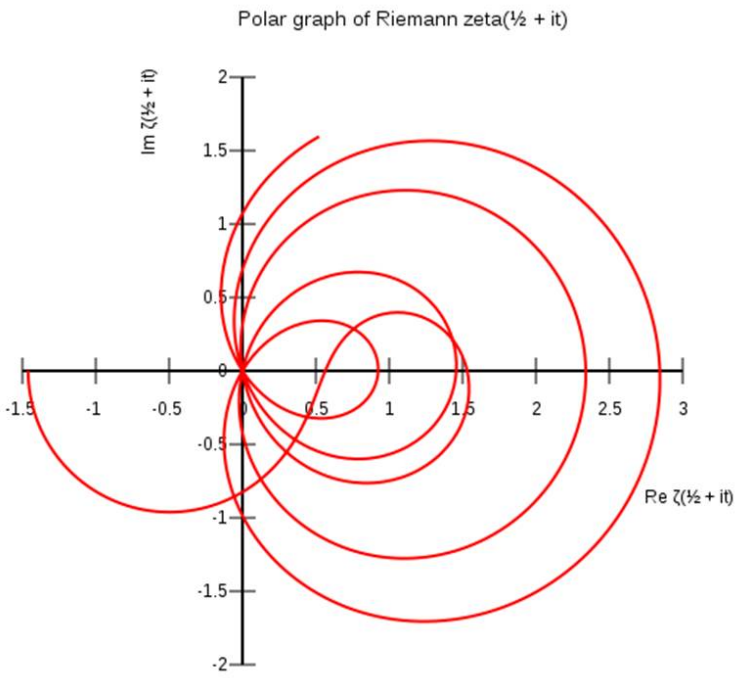
El teorema de los números primos

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.
- Probó que no hay ceros de $\zeta(s)$ fuera de la banda $0 \leq \Re(s) \leq 1$, salvo los ceros triviales $s = -2, -4, -6, \ldots$
- Dio una fórmula explícita de $\pi(x)$ en términos de los ceros complejos de $\zeta(s)$
- Y ...

La Hipótesis de Riemann

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



Hadamard y **de la Vallée Poussin** probaron que no hay ceros en la recta $\Re(s) = 1$, de lo que se deducía el teorema de los números primos $\pi(n) \sim n/\log n \sim \mathrm{li}(n)$.

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

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

La Hipótesis de Riemann

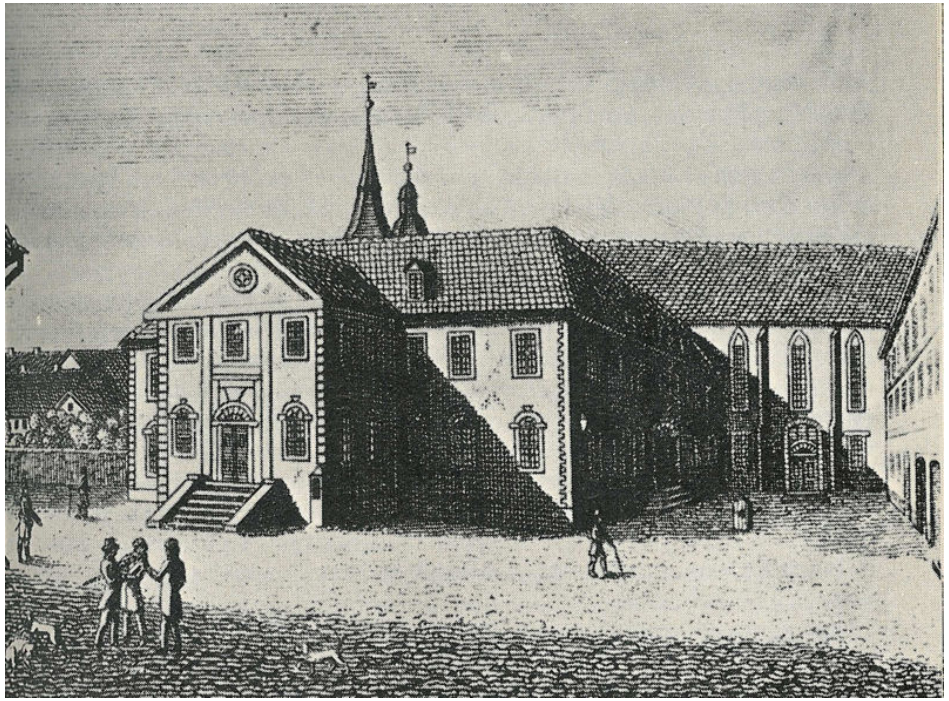
- Es uno de los problemas del milenio del **Instituto Clay**. Su solución está valorada en un millón de dólares.
- Ya fue incluida por **Hilbert** en su famosa lista de 23 problemas planteados en el ICM de París en 1900,
- **Hardy** y **Littlewood** trabajaron en ella intensamente en la primera parte 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."

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.

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.

¿Se acuerdan de la sucesión 1, 2, 3, 5, 7, 11, 15, 22, 30,...?

El número siguiente de la sucesión es 42.

Para su información son los números de partición P_n y corresponden al número de maneras diferentes de dividir n piedras en pilas separadas.

Por ejemplo

$$\left.\begin{array}{rcl} 3 & = & 3 \\ 3 & = & 1+2 \\ 3 & = & 1+1+1 \end{array}\right\} (3 \text{ maneras}) \qquad \left.\begin{array}{rcl} 4 & = & 4 \\ 4 & = & 1+3 \\ 4 & = & 1+1+2 \\ 4 & = & 2+2 \\ 4 & = & 1+1+1+1 \end{array}\right\} (5 maneras)$$

- La densidad de los niveles de energía en ciertos sistemas cuánticos simples se reduce a la comprensión del crecimiento de los números de partición.

- Una fórmula exacta para para determinar P_n fue calculada por **Rademacher** en 1937, mejorando resultados debidos a **Hardy** y **Ramanujan**.

Hardy

Ramanujan

Algunos problemas abiertos

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:

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

Conjetura de Legendre

Hay un número primo entre n^2 y $(n+1)^2$ para todo número natural n.
Ejemplos:
Para $n = 1$, entre 1^2 y 2^2, está 2 y 3.
Para $n = 2$, entre $2^2 = 4$ y $3^2 = 9$, está 5 y 7.
Para $n = 3$, entre $3^2 = 9$ y $4^2 = 16$, está 11 y 13.

Conjetura $n^2 + 1$

Hay infinitos números primos de la forma $n^2 + 1$.
Ejemplos:

$$2 = 1^2 + 1, \quad 5 = 2^2 + 1, \quad 17 = 4^2 + 1, \quad 37 = 6^2 + 1, \ldots$$

Todos estos problemas fueron ya recogidos por **Landau** en 1912.

Una "consecuencia" del teorema de los números primos

"Demostración" del teorema de los primos gemelos usando el teorema de los números primos.

(1) Elegimos un número n al azar entre 1 y N.

(2) La probabilidad de que n sea primo es $1/\log N$.

(3) La probabilidad de que $n+2$ sea primo es $1/\log N$.

(4) Suponiendo que los sucesos (2) y (3) son más o menos independientes, la probabilidad de que n y $n+2$ sean los dos primos es $1/(\log N)^2$.

Una "consecuencia" del teorema de los números primos

(5) Luego el número de primos gemelos entre 1 y N debería ser alrededor de $N/(\log N)^2$.

(6) Como $N/(\log N)^2$ tiende a infinito cuando $N \to \infty$, debe haber infinitos primos gemelos.

Una "consecuencia" del teorema de los números primos

(5) Luego el número de primos gemelos entre 1 y N debería ser alrededor de $N/(\log N)^2$.

(6) Como $N/(\log N)^2$ tiende a infinito cuando $N \to \infty$, debe haber infinitos primos gemelos.

Genial!

Hemos probado la conjetura de los primos gemelos, abierta desde Euclides!!

Una "consecuencia" del teorema de los números primos

(5) Luego el número de primos gemelos entre 1 y N debería ser alrededor de $N/(\log N)^2$.

(6) Como $N/(\log N)^2$ tiende a infinito cuando $N \to \infty$, debe haber infinitos primos gemelos.

Genial!

Hemos probado la conjetura de los primos gemelos, abierta desde Euclides!!

¡ La prueba no es correcta !

- Desgraciadamente la prueba no es correcta.
- Repitiéndola verificaríamos que hay infinitos primos adyacentes n y $n+1$; lo que es claramente falso. **¡Lástima!**
- El problema es el supuesto de independencia de los dos sucesos del punto (4).
- Curiosamente, este tipo de razonamientos probabilísticos (corregidos por supuesto!) han tenido una gran importancia en la investigación reciente en teoría de números.

Algunos resultados sorprendentes

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.

Vinogradov, 1937

Todo número impar n lo bastante grande se puede escribir como la suma de tres números primos.

- Liu-Wang probaron en 2002 que es cierto si $n > 10^{1346}$.
- También es conocido para $n < 10^{20}$.

Algunos resultados sorprendentes

Teorema de Chen, 1966

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

Goldston, Yildirim, Pintz, 2005

La diferencia $p_{n+1} - p_n$ entre dos primos consecutivos es menor que $(\log p_n)^{8/9}$ para infinitos valores de n.

- La conjetura de los primos gemelos asegura que $p_{n+1} - p_n = 2$ infinitas veces.

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

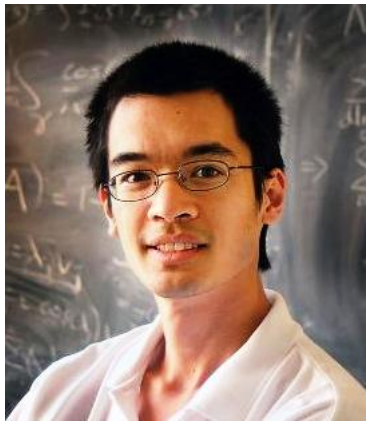
Teorema de Green y Tao, 2004

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.

Progresiones aritméticas en los primos

La demostración de Green y Tao es muy profunda. Combina técnicas de teoría analítica de números, análisis armónico y teoría ergódica.

Teorema de Szemerédi, 1975.

Todo subconjunto A de los números enteros que tenga densidad superior positiva contiene progresiones aritméticas arbitrariamente largas.

El resultado no se puede aplicar directamente porque los primos no tienen densidad superior positiva.

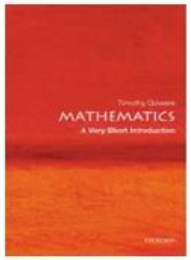
Problema abierto de Erdös.

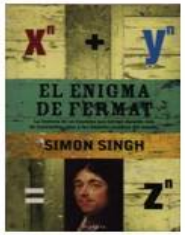
¿Contiene todo subconjunto X de naturales tal que $\sum_{n\in X} \frac{1}{n} = \infty$ progresiones artiméticas arbitrariamente largas?

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."

Lecturas recomendadas





- **Apostolos Doxiadis**, El tío Petros y la conjetura de Goldbach, *Zeta* 1992.
- **Marcus du Sautoy**, La Música de los Números Primos, *Acantilado* 2007.
- **Timothy Gowers**, Mathematics. A very short introduction, *Oxford University Press* 2002.
- **Gabriel Navarro**, Un curso de números, *Publicacions Universitat de València* 2007.
- **Simon Singh**, El enigma de Fermat, *Planeta* 1997.