Me encantan los números

Fernando Chamizo Lorente

Universidad Autónoma de Madrid

http://www.uam.es/fernando.chamizo

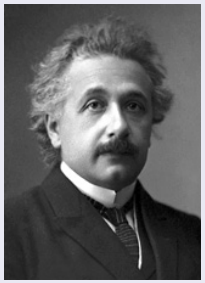
X Encuentro Nacional de Estudiantes de Matemáticas

Madrid, 23 de julio 2009


BLA
Bla
Bla

Lo que dijeron los sabios...

Einstein (1879–1955) Premio Nobel de Física en 1921



"¿Cómo puede ser que las matemáticas, siendo después de todo un producto del pensamiento humano independiente de la experiencia, se adapte tan admirablemente a los objetos de la realidad?"

E.P. Wigner (1902–1995) Premio Nobel de Física en 1963

"La enorme utilidad de las matemáticas en las ciencias naturales es algo que roza el misterio y que no tiene explicación racional".

"El milagro de lo apropiado que es el lenguaje de las matemáticas para la formulación de las leyes de la física es un regalo maravilloso que ni entendemos ni merecemos".

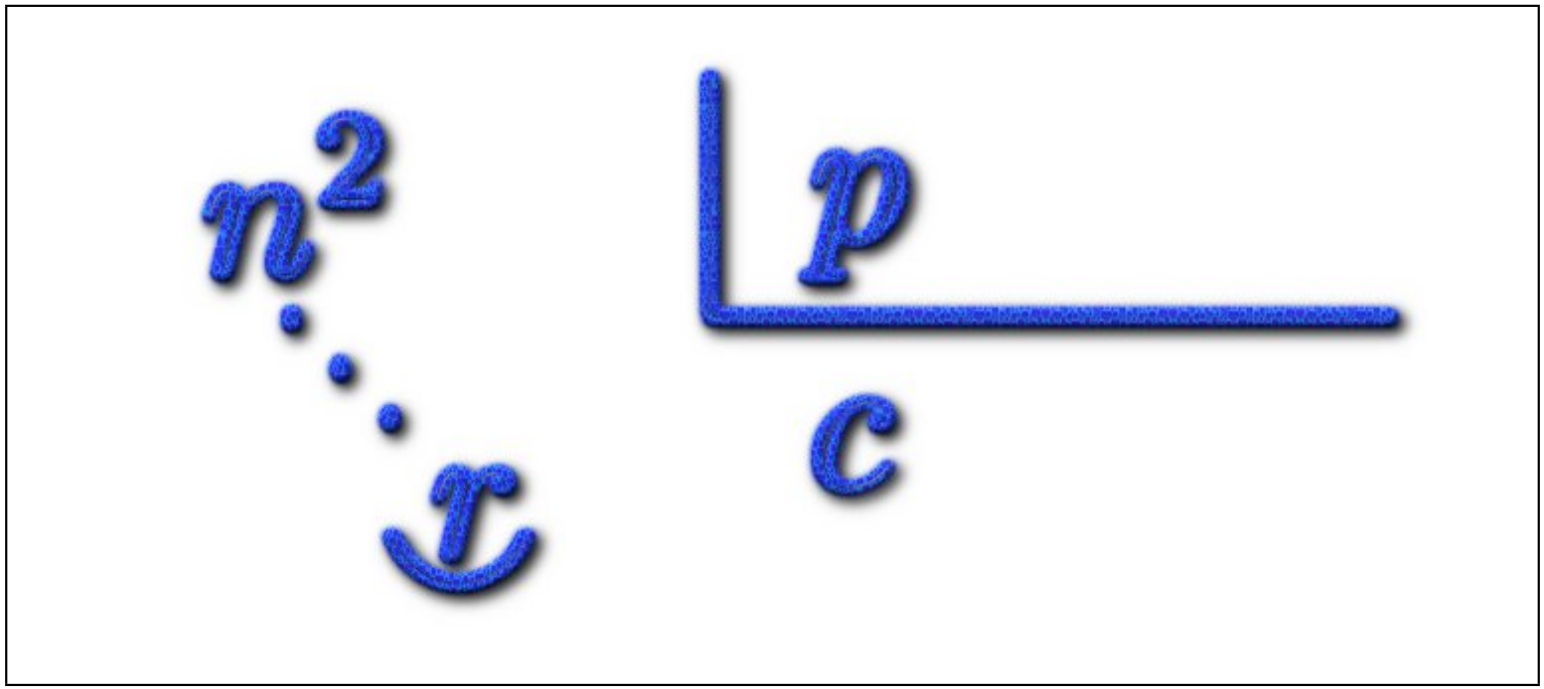
Una pregunta más básica:

¿Cómo es posible que los números, que son "naturales", tengan propiedades matemáticas profundas?

¿Por qué hay muchos problemas de teoría de números con enunciado sencillo y solución complicada?
¿Por qué para entener los números tenemos que estudiar cosas que aparentemente no tienen nada que ver con ellos?

En Matemáticas todo está conectado

En otras áreas de la Ciencia hay una división más clara entre diferentes temas.


n^2
p
x
c

Dividiendo cuadrados...

¿Es n^2+1 divisible por 103 para algún n?

¿Qué números se obtienen al factorizar n^2+1?

$1^2+1=\mathbf{2}$, $5^2+1=2\cdot\mathbf{13}$, $9^2+1=2\cdot\mathbf{41}$, $13^2+1=2\cdot5\cdot17$
$2^2+1=\mathbf{5}$, $6^2+1=\mathbf{37}$, $10^2+1=\mathbf{101}$, $14^2+1=\mathbf{197}$
$3^2+1=2\cdot5$, $7^2+1=2\cdot5^2$, $11^2+1=2\cdot\mathbf{61}$, $15^2+1=2\cdot\mathbf{113}$
$4^2+1=\mathbf{17}$, $8^2+1=5\cdot13$, $12^2+1=5\cdot\mathbf{29}$, $16^2+1=\mathbf{257}$

Posibles primos: 2, 5, 13, 17, 29, 37, 41, 61, 101, 113, 197, 257
Salvo el 2, sus factores primos difieren en múltiplos de 4

¿Por qué los factores primos de n^2+3 mayores que 3 siempre difieren en múltiplos de 6?

Primos módulo 4

1	**2**	**3**	4
5	6	**7**	8
9	10	**11**	12
13	14	15	16
17	18	**19**	20
21	22	**23**	24
25	26	27	28
29	30	**31**	32
33	34	35	36
37	38	39	40
41	42	**43**	44
45	46	**47**	48
49	50	51	52
53	54	55	56
57	58	**59**	60
61	62	63	64
65	66	**67**	68
69	70	**71**	72
73	74	75	76

Factores primos de $n^2 + 1$

1	**2**	**3**	4
5	6	**7**	8
9	10	**11**	12
13	14	15	16
17	18	**19**	20
21	22	**23**	24
25	26	27	28
29	30	**31**	32
33	34	35	36
37	38	39	40
41	42	**43**	44
45	46	**47**	48
49	50	51	52
53	54	55	56
57	58	**59**	60
61	62	63	64
65	66	**67**	68
69	70	**71**	72
73	74	75	76

Primos módulo 6

1	**2**	**3**	4	**5**	6
7	8	9	10	**11**	12
13	14	15	16	**17**	18
19	20	21	22	**23**	24
25	26	27	28	**29**	30
31	32	33	34	35	36
37	38	39	40	**41**	42
43	44	45	46	**47**	48
49	50	51	52	**53**	54
55	56	57	58	**59**	60
61	62	63	64	65	66
67	68	69	70	**71**	72
73	74	75	76	77	78
79	80	81	82	**83**	84
85	86	87	88	**89**	90
91	92	93	94	95	96
97	98	99	100	**101**	102
103	104	105	106	**107**	108
109	110	111	112	**113**	114

Factores primos de $n^2 + 3$

1	**2**	**3**	4	**5**	6
7	8	9	10	**11**	12
13	14	15	16	**17**	18
19	20	21	22	**23**	24
25	26	27	28	**29**	30
31	32	33	34	35	36
37	38	39	40	**41**	42
43	44	45	46	**47**	48
49	50	51	52	**53**	54
55	56	57	58	**59**	60
61	62	63	64	65	66
67	68	69	70	**71**	72
73	74	75	76	77	78
79	80	81	82	**83**	84
85	86	87	88	**89**	90
91	92	93	94	95	96
97	98	99	100	**101**	102
103	104	105	106	**107**	108
109	110	111	112	**113**	114

Primos módulo 7

1	**2**	**3**	4	**5**	6	**7**
8	9	10	**11**	12	**13**	14
15	16	**17**	18	**19**	20	21
22	**23**	24	25	26	27	28
29	30	**31**	32	33	34	35
36	**37**	38	39	40	**41**	42
43	44	45	46	**47**	48	49
50	51	52	**53**	54	55	56
57	58	**59**	60	**61**	62	63
64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77
78	**79**	80	81	82	**83**	84
85	86	87	88	**89**	90	91
92	93	94	95	96	**97**	98
99	100	**101**	102	**103**	104	105
106	**107**	108	**109**	110	111	112
113	114	115	116	117	118	119
120	121	122	123	124	125	126
127	128	129	130	**131**	132	133

Factores primos de $n^2 + 7$

1	**2**	**3**	4	**5**	6	**7**
8	9	10	**11**	12	**13**	14
15	16	**17**	18	**19**	20	21
22	**23**	24	25	26	27	28
29	30	**31**	32	33	34	35
36	**37**	38	39	40	**41**	42
43	44	45	46	**47**	48	49
50	51	52	**53**	54	55	56
57	58	**59**	60	**61**	62	63
64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77
78	**79**	80	81	82	**83**	84
85	86	87	88	**89**	90	91
92	93	94	95	96	**97**	98
99	100	**101**	102	**103**	104	105
106	**107**	108	**109**	110	111	112
113	114	115	116	117	118	119
120	121	122	123	124	125	126
127	128	129	130	**131**	132	133

Euler (1751) enunció 59 "teoremas" experimentales relacionados con el tema.

Problema general

Euler decía que un primo p *pertenece* a $n^2 + k$ si $p|n^2 + k$ para algún n. El problema general consiste en caracterizar los primos que pertenecen a $n^2 + k$.

Con argumentos elementales (completar cuadrados) la solución de este problema permitiría caracterizar los enteros que dividen a algún valor de cualquier polinomio fijado de segundo grado $P(n) = an^2 + bn + c$.

Caracterizar $p \in n^2 + 5$ ya quedaba fuera de los métodos del siglo XVIII, aunque experimentalmente es fácil intuir (como hizo Euler) que el resultado es $\{2, 5\} \cup \{p \equiv 1, 4 \pmod 5\}$.

Una de las pocas caracterizaciones completas que se sabían probar antes de Gauss era:

Fermat (?) - Euler (1758)

$\{\text{factores primos de } n^2+1\} = \{2\} \cup \{\text{primos de la forma } 4n+1\}$.

Con la notación de Euler

$$p \in n^2+1 \iff p = 2 \text{ ó } p \equiv 1 \pmod 4$$

Prueba (parte difícil): $\mathbb{Z}_p^*$ cíclico $\{1,\ldots,p-1\} = \{g^1, g^2, \ldots, g^{p-1}=1\}$

Si $p = 4n+1$

$$\{x_j = g^{(p-1)j/4},\ j = 0,1,2,3\} = \{\text{raíces de } x^4-1 \text{ mód } p\}$$

$x^4-1 = (x^2-1)(x^2+1) \Rightarrow$ **$x^2+1=0$ tiene solución mód p.**

Euler (1760) (una curiosa reducción)

Para estudiar $p \in n^2 + k$ basta considerar k primo porque

$$p \in n^2 + ab \Leftrightarrow \begin{cases} p \in n^2 + a \text{ y } p \in n^2 + b \\ \text{ó} \\ p \notin n^2 + a \text{ y } p \notin n^2 + b \end{cases}$$

si $\frac{p-1}{2}$ es par $p \nmid ab$. Para $\frac{p-1}{2}$ impar se cumple cambiando el primer término por $p \notin n^2 + ab$.

Ej. No existe n tal que $13|n^2 + 5$ ni n tal que $13|n^2 + 7 \Rightarrow$ existe n tal que $13|n^2 + 35$. De hecho $2^2 + 35 = 3 \cdot 13$.

Gauss resolvió el problema gracias a su ley de reciprocidad cuadrática:

Ley de reciprocidad cuadrática. Gauss (1796)

Si $p, q > 2$ primos distintos

- Si $\frac{p+1}{2}$, $\frac{q+1}{2}$ impares: $p \in n^2 + q \Leftrightarrow q \in n^2 + p$
- Si $\frac{p+1}{2}$ ó $\frac{q+1}{2}$ par: $p \in n^2 + q \Leftrightarrow q \notin n^2 + p$

Con ello se tiene un algoritmo para obtener los teoremas que Euler no supo demostrar.

Ej. $\frac{7+1}{2}$ par $p \in n^2 + 7 \Leftrightarrow 7 \notin n^2 + p$. Trabajando módulo 7, $k^2 + p \not\equiv 0$ con $0 < k < 7$ da lugar a $p \equiv 1, 2, 4 \pmod 7$.

¿Por qué razón una simetría tan simple como la ley de reciprocidad cuadrática no es inmediata?
¿Por qué las pruebas de la ley de reciprocidad cuadrática son truculentas? (Gauss dio seis demostraciones)

Desde el propio Gauss los matemáticos han buscado generalizaciones que nos muestren la ley de reciprocidad cuadrática como un caso particular de una simetría más profunda.

$p \in n^2 + k$ es lo mismo que decir que $x^2 + k$ tiene sus dos raíces en $\mathbb{Z}_p$ y la ley de reciprocidad cuadrática caracteriza p mediante condiciones de congruencia.

Problema (*Ley de "reciprocidad" generalizada*)

Dado un polinomio de grado d caracterizar mediante condiciones de congruencia los p para los cuales tiene d raíces en $\mathbb{Z}_p$.

En la actualidad el problema se sabe resolver cuando

¡el grupo de Galois sobre $\mathbb{Q}$ del polinomio es abeliano!

¿Por qué un problema de congruencias (restos al dividir) tiene que ver con el grupo de Galois (automorfismos en extensiones algebraicas de $\mathbb{Q}$)?
¿Hay alguna otra simetría que se aplique al caso no abeliano?

L. Euler
s. XVIII

$\longrightarrow$

C.F. Gauss
s. XIX

$\longrightarrow$

E. Artin
s. XX

Curioso

Los divisores de un polinomio de segundo grado parecen no ser aleatorios.

Curioso, Insospechado

Los divisores de un polinomio de segundo grado parecen no ser aleatorios.

Hay una simetría entre diferentes polinomios que no es sencilla de probar.

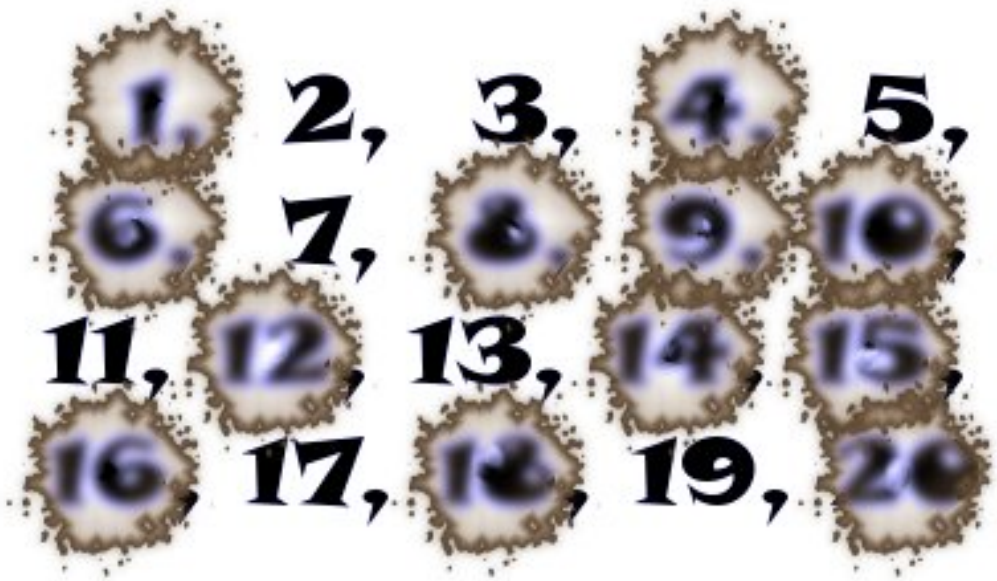
Curioso, Insospechado y Alucinante

Los divisores de un polinomio de segundo grado parecen no ser aleatorios.

Hay una simetría entre diferentes polinomios que no es sencilla de probar.

Extender una forma de esta simetría a grados superiores requiere temas avanzados de álgebra.

Primos



La distribución de los primos

Prueba de Euler de la infinitud de los primos 1737

$$\begin{aligned}\prod (1-\frac{1}{p})^{-1} &= \prod (1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\dots) \\ &= \sum \frac{1}{n} = \infty \quad (\log\infty \text{ para Euler})\end{aligned}$$

Tomando logaritmos y usando $-\log(1-x) \sim x$ para x pequeño, Euler concluía

$$\sum \frac{1}{p} = \log\log\infty$$

y como $\log\log\infty < \log\infty$ (¿?) los primos son "infinitamente menos numerosos que los naturales".

Con tablas extensas (Gauss) resulta que la probabilidad de que un número de tamaño N sea primo es con gran aproximación $1/\log N$. Matemáticamente, si $\pi(x) = \#\{p \leq x\}$ para x grande

$$\pi(x) \sim \int_2^x \frac{dt}{\log t} \quad \left(\sim \frac{x}{\log x} \text{ aproximación peor } \right)$$

donde $f \sim g$ significa $f/g \to 1$ cuando $x \to \infty$.

Preguntas

- ¿Por qué razón al contar primos aparece un logaritmo?
- ¿Cómo de buena es la aproximación?

Las respuestas no empezaron a gestarse hasta 60 años después de notarse este fenómeno y tuvieron que pasar otros 40 para materializarse en resultados matemáticos rigurosos.

C.F. Gauss

Unter	gibt es Primzahlen	Integral $\int \frac{dn}{\log n}$	Abweich.
500000	41556	41606,4	+ 50,4
1000000	78501	79627,5	+ 126,5
1500000	114112	114263,1	+ 151,1
2000000	148883	149054,8	+ 171,8
2500000	183016	183245,0	+ 229,0
3000000	216745	216970,6	+ 225,6

C.F. Gauss

x	$\pi(x)$	$\int_2^x - \pi(x)$	$\pi(x)/\int_2^x$
10^4	1 229	17	0.986
10^5	9 592	38	0.9960
10^6	78 498	130	0.9983
10^7	664 579	339	0.99949
10^8	5 761 455	754	0.99987
10^9	50 847 534	1 701	0.999967
10^{10}	455 052 511	3 104	0.9999932

$$\frac{10^{10}}{\log 10^{10}} = 434\ 294\ 481{,}9 \qquad \pi(10^{10})/\frac{10^{10}}{\log 10^{10}} = 1{,}047\ldots$$

$$\text{Euler} \quad \to \quad \prod (1-\frac{1}{p^s})^{-1} = \sum \frac{1}{n^s} := \zeta(s)$$

Riemann 1859

Se puede "despejar" de esta identidad usando variable compleja:

$$\log + \text{Taylor} \quad \to \quad \sum (\frac{1}{p^s} + \frac{1}{2p^{2s}} + \frac{1}{3p^{3s}} + \dots) = \log \zeta(s)$$

$$\text{Tma de los residuos} \quad c>1 \quad \to \quad \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{t^s}{s} ds = \begin{cases} 1 \text{ si } t>1 \\ 0 \text{ si } 0<t<1 \end{cases}$$

De aquí

$$\underbrace{\pi(x) + \frac{1}{2}\pi(x^{1/2}) + \frac{1}{3}\pi(x^{1/3}) + \dots}_{\pi(x)+O(x^{1/2})} = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{x^s \log \zeta(s)}{s} ds$$

¡La cantidad de primos se escribe como una integral compleja!

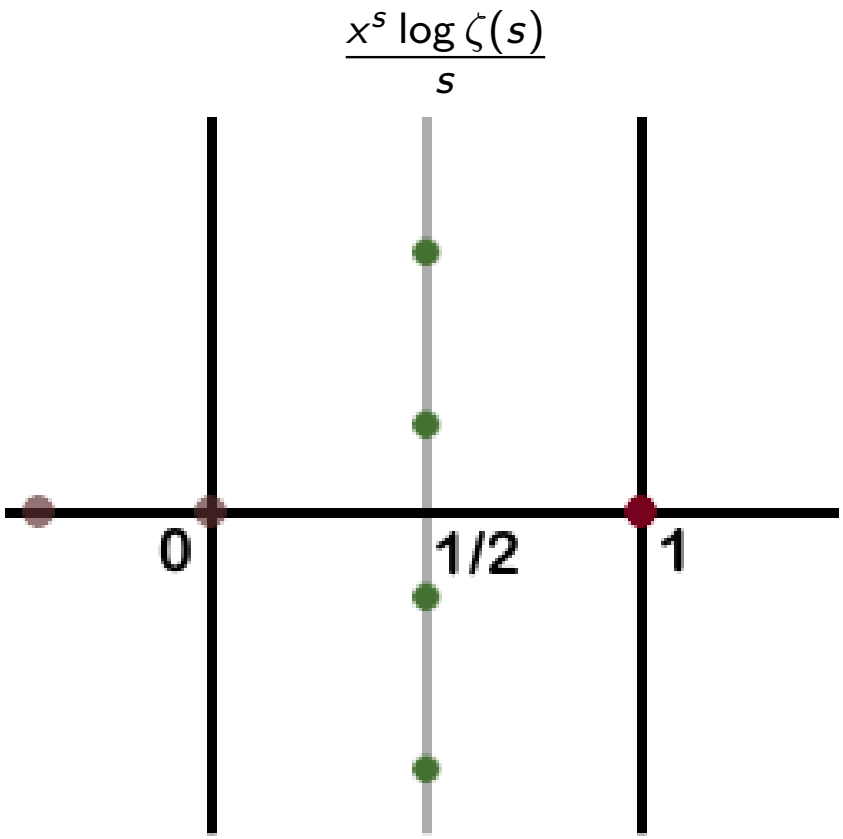
Pero las integrales complejas se pueden calcular a menudo en términos de las singularidades del integrando.

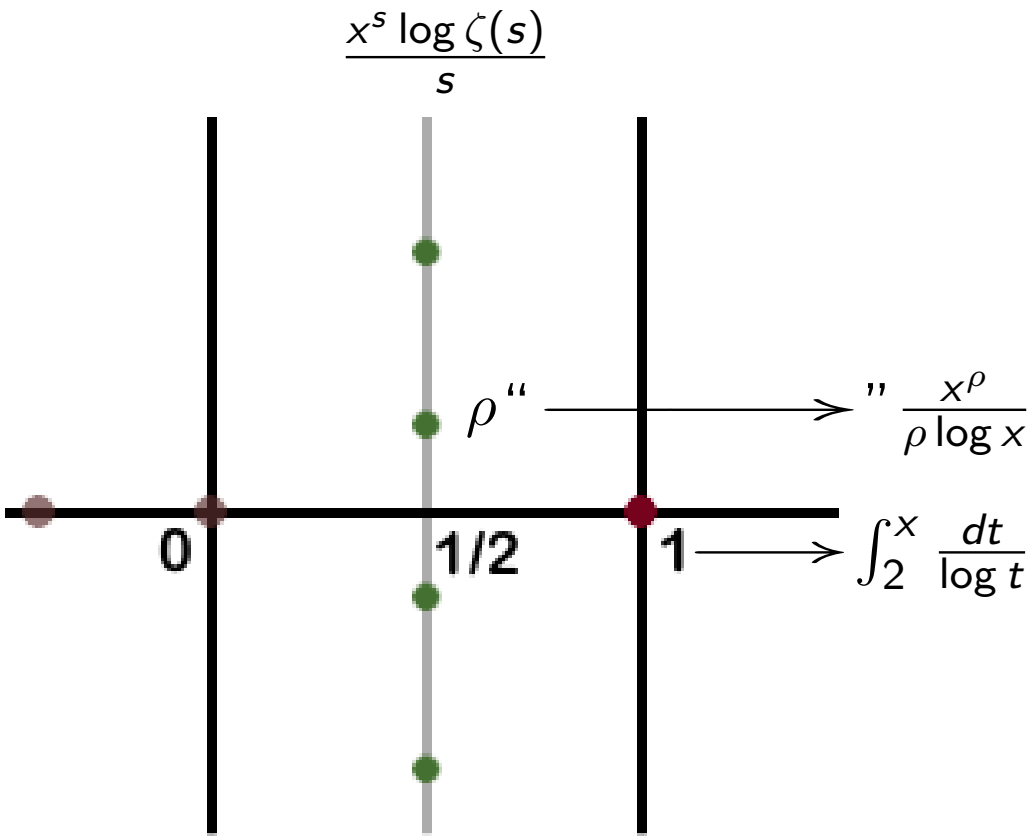
Singularidades de $\log \zeta(s) \rightarrow$ ceros (y polos) de $\zeta(s)$.

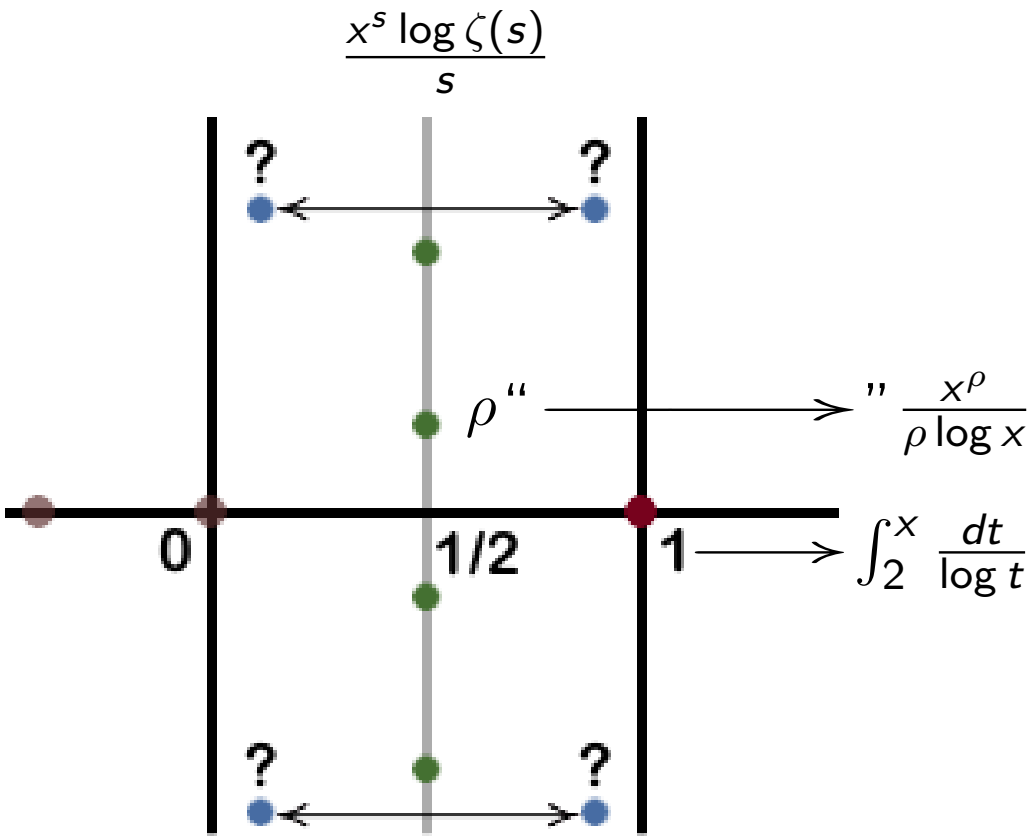
Riemann

- $\zeta(s)$ se extiende a $\mathbb{C}$ con un sólo polo en $s = 1$
- Los ceros con $\mathrm{Re}(s) > 0$ tienen simetrías $s \leftrightarrow 1 - s$ y $s \leftrightarrow 1 - \overline{s}$
- Si no hay ceros en un semiplano que contiene a $\mathrm{Re}(s) > \sigma$, entonces

$$\left|\pi(x) - \int_2^x \frac{dt}{\log t}\right| < Cx^{\sigma}$$


$\frac{x^s \log \zeta(s)}{s}$
0
1/2
1


$\frac{x^s \log \zeta(s)}{s}$
ρ " → " $\frac{x^\rho}{\rho \log x}$
0
1/2
1
$\int_2^x \frac{dt}{\log t}$



Cuanto más a la derecha estén las singularidades, distintas de $s = 1$, mayor es el error en la aproximación $\pi(x) \sim \int_2^x \frac{dt}{\log t}$

El menor error se obtendría si los ceros de $\zeta(s)$ con $\mathrm{Re}(s) > 0$ estuvieran en fila india en $\mathrm{Re}(s) = \frac{1}{2}$ (Hipótesis de Riemann)

¿Se cumple la Hipótesis de Riemann?

¿Por qué razón los ceros de $\zeta(s)$ deben estar en una línea?
No se sabe pero se ha comprobado numéricamente para 10^{13} ceros

Curioso

Los primos son aparentemente caóticos pero su densidad decae como un logaritmo.

Curioso, Insospechado

Los primos son aparentemente caóticos pero su densidad decae como un logaritmo.

Este comportamiento se demostró empleando integrales complejas y métodos de análisis.

Curioso, Insospechado y Alucinante

Los primos son aparentemente caóticos pero su densidad decae como un logaritmo.

Este comportamiento se demostró empleando integrales complejas y métodos de análisis.

Hay un "si y sólo si" relacionando el error al contar números primos con los ceros de cierta función de variable compleja.

$$2N = p_1 + p_2$$

$$2N + 1 = p_1 + p_2 + p_3$$

Primos contra sumas

Los primos están asociados a la factorización (estructura multiplicativa).
Los problemas aditivos con primos suelen ser difíciles.

¿Se puede escribir un número N como suma de k primos?

$$r_k(N) = \#\{(p_1, p_2, \ldots, p_k) \ : \ p_1 + p_2 + \cdots + p_k = N\}$$

¿Se cumple $r_k(N) > 0$?

Condición natural: N y k con la misma paridad (sólo hay un primo par).

Conjetura de Goldbach

$r_2(N) > 0$ para todo $N \geq 4$ par.

Mejores resultados

Teorema de Vinogradov (1937) (enunciado simplificado)

N impar, $N >$ constante muy grande $\Rightarrow r_3(N) > 0$

Teorema de Chen (1966) (enunciado simplificado)

N par, $N >$ cte muy grande $\Rightarrow N = p_1 + p_2$ ó $N = p_1 + p_2 p_3$

I.M. Vinogradov
(1891-1983)

J.-R. Chen
(1933-1996)

El teorema de Vinogradov. Algunas ideas

Exponencial: mundo aditivo $\leftrightarrow$ mundo multiplicativo $\quad e^{x+y} = e^x \cdot e^y$

$$e^{it} = \cos t + i \operatorname{sen} t, \qquad \int_0^1 e^{2\pi ikx} e^{-2\pi imx}\, dx = \begin{cases} 1 & \text{si } k = m \\ 0 & \text{si } k \neq m \end{cases}$$

Fórmula fundamental

$$r_3(N) = \int_0^1 \left(\sum_{p<N} e^{2\pi ipx} \right)^3 e^{-2\pi iNx}\, dx$$

porque

$$\left(\sum_{p<N} e^{2\pi ipx} \right)^3 = \sum_{p_1,p_2,p_3<N} e^{2\pi i(p_1+p_2+p_3)x}$$

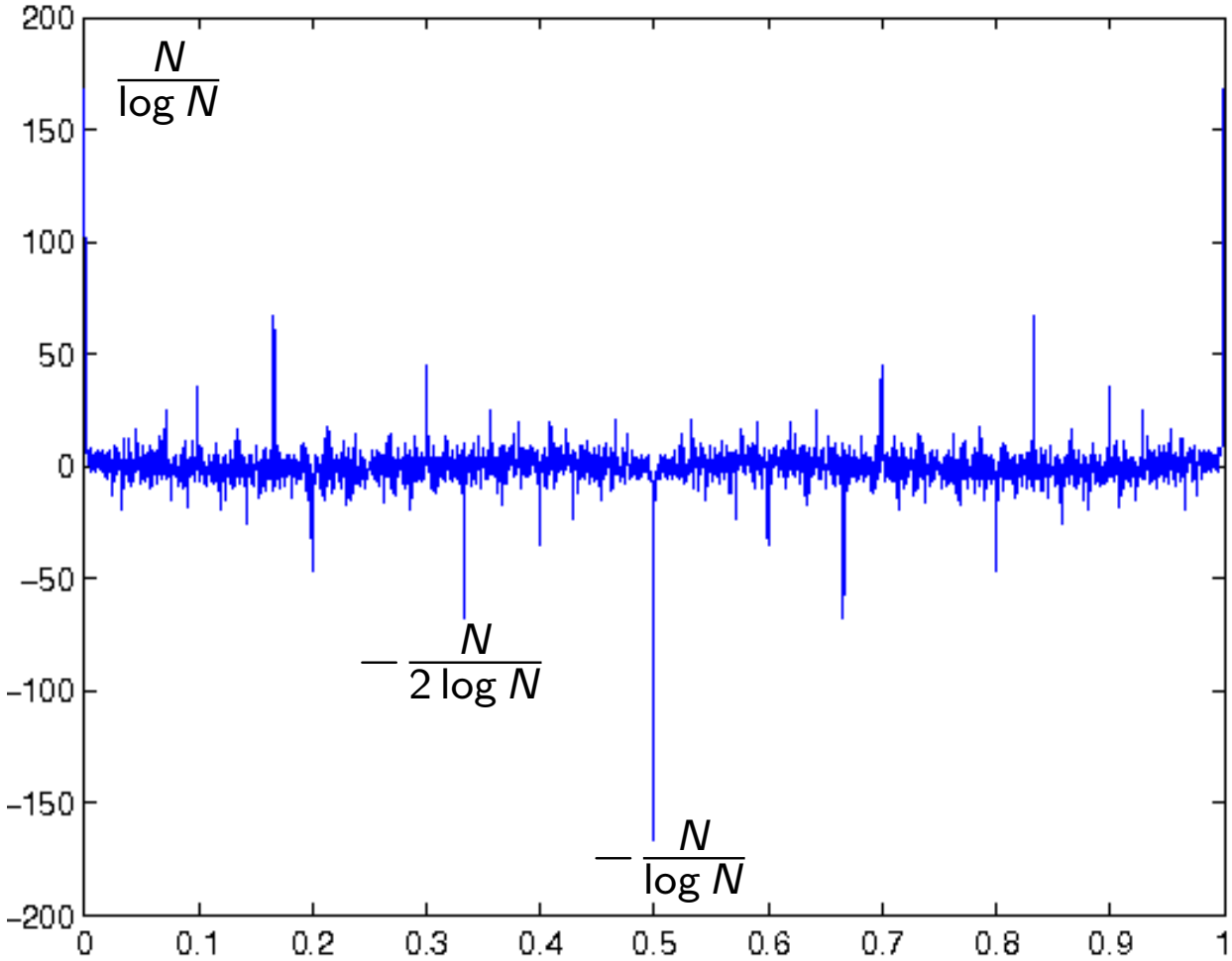
$$r_3(N) = \int_0^1 \big(f(x)\big)^3 e^{-2\pi i N x}\, dx, \qquad f(x) = \sum_{p<N} e^{2\pi i p x}$$

Sólo es útil si sabemos decir algo de f

Recordemos $\text{Prob}\big(\{n \in [1, N] \text{ primo}\}\big) \sim 1/\log N$

- $f(0) = f(1) \sim \dfrac{N}{\log N}$
- $f(1/2) = 1 + \displaystyle\sum_{2<p<N} (-1) \sim -\frac{N}{\log N}$
- $f(1/3) = 1 + \displaystyle\sum_{\substack{p<N \\ p\equiv 1 \ (3)}} e^{2\pi i/3} + \sum_{\substack{p<N \\ p\equiv 2 \ (3)}} e^{4\pi i/3} \sim -\frac{N}{2\log N}$

$$f(x) = \sum_{p<N} e^{2\pi i p x}$$



$$r_3(N) = \int_0^1 \big(f(x)\big)^3 e^{-2\pi i N x}\, dx, \qquad f(x) = \sum_{p<N} e^{2\pi i p x}$$

$$f(0) = f(1) \sim \frac{N}{\log N}, \quad f(1/2) \sim -\frac{N}{\log N}, \quad f(1/3) \sim -\frac{N}{2\log N}$$

1. f no oscila en intervalos de longitud $< 1/N$
2. $\sum e^{2\pi i p x}$ sólo tiene "resonancias" cerca de los racionales de denominador pequeño $\Rightarrow$ en el resto f es pequeña

Teorema. Para N impar grande

$$r_3(N) \text{“}\sim\text{”} \frac{1}{N}\left(\frac{N}{\log N}\right)^3 \left(1^3 + (-1)^3 e^{-\pi i} + \big(-\frac{1}{2}\big)^3 e^{-2\pi i/3} + \dots\right)$$

Evaluando la serie (!) el resultado preciso que se prueba es:

Teorema. Para N impar grande

$$r_3(N) \sim \frac{N^2}{2\log^3 N} \prod_{p\nmid N}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p\mid N}\left(1-\frac{1}{(p-1)^2}\right)$$

Si pudiéramos copiar el procedimiento:

Teorema. Para N par grande

$$r_2(N) \sim \frac{N}{\log^2 N} \prod_{p\nmid N}\left(1-\frac{1}{(p-1)^2}\right)\prod_{p\mid N}\left(1+\frac{1}{p-1}\right)$$

que experimentalmente parece verificarse.

Buena noticia

- El método es muy general y permite tratar de la misma forma otros problemas aditivos con primos o con otros conjuntos de enteros.

Malas noticias

- La constante en el teorema es tan grande que ni siquiera se ha podido alcanzar con ordenadores y no sabemos si $r_3(N) > 0$ para $N \geq 7$ impar.
- Al aplicar el método a $r_2(N)$ los términos de error en las aproximaciones superan al término principal. De hecho hay razones teóricas que impiden aplicar el método en esta forma a $r_2(N)$.

Unas palabras sobre criba

La prueba del teorema de Chen es difícil de describir. Se basa en métodos muy avanzados de criba.
El punto de partida de estos métodos es la selección de los primos de una sucesión utilizando el principio de inclusión-exclusión, iterar la identidad $\#(A \cup B) = \#A + \#B - \#(A \cap B)$.

Por ejemplo:

$$\#\{\text{primos } p \in [A, B]\} \leq B - \#\bigcup_{p<A} \{\text{múltiplos de } p\}$$

y si aplicásemos directamente el principio de inclusión-exclusión se tendrían demasiado sumandos.

Unas palabras sobre criba

Los métodos de criba buscan versiones aproximadas del principio de inclusión-exclusión con menos sumandos válidas para detectar primos o números con pocos factores.

La estimación de los sumandos pasa por considerar funciones de variable compleja más complicadas que la introducida por Riemann y cuyos ceros son todavía más desconocidos.

Esta dificultad también aparecía en el teorema de Vinogradov y por ello durante algún tiempo tras la prueba no se supo ningún N a partir del cual se pudiera asegurar $r_3(N) > 0$.

Curioso

Los números impares parecen escribirse como suma de tres primos de muchas formas distintas.

Curioso, Insospechado

Los números impares parecen escribirse como suma de tres primos de muchas formas distintas.

Se demostró para impares grandes empleando una especie de serie de Fourier con frecuencias primas.

Curioso, Insospechado y Alucinante

Los números impares parecen escribirse como suma de tres primos de muchas formas distintas.

Se demostró para impares grandes empleando una especie de serie de Fourier con frecuencias primas.

Para acercarse a la conjetura de Goldbach se han unido desigualdades combinatorias muy complicadas con un estudio analítico de la distribución de los primos en progresiones aritméticas.

$$x^n + y^n = z^n$$

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

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

$$x^n + y^n = z^n$$

UTF

↓ Kummer

Teoría de ideales

Prueba para muchos exponentes

UTF

↓ Kummer

Teoría de ideales

Prueba para muchos exponentes

Funciones e integrales elípticas

↓ Gauss, Jacobi, Weierstrass, Klein, Poincaré

Formas modulares

Formas diferenciales en superficies de Riemann

UTF

↓ Kummer

Teoría de ideales

Prueba para muchos exponentes

Funciones e integrales elípticas

↓ Gauss, Jacobi, Weierstrass, Klein, Poincaré

Formas modulares

Formas diferenciales en superficies de Riemann

Ciertas formas modulares

Conjetura:

Eichler-Shimura →

← (Taniyama)

Curvas elípticas sobre $\mathbb{Q}$

UTF

↓ Kummer

Teoría de ideales

Prueba para muchos exponentes

Funciones e integrales elípticas

↓ Gauss, Jacobi, Weierstrass, Klein, Poincaré

Formas modulares

Formas diferenciales en superficies de Riemann

Ciertas formas modulares ⟶ (Eichler-Shimura) ⟵ (Taniyama) Curvas elípticas sobre $\mathbb{Q}$

Conjetura:

UTF falso ⟹ (Frey) Curva elíptica extraña ⟹ Ribet Conjetura falsa

UTF

↓ Kummer

Teoría de ideales

Prueba para muchos exponentes

Funciones e integrales elípticas

↓ Gauss, Jacobi, Weierstrass, Klein, Poincaré

Formas modulares

Formas diferenciales en superficies de Riemann

Ciertas formas modulares ⟶ (Eichler-Shimura) ⟵ (Taniyama) Curvas elípticas sobre $\mathbb{Q}$

Conjetura:

UTF falso ⟹ (Frey) Curva elíptica extraña ⟹ (Ribet) Conjetura falsa

Wiles (y otros) ⟹ Conjetura cierta ⟹ **UTF**

El *último teorema de Fermat* es un problema de teoría de números de enunciado elemental. En su solución se han utilizado muchas de las herramientas de diversas asignaturas que suelen componer la licenciaturas de matemáticas como:
Teoría de números, geometría algebraica, variable compleja (formas modulares), topología, álgebra lineal, teoría de grupos, teoría de Galois.
Y por supuesto técnicas más avanzadas que exceden la licenciatura.

En la prueba se han creado matemáticas muy interesantes al lado de las cuales el último teorema de Fermat es una mera curiosidad histórica.

¿Es realmente necesario ir tan lejos? ¿Por qué nadie ha conseguido utilizar matemáticas elementales para llegar a una prueba?


Alucinante

Referencias

Para saber más:

- F.J. Cilleruelo; A. Córdoba.*La teoría de los números*. Mondadori, Madrid 1992.
- Y. Hellegouarch. *Invitation to the mathematics of Fermat-Wiles*. Academic Press, Inc., San Diego, CA, 2002.
- S. Lang. *El placer estético de las matemáticas*. Alianza Universidad 1992.
- H.E. Rosen. *A course in number theory*. The Clarendon Press, Oxford University Press, New York, 1994.
- I. Stewart. *De aquí al infinito*. Crítica 1998.
- I. Stewart. *Cartas a una joven matemática*. Crítica 2006.

Hay copia de esta presentación en `http://www.uam.es/fernando.chamizo`