LOS PRIMEROS 50 MILLONES DE NÚMEROS PRIMOS

DON ZAGIER

Me gustaría hablarles hoy sobre una materia que, aunque nunca he trabajado en ella, me ha cautivado siempre extraordinariamente, y que ha fascinado a los matemáticos desde la antiguedad hasta el presente —es decir, la cuestión de la distribución de los números primos.

Todos ciertamente conocen lo que es un número primo: es un número natural mayor que 1 que no es divisible por otro número natural excepto por 1. Esta al menos es la definición del especialista en Teoría de Números; otros matemáticos a veces dan otras definiciones. Para el especialista en Teoría de Funciones, por ejemplo, un número primo es una raíz de la función analítica

$$1 - \frac{\operatorname{sen} \dfrac{\pi\,\Gamma(s)}{s}}{\operatorname{sen} \dfrac{\pi}{s}};$$

para el dedicado al Álgebra es *"la característica de un cuerpo finito"* ó *"un punto de* $\operatorname{Spec}(\mathbf{Z})$*"* ó *"una valuación no arquimediana"*; un especialista en Combinatoria definirá los número primos inductivamente por la recurrencia [1]

$$p_{n+1} = \left[1 - \log_2\left(\frac{1}{2} + \sum_{r=1}^{n} \sum_{1 \le i_1 < \cdots < i_r \le n} \frac{(-1)^r}{2^{p_{i_1} \cdots p_{i_r}} - 1}\right)\right],$$

donde $[x]$ denota el mayor entero $\le x$; y finalmente, los lógicos han definido recientemente los primos como los valores positivos del polinomio [2]

$$\begin{aligned}
&F(a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,\\
&\qquad p,q,r,s,t,u,v,w,x,y,z) =\\
&[k+2]\,[1-(wz+h+j-q)^2-(2n+p+q+z-e)^2\\
&-(a^2y^2-y^2+1-x^2)^2-(\{e^4+2e^3\}\{a+1\}^2-1-o^2)^2\\
&\qquad -(16\{k+1\}^3\{k+2\}\{n+1\}^2+1-f^2)^2\\
&-(\{(a+u^4-u^2a)^2-1\}\{n+4dy\}^2+1-\{x+cu\}^2)^2\\
&-(ai+k+1-l-i)^2-(\{gk+2g+k+1\}\{h+j\}-h-z)^2\\
&-(16r^2y^4\{a^2-1\}+1-u^2)^2-(p-m+l\{a-n-1\}\\
&\qquad +b\{2an+2a-n^2-2n-2\})^2\\
&\qquad -(z-pm+pla-p^2l+t\{2ap-p^2-1\})^2\\
&-(q-x+y\{a-p-1\}+s\{2ap+2a-p^2-2p-2\})^2\\
&\qquad -(a^2l^2-l^2+1-m^2)^2-(n+l+v-y)^2].
\end{aligned}$$

Pero espero que estén satisfechos con la primera definición que les dí.

Hay dos hechos sobre la distribución de los números primos de las que espero convencerles tan fuertemente que queden permanentemente grabadas en sus corazones. La primera es que, a pesar de su sencilla definición y de su papel como ladrillos en la construcción de los números naturales, los números primos pertenecen a la clase más arbitraria y perversa de los objetos estudiados por los matemáticos: crecen como malas hierbas entre los números naturales, parecen no obedecer otra ley que las del azar, y nadie puede predecir donde brotará el siguiente. El segundo hecho es incluso más sorprendente, pues afirma justo lo contrario: que los números primos exhiben sorprendentes regularidades, que hay leyes que gobiernan su comportamiento, y que obedecen estas leyes casi con precisión militar.

Para sostener la primera de estas afirmaciones, déjenme comenzar mostrándoles una lista de los números primos y compuestos hasta 100 (en la que aparte del 2 he incluido sólo los números impares).

Mathematical Intelligencer, **0**, (1977), 7–19.

Este artículo es una versión revisada de la lección inaugural del autor (*Antrittsvorlesung*) leída el 5 de mayo de 1975 en la Universidad de Bonn. Traducido del alemán por R. Perlis. La versión alemana original será publicada también en *Beihefte zu Elemente der Mathematik*, N° 15, Birkhäuser Verlag, Basel.

[1] J. M. Gandhi, *Formulae for the* n^{th} *prime*, Proc. Washington State Univ. Conf. on Number Theory, Washington State Univ., Pullman, Wash., (1971), 96–106.

[2] J. P. Jones, *Diophantine representation of the set of prime numbers*, Notices of the Amer. Math. Soc. **22**, (1975), A–326.

PRIMOS			COMPUESTOS		
2	23	59	9	45	75
3	29	61	15	49	77
5	31	67	21	51	81
7	37	71	25	55	85
11	41	73	27	57	87
13	43	79	33	63	91
17	47	83	35	65	93
19	53	89	39	69	95
		97			99

y otras dos listas con los primos comprendidos entre los 100 números que preceden y siguen inmediatamente a 10 millones:

Números primos entre 9 999 900 **y** 10 000 000		**Números primos** entre 10 000 000 **y** 10 000 100
9 999 901	9 999 943	10 000 019
9 999 907	9 999 971	10 000 079
9 999 929	9 999 973	
9 999 931	9 999 991	
9 999 937		

Imagino que estarán de acuerdo conmigo en que no hay razón aparente del porqué un número es primo y otro no. Por el contrario, mirando estos números uno tiene la sensación de estar en presencia de uno de los inexplicables secretos de la creación. Que incluso los matemáticos no han penetrado en este secreto se muestra convincentemente viendo el ardor con el cual buscan números primos cada vez más grandes —con números que crecen regularmente, como cuadrados o potencias de dos, nadie se molestaría en escribir ejemplos mayores que los previamente conocidos, pero para los números primos algunos se han tomado un gran trabajo en hacer justo eso. Por ejemplo, en 1876 Lucas probó que el número $2^{127}-1$ es primo, y durante 75 años esto no se mejoró —lo que quizás no es sorprendente cuando uno ve este número:

$$2^{127}-1 = 170141183460469231731687303715884105727.$$

No fue hasta 1951, con la aparición de los computadores electrónicos, que fueron descubiertos primos mayores. En la tabla que aparece a continuación, pueden ver los datos de los sucesivos records [3]

Los mayores primos conocidos			
p	digitos	Año	Autor
$2^{127}-1$	39	1876	Lucas
$\frac{1}{17}(2^{148}+1)$	44	1951	Ferrier
$114(2^{127}-1)+1$	41	1951	Miller +
$180(2^{127}-1)^2+1$	79		Wheeler+ EDSAC 1
$2^{521}-1$	157	1952	Lehmer+ Robinson + SWAC
$2^{607}-1$	183		
$2^{1729}-1$	386		
$2^{2203}-1$	664		
$2^{2281}-1$	687		
$2^{3217}-1$	969	1957	Riesel + BESK
$2^{4253}-1$	1281	1961	Hurwitz+ Selfridge+ IBM 7090
$2^{4423}-1$	1332		
$2^{9689}-1$	2917	1963	Gillies +ILIAC 2
$2^{9941}-1$	2993		
$2^{11213}-1$	3376		
$2^{19937}-1$	6002	1971	Tuckerman +IBM360

Más interesante, sin embargo, es la cuestión de las leyes que gobiernan a los números primos. Ya hemos visto una lista de los primos hasta el 100. Aquí les presento la misma información gráficamente. La función designada por $\pi(x)$ (sobre la que les hablaré continuamente a partir de este momento) es el número de números primos que no superan a x; por tanto $\pi(x)$ comienza en 0 y salta en una unidad en cada número primo 2, 3, 5, etc. Ya en este gráfico podemos ver que, a pesar de pequeñas oscilaciones, $\pi(x)$ en conjunto crece bastante regularmente.

[3] Hay buenas razones por las que tantos de estos números tienen la forma $M_k = 2^k - 1$: Un teorema de Lucas establece que M_k ($k > 2$) es primo si y sólo si M_k divide a L_{k-1}, donde los números L_n se definen inductivamente por $L_1 = 4$, y $L_{n+1} = L_n^2 - 2$ (así que $L_2 = 14$, $L_3 = 194$, $L_4 = 37634$, ...) y, por tanto es mucho más fácil comprobar que M_k es primo que comprobarlo para otro número del mismo orden de magnitud.
Los números primos de la forma $2^k - 1$ (para lo que k mismo debe necesariamente ser primo) se llaman primos de Mersenne (por el matemático francés Mersenne que en 1644 confeccionó una lista de tales primos hasta 10^{79}, correcta hasta 10^{18}) y juegan un papel en conexión con un problema de teoría de números completamente diferente. Euclides descubrió que cuando $2^p - 1$ es primo entonces el número $2^{p-1}(2^p-1)$ es "*perfecto*", esto es, igual a la suma de sus divisores propios (por ejemplo $6 = 1+2+3$, $28 = 1+2+4+7+14$, $496 = 1+2+4+8+16+31+62+124+248$) y Euler mostró que cualquier número perfecto par tiene esta forma. No se sabe si hay algún número perfecto impar; si existen, deben ser mayores que 10^{100}. Hay exactamente 24 valores de $p < 20{,}000$ para los que $2^p - 1$ sea primo.

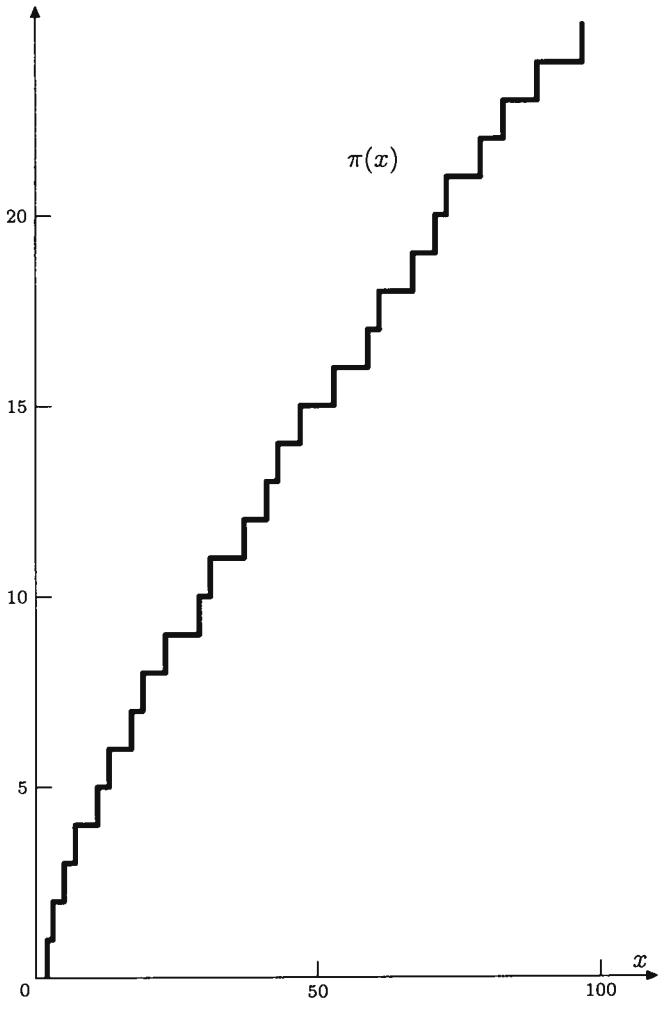

FIGURA 1

Pero si extendemos el dominio de valores de x desde cien hasta cincuenta mil, entonces esta regularidad se hace sorprendentemente clara, pues el gráfico ahora aparece así:

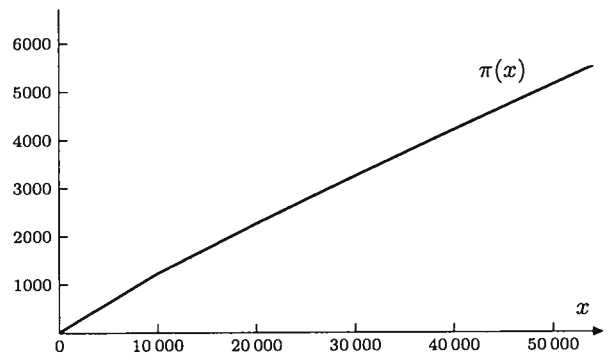

FIGURA 2

Para mí, la suavidad con que esta curva sube es uno de los hechos más sorprendentes en las matemáticas.

Pero donde la naturaleza revela un esquema, es seguro que aparecerán científicos buscando una explicación. La regularidad observada en los primos no es excepción a esta regla. No es difícil encontrar una fórmula empírica que dé una buena descripción del crecimiento de los números primos. Por debajo de 100 hay 25 primos, esto es, la cuarta parte de los números; por debajo de 1000 hay 168, o sea alrededor de un sexto; hasta 10.000 hay 1229 primos, es decir alrededor de un octavo. Si extendemos esta lista, calculando la proporción de números primos entre los números naturales hasta cien mil, un millón, etc., entonces encontramos la siguiente tabla (en la que los valores de $\pi(x)$, tabulados tan fácilmente aquí, representan miles de horas de monótonos cálculos).

x	$\pi(x)$	$x/\pi(x)$
10	4	2,5
100	25	4,0
1000	168	6,0
10,000	1,229	8,1
100,000	9,592	10,4
1,000,000	78,498	12,7
10,000,000	664,579	15,0
100,000,000	5,761,455	17,4
1,000,000,000	50,847,534	19,7
10,000,000,000	455,052,512	22,0

Vemos aquí que la razón de x a $\pi(x)$ salta aproximadamente $2,3$ cuando pasamos de una potencia de 10 a la siguiente. Un matemático inmediatamente reconoce $2,3$ como el logaritmo de 10 (respecto a la base e, naturalmente). Somos conducidos por tanto a conjeturar que

$$\pi(x) \sim \frac{x}{\log x}$$

donde el símbolo $\sim$ significa que la razón

$$\pi(x)/(x/\log x)$$

tiende a 1 cuando x tiende a infinito. Esta relación (que no fue probada hasta 1896) se conoce como el *teorema de los números primos*. Gauss, el mayor matemático de todos, la descubrió a la edad de quince años estudiando las tablas de números primos contenido en un libro de logaritmos que le habían regalado el año anterior. Durante toda su vida Gauss estuvo muy interesado en la distribución de los números primos e hizo extensos cálculos. En una carta a Enke [4] describe cómo, muy a menudo,

[4] C. F. Gauss, Werke II (1892) 444–447. Para una discusión de la historia de las varias aproximaciones a $\pi(x)$, en la que aparece la traducción inglesa de esta carta, ver L. J. Goldstein, *A history*

empleaba un cuarto de hora perdido en contar otra *chiliada* más (esto es, un intervalo de 1,000 números) aquí y allí, hasta que finalmente había contado todos los números primos hasta 3 millones (!) y comparaba su distribución con la fórmula que él había conjeturado.

El teorema de los números primos establece que $\pi(x)$ es asintóticamente —es decir, con un error relativo del 0 %— igual a $x/\log x$. Pero si comparamos el gráfico de la función $x/\log x$ con el de $\pi(x)$, vemos que aunque la función $x/\log x$ cualitativamente refleja el comportamiento de $\pi(x)$, ciertamente no concuerda con ella lo suficiente para explicar la suavidad de la última:

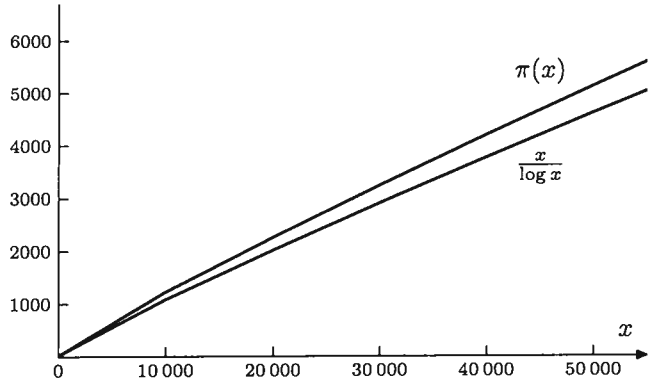

FIGURA 3

Así pues es natural buscar mejores aproximaciones. Si miramos de nuevo nuestra tabla de proporciones de x a $\pi(x)$, encontramos que esta proporción es casi exactamente $\log x - 1$. Con cálculos más cuidadosos y con datos más detallados sobre $\pi(x)$, Legendre [5] encontró en 1808 que una aproximación particularmente buena se obtiene si en lugar de 1 restamos 1,08366 de $\log x$, es decir

$$\pi(x) \approx \frac{x}{\log x - 1,08366}$$

Otra buena aproximación a $\pi(x)$, que fue primeramente dada por Gauss, se obtiene tomando como punto de partida el hecho empírico de que la frecuencia de los números primos en la proximidad de un número grande x es casi exactamente $1/\log x$. De aquí que el número de números primos hasta x debiera ser aproximadamente dado por la *suma logarítmica*

$$\mathrm{Ls}(x) = \frac{1}{\log 2} + \frac{1}{\log 3} + \cdots + \frac{1}{\log x}$$

o, lo que es esencialmente lo mismo [6] por la *integral logarítmica*

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\log t}\, dt.$$

Si comparamos ahora el grafo de $\mathrm{Li}(x)$ con el de $\pi(x)$, vemos que en los límites de aproximación de nuestro dibujo, las dos figuras coinciden exactamente.

No merece la pena mostrar también la gráfica de la aproximación de Legendre, pues en el rango del gráfico es incluso una mejor aproximación de $\pi(x)$.

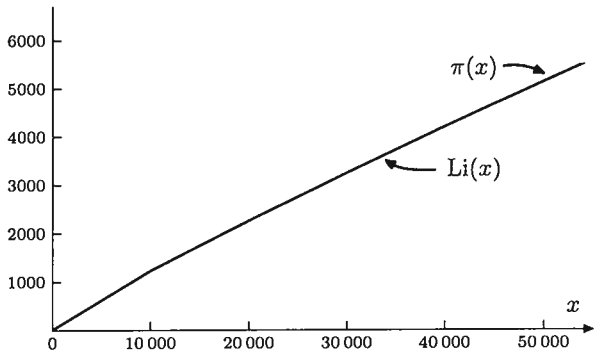

FIGURA 4

Hay otra aproximación que deseo mencionar. Las investigaciones de Riemann sobre los números primos sugieren que la probabilidad de que un número grande x sea primo sería incluso más próxima a $1/\log x$ si se contaran no sólo los números primos sino también las potencias de los primos, contando el cuadrado de un primo como la mitad de un primo, el cubo de un primo como un tercio de un primo, etc. Esto conduce a la aproximación

$$\pi(x) + \frac{1}{2}\pi(\sqrt{x}) + \frac{1}{3}\pi(\sqrt[3]{x}) + \cdots = \mathrm{Li}(x)$$

o, de manera equivalente [7]

$$\pi(x) = \mathrm{Li}(x) - \frac{1}{2}\mathrm{Li}(\sqrt{x}) - \frac{1}{3}\mathrm{Li}(\sqrt[3]{x}) - \cdots$$

of the prime number theorem, Amer. Math. Monthly, **80** (1973) 599–615.

[5] A. M. Legendre, *Essai sur la theorie des Nombres*, segunda ed., Paris, 1808, p. 394.

[6] Más precisamente

$$\mathrm{Ls}(x) - 1,5 < \mathrm{Li}(x) < \mathrm{Ls}(x),$$

esto es, la diferencia entre $\mathrm{Li}(x)$ y $\mathrm{Ls}(x)$ está acotada. Debemos también mencionar que la integral logarítmica es a menudo definida como el valor principal de Cauchy

$$\mathrm{Li}(x) = \text{v.p.}\int_0^x \frac{dt}{\log t} \underset{DEF}{=} \lim_{\epsilon\to 0}\left(\int_0^{1-\epsilon} \frac{dt}{\log t} + \int_{1-\epsilon}^{x} \frac{dt}{\log t}\right),$$

pero esta definición difiere de la dada en el texto sólo por una constante.

[7] Los coeficientes se forman como sigue: el coeficiente de $\mathrm{Li}(\sqrt[n]{x})$ es $+1/n$ si n es el producto de un número par de primos distintos, $-1/n$ si n es el producto de un número impar de primos distintos, y 0 si n contiene factores primos multiples.

En honor de Riemann la función en el lado derecho de esta fórmula se denota por $R(x)$. Representa una aproximación sorprendentemente buena a $\pi(x)$, como muestran los siguientes valores

x	$\pi(x)$	$R(x)$
100.000.000	5.761.455	5.761.552
200.000.000	11.078.937	11.079.090
300.000.000	16.252.325	16.252.355
400.000.000	21.336.326	21.336.185
500.000.000	26.355.867	26.355.517
600.000.000	31.324.703	31.324.622
700.000.000	36.252.931	36.252.719
800.000.000	41.146.179	41.146.248
900.000.000	46.009.215	46.009.949
1.000.000.000	50.847.534	50.847.455

Para aquellos en la audiencia que conocen algo de la Teoría de Funciones, quizás deba añadir que $R(x)$ es una función entera de $\log x$, dada por la serie de potencias rápidamente convergente

$$R(x) = 1 + \sum_{n=1}^{\infty} \frac{1}{n\zeta(n+1)} \frac{(\log x)^n}{n!},$$

donde $\zeta(n+1)$ es la función zeta de Riemann[8].

En este punto debo señalar que las aproximaciones de Gauss y Legendre a $\pi(x)$ fueron obtenidas sólo empíricamente, y que incluso Riemann aunque fue conducido a la función $R(x)$ por consideraciones teóricas nunca probó el teorema de los números primos. Esto fue primeramente conseguido en 1896 por Hadamard e (independientemente) por de la Vallée Poussin. Sus demostraciones se basan en el trabajo de Riemann.

Siguiendo con el tema de la predictabilidad de los números primos quisiera dar unos pocos ejemplos númericos más. Como ya hemos mencionado la probabilidad de que un número del orden de magnitud x sea primo es aproximadamente igual a $1/\log x$, esto es, el número de primos en un intervalo de longitud a próximo a x debiera ser aproximadamente $a/\log x$, al menos si el intervalo es lo suficiente grande para hacer las estadisticas razonables, pero pequeño en comparación con x. Por ejemplo, esperamos encontrar alrededor de 8142 primos en el intervalo entre 100 millones y 100 millones más 150,000 ya que

$$\frac{150{,}000}{\log(100{,}000{,}000)} = \frac{150{,}000}{18{,}427\ldots} \approx 8142.$$

De acuerdo con esto la probabilidad de que dos números aleatorios cercanos a x sean ambos primos es aproximadamente $1/(\log x)^2$. Por tanto si uno pregunta cuántos primos gemelos (esto es, pares de primos que difieran en dos unidades, como 11 y 13 o 59 y 61) hay entre x y $x+a$, podemos esperar que sean $a/(\log x)^2$. De hecho, debemos esperar algo más, puesto que el hecho de ser n primo cambia ligeramente la probabilidad de que $n+2$ lo sea (por ejemplo, $n+2$ es ciertamente impar). Un argumento heurístico fácil [9] nos dice que el número esperado de primos gemelos es $C \cdot a/(\log x)^2$ en el intervalo $[x, x+a]$ donde C es una constante cuyo valor es alrededor de $1,3$ (más exactamente: C=1,3203236316...). Por tanto entre 100 millones y 100 millones más 150,000 debe haber alrededor de

$$(1,32\ldots)\frac{150{,}000}{(18,427)^2} \approx 584$$

pares de primos gemelos. Presentamos ahora datos calculados por Jones, Lal y Blundon [10] dando el número exacto de primos y primos gemelos en este intervalo, así como en varios intervalos de la misma longitud alrededor de mayores potencias de 10:

[8] Ramanujan ha dado las siguientes formas alternativas de esta función:

$$R(x) = \int_0^{+\infty} \frac{(\log x)^t\, dt}{t\,\Gamma(t+1)\zeta(t+1)}$$

($\zeta(s)$ es la función zeta de Riemann y $\Gamma(s)$ la función gamma)

$$R(e^{2\pi x}) \doteq \frac{2}{\pi}\Big(\frac{2}{B_2}x + \frac{4}{3B_4}x^3 + \frac{6}{5B_6}x^5 + \cdots\Big) = \frac{2}{\pi}\Big(12x + 40x^3 + \frac{252}{5}x^5 + \cdots\Big)$$

(donde B_k es el k-ésimo número de Bernoulli y el símbolo $\doteq$ significa que la diferencia de los dos miembros tiende a 0 cuando x crece a infinito). Ver G. H. , *Ramanujan: Twelve Lectures on Subjects Suggested by His Life and Work*, Cambridge University Press, 1940, Chapter 2.

[9] Es éste: La probabilidad de que en un par (m,n) escogido al azar ambos m y n cumplan que son $\not\equiv 0 \pmod p$ es obviamente $[(p-1)/p]^2$, mientras que para un número al azar n, la probabilidad de que n y $n+2$ sean ambos $\not\equiv 0 \pmod p$ es $1/2$ para $p=2$ y $(p-2)/p$ para $p \neq 2$. Por tanto la probabilidad para que n y $n+2$ módulo p sean primos gemelos difiere por un factor $\frac{p-2}{p}\cdot\frac{p^2}{(p-1)^2}$ para $p \neq 2$ y 2 en el caso de $p=2$ de la correspondiente probabilidad para dos números independientes m y n. En conjunto, hemos mejorado por tanto nuestras probabilidades en un factor

$$C = 2 \cdot \prod_{p>2, p \text{ primo}} \frac{p^2-2p}{p^2-2p+1} = 1,32032.$$

Para una presentación más cuidadosa de este argumento, ver Hardy y Wright *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford. 1960, § 22.20 (p. 371–373).

[10] M. F. Jones, M. Lal, y W. J. Blundon, *Statistics on certain large primes*, Math. Comp. **21** (1967) 103–107.

INTERVALOS	NÚMEROS PRIMOS		PRIMOS GEMELOS	
	esperados	encontrados	esperados	encontrados
(100 000 000, 100 150 000)	8142	8154	584	601
(1 000 000 000, 1 000 150 000)	7328	7242	461	466
(10 000 000 000, 10 000 150 000)	6514	6511	374	389
(100 000 000 000, 100 000 150 000)	5922	5974	309	276
(1 000 000 000 000, 1 000 000 150 000)	5429	5433	259	276
(10 000 000 000 000, 10 000 000 150 000)	5011	5065	221	208
(100 000 000 000 000, 100 000 000 150 000)	4653	4643	191	186
(1 000 000 000 000 000, 1 000 000 000 150 000)	4343	4251	166	161

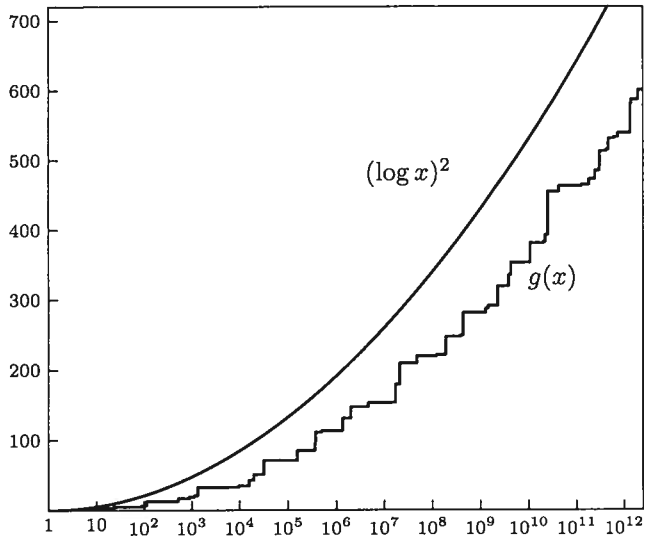

FIGURA 5

Como puede verse, el acuerdo con la teoría es extremadamente bueno. Esto es especialmente sorprendente en el caso de los primos gemelos, puesto que todavía no se ha podido probar que existan infinitos de tales parejas de primos, menos aún que se distribuyan de acuerdo con la ley conjeturada.

Quiero dar una última ilustración de la predictabilidad de los números primos, el caso de las lagunas entre números primos. Si se miran las tablas de primos, se encuentran a veces intervalos inusualmente largos, por ejemplo entre 113 y 127, que no contienen primos. Sea $g(x)$ la longitud del mayor intervalo libre de primos o *laguna* hasta x. Por ejemplo la mayor laguna hasta 200 es el intervalo desde 113 hasta 127 mencionado antes, de manera que $g(200) = 14$. Naturalmente el número $g(x)$ crece muy erráticamente, pero un argumento heurístico sugiere la fórmula asintótica [11]

$$g(x) \sim (\log x)^2.$$

En la siguiente gráfica podemos ver lo bien que la función $g(x)$, tan salvajemente irregular, se ajusta al comportamiento esperado.

[11] D. Shanks, *On maximal gaps between successive primes*, Math. Comp. **18** (1964) 646–651. El gráfico de $g(x)$ se obtuvo de las tablas encontradas en los siguientes artículos: L. J. Lander and T. R. Parkin, *On first appearance of prime differences*, Math. Comp. **21** (1967) 483–488, R. P. Brent, *The first occurrence of large gaps between successive primes*, Math. Comp. **27** (1973) 959–963

Hasta ahora he documentado mejor mi afirmación sobre el orden de los primos que mi afirmación sobre su desorden. Además, tampoco he cumplido la promesa hecha en mi título de mostrarles los primeros 50 millones de primos, solamente he mostrado unos pocos miles. Por esto aquí muestro un gráfico de $\pi(x)$ comparado con las aproximaciones de Legendre, Gauss y Riemann hasta 10 millones [12]. Puesto que estas cuatro funciones están tan próximas que sus gráficos son indistinguibles al ojo — como ya vimos en el dibujo hasta 50,000— he dibujado solamente las diferencias entre ellas:

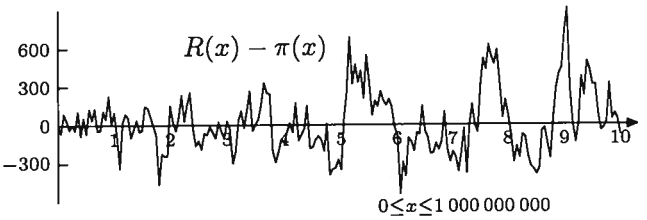

FIGURA 7

Las oscilaciones de la función $R(x) - \pi(x)$ se hacen más y más grandes, pero incluso para estos valores, casi inconcebiblemente grandes de x, nunca

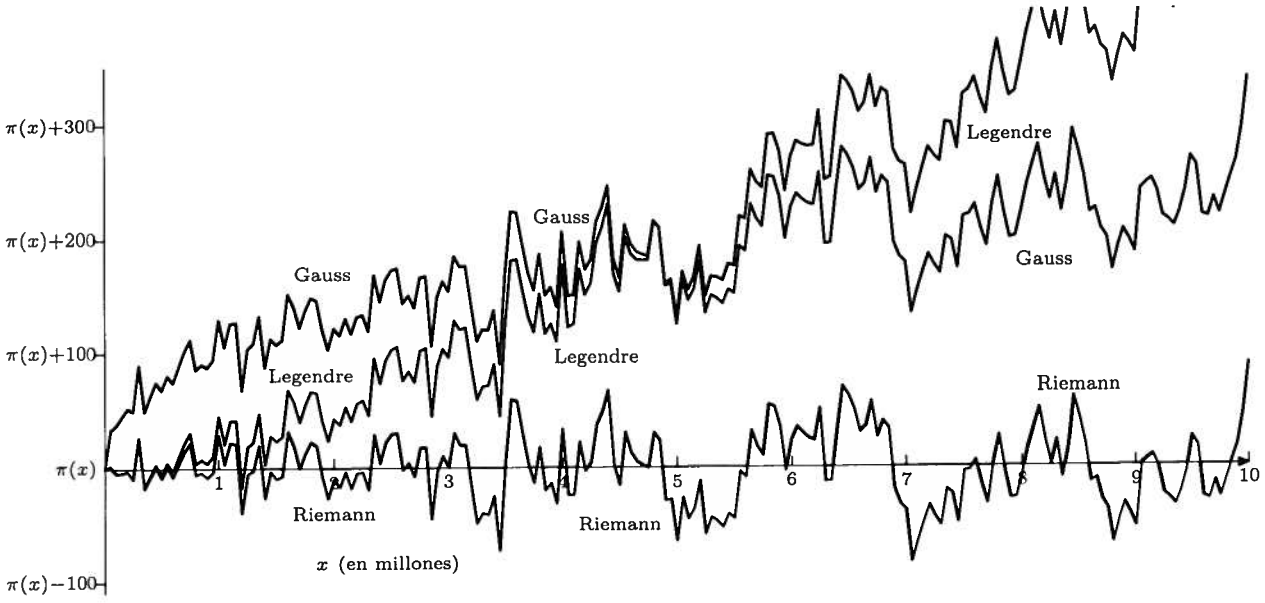

FIGURA 6

Este gráfico, pienso, muestra en lo que se mete la persona que decide estudiar Teoría de Números. Como puede verse, para x pequeños (hasta aproximadamente un millón) la aproximación de Legendre $x/(\log x - 1{,}08366)$ es considerablemente mejor que la de Gauss $\mathrm{Li}(x)$, pero despues de 5 millones $\mathrm{Li}(x)$ es mejor, y puede probarse que $\mathrm{Li}(x)$ sigue siendo la mejor cuando x crece.

Pero hasta 10 millones hay sólo unos 600 mil números primos; para mostrarles los prometidos 50 millones de primos, tengo que llegar no a 10 millones: tengo que subir hasta los 1000 millones. En este rango el gráfico de $R(x) - \pi(x)$ aparece como sigue[13]:

superan unos pocos cientos.

En conexión con estos datos debemos mencionar aún otro hecho sobre el número de números primos $\pi(x)$. En la figura hasta 10 millones, la aproximación de Gauss era siempre mayor que $\pi(x)$. Esto sigue así hasta mil millones, como puede verse en la figura 8 en la página siguiente (donde estos datos se dibujan en una escala logarítmica).

Seguro que esta gráfica nos da la impresión de que con x crecientes las diferencias $\mathrm{Li}(x) - \pi(x)$ crecen continuamente hasta infinito, esto es que la integral logarítmica de forma consistente sobreestima el número de primos hasta x (esto estaría de acuerdo también con la observación de que $R(x)$ es una aproximación mejor que $\mathrm{Li}(x)$, puesto que $R(x)$ es siempre menor que $\mathrm{Li}(x)$). Pero esto es falso: puede probarse que existen puntos donde la oscilaciones

[12] Los datos para este gráfico están tomados de las tablas de números primos de Lehmer (D. N. Lehmer, *List of prime numbers from* 1 *to* 10,006,721, Hafner Publishing Co., New York, 1956).

[13] Éste y el siguiente gráfico estan hechos usando los valores de $\pi(x)$ encontrados en D. C. Mapes, *Fast method for computing the number of primes less than a given limit*, Math. Comp. **17**, (1963), 179–185. En contraste con los datos de Lehmer usados en los gráficos previos, estos valores fueron calculados mediante una fórmula para $\pi(x)$ y no contando los primos hasta x.

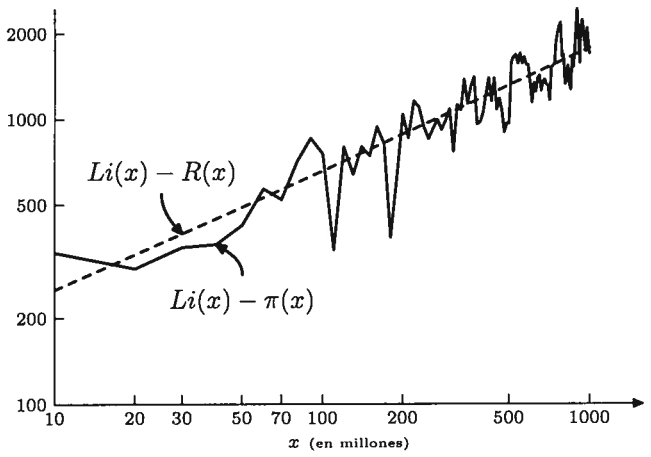

FIGURA 8

de $R(x) - \pi(x)$ son tan grandes que $\pi(x)$ de hecho llega a ser mayor que $\mathrm{Li}(x)$. Hasta ahora no se ha encontrado ningún tal número, y quizás nunca llegue a encontrarse uno, pero Littlewood probó que existen y Skewes [14] probó que hay uno que es menor que

$$10^{10^{10^{34}}}$$

(un número del que Hardy dijo una vez que seguro que era el mayor que haya sido utilizado con un propósito definido en matemáticas). En cualquier caso, este ejemplo muestra qué imprudente puede resultar fundamentar conclusiones sobre los primos tan sólo en datos numéricos.

En la última parte de mi conferencia quisiera hablar sobre algunos resultados teóricos sobre $\pi(x)$ para que no se vayan con la sensación de haber visto sólo matemática experimental. Un no iniciado ciertamente pensaría que la propiedad de ser primo es demasiado aleatoria para que nosotros podamos probar algo sobre ella. Esto fue refutado ya hace 2200 años por Euclides, quien probó la existencia de infinitos primos. Su argumento puede ser formulado en una frase: Si sólo hubiera un número finito de primos, entonces multiplicándolos todos y sumando 1, obtendríamos un número que no es divisible por ningún primo, y eso es imposible. En el siglo XVIII, Euler probó más, que la suma de los inversos de los números primos diverge, es decir, eventualmente excede cualquier número dado previamente. Su demostración, que es también muy simple, usa la función

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots,$$

cuya importancia en el estudio de $\pi(x)$ fue completamente reconocida sólo más tarde, con el trabajo de Riemann. Es divertido señalar que, aunque la suma de los inversos de todos los primos es divergente, esta suma sobre todos los primos conocidos (digamos que los primeros 50 millones) es menor que cuatro [15]. El primer resultado importante en la dirección de la teoría de los números primos fue probado por Chebyshev en 1850.[16] Probó que para x suficientemente grande

$$0{,}89\frac{x}{\log x} < \pi(x) < 1{,}11\frac{x}{\log x},$$

es decir, el teorema de los números primos es correcto con un error relativo de a lo más el 11 %. Su demostración usa los coeficientes binomiales y es tan bonita que no puedo resistir al menos bosquejar una versión simplificada de la prueba (con constantes un poco peores).

En una dirección probaremos

$$\pi(x) < 1{,}7\frac{x}{\log x}.$$

Esta desigualdad es válida para $x < 1200$. Supongamos por inducción que ha sido probada para $x < n$ y consideremos el coeficiente binomial central

$$\binom{2n}{n}.$$

[14] S. Skewes, *On the difference* $\pi(x) - Li(x)$ *(I)* J. London Math. Soc. **8**, (1933), 277–283. La demostración de Skewes de esta cota supone la validez de la hipótesis de Riemann que discutiremos más adelante. Veintidos años más tarde (*On the difference* $\pi(x) - Li(x)$ *(II)*, Proc. London. Math. Soc. (3) **5**, (1955), 48–70) probó sin usar la hipótesis de Riemann que existe un x menor que la cota (más grande aún)

$$10^{10^{10^{964}}}$$

para el cual $\pi(x) > \mathrm{Li}(x)$. Esta cota ha sido disminuida a

$$10^{10^{529{,}7}}$$

por Cohen y Mayhew y a $1{,}65 \times 10^{1165}$ por Lehman (*On the difference* $\pi(x) - Li(x)$, Acta Arithm. **11**, (1966), 397–410). Lehman muestra incluso que hay un intervalo de al menos 10^{500} números entre $1{,}53 \times 10^{1165}$ y $1{,}65 \times 10^{1165}$ donde $\pi(x)$ supera a $\mathrm{Li}(x)$. Como consecuencia de su investigación, parece probable que haya un número próximo a $6{,}663 \times 10^{370}$ donde $\pi(x) > \mathrm{Li}(x)$ y que no existe ningún número menor que 10^{20} con esta propiedad.

[15] Ya que (como conjeturó Gauss en 1796 y probó Mertens en 1874)

$$\sum_{p<x} \frac{1}{p} = \log\log x + C + \varepsilon(x),$$

donde $\varepsilon(x) \to 0$ cuando x tiende a infinito y $C \approx 0{,}261497$ es una constante. Esta expresión es menor que 3,3 cuando $x = 10^9$, incluso para $x = 10^{18}$ es todavía menor que 4.

[16] P. L. Chebyshev, *Recherches nouvelles sur les nombres premiers*, Paris, 1851, C. R. Paris **29**, (1849), 397–401, 738–739. Una presentación moderna (en alemán) de la prueba de Chebyshev puede verse en W. Schwarz, *Einführung in Methoden und Ergebnisse der Primzahltheorie* BI-Hochschultaschenbuch 278/278a, Mannheim 1969, Chapt. II.4, p. 42–48.

Puesto que

$$2^{2n} = (1+1)^{2n} = \binom{2n}{0} + \binom{2n}{1} + \cdots + \binom{2n}{n} + \cdots + \binom{2n}{2n}$$

este coeficiente es a lo más 2^{2n}. Por otro lado

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \frac{(2n)\cdot(2n-1)\cdots(n+2)\cdot(n+1)}{n\cdot(n-1)\cdots 2\cdot 1}.$$

Cada primo p menor que $2n$ aparece en el numerador, pero ciertamente ningún p mayor que n puede aparecer en el denominador. Por tanto

$$\binom{2n}{n}$$

es divisible por cada primo entre n y $2n$:

$$\prod_{n<p\le 2n} p \,\Big|\, \binom{2n}{n}.$$

Pero el producto tiene $\pi(2n)-\pi(n)$ factores, cada uno mayor que n, así que obtenemos

$$n^{\pi(2n)-\pi(n)} \le \prod_{n<p\le 2n} p \le \binom{2n}{n} < 2^{2n}$$

o, si tomamos logaritmos

$$\pi(2n)-\pi(n) < \frac{2n\log 2}{\log n} < 1{,}39\frac{n}{\log n}.$$

Por inducción, el teorema es válido para n, así que $\pi(n) < 1{,}7(n/\log n)$, y sumando estas relaciones resulta

$$\pi(2n) < 3{,}09\frac{n}{\log n} < 1{,}7\frac{2n}{\log(2n)}, \qquad (n > 1200).$$

Entonces el teorema es válido para $2n$. Puesto que

$$\pi(2n+1) \le \pi(2n)+1 < 3{,}09\frac{n}{\log n} + 1 \le 1{,}7\frac{2n+1}{\log(2n+1)}, \qquad (n > 1200),$$

es también válido para $2n+1$, completando la inducción.

Para la cota en la otra dirección, necesitamos un lema sencillo que puede probarse fácilmente usando la bien conocida fórmula para la potencia de p que divide a $n!$[17]:

Lema 1. *Sea p un primo. Si p^{ν_p} es la mayor potencia de p que divide a $\binom{n}{k}$, entonces*

$$p^{\nu_p} \le n.$$

Corolario 2. *Cada coeficiente binomial $\binom{n}{k}$ satisface*

$$\binom{n}{k} = \prod_{p\le n} p^{\nu_p} \le n^{\pi(n)}.$$

Si sumamos las desigualdades del corolario para todos los coeficientes binomiales con un n fijo, encontramos

$$2^n = (1+1)^n = \sum_{k=0}^{n}\binom{n}{k} \le (n+1)\cdot n^{\pi(n)}$$

y tomando logaritmos

$$\pi(n) \ge \frac{n\log 2}{\log n} - \frac{\log(n+1)}{\log n} > \frac{3}{2}\frac{n}{\log n}, \qquad (n > 200).$$

Para terminar, quisiera decir unas pocas palabras sobre el trabajo de Riemann. Aunque Riemann nunca probó el teorema de los números primos, hizo algo que de alguna forma es mucho más sorprendente —descubrió una fórmula exacta para $\pi(x)$. Esta fórmula tiene la forma

$$\pi(x) + \frac{1}{2}\pi(\sqrt{x}) + \frac{1}{3}\pi(\sqrt[3]{x}) + \cdots = \mathrm{Li}(x) - \sum_{\varrho}\mathrm{Li}(x^{\varrho})$$

donde el índice de la suma recorre las raíces de la función $\zeta(s)$[18]. Estas raíces (aparte de los llamados ceros *triviales* $\varrho = -2, -4, -6, \ldots$, que aportan una contribución despreciable a la fórmula) son números

[17] La mayor potencia de p que divide a $n!$ es p^a, donde

$$a = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots,$$

y $\lfloor x \rfloor$ es el mayor entero $\le x$. Así en la notación del lema

$$\nu_p = \sum_{r\ge 1}\left(\left\lfloor \frac{n}{p^r}\right\rfloor - \left\lfloor \frac{k}{p^r}\right\rfloor - \left\lfloor \frac{n-k}{p^r}\right\rfloor\right).$$

Cada sumando en esta suma es o bien 0 ó 1 y desde luego es 0 para $r > (\log n/\log p)$ (puesto que entonces $\lfloor n/p^r \rfloor = 0$). Así pues $\nu_p \le (\log n/\log p)$, de donde sigue la afirmación.

[18] La definición de $\zeta(s)$ como

$$1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

dada anteriormente tiene sentido sólo cuando s es un número complejo cuya parte real es mayor que 1 (puesto que la serie converge sólo para estos valores de s) y en este dominio $\zeta(s)$ no tiene ceros. Pero la función $\zeta(s)$ puede ser extendida a una función para todos los números complejos s, de manera que tiene sentido hablar de sus raíces en todo el plano complejo. El modo más sencillo de extender la definición de $\zeta(s)$ al menos al semiplano $\mathrm{Re}(s) > 0$ es

complejos cuyas partes reales están entre 0 y 1. Las primeras diez de ellas son como sigue[19]:

$$\varrho_1 = \frac{1}{2} + 14{,}134725\,i \qquad \overline{\varrho}_1 = \frac{1}{2} - 14{,}134725\,i$$
$$\varrho_2 = \frac{1}{2} + 21{,}022040\,i \qquad \overline{\varrho}_2 = \frac{1}{2} - 21{,}022040\,i$$
$$\varrho_3 = \frac{1}{2} + 25{,}010858\,i \qquad \overline{\varrho}_3 = \frac{1}{2} - 25{,}010858\,i$$
$$\varrho_4 = \frac{1}{2} + 30{,}424876\,i \qquad \overline{\varrho}_4 = \frac{1}{2} - 30{,}424876\,i$$
$$\varrho_5 = \frac{1}{2} + 32{,}935062\,i \qquad \overline{\varrho}_5 = \frac{1}{2} - 32{,}935062\,i$$

Es fácil probar que con cada raíz aparece su compleja conjugada. Pero que la parte real de cada raíz sea exactamente $1/2$ no está todavía probado: esta es la famosa hipótesis de Riemann, que tendría importantes consecuencias para la Teoría de Números[20]. Ha sido verificada para 7 millones de raíces.

Con la ayuda de la función de Riemann $R(x)$ introducida antes podemos escribir la fórmula de Riemann en la forma

$$\pi(x) = R(x) - \sum_{\varrho} R(x^{\rho})$$

La k-ésima aproximación a $\pi(x)$ que proporciona esta fórmula es la función

$$R_k(x) = R(x) + T_1(x) + T_2(x) + \cdots + T_k(x),$$

donde $T_n(x) = -R(x^{\varrho_n}) - R(x^{\overline{\varrho}_n})$ es la contribución del n-ésimo par de raíces de la función zeta. Para cada n la función $T_n(x)$ es una función oscilante y suave de x. Las primeras son como sigue[21]:

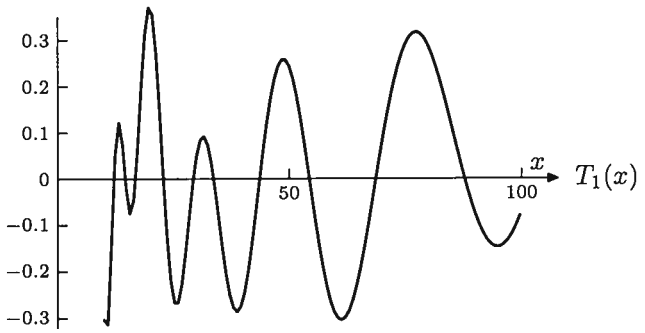

FIGURA 9

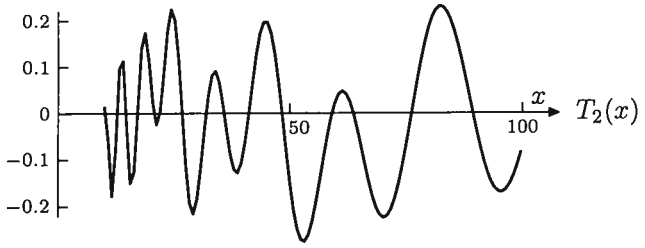

FIGURA 10

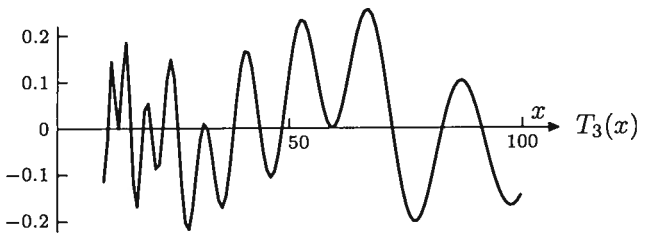

FIGURA 11

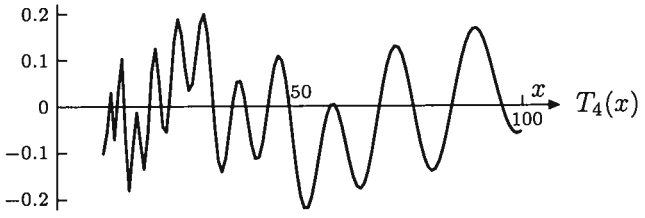

FIGURA 12

Por tanto $R_k(x)$ es también una función suave para cada k. Cuando k crece, estas funciones aproximan a $\pi(x)$. Aquí, por ejemplo, están los gráficos de las aproximaciones décima y veintinueveava,

usar la identidad

$$\Big(1-\frac{2}{2^s}\Big)\zeta(s) = 1+\frac{1}{2^s}+\frac{1}{3^s}+\cdots-2\Big(\frac{1}{2^s}+\frac{1}{4^s}+\cdots\Big) = \sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n^s},$$

que es válido para $\mathrm{Re}(s) > 1$, y observar que la serie de la derecha converge para todo s con parte real positiva. Con esto, las raíces *interesantes* de la función zeta, es decir, las raíces $\varrho = \beta + i\gamma$ con $0 < \beta < 1$, pueden ser caracterizadas en una forma elemental por las dos ecuaciones

$$\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n^{\beta}}\cos(\gamma\log n) = 0, \qquad \sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n^{\beta}}\,\mathrm{sen}(\gamma\log n) = 0$$

La suma sobre las raíces ϱ en la fórmula de Riemann no es absolutamente convergente y por tanto debe ser sumado en un orden conveniente (es decir, de acuerdo con los valores absolutos de $\mathrm{Im}(\varrho)$ crecientes).

Finalmente, debo mencionar que, aunque Riemann afirmó la fórmula para $\pi(x)$ correctamente en 1859, no fue probada hasta 1895 (por Von Mangoldt).

[19]Estas raíces fueron calculadas ya en 1903 por Gram (J. P. Gram, *Sur les zeros de la fonction $\zeta(s)$ de Riemann*, Acta Math., **27**, (1903), 289–304). Para una bonita presentación de la teoría de la función zeta de Riemann, ver H. M. Edwards, *Riemann's zeta function*, Academic Press, New York, 1974.

[20]En particular la hipótesis de Riemann implica (y de hecho es equivalente a la afirmación) que el error de la aproximación de Gauss $\mathrm{Li}(x)$ a $\pi(x)$ es a lo más una constante por $x^{1/2}\log x$. En la actualidad no es ni siquiera conocido si este error es menor que x^c para alguna constante $c < 1$.

[21]Éste y los siguientes gráficos estan tomados de H. Riesel y G. Göhl, *Some calculations related to Riemann's prime number formula*, Math. Comp., **24**, (1970), 969–983.

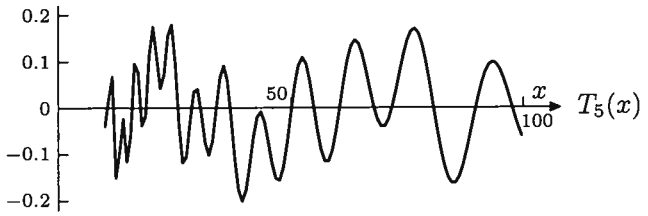

FIGURA 13

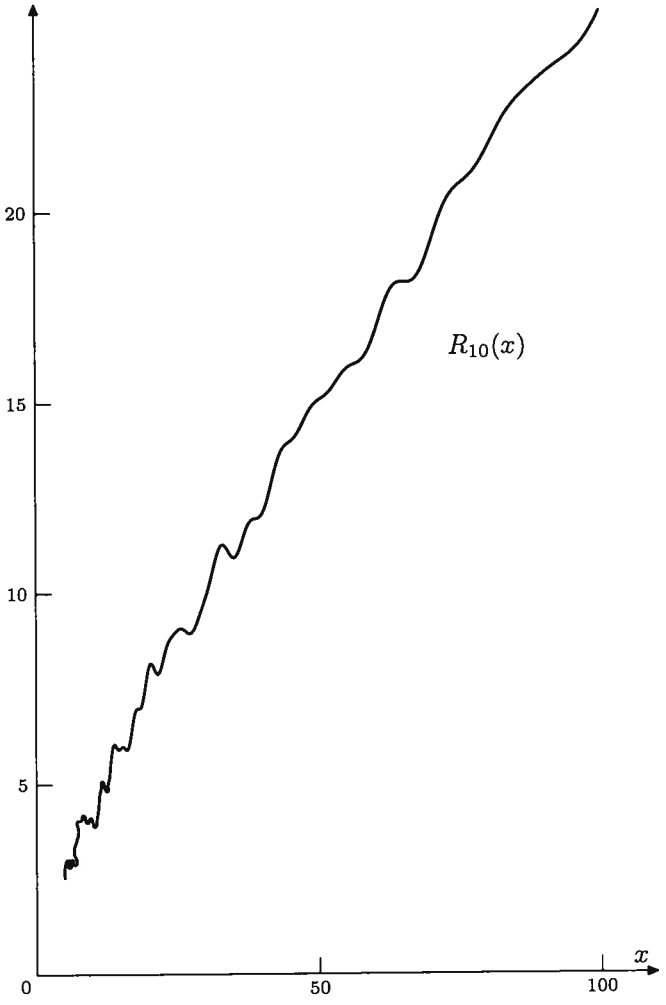

FIGURA 19

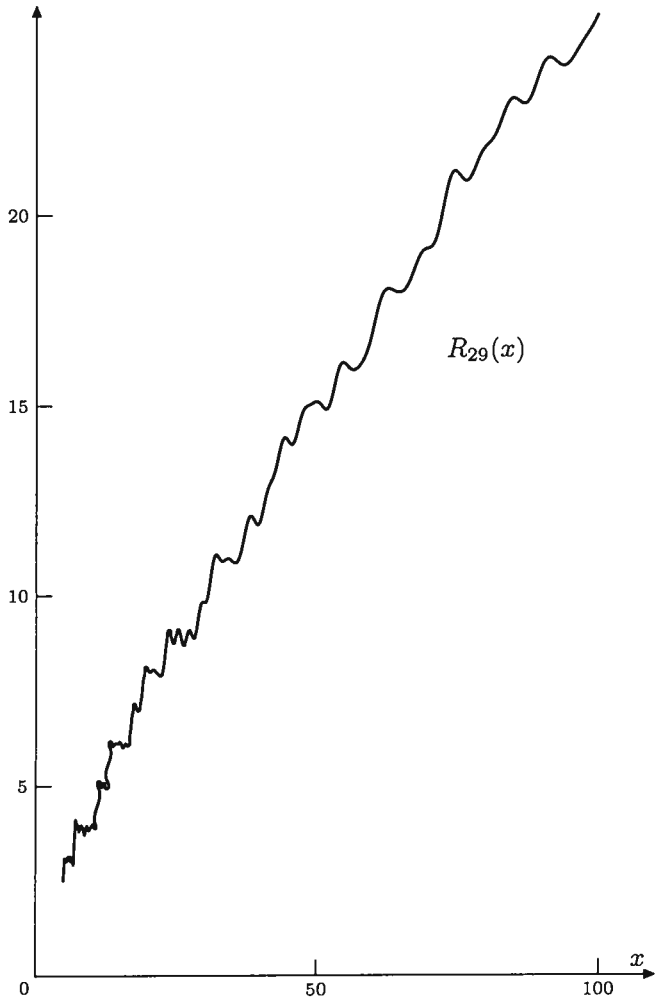

FIGURA 20

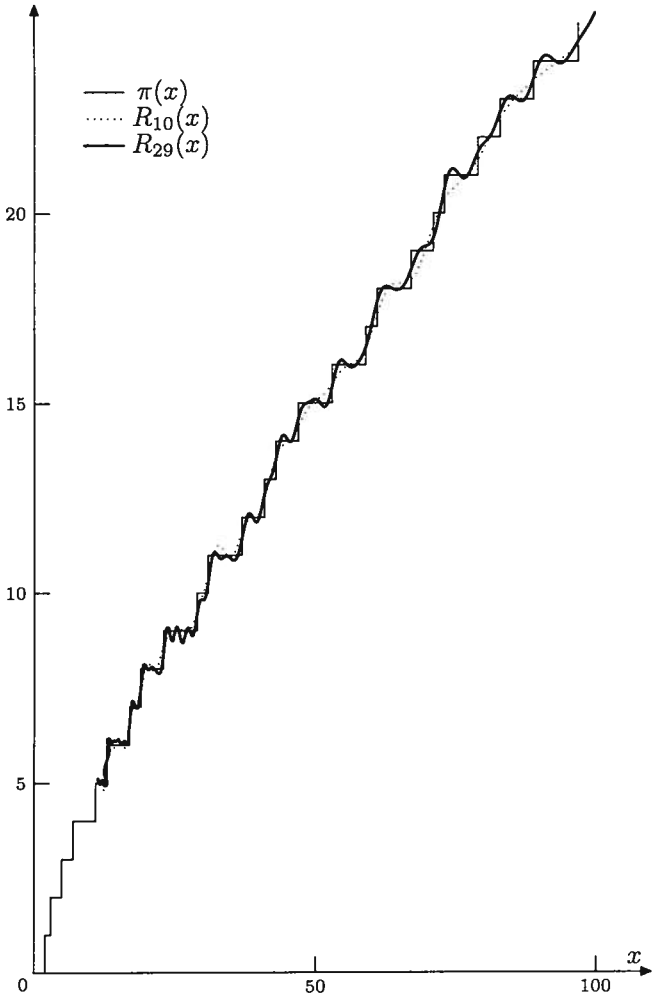

FIGURA 21

si comparamos estas curvas con el gráfico de $\pi(x)$ hasta 100 (p. 9) obtenemos el siguiente gráfico:

Espero que con éste y los otros gráficos que les he mostrado, les haya comunicado una cierta impresión de la inmensa belleza de los números primos y de las infinitas sorpresas que guardan para nosotros.

Traducido por J. Arias de Reyna, febrero 2003.