El diablo de los números

Sección a cargo de

Javier Cilleruelo Mateo

Carreras de números primos

por

Andrew Granville y Greg Martin[1]

No hay nada como un día en las carreras ... La aceleración del pulso cuando suena el pistoletazo de salida, la emoción cuando tu favorito se pone en cabeza (o la angustia si otro va por delante del tuyo) y el temor (o la esperanza) de que el líder pueda cambiar. ¿Y si la carrera es un maratón? Puede que uno de los contendientes sea mucho más rápido que todos los demás, que tome la delantera y marche a la cabeza del grupo durante toda la carrera. O puede que la carrera sea mucho más dramática y que cambie de líder una y otra vez.

Nuestra carrera involucra a los números primos impares, divididos en dos equipos dependiendo del resto que resulta al dividirlos entre 4. En esta carrera módulo[2] 4, el equipo 3 está formado por los primos de la forma $4n+3$, y el equipo 1 por los primos de la forma $4n+1$:

Carrera módulo 4, equipo 3:	3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83 ...
Carrera módulo 4, equipo 1:	5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 93, 97 ...

[1] Andrew Granville, actualmente profesor en la Universidad de Montreal, es una de las mayores autoridades en teoría de números. También destaca por su habilidad para divulgar matemáticas complicadas a grandes audiencias. Su campo de investigación es extenso y variado: teoría analítica de números, computación, análisis armónico, combinatoria, geometría algebraica. Entre sus muchas contribuciones a las matemáticas se encuentra la demostración, junto con Carl Pomerance y William "Red" Alford, de la infinitud de los números de Carmichael.

Greg Martin es profesor en la Universidad de British Columbia. En 2002 fue galardonado por la *Mathematical Association of America* con el premio Lester R. Ford por sus excelentes artículos de divulgación.

Este artículo ha sido escrito para La Gaceta de la Real Sociedad Matemática Española y para el *American Mathematical Monthly*.

[2] Es habitual referirse a los enteros de la progresión aritmética $qn+a$ como "congruentes con $a \pmod q$", y por eso hablamos de la "carrera módulo q".

La carrera módulo 4 sólo cuenta con dos participantes y es una especie de maratón, ¡ya que continúa indefinidamente!

Mirando las listas de arriba, da la impresión de que el equipo 3 va a estar siempre en cabeza; es decir, parece que siempre hay al menos tantos primos de la forma $4n + 3$ como de la forma $4n + 1$.

Otros datos adicionales, que recogemos en la Tabla 1, parecen confirmar nuestras observaciones iniciales.

x	Número de primos $4n + 3$ hasta x	Número de primos $4n + 1$ hasta x
100	13	11
200	24	21
300	32	29
400	40	37
500	50	44
600	57	51
700	65	59
800	71	67
900	79	74
1000	87	80
2000	155	147
3000	218	211
4000	280	269
5000	339	329
6000	399	383
7000	457	442
8000	507	499
9000	562	554
10000	619	609
20000	1136	1125
50000	2583	2549
100000	4808	4783

Tabla 1: El número de primos de la forma $4n + 1$ y $4n + 3$ hasta x.

Incluso en esta tabla más extensa la carrera está muy reñida, aunque el equipo 3 siempre parece mantener una ligera ventaja. Este fenómeno fue observado por primera vez en una carta escrita por Tchébychev a M. Fuss el 23 de marzo de 1853:

> Hay una notable diferencia cuando dividimos los números primos en las dos formas $4n + 3$ y $4n + 1$: la primera de ellas contiene una cantidad mayor que la segunda.

Este sesgo resulta quizás inesperado en vista de un importante resultado en teoría analítica de los números conocido como "el teorema de los números

primos para progresiones aritméticas". Este resultado nos dice que, para todo módulo q, los primos tienden a distribuirse equitativamente entre las diferentes progresiones $qn + a$ tales que[3] $\mathrm{mcd}(a, q) = 1$.

Más concretamente, se sabe que para cualesquiera a y b tales que $\mathrm{mcd}(q, a) = \mathrm{mcd}(q, b) = 1$,

$$\frac{\#\{\text{primos } qn + a \leq x\}}{\#\{\text{primos } qn + b \leq x\}} \longrightarrow 1 \quad \text{cuando } x \to \infty. \tag{1}$$

Este límite no nos ayuda a predecir[4] quién ganará la carrera módulo q. De hecho, este resultado *asintótico* no nos ofrece ninguna información sobre los detalles más finos de estas estimaciones sobre los números primos, y ni verifica ni contradice nuestra observación de que el equipo 3 siempre parece estar por delante del equipo 1.

Llega el momento de ser honestos: hemos hecho una pequeña trampa en la manera de presentar los datos de la tabla anterior. Si nos molestáramos en mirar los primos de los equipos 1 y 3 para *todos* los valores de x, y no sólo para los que aparecen en la tabla, encontraríamos con que en ocasiones se produce un vuelco en la carrera: de vez en cuando el equipo 1 alcanza la cabeza, aunque sólo brevemente. El equipo 1 se pone en cabeza por primera vez en el primo 26861; sin embargo, como 26863 es primo, el equipo 3 empata y recupera el liderato hasta que el equipo 1 consigue ponerse en cabeza otra vez en el 616841 y durante varios números hasta el 633798.

El equipo 3 vuelve entonces a la cabeza hasta que el equipo 1 recupera el liderato en el 12306137 y lo mantiene hasta el 12382326.

Vuelve entonces el equipo 3 a ponerse en cabeza hasta que el equipo 1 se la arrebata en el 951784481 y la mantiene durante varios números más hasta el 952223506.

El equipo 3 lidera a partir de ahí la carrera hasta que el equipo 1 se pone de nuevo por delante en el 6309280697 y mantiene esa posición hasta el 6403150362.

En ese momento, el equipo 3 vuelve a recuperar el mando hasta que el equipo 1 consigue estar en cabeza otra vez en el 18465126217 y durante varios números más hasta el 19033524538.

De nuevo vuelve el equipo 3 al liderato, que mantiene hasta al menos el número 20000000000.

---

[3] Obsérvese que esta restricción es necesaria, ya que todo entero de la forma $qn + a$ es divisible por el máximo común divisor de a y q, y en ese caso, si $\mathrm{mcd}(a, q) > 1$, no puede ser primo excepto a lo más para un valor de n.

[4] Si la fracción $\#\{\text{primos } 4n + 3 \leq x\}/\#\{\text{primos } 4n + 1 \leq x\}$ convergiera a un número mayor que 1 cuando $x \to \infty$, entonces sabríamos que $\#\{\text{primos } 4n+3 \leq x\} > \#\{\text{primos } 4n+1 \leq x\}$ para todo x suficientemente grande y, a la larga, el equipo 3 iría siempre por delante del equipo 1.

Así que parece que, de vez en cuando, hay más primos de la forma $4n+1$ que de la forma $4n+3$, aunque estas ventajas se mantienen sólo brevemente para volver a desaparecer por un largo periodo. Sin embargo, con estos datos, podríamos aventurar que, *de cuando en cuando*, $4n+1$ estará en cabeza a lo largo de esta maratón. Y de hecho éste es el caso:

Teorema 1 **(J.E. Littlewood, 1914)**. *Existen valores de x arbitrariamente grandes para los que hay, hasta x, más primos de la forma $4n+1$ que de la forma $4n+3$. De hecho existen valores de x arbitrariamente grandes para los que*

$$\#\{\textit{primos } 4n+1 \le x\} - \#\{\textit{primos } 4n+3 \le x\} \ge \frac{1}{2}\frac{\sqrt{x}}{\ln x}\ln\ln\ln x\,. \qquad (2)$$

A primera vista, éste parece ser el final de la historia. Sin embargo, al reflexionar sobre cuán poco tiempo consigue el equipo 1 mantenerse en cabeza, cuesta dejar a un lado la sospecha de que el equipo 3 conseguirá estar en cabeza "casi todo el tiempo". Es decir, que a pesar del resultado de Littlewood, "para casi todo x" habrá más primos de la forma $4n+3$ hasta x que de la forma $4n+1$. En 1962, Knapowski y Turán hicieron una conjetura consistente con el resultado de Littlewood, pero que también concuerda con la observación de Tchébychev:

Conjetura 1. *Cuando $X \to \infty$, el porcentaje de enteros $x \le X$ para los que hay más primos, hasta x, de la forma $4n+3$ que de la forma $4n+1$ tiende al 100%.*

Esta conjetura puede ser parafraseada como

Tchébychev estaba en lo cierto "casi todo el tiempo".

Miremos los datos anteriores desde este punto de vista:

X en el rango	Máximo porcentaje de $x \le X$ para el que hay más primos $4n+1 \le x$ que $4n+3$
$0-26860$	0%
$0-500000$	$\approx 0.01\%$
$0-10^7$	$\approx 2.6\%$
10^7-10^8	$\approx 0.6\%$
10^8-10^9	$\approx 0.1\%$
10^9-10^{10}	$\approx 1.6\%$
$10^{10}-10^{11}$	$\approx 2.8\%$

¿Nos convence esto de que la conjetura de Knapowski–Turán es probablemente cierta? ¿Tiende a 0 el porcentaje de la columna derecha cuando x tiende a infinito? Los porcentajes son evidentemente muy bajos, pero con tan pocos

datos no resulta obvio que vayan a tender a 0. Hace unos años apareció un maravilloso artículo de Richard Guy en el *Monthly* titulado "*La ley de los pequeños números*", en el que Guy mostraba varios fenómenos fascinantes que eran "evidentes" para enteros pequeños y que fallaban para enteros más grandes. ¿Podría ser éste uno de esos fenómenos?

Otra carrera de primos: primos de la forma $3n+2$ y $3n+1$

Hay otras carreras de primos, además de la disputada entre primos de la forma $4n+3$ y $4n+1$. Por ejemplo, la carrera módulo 3 tiene lugar entre los primos de la forma $3n+2$ y los primos de la forma $3n+1$. La carrera empieza así:

Carrera módulo 3, equipo 2:	2, 5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, ...
Carrera módulo 3, equipo 1:	7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, ...

En esta carrera, el equipo 2 se pone en cabeza desde un primer momento y no la abandona. Es decir, *parece* que siempre va a haber al menos tantos primos de la forma $3n+2$ hasta x como de la forma $3n+1$. De hecho el equipo 2 permanece en cabeza hasta 10 millones y más, véase[5] la Tabla 2.

Quizás la experiencia con la carrera módulo 4 hará que el lector desconfíe de que el equipo 2 vaya a estar siempre por delante en esta carrera módulo 3. Hará bien el lector en mostrarse escéptico, porque el artículo de Littlewood de 1914 también se puede aplicar a esta carrera: hay infinitos valores de x para los que hay más primos de la forma $3n+1$ hasta x que de la forma $3n+2$ (para esta carrera también es cierta una desigualdad análoga a (2)).

Así que el equipo 1 se pone por delante del equipo 2 infinitas veces. Pero, ¿para qué valor de x ocurre por primera vez? Sabemos que ese número es mayor que diez millones y, de hecho, el equipo 1 se pone en cabeza por primera vez en $x = 608981813029$. Esto fue descubierto el día de Navidad de 1976 por Bays y Hudson. ¡Parece que el equipo 2 domina en esta carrera incluso más de lo que el equipo 3 domina en la carrera módulo 4!

Otra carrera de primos: el último dígito de un primo

Después de oír cosas como que "el equipo 2 mantiene la cabeza durante medio trillón de valores consecutivos de x", uno puede llegar a hartarse del día en las carreras. Así que vayamos con una carrera con más competidores, con la esperanza de que sea más difícil que uno de ellos domine toda la carrera. Una popular carrera entre cuatro es la que disputan los primos que terminan en 1, los que lo hacen en 3, los que acaban en 7 y los que terminan en 9.

[5] El equipo 1 tampoco alcanza la cabeza en los valores intermedios de x no incluidos en la tabla.

x	Equipo 2	Equipo 1
100	13	11
200	24	21
300	33	28
400	40	37
500	49	45
600	58	50
700	65	59
800	71	67
900	79	74
1000	87	80
2000	154	148
3000	222	207
4000	278	271
5000	338	330
6000	398	384
7000	455	444
8000	511	495
9000	564	552
10000	617	611
20000	1137	1124

x	Equipo 2	Equipo 1
30000	1634	1610
40000	2113	2089
50000	2576	2556
60000	3042	3014
70000	3491	3443
80000	3938	3898
90000	4374	4338
100000	4807	4784
200000	8995	8988
300000	13026	12970
400000	16967	16892
500000	20804	20733
600000	24573	24524
700000	28306	28236
800000	32032	31918
900000	35676	35597
1000000	39266	39231
2000000	74520	74412
5000000	174322	174190
10000000	332384	332194

Tabla 2: La columna "Equipo j" contiene el número de primos de la forma $3n + j$ hasta x.

Basándonos en estos pocos datos, parece que los dos equipos de las líneas centrales son los que normalmente están en cabeza. Sin embargo, antes de hacer apuesta alguna, examinemos algún dato más (véase la Tabla 4). Salvo por un breve adelantamiento del equipo 1 al equipo 3 en torno a $x = 500000$, parece que los dos equipos centrales comparten el liderazgo.

Después de observar estas carreras durante un rato, empezamos a tener la sensación de que cada carrera es de algún modo predecible —quizás no en los pequeños detalles, pero sí en un dibujo a gran escala—. Y que si analizáramos una carrera similar (una carrera módulo q para otro valor de q distinto de 4, 3 ó 10), también deberíamos esperar la supremacía de algunos equipos sobre otros. ¿Pero cómo podríamos predecir cuáles son con antelación, sin necesidad de observar la carrera durante un largo tiempo?

Antes de que podamos esperar entender qué equipo mantiene el liderato más a menudo, necesitamos estudiar cómo evolucionan los respectivos recuentos de primos. E incluso antes de intentar entender el número de primos de la forma $qn + a$ (para a y q dados) que hay hasta x, deberíamos empezar por conocer cuántos primos hay hasta x. Quizás es ésta la pregunta de teoría de números más importante del siglo XIX, una pregunta que continuó atrayendo a

Último dígito:	**1**	**3**	**7**	**9**	Último dígito:	**1**	**3**	**7**	**9**
		3	7			101	103	107	109
	11	13	17	19			113		
		23		29				127	
	31		37			131		137	139
	41	43	47						149
		53		59		151		157	
	61		67				163	167	
	71	73		79			173		179
		83		89		181			
			97			191	193	197	199
Hasta 100:	5	7	6	5	Hasta 200:	10	12	12	10

Tabla 3: Las columnas "Último dígito j" contienen los primos de la forma $10n + j$ hasta 100, y entre 100 y 200, respectivamente.

investigadores durante el siglo XX y que aún hoy en día nos oculta celosamente la mayor parte de sus secretos.

¿Qué se sabe acerca del número de primos que son menores o iguales que x?

Aunque los problemas en teoría de números no han estado siempre matemáticamente *en vogue*, en torno a la mitad del siglo XIX el problema de contar primos había llamado la atención de matemáticos tan respetables como Legendre, Tchébychev y el prodigioso Gauss. Aunque los resultados más rigurosos de este tiempo se debieron a Tchébychev, sería la predicción de Gauss la que iba a llevar a un mejor entendimiento de las carreras de números primos.

Cuando le preguntaron acerca de la frecuencia con la que los primos aparecían, ofreció la siguiente respuesta:

> "Cuando era un niño reflexioné sobre esta cuestión y determiné que, alrededor de x, los primos aparecen con densidad $1/\ln x$."
>
> — C. F. Gauss (24 de Diciembre de 1849), carta a Encke.

Esta observación de Gauss puede ser interpretada como la predicción de que

$$\#\{\text{primos} \leq x\} \approx \sum_{n=2}^{[x]} \frac{1}{\ln n} \approx \int_2^x \frac{dt}{\ln t} = \mathrm{Li}(x)\,.$$

x	Último dígito:	**1**	**3**	**7**	**9**
100		5	7	6	5
200		10	12	12	10
500		22	24	24	23
1000		40	42	46	38
2000		73	78	77	73
5000		163	172	169	163
10000		306	310	308	303
20000		563	569	569	559
50000		1274	1290	1288	1279
100000		2387	2402	2411	2390
200000		4478	4517	4503	4484
500000		10386	10382	10403	10365
1000000		19617	19665	19621	19593

Tabla 4: La columna "Último dígito j" contiene el número de primos de la forma $10n + j$ hasta x.

Comparemos la predicción de Gauss[6] con los recuentos más recientes de números primos hasta x. (Llamaremos "Exceso" a la cantidad $\mathrm{Li}(x) - \pi(x)$, redondeada al entero más cercano, que es la diferencia entre la predicción de Gauss $\mathrm{Li}(x)$ y la función $\pi(x)$, el verdadero número de primos hasta x.)

Podemos hacer varias observaciones a partir de estos excesos: obsérvese primero que la anchura de la última columna es siempre aproximadamente la mitad del ancho de la columna del medio. En otras palabras, el exceso parece ser siempre aproximadamente como la raíz cuadrada del término principal $\pi(x)$. El término de error también parece ser siempre positivo, así que podríamos aventurar que

$$0 < \mathrm{Li}(x) - \pi(x) < \sqrt{\pi(x)}$$

para todo x. De hecho, el exceso parece ser monótonamente creciente, lo que sugiere que deberíamos ser capaces de aproximar mejor $\pi(x)$ restando al término principal $\mathrm{Li}(x)$ algún término secundario de comportamiento suave, una cuestión a la que volveremos más tarde. Pero, por ahora, volvamos a las carreras ...

La función $\mathrm{Li}(x)$ no cuenta primos, pero sí que parece estar cerca de $\pi(x)$, y un poco por delante. Así que, para la carrera entre $\mathrm{Li}(x)$ y $\pi(x)$, podemos preguntarnos si $\mathrm{Li}(x)$ mantendrá *siempre* la cabeza. El asombroso resultado de Littlewood también se aplica aquí:

[6] De hecho, Euler hizo una "predicción" similar aunque menos conocida algunos años ante que Gauss.

x	$\pi(x) = \#\{\text{primos} \leq x\}$	Exceso: $\text{Li}(x) - \pi(x)$
10^8	5761455	753
10^9	50847534	1700
10^{10}	455052511	3103
10^{11}	4118054813	11587
10^{12}	37607912018	38262
10^{13}	346065536839	108970
10^{14}	3204941750802	314889
10^{15}	29844570422669	1052618
10^{16}	279238341033925	3214631
10^{17}	2623557157654233	7956588
10^{18}	24739954287740860	21949554
10^{19}	234057667276344607	99877774
10^{20}	2220819602560918840	222744643
10^{21}	21127269486018731928	597394253
10^{22}	201467286689315906290	1932355207

Tabla 5: Primos hasta varios x, y el exceso en la predicción de Gauss.

Teorema 2 **(Littlewood, 1914)**. *Existen valores de x arbitrariamente grandes para los que $\pi(x) > Li(x)$, es decir, para los que*

$$\#\{\text{primos} \leq x\} > \int_2^x \frac{dt}{\ln t}.$$

Así que, ¿cuál es el x_1 más pequeño para el que $\pi(x_1) > \text{Li}(x_1)$? Skewes obtuvo, a partir de la demostración de Littlewood, una cota superior para x_1, aunque en verdad no muy manejable. En concreto, probó que

$$\text{Skewes (1933):} \qquad x_1 < 10^{10^{10^{10^{34}}}},$$

y para obtenerla necesitó asumir una hipótesis muy significativa: la "Hipótesis de Riemann", una conjetura que discutiremos más tarde. Durante mucho tiempo, este "número de Skewes" fue conocido como el mayor número con un significado matemático "interesante". Skewes dio más tarde una cota superior que no dependía de ningún resultado todavía no demostrado. A cambio, la cota era todavía más monstruosa. Desde entonces se han obtenido diversas mejoras:

$$\begin{aligned}
\text{Skewes (1955):} &\qquad x_1 < 10^{10^{10^{10^{1000}}}} \\
\text{Lehman (1966):} &\qquad x_1 < 2 \times 10^{1165} \\
\text{te Riele (1987):} &\qquad x_1 < 6.658 \times 10^{370} \\
\text{Bays and Hudson (1999):} &\qquad x_1 < 1.3982 \times 10^{316}
\end{aligned}$$

Como discutiremos más tarde, Bays y Hudson dieron sólidas razones para creer que en realidad x_1 es algún entero cercano a 1.3982×10^{316}. ¡Es una afirmación extraordinaria! Con la tecnología y los algoritmos de los que ahora disponemos (y no son previsibles mejoras significativas), sólo podemos contar primos hasta cerca de $x = 10^{22}$. Entonces, ¿cómo pueden predecir que el valor de x_1 será tan enorme cuando esta predicción está tan lejos del punto donde es posible computar $\pi(x)$ directamente?

Explicaremos esto más tarde. Aunque ya podríamos pensar que si el primer número x para el que $\pi(x)$ está por encima de $\mathrm{Li}(x)$ es tan gigantesco, entonces seguramente los números x para los que $\pi(x) > \mathrm{Li}(x)$ son incluso más escasos que los correspondientes números "perdedores" en las carreras que hemos examinado anteriormente.

Estimando con precisión el número de primos

Hasta la mitad del siglo XIX, los intentos de estimar $\pi(x)$ el número de primos $\leq x$ eran relativamente directos, y estaban basados en teoría elemental de números y en principios combinatorios, o en la teoría de las formas cuadráticas. Sin embargo, en 1859, el gran geómetra Riemann afrontó el reto de contar los primos de una manera muy diferente. Sólo escribió un artículo que pueda ser considerado de teoría de números, pero esa única corta memoria tendría un impacto que ha perdurado cerca de siglo y medio, y sus ideas ayudarían a definir el área que ahora llamamos teoría analítica de números.

La memoria de Riemann describía un sorprendente enfoque del problema, que usaba la teoría del análisis complejo (que por entonces era aún un área en desarrollo[7]). El nuevo enfoque propuesto por Riemann parecía alejarse del contexto original del problema. Sin embargo, tenía dos características fundamentales:

- era potencialmente un camino práctico para resolver el problema de una vez por todas;
- permitía hacer predicciones muy similares, aunque no idénticas, a las de Gauss. De hecho, como veremos más tarde, sugería un término secundario para compensar de algún modo el exceso que vimos anteriormente.

El método de Riemann es demasiado complicado como para ser descrito aquí en su totalidad, pero rescataremos de él lo necesario para entender mejor la función $\pi(x)$. Para empezar, consideremos la predicción principal de la memoria de Riemann, que reescribimos en un lenguaje completamente elemental:

$$\mathrm{mcm}[1, 2, 3, \ldots, x] \approx e^x \quad \text{cuando } x \to \infty.$$

[7]De hecho, la memoria de Riemann sobre este problema de teoría de números fue un factor decisivo en el desarrollo de la teoría de funciones analíticas, principalmente en sus aspectos globales.

Ahora, uno puede verificar fácilmente que

$$\left(\prod_{p\leq x} p\right) \times \left(\prod_{p^2\leq x} p\right) \times \left(\prod_{p^3\leq x} p\right) \times \cdots = \text{mcm}[1, 2, 3, \ldots, x],$$

puesto que la potencia de cualquier primo p que divida al entero en cada lado de la ecuación es precisamente la potencia más grande de p menor o igual que x.

Combinando esta identidad con la estimación anterior y tomando logaritmos naturales en ambos lados, obtenemos que

$$\left(\sum_{p\leq x} \ln p\right) + \left(\sum_{p^2\leq x} \ln p\right) + \left(\sum_{p^3\leq x} \ln p\right) + \cdots \approx x \text{ cuando } x \to \infty.$$

Observe el lector que los primos en la primera suma son precisamente los primos contados en $\pi(x)$, los primos en la segunda suma son los contados en $\pi(x^{1/2})$, y así sucesivamente. Una técnica llamada sumación por partes (análoga a la integración por partes que usaríamos para ocuparnos de un factor $\ln x$ en un integrando) nos permite sustituir el factor $\ln p$ por el factor 1. Cuando se aplica la sumación parcial a la aproximación anterior, el resultado es

$$\pi(x) + \tfrac{1}{2}\pi(x^{1/2}) + \tfrac{1}{3}\pi(x^{1/3}) + \cdots \approx \int_2^x \frac{dt}{\ln t} = \text{Li}(x).$$

Si "despejamos" $\pi(x)$ de la manera apropiada, encontramos la forma equivalente

$$\pi(x) \approx \text{Li}(x) - \frac{1}{2}\,\text{Li}(x^{1/2}) + \cdots$$

Así que el método de Riemann nos lleva a una predicción como la de Gauss, pero con un ingrediente extra; a saber, predice un término secundario que podríamos esperar compensara la desviación que observábamos en la predicción de Gauss. Revisemos los datos y veamos cómo se ajusta la predicción de Riemann. Véase la Tabla 6 (la "desviación de Riemann" se refiere a $\text{Li}(x) - \frac{1}{2}\text{Li}(\sqrt{x}) - \pi(x)$, mientras que la "desviación de Gauss" se refiere a $\text{Li}(x) - \pi(x)$, como antes):

La predicción de Riemann parece ser un poco mejor que la de Gauss, aunque no mucho más. Sin embargo, el que el error en la predicción de Riemann tome valores positivos y negativos sugiere que, quizás, esté cerca de lo mejor que se pueda conseguir.

x	$\#\{\text{primos} \leq x\}$	Desviación de Gauss	Desviación de Riemann
10^8	5761455	753	131
10^9	50847534	1700	−15
10^{10}	455052511	3103	−1711
10^{11}	4118054813	11587	−2097
10^{12}	37607912018	38262	−1050
10^{13}	346065536839	108970	−4944
10^{14}	3204941750802	314889	−17569
10^{15}	29844570422669	1052618	76456
10^{16}	279238341033925	3214631	333527
10^{17}	2623557157654233	7956588	−585236
10^{18}	24739954287740860	21949554	−3475062
10^{19}	234057667276344607	99877774	23937697
10^{20}	2220819602560918840	222744643	−4783163
10^{21}	21127269486018731928	597394253	−86210244
10^{22}	201467286689315906290	1932355207	−126677992

Tabla 6: Primos hasta varios valores de x y las desviaciones en las predicciones de Gauss y Riemann.

Volviendo a la principal predicción de la memoria de Riemann, podemos calcular algunos datos para comprobar su precisión:

x	Entero más cercano a $\ln(\text{mcm}[1, 2, 3, \ldots, x])$	diferencia
100	94	−6
1000	997	−3
10000	10013	13
100000	100052	52
1000000	999587	−413

La predicción de Riemann se ha ido precisando con los años, y ahora se puede expresar de manera explícita como

$$\left| \ln(\text{mcm}[1, 2, \cdots, x]) - x \right| \leq 2\sqrt{x} \ln^2 x \quad \text{para todo } x \geq 100.$$

De hecho, esta desigualdad es equivalente[8] a la famosa *Hipótesis de Riemann*, quizás el problema sin resolver de mayor relevancia en las matemáticas. La Hipótesis de Riemann es una afirmación, propuesta por Riemann en su memoria y aún sin demostrar, acerca de los ceros de una cierta función del análisis complejo que está estrechamente relacionada con la distribución de los primos. Para intentar ilustrar cómo Riemann conectó estas dos áreas aparentemente

[8] Al igual que la desigualdad $|\pi(x) - \text{Li}(x)| \leq \sqrt{x} \ln x$ para todo $x \geq 3$.

tan lejanas, la teoría de los números y el análisis complejo, necesitamos hablar primero acerca de la manera de escribir funciones como combinaciones de "ondas".

Haciendo la ola[9]

Probablemente se haya preguntado qué tienen que ver las "ondas de radio" y las "ondas de sonido" con las ondas que aparecen, por ejemplo, en las gráficas de las funciones seno y coseno. Habitualmente, los sonidos no parecen ser muy "ondulantes", sino más bien quebrados: se detienen, vuelven a comenzar, cambian abruptamente ... Entonces, ¿cuál es la relación? La idea es que todos los sonidos se pueden convertir en una suma de ondas. Por ejemplo, imaginemos que nuestro "sonido" es simplemente la línea ascendente

$$y = x - \frac{1}{2},$$

considerada sobre el intervalo $0 \leq x \leq 1$, que aparece en el primer gráfico de la Figura 1.

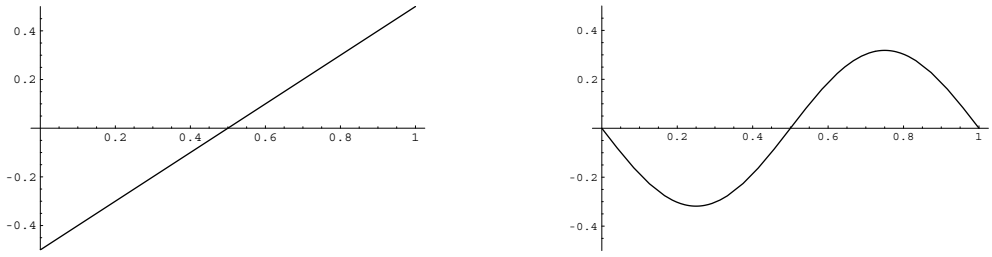

Figura 1: La línea $y = x - \frac{1}{2}$ y la onda $y = -\frac{1}{\pi}\operatorname{sen} 2\pi x$.

Si tratamos de aproximar la gráfica de la izquierda con una "onda", lo podemos hacer bien en el medio de la línea usando la función

$$y = -\frac{1}{\pi}\operatorname{sen} 2\pi x.$$

Sin embargo, como se ve en el segundo gráfico de la Figura 1, la aproximación es bastante mala cuando $x < 1/4$ ó cuando $x > 3/4$.

¿Cómo podemos mejorar esta aproximación? La idea consiste en "sumar" una segunda onda a la primera: una segunda onda que recorra dos ciclos completos sobre el intervalo $0 \leq x \leq 1$, en lugar de uno sólo. Esto corresponde

[9] *N. de T.*: las palabras ola y onda tienen la misma traducción en inglés.

a oír el sonido de dos ondas al mismo tiempo, superpuestas; matemáticamente, sumamos literalmente las dos funciones. El resultado de sumar la función

$$y = -\frac{1}{2\pi}\,\mathrm{sen}\,4\pi x$$

es que se produce una mejor aproximación para un rango de valores de x algo más grande que el que obtuvimos con una sola onda, como se ve en la Figura 2.

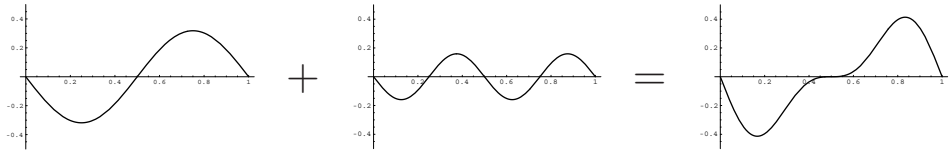

Figura 2: Suma de la onda $y = -\frac{1}{2\pi}\,\mathrm{sen}\,4\pi x$ y la onda $y = -\frac{1}{\pi}\,\mathrm{sen}\,2\pi x$

Podríamos continuar de esta manera, sumando más y más ondas que recorran 3, 4 ó 5 ciclos completos en el intervalo, y conseguiríamos aproximaciones cada vez mejores a la línea recta original. La aproximación que se obtiene utilizando cien ondas superpuestas es realmente buena, excepto[10] cerca de los extremos 0 y 1, como se aprecia en la Figura 3.

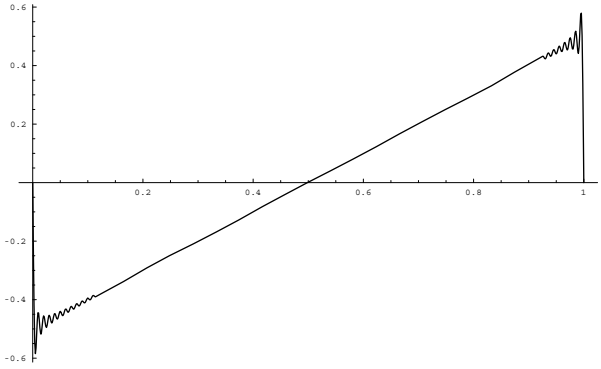

Figura 3: La suma de cien ondas cuidadosamente elegidas

[10] El que las sumas finitas de ondas no se aproximen bien a la función original en lugares poco "ondulados", como son los extremos o los puntos de discontinuidad, es un persistente problema del análisis de Fourier conocido como el "fenómeno de Gibbs".

Si fuéramos observando cómo se van construyendo estas sucesivas aproximaciones, añadiendo una nueva onda cada vez, enseguida estaríamos dispuestos a apostar que cuantas más ondas permitiéramos, mejor aproximación tendríamos, y que llegaríamos quizás a obtener tanta precisión como deseáramos. Si permitiéramos un pequeño error en la aproximación (y cerráramos los ojos a lo que sucede muy cerca de los extremos), podríamos de hecho construir una aproximación lo bastante buena utilizando un número suficiente de ondas. Sin embargo, para construir una copia "perfecta" de la línea recta original necesitamos usar infinitas ondas seno. Más precisamente, las que aparecen en el lado derecho de la fórmula

$$x - \frac{1}{2} = -2\sum_{n=1}^{\infty} \frac{\operatorname{sen}(2\pi n x)}{2\pi n},$$

que se puede demostrar cierta para todo $0 < x < 1$. (Podemos descubrir, en los términos $n = 1$ y $n = 2$ de esta suma, las dos ondas que hemos elegido para las Figuras 1 y 2.) Esta fórmula no es de uso práctico, ya que realmente no podemos transmitir infinitas ondas a la vez ... ¡pero es una fórmula magnífica a pesar de todo!

En general, para toda función $f(x)$ definida sobre el intervalo $0 < x < 1$ que no sea "demasiado irregular", podemos encontrar números a_n y b_n tales que $f(x)$ puede ser escrita como suma de funciones trigonométricas, es decir

$$f(x) = a_0 + \sum_{n=1}^{\infty} \big(a_n \cos(2\pi n x) + b_n \operatorname{sen}(2\pi n x)\big).$$

Esta fórmula, y la manera de calcular los coeficientes a_n y b_n, es una de las principales identidades del "Análisis de Fourier", que junto a sus muchas generalizaciones son el área de las matemáticas conocida como análisis armónico. En términos de ondas, los números $2\pi n$ son las "frecuencias" de las ondas (que controlan lo rápido que recorren sus ciclos), mientras los coeficientes a_n y b_n son sus "amplitudes" (que controlan lo alto y lo bajo que llegan).

La revolucionaria fórmula de Riemann

La idea de Riemann puede ser parafraseada, de manera simple aunque algo sorprendente, en los siguientes términos:

Intenta contar los primos como suma de ondas.

La fórmula precisa que él propuso es algo técnica para este artículo, pero podemos captar su esencia a partir de la siguiente aproximación cuando x es grande. Esta fórmula, aunque nadie duda de que es correcta, no ha sido

probada todavía:

$$\frac{\#\{\text{primos} \le x\} - \displaystyle\int_2^x \frac{dt}{\ln t}}{\dfrac{\sqrt{x}}{\ln x}} \approx -1 - 2 \sum_{\substack{\text{los números reales } \gamma>0 \\ \text{tales que } \frac{1}{2}+i\gamma \\ \text{es un cero de } \zeta(s)}} \frac{\operatorname{sen}(\gamma \ln x)}{\gamma} \qquad (3)$$

El numerador de la parte izquierda de esta fórmula es el término de error cuando se compara la predicción de Gauss $\mathrm{Li}(x)$ con $\pi(x)$, el número de primos menores o iguales que x. Vimos anteriormente que las desviaciones parecían ser aproximadamente del tamaño de la raíz cuadrada de x, así que el denominador $\sqrt{x}/\ln x$ parece apropiado para estar dividiendo dicha cantidad. El lado derecho de la fórmula tiene mucho en común con nuestra fórmula para $x-1/2$. Es una suma de funciones seno, en la que los números γ son usados de dos maneras diferentes en el lugar de $2\pi n$: cada γ se usa dentro del seno (como la "frecuencia") y el inverso de cada γ es el coeficiente del seno (como la "amplitud"). Incluso se tiene el mismo factor 2 en cada fórmula. Sin embargo, los números γ que aquí aparecen son mucho más sutiles que los números $2\pi n$ en la fórmula correspondiente para $x - 1/2$.

La *función zeta de Riemann* $\zeta(s)$ se define como

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

Aquí, s es un número complejo, que escribiremos como $s = \sigma + it$ cuando queramos referirnos a sus partes real e imaginaria σ y t de manera separada. Si s es un número real, sabemos de los primeros cursos de cálculo que la serie que define $\zeta(s)$ converge si y sólo si $s > 1$; es decir, podemos sumar la serie infinita y obtener un valor finito y único. De manera similar, se puede demostrar que la serie converge sólo para números complejos s tales que $\sigma > 1$. Pero, ¿qué ocurre cuando $\sigma \le 1$? ¿Cómo sortearemos el hecho de que la serie no se puede sumar (es decir, no converge)?

Afortunadamente, existe un fenómeno maravillosos en la teoría de funciones de una variable compleja llamado "continuación analítica". Nos dice que las funciones que originalmente están definidas sólo para ciertos números complejos tienen una única definición "adecuada" para otros números complejos. En este caso, la definición de $\zeta(s)$ dada anteriormente sólo tiene sentido cuando $\sigma > 1$, pero la "continuación analítica" nos permite definir $\zeta(s)$ para todo número complejo s distinto de $s = 1$ (véase [25] para más detalles).

Esta descripción del proceso de continuación analítica parece mágico, a la vez que desconcertante. Por suerte, hay una manera bastante explícita de demostrar cómo $\zeta(\sigma + it)$ puede definirse "adecuadamente", al menos para la

región $\sigma > 0$. Empecemos con la expresión $(1-2^{1-s})\zeta(s)$ y efectuemos algunos juegos de manos con ella:

$$\begin{aligned}\left(1-2^{1-s}\right)\zeta(s) &= \left(1-\frac{2}{2^s}\right)\zeta(s) = \zeta(s) - \frac{2}{2^s}\,\zeta(s)\\ &= \sum_{n\geq 1}\frac{1}{n^s} - 2\sum_{m\geq 1}\frac{1}{(2m)^s}\\ &= \sum_{n\geq 1}\frac{1}{n^s} - 2\sum_{\substack{n\geq 1\\ n \text{ par}}}\frac{1}{n^s} = \sum_{\substack{m\geq 1\\ m \text{ impar}}}\frac{1}{m^s} - \sum_{\substack{n\geq 1\\ n \text{ par}}}\frac{1}{n^s}\\ &= \left(\frac{1}{1^s}-\frac{1}{2^s}\right)+\left(\frac{1}{3^s}-\frac{1}{4^s}\right)+\left(\frac{1}{5^s}-\frac{1}{6^s}\right)+\cdots\end{aligned}$$

Despejando $\zeta(s)$, tenemos que

$$\zeta(s) = \frac{1}{(1-2^{1-s})}\left\{\left(\frac{1}{1^s}-\frac{1}{2^s}\right)+\left(\frac{1}{3^s}-\frac{1}{4^s}\right)+\left(\frac{1}{5^s}-\frac{1}{6^s}\right)+\cdots\right\}.$$

Todas estas manipulaciones son válidas para números complejos $s = \sigma+it$ con $\sigma > 1$. Sin embargo ocurre que la serie entre paréntesis también converge para $\sigma > 0$. Entonces podemos tomar esta última ecuación como la nueva definición "adecuada" de la función zeta de Riemann sobre este nuevo dominio, más grande que el inicial. Obsérvese que el factor $1/(1-2^{1-s})$ no está definido en el número especial $s = 1$; la función zeta de Riemann tiene un problema intrínseco aquí que no puede ser evitado con ningún reordenamiento inteligente de la serie.

La fórmula de Riemann (3) depende de los ceros de la continuación analítica de $\zeta(s)$. Los ceros más fáciles de identificar son los enteros pares negativos; es decir

$$\zeta(-2) = 0,\ \zeta(-4) = 0,\ \zeta(-6) = 0,\ \ldots,$$

que son los llamados "ceros triviales" de la función zeta. Se puede demostrar que cualquier otro cero complejo $\sigma+it$ de $\zeta(s)$ (esto es, que satisfacen $\zeta(\sigma+it) = 0$) debe cumplir que $0 \leq \sigma \leq 1$; estos misteriosos ceros de la función zeta son los llamados "ceros no triviales".

Después de algunos cálculos, Riemann observó que todos los ceros no triviales de la función zeta parecían caer sobre la línea $\mathrm{Re}(s) = 1/2$. En otras palabras, formuló su famosa hipótesis:

> Si $\sigma+it$ es un número complejo con $0 \leq \sigma \leq 1$ y $\zeta(\sigma+it) = 0$, entonces $\sigma = \frac{1}{2}$.

Esta afirmación, que nadie ha conseguido probar todavía, es la famosa *Hipótesis de Riemann*.

Si la Hipótesis de Riemann fuera cierta, entonces podríamos escribir todos los ceros no triviales de la función zeta de la forma $\rho = 1/2 + i\gamma$ (junto con sus conjugados $1/2 - i\gamma$), donde γ es un número real positivo. Éstos son los misteriosos números γ que aparecen en la fórmula (3), la cual es cierta si y sólo si la Hipótesis de Riemann es cierta. Existe una fórmula similar en el caso de que la Hipótesis de Riemann fuera falsa, pero es bastante complicada y técnicamente mucho menos agradable. La razón es que, en ese caso, los coeficientes $1/\gamma$, que son constantes en (3), serían reemplazados por funciones de x. Sería preferible que la Hipótesis de Riemann fuera cierta porque proporciona una fórmula (3) más sencilla ... y porque la tal fórmula es una delicia. Es más, la fórmula (3) se parece tanto a las fórmulas de las ondas del sonido, que hay quien afirma que (3) nos revela que "*los primos tienen la música dentro de sí*".

Podemos preguntarnos cómo sumar la suma infinita en (3). Es sencillo: sume según el orden de los valores ascendentes de γ y la suma convergerá.

Gente muy capaz ha calculado miles de millones de ceros de $\zeta(s)$, y todos los ceros simples que han obtenido han caído directamente sobre la línea $\sigma = 1/2$. Por ejemplo, los ceros no triviales más cercanos al eje real[11] son $s = 1/2 + i\gamma_1$ y $s = 1/2 - i\gamma_1$, donde $\gamma_1 \approx 14.1347\ldots$. Se cree que los números positivos γ que aparecen en los ceros no triviales son más o menos como números aleatorios, en el sentido de que ninguno de ellos está relacionado con otros por ecuaciones lineales simples con coeficientes enteros (o incluso ecuaciones polinómicas con coeficientes algebraicos). Sin embargo, como todo lo que sabemos hacer son aproximaciones numéricas de estos ceros no triviales con una precisión determinada, no podemos decir mucho sobre la naturaleza precisa de los números γ.

La carrera de primos $\pi(x)$ versus $\mathrm{Li}(x)$

Entonces, ¿cómo usar esta variación con Análisis de Fourier para localizar el x más pequeño para el que

$$\#\{\text{primos} \le x\} > \int_2^x \frac{dt}{\ln t} \ ?$$

La idea es aproximar

$$\frac{\#\{\text{primos} \le x\} - \displaystyle\int_2^x \frac{dt}{\ln t}}{\sqrt{x}/\ln x}$$

usando la fórmula (3). De la misma manera que con la línea $x - 1/2$, aquí también esperamos obtener una buena aproximación simplemente sumando la fórmula del lado derecho de (3) sobre los primeros ceros de $\zeta(s)$ (esto es, los cien, o los mil, o el millón de valores γ más pequeños con $\zeta(1/2 + i\gamma) = 0$,

[11] Ya que $\zeta(1/2 + i\gamma) = 0$ si y sólo si $\zeta(1/2 - i\gamma) = 0$.

dependiendo del nivel de precisión que queramos). En otras palabras, aproximamos

$$\frac{\#\{\text{primos} \leq x\} - \displaystyle\int_2^x \frac{dt}{\ln t}}{\sqrt{x}/\ln x} \approx -1 - 2 \sum_{\substack{\frac{1}{2}+i\gamma \text{ es un cero de } \zeta(s) \\ 0<\gamma<T}} \frac{\operatorname{sen}(\gamma \ln x)}{\gamma}$$

eligiendo T de manera que se incluyan los ceros que deseemos. En la Figura 4 mostramos la gráfica de la función[12] $(\mathrm{Li}(x) - \pi(x))/(\frac{1}{2}\mathrm{Li}(\sqrt{x}))$ cuando x varía entre 10^4 y 10^8, junto con tres gráficas de aproximaciones utilizando los primeros 10, 100 y 1000 valores de γ, respectivamente. Vemos que las aproximaciones mejoran cuantos más ceros consideremos.

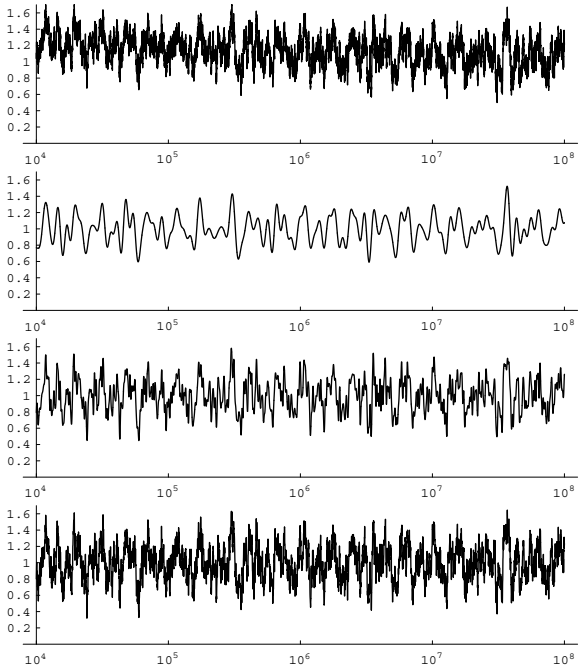

Figura 4: Una gráfica de $(\mathrm{Li}(x) - \pi(x))/(\frac{1}{2}\mathrm{Li}(\sqrt{x}))$, seguida por las aproximaciones usando 10, 100 y 1000 ceros de $\zeta(s)$.

[12] Cuando x es grande, $\frac{1}{2}\mathrm{Li}(\sqrt{x}) \approx \sqrt{x}/\log(x)$. Hemos preferido utilizar la segunda expresión por ser funciones más familiares. Sin embargo, al tratar con los "pequeños" valores de x como los de estas gráficas, usar la función $\frac{1}{2}\mathrm{Li}(x)$ permite mostrar más claramente las similitudes que queremos resaltar.

Fueron cálculos de este tipo los que llevaron a Bays y Hudson a conjeturar que la primera vez en que $\pi(x)$ supera a $\mathrm{Li}(x)$ ocurre aproximadamente en 1.398×10^{316}.

La carrera módulo 4

En 1959, Shanks sugirió estudiar la carrera módulo 4 dibujando un histograma de los valores de la función

$$\frac{\#\{\text{primos } 4n+3 \leq x\} - \#\{\text{primos } 4n+1 \leq x\}}{\sqrt{x}/\ln x}. \tag{4}$$

En la Figura 5 se muestra dicho histograma para mil valores $x = 1000, 2000, 3000, \ldots, 10^6$.

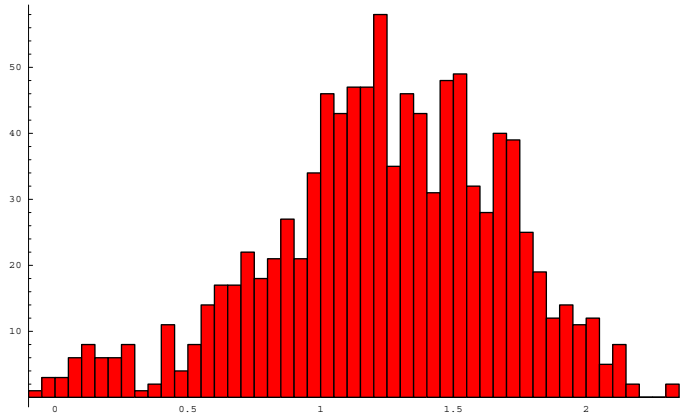

Figura 5: Un histograma para los valores de (4) en $x = 1000k,\ 1 \leq k \leq 1000$

Un histograma de lo más sugerente: uno podría intuir que si incorporáramos más y más valores, entonces el histograma se parecería más y más a una curva acampanada centrada en 1. El resultado de Littlewood (2) implica que la cola tiende a ∞ cuantos más valores se usan, dado que el cociente en la ecuación (4) será al menos tan grande como $\ln\ln\ln x$ para infinitos valores[13] de x. El que el rango del histograma anterior sea infinito no resulta evidente a partir de la figura anterior, pero esto no es tan sorprendente, puesto que

"$\ln\ln\ln x$ *tiende a infinito con gran dignidad.*" —Dan Shanks, 1959

[13]De hecho, Littlewood también demostró la desigualdad con los términos de la izquierda intercambiados, así que el histograma tiende a $-\infty$ también.

En (3) vimos cómo la diferencia entre $\pi(x)$ y $\mathrm{Li}(x)$ podía aproximarse por una suma de ondas cuyas frecuencias y amplitudes dependían de los ceros de la función zeta de Riemann. Para contar los primos hasta x de la forma $4n+1$, o de la forma $4n+3$, o de la forma $qn+a$ con $\mathrm{mcd}(a,q)=1$, hay una fórmula análoga a (3) que depende de los ceros de las *funciones L de Dirichlet*, parientes de la función zeta de Riemann, que también tienen unas definiciónes naturales aunque ligeramente más complicadas. Por ejemplo, la función L de Dirichlet asociada a la carrera entre primos de la forma $4n+3$ y $4n+1$ es

$$L(s) = \frac{1}{1^s} - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \dots.$$

Obsérvese que ésta (y cualquier otra función L de Dirichlet) converge para todo $s = \sigma + it$ con $\sigma > 0$. Existe una linda fórmula, análoga a (3), para el número de primos hasta x de la forma $qn+a$. Esta fórmula es cierta si y sólo si todos los ceros de estas funciones L de Dirichlet que están en la banda $0 \le \mathrm{Re}(s) \le 1$ satisfacen $\mathrm{Re}(s) = 1/2$. Esta afirmación es conocida como la *Hipótesis Generalizada de Riemann*. Por ejemplo, si esta hipótesis fuera cierta para la función $L(s)$ definida antes, tendríamos la fórmula

$$\frac{\#\{\text{primos } 4n+3 \le x\} - \#\{\text{primos } 4n+1 \le x\}}{\sqrt{x}/\ln x} \approx$$
$$\approx 1 - 2 \sum_{\substack{\text{Números reales } \gamma > 0 \text{ tales que} \\ \frac{1}{2}+i\gamma \text{ es un cero de } L(s)}} \frac{\mathrm{sen}(\gamma \ln x)}{\gamma}.$$

En consecuencia, podríamos tratar de estudiar la carrera módulo 4 calculando el lado derecho de esta fórmula, truncándolo para involucrar sólo cien, mil, o un millón de ceros de $L(s)$. He aquí una gráfica que muestra lo bien que se ajusta a los datos reales la aproximación con 1000 ceros.

Las tres primeras veces en las que el equipo 1 se pone en cabeza (véanse al principio del artículo los valores exactos) son claramente visibles en ambas gráficas. Un aspecto muy conveniente de esta aproximación es que no se vuelve mucho más difícil cuando x se hace muy grande, algo que sí ocurre cuando uno intenta contar exactamente el número de primos hasta x.

En 1999, Bays y Hudson utilizaron estas aproximaciones para predecir más "cambios de signo" en (4) para x hasta 10^{1000}. Los dos siguientes que predijeron fueron $\approx 1.4898\times10^{12}$ que fue encontrado en 1488478427089, y $\approx 9.3190\times10^{12}$.

¿De dónde vienen estos sesgos?

Hemos analizado varios ejemplos de carreras de primos y descubierto los sesgos que ciertas progresiones aritméticas parecen tener respecto a otras. Aunque ya hemos visto que estas desviaciones pueden calcularse a través de fórmulas

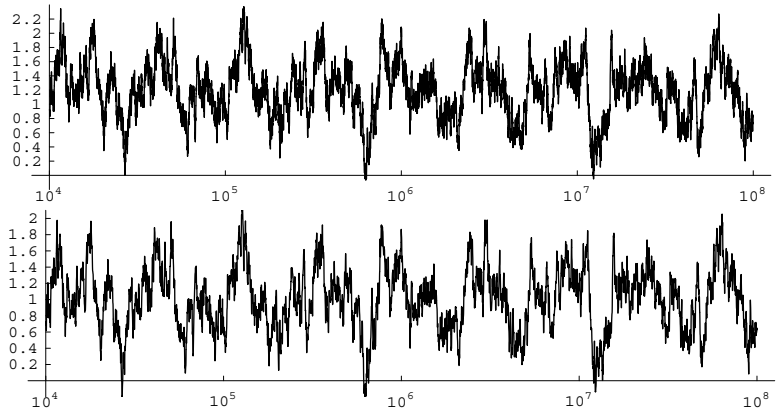

Figura 6: Gráfica de la función de (4) y aproximación con 1000 ceros de $L(s)$.

complicadas como (3), no es fácil entender, ni tampoco tener intuición alguna sobre cómo podríamos predecir, sin necesidad de llevar a cabo enormes cálculos, cuál de dos progresiones dadas domina habitualmente a la otra. Así que vamos a resumir lo visto hasta ahora en las diversas carreras de primos, para buscar un patrón que nos permita encontrar alguna manera sencilla de hacer tales predicciones. Hemos descubierto que parecía haber, al menos la mayor parte del tiempo,

> más primos de la forma $4n+3$ que de la forma $4n+1$;
> más primos de la forma $3n+2$ que de la forma $3n+1$;
> más primos de la forma $10n+3$ y $10n+7$ que $10n+1$ y $10n+9$.

¿Capta el lector algún patrón? Es posible que no sean todavía datos suficientes como para hacer una buena predicción. Pero comprobemos una carrera más de primos, la que disputan los de la forma $8n+1$, $8n+3$, $8n+5$ y $8n+7$:

Es una carrera algo extraña, porque el único patrón claro que podemos detectar es que parece haber

> más primos de la forma $8n+3$, $8n+5$, y $8n+7$ que de la forma $8n+1$

(esto es cierto para todos los x entre 23 y 10^6). Pero esta "rareza" debería ayudar a cualquier estudiante de teoría de números, que sabe bien que los cuadrados impares[14] son de la forma $8n+1$, a predecir un patrón.

Durante nuestra discusión sobre el mcm$[1,2,\ldots,n]$ y su relación con $\pi(x)$, la función que cuenta los primos hasta x, vimos que la predicción de Riemann

[14] Obsérvese que $(2m-1)^2 = 8\binom{m}{2}+1 \equiv 1 \pmod 8$ para todos los enteros impares $2m-1$.

x	$8n+1$	$8n+3$	$8n+5$	$8n+7$
1000	37	44	43	43
2000	68	77	79	78
5000	161	168	168	171
10000	295	311	314	308
20000	556	571	569	565
50000	1257	1295	1292	1288
100000	2384	2409	2399	2399
200000	4466	4495	4511	4511
500000	10334	10418	10397	10388
1 millón	19552	19653	19623	19669

Tabla 7: Número de primos $8n+j$ para $j = 1, 3, 5, 7$ hasta varios valores de x.

$\pi(x) + \#\{\text{primos } p \text{ con } p^2 \leq x\}/2$ es la que mejor se aproxima por $\int_2^x \frac{dt}{\ln t}$, así que son los cuadrados de los primos los "responsables" de que $\mathrm{Li}(x)$ supere a $\pi(x)$ la mayor parte del tiempo.

Estas evidencias[15] apuntan a que los cuadrados de los primos desempeñan un importante papel en tales desviaciones. Comprobemos las progresiones aritméticas a las que pertenecen los cuadrados de los primos para los módulos anteriores:

para todo primo p que no divide a 4, p^2 es de la forma $4n+1$;
para todo primo p que no divide a 3, p^2 es de la forma $3n+1$;
para todo primo p que no divide a 10, p^2 es de la forma $10n+1$ ó $10n+9$;
para todo primo p que no divide a 8, p^2 es de la forma $8n+1$.

Así todo el tiempo. Parece que normalmente $qn+a$ tiene menos primos que $qn+b$ si a es un cuadrado módulo q y b no.

¿Qué fenómeno es el que realmente estamos observando?

Hemos observado "insistentes" sesgos en favor de una progresión aritmética sobre otra, es decir, un líder "habitual" en las carreras entre números primos. Hasta ahora, sin embargo, no hemos exhibido una descripción precisa de esta desviación ni hemos definido un número que mida cuán grande es. En una sección anterior salió a relucir la conjetura de Knapowski y Turán de 1962: si elegimos "al azar" un número x muy grande, entonces es "casi seguro" que habrá más primos $4n+3 \leq x$ que $4n+1 \leq x$ (obviamente, esta conjetura se puede generalizar a otras carreras de primos). Sin embargo, las evidencias en este sentido que ofrecían nuestros datos no eran del todo convincentes.

[15] Admitimos que evidencias algo circunstanciales.

En realidad, estudiando la fórmula explícita (3), Kaczorowski (1993) y Sarnak (1994) demostraron, de manera independiente, que la conjetura de Knapowski–Turán era falsa.

De hecho, la cantidad

$$\frac{1}{X}\#\{x \leq X;\ \text{hasta } x,\ \text{hay más primos } 4n+3 \text{ que } 4n+1\}$$

no tiende a ningún límite cuando $X \to \infty$, sino que fluctúa. Un estado del arte no muy satisfactorio, aunque pudiera ocurrir que no fuéramos capaces de decir nada más al respecto: pudiera ser que los fenómenos que hemos observado fueran ciertos sólo para "números pequeños"[16] y que, yéndonos muy lejos, la carrera no tuviera sesgos en favor de progresión alguna.

Aunque resulta que no es éste el caso. En 1994, Rubinstein y Sarnak hicieron una observación muy acertada. Después de determinar que ninguna progresión domina a otra en un porcentaje fijo del tiempo[17], y que por tanto esta línea de pensamiento parecía cerrada, Rubinstein y Sarnak se dijeron que quizás la manera *obvia* de contar carreras de primos no es necesariamente la *correcta*, al menos en este contexto. Observaron que si se cuenta de manera un poco diferente (en términos técnicos, "si se utiliza una medida diferente"), entonces se consigue una respuesta mucho más satisfactoria. Más aún, se obtiene un panorama completo de resultados que explican de manera natural todos los fenómenos observados.

En Matemáticas, ocurre en ocasiones que es la observación más simple, y no la técnica pura y dura, la clave para desbloquear un misterio; y desde luego éste fue el caso en este problema. La idea básica de Rubinstein y Sarnak fue contar $1/x$, en lugar de 1, por cada $x \leq X$ para el que hubiera más primos de la forma $4n+3$ hasta x que de la forma $4n+1$. Por supuesto, la suma total $\sum_{x \leq X} 1/x$ no es X, sino aproximadamente $\ln X$, así que necesitamos utilizar la escala correspondiente. Al hacerlo, se obtiene un notable resultado:

Teorema 3 **(Rubinstein y Sarnak, 1994)**.

$$\frac{1}{\ln X} \sum_{\substack{x \leq X:\ \text{hay más primos} \\ 4n+3 \text{ que } 4n+1 \text{ hasta } x}} \frac{1}{x} \longrightarrow 0.9959\ldots \qquad \textit{cuando } X \to \infty.$$

En otras palabras, con la medida adecuada, ¡Tchébychev estaba en lo cierto el 99.59% del tiempo! Además, su idea se puede aplicar a las otras carreras de primos que hemos estudiado. Por ejemplo, en la carrera módulo 3,

$$\frac{1}{\ln X} \sum_{\substack{x \leq X:\ \text{hay más primos} \\ 3n+2 \text{ que } 3n+1 \text{ hasta } x}} \frac{1}{x} \longrightarrow 0.9990\ldots \qquad \text{cuando } X \to \infty,$$

[16] "Pequeños" en una escala apropiada.

[17] Esto es, que la conjetura de 1962 de Knapowski y Turán es falsa.

así que el equipo 1 tiene aproximadamente una posibilidad entre mil de estar por delante del equipo 3 en un tiempo dado, si se mide "estar por delante" de esta manera.

¿Y qué ocurre para la carrera entre $\pi(x)$ y $\mathrm{Li}(x)$? Hay que recordar que no esperamos encontrar un contraejemplo hasta que no lleguemos al inmenso valor $x \approx 1.3982 \times 10^{316}$. En este caso, Rubinstein y Sarnak demostraron que

$$\frac{1}{\ln X} \sum_{x \leq X \,:\, \pi(x) < \mathrm{Li}(x)} \frac{1}{x} \;\longrightarrow\; 0.99999973\ldots \text{ cuando } X \to \infty.$$

Esto es, de nuevo con la medida apropiada, ¡$\pi(x) < \mathrm{Li}(x)$ cerca del 99.999973% del tiempo! No sorprende que el primer punto donde $\pi(x) > \mathrm{Li}(x)$ esté tan sumamente lejos.

Esta exitosa vara de medir se denomina la *medida logarítmica* (por el "factor de normalización" $\ln X$). Aparece en muchos contextos en matemáticas, y fue incluso usado por Winter en 1941 en un contexto relacionado, pero nunca de manera tan estimulante y transparente como por Rubinstein y Sarnak.

Sus magníficos resultados se han demostrado asumiendo hipótesis muy plausibles. Por una parte, aceptan la Hipótesis Generalizada de Riemann (en otras palabras, que maravillosas fórmulas análogas a (3) pueden ser usadas para contar primos de la forma $qn + a$ hasta x), y por otra asumen que los números γ que aparecen en estas fórmulas —las partes imaginarias de los ceros de funciones L de Dirichlet— son de hecho linealmente independientes sobre los números racionales. Sería realmente impactante que alguna de estas dos hipótesis fuera falsa, aunque parece improbable que alguna de ellas pueda ser demostrada en un futuro próximo.

¿Cómo demostrar estos resultados?

Las demostraciones de los resultados mencionados arriba, y las de los discutidos en las secciones siguientes, son por supuesto demasiado técnicas como para ser descritas en su totalidad aquí. Sin embargo, todas ellas dependen de un análisis cuidadoso de la fórmula (3) y sus análogos para las carreras módulo q. Asumir la Hipótesis Generalizada de Riemann asegura, para empezar, que en todos los casos considerados existe una fórmula del tipo (3). Para analizar su valor, necesitamos considerar la suma del lado derecho de (3) y, en particular, los valores de los diversos términos y cómo interactúan entre ellos: cada término $-2\,\mathrm{sen}(\gamma \ln x)/\gamma$ es una onda sinusoidal que oscila regularmente[18] entre -2γ y 2γ. Como ya vimos cuando estudiamos cómo estas ondas podían combinarse para dar aproximaciones a una línea recta, si los valores de γ se

[18] "Regularmente" si consideramos a $\ln x$ como la variable, en lugar de a x. De hecho, ésta es realmente la razón por la que la "medida logarítmica" es la más apropiada para nuestros recuentos de números primos.

pudieran elegir de manera que las ondulaciones individuales se sincronizaran, entonces la suma podría dar lugar a formas sorprendentes. Esto nos lleva a la segunda hipótesis: si asumimos que las ondas no pueden combinarse de ciertas maneras poco comunes, entonces el valor de la suma debería mantenerse pequeño y sin sorpresas. En otras palabras, esperaríamos que una buena parte de los términos fueran positivos y otra buena parte negativos, y que hubiera una cancelación significativa. Esto es lo que se logra asumiendo que los números γ sean linealmente independientes sobre los números racionales. Bajo esta segunda hipótesis, los valores de los términos $\operatorname{sen}(\gamma \ln x)$ no pueden estar bien sincronizados para muchos valores de x, y entonces podemos probar resultados. De hecho, nos encontramos con que son los valores γ más pequeños los que tienen mayor influencia sobre el valor de la suma (lo que tampoco resulta sorprendente, puesto que el término correspondiente a γ tiene un factor γ en el denominador).

Calcular los valores numéricos precisos de la frecuencia con la que un equipo está por delante de otro es todavía más delicado. Ya no basta argumentar que la suma es "grande" o "pequeña"; necesitamos saber exactamente la frecuencia con la que la suma en (3) es más grande que $-\frac{1}{2}$ o menos que $-\frac{1}{2}$, ya que es en este valor en el que el lado derecho pasa de ser positivo a negativo. Pues resulta que es posible calcular exactamente la frecuencia con la que esto ocurre si usamos el análisis de Fourier (tradicional): reescribimos la suma de las ondas en (3), cuyas frecuencias dependen de los ceros de la función zeta de Riemann, como una suma de "ondas de Fourier" donde las frecuencias dependen de los números $2\pi n$. Aunque es demasiado complicado dar una fórmula cerrada, uno puede, con astutas técnicas computacionales, aproximar sus valores numéricos con gran precisión.

Cuadrados y no cuadrados: el método de Littlewood

Ya hemos comentado en varias ocasiones las consecuencias del artículo[19] de Littlewood de 1914. El método es lo suficientemente poderoso como para probar algunos resultados bastante generales, pero no en particular los que se refieren a una progresión contra otra. Para un primo q, definamos como equipo S al conjunto de los primos que son congruentes con un cuadrado módulo q, y sea el equipo N el formado por el resto de primos. Usando el método de Littlewood se puede demostrar que ambos equipos están en cabeza infinitas veces[20], y la ventaja hasta x llega a ser tan grande como $c\sqrt{x}\ln\ln\ln x/(\ln x)$ para alguna constante $c > 0$ que depende sólo de q. Un ejemplo de esta situación lo constituye la carrera módulo $q = 5$, donde S contiene los primos cuyos últimos dígitos son 1 y 9 (y también 5); así que estamos, de nuevo, con la carrera

[19] Que en realidad sólo analiza la carrera de $\pi(x)$ *versus* $\operatorname{Li}(x)$.

[20] En otras palabras, existen x e y arbitrariamente grandes tales que hay más primos en S que en N hasta x; y tales que hay más primos en N que en S hasta y.

módulo 10. Recuérdese que, según las tablas de datos de que disponíamos, el equipo N mantenía habitualmente la cabeza.

Hay otras carreras más complicadas que pueden ser analizadas utilizando el método de Littlewood. Estas carreras involucran siempre una partición de los primos en dos clases de, aparentemente, el mismo tamaño. Para q impar, el conjunto S está formado por aquellos primos p para los que

$$\#\{\ell \text{ primo} : \ \ell \text{ divide a } q \text{ y } p \text{ no es congruente a un cuadrado módulo } \ell\}$$

es par. Para q par, la estructura de S es similar pero más complicada.

Más resultados de Rubinstein y Sarnak (1994)

En una carrera de números primos entre dos progresiones aritméticas módulo q, ¿cuándo vemos un sesgo y cuándo no? ¿Está cada progresión aritmética "en cabeza" exactamente el 50% del tiempo (en la medida logarítmica) o no?

O quizás más importante: ¿podemos decidir esto sin necesidad de hacer cálculos complicados? Antes vimos que "habitualmente" parecía haber más primos hasta x de la forma $qn + b$ que de la forma $qn + a$, si es que a es un cuadrado módulo q y b no lo es. En realidad, bajo las dos hipótesis mencionadas anteriormente, Rubinstein y Sarnak demostraron que eso es cierto: la medida logarítmica del conjunto de los x para los que hay más primos de la forma $qn + b$ hasta x que de la forma $qn + a$ es estrictamente más grande que $1/2$, aunque siempre menor que 1. En otras palabras, todo no cuadrado está por delante de cualquier cuadrado más de la mitad del tiempo, aunque no el 100% del tiempo.

Nos podemos hacer la misma pregunta cuando a y b son ambos cuadrados módulo q, o bien cuando ninguno de los dos lo es. En este caso, y bajo las mismas hipótesis, Rubinstein y Sarnak demostraron que $\#\{\text{primos } qn + a \leq x\} > \#\{\text{primos } qn + b \leq x\}$ ocurre exactamente la mitad del tiempo. De hecho demostraron bastante más. Para describir sus resultados, necesitamos definir ciertos términos de error relacionados con estas estimaciones de números primos y describir qué queremos decir por sus "distribuciones límite". Como comentamos anteriormente, los valores de la función cuenta-primos $\#\{\text{primos } qn + a \leq x\}$ son aproximadamente iguales cuando recorremos los valores de a (hasta q) que no tienen factores comunes con q. De hecho, vimos que el cociente de dos cualesquiera de ellos tendía a 1 cuando $x \to \infty$. Esto implica que

$$\frac{\#\{\text{primos } qn + a \leq x\}}{\pi(x)/\phi(q)} \to 1 \qquad \text{cuando } x \to \infty,$$

donde $\pi(x) = \#\{\text{primos} \leq x\}$ y $\phi(q)$ es el número de enteros positivos a hasta q tales que $\text{mcd}(a, q) = 1$. Como ya hemos visto que es natural analizar

la diferencia entre estas cantidades dividiendo por $\sqrt{x}/\ln x$, definamos

$$\mathrm{Error}(x;q,a) = \frac{\#\{\text{primos } qn+a \le x\} - \pi(x)/\phi(q)}{\sqrt{x}/\ln x}.$$

Rubinstein y Sarnak sugirieron que, para estudiar adecuadamente carreras de primos entre progresiones aritméticas a módulo q y b módulo q, se debería mirar la distribución de los valores de los pares ordenados

$$\big(\mathrm{Error}(x;q,a), \mathrm{Error}(x;q,b)\big)$$

cuando x varía, definiendo esta distribución otra vez con respecto a la medida logarítmica. Más concretamente, dados unos números reales $\alpha < \beta$ y $\alpha' < \beta'$, deberíamos preguntarnos por la frecuencia con la que $\alpha \le \mathrm{Error}(x;q,a) \le \beta$ y $\alpha' \le \mathrm{Error}(x;q,b) \le \beta'$. Esta frecuencia se define mediante el límite de las integrales

$$\lim_{Y\to\infty} \frac{1}{\ln Y} \int\limits_{\substack{0\le y\le Y,\\ \mathrm{Error}(y;q,a)\in[\alpha,\beta] \text{ y } \mathrm{Error}(y;q,b)\in[\alpha',\beta']}} \frac{1}{y}\,dy$$

(un límite que ellos probaron que existía). Rubinstein y Sarnak demostraron que si a y b son ambos cuadrados módulo q (o si ninguno de ellos lo es), entonces esta distribución es simétrica, esto es

$$\alpha \le \mathrm{Error}(x;q,a) \le \beta \quad \text{y} \quad \alpha' \le \mathrm{Error}(x;q,b) \le \beta'$$

ocurre con la misma frecuencia que

$$\alpha' \le \mathrm{Error}(x;q,a) \le \beta' \quad \text{y} \quad \alpha \le \mathrm{Error}(x;q,b) \le \beta.$$

En otras palabras, que no hay señal alguna de sesgo: las progresiones aritméticas a módulo q y b módulo q son intercambiables en el límite.

El estudio fue mucho más general. Por ejemplo, se preguntaron acerca de las veinticuatro posibles ordenaciones de las cuatro funciones cuenta-primos siguientes:

$$\#\{\text{primos } 8n+1 \le x\}, \quad \#\{\text{primos } 8n+3 \le x\},$$
$$\#\{\text{primos } 8n+5 \le x\}, \quad \#\{\text{primos } 8n+7 \le x\}.$$

Rubinstein y Sarnak demostraron que cada ordenación ocurre para infinitos valores de x; de hecho, cada una de ellas ocurre con probabilidad positiva (en la medida logarítmica). Esto se puede generalizar a cualquier módulo q y a tantas progresiones aritméticas $a_1, \dots a_r \pmod q$ como queramos. Es decir, se puede estudiar la distribución de

$$(\mathrm{Error}(x;q,a_1), \mathrm{Error}(x;q,a_2), \dots, \mathrm{Error}(x;q,a_r)).$$

Aceptando sólo la Hipótesis Generalizada de Riemann, demostraron que la función de distribución[21] existe para este vector de términos de error. Asumiendo también la independencia lineal de los γ sobre los números racionales, demostraron que para cualesquiera números $a_1, \dots a_r$ distintos módulo q, ninguno de los cuales tiene factores en común con q, la ordenación

$$\#\{\text{primos } qn+a_1 \le x\} < \#\{\text{primos } qn+a_2 \le x\} < \cdots < \#\{\text{primos } qn+a_r \le x\}$$

ocurre para una proporción positiva (con la medida logarítmica) de valores de x. También demostraron que, para cualquier r fijo, estas proporciones se acercan de manera creciente a $1/r!$ conforme q va creciendo. Parece extremadamente improbable que esta proporción sea exactamente $1/r!$, pero no podemos probar si es así o no, excepto en la siguiente situación especial.

Antes vimos que la función de distribución es simétrica cuando tenemos una carrera de dos progresiones y ambas son cuadrados (o ambas no cuadrados) módulo q. Sorprendentemente, Rubinstein y Sarnak demostraron que existe sólo otra situación en la que la función de distribución es simétrica, no importa cómo intercambiemos unas variables con las otras, a saber, las carreras entre tres progresiones aritméticas de la forma

$$a \pmod q, \qquad a\omega \pmod q \quad \text{y} \quad a\omega^2 \pmod q\,,$$

donde $\omega^3 \equiv 1$ módulo q pero $\omega \not\equiv 1$ módulo q.

Sin embargo, el resultado de Rubinstein y Sarnak acerca de que la función de distribución no es habitualmente simétrica deja aún abierta la posibilidad de que cada ordenación en una carrera ocurra con la misma frecuencia[22].

Vimos antes el histograma de Shanks de los valores de $\text{Error}(x;4,3) - \text{Error}(x;4,1)$ para varios valores de x, y predijimos que "el histograma se parecería más y más a la curva de una campana centrada en 1" cuando considerásemos más valores. Una consecuencia quizás sorprendente del trabajo de Rubenstein y Sarnak es que esto no es lo que ocurre: la correspondiente función de distribución no es tan sencilla y elegante como la clásica campana de Gauss.

¿Qué investigación se está haciendo ahora?

Después del gran (y, al mismo tiempo, bastante sorprendente) resultado de Littlewood de 1914, se produjo un receso en la investigación en "la teoría comparativa de primos" hasta los cincuenta y los sesenta. En esos años, las ideas de Littlewood se generalizaron en diversas direcciones, algunas sugeridas directamente por el trabajo de Littlewood, y también por los valiosos cálculos de Shanks, Hudson y otros. En los noventa parecía que la mayor parte de

[21] Definida por un cierto límite de integrales, análogo al que vimos una pocas líneas atrás.
[22] Ya que, por ejemplo, una función puede ser positiva la mitad del tiempo sin ser simétrica.

lo que se podía hacer en este área ya había sido hecho (y que no quedaba mucho por hacer), aunque Kaczorowski seguía por entonces probando algunos resultados nuevos.

En 1993, Giuliana Davidoff dictó un curso de últimos años de licenciatura sobre teoría analítica de números en el Mount Holyoke College. Al encontrarse con muchos alumnos especialmente interesados, la profesora Davidoff decidió organizar un divertido "*Research Experience for Undergraduates*" (REU), que se ocuparía de investigar las carreras de números primos[23]. Junto con los estudiantes Caroline Osowsky, Yi Wang, Jennifer vanden Eyden y Nancy Wrinkle, realizaron importantes cálculos y demostraron varios resultados que aparecen en el primer apéndice de este artículo.

Por casualidad, Davidoff coincidió con Sarnak en las vacaciones de verano. Ella le describió su proyecto REU y la manera en que estaban desarrollando el enfoque computacional de Stark de estas cuestiones. Sarnak escribe[24]:

> Yo no estaba familiarizado con este asunto de la desviación de Chebyshev y llegó a fascinarme. En particular estaba [. . .] muy interesado en asignar un número explícito a la probabilidad de que $\pi(x)$ superase a $\mathrm{Li}(x)$.

Sarnak continúa:

> Cuando regresé a Princeton *chateé* con Fernando[25] sobre esto y empecé a trabajar en ello [. . .] Estaba claro que había que calcular muchos ceros.

Sarnak había discutido anteriormente con un brillante estudiante de licenciatura, Mike Rubinstein, en torno a otras cuestiones sobre la distribución de los números primos.

> Mike, que estaba buscando un tema para su tesina, se interesó mucho mucho por el asunto, y pasado un tiempo él y yo colaboramos en el problema, lo que condujo a nuestro artículo.

Fue una tesina extraordinaria, que llegó a convertirse en uno de los artículos más influyentes en la teoría analítica de números reciente. Rubinstein terminaría su tesis[26] y se ha convertido en uno de los investigadores líderes en el mundo en los cálculos relativos a los diferentes tipos y aspectos de las funciones zeta.

Un poco después, el segundo autor de este artículo leyó el artículo de Rubinstein y Sarnak y se interesó por la determinación de las "probabilidades"

[23] Bajo el más formal título de "*Topics in comparative number theory*".

[24] En un correo electrónico al primer autor de este artículo.

[25] Fernando Rodríguez-Villegas, ahora en la Universidad de Texas en Austin, pero entonces en Princeton haciendo un *postdoc*, que tenía mucha experiencia computacional.

[26] Michael Rubinstein es en la actualidad profesor de la Universidad de Waterloo.

para algunas de las carreras de primos a tres que no contemplaba el trabajo Rubinstein y Sarnak: por ejemplo, la carrera entre los tres contendientes

$$\#\{\text{primos } 8n+3 \le x\},\ \ \#\{\text{primos } 8n+5 \le x\} \text{ y } \#\{\text{primos } 8n+7 \le x\};$$

obsérvese que ninguna de estas progresiones aritméticas contiene cuadrados.

Junto con su colega Andrey Feuerverger, por entonces en la Universidad de Toronto[27], creó una técnica para determinar las frecuencias de las diferentes ordenaciones entre los participantes en una carrera de números primos con más de dos contendientes. De manera inesperada, descubrieron que cada una de las seis ordenaciones de los tres contendientes en la carrera de antes no ocurre necesariamente la sexta parte del tiempo. De hecho,

$$\#\{\text{primos } 8n+3 \le x\} > \#\{\text{primos } 8n+5 \le x\} > \#\{\text{primos } 8n+7 \le x\}$$

ocurre para aproximadamente el 19.2801% de los enteros x (en la medida logarítmica), mientras que

$$\#\{\text{primos } 8n+5 \le x\} > \#\{\text{primos } 8n+3 \le x\} > \#\{\text{primos } 8n+7 \le x\}$$

ocurre para aproximadamente el 14.0772% de los enteros x.

Algo muy extraño, porque, en la carrera entre primos de la forma $8n+3$ y de la forma $8n+5$, ambos están por delante la mitad del tiempo, aunque si *sólo* miramos a valores de x para los que estos dos tipos de primos están por delante de los primos $8n+7$, ¡entonces los primos $8n+3$ están por delante con más frecuencia que los primos $8n+5$!

Más carreras esotéricas

Se conocen resultados que dan fórmulas asintóticas para el número de primos con ciertas propiedades. Por ejemplo, ¿cuándo 2 es un cubo módulo un primo p? Es sencillo comprobar que así ocurre para todos los primos de la forma $3n+2$, así que nos centraremos en otros tipos de primos. Se sabe que, asintóticamente, es también cierto para la tercera parte de los primos de la forma $3n+1$. Por tanto, nos podemos preguntar si, habitualmente, un poco más (o un poco menos) de la tercera parte de los primos $p = 3n+1$ tienen la propiedad de que 2 es un cubo módulo p. En su reciente tesis doctoral en la Universidad de British Columbia, Nathan Ng[28] se dio cuenta de que esta pregunta se podía contestar usando técnicas similares a las de Rubenstein y Sarnak, puesto que el recuento de estos primos depende, de una manera análoga, de los ceros de un nuevo tipo de función L. De hecho, Ng observó que

[27] Donde estaba disfrutando de una estancia postdoctoral, antes de irse a la Universidad de British Columbia.

[28] Nathan Ng es en la actualidad profesor de la Universidad de Ottawa.

estos resultados se pueden generalizar a muchos casos en los que disponemos de fórmula asintótica para un conjunto de primos que pueden ser descritos mediante la teoría de Galois[29].

En su trabajo, Ng dio el siguiente lindo ejemplo. Series de potencias como

$$q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n}) = \sum_{n=1}^{\infty} a_n q^n$$

aparecen frecuentemente en geométrica aritmética; son ejemplos de *formas modulares*, que tienen todo tipo de propiedades aparentemente milagrosas (véase el libro de Serre [22]). Uno de esos milagros es que, para todo primo p, el valor de a_p es $2, 0$ ó -1, y que las proporciones de cada uno son $1/6$, $1/2$ y $1/3$ respectivamente. Bajo las hipótesis adecuadas, Ng demostró que, en la medida logarítmica, que $2\#\{p \le x, a_p = 0\} > 6\#\{p \le x, a_p = 2\}$ para $\approx 98.30\%$ de los valores de x, que $2\#\{p \le x, a_p = 0\} > 3\#\{p \le x, a_p = -1\}$ para $\approx 72.46\%$ de los valores de x, y que $3\#\{p \le x, a_p = -1\} > 6\#\{p \le x, a_p = 2\}$ para $\approx 95.70\%$ de los valores de x.

Parejas de primos

El primer autor se involucró en este asunto tras una invitación para participar en el congreso de la MAA en Montgomery, Alabama, en 2001, que le proporcionó una buena excusa para leer acerca de este fascinante tema. Una posterior discusión con estudiantes le condujo a la idea de crear en 2001-2002 un grupo de investigación VIGRE[30] en la Universidad de Georgia para investigar cuestiones sobre carreras de primos gemelos.

Para todo número par d, se cree que existen infinitos números enteros n para los que n y $n+d$ son primos. Cuando $d = 2$, es la famosa *Conjetura de los Primos Gemelos*. Por el momento no sabemos demostrar si hay infinitas "parejas de primos" $(n, n+d)$ para ningún valor de d. A pesar de esto, podemos predecir cuántos debería haber hasta x. Por ejemplo, para potencias de dos, se cree que

$$\frac{\#\{\text{parejas de primos } (n, n+2^j) \text{ hasta } x\}}{\#\{\text{parejas de primos } (n, n+2^k) \text{ hasta } x\}} \longrightarrow 1 \quad \text{cuando } x \to \infty$$

[29] Las funciones L en cuestión son las funciones L de Artin, y las fórmulas asintóticas para las clases conjugadas bajo las aplicaciones de Frobenius apropiadas se obtienen utilizando el teorema de densidad de Cebotarev. Se pueden demostrar resultados análogos asumiendo la holomorfía para estas funciones L, así como la Hipótesis de Riemann y la independencia lineal de los ceros de las funciones L sobre los racionales.

[30] El último acrónimo procedente de Washington: un nuevo tipo de beca que potencia la "Integración Vertical" de la investigación, desde los estudiantes de licenciatura brillantes hasta los profesores universitarios.

para todos enteros positivos j y k. Comparando las primeras cuatro potencias de 2, obtenemos los resultados que se recogen en la Tabla 8.

$n \leq x$	$(n, n+2)$	$(n, n+4)$	$(n, n+8)$	$(n, n+16)$
100	8	9	9	9
200	15	14	14	13
500	24	27	24	24
1000	35	41	38	39
2000	61	65	63	60
5000	143	141	141	135
10000	205	203	208	200
$20K$	342	344	353	331
$50K$	705	693	722	707
$100K$	1224	1216	1260	1233
$200K$	2160	2136	2194	2138
$500K$	4565	4559	4641	4631
1 millón	8169	8144	8242	8210

Tabla 8: El número de parejas de primos $(n,\ n+2^k)$ hasta x, para $k = 1, 2, 3, 4$ y para diferentes valores de x.

De estos datos iniciales parece desprenderse que existe un sesgo en favor de los primos $(n, n+8)$, al menos a partir de que x sea diez mil o más. Sin embargo, no se conoce una fórmula explícita como (3) que nos conduzca a un enfoque fructífero de este problema. En el segundo apéndice de este artículo presentamos el trabajo de un equipo de estudiantes de la Universidad de Georgia que analizaron más datos y trataron de hacer predicciones.

Existen bastantes otras cuestiones naturales relativas a las carreras de números primos que han sido objeto de investigación en los últimos años.

Puede tardarse mucho tiempo en alcanzar el liderato

Aunque el equipo 1 consigue ponerse ocasionalmente en cabeza en la carrera módulo 4, tarda un buen rato en hacerlo. De hecho, la primera vez que lo hace, y sólo durante un breve intervalo, x es más grande que 25000; la primera vez que el equipo 1 conserva el liderazgo durante un intervalo largo, x es más grande que medio millón. De la misma manera, en la carrera módulo 3, x es más grande que un billón cuando el equipo 1 se pone en cabeza. En la carrera de $\pi(x)$ contra $\mathrm{Li}(x)$, no sabemos exactamente cuándo se pone $\pi(x)$ en cabeza por vez primera, aunque la respuesta es sin duda alguna enorme.

Otra situación interesante es aquélla en la que un equipo es superado por los demás. Por ejemplo, como ya vimos, los primos de la forma $8n+1$ quedan muy por detrás de al menos uno de los tipos de primos $8n+3,\ 8n+5$ ó $8n+7$ (porque todos los cuadrados impares, incluidos los cuadrados de los primos,

son de la forma $8n + 1$, una pesada carga para el equipo 1). De hecho, la primera vez que el equipo 1 consigue abandonar la cola está más allá de 500 millones: por ejemplo, $x = 588067889$ es la primera vez que hay más primos de la forma $8n + 1$ hasta x que de la forma $8n + 5$; y $x \approx 1.982 \times 10^{14}$ es la primera vez que hay más primos de la forma $8n + 1$ hasta x que de la forma $8n+7$. Kaczorowski, e independientemente Rubinstein y Sarnak, demostraron que el equipo 1 marcha en primera posición en esta carrera de cuatro para una proporción positiva de valores de x; sin embargo, la primera vez que esto ocurre está más allá de 10^{28}.

¿Por qué les cuesta tanto a algunos corredores conseguir ponerse en cabeza? Para entender esto necesitamos examinar los términos más "importantes" en la formula (3), a saber, el término "-1" y los primeros sumandos, aquéllos para los que γ es pequeño. Estos primeros sumandos, que se corresponden con los ceros no triviales de la función zeta de Riemann que están más cerca del eje real, tienen valores de γ aproximadamente iguales a 14.13, y 21.02, 25.01, 30.42, ... En particular, estos sumandos son todos ellos $< 1/7$ en valor absoluto, así que son pequeños en comparación con el término inicial "-1". Incluso si pudiéramos encontrar un valor de x para el que muchos de los términos iniciales $\operatorname{sen}(\gamma \ln x)$ fueran cercanos a "-1", necesitaríamos que al menos los primeros 21 términos de la suma fueran suficientemente negativos para compensarlo. Así que estos valores de x deben ser especiales, en el sentido de que muchos de los términos $\operatorname{sen}(\gamma \ln x)$ estén cerca de -1 simultáneamente.

Si miramos a la carrera módulo q cuando q se hace grande, resulta que los números relevantes γ se hacen más pequeños (esto es, los ceros de la función L de Dirichlet apropiada caen más cerca del eje real), y por lo tanto los cambios en la cabeza se suceden más pronto y más frecuentemente.

Sin embargo, el que γ tome valores muy pequeños acarrea ciertos problemas. Por ejemplo, cuando $q = 163$, la suma correspondiente tiene un γ especialmente pequeño, a saber $\gamma \approx 0.2029$. Así que este único sumando tiene un gran impacto sobre la respuesta final, puesto que el denominador es muy pequeño. La primera vez que $\operatorname{sen}(\gamma \ln x)$ está cerca de -1 es cuando $\gamma \ln x$ está cerca de $3\pi/2$; ¡que corresponde a un valor de x alrededor de 12000 millones! Y si, debido a los restantes términos, este x no nos valiera, el siguiente valor lo encontraríamos cuando $\gamma \ln x$ estuviera cercano a $7\pi/2$, que correspondería a $x \approx 3.43 \times 10^{23}$. ¡No debe sorprender que se tarde tanto en ver los efectos predichos!

Compartiendo la cabeza

En una carrera entre dos contendientes que estén adelantándose el uno al otro, habrá muchos momentos en los que estén empatados: como hay valores de x arbitrariamente grandes para los que $\#\{\text{primos } qn + a \leq x\} > \#\{\text{primos } qn + b \leq x\}$, y también valores de x arbitrariamente grandes para los que $\#\{\text{primos } qn + a \leq x\} < \#\{\text{primos } qn + b \leq x\}$, y como estas fun-

ciones toman sólo valores enteros, debe haber infinitos enteros x para los que $\#\{\text{primos } qn + a \leq x\} = \#\{\text{primos } qn + b \leq x\}$.

¿Y si la carrera tiene más participantes? Incluso si cada uno de los contendientes se pone en cabeza infinitas veces, no parece haber ninguna razón simple que justifique que todos ellos estén empatados alguna vez. Así que nos podemos preguntar si existen infinitos x para los que

$$\#\{\text{primos } qn+a \leq x\} = \#\{\text{primos } qn+b \leq x\} = \#\{\text{primos } qn+c \leq x\} = \cdots$$

Feuerverger y Martin conjeturan que *hay* infinitos empates de este tipo en una carrera de tres equipos módulo q, pero que *no* los hay en carreras de cuatro o más. Su convincente argumento es como sigue: considérese el vector de dimensión $(k-1)$ cuya componente i, $1 \leq i \leq k-1$, es la diferencia

$$\#\{\text{primos } qn + a_i \leq x\} - \#\{\text{primos } qn + a_{i+1} \leq x\}. \tag{5}$$

Obsérvese que las k funciones $\#\{\text{primos } qn + a_i \leq x\}$ estarán empatadas entre sí precisamente cuando este vector de dimensión $(k-1)$ sea el vector $(0, 0, \ldots, 0)$. Conforme x va aumentando, este vector cambia cada vez que x sea un número primo de alguna de las progresiones aritméticas que estemos considerando, y este cambio consiste en añadir uno de los vectores

$$(1, 0, \ldots, 0),\ (-1, 1, 0, \ldots, 0),\ \ldots,\ (0, \ldots, 0, -1, 1, 0, \ldots, 0),\ \ldots,\ (0, \ldots, 0, -1),$$

dependiendo de si el primo es de la forma $qn+a_1$, ó $qn+a_2 \ldots$, ó $qn+a_k$, respectivamente. El teorema de los números primos para progresiones aritméticas nos dice que cada uno de estos vectores son aproximadamente igual de probables.

A partir de esto, Feuerverger y Martin sugieren que la evolución del vector $(k-1)$-dimensional en (5) puede ser modelizada por un "camino aleatorio" sobre el retículo de dimensión $k-1$ generado por los vectores descritos en (6). Se sabe que, con probabilidad 1, un camino aleatorio sobre un retículo de dimensión uno o dos vuelve al origen (realmente visitará todos los puntos del retículo) infinitas veces, pero un camino aleatorio de dimensión tres o mayor volverá al origen sólo un número finito de veces. Éste es el fundamento de la conjetura de Feuerverger y Martin, pues en este modelo los retículos de dimensión uno y dos se corresponden con las carreras de primos con uno y dos participantes, respectivamente.

Ciertas simetrías especiales

Asumiendo la Hipótesis Generalizada de Riemann, Feuerverger y Martin demostraron que determinadas configuraciones

$$\#\{\text{primos } qn+a_1 \leq x\} < \#\{\text{primos } qn+a_2 \leq x\} < \cdots < \#\{\text{primos } qn+a_r \leq x\}$$

ocurren exactamente con la misma frecuencia[31] que otras configuraciones

$$\#\{\text{primos } qn+b_1 \le x\} < \#\{\text{primos } qn+b_2 \le x\} < \cdots < \#\{\text{primos } qn+b_r \le x\}$$

en las siguientes situaciones:

- si los a_i y los b_i son inversos módulo q; es decir, si $a_i b_i \equiv 1$ módulo q para todo i;
- si la lista de los b_i es justamente la lista de los a_i, pero invertida, es decir, $b_i = a_{r+1-i}$ para todo i, y si además son todos cuadrados módulo q (o ninguno de ellos lo es);
- si existe un entero m tal que $a_i \equiv m b_i$ módulo q para cada i, y además ocurre alguna de las siguientes circunstancias:
  - todos los a_i son cuadrados módulo q; o
  - para todo i, los dos números a_i y b_i son ambos cuadrados módulo q, o bien ninguno de ellos lo es; o
  - para todo i, exactamente uno de los dos números a_i y b_i es un cuadrado módulo q.

Probablemente las ordenaciones aparecen con diferentes frecuencias si no están relacionadas por alguna simetría especial.

¿Y si la Hipótesis de Riemann fuera falsa?

Algunos resultados famosos en teoría de números se han demostrado en dos partes: primero suponiendo que la Hipótesis de Riemann fuera cierta, y segundo, suponiendo que fuera falsa. El pionero trabajo de Sarnak y Rubinstein asumía dos hipótesis, la primera de las cuales era la Hipótesis Generalizada de Riemann. Es lícito preguntarse si podemos obtener resultados similares, quizás con una demostración bastante diferente, suponiendo que la Hipótesis Generalizada de Riemann fuera falsa.

Si fuera falsa, resulta que es más fácil demostrar que

$$\#\{\text{primos } qn + a \le x\} > \#\{\text{primos } qn + b \le x\}$$

para una proporción positiva[32] de x, puesto que el término "-1" en la fórmula análoga a (3) pasa a ser irrelevante, y este término era el que provocaba el sesgo cuando asumíamos la Hipótesis Generalizada de Riemann. Sin embargo, no está claro que esto suceda el 50% de las veces. Si pudiéramos demostrarlo asumiendo que la Hipótesis Generalizada de Riemann es falsa, entonces

[31] Con respecto a la medida logarítmica del conjunto de tales valores x.
[32] En la medida logarítmica.

tendríamos una demostración incondicional de que la carrera módulo q entre cuadrados y no cuadrados es una carrera nivelada (combinando dicha demostración con el trabajo de Rubinstein y Sarnak).

El comportamiento de las carreras de números primos debería ser genuinamente diferente si la Hipótesis de Riemann Generalizada no fuera cierta. En 2001, Ford y Konyagin demostraron que si la Hipótesis Generalizada de Riemann fuera falsa –falsa en un sentido muy especial, aunque factible–, entonces habría algunas ordenaciones de las funciones cuenta-primos que nunca ocurrirían.

Para describir una de sus construcciones, necesitamos discutir una generalización de la función zeta de Riemann. Defínase χ como la función para la que

$$\chi(5m) = 0,\ \chi(5m \pm 1) = \pm 1, \text{ y } \chi(5m \pm 2) = \pm i \ \text{ para todos los enteros } m;$$

y sea

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$$

(otro ejemplo de función L de Dirichlet). Supongamos que la Hipótesis Generalizada de Riemann es cierta *excepto* por el hecho de que $L(s, \chi)$ tiene un cero simple $\sigma + i\gamma$ con $\sigma > 1/2,\ \gamma \geq 0$, y por el hecho de que $L(s, \overline{\chi})$ tiene también un cero en $\sigma - i\gamma$ (los ceros siempre vienen en pares conjugados). La fórmula análoga a (3) es

$$\frac{\#\{\text{primos } 5n + a \leq x\} - \frac{1}{4}\pi(x)}{x^\sigma / \ln x} \approx -2\text{Re}\left(\chi(a)\frac{(\cos(\gamma \log x) + i\,\text{sen}(\gamma \log x))}{\sigma + i\gamma}\right),$$

para $1 \leq a \leq 4$. Más explícitamente,

$$\frac{1}{2}(\sigma^2 + \gamma^2)\frac{\#\{\text{primos } 5n + 1 \leq x\} - \frac{1}{4}\pi(x)}{x^\sigma / \ln x} \approx -\sigma \cos(\gamma \ln x) - \gamma\,\text{sen}(\gamma \ln x)$$

$$\frac{1}{2}(\sigma^2 + \gamma^2)\frac{\#\{\text{primos } 5n + 2 \leq x\} - \frac{1}{4}\pi(x)}{x^\sigma / \ln x} \approx \sigma\,\text{sen}(\gamma \ln x) - \gamma \cos(\gamma \ln x)$$

$$\frac{1}{2}(\sigma^2 + \gamma^2)\frac{\#\{\text{primos } 5n + 3 \leq x\} - \frac{1}{4}\pi(x)}{x^\sigma / \ln x} \approx -\sigma\,\text{sen}(\gamma \ln x) + \gamma \cos(\gamma \ln x)$$

$$\frac{1}{2}(\sigma^2 + \gamma^2)\frac{\#\{\text{primos } 5n + 4 \leq x\} - \frac{1}{4}\pi(x)}{x^\sigma / \ln x} \approx \sigma \cos(\gamma \ln x) + \gamma\,\text{sen}(\gamma \ln x)$$

Asombrosamente, ¡esto implica que la configuración

$$\begin{aligned}\#\{\text{primos } 5n + 3 \leq x\} &< \#\{\text{primos } 5n + 2 \leq x\} \\ &< \#\{\text{primos } 5n + 4 \leq x\} < \#\{\text{primos } 5n + 1 \leq x\}\end{aligned}$$

no se puede dar si x es suficientemente grande! ¿Por qué? La primera desigualdad implica que

$$\begin{aligned} -\sigma \operatorname{sen}(\gamma \ln x) + \gamma \cos(\gamma \ln x) &\lessapprox \sigma \operatorname{sen}(\gamma \ln x) - \gamma \cos(\gamma \ln x) \\ \iff 0 &\lessapprox \sigma \operatorname{sen}(\gamma \ln x) - \gamma \cos(\gamma \ln x), \end{aligned}$$

donde el signo $\lessapprox$ significa que la desigualdad es cierta salvo por un error que tiende a cero cuando x tiende a infinito. De la misma manera, la tercera desigualdad implica que $\sigma \cos(\gamma \ln x) + \gamma \operatorname{sen}(\gamma \ln x) \lessapprox 0$. Las tres desigualdades son equivalentes a

$$0 \lessapprox \sigma \operatorname{sen}(\gamma \ln x) - \gamma \cos(\gamma \ln x) \lessapprox \sigma \cos(\gamma \ln x) + \gamma \operatorname{sen}(\gamma \ln x) \lessapprox 0,$$

lo que implica que

$$\sigma \operatorname{sen}(\gamma \ln x) - \gamma \cos(\gamma \ln x) \approx 0 \quad \text{y} \quad \sigma \cos(\gamma \ln x) + \gamma \operatorname{sen}(\gamma \ln x) \approx 0\,.$$

Sin embargo, si multiplicamos por $\operatorname{sen}(\gamma \ln x)$ y $\cos(\gamma \ln x)$ respectivamente, obtenemos que

$$\sigma \operatorname{sen}^2(\gamma \ln x) - \gamma \cos(\gamma \ln x) \operatorname{sen}(\gamma \ln x) \approx 0$$

y

$$\sigma \cos^2(\gamma \ln x) + \gamma \cos(\gamma \ln x) \operatorname{sen}(\gamma \ln x) \approx 0\,,$$

y si las sumamos deducimos que

$$\sigma = \sigma \operatorname{sen}^2(\gamma \ln x) + \sigma \cos^2(\gamma \ln x) \approx 0.$$

Pero esto es ridículo, porque dice que la constante $\sigma > \frac{1}{2}$ tiende a 0 cuando x tiende a infinito.

Ford y Konyagin probaron más cosas. Para cada trío de progresiones aritméticas módulo q, existe una forma posible (aunque también muy particular) de prescribir ceros de la correspondiente función L de Dirichlet que violan la Hipótesis Generalizada de Reimann para la que una de las seis configuraciones de estas tres progresiones aritméticas no suceda a partir de un cierto valor de x. Además, los ceros en estas configuraciones se podrían situar arbitrariamente lejos del eje real, lo que implicaría que no habría modo de descartar tal posibilidad mediante cálculos finitos.

Parece que su método se puede extender para demostrar que determinadas carreras entre dos progresiones aritméticas mantienen el mismo líder a partir de un punto en adelante, a condición de que existiera otra contradicción, técnicamente posible, aunque bastante rebuscada, con la Hipótesis Generalizada de Riemann.

En el trabajo de Ford y Konyagin aparecen otras construcciones similares. En el caso de las carreras entre r contendientes, con $r \geq 4$, han construido

configuraciones de "violaciones" que no permiten que más de r^2 (de las $r!$ posibles) ordenaciones de las r progresiones aritméticas sucedan infinitas veces.

Parece, pues, que será muy difícil obtener resultados independientes de estas hipótesis.

Agradecimientos. La sección "Haciendo la hola" se inspira en el delicioso artículo [4] de Enrico Bombieri. Los autores agradecen a Carter Bats, Kevin Ford, Richard Hudson and Nathan Ng por proporcionarles partes de sus trabajos que todavía no han sido publicados. Y nuestro agradecimiento también a Guiliana Davidoff y Michael Guy por preparar los apéndices.

Referencias

[1] C. Bays and R. H. Hudson, Details of the first region of integers x with $\pi_{3,2}(x) < \pi_{3,1}(x)$. *Math. Comp.* **32** (1978), no. 142, 571–576.

[2] C. Bays and R. H. Hudson, Zeros of Dirichlet L-functions and irregularities in the distribution of primes. *Math. Comp* **69** (2000), 861–866.

[3] C. Bays and R. H. Hudson, A new bound for the smallest x with $\pi(x) > \mathrm{Li}(x)$. *Math. Comp* **69** (2000), 1285–1296.

[4] E. Bombieri, Prime Territory: Exploring the infinite landscape at the base of the number system. *The Sciences* **32** (1992), no. 5, 30–36.

[5] H. Davenport, *Multiplicative Number Theory*. Springer, Berlin, 1980.

[6] G. Davidoff, C. Osowski, J. Vanden Eynden, Y. Wang, N. Wrinkle, Extensions of some results of Harold Stark on comparative prime number theory, por aparecer.

[7] G. Davidoff, A generalization of Littlewood's Theorem, por aparecer.

[8] A. Feuerverger and G. Martin, Biases in the Shanks-Rényi prime number race. *Experiment. Math.* **9** (2000), no. 4, 535–570.

[9] K. Ford and S. Konyagin, The prime number race and zeros of Dirichlet L-functions off the critical line. *Duke Math. J.* **113** (2002), 313–330.

[10] K. Ford and S. Konyagin, The prime number race and zeros of Dirichlet L-functions off the critical line, II. In *Bonner Mathematische Schiften* (D. R. Heath-Brown, B. Z. Moroz, editors) **360**. Bonn, Germany, 2003.

[11] R. G. Guy, The strong law of small numbers. *Amer. Math. Monthly* **95** (1988), 697–712.

[12] G. H. Hardy, and J. E. Littlewood, Some problems of Partitio Numerorum III: On the expression of a number as a sum of primes. *Acta Math.* **44** (1922), 1–70.

[13] R. H. Hudson, A common combinatorial principle underlies Riemann's formula, the Chebyshev phenomenon, and other subtle effects in comparative prime number theory, I. *J. Reine Angew. Math.* **313** (1980), 133–150.

[14] J. Kaczorowski, On the Shanks-Rényi race problem. *Acta Arith.* **74** (1996), no. 1, 31–46.

[15] J. Kaczorowski, On the distribution of primes (mod 4). *Analysis* **15** (1995), no. 2, 159–171.

[16] S. Knapowski and P. Turán, Comparative prime-number theory, I-III. *Acta Math. Acad. Sci. Hungar* **13** (1962), 299–364.

[17] S. Knapowski and P. Turán, Comparative prime-number theory, IV-VIII. *Acta Math. Acad. Sci. Hungar* **14** (1963), 31–250.

[18] J. E. Littlewood, Distribution des nombres premiers. *C. R. Acad. Sci. Paris* **158** (1914), 1869–1872.

[19] G. Martin, Asymmetries in the Shanks-Rényi prime number race. In *Number theory for the millennium, II (Urbana, IL, 2000)*, 403–415. A K Peters, Natick, MA, 2002.

[20] N. Ng, *Limiting distributions and zeros of Artin L-functions*. Ph.D. Thesis, University of British Columbia, 2000.

[21] M. Rubinstein and P. Sarnak, Chebyshev's Bias. *Experimental Mathematics* **3** (1994), 173–197.

[22] J.-P. Serre, *A course in arithmetic*. Springer, Berlin, 1973.

[23] D. Shanks, Quadratic residues and the distribution of primes. *Math. Comp* **13** (1959), 272–284.

[24] H. M. Stark, A problem in comparative prime number theory. *Acta. Arith.* **68** (1971), 311–320.

[25] E. C. Titchmarsh, *The theory of the Riemann zeta-function*, second edition. Oxford University Press, New York, 1986.

[26] A. Winter, On the distribution function of the remainder term of the prime number theorem. *Amer. J. Math* **63** (1941), 233–248.

Andrew Granville
Département de Mathématiques et Statistique
Université de Montréal
CP 6128 succ Centre-Ville
Montréal QC H3C 3J7, Canada
Correo-electrónico: andrew@dms.umontreal.ca

Greg Martin
Department of Mathematics
University of British Columbia
Room 121, 1984 Mathematics Road
Vancouver, BC V6T 1Z2, Canada
Correo-electrónico: gerg@math.ubc.ca

Traducción de Francisco Javier Cilleruelo Mateo y Pablo Fernández Gallardo

Apéndice I. Un REU[33] del Mount Holyoke College

por *Giuliana Davidoff*

En mi clase de teoría analítica de números de la licenciatura pido habitualmente a mis alumnos que recojan datos sobre diversas cuestiones, para que con ellos formulen conjeturas y para que, luego, expongan sus resultados al resto de la clase. Después de haber visto muchos ejemplos donde los teoremas confirmaban las evidencias experimentales iniciales, les pedí que recogieran datos sobre la carrera módulo 4, para luego sorprenderlos con el teorema de Littlewood. Después decidimos investigar las carreras módulo 3, 5, 7, y 11, y en particular si el equipo N, el conjunto de los primos que no son congruentes con un cuadrado módulo q, se halla habitualmente por delante del equipo S, el conjunto de los primos que son congruentes con un cuadrado módulo q. Curiosamente, los resultados que encontraron eran diferentes dependiendo de los módulos que se tratasen, y decidimos estudiar este fenómeno durante el programa de verano REU.

Los estudiantes empezaron buscando, en la literatura existente, lo referente a cambios de signo, y pidieron ayuda e información a través de una página *web* de teoría de números. En pocos días recibimos una generosa respuesta de Andrew Odlyzko, quien nos señaló ciertos resultados numéricos de Robert Rumely relacionados con nuestro problema, lo que nos permitió empezar nuestro propio trabajo en serio.

Nos fascinó sobre todo un artículo [24] de Harold Stark de 1971 en el que sugería un método para estudiar carreras entre primos de dos progresiones aritméticas dadas. Hasta entonces, no se conocía procedimiento general alguno para demostrar que cada equipo se ponía por delante infinitas veces en la carrera entre primos de la forma $qn + a$ y primos de la forma $qn + b$, donde a es un cuadrado módulo q y b no lo es. Los resultados de Stark pertenecían a un caso no contemplado por los trabajos anteriores de Littlewood [18] y de Knapowski y Turán [16, 17]. Como él mismo señaló, parecía especialmente difícil demostrar que $qn + a$ fuera a estar en cabeza infinitas veces, incluso en el caso de los primos de la forma $5n + 4$ contra los primos de la forma $5n + 2$.

Stark reescribe el problema en términos de dos funciones auxiliares (expresiones complicadas, análogas a (3), dadas por ceros de varias funciones L de Dirichlet), y de esta manera crea un maravilloso escenario en el que es capaz de obtener un teorema a partir de un cálculo numérico. Así fue capaz de demostrar que

$$\#\{\text{primos } 5n + 4 \leq x\} > \#\{\text{primos } 5n + 2 \leq x\}$$

para infinitos valores de x, asumiendo la Hipótesis Generalizada de Riemann.

[33] *Research Experience for Undergraduates*. El grupo de investigación estaba formado por los estudiantes Caroline Osowski, Jennifer vanden Eynden, Yi Wang, y Nancy Wrinkle.

De hecho lo hizo asumiendo algo más débil: solo necesitó que las funciones L de Dirichlet asociadas a esta carrera no tuvieran ceros reales en el intervalo $(1/2, 1)$.

El grupo REU empezó por hacer un estudio numérico detallado de la fórmula de Stark para esta carrera módulo 5, con objeto de apreciar cómo variaban sus complicadas expresiones con el número de primos. Y encontramos que había unas correlaciones muy buenas, aunque algo menores cuando utilizábamos menos ceros para aproximar la fórmula análoga a la de la parte derecha de (3). Utilizando los resultados de Stark y nuestros propios cálculos numéricos, pudimos demostrar el resultado esperado en los primeros casos que él no trataba.

Teorema 4 **([6])**. *Asumamos que las funciones L de Dirichlet no tienen ceros reales en el intervalo $(1/2, 1)$. Para $a = 1$, 2, ó 4 (los cuadrados módulo 7) y para $b = 3$, 5, ó 6 (los no cuadrados módulo 7), existen infinitos valores de x para los que*

$$\#\{primos\ 7n + a \leq x\} > \#\{primos\ 7n + b \leq x\}.$$

De hecho, existe una constante $c > 0$ tal que

$$\#\{primos\ 7n + a \leq x\} - \#\{primos\ 7n + b \leq x\} > c\sqrt{x}/\log x$$

para infinitos valores de x.

La prueba del teorema se basa en cálculos de la fórmula de Stark utilizando tablas existentes de ceros de funciones L de Dirichlet. Quizás podíamos haber continuado con este problema sobre carreras, módulo a módulo. Sin embargo, la pregunta que nos interesó inicialmente era si el equipo S tomaba la delantera infinitas veces frente al equipo N. Para estudiar esto tuvimos que modificar adecuadamente las fórmulas de Stark. En esta ocasión descubrimos que las fórmulas sólo involucraban los ceros de la función L de Dirichlet

$$\sum_{n \geq 1} \frac{(n/q)}{n^s},$$

donde $(n/q) = 1$ si n es un cuadrado módulo q, $(n/q) = 0$ si q divide n y $(n/q) = -1$ si n no es un cuadrado módulo q.

Encontramos las mismas correlaciones entre la verdadera estimación y nuestra aproximación; si el verano no hubiera acabado, seguramente habríamos probado que el liderato cambia infinitas veces en esta carrera módulo 7.

Más tarde, pude continuar con la cuestión y demostrar [6] que, efectivamente, la cabeza cambia infinitas veces en la carrera equipo S *versus* equipo N, para cualquier módulo q, asumiendo una versión débil de la Hipótesis Generalizada de Riemann, en la que solo se necesita suponer que los ceros reales de la función L de Dirichlet anterior caen a la izquierda del supremo de las partes reales de los ceros complejos (lo que ocurre, en particular, cuando la función L de Dirichlet no tiene ceros reales).

Apéndice II. Un grupo de investigación VIGRE de la Universidad de Georgia[34]

por *Michael Guy*

El problema de los primos gemelos, la afirmación de que hay infinitos pares de primos $(p, p+2)$, es uno de las más famosas cuestiones sin resolver de la Teoría de Números clásica. Tiene diversas generalizaciones, pero aquí nos ocuparemos de la cuestión de si hay infinitos pares de primos $(p, p+2k)$ para cualquier entero para positivo $2k$. La siguiente conjetura sobre el número de tales pares que hay hasta x se debe, esencialmente, a Hardy y Littlewood [12].

La conjetura de Hardy-Littlewood. *Sea k un entero positivo, y sea $\pi_{2k}(x)$ el número de parejas de primos $(p, p+2k)$ con $p \leq x$. Entonces*

$$\pi_{2k}(x) \sim 2C_2 \prod_{p|k,\ p>2} \frac{p-1}{p-2} \cdot \mathrm{Li}_2(x),$$

donde

$$C_2 = \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \quad \text{y} \quad \mathrm{Li}_2(x) = \int_2^x \frac{1}{(\log t)^2} dt.$$

Decidimos investigar el problema recogiendo y analizando datos. Nuestro programa encontraba parejas de primos utilizando una criba de Eratóstenes modificada. Algunos de los datos iniciales están recogidos en la siguiente tabla:

x	$\pi_2(x)$	$\pi_4(x)$	$\pi_6(x)$	$\pi_8(x)$	$\pi_{10}(x)$
10^3	35	41	74	38	51
10^4	205	203	411	208	270
10^5	1224	1216	2447	1260	1624
10^6	8169	8,144	16386	8242	10,934
10^7	58980	58622	117207	58595	78211
10^8	440312	440258	879908	439908	586811
10^9	3424506	3424680	6849047	3426124	4567691
10^{10}	27412679	27409999	54818296	27411508	36548839
10^{11}	224376048	224373161	448725003	224365334	299140330
10^{12}	1870585220	1870585459	3741217498	1870580394	2494056601

Tabla 9: $\pi_{2k}(x)$ es el número de parejas de primos $p, p+2k$ con $p \leq x$.

Obsérvese que las columnas $2k = 2, 4$ y 8 son muy semejantes. Al dibujar los datos para cada $2k \leq 30$, nos dimos cuenta de que $\pi_{2k}(x)$ y $\pi_{2\ell}(x)$ están

[34]El grupo de investigación estaba formado por los estudiantes Michael Beck, Zubeyir Cinkir, Michael Guy, Brian Lawler, Eric Pine, Paul Pollack, and Charles Pooh, y el mentor postdoctoral Jim Solazzo.

muy próximos si los factores primos de $2k$ y de 2ℓ son los mismos. La conjetura de Hardy y Littlewood predice que, en estas circunstancias, $\pi_{2k}(x) \sim \pi_{2\ell}(x)$, así que creímos interesante estudiar estas "carreras de primos gemelos".

Si queremos comparar $\pi_2(x)$ y $\pi_6(x)$, tiene sentido "renormalizar" estas cantidades para que las predicciones de Hardy y Littlewood coincidan. La conjetura predice que $\frac{1}{2}\pi_6(x)$ debería ser aproximadamente $\pi_2(x)$, así que parece razonable comparar estas dos cantidades. En general, definimos

$$\pi'_{2k}(x) = \pi_{2k}(x) \cdot \prod_{p|k,\ p>2} \frac{p-2}{p-1} \quad \text{para cada } k \geq 1 \quad \text{y} \quad \pi_{\text{HL}}(x) = 2C_2 \cdot \text{Li}_2(x).$$

La conjetura de Hardy y Littlewood predice que $\pi'_{2k}(x) \sim \pi_{\text{HL}}(x)$ para todo k, y en la Tabla 10 exhibimos sus diferencias.

x	$\pi_{\text{HL}}(x)$	$\pi'_2 - \pi_{\text{HL}}$	$\pi'_4 - \pi_{\text{HL}}$	$\pi'_6 - \pi_{\text{HL}}$	$\pi'_8 - \pi_{\text{HL}}$	$\pi'_{10} - \pi_{\text{HL}}$
10^3	45	-10	-4	-8	-7	-7
10^4	214	-9	-11	-9	-6	-12
10^5	1248	-24	-32	-25	12	-30
10^6	8248	-79	-104	-55	-6	-48
10^7	58753	227	-131	-150	-158	-95
10^8	440367	-55	-109	-413	-459	-259
10^9	3425,308	-802	-628	-785	816	460
10^{10}	27411416	1263	-1417	-2268	92	213
10^{11}	224368866	7182	4295	-6365	-3532	-13619
10^{12}	1870559881	25339	25578	48868	20513	-17430

Tabla 10: La carrera de los primos gemelos renormalizada.

¡Qué aproximación tan extraordinaria! Da la impresión de que $|\pi'_{2k}(x) - \pi_{\text{HL}}(x)|$ es normalmente bastante menor que $\sqrt{x}$. De hecho, recogimos datos para $k = 1, \ldots, 50$ en este rango de x, y nuestra predicción parecía ser muy buena.

Sin embargo, después de todo, éste es un artículo sobre carreras de primos, y lo que queremos es investigar si hay algunos ganadores (o perdedores) particulares en esta carrera. Diseñamos nuestro programa para que fuera tomando nota de cuándo había un cambio en la primera o última posición, y para que nos informara de ello.

Al comienzo de nuestra investigación, creímos haber detectado los que pensábamos eran los ganadores y perdedores de esta carrera entre primos. Basándonos en los datos hasta 5×10^9, parecía que los pares $(p, p+60)$ y $(p, p+80)$ iban por delante de los otros con los mismos divisores primos. Sin embargo, tras contar hasta 10^{12}, dejaron de ser los ganadores habituales. De la misma manera, ciertos pares de primos eran perdedores de forma consistente al comienzo de la carreras, pero dejaban de serlo más tarde. Como curiosidad interesante, ¡nuestro programa descubrió que hay 14455 cambios en el liderato entre 10^3 y 10^9! Así que, al final, ésta parece ser una carrera en la que no hay vencedores o perdedores claros, y sí muchas preguntas todavía por resolver.