El diablo de los números

Sección a cargo de

Javier Cilleruelo Mateo

Un buen milenio para los primos*

por

Andrew Granville†

Los números primos, los «ladrillos» con los que se construyen los enteros, son una parte central de las matemáticas. Entender su distribución es uno de los problemas más naturales, y por tanto más antiguos, de las matemáticas. Una vez que los antiguos griegos probaron que hay infinitos primos, fue natural preguntarse cuántos había hasta un valor dado, quizás un valor muy grande, cuántos en ciertas sucesiones especiales (por ejemplo, los primos de la forma «un cuadrado más uno»), y cómo identificar rápidamente a los primos. Si examinamos tablas de números primos parece que están «distribuidos al azar» aunque, como Bob Vaughan dijo una vez, todavía no sabemos lo que significa «al azar». Responder a estas preguntas es por tanto una tarea difícil, y cada logro obtenido ha requerido de nuevos e influyentes métodos e ideas. En los últimos treinta años había habido muy pocos resultados de este tipo, pero en la última década ha habido varias sorpresas, algunas de las cuales trataremos a continuación:

- Identificación de primos.
- Valores primos de algunos polinomios de grado mayor que 2 en dos variables.
- Progresiones aritméticas de primos.
- Espacios pequeños entre primos.
- Conexiones entre la distribución de los primos y matrices seleccionadas aleatoriamente.

*Con el título *A good new millenium for the primes*, este artículo apareció originalmente en *The Madrid Intelligencer*, Springer (2006), 32–36, publicado con ocasión del *International Congress of Mathematicians* de 2006. *La Gaceta* agradece al autor y a Springer-Verlag la autorización para publicarlo, y a Carlos Vinuesa del Río su traducción y el diseño de la Figura 1.

†El autor fue parcialmente financiado por una beca del Consejo de Investigación en Ciencias Naturales e Ingeniería de Canadá.

1. Historia

A principios del siglo XIX surgieron las primeras conjeturas buenas para una estimación asintótica[1] de $\pi(x)$, el número de primos hasta x. Ninguna mejor que la observación que Gauss hizo a los 16 años, estudiando tablas de primos hasta 3 millones, de que «la densidad de los primos alrededor de x es más o menos $1/\log x$». Interpretando esto, podemos concluir que $\pi(x)$ es como $\int_2^x \frac{dt}{\log t}$, que denotamos por $\mathrm{Li}(x)$. Comparando esta predicción (redondeada al entero más cercano) con los últimos datos que se tienen (Tabla 1), vemos que la predicción de Gauss es increíblemente precisa. Parece que siempre hay un exceso, pero como la anchura de la columna de la derecha es aproximadamente la mitad que la de la otra parece que la diferencia no es mayor que algo así como $\sqrt{x}$.

x	$\pi(x) = \#\{\text{primos} \le x\}$	Exceso: $\mathrm{Li}(x) - \pi(x)$
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 1: Primos hasta varios x, y exceso de la predicción de Gauss.

¿Hay infinitos primos en la progresión aritmética $a \mod q$ (es decir, a, $a+q$ $a+2q$, $\dots$)? Si observamos que (a,q) divide a todos los elementos de la progresión aritmética $a \mod q$, nos damos cuenta de que debemos tener $(a,q) = 1$. En 1837 Dirichlet probó que ésta es la única restricción, es decir, que todas las progresiones aritméticas $a \mod q$ con $(a,q) = 1$ contienen en efecto infinitos primos.

A mediados del siglo XIX, Riemann definió lo que ahora llamamos la *función zeta de Riemann*, $\zeta(s) := \sum_{n\ge 1} 1/n^s$ cuando esta serie converge absolutamente, es decir, cuando $\mathrm{Re}(s) > 1$. En el resto del plano complejo, podemos dar una definición nueva y consistente de esta función, su continuación meromorfa (con un único polo que es un polo simple en $s = 1$). Riemann mostró cómo los ceros de esta continuación

[1] Esto es, una estimación que es correcta salvo por un factor que $\to 1$ cuando $x \to \infty$.

meromorfa están ligados con la distribución de los números primos vía la siguiente *fórmula explícita*

$$\sum_{\substack{p \text{ primo}, \ m\geq 1 \\ p^m \leq x}} \log p = x - \frac{\zeta'(0)}{\zeta(0)} - \sum_{\rho\,:\,\zeta(\rho)=0} \frac{x^\rho}{\rho}, \quad \text{válida cuando } x \in \mathbb{Z} + 1/2.$$

Riemann conjeturó que, si $\zeta(\rho) = 0$, entonces $\mathrm{Re}(\rho) = 1/2$ o ρ es un entero negativo par. En tal caso cada $|x^\rho/\rho| = x^{\mathrm{Re}(\rho)}/|\rho| \leq x^{1/2}/|\rho|$, y entonces obteniendo una buena estimación para el número de ceros hasta altura T podemos deducir, de una ligera variante de la fórmula explícita[2], que $|\pi(x) - \mathrm{Li}(x)| \leq \sqrt{x}\log 5x$, para todo $x \geq 5$. Evidentemente si uno sólo puede probar que los ceros están suficientemente alejados de la recta $\mathrm{Re}(s) = 1$ entonces las mismas ideas se pueden usar para probar que $\pi(x) \sim \mathrm{Li}(x)$ ($\sim x/\log x$), el *teorema de los números primos*, algo que Hadamard y de la Vallée Poussin lograron en 1896. Con métodos similares, de la Vallée Poussin pudo establecer que hay aproximadamente el mismo número de primos hasta x en cada progresión aritmética $a \mod q$ con $(a, q) = 1$, si x es suficientemente grande.

2. Identificar si un entero dado es primo

> «El problema de distinguir los números primos de los compuestos ... es ... uno de los más importantes y útiles en aritmética ... La dignidad de la ciencia misma parece requerir que todos los medios posibles sean explorados para resolver un problema tan elegante y célebre.»
>
> C. F. Gauss (1801).

El uso de la factorización y los tests de primalidad en matemáticas aplicadas (criptografía) han inspirado mucha investigación matemática en los últimos veinte años. En la práctica sabíamos desde hace mucho tiempo cómo determinar si un número grande era primo (para números de hasta 10 000 dígitos), pero hasta hace poco nuestros algoritmos rápidos pecaban de una de estas dos cosas: o bien no estaba *garantizado* que funcionaran siempre, o no estaba probado incondicionalmente que fueran rápidos (aunque esperamos que lo sean). En 2002, Manindra Agrawal, Neeraj Kayal y Nitin Saxena [1, 6], desarrollaron brillantemente un «test de primalidad determinista en tiempo polinomial» a partir de las ideas que ya estaban en juego. Su test puede enunciarse como una caracterización elegante (y rápidamente verificable) de los números primos:

Para un entero dado $n \geq 2$, sea r un entero positivo $< n$, para el que n tiene orden $> (\log n)^2$ módulo r. Entonces n es primo si y sólo si n no es una potencia perfecta, n no tiene ningún factor primo $\leq r$, y $(x+a)^n - x^n - a$ es una combinación lineal en $\mathbb{Z}[x]$ de n y $x^r - 1$, para todo entero a, $1 \leq a \leq \sqrt{r}\log n$.

[2]Donde truncamos la suma para que sólo incluya los ceros con $|\mathrm{Im}(\rho)| \leq T$, a costa de un término de error $O(x(\log xT)^2/T)$.

3. Valores primos de polinomios

En cualquier cuerpo de números $K/\mathbb{Q}$, el número de ideales primos de norma $\leq x$ en una clase de ideales dada es $\sim c\,\mathrm{Li}(x)$ para una constante apropiada $c > 0$. El ejemplo más sencillo de esto es cuando $[K : \mathbb{Q}] = 2$ que, tomando normas, corresponde al número de valores primos distintos que toma una cierta forma cuadrática binaria irreducible. De hecho todos los ejemplos en el teorema del ideal primo corresponden a los valores primos que toman ciertos polinomios homogéneos de grado $d = [K : \mathbb{Q}]$ en d variables. Este tipo de resultado fue probado por vez primera por Landau usando una variante (simple) del método de de la Vallée Poussin.

Todas las sucesiones de valores de polinomios que se pueden considerar con estas técnicas tienen una cosa en común: no son muy dispersas, pues contienen más de $x^{1-\epsilon}$ elementos hasta x. Transcurrió un siglo desde la prueba del teorema de los números primos hasta que John Friedlander y Henryk Iwaniec [3] probaron en 1998 que una cierta sucesión más dispersa de valores de un polinomio contiene una sucesión infinita de números primos, a saber, que hay infinitos primos de la forma $a^2 + b^4$, incluso determinando su frecuencia.

Encontrar una sucesión comparativamente tan pequeña (que contiene $\sim cx^{3/4}$ elementos hasta x), supuso un brillante desarrollo de la *criba asintótica* de Enrico Bombieri. Esta criba permitió a Friedlander e Iwaniec vencer el conocido «fenómeno de paridad», que en el pasado había sido una barrera contra el uso de los métodos de criba en cuestiones sobre la distribución de los primos. Inspirados por su trabajo, Heath-Brown y Moroz [8] determinaron en 2002 con qué frecuencia es prima una forma cúbica binaria (una sucesión todavía más dispersa de valores con $\sim cx^{2/3}$ enteros hasta x), como por ejemplo $a^3 + 2b^3$, un logro extraordinario. Quizá el próximo objetivo sean los valores primos de $4a^3 + 27b^2$, el discriminante de la omnipresente curva elíptica $y^2 = x^3 + ax + b$; esta sucesión es menos dispersa ($x^{5/6+o(1)}$ enteros hasta x), pero es más difícil trabajar con ella, ya que la forma $4a^3 + 27b^2$ no factoriza en $\mathbb{C}[a, b]$.

4. Progresiones aritméticas de primos

No hay pares de primos consecutivos[3] (lo cual es muy fácil de probar porque uno de los dos números tendría que ser par), pero encontramos muchos *primos gemelos*, esto es pares de primos cuya diferencia es exactamente 2, por ejemplo 3 y 5, 5 y 7, 11 y 13, 17 y 19,... Pronto se llega a la conjetura de que habrá infinitos pares de este tipo, y de hecho a la de que habrá infinitos pares de primos n, $n + d$ si (y sólo si) d es par. Para generalizar esto a primos trillizos o cuatrillizos tenemos que proceder de modo similar y tener cuidado con la divisibilidad entre otros primos pequeños (por ejemplo, uno de los números n, $n + 2$, $n + 4$ es siempre divisible entre 3) pero la conjetura general es que k polinomios con coeficientes enteros (quizá en varias variables) pueden ser primos simultáneamente para infinitas colecciones de

[3]Nota del traductor: Obviamente sí que hay un par de primos consecutivos, a saber el 2 y el 3, pero sólo ése.

valores enteros de las variables siempre que los polinomios sean todos irreducibles con coeficientes principales positivos y que no haya un primo p que divida a todos los valores del producto de los polinomios. Por lo tanto, creemos que hay infinitos pares de enteros a y d tales que a, $a+d$, $a+2d$, ..., $a+(k-1)d$ son todos primos (la Tabla 2 muestra los ejemplos más pequeños de estas progresiones aritméticas de primos, de longitud 3, 4, ..., 21).

Longitud	Progresión Aritmética	Último término
3	$3+2n$	7
4	$5+6n$	23
5	$5+6n$	29
6	$7+30n$	157
7	$7+150n$	907
8	$199+210n$	1669
9	$199+210n$	1879
10	$199+210n$	2089
11	$110437+13860n$	249037
12	$110437+13860n$	262897
13	$4943+60060n$	725663
14	$31385539+420420n$	36850999
15	$115453391+4144140n$	173471351
16	$53297929+9699690n$	198793279
17	$3430751869+87297210n$	4827507229
18	$4808316343+717777060n$	17010526363
19	$8297644387+4180566390n$	83547839407
20	$214861583621+18846497670n$	572945039351
21	$5749146449311+26004868890n$	6269243827111

Tabla 2: Las progresiones aritméticas de k primos con el último término más pequeño (se puede conjeturar que el último término debería ser aproximadamente $(ke^{1-\gamma}/2)^{k/2}$, lo cual cuadra bastante bien con los datos de la tabla[5]).

Hasta hace no mucho, esto sólo se había probado para $k=3$ (de hecho había varias pruebas distintas en la literatura), sin embargo en 1990 Antal Balog [2] dio una bonita vuelta de tuerca al tema. Demostró que hay infinitos cuadrados de primos 3×3, donde cada fila y cada columna tiene tres primos en progresión aritmética, e infinitos cubos de primos $3\times 3\times 3$ de este tipo, e incluso que lo mismo ocurre ¡en cualquier dimensión!

Dado que, en tanto tiempo, nadie había trabajado en el aparentemente imposible problema de los primos en progresiones aritméticas, supuso una enorme sorpresa el hecho de que, en 2004, Ben Green y Terry Tao anunciaran que efectivamente habían probado que, para todo k, hay infinitos pares de enteros a y d tales que a, $a+d$, $a+2d$, ..., $a+(k-1)d$ son todos primos, dando incluso una cota superior (mastodóntica) para el más pequeño de estos pares.

[5]La constante de Euler-Mascheroni γ se define como $\lim_{n\to\infty}\left\{\left(\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{n}\right)-\log n\right\}$.

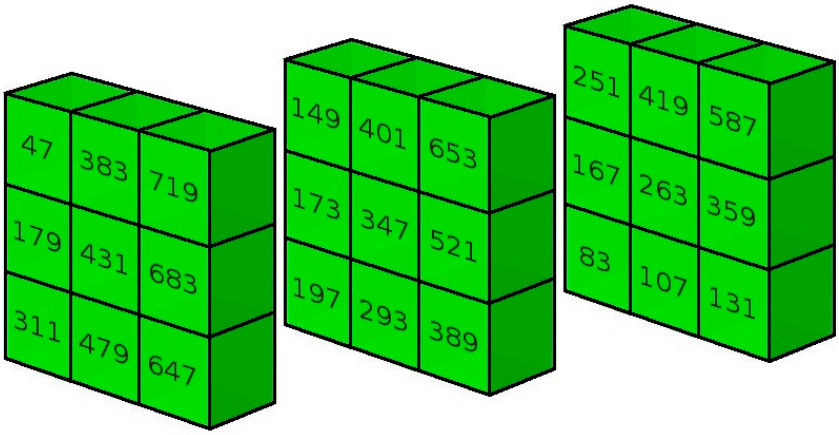

Figura 1: Un «cubo de Balog» de primos $3 \times 3 \times 3$.

Los métodos empleados son nuevos para la teoría analítica de números y son mejor descritos por el término *combinatoria aditiva*, una mezcla de análisis armónico, combinatoria, teoría ergódica, teoría de grafos, teoría combinatoria de grupos y teoría de números, inspirada en las pautas innovadoras introducidas por Tim Gowers [5]. Mirando hacia atrás, el teorema de Gregory Freiman de los años 60 sobre la estructura de la suma de conjuntos y varias ideas de Imre Ruzsa desarrollando esto y enlazándolo con el análisis armónico han sido clave para estos nuevos desarrollos. El teorema de Freiman dice que si $A + A = \{a + b : a, b \in A\}$ es «pequeño» para un conjunto dado de enteros A, entonces el conjunto A debe ser un subconjunto «grande» de una progresión aritmética generalizada de dimensión pequeña. Una progresión aritmética generalizada es un conjunto de la forma $\{a_0 + a_1 m_1 + \cdots + a_d m_d,$ donde $0 \leq m_j \leq M_j$ para cada $j\}$.

La asombrosa nueva[6] técnica de Green y Tao promete revolucionar la teoría de números analítica. Todavía podría responder muchas más preguntas sobre la distribución de las «tuplas» de primos y han hecho grandes esfuerzos para replantear el método de manera que se adapte mejor a la teoría de números analítica clásica, así como para interpretar mejor qué significa que una norma de Gowers sea grande.

Un detalle final de la prueba del teorema de las progresiones aritméticas de k primos vino con una mayoración de los primos por ciertas funciones con pesos provenientes de las ideas de cribas, originalmente construidas por Selberg, pesos que también aparecen en el siguiente gran avance.

5. Cribas

Los primos son enteros que no son divisibles entre ningún primo «relativamente pequeño». Así que para contar primos en una sucesión A borramos aquellos ele-

[6] Aunque tiene varios rasgos en común con el método del círculo.

mentos divisibles entre 2, 3,..., todos los primos pequeños. Si A es el conjunto de enteros hasta x entonces el número de elementos de A divisibles entre d es x/d con un término de error menor o igual que 1; y en los problemas típicos de criba el número de elementos divisibles entre d es $w(d)|A|/d$ (donde $w(\cdot)$ es una función multiplicativa[7]) con un término de error pequeño, al menos en media. Si uno intenta estimar los primos de A directamente a partir de esta información, por ejemplo por el principio de inclusión-exclusión, encuentra que los términos de error se acumulan e «inundan» al término principal. Por lo tanto es conveniente o bien realizar una modificación adecuada del principio de inclusión-exclusión (*la criba combinatoria*), o bien intentar obtener cotas superiores e inferiores para el número de primos en A tratando cada una de estas cuestiones como un problema de optimización sujeto a ciertas restricciones (las cotas para los términos de error). En principio podríamos resolver este tipo de problemas vía los multiplicadores de Lagrange, pero hay tantas variables y una solución así es tan complicada que uno no puede trabajar con ello. Así Atle Selberg pulió las restricciones de nuestro problema de optimización de tal manera que pudiera encontrar elegantemente cotas que son normalmente más fuertes que las que se obtienen con la criba combinatoria, y que son relativamente fáciles de usar en las aplicaciones. Tal como los hemos descrito, los métodos de criba típicamente identifican los enteros hasta x sin factores primos $\leq y$, donde y es una potencia fija[8] de x, aunque una potencia considerablemente más pequeña que $1/2$. Jing-Run Chen empleó esta *criba de Selberg* (junto con otras cosas) para mostrar que hay infinitos primos p para los que $p+2$ tiene a lo sumo dos factores primos. Selberg observó el fenómeno de paridad, que su formulación de los problemas de criba no podía distinguir fácilmente entre enteros con un número impar de factores primos y enteros con un número par de factores primos; por lo que se necesita algún nuevo ingrediente para probar que hay infinitos primos gemelos.

6. Espacios pequeños entre primos

El teorema de los números primos nos dice que hay $\sim x/\log x$ primos hasta x, por lo que el espacio medio entre primos hasta x es $\sim \log x$. Podemos preguntarnos si hay espacios entre primos consecutivos que sean considerablemente más grandes o considerablemente más pequeños que la media. Escribiendo $p_1 = 2, p_2 = 3, p_3 = 5,\ldots$ para los primos, nos preguntamos, por tanto,

$$¿\ \limsup_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} = \infty \ \text{ y } \ \liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} = 0\ ?$$

La primera igualdad es bastante fácil de probar, simplemente exhibiendo sucesiones largas de enteros consecutivos que tienen un factor primo pequeño. Los mayores espacios que se conocen tienen tamaño $c\log p_n \log\log p_n \log\log\log\log p_n/(\log\log\log p_n)^2$ para cierta constante $c>0$; en los últimos 68 años sólo se ha mejorado el valor de c,

[7] Esto es, $w(mn) = w(m)w(n)$ si $(m,n)=1$.

[8] Nótese que si todos los factores primos de n son $> n^{1/3}$ entonces n no tiene más de dos factores primos.

¡y Paul Erdős ofreció 10 000 dólares por una prueba de que se puede hacer $c \to \infty$ en este resultado! Se conjetura que los espacios son tan grandes como $c'(\log p_n)^2$, para algún $c' > 1$.

La segunda pregunta, si hay espacios considerablemente más pequeños que los espacios medios entre primos, resistió todos los ataques durante mucho más tiempo, de hecho el trabajo en esta dirección inspiró el desarrollo de la *gran criba* (una herramienta que ha tenido más éxito para dar estimaciones del número de primos al comienzo de progresiones aritméticas). Hasta hace poco los espacios más pequeños que se habían probado eran un poquito menores que $\frac{1}{4}\log p_n$, lo cual parece un poco patético dado que ¡creemos que hay infinitos espacios de longitud 2! Es más, hace ya casi cuarenta años del resultado de Chen de que hay infinitos primos p para los que $p+2$ tiene a lo sumo dos factores primos. Así, fue una gran sorpresa cuando, en 2005, Dan Goldston, János Pintz y Cem Yıldırım [4] anunciaran que podían probar finalmente que hay espacios pequeños entre primos, de hecho que $p_{n+1} - p_n \leq (\log p_n)^{1/2+\epsilon}$ en infinitas ocasiones. Si el resultado es sorprendente, la prueba lo es todavía más, pues usa ideas que han estado rondando en la teoría de criba durante cincuenta años, y porque parece contradecir el «fenómeno de paridad» del que hemos hablado antes. Por supuesto, el método no es *exactamente* la formulación de Selberg de la criba, pero es tan parecido que es completamente inesperado.

Estos nuevos métodos no parecen ser suficientemente fuertes para probar que hay infinitos pares de primos gemelos, aunque es verosímil que pudieran ser desarrollados para probar la afirmación ligeramente más débil de que $p_{n+1} - p_n \leq B$ en infinitas ocasiones, para alguna constante absoluta B (de hecho esto se obtendría si supiéramos que los primos están bien distribuidos al comienzo de progresiones aritméticas, en progresiones aritméticas ligeramente más cortas que las que da la gran criba). Una posibilidad emocionante.

7. La distribución de los primos y matrices seleccionadas aleatoriamente

Nuestra Tabla 1, que contaba el número de primos, nos da buenos motivos para pensar que el número esperado de primos hasta x es como $\mathrm{Li}(x)$. Entonces ¿cuál es la varianza? En otras palabras, la media de $(\pi(x) - \mathrm{Li}(x))^2$. Si examinamos la modificación adecuada de la fórmula explícita vemos que los términos ahora involucran pares de ceros de la función zeta de Riemann, y cuando hacemos la media (i. e., integramos sobre un rango de valores de x) entonces los únicos términos significativos son aquéllos en los que la distancia entre dos ceros es pequeña. Por lo tanto, si asumimos la hipótesis de Riemann y denotamos sus ceros por $1/2 \pm i\gamma_1$, $1/2 \pm i\gamma_2$, $1/2 \pm i\gamma_3$,... donde $0 < \gamma_1 < \gamma_2 < \ldots$, entonces es de interés determinar con qué frecuencia $\gamma_{n+k} - \gamma_n$ es pequeño. En 1973, Montgomery [9] dio buenas evidencias que sugerían que esta función de distribución es algo sorprendente: que los ceros no están espaciados de la misma manera que el mismo número de puntos elegidos al azar hasta cierta altura, sino de acuerdo con una función notablemente distinta, una que sugiere que los ceros de $\zeta(s)$ se repelen entre sí en comparación con puntos

seleccionados al azar. Más concretamente, el número esperado de $m > n$ para los que $\gamma_m - \gamma_n$ no es mayor que α veces el espacio medio entre ceros (hasta esta altura) es

$$\int_0^\alpha \left\{1 - \left(\frac{\sin \pi t}{\pi t}\right)^2\right\} dt.$$

A Dyson le extrañaba que la función de distribución de Montgomery para los $\gamma_{n+k} - \gamma_n$ era la misma que la de los pares de autovalores de matrices seleccionadas aleatoriamente (algo con lo que uno se topa estudiando los niveles de energía en caos cuántico), y sugirió que quizá las estadísticas para los ceros tomados de tres en tres o de cuatro en cuatro (o más) a la vez, de hecho todas las estadísticas de espaciamiento local, podrían ser las mismas que las de los autovalores. Estudiando un montón de evidencias computacionales debidas a Odlyzko, se dieron buenas evidencias teóricas a la sugerencia de Dyson en un monumental artículo de 1996 escrito por Zeev Rudnick y Peter Sarnak [10].

Extrapolando, Sarnak conjeturó que quizá los ceros de todas las funciones zeta de interés satisfacen las mismas estadísticas de espaciamiento local que las matrices seleccionadas aleatoriamente (de dimensión creciente), donde las matrices se «seleccionan aleatoriamente» sólo de ciertos grupos clásicos. Pruebas computacionales revelaron una teoría cautivadora (bastante conjetural), y Nick Katz y Sarnak incluso probaron una versión (débil) de este tipo de teoría para funciones zeta en cuerpos finitos.

Físicos matemáticos encabezados por Sir Michael Berry y Jon Keating han unido sus fuerzas con los expertos en funciones zeta para construir un marco conjetural donde entender mejor las muchas misteriosas propiedades de $\zeta(s)$. Quizá es justo decir que poco se ha probado incondicionalmente para $\zeta(s)$ como consecuencia de ello, pero realmente ahora comprendemos mucho mejor varias cuestiones sobre los ceros y el tamaño de las funciones zeta.

8. Conclusión

Ha sido un maravilloso nuevo milenio para nuestra comprensión de la distribución de los primos y, mejor aún, hemos visto nuevos métodos apasionantes (de combinatoria aditiva), nuevas perspectivas proféticas (de matrices aleatorias), y el desarrollo de un método clave, las cribas, mucho más allá de donde parecía estar estancado (Friedlander e Iwaniec) e incluso hemos visto que el fenómeno de paridad, que parecía ser un obstáculo fundamental, no lo es ¡y todavía tenemos que entender bien por qué no lo es! Seguro que nos aguardan tiempos todavía mejores, pero siempre debemos tener en mente que

> «Los matemáticos han intentado en vano descubrir algún orden en la sucesión de los números primos pero tenemos muchos motivos para creer que hay algunos misterios en los que la mente humana nunca podrá penetrar.»
>
> L. Euler (1770).

Agradecimientos: El autor agradece a John Friedlander, K. Soundararajan y a los editores de *The Madrid Intelligencer* sus comentarios a las versiones anteriores de este artículo.

Referencias

[1] Manindra Agrawal, Neeraj Kayal y Nitin Saxena, *Primes is in P*, Ann. of Math. (2) **160** (2004), no. 2, 781–793.

[2] Antal Balog, *The prime k-tuplets conjecture on average*, en «Analytic Number Theory» (eds. B.C. Berndt et al.), Birkhäuser, Boston (1990), 165–204.

[3] John Friedlander y Henryk Iwaniec, *The polynomial $X^2 + Y^4$ captures its primes*, Ann. of Math. (2) **148** (1998), 945–1040.

[4] Dan Goldston, János Pintz y Cem Yildirim, *Primes in Tuples I*, aparecerá en Ann. of Math. (2), preprint: `http://xxx.arxiv.org/math.NT/0508185`

[5] Tim Gowers, *A new proof of Szemerédi's Theorem for arithmetic progressions of length four*, GAFA **8** (1998), 529–551.

[6] Andrew Granville, *It is easy to determine whether a given integer is prime*, Bull. Amer. Math. Soc. **42** (2005), 3–38.

[7] Ben Green y Terence Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (2) **167** (2008), no. 2, 481–547.

[8] Roger Heath-Brown y Boris Moroz, *Primes represented by binary cubic forms*, Proc. London Math. Soc. **84** (2002), 257–288.

[9] Hugh Montgomery, *The Pair Correlation of Zeros of the Zeta Function*, Proc. Symp. Pure Math. (Amer. Math. Soc., Providence) **24** (1973), 181–193.

[10] Zeev Rudnick y Peter Sarnak, *Zeros of principal L-functions and random matrix theory*, Duke Math. J. **81** (1996), 269–322.

Andrew Granville, Département de Mathématiques et de Statistiques, Université de Montréal, CP 6128 succ. Centre-Ville, Montréal QC H3C 3J7, Canada

Correo electrónico: `andrew@dms.umontreal.ca`

Página web: `http://www.dms.umontreal.ca/~andrew/`

Traducido por Carlos Vinuesa del Río, Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049 Madrid, España

Correo electrónico: `c.vinuesa@uam.es`

Página web: `http://www.uam.es/personal_pdi/ciencias/cvinuesa/`