El diablo de los números

Sección a cargo de

Javier Cilleruelo Mateo

El método del círculo

por

Fernando Chamizo, Elena Cristóbal y Adrián Ubis

1 Introducción

Si se pidiera al matemático aficionado, orgulloso vencedor de *sudokus* y cubos de Rubik, que mencionase un problema difícil de su querida ciencia, es posible que se refiriera a un problema aditivo de teoría de números: ¿Se puede escribir alguna potencia k-ésima como suma de dos potencias k-ésimas? (Fermat), ¿Es todo número natural suma de 19 cuartas potencias? (Waring), ¿Es todo impar mayor que 5 suma de tres primos y todo número par mayor que 2 suma de dos primos? (Goldbach).

La simplicidad de la suma y la inconmensurabilidad entre enunciado y dificultad han hecho de este tipo de problemas alimento incombustible de la literatura de divulgación. Para el matemático profesional problemas tan anecdóticos como los anteriores se han mostrado muy fructíferos más allá de su valor histórico, ya que en el empeño de su solución se han creado verdaderas teorías matemáticas de gran valor y belleza.

En las siguientes páginas nos proponemos describir una técnica analítica que permite tratar problemas aditivos cuando heurísticamente se esperan muchas soluciones. Por ejemplo, de la lista anterior se puede aplicar a todos los problemas menos al primero (las sumas de dos potencias grandes dejan muchos huecos libres), aunque como es bien sabido no se tenga una solución completa del último.

Esta técnica es el *método del círculo* cuyo nacimiento se remonta a 1918, cuando Hardy y Ramanujan lo introdujeron en un famoso artículo [Ha-Ra] para estudiar las particiones. Más adelante Hardy y Littlewood lo desarrollaron en varios exitosos trabajos. También es destacable la variante de Kloosterman

[Kl] y sobre todo las contribuciones de Vinogradov, a quien se debe en gran medida la formulación actual.

Para los fanáticos de la teoría analítica de números el método del círculo es parte de su vajilla de plata y en ella se han servido guisos tan suculentos como:

- Una fórmula asintótica para el número de particiones que se convierte en exacta si se admiten series infinitas.
- La demostración de que todo natural es suma de cierta cantidad de potencias k-ésimas cualquiera que sea k (problema de Waring), estimando el número necesario de ellas y obteniendo una aproximación para el número de representaciones.
- La prueba de que todo número impar suficientemente grande es suma de tres primos (teorema de Vinogradov).
- La prueba de que casi todo número par (en el sentido de la densidad) es suma de dos primos.

El no iniciado puede sentirse un poco perplejo al saber que una técnica analítica es aplicable con tal versatilidad a la teoría de números. A primera vista los argumentos con distancias "epsilónicas" a los que nos acostumbra el análisis nada tienen que ver con el conjunto discreto por excelencia: los naturales, y su más destacado descendiente aritmético: los primos.

El puente que favorece esta conexión es el motor que anima gran parte de la teoría analítica de números:

extraer información a partir de las singularidades

Un ejemplo bien conocido es la teoría que rodea al teorema de los números primos (el antiguo artículo divulgativo [Ra1] puede iluminar más al lector acerca de la inesperada conjunción de aritmética y análisis). Sin entrar en detalles, Riemann encontró una relación directa entre el número de primos menores que una cantidad dada y las singularidades de $-\zeta'(s)/\zeta(s)$ (donde $\zeta(s)$ es la función zeta de Riemann) de forma que un resultado acerca de la localización de dichas singularidades se transforma inmediatamente en un resultado sobre la distribución de los primos.

El rasgo distintivo del método del círculo es que, en cierto modo, las singularidades se distribuyen densamente en la circunferencia unidad y se intenta separar las contribuciones principales. Para respetar el desarrollo histórico ilustraremos el método con el ejemplo de las particiones (véase [Ji] para otros aspectos interesantes del problema). No es difícil demostrar que[1]

$$1 + \sum_{n=1}^{\infty} p(n) z^n = \prod_{m=1}^{\infty} \frac{1}{1 - z^m}$$

[1] $(1 - z^m)^{-1} = 1 + z^{1 \cdot m} + z^{2 \cdot m} + z^{3 \cdot m} + \dots$ y al multiplicar estos factores el término $z^{a_1 \cdot m_1 + \dots + a_r \cdot m_r}$ corresponde a la partición $m_1 + \overset{a_1 \text{ veces}}{\dots} + m_1 + \dots + m_r + \overset{a_r \text{ veces}}{\dots} + m_r$.

donde $p(n)$ es el número de particiones de n: el número de formas en que n se puede expresar como suma de enteros positivos sin importar el orden ni el número de sumandos, por ejemplo $p(4) = 5$ (porque 4 es 4, 1+3, 2+2, 1+1+2 y 1+1+1+1).

El método del círculo comienza con la fórmula integral de Cauchy

$$p(n) = \frac{1}{2\pi i} \int_{|z|=r} \frac{F(z)}{z^{n+1}}\, dz \qquad \text{donde} \quad F(z) = \prod_{m=1}^{\infty} \frac{1}{1-z^m}, \tag{1}$$

para $0 < r < 1$. No podemos aprovechar la singularidad en $z = 0$ porque el cálculo de residuos nos llevaría al principio, por ello intentamos aproximarnos a las singularidades salvajes en el borde del disco de convergencia, la frontera natural de F. Cuando z se acerca a 1, digamos radialmente, $F(z)$ debe crecer realmente rápido porque es un "producto infinito de polos de orden 1". En las cercanías de $z = 1$ hay una gran montaña exponencial que se puede estudiar con precisión utilizando técnicas de análisis. Si ahora nos dirigimos hacia $z = -1$, sólo la mitad de los factores de F tiene polos y esto se combina con el hecho de que el residuo de $(1 - z^{2n})^{-1}$ en $z = -1$ es la mitad que el de $(1 - z^n)^{-1}$ en $z = 1$ y se puede probar que la montaña en las cercanías de $z = -1$ tiene la raíz cuarta de altura cuando estamos igualmente cerca. Así podríamos repetir el argumento en las cercanías de todas las raíces de la unidad $z = e^{2\pi i a/q}$ donde están las singularidades, y deducir que la contribución es menor cuanto mayor es q (ver Fig. 1).

Si r está cercano a 1 entonces en los arcos de $\{|z| = r\}$ próximos a las singularidades más grandes se puede aproximar muy bien la contribución a la integral (1). Éstos son los llamados *arcos mayores* con la nomenclatura introducida por Hardy y Littlewood. En el resto de la circunferencia, los llamados *arcos menores*, sólo vemos "ruido" formado por la interferencia de singularidades que son demasiado débiles para manifestarse contundentemente. En ellos sólo se emplea una cota superior para $|F(z)|$ y se espera que estos arcos menores hagan honor a su nombre contribuyendo poco a (1). Es cierto que podríamos sentir mejor estas singularidades débiles escogiendo r más cercano a 1 pero combinarlas requeriría obtener mucha cancelación en una suma con multitud de sumandos y cualquier estudiante de cálculo numérico sabe que la batalla de la precisión está reñida con restar números grandes próximos.

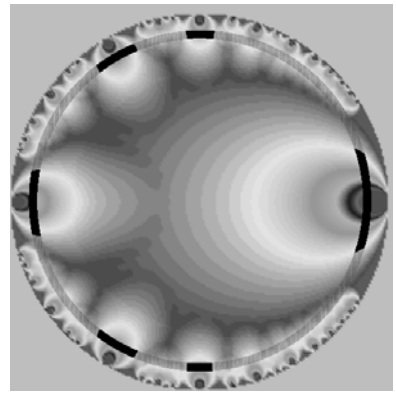

Fig. 1. Curvas de nivel de $|F(z)|$ y algunos arcos mayores

Para el lector ávido de fórmulas, diremos que cerca de la singularidad en $z = 1$ se cumple $F(z) \sim \sqrt{(1-z)/2\pi}\, \exp(\pi^2(1+z)/(12-12z))$ y que integrando en el arco $|z| = 1 - \pi/\sqrt{6n}$, $|\mathrm{Arg}\ z| < n^{-5/7}$ ya se obtiene la asombrosa fórmula asintótica para las particiones

$$p(n) \sim \frac{1}{4n\sqrt{3}}\, e^{\pi\sqrt{2n/3}}.$$

Teniendo en cuenta el resto de las singularidades se obtienen fórmulas más precisas, y en este problema específico se podría llegar hasta una igualdad (con una serie infinita) deformando los arcos mayores para que se ajusten a las curvas de nivel de las "montañas" formadas por las singularidades [Ra2]. Sin embargo en la mayor parte de los problemas los arcos mayores tienen una medida minúscula en comparación con los menores y la contribución de éstos no es en absoluto desdeñable.

Una de las grandes bazas del método del círculo es su versatilidad. En un contexto general tenemos $\mathcal{C} \subset \mathbb{N}$ y queremos saber el número de representaciones de N como suma de k elementos de $\mathcal{C}$, esto es,

$$r_k(N) = \{(c_1, c_2, \ldots, c_k) \in \mathcal{C}^k \ :\ N = c_1 + c_2 + \cdots + c_k\}.$$

Tomando la función

$$F(z) = \sum_{c \in \mathcal{C}} z^c$$

y elevándola a k nos encontramos con que $r_k(N)$ aparece como el coeficiente de una serie,

$$(F(z))^k = \sum r_k(n) z^n.$$

La ventaja es que ahora utilizando la fórmula integral de Cauchy es posible expresar $r_k(N)$ en función de $F(z)$. Se tiene

$$r_k(N) = \frac{1}{2\pi i} \int_{|z|=r} \frac{\big(F(z)\big)^k}{z^{N+1}}\, dz. \tag{2}$$

De nuevo lo natural es que $F(z)$ sea más singular cuando $z \to e^{2\pi i a/q}$ con q pequeño, porque así es más fácil que los exponentes enteros y las frecuencias racionales resuenen. El estudio de tales resonancias está íntimamente ligado a la distribución de los elementos de $\mathcal{C}$ módulo q. Por ello el método del círculo se manifiesta en muchos casos como una especie de principio local-global con término de error.

En algunos de los trabajos pioneros (especialmente al estudiar particiones y sumas de cuadrados) tenía su sentido considerar funciones $F(z)$ dadas por

sumas infinitas para preservar ciertas propiedades modulares. Vinogradov se percató de que en la generalidad de los problemas se eliminaban dificultades técnicas truncando la serie, así es evidente que (2) todavía se cumple si la sumación se restringe a $\mathcal{C}_N = \mathcal{C} \cap [0, N]$ y nada impide elegir entonces $r = 1$, pues ya no hay singularidades en sentido estricto sino valores grandes. En la circunferencia unidad se vuelve natural el cambio $z = e^{2\pi i x}$ y, en suma, la formulación de Vinogradov de (2) es

$$r_k(N) = \int_{-1/2}^{1/2} \big(f(x)\big)^k \, e(-Nx)\, dx \qquad \text{con} \quad f(x) = \sum_{c \in \mathcal{C}_N} e(cx)$$

donde $e(t)$ no es más que una abreviatura para $e^{2\pi i t}$ que utilizaremos en lo sucesivo. Al haber desenrollado la circunferencia con un cambio de variable, los arcos mayores pasarán a ser ahora intervalos alrededor de racionales de denominador pequeño y de nuevo se espera que la contribución del arco que contiene a $x = 0$ sea la mayor.

Entre los numerosos ejemplos que se podrían estudiar, analizaremos con más detalle en las secciones siguientes la representación como suma de primos y como suma de potencias. Nuestro propósito no es incluir las pruebas completas pero sí un esquema sustancioso de ellas.

2 Goldbach, Vinogradov y el método del círculo

Fig. 2. L. Euler

"La matemática tiene la reputación, completamente falsa, de producir conclusiones infalibles. Su infalibilidad no es nada más que la identidad. Dos veces dos no es cuatro, es sólo dos veces dos y eso es lo que llamamos cuatro para abreviar. Pero el cuatro después de todo no es nada nuevo. Y así sigue y sigue en sus conclusiones, sólo que en las fórmulas más complejas la identidad se oculta de nuestra vista" (Goethe).

Parece sencillo, pero cuando la identidad se esconde produce grandes quebraderos de cabeza y más aún cuando es imposible llegar a ella desde razonamientos lógicos, si no, que se lo digan a los matemáticos de principios del siglo XX, cuando aterrizaban los incomprendidos teoremas indecidibles. Por fortuna no es esto lo que sucede con la conjetura de Goldbach, aunque la comunidad matemática ni siquiera sabe si es posible encontrar los pasos lógicos adecuados para completar la demostración. El enunciado vio la luz en junio de 1742 cuando Christian Goldbach escribió a

Leonhard Euler la famosa carta donde afirmaba que todo número par mayor que dos es suma de dos primos y todo número impar mayor que cinco suma de tres (considerando al 1 como primo).

Esta conjetura es un claro exponente de la desafiante belleza de las matemáticas, si no ¿cómo concebir que durante tres siglos un gran número de matemáticos haya dedicado numerosos esfuerzos destinados a demostrar una afirmación que aparentemente no tiene mayor utilidad?

Veamos un poco la historia, lo que se ha logrado y lo que falta por hacer. Durante los siglos XVIII y XIX no hubo avances reseñables debido a que aún no se tenían métodos adecuados para tratar los complicados problemas aditivos. Sin embargo en el siglo XX se han sucedido muchos resultados parciales. En 1923 Hardy y Littlewood empleando el método del círculo lograron demostrar condicionalmente (bajo la hipótesis de Riemann generalizada) que todo número impar "grande" es suma de tres primos. Más tarde Vinogradov introdujo algunas mejoras en el método y en 1937 volvió a probar este resultado pero ahora sin necesidad de suponer ninguna hipótesis adicional.

Fig. 3. I.M. Vinogradov

Como es bien conocido la conjetura binaria continúa siendo hoy un problema abierto. Con el fin de generar publicidad para el libro "El tío Petros y la conjetura de Goldbach" en el año 2000 un editor británico ofreció un premio de un millón de dólares a quien la demostrase antes de abril de 2002. Nadie lo reclamó.

En estos momentos al lector le surgirá la pregunta natural de si se ha conseguido algo en el caso par. Pues bien, empleando el método del círculo, Chudakov, van der Corput y Estermann probaron independientemente en 1938 que casi todo número par se puede expresar como suma de dos primos (véase [Va]). En 1966, Chen mostró utilizando métodos de criba que todo número par lo bastante grande puede escribirse como suma de un primo y un número que tiene a lo más dos factores primos.

En esta sección trataremos de explicar las ideas principales del teorema de Vinogradov: *todo número impar suficientemente grande se puede expresar como suma de tres primos.*

Estimaremos $r_3(N)$, el número de representaciones de un entero, N, como suma de tres primos. Si probamos que es mayor que cero para todo N impar suficientemente grande, el teorema de Vinogradov queda demostrado.

Tomemos la función

$$f_N(x) = \sum_{p \leq N} e(px),$$

procediendo como en la introducción obtenemos

$$r_3(N) = \int_{-1/2}^{1/2} f_N^3(x) e(-Nx) dx.$$

Como ya se ha dicho, el método del círculo consiste en dividir el intervalo de integración en dos subconjuntos, los arcos mayores y los arcos menores (los denotaremos $\mathfrak{M}$ y $\mathfrak{m}$ respectivamente). Que el método funcione se debe a que se obtiene una aproximación muy precisa de la integral en los arcos mayores. A la vez se consigue que estos arcos sean suficientemente grandes como para minimizar la influencia de los arcos menores en los que "sólo empleamos una cota superior" y lo decimos entre comillas porque obtener esta cota no es nada fácil. De hecho, la mayoría de las veces en las que el método del círculo no se puede aplicar a un problema aditivo es porque no se sabe demostrar que la contribución de los arcos menores es más pequeña que la del término principal.

Por lo que se ha visto hasta el momento del método del círculo, se evidencia claramente que las estrellas de la película son las singularidades del integrando. Así pues, no podremos proseguir sin estudiarlas en profundidad. Para ello dibujamos la gráfica de la parte real de $f_N(x)$. Alcanza los valores más grandes en racionales de denominador pequeño: 1, 1/2, 1/3, 2/3, ...

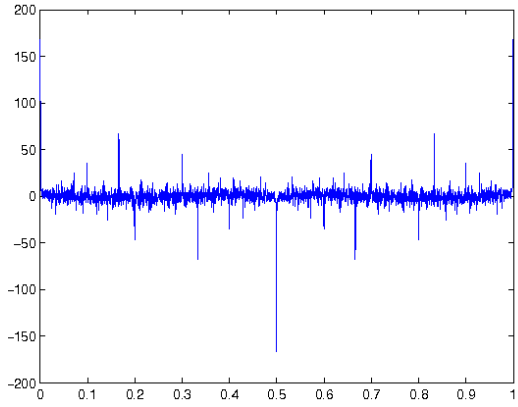

Fig. 4. Parte real de $f_N(x)$.

Para entender bien la naturaleza de los picos en estos racionales es necesario que recordemos el teorema de los números primos en progresiones aritméticas:

Sea $\{qn + a\}$ una progresión aritmética con q y a primos entre sí; la cantidad de primos menores o iguales que x en dicha progresión, $\pi(x; q, a)$, cumple:

$$\pi(x; q, a) \sim \frac{1}{\phi(q)} \frac{x}{\log x},$$

donde la función $\phi(q)$ de Euler indica la cantidad de números menores o iguales que q y coprimos con él.

Utilizando el teorema y teniendo presente que $e(1/2) = -1$ y $e(1/3) + e(2/3) = -1$ es fácil ver que

$$f_N(1/2) = 1 - \pi(N; 2, 1) \sim -\frac{N}{\log N} \quad \text{y} \quad f_N(1/3) = f_N(2/3) \sim -\frac{N}{2\log N}.$$

En general, si a/q es una fracción irreducible, en muchas ocasiones $f_N(a/q)$ es comparable a $N/\phi(q)\log N$. Sin embargo, como $e(1/4) + e(3/4) = 0$ nos encontramos con que $f_N(1/4)$ no es grande. Esto es debido a que cuatro tiene factores primos repetidos, (más adelante volveremos sobre este asunto).

Reflexionando sobre la evaluación que hemos obtenido para $f_N(x)$ y siendo algo más precisos podemos dar una aproximación de $f_N(x)$ alrededor de racionales de denominador pequeño.

Vayamos con ello: la "densidad" de los primos entre los naturales hasta N es $\pi(N)/N \sim 1/\log N$, con lo cual muy cerca de $x = 0$ se debería cumplir algo así como

$$f_N(x) \sim \frac{D(x)}{\log N} \qquad \text{con} \qquad D(x) = \sum_{n \le N} e(nx).$$

Si estamos muy cerca por ejemplo de $x = 1/2$, la aproximación debe ser

$$f_N(x) \sim -\frac{D(x - 1/2)}{\log N}$$

simplemente porque todos los primos, excepto $p = 2$, son impares y por tanto $e(px) = -e(p(x-1/2))$. Si $x = 1/3$, debemos considerar el hecho de que $e(p/3)$ es $e(1/3)$ ó $e(2/3)$ dependiendo de si $p \equiv 1 \pmod 3$ o $p \equiv 2 \pmod 3$. Como por el teorema de los números primos en progresiones aritméticas sabemos que la mitad de los primos está en cada una de las dos progresiones aritméticas que hay módulo tres, se tiene

$$f_N(x) \sim \left(\frac{e(1/3)}{2\log N} + \frac{e(2/3)}{2\log N}\right) D(x - 1/3) = -\frac{D(x - 1/3)}{2\log N}.$$

De forma general se espera (y de hecho se prueba) que muy cerca de la fracción irreducible $x = a/q$ se cumpla

$$f_N(x) = \frac{c_q(1)}{\phi(q)\log N} D(x - a/q) + \text{ términos de error},$$

con $c_q(\cdot)$ la *suma de Ramanujan* que en general se define como

$$c_q(N) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e\left(\frac{Na}{q}\right)$$

donde (a,q) es el máximo común divisor de a y q. Sorprendentemente la suma se puede "evaluar" (ver teoremas 67 y 272 de [Ha-Wr]):

$$c_q(N) = \frac{\mu(q/(q,N))\phi(q)}{\phi(q/(q,N))},$$

siendo $\mu(n)$ la función de Möbius la cual cumple que $\mu(q) = 0$ si q tiene algún factor primo repetido, $\mu(q) = (-1)^k$ si q es producto de k primos distintos y $\mu(1) = 1$.

Una vez conocidas las sumas de Ramanujan, evaluándolas en $N = 1$, podemos expresar $f_N(x)$ como

$$f_N(x) = \frac{\mu(q)}{\phi(q)\log N} D(x - a/q) + \text{ términos de error.}$$

Como $\mu(4) = 0$, es lógico que antes nos hallamos encontrado con que $f_N(1/4)$ no era grande.

La prueba de verdad para conseguir la aproximación asintótica sólo consiste en sumar por partes empleando el teorema de los números primos en progresiones aritméticas. Los pocos conocimientos que se tienen en la dirección de la hipótesis de Riemann generalizada se reflejan en que realmente el término de error no se *come* al principal sólo cuando q es muy pequeño (como un logaritmo de N) y x está realmente muy cerca de a/q.

La función $D(x)$ es pequeña si x no está cerca de los enteros, lo que sugiere que no se pierde mucho aproximando $\int_{|x|<\epsilon}(D(x))^3 e(-Nx)\ dx$ por $\int_{-1/2}^{1/2}(D(x))^3 e(-Nx)\ dx$. Teniendo esto en cuenta, la parte principal de la contribución de los arcos mayores es

$$\sum_{(a,q)=1} \frac{\mu^3(q)e(-Na/q)}{\phi^3(q)(\log N)^3} \int_{-1/2}^{1/2} (D(x))^3 e(-Nx)\ dx \sim \sum_q \frac{\mu^3(q)c_q(-N)N^2}{2\phi^3(q)(\log N)^3}.$$

Usando las propiedades de $c_q(-N)$ (véase [Va]) no es difícil escribir esta suma de funciones multiplicativas como el producto

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

Ahora sólo falta acotar los arcos menores, lo que no es nada fácil. Vinogradov logró demostrar que en ellos

$$\max |f_N(x)| < CN \log^{-A} N$$

para cualquier A (siendo C una constante que depende de A). Su razonamiento pasa por un ingenioso argumento de criba que traslada las "ondas" con frecuencias primas a otras con frecuencias enteras cuyas interferencias son más sencillas de estudiar. Utilizando la acotación de Vinogradov se tiene

$$\int_{\mathfrak{m}} f_N^3(x)e(-Nx)dx < C\frac{N}{\log^A N}\int_{-1/2}^{1/2}|f_N(x)|^2dx$$

y ahora recordando la identidad de Parseval y el teorema de los números primos,

$$\int_{-1/2}^{1/2}|f_N(x)|^2 = \sum_{p\leq N} 1 = \pi(N) \sim \frac{N}{\log N},$$

por tanto la integral sobre los arcos menores es,

$$\int_{\mathfrak{m}} f_N^3(x)e(-Nx)dx < C\frac{N^2}{\log^{A+1} N}.$$

Una vez que conocemos la contribución de los arcos mayores y menores resulta,

$$r_3(N) = \frac{N^2}{2(\log N)^3}\prod_{p|N}\left(1-\frac{1}{(p-1)^2}\right)\prod_{p\nmid N}\left(1+\frac{1}{(p-1)^3}\right) + \text{términos de error}$$

El primer producto para N par "no funciona", se anula, y por tanto no se obtiene ninguna fórmula asintótica en este caso. Además como $N = p_1+p_2+p_3$, para que N sea par forzosamente algún p_i debe ser 2. Suponiendo que $p_1 = 2$,

$$N = 2 + p_2 + p_3 \Longrightarrow N - 2 = p_2 + p_3,$$

esto sería la Conjetura binaria de Goldbach, demasiado bueno para ser cierto. ¿Dónde falla? ¿Qué ocurre si se repite el argumento anterior para un N par y dos primos? A día de hoy no se sabe demostrar que la contribución de los arcos menores sea más pequeña que el término principal (a no ser que se promedie en N, de ahí los resultados de 1938 para el caso par).

3 El problema de Waring

El número 47 no puede escribirse como suma de dos o tres cuadrados. Sin embargo

$$47 = 6^2 + 3^2 + 1^2 + 1^2 = 5^2 + 3^2 + 3^2 + 2^2.$$

Es sencillo expresar un número pequeño como suma de cuatro cuadrados, y podríamos conjeturar que esta propiedad en realidad se cumple para cualquier

natural. Probablemente Diofanto conocía ya este hecho aunque no fue publicado hasta 1621 por Bachet. Más tarde Fermat dijo poseer una demostración, de la que sin embargo no tenemos constancia. Finalmente Lagrange publicó la primera prueba en 1770 (ver [Ha-Wr]), basándose en trabajos de Euler.

Ese mismo año, E. Waring afirmó en su libro *Meditationes Algebraicae* que esto no era una propiedad específica de los cuadrados, sino que 9 cubos o 19 cuartas potencias bastaban para representar todo número natural, y en general que para cualquier número k existe un número s tal que todo natural se puede escribir como suma de s potencias k-ésimas. No parece que Waring tuviera idea de cómo probar esta conjetura, que a partir de entonces se conoce como problema de Waring. En principio era más complicado el caso general que el probado por Lagrange ($k = 2$) porque para este último se contaba con la teoría de formas cuadráticas, que no tenía un equivalente para el resto de los exponentes. Pero Liouville se percató de que el caso $k = 4$ se podía reducir al Teorema de Lagrange por medio de la identidad

$$6(x_1^2 + x_2^2 + x_3^2 + x_4^2)^2 = \sum_{1 \le i < j \le 4} [(x_i + x_j)^4 + (x_i - x_j)^4].$$

De ella podemos deducir que los números de la forma $6m^2$ se pueden representar como suma de 12 cuartas potencias, y por tanto todo múltiplo de 6 como suma de 48 cuartas potencias. En general, cualquier número lo podemos expresar en la forma $6n + r$ con $0 \le r \le 5$, y escribiendo r como suma de unos vemos que todo natural se puede escribir con 53 cuartas potencias.

Fig 5. G.H. Hardy

Tras este resultado se demostraron otros casos con k pequeño y finalmente, en 1909, Hilbert probó la conjetura de Waring para cualquier k (ver [El]). Lo hizo creando identidades como la de Liouville para cada k, usando ideas desarrolladas por Hurwitz. El problema de estas pruebas es que el número s de sumandos que se consigue es gigantesco en comparación con k, y además apenas se obtiene información sobre la estructura de las respresentaciones.

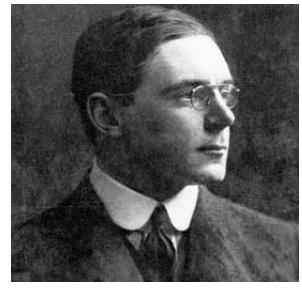

Fig 6. J.E. Littlewood

En 1920 Hardy y Littlewood [Ha-Li1] resolvieron estas dificultades de forma brillante hallando con el método del círculo una fórmula asintótica para

el número de soluciones de

$$x_1^k + x_2^k + \ldots + x_s^k = N,$$

con $x_j \in \mathbb{N}$. Si denotamos por $r(N)$ a dicha cantidad, obtuvieron que para $s > k2^{k-1}$ se cumple

$$r(N) \sim \rho \mathfrak{S}(N) N^{\frac{s}{k}-1}$$

donde $\rho > 0$ es una constante, $\mathfrak{S}(N)$ una función que se mantiene entre dos constantes positivas y representa cierta propiedad aritmética de N, y el término $N^{s/k-1}$ surge de forma natural si tenemos en cuenta que hay $[N^{1/k}]$ potencias k-ésimas menores o iguales que N y el resultado de sumar s de ellas va a estar entre 1 y sN. En particular esta fórmula resuelve el problema de Waring.

Vamos a mostrar un esquema de la prueba de este resultado (la demostración completa se puede consultar en [Da2] o [Va]). Comenzamos con la representación

$$r(N) = \int_0^1 (F(x))^s e(-Nx)dx, \qquad \text{con} \quad F(x) = \sum_{n \leq N^{1/k}} e(n^k x).$$

Como siempre, $F(x)$ tendrá mayor tamaño sobre puntos cercanos a los racionales de denominador pequeño, lo que motiva la división

$$r(N) = \int_{\mathfrak{M}} (F(x))^s e(-Nx)dx + \int_{\mathfrak{m}} (F(x))^s e(-Nx)dx,$$

donde $\mathfrak{M}$ es la unión de los arcos mayores $\mathfrak{M}_{a,q}$ para $1 \leq a \leq q \leq N^{\frac{1}{2k}}$, $(a,q) = 1$ con $\mathfrak{M}_{1,1} = [0, N^{-1+\frac{1}{2k}}) \cup (1 - N^{-1+\frac{1}{2k}}, 1]$ y en el resto de los casos

$$\mathfrak{M}_{a,q} = \{x \in [0,1] : |x - a/q| \leq N^{-1+\frac{1}{2k}}\}.$$

Los arcos menores $\mathfrak{m}$ son el conjunto complementario de los mayores.

Veamos cómo se comporta F sobre $\mathfrak{M}_{a,q}$. Lo que hacemos es agrupar los sumandos donde n tenga el mismo resto módulo q, porque apuntarán más o menos en la misma dirección:

$$F(\frac{a}{q} + \beta) = \sum_{r=1}^{q} e\big(\frac{ar^k}{q}\big) \sum_{\substack{n \equiv r \,(\mathrm{mod}\ q) \\ n \leq N^{1/k}}} e(\beta n^k).$$

Podemos aproximar la suma interior por una integral, obteniendo

$$F(\frac{a}{q} + \beta) \sim S_{a,q} \frac{1}{q} \int_0^{N^{1/k}} e(\beta y^k)dy = \frac{S_{a,q}}{q} N^{\frac{1}{k}} \int_0^1 e(\beta N u^k)du,$$

con

$$S_{a,q} = \sum_{r=1}^{q} e\big(\frac{ar^k}{q}\big).$$

Observamos que cuando estamos muy cerca de un a/q fijo, F es como una constante por $N^{1/k}$. Deduzcamos cuál es la aportación de la integral sobre el arco $\mathfrak{M}_{a,q}$:

$$\int_{\mathfrak{M}_{a,q}} F(x)^s e(-Nx)dx \sim N^{\frac{s}{k}} \frac{S_{a,q}^s}{q^s} \int_{-N^{-1+\frac{1}{2k}}}^{N^{-1+\frac{1}{2k}}} \Big(\int_0^1 e(\beta N u^k)du \Big)^s e\big(-N(\beta + \frac{a}{q})\big)d\beta$$

$$\sim N^{\frac{s}{k}-1} \frac{S_{a,q}^s}{q^s} e\big(-N\frac{a}{q}\big) \int_{-N^{\frac{1}{2k}}}^{N^{\frac{1}{2k}}} \Big(\int_0^1 e(tu^k)du \Big)^s e(-t)dt.$$

Es sencillo darse cuenta de que la integral

$$\rho = \int_{-\infty}^{\infty} (\int_0^1 e(tu^k)du)^s e(-t)dt$$

es absolutamente convergente para $s > k$, de donde deducimos que

$$\int_{\mathfrak{M}_{a,q}} F(x)^s e(-Nx)dx \sim \rho N^{\frac{s}{k}-1} \frac{S_{a,q}^s}{q^s} e(-N\frac{a}{q}).$$

La suma de las contribuciones de los arcos $\mathfrak{M}_{a,q}$ produce

$$\int_{\mathfrak{M}} F(x)^s e(-Nx)dx \sim \rho N^{\frac{s}{k}-1} \sum_{q \le N^{1/2k}} \sum_{(a,q)=1} \frac{S_{a,q}^s}{q^s} e(-N\frac{a}{q}).$$

Se puede ver que en $S_{a,q}$ hay mucha cancelación, lo que justifica la convergencia absoluta de la serie

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} \sum_{(a,q)=1} \frac{S_{a,q}^s}{q^s} e(-N\frac{a}{q})$$

y por tanto la fórmula

$$\int_{\mathfrak{M}} F(x)^s e(-Nx)dx = \rho N^{s/k-1}(\mathfrak{S}(N) + o(1)).$$

En los arcos menores el tamaño de la función $F(x)$ va a ser sensiblemente menor. En particular, se puede probar que

$$\max_{x\in\mathfrak{m}} |F(x)| = O(N^{\frac{1}{k}(1-2^{1-k})}).$$

Así, la aportación de los arcos menores es

$$\int_{\mathfrak{m}} F(x)^s e(-Nx) = O(N^{\frac{s}{k}-2^{1-k}\frac{s}{k}}),$$

y finalmente llegamos a la fórmula

$$r(N) = \rho\mathfrak{S}(N)N^{\frac{s}{k}-1} + o(N^{\frac{s}{k}-1}) \tag{3}$$

para todo $s \geq k2^{k-1}+1$.

La integral ρ es la densidad de las soluciones en números reales de la ecuación de Waring. Es decir, si $v(y)$ es el volumen del conjunto

$$\{(x_1,\ldots,x_s)\in\mathbb{R}^n : y-1/2 < x_1^k+\ldots+x_s^k < y+1/2, x_j>0\},$$

entonces se cumple $\rho = \lim_{y\to\infty} v(y)/y^{s/k-1}$. Por otra parte, se puede probar que

$$\mathfrak{S}(N) = \prod_p d_p(N)$$

donde el producto recorre los primos y

$$d_p(N) = \lim_{\alpha\to\infty} \frac{\#\{(x_1,\ldots,x_s) : 1\leq x_j\leq p^\alpha,\, x_1^k+\ldots+x_s^k \equiv N \pmod{p^\alpha}\}}{p^{\alpha(s-1)}}$$

expresa la densidad límite de las soluciones módulo potencias del primo p de la ecuación de Waring (densidad en $\mathbb{Z}_p$). Esto da cuenta de la influencia de las congruencias en el número de soluciones, y en concreto concuerda con el hecho de que si la ecuación de Waring no tiene solución módulo algún número, entonces $r(N)=0$. Además, la fórmula asintótica nos dice que podemos encontrar N con muchas representaciones simplemente buscando valores que hagan $d_p(N)$ grande para varios primos pequeños, debido a que si p grande $d_p(N)$ se mantiene acotado. Es decir, nos da cierto control sobre la estructura de las soluciones.

Hardy y Littlewood [Ha-Li2] consiguieron probar la fórmula asintótica (3) para todo $s \geq (k-2)2^{k-1}+5$, y mejorando ligeramente su argumento esto se puede rebajar hasta $s \geq 2^k+1$. Las innovaciones de Vinogradov le permitieron controlar de manera más precisa la función F sobre los arcos menores, consiguiendo (3) para todo $s \geq Ck^2\log k$, donde C es una constante.

Volviendo al problema original de Waring, denotemos $g(k)$ al mínimo s tal que todo natural se puede expresar como suma de s potencias k-ésimas. Vamos a ver que $g(k)$ está determinado por las particularidades de los números pequeños. Al comenzar los naturales en el 1, los números relativamente pequeños necesitarán muchos 1^k para ser representados, no se puede jugar con las potencias anteriores porque no las hay. Por ejemplo, digamos que queremos expresar 6399 como suma de octavas potencias. Como $6399 < 3^8$, nos vemos constreñidos a usar sólo sumandos 1^8 y 2^8, y así es fácil ver que 6399 requiere 279 octavas potencias. Considerando el número $2^k[(3/2)^k] - 1$ en vez de 6399, se deja al lector verificar que el argumento anterior en general implica

$$g(k) \geq 2^k + [(3/2)^k] - 2. \tag{4}$$

Cuando N es más grande, el número de potencias necesarias para representarlo disminuye. De hecho, usando el método del círculo para N grande y estudiando de forma separada los N pequeños, Dickson [Di1], [Di2] probó que (4) es en realidad una igualdad para $k \neq 4$ siempre que se cumpla la desigualdad $(3/2)^k - [(3/2)^k] \leq 1 - 2^{-k}[(3/2)^k]$. Mahler [Ma] demostró que es cierta para k suficientemente grande, resolviendo de esa manera el problema de Waring casi por completo.

De esta forma, se perfila como una cuestión más interesante el estudio de $G(k)$, que Hardy y Littlewood definieron como el mínimo número de potencias k-ésimas necesarias para representar todo número N suficientemente grande. La fórmula asintótica prueba que $G(k) \leq 2^k + 1$. En 1935 Vinogradov [Vi2] probó, sustituyendo la fórmula asintótica por una cota inferior para $r(N)$, la desigualdad $G(k) < (2 + o(1))k \log k$. Cuatro años después H. Davenport obtuvo $G(4) = 16$, siendo éste el único valor conocido de G aparte del que se deduce del Teorema de Lagrange ($G(2) = 4$). En 1942 Linnik probó que $G(3) \leq 7$. En los últimos años se han producido importantes avances, usando como base el método del círculo, principalmente debidos a R.C. Vaughan y T.D. Wooley (ver [Va-Wo]).

Mirando el número de representaciones en promedio se deduce fácilmente que $G(k) \geq k + 1$. Se pueden conseguir otras cotas inferiores a partir de congruencias (por ejemplo, $G(2) > 3$ porque $x^2 + y^2 + z^2 \equiv 7$ no tiene solución módulo 8) y se cree que tomando el máximo de todas ellas se obtiene el valor exacto de $G(k)$, que en cualquier caso sería siempre inferior a $4k + 1$.

Agradecimientos: Queremos agradecer a Elías Baro, Fernando Charro, Javier Cilleruelo y Jorge Jiménez la lectura crítica de la versión preliminar.

Referencias

[Da1] H. Davenport, *Multiplicative number theory*, 2nd ed. Graduate texts in mathematics 74. Springer-Verlag, 1980.

[Da2] H. Davenport, *Analytic methods for Diophantine equations and Diophantine inequalities*. Second edition. Cambridge University Press, Cambridge, 2005.

[Di1] L.E. Dickson, Proof of the Ideal Waring Theorem for Exponents 7-180. *Amer. J. Math.* **58** (1936) 3, 521–529.

[Di2] L.E. Dickson, Solution of Waring's Problem. *Amer. J. Math.* **58** (1936) 3, 530–535.

[El] W.J. Ellison, Waring's Problem. *The American Mathematical Monthly* **78** (1971) 1, 10–36.

[El-El] W.J. Ellison, F. Ellison, *Prime Numbers*. Hermann, 1975.

[Ha-Li1] G.H. Hardy, J.E. Littlewood, Some Problems of 'Partitio Numerorum'; I: A new solution of Waring's problem. *Gött. Nachr.* 1920, 33–54.

[Ha-Li2] G.H. Hardy, J.E. Littlewood, Some Problems of 'Partitio Numerorum': II. Proof that every large number is the sum of at most 21 biquadrates. *Math. Z.* **9** (1921) 1-2, 14–27.

[Ha-Ra] G.H. Hardy, S. Ramanujan, Asymptotic formulae in combinatorial analysis. *Proc. London Math. Soc., ser. 2* **17** (1918) 75–115.

[Ha-Wr] G. H. Hardy, E. M. Wright, *An Introduction to the theory of numbers*. 5th ed. Oxford: Oxford University Press, 1979.

[Ji] J. Jiménez Urroz, De partitione numerorum. La Gaceta de la RSME **5** (2002) 2, 443–454.

[Kl] H.D. Kloosterman, On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$. *Acta Mathematica* **49** (1926), 407–464.

[Ma] K. Mahler, On the fractional parts of the powers of a rational number. II. *Mathematika* **4** (1957), 122–124.

[Ra1] H. Rademacher, Trends in research: the analytic number theory. *Bull. Amer. Math. Soc.* **48** (1942), 379–401.

[Ra2] H. Rademacher, On the expansion of the partition function in a series. *Ann. of Math. (2)* **44** (1943), 416–422.

[Va] R.C. Vaughan, *The Hardy-Littlewood method*. Cambridge tracts in Mathematics 80. Cambridge University Press, 1981.

[Va-Wo] R.C. Vaughan, T.D. Wooley, *Waring's problem: a survey*. En A.K. Peters, *Surveys in Number Theory*, Natick, MA, 2003. pp. 285–324.

[Vi1] I.M. Vinogradov, *The method of trigonometrical sums in the theory of numbers*. Dover Publications, Inc., Mineola, NY, 2004.

[Vi2] I.M. Vinogradov, On an upper bound for $G(n)$. *Izv. Akad. Nauk SSSR* **23** (1959), 637–642.

Fernando Chamizo
Elena Cristóbal
Adrián Ubis
Departamento de Matemáticas, Facultad de Ciencias,
Universidad Autónoma de Madrid, 28049 Madrid
Correos electrónicos: fernando.chamizo@uam.es,
elena.cristobal@uam.es,
adrian.ubis@uam.es