El diablo de los números

Sección a cargo de

Javier Cilleruelo Mateo

La conjetura de Goldbach

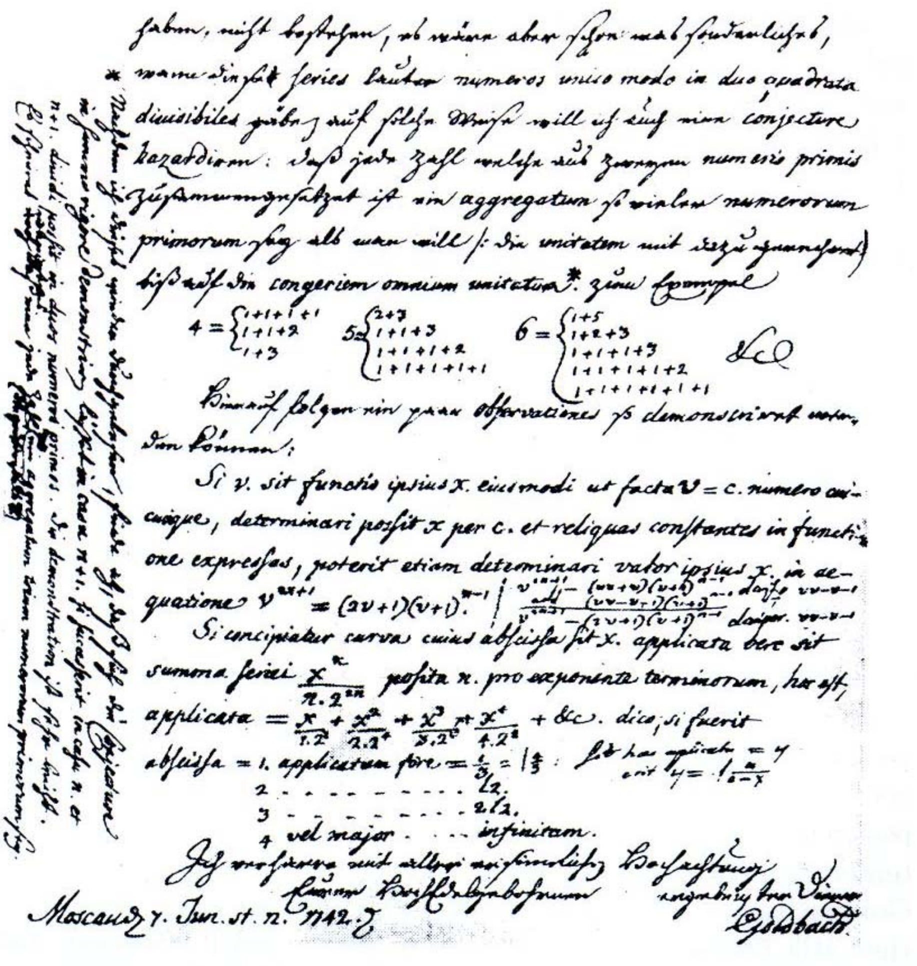
En una carta dirigida a Euler y fechada el 7 de Junio de 1742, Christian Goldbach (1690-1764) afirmaba haber observado que todo número par mayor que 2 podía escribirse como suma de dos primos; y que todo número impar mayor que 5 se podía representar como suma de tres. La resolución de la conjetura de Goldbach, como es conocido el primero de estos problemas, está considerado como uno de los problemas más difíciles de las matemáticas.

Parece una broma el que un problema de enunciado tan sencillo sea inaccesible con las herramientas matemáticas tan poderosas con las que se cuenta hoy en día. Sin embargo no es una excepción; hace solo cuatro años que Andrew Wiles consiguió demostrar el "último teorema de Fermat", el cual competía con la conjetura de Goldbach en sencillez y belleza.

En los últimos meses la conjetura de Goldbach se ha popularizado, más si cabe, debido a un motivo más prosaico. Una editorial ha ofrecido un millón de libras a quien resuelva la conjetura en un plazo de 2 años. No esta claro si este incentivo intenta potenciar la investigación en la teoría de los números o simplemente es una operación de propaganda de un libro reciente de la misma editorial, *"Uncle Petros and Goldbach's Conjecture"* (El Tío Petros y la Conjetura de Goldbach), del griego Apostolos Doxiadis. Sea como fuere, cualquier excusa es buena para hablar una vez más de este problema y de las matemáticas tan extraordinarias a las que ha dado lugar.

¿Por qué se piensa que la conjetura es cierta?

$\mathbf{4} = 2 + 2,$
$\mathbf{6} = 3 + 3,$
$\mathbf{8} = 3 + 5 = 5 + 3,$
$\mathbf{10} = 3 + 7 = 5 + 5 = 7 + 3,$
$\mathbf{12} = 5 + 7 = 7 + 5,$
$\mathbf{14} = 3 + 11 = 7 + 7 = 11 + 3,$
$\mathbf{16} = 3 + 13 = 5 + 11 = 11 + 5 = 13 + 3,$
$\mathbf{18} = 5 + 13 = 7 + 11 = 11 + 7 = 13 + 5,$
$\mathbf{20} = 3 + 17 = 7 + 13 = 13 + 7 = 17 + 3,$
$\mathbf{22} = 3 + 19 = 5 + 17 = 11 + 11 = 17 + 5 = 19 + 3,$



Carta de Goldbach a Euler

La conjetura ha sido verificada para todos los números pares menores que 4×10^{14} por Joerg Richstein (1998).

Los primeros números pares que acabamos de comprobar, no sólo son representables como suma de dos primos, sino que el número de representaciones de n como suma de dos primos, al que llamaremos $r_2(n)$, parece crecer con n. Esto se debe, entre otras cosas, a que los primos son bastante numerosos.

Si definimos $\pi(x)$ como el número de primos menores o iguales que x, el teorema del número primo afirma que $\pi(x) \sim x/\log x$. En otras palabras, la probabilidad de que un entero de tamaño n sea primo es aproximadamente

$1/\log n$. Desde este punto de vista probabilístico, es fácil comprobar que el número esperado para $r_2(n)$ debería ser aproximadamente $n/\log^2 n$. Sin embargo este argumento, basado simplemente en la densidad de los primos, no sólo no es riguroso, sino que ofrece una visión equivocada del problema. Podemos ofrecer ejemplos de conjuntos de impares más "numerosos" que los primos donde hay infinitos pares que no son suma de dos elementos del conjunto. Por ejemplo, con los impares de la forma $4k+1$, que son mucho más numerosos que los primos, no podemos representar los múltiplos de 4.

Esta última observación nos invita a pensar que no sólo debemos tener en cuenta que hay muchos primos, sino que también habrá que ver cómo se distribuyen en progresiones aritméticas. Si, por ejemplo, todos los primos, salvo quizás un número finito de ellos, fueran de la forma $6k+1$, habría infinitos números pares de la forma $6n+4$ que no se podrían representar como suma de dos primos. Pero este no es el caso. Dirichlet generalizó el teorema del número primo para progresiones aritméticas demostrando que existen infinitos primos en todas las progresiones aritméticas $qk+d$, $k=0,1,2,\ldots$ siempre que q y d no tengan divisores comunes, ya que de otra manera no sería posible. Si llamamos $\pi(x,q;d)$ al número de tales primos menores que x, el teorema del número primo para progresiones aritméticas afirma que

$$\pi(x,q;d) \sim \frac{1}{\varphi(q)}\frac{x}{\log x},$$

donde $\varphi(q)$ indica el número de restos primos con q en el conjunto $\{1,\ldots,q-1\}$. En otras palabras, los primos están bien distribuidos en progresiones aritméticas.

El teorema de Vinogradov

Cuando los matemáticos se enfrentan a un problema difícil suelen intentar un problema de las mismas características pero más accesible. Una manera de relajar la conjetura de Goldbach consiste en considerar representaciones con más de dos sumandos. ¿Es cierto que todo número impar mayor que 5 se puede escribir como suma de tres primos? Si aludimos nuevamente a los argumentos probabilísticos comentados anteriormente deberíamos esperar que el número de representaciones de n como suma de tres primos, $r_3(n)$, debería ser, aproximadamente $n^2/\log^3 n$. Y cuantos más sumandos permitamos, mayor número de representaciones debemos esperar.

A principios de siglo se demostró, utilizando los métodos de criba que comentaremos en la siguiente sección, que los números representables como suma de dos primos tienen densidad positiva en los números enteros; es decir, una proporción positiva de ellos son representables como suma de dos primos. Por otra parte, Schnirelman había demostrado que si una sucesión de densidad positiva contiene al 0 y al 1, al sumarla con ella misma un número suficiente de veces, obtenemos todos los enteros positivos. De esta manera Schnirelman logró demostrar que todo número entero suficientemente grande puede escribir como suma de, a lo más, 800.000 números primos. Afinando el método se pudo ir reduciendo el número de sumandos. Pero aún así se vio que este método tenía sus limitaciones y que había pocas esperanzas de reducir el número de sumandos a 3, (problema ternario de Goldbach) y mucho menos a 2 (la conjetura de Goldbach).

Se necesitaban nuevas ideas y éstas vinieron de la mano de dos grandes matemáticos, G.H. Hardy y J.E. Littlewood. El método del círculo, como así se denomina a su original método, es una de las maravillas de la matemáticas. Lo comentaremos brevemente y sin demasiados detalles.

Consideremos el polinomio trigonométrico $S(\alpha) = \sum_{p \leq n} e^{2\pi i \alpha p}$ y calculemos la siguiente integral

$$\int_0^1 S^3(\alpha) e^{-2\pi i n \alpha} = \sum_{p,q,r} \int_0^1 e^{2\pi(p+q+r-n)i}.$$

Todas las integrales se anulan excepto aquellas para las que $p+q+r=n$, que valen 1. Es decir,

$$r_3(n) = \int_0^1 S^3(\alpha) e^{-2\pi i n \alpha}.$$

Aparentemente hemos complicado el problema porque parece difícil hallar el valor de $S(\alpha)$. Pero, intentemos calcularlo para algunos valores concretos. Por ejemplo $S(0) = \pi(n)$ y $S(1/2) = -\pi(n)$. Para $\alpha = 1/3$ el valor de $e^{2\pi i \frac{p}{3}}$ dependera de si p es de la forma $3k+1$ o de la forma $3k+2$. Es decir,

$$S(1/3) = \pi(n,3;1) e^{\frac{2\pi}{3} i} + \pi(n,3;2) e^{\frac{4\pi}{3} i}.$$

Pero el teorema de Dirichlet para primos en progresiones aritméticas afirma que

$$\pi(n;3,1) \sim \pi(n;3,2) \sim \frac{1}{2} \frac{n}{\log n},$$

de donde

$$S(1/3) \sim -\frac{1}{2} \frac{n}{\log n},$$

y en general, utilizando el mismo argumento, se tiene

$$S(a/q) \sim \frac{n}{\log n} \frac{1}{\phi(q)} \sum_{1 \leq l \leq q, (l,q)=1} e^{2\pi \frac{l}{q} i}.$$

Hardy y Littlewood observaron que la mayor contribución de la integral provenía de los α cercanos a racionales de denominador pequeño. La integral sobre estos intervalos centrados en racionales a/q, $(a,q)=1$, puede ser evaluada en función de los $S(a/q)$. A estos intervalos se les denomina arcos mayores y la integral sobre ellos va a constituir el término principal de la integral. Si por el contrario α no está cerca de estos racionales (arcos menores), entonces la suma trigonométrica $S(\alpha)$ tiene bastante cancelación, la suficiente para que la integral sobre los arcos menores sea "pequeña" comparada con la integral sobre los arcos mayores. De esta manera Hardy y Littlewood (1923) demostraron

Teorema (Hardy-Littlewood) *Si la Hipótesis de Riemann Generalizada es cierta, entonces*

$$r_3(n) \sim \sigma_3(n) \frac{n^2}{\log^3 n}.$$

La función $\sigma_3(n)$ tiene una expresión explícita que depende de n, pero comprendida entre dos constantes.

En 1937 Vinogradov demostró, sin necesidad de asumir la Hipótesis de Riemann, lo que hoy se conoce por el Teorema de Vinogradov.

Teorema. (Vinogradov) *Todo número impar suficientemente grande se puede escribir como suma de tres primos.*

En 1989 Chen and Wang consiguieron sustituir la imprecisa expresión "suficientemente grande" por "todo impar mayor que 10^{43000}". Sin embargo este número es todavía demasiado grande como para comprobar si los impares anteriores son representables como suma de tres primos. J.M.Deshouillers, G.Effinger, H.te Riele y D.Zinoviv, asumiendo la Hipótesis de Riemann generalizada, han conseguido rebajar este número hasta 2×10^{12}, accesible a las técnicas de computación actuales.

Teorema. (Deshouillers et al.) *Si la Hipótesis de Riemann Generalizada es cierta, entonces todo número impar mayor que* 5 *se puede escribir como suma de tres primos.*

El mejor resultado incondicional (sin suponer a Hipótesis de Riemann), válido para todos los números pares se debe a O. Ramaré (1995).

Teorema. (Ramaré) *Todo número par se puede escribir como la suma de, a lo más,* 6 *primos.*

Por ejemplo, todavía no se sabe si todo número impar mayor que 1 se puede escribir como suma de, a lo más, 5 primos.

La Hipótesis de Riemann Generalizada, que ha aparecido frecuentemente en el texto, está íntimamente relacionada con el error se comete al estimar el número de primos en progresiones aritméticas. Si fuera cierta, el error que se cometería en dichas estimaciones sería pequeño y la estimación de los $S(\alpha)$ sería más precisa.

Cuando se aplica el método del círculo a la conjetura de Goldbach, incluso asumiendo la Hipótesis de Riemann, la acumulación de errores que se obtiene cuando se estima la integral es mucho mayor que lo que se supone debe ser el término principal proveniente de los arcos mayores. Si se pudiera demostrar que este error es menor que el término principal, se obtendría, como conjeturaron

Hardy y Littlewood, $r_2(n) \sim \sigma_2(n)\frac{n}{\log^2 n}$, donde aquí de nuevo, $\sigma_2(n)$ es mayor que una constante positiva para todo n.

Aunque ya hemos comentado que la estimación de los errores en el método del círculo es muy mala, se pueden obtener buenos resultados en media. De esta manera Estermann (1938) demostró que "casi todos" los números pares satisfacen la conjetura de Goldbach. Es decir, si llamamos $N_2(x)$ al número de pares menores que x no representables como suma de dos primos, entonces $\lim_{x\to\infty} N(x)/x = 0$.

El teorema de chen

Otra manera de acercarse al problema es relajar la condición de primos por la de *casiprimos* (primos o producto de dos primos). En 1966, Chen Jing-Run, utilizando un método de criba muy sofisticado, obtuvo el siguiente resultado.

Teorema. (Chen) *Todo número par suficientemente grande puede escribirse como suma de un primo y un casiprimo.*

Comentemos brevemente qué son los métodos de criba. De todos es conocido la criba de Eratóstenes para la obtención de números primos. Si un número menor que x es compuesto, debe ser divisible por algún primo menor que $\sqrt{x}$. Si vamos eliminando los múltiplos de 2, los de 3, los de 5, así hasta $\sqrt{x}$, lo números menores que x que sobrevivan a esta criba deberán ser primos.

Supóngamos que queremos obtener el número de representaciones de un entero n par como suma de dos primos. Podemos proceder de una manera similar escribiendo todos los números $m(n-m)$, $m < n$. Si m ó $n-m$ no es primo, el número $m(n-m)$ deber tener un divisor primo menor que $n^{1/3}$. Entonces podemos ir tachando aquellos números que sean múltiplos de primos menores que $n^{1/3}$. Los números que sobrevivan a la criba serán de la forma $m = p$, $n - m = q$. Es, decir, $n = p + q$. El problema es que cuando queremos contar el número de los que vamos tachando tenemos que aplicar el principio de inclusión-exclusión. Por ejemplo, después de restar los múltiplos de 3 y los múltiplos de 5, debemos sumar los múltiplos de 15 porque los hemos restado dos veces anteriormente. En todo este proceso se va acumulando un error que no somos capaces de controlar porque $n^{1/3}$ es demasiado grande. Chen consiguió controlar dicho error "cribando" con los primos menores que $n^{1/4}$; pero los números que sobreviven en este caso son de la forma $m(n-m) = pq$ o de la forma $m(n-n) = pqr$. Es decir, $n = p + q$ ó $n = p + qr$.

Los primos gemelos

No podemos escribir sobre la conjetura de Goldbach sin mencionar la conjetura sobre la infinitud de los primos gemelos. En 1849 A. de Polignac conjeturó que para todo número par $2n$ había infinitas parejas de primos cuya diferencia era $2n$. El caso $n = 1$ corresponde una famosa conjetura. ¿Existen infinitas parejas de primos $p, p+2$? A tales parejas se les denomina primos gemelos. Por ejemplo $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(59,61)$ y $(71,73)$ son todas las parejas de primos gemelos menores que 100. La mayor pareja de primos gemelos que se conoce se debe La Barbera, Jobling y Gallot (Octubre de 2000).

$$1693965 \times 2^{66443} \pm 1.$$

Este problema, de 2000 años de antiguedad, está intimamente relacionado con el de la conjetura de Goldbach. El primer resultado notable acerca de los primos gemelos se debe a Vigo Brun, quien demostró, utilizando métodos de criba, que la suma de sus inversos es finita.

Teorema. (Brun) $\sum_{p,p+2=p'} \frac{1}{p} < \infty$.

Por supuesto, esto no significa que haya un número finito de ellos; aunque sí que nos indica que no pueden ser demasiado numerosos. Conviene recordar aquí que la suma de los inversos de los primos es infinita.

También podemos aplicar el método de la criba al problema de los primos gemelos. En este caso escribiremos los números de la forma $m(m+2)$ para todo impar $m \leq x$. Si cribamos por todos los primos menores que $x^{1/3}$ obtenemos primos gemelos menores que x. El argumentó utilizado por Chen en la Conjetura de Goldbach, cribando sólo hasta los primos menores que $x^{1/4}$, permite una cota inferior, que tiende a infinito con x, para el número de parejas donde uno es primo y el otro casiprimo.

Teorema. (Chen) *Existen infinitas parejas que difieren en dos unidades donde uno de ellos es primo y el otro es casiprimo.*

Para terminar, quisiera añadir una reciente y sorprendente caracterización del problema de los primos gemelos debida a María Suzuki.

Teorema. (María Suzuki) *Existen infinitas parejas de primos gemelos si y solo si existen infinitos enteros positivos n que no se pueden escribir de la forma $n = 6|ab| + a + b$, con a, b enteros.*

La demostración es elemental y su lectura recomendable.

Lecturas recomendables

Para saciar la curiosidad de los lectores más interesados recomiendo los siguientes textos, artículos y páginas web relacionados con la conjetura de Goldbach.

[1] Cilleruelo, Javier, Córdoba, Antonio. *La Teoría de os números,* Mondadori (1992). Hay un capítulo dedicado a los métodos de criba donde se demuestra el teorema de Vigo Brun y el teorema de Schnirelmann.

[2] Guy, Richard. *Unsolved Problems in Number Theory, 2nd edition,* Springer-Verlag, New York, (1995). Extensa colección de problemas sin resolver, con muchas referencias.

[3] HARDY, G. H., WRIGHT, E. *An introduction to the Theory of Numbers,* Oxford at the Clarendom Press (1997). Un clásico de la teoría de los números.

[4] NATHANSON, MELVYN B. *Additive number theory: The Classical Bases,* Graduate Texts in Mathematics 165, Springer-Verlag (1996). Un texto avanzado y bien escrito, que incluye las demostraciones del Teorema de Vinogradov y del Teorema de Chen.

[5] RIBENBOIM, PAULO. *The New Book of Prime Number Records, 3rd edition* Springer-Verlag, New York (1995). Un libro de fácil lectura muy recomendable.

[6] WANG, Y. *Goldbach's conjecture* World Scientific Publ., Singapore (1984).

Páginas web de interés para un público mayoritario:

`http://platea.pntic.mec.es/~aperez4/` Una página excelente de matemáticas, en castellano.

`http://members.es.tripod.de/somriure/index.htm` Una página en castellano dedicada a la teoría de números

`http://mathworld.wolfram.com/GoldbachConjecture.html` Una página sobre la Conjetura de Goldbach con bastantes referencias.

Páginas web de interés para profesionales:

`http://www.dpmms.cam.ac.uk/Number-Theory-Web/web.html` La página de referencia para todos los profesionales de la teoría de lod números.

`http://www.math.uga.edu/~andrew/` Página personal de Andrew Granville con artículos muy buenos de teoría de números que se pueden descargar.

`http://www.dpmms.cam.ac.uk/~wtg10/` Página personal del medalla Fields Tim Gowers. Contiene su versión del Teorema de Vinogradov y enlaces muy seleccionados.

Bibliografía

[1] CHEN, JING- RUN. *On the representation of a large even number as the sum of a prime and the product of at mot two primes,* Sci. Sinica, 16 (1973), 157-176.

[2] DESHOUILLERS, J. M., EFFINGER, G. RIELE H. TE ZINOVIEV, D. *A Complete Vinogradov 3-Primes Theorem under the Riemann Hypothesis,* ERA Amer.Math.Soc.,3 (1997), 94-104.

[3] ESTERMANN, T. *On Goldbach's Problem: Proof that Almost All Even Positive Integers are Sums of Two Primes* Proc. London Math. Soc. Ser. 2 44, (1938), 307-314.

[4] HARDY, G. H., LITTLEWOOD, J.E. *Some problems of "Partitio Numerorm", III: On the expression of a number as a sum of primes,* Acta MAth, 44 (1923), 1-70.

[5] RAMARÉ, O. *On Schnirelmann's constant,* Ann. Sc. Norm. Super. Pisa, 22:4 (1995), 645-706.

[6] RICHSTEIN, JOERG *Verifying the Goldbach Conjecture up to* 4×10^{14}, Mathematics of Computation, (por aparecer)

[7] Suzuki, Maria. *Alternative Formulations of the Twin Prime Problem,* American Mathematical Monthly, 107 (Enero-2000), 55-56.

[8] Vinogradov, I. M. *Representation of an odd number as the sum of three primes,* Dokl. Akad. Nauk SSSR, 15 (1937), 169-172.

Javier Cilleruelo Mateo, Departamento Matemáticas,
Universidad Autónoma de Madrid,
Cantoblanco, 28049 Madrid.
correo electrónico: `franciscojavier.cilleruelo@uam.es`