MARGARITA MATHEMATICA EN MEMORIA DE
JOSÉ JAVIER (CHICHO) GUADALUPE HERNÁNDEZ
(Luis Español y Juan L. Varona, editores),
Servicio de Publicaciones, Universidad de La Rioja,
Logroño, Spain, 2001.

PERSPECTIVAS EN LA TEORÍA DE LOS NÚMEROS

J. M. ALDAZ Y A. BRAVO

En memoria de Chicho, a quien, entre otras cosas,
debemos nuestro interés por la Teoría de los Números

Abstract. We explore, in a fairly elementary fashion, a variety of topics in the Theory of Numbers, presenting along the way some conjectures and open problems.

1. Introducción

El objetivo de esta contribución de carácter expositorio es presentar brevemente algunos resultados y conjeturas en la Teoría de los Números, de tal modo que despierten en los no especialistas el deseo de aprender más sobre la materia, y con la esperanza de que incluso los especialistas encuentren aquí algo de interés.

Los problemas que a lo largo de la historia se han planteado en relación con los números naturales frecuentemente han originado una gran variedad de técnicas para su resolución, notablemente en el Álgebra y el Análisis, pese a lo cual muchos de estos problemas continúan sin resolverse.

El primer problema abierto que presentamos es probablemente el más antiguo de toda la Matemática:

¿Existen números perfectos impares?

Recordemos que la secta pitagórica atribuía a los naturales diversas propiedades de carácter místico. La noción de que todo era número o razón entre números llevó directamente al estudio de la conmensurabilidad del lado de un cuadrado con su diagonal, y eventualmente a la demostración de la irracionalidad de la raíz de dos, lo que por cierto no encajaba muy bien con dicha doctrina.

En este contexto cultural era inevitable que se explorasen relaciones más o menos ocultas entre distintos naturales. Se desarrollaron así nociones como la de *número perfecto*: n es perfecto si es igual a la suma de todos sus divisores propios, es decir, aquellos divisores estrictamente menores que n.

El número perfecto más pequeño es $6 = 1 + 2 + 3$. Euclides probó que si $2^\alpha - 1$ es primo, entonces $2^{\alpha-1}(2^\alpha - 1)$ es perfecto. Por su parte, Euler demostró que todo número perfecto par tiene esta forma (mencionamos que si $2^\alpha - 1$ es primo

2000 *Mathematics Subject Classification.* 11–01.
Key words and phrases. Number Theory.
La investigación del primer autor está subvencionada por el proyecto BFM2000-0206-C04-03 de la DGI y la ayuda API-01/B38 de la UR.
La investigación del segundo autor está subvencionada por el proyecto BFM2000-0026 de la DGI.

entonces α también lo es; esta condición con frecuencia se añade en los textos a la caracterización precedente). Por tanto, los perfectos pares se conocen perfectamente, valga la redundancia, pero de los perfectos impares ni siquiera se sabe si existe alguno.

Si la respuesta al problema anterior es positiva, entonces quizá se resuelva mediante el uso de ordenadores, los cuales han tenido ya una incidencia considerable como medio de someter conjeturas a pruebas diversas. Con frecuencia los matemáticos actúan como el rey del cuento, que disparaba una flecha, y allá donde hubiese caído colocaba la diana. De modo que si un problema no sale, siempre se puede cambiar más o menos ligeramente hasta que se obtenga algún resultado, o bien hasta que se convierta en una conjetura o problema distinto. De esta forma nuevos conceptos y definiciones van desarrollándose. En relación a los números perfectos, mencionamos las siguientes variantes. Sea $s(n)$ la suma de los divisores propios de n, para $n > 1$. Con esta notación n es perfecto si $s(n) = n$. Además, decimos que los números m y n son *amigos* si $s(m) = n$ y $s(n) = m$, y finalmente que $n_1, \ldots, n_k$ son *sociables* si $s(n_1) = n_2, \ldots, s(n_{k-1}) = n_k, s(n_k) = n_1$. Definamos $S_1(n) = s(n)$, y para $k \geq 1$, $S_{k+1}(n) = s(S_k(n))$. La conjetura de Catalan-Dickson afirma lo siguiente:

Para todo n, la sucesión $\{S_k(n)\}_{k=1}^{\infty}$ contiene tan solo un número finito de términos distintos.

Es decir, o bien la sucesión termina al ser $S_k(n)$ primo para algún k, en cuyo caso $S_{k+1}(n) = 1$ y el siguiente término no esta definido, o bien la sucesión cae en un ciclo de números amigos o sociables. El número más pequeño para el que se desconoce si la sucesión anterior contiene infinitos términos distintos o no es 276. Resultados obtenidos mediante el uso de ordenadores en este tema, así como información adicional, pueden hallarse en [3, 2].

Vemos pues que algunos problemas de Teoría de Números han despertado interés desde los albores de nuestra civilización, mostrando en ocasiones considerable resistencia a los ataques, primero de la razón pura, y últimamente de la razón asistida por el silicio.

Las distintas secciones de este trabajo, aunque relacionadas entre sí, han sido escritas de modo que puedan leerse independientemente unas de otras, y en el orden que el lector desee.

2. Los números primos

Las dos «realidades fundamentales» sobre los primos son: (i) que hay muchos, y (ii) que son escasos. O más precisamente, su número es infinito pero su densidad o frecuencia es cero. En general usaremos p para denotar a un primo arbitrario.

Sería concebible a priori que bastase una cantidad finita de primos para, tomando productos, obtener todos los naturales. Como es bien sabido, la primera demostración de que este no es el caso se debe a Euclides, quien notó que dados los N primeros primos $p_1, \ldots, p_N$, debe haber otro en el intervalo $(p_N, p_1 p_2 \cdots p_N + 1]$, ya que el extremo superior no es divisible por ninguno de los números $p_1, \ldots, p_N$.

Este argumento puede reusarse, con variaciones menores, para obtener resultados análogos sobre primos en determinadas progresiones aritméticas. Por ejemplo, para ver que existen infinitos primos de la forma $4n+3$, dados los N primeros primos $p_1, \ldots, p_N$ en la sucesión $\{4n+3\}_{n=0}^{\infty}$, existe al menos otro más en el intervalo $(p_N, 4p_1p_2\cdots p_N - 1]$, puesto que $4p_1p_2\cdots p_N - 1$ debe tener algún divisor primo de la forma $p = 4k+3$.

La prueba más «original» que conocemos sobre la infinitud de los primos se debe a Furstenberg ([8]): declaramos abiertos básicos en $\mathbb{Z}$ a las sucesiones aritméticas (junto con el vacío), y consideramos la topología generada por dicha base. Cada sucesión aritmética, además de un abierto, también es un conjunto cerrado, al ser su complementario unión finita de sucesiones aritméticas. Si el número de primos es finito, entonces la unión sobre todos los primos $\cup_p\{np : n \in \mathbb{Z}\}$ es un cerrado, luego su complementario $\{1, -1\}$ es abierto, lo que contradice el hecho de que los abiertos básicos no vacíos son infinitos.

La demostración de Euclides nos proporciona un intervalo de longitud finita en el que necesariamente encontraremos un nuevo primo. Usando argumentos más complicados, se puede reducir el tamaño de dicho intervalo. Así, el postulado de Bertrand nos dice que entre n y $2n$ siempre hay un primo, y el postulado generalizado de Bertrand, que para todo $\varepsilon > 0$ existe un $N(\varepsilon)$ tal que si $m > N(\varepsilon)$, entonces hay un primo entre m y $(1+\varepsilon)m$. El postulado generalizado de Bertrand es consecuencia directa del Teorema de los Números Primos, que enunciaremos más adelante.

Otra prueba de la infinitud de los primos fue dada por Euler, quien demostró el resultado más fuerte

$$\sum_p \frac{1}{p} = \infty.$$

La considerable importancia histórica de este teorema se debe fundamentalmente a que, para obtenerlo, Euler definió la siguiente función:

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \text{donde} \quad s \in (1, \infty),$$

probando la fórmula producto

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1},$$

que revela la conexión entre ζ y los números primos.

De hecho, la conexión es mucho más profunda de lo que aparece a primera vista. Riemann reinterpretó $\zeta(s)$ como función de una variable compleja s. La serie es claramente convergente en $\{\Re s > 1\}$, y Riemann demostró que tal función puede extenderse analíticamente a $\mathbb{C} \setminus \{1\}$, conjeturando que:

Todos los ceros de ζ en la banda crítica $\{0 \leq \Re s \leq 1\}$ se encuentran sobre la recta $\{\Re s = 1/2\}$.

Esta es la celebrada Hipótesis de Riemann, considerada por muchos el problema abierto más importante de todas las Matemáticas, y por cuya resolución el Instituto Clay ofrece un millón de dólares. Para los jóvenes hay otro premio: una medalla.

De la fórmula producto de Euler, válida en $\{\Re s > 1\}$, se deduce fácilmente que ζ no se anula en $\{\Re s > 1\}$. Tomando límites desde la derecha, puede verse (pero no fácilmente, la prueba es muy astuta) que tampoco se anula sobre $\{\Re s = 1\}$, lo cual implica el Teorema de los Números Primos. La demostración en 1896 de que ζ no tiene ceros en $\{\Re s = 1\}$ sirvió a Hadamard y a de la Vallée Poussin para alcanzar la inmortalidad (matemática).

Sea $\pi(x)$ el número de primos menores o iguales que x. La Hipótesis de Riemann, de ser cierta, implicaría que las desviaciones de $\pi(x)$ con respecto a la fórmula asintótica dada por el Teorema de los Números Primos, son «las mínimas posibles». Pero de momento, ni siquiera se ha conseguido probar la existencia de algún $\varepsilon > 0$ tal que ζ esté libre de ceros en $\{\Re s > 1 - \varepsilon\}$.

Por lo que se refiere a la segunda «realidad fundamental» sobre los primos, claramente cuanto mayor es un número natural, menor es la «probabilidad» de que sea primo, al tener por debajo más potenciales divisores. Demostramos a continuación que la frecuencia de los primos entre n y $2n$ tiende a cero cuando n tiende a infinito, es decir, que

$$\lim_{n\to\infty} \frac{\pi(2n) - \pi(n)}{n} = 0.$$

Una estimación muy conocida, que resulta útil tanto para probar el postulado de Bertrand como el propio Teorema de los Números Primos, es la siguiente: puesto que cada primo p tal que $n < p \leq 2n$ divide al numerador del coeficiente binomial $\binom{2n}{n}$ pero no al denominador, tenemos que $\prod_{n<p\leq 2n} p$ divide a $\binom{2n}{n}$, luego

$$n^{\pi(2n)-\pi(n)} < \prod_{n<p\leq 2n} p \leq \binom{2n}{n} \leq (1+1)^{2n} = 2^{2n}.$$

Tomando logaritmos se obtiene

$$(\pi(2n) - \pi(n)) \log n < 2n \log 2,$$

de donde se sigue que el límite anterior es cero. Como veremos a continuación, de aquí se deduce fácilmente que

$$\lim_{n\to\infty} \frac{\pi(n)}{n} = 0$$

(resultado que también puede obtenerse directamente modificando, con un poco más de esfuerzo, el argumento anterior). Siendo la diferencia entre

$$\frac{\pi(2n)}{2n} \qquad \text{y} \qquad \frac{\pi(2n+1)}{2n+1}$$

despreciable para n grande, claramente

$$\limsup_{n\to\infty} \frac{\pi(n)}{n} = \limsup_{n\to\infty} \frac{\pi(2n)}{2n},$$

puesto que el lado izquierdo tan solo se distingue del derecho en que no consideramos enteros impares en este último. Por otra parte,

$$2 \limsup \frac{\pi(2n)}{2n} = \limsup \frac{\pi(2n)}{n}$$
$$\leq \limsup \frac{\pi(2n) - \pi(n)}{n} + \limsup \frac{\pi(n)}{n}$$

$$= \limsup \frac{\pi(n)}{n} = \limsup \frac{\pi(2n)}{2n},$$

luego todos los límites existen y valen cero.

El Teorema de los Números Primos nos proporciona la conducta asintótica de $\pi(x)$:

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1.$$

En vez de usar

$$\frac{x}{\log x}$$

para aproximar $\pi(x)$, puede emplearse el logaritmo integral

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

en general con mejores resultados (es fácil comprobar que $\frac{x}{\log x}$ y $\mathrm{Li}(x)$ son asintóticamente equivalentes). De hecho, la Hipótesis de Riemann es equivalente a la siguiente versión óptima del Teorema de los Números Primos:

$$\pi(x) = \mathrm{Li}(x) + O(x^{1/2}\log x).$$

Se sabe que el error no puede ser menor.

Mencionamos por último la siguiente acotación explícita para el enésimo primo p_n: Si $n > 1$, entonces

$$n\log n + n(\log\log n - 10) < p_n < n\log n + n(\log\log n + 8);$$

y comenzando con valores más altos de n, las constantes -10 y 8 pueden sustituirse por otras mejores.

El lector interesado en proseguir más allá encontrará buena parte de lo que aquí se ha relatado en los libros de texto habituales de Teoría de Números, mientras que para resultados más especiales sobre los primos, hemos usado (y recomendamos) [11]. La mejor demostración que conocemos del Teorema de los Números Primos es la versión de D. Zagier de la prueba de D. J. Newman (véase [12]). No nos cabe duda de que en el futuro reemplazará a las que hoy en día pueden hallarse en los libros de texto.

3. La función ϕ de Euler

Además de la distribución de los primos, nos interesa conocer qué sucede con los números que son coprimos con un entero positivo dado. La función ϕ de Euler $\phi(n)$ cuenta el número de enteros positivos menores o iguales que n y primos con n. Naturalmente, a la hora de probar resultados interesa no una descripción verbal como la anterior, sino una fórmula que nos dé el valor de ϕ sobre cada $n \geq 1$. Tal fórmula es

$$\phi(n) = n\prod_{p\mid n}\left(1 - \frac{1}{p}\right), \tag{1}$$

con la convención de que el producto vacío vale 1.

Como sucede con otras funciones aritméticas, la conducta de ϕ es irregular y en ocasiones difícil de predecir. Parece intuitivamente claro, y además es cierto, que cuando $n \to \infty$ lo mismo ocurre con $\phi(n)$: números grandes tienen muchos coprimos por debajo. Pero naturalmente hay muchas formas de acercarse al infinito, y puede interesarnos averiguar cómo lo hace $\phi(n)$.

Por ejemplo, planteémonos la pregunta:

¿Existe algún entero positivo n tal que $\phi(n) > \phi(6n)$?

Pudiera pensarse que dado que $6n$ es «bastante más grande» que n, simplemente por «fuerza bruta» $6n$ tendrá más coprimos por debajo que n, es decir, que la desigualdad contraria $\phi(n) < \phi(6n)$ es cierta. Además, un examen de lo que sucede para valores pequeños de n refuerza esta conjetura.

¿Pero qué ocurre si n es «grande»? La fórmula (1) requiere conocer la factorización en primos de n, lo que para naturales arbitrarios de, digamos, 200 dígitos o más, está completamente fuera del alcance de los algoritmos existentes hoy en día (en esta falta de algoritmos eficientes de factorización se basan los métodos modernos de criptografía). De modo que una estrategia puramente computacional deja de funcionar cuando n pasa del centenar largo de dígitos. Pero dado que la diferencia $6n - n$ tiende a infinito cuando $n \to \infty$, si n es grande, esperamos que suceda lo mismo que cuando n es pequeño, y «con mayor razón».

De hecho, las anteriores consideraciones apuntan en el camino correcto. Puede verse, por aplicación directa de (1), que efectivamente $\phi(n) < \phi(6n)$ para todo n. Ahora bien,

¿qué sucede si comparamos $\phi(6n)$ con $\phi(6n+1)$?

En este caso el tamaño de $6n$ y $6n+1$ es parejo, siendo su diferencia la mínima posible, de modo que cabe esperar que se produzcan oscilaciones en la desigualdad. Y efectivamente así ocurre: la desigualdad cambia de sentido un número infinito de veces. Pero entonces, si lo que sospechamos resulta ser cierto, ¿en qué consiste la dificultad de la que hablábamos al principio de este párrafo? En que la evidencia numérica para valores pequeños de n puede resultar engañosa: hemos comprobado, mediante un sencillo programa de ordenador, qué sucede con cada $n \leq 335\,000\,000$, y en cada caso se verifica que $\phi(6n) < \phi(6n+1)$ (no se conoce el número más pequeño para el cual la desigualdad se invierte, aunque determinarlo tampoco debería resultar excesivamente complicado).

Si comparamos $\phi(30n)$ con $\phi(30n+1)$, de nuevo la evidencia numérica parece sugerir que la desigualdad $\phi(30n) < \phi(30n+1)$ siempre se cumple. De hecho, G. Martin ha determinado el menor n tal que $\phi(30n) > \phi(30n+1)$: es del orden de 2.329×10^{1115}. En estos dos casos el tamaño de las sucesiones aritméticas empleadas es similar, con lo que a priori no hay razones para conjeturar que el valor de ϕ sobre una de ellas dominará siempre su valor sobre la otra. ¿Qué pasa si utilizamos, por ejemplo, n y $6n+1$? Computaciones realizadas por María Iriarte, estudiante de Licenciatura en la Universidad de La Rioja, muestran que para toda $n \leq 10^{10\,000}$ tenemos $\phi(n) < \phi(6n+1)$. Empleando coeficientes más grandes, encontramos que para toda $n \leq 10^{10\,000\,000}$, se verifica $\phi(210n) < \phi(6\,469\,693\,230n + 31)$.

Y sin embargo, en todos los ejemplos anteriores la desigualdad se invierte un número infinito de veces, como consecuencia del siguiente teorema de D. J. Newman sobre la conducta de ϕ en sucesiones aritméticas:

Sean a, b, c, d, enteros no negativos tales que $a, c > 0$. Si $ad - bc \neq 0$, entonces para infinitos valores de n,

$$\phi(an + b) < \phi(cn + d).$$

De hecho, una versión más fuerte de este resultado también es cierta:

Sean a, b, c, d enteros no negativos tales que $a, c > 0$. Entonces existe una sucesión $\{n_k\}$ tal que

$$\lim_k \frac{\phi(an_k + b)}{\phi(cn_k + d)} = 0 \qquad (2)$$

si y sólo si $ad - bc \neq 0$.

La idea básica de por qué este sorprendente resultado es válido, puede ilustrarse de modo sencillo utilizando un par concreto de sucesiones aritméticas: tomamos $\{cn + d\} = \{2n\}$ y $\{an + b\} = \{2n + 1\}$. Para escoger n_k nos interesa que en términos relativos el numerador sea lo más pequeño posible. Dado que

$$\frac{\phi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

y que cada factor en el lado derecho es menor que uno, escogemos n con el máximo posible de divisores primos, y estos tan pequeños como podamos. En nuestro caso concreto, puesto que $\{2n + 1\}$ es impar, tomamos

$$2n_k + 1 := \prod_{i=2}^{k} p_i.$$

La fórmula producto de Euler nos dice que

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{i=1}^{\infty} \left(1 - \frac{1}{p_i^s}\right)^{-1}.$$

Haciendo que $s \to 1$ concluimos que

$$\infty = \prod_{i=1}^{\infty} \left(1 - \frac{1}{p_i}\right)^{-1},$$

o equivalentemente, que

$$\prod_{i=1}^{\infty} \left(1 - \frac{1}{p_i}\right) = 0,$$

obteniéndose el mismo resultado si el producto comienza con cualquier otro índice distinto de 1. Por tanto,

$$\lim_k \frac{\phi(2n_k + 1)}{2n_k + 1} = \prod_{i=2}^{\infty} \left(1 - \frac{1}{p_i}\right) = 0.$$

Como

$$\lim_k \frac{\phi(2n_k + 1)}{\phi(2n_k)} = \lim_k \frac{\frac{\phi(2n_k+1)}{2n_k+1}}{\frac{\phi(2n_k)}{2n_k}},$$

basta comprobar que el denominador está acotado inferiormente por un número estrictamente positivo. Ahora bien, ¿qué primos dividen a $2n_k = \prod_{i=2}^{k} p_i - 1$? Evidentemente 2 es uno de ellos. Si $q > 2$ es primo y divide a $\prod_{i=2}^{k} p_i - 1$, entonces $q > p_k$. Por consideraciones evidentes de tamaño, no puede haber más de k primos q con esta propiedad, de donde se sigue que

$$\frac{\phi(2n_k)}{2n_k} = \prod_{q|2n_k} \left(1 - \frac{1}{q}\right) \geq \frac{1}{2}\left(1 - \frac{1}{p_k}\right)^k \geq \frac{1}{2}\left(1 - \frac{1}{p_k}\right)^{p_k}.$$

La prueba concluye notando que esta última expresión tiende a $(2e)^{-1}$ cuando $k \to \infty$.

Probablemente sea posible demostrar un resultado aún más fuerte. No es particularmente complicado verificar que si $ad - bc = 0$, entonces el cociente

$$\frac{\phi(an+b)}{\phi(cn+d)}$$

toma sólo un número finito de valores cuando n recorre los enteros positivos. Creemos, aunque de momento su demostración nos ha eludido, que la siguiente afirmación es cierta: si $ad - bc \neq 0$, entonces la sucesión

$$\left\{\frac{\phi(an+b)}{\phi(cn+d)}\right\}_{n=1}^{\infty}$$

es densa en $[0, \infty)$.

Naturalmente, existen abundantes problemas abiertos sobre la conducta de ϕ. Dos conjeturas relacionadas entre sí, una de las cuales ha sido resuelta recientemente, son las de Sierpiński y Carmichael. Sea n un entero positivo. Carmichael conjeturó que:

Si la ecuación $\phi(x) = n$ tiene una solución, entonces tiene al menos dos soluciones.

Es decir, para ningún entero positivo n se da el caso que $\phi(x) = n$ tenga exactamente una solución. Kevin Ford ha demostrado que no hay contraejemplos por debajo de $10^{10\,000\,000\,000}$, pero en principio nada excluye que los haya por encima de esa cifra.

Por su parte, Sierpiński conjeturó que:

Para todo $k > 1$ existe un n tal que la ecuación $\phi(x) = n$ tiene exactamente k soluciones.

Recientemente Kevin Ford ha probado que la conjetura de Sierpiński es cierta.

En esta sección aprovechamos para citarnos: la prueba de (2) en el caso general aparece en [1]. El resultado de D. J. Newman se publicó en [5], y la determinación del entero más pequeño que satisface $\phi(30n) > \phi(30n+1)$, en [4]. Para las conjeturas de Sierpiński y Carmichael nos remitimos a los artículos originales de Kevin Ford [6] y [7].

4. La conjetura *abc*

Describimos en esta última sección la que, según Serge Lang, es una de las mejores conjeturas del siglo.

Consideremos dos enteros coprimos a y b, tales que cada uno de ellos tiene pocos factores primos, por ejemplo 2^n y 3^m, con n y m grandes. Entonces $a+b$ también es coprimo con a y con b. Aparte de eso ¿es posible decir algo interesante sobre la factorización de $a+b$ en primos? Veamos algunos ejemplos concretos:

$$2^{10}+3^{10} = 13 \times 4621$$
$$2^{20}+3^{20} = 41 \times 97 \times 281 \times 3121$$
$$2^{30}+3^{30} = 13 \times 61 \times 2341 \times 4621 \times 24001$$
$$2^{40}+3^{40} = 17 \times 401 \times 1783433557073281$$
$$2^{50}+3^{50} = 13 \times 4621 \times 11701 \times 9802501 \times 104189401$$
$$2^{94}+3^{90} = 8727963568087732232932026045561125726029033$$
$$2^{100}+3^{100} = 41 \times 97 \times 281 \times 3121 \times 742801 \times 20017001 \times 9937984196743741414107401.$$

Observamos que, al contrario de lo que sucede con a y b, los factores primos de $a+b$ aparecen con exponentes muy bajos (en los ejemplos anteriores, con exponente 1). De modo que se verifica la desigualdad

$$a+b \leq \prod_{p|ab(a+b)} p.$$

En el caso general no cabe esperar una acotación tan simple, al ser posible que algún factor primo de $a+b$ aparezca con potencia mayor que 1. Pero una acotación del tipo

$$a+b \leq K \Bigg(\prod_{p|ab(a+b)} p \Bigg)^{1+\varepsilon},$$

donde $\varepsilon > 0$ y K es una constante, sí resulta verosímil. En esencia este es el contenido de la conjetura *abc*. El nombre viene de que en vez de emplearse a, b, y $a+b$, la conjetura se suele enunciar de forma más simétrica:

Supongamos que los enteros a, b, c son coprimos dos a dos y satisfacen $a+b+c=0$. Entonces para todo $\varepsilon > 0$ existe una constante $K(\varepsilon)$, dependiente de ε pero no de a y b, tal que

$$\max\{|a|, |b|, |c|\} \leq K(\varepsilon) \Bigg(\prod_{p|abc} p \Bigg)^{1+\varepsilon}.$$

Como se ve, de ser cierta la conclusión, nos proporcionaría información fundamental sobre la factorización de sumas de enteros en primos. No es pues sorprendente que resulte útil para abordar el problema de la existencia o no de soluciones de ecuaciones diofánticas. Por ejemplo, la versión débil de la conjetura *abc* que se obtiene al reemplazar «para todo $\varepsilon > 0$» por «existe un $\varepsilon > 0$», implica la siguiente versión débil del Teorema de Fermat-Wiles:

Existe una constante $M(\varepsilon)$ tal que, para todo $n \geq M(\varepsilon)$, la ecuación $x^n + y^n = z^n$ carece de soluciones no triviales en enteros.

Veamos cómo deducir esta versión de la conjetura débil *abc*. Decir que $x^n + y^n = z^n$ carece de soluciones no triviales en enteros es claramente equivalente a decir que carece de soluciones en enteros positivos. Supongamos que los enteros positivos x, y

y z satisfacen $x^n + y^n = z^n$. Hemos de probar que existe un $M(\varepsilon)$ tal que $n < M(\varepsilon)$, es decir, que n está acotada (en el Teorema de Fermat-Wiles la cota explícita es 3).

Cancelando factores comunes si los hubiera, podemos asumir que x, y y z son coprimos dos a dos. Usando la conjetura débil tenemos que existe un $\varepsilon > 0$ tal que

$$z^n \le K(\varepsilon)\Bigg(\prod_{p \mid x^n y^n z^n} p\Bigg)^{1+\varepsilon} = K(\varepsilon)\Bigg(\prod_{p \mid xyz} p\Bigg)^{1+\varepsilon}$$
$$\le K(\varepsilon)\,(xyz)^{1+\varepsilon} < K(\varepsilon)\,\big(z^3\big)^{1+\varepsilon}.$$

Dado que $z \ge 2$, tomando logaritmos tenemos que las únicas soluciones posibles se obtienen cuando

$$n < 3(1+\varepsilon) + \frac{\log K(\varepsilon)}{\log z} \le 3(1+\varepsilon) + \frac{\log K(\varepsilon)}{\log 2} =: M(\varepsilon),$$

como queríamos demostrar.

Si bien este resultado es más débil que el de Wiles, la técnica empleada también resulta útil al estudiar ecuaciones diofánticas donde la conexión con las curvas elípticas no existe, y por tanto los métodos de Wiles son inaplicables.

La conjetura *abc* se debe a Masser y Oesterle (1985). Históricamente surgió a partir de un resultado análogo para polinomios, el Teorema de Mason-Stothers, probado primero por Stothers (1981) e independientemente por Mason (1983). Información adicional sobre la conjetura puede hallarse, por ejemplo, en [9] y [10].

Referencias

[1] J. M. Aldaz, A. Bravo, S. Gutiérrez y A. Ubis, A theorem of D. J. Newman on Euler's ϕ function and arithmetic progressions, *Amer. Math. Monthly* **108** (2001), 364–367.

[2] M. Benito, W. Creyaufmüller, J. L. Varona y P. Zimmermann, Aliquot sequence 3630 ends after reaching 100 digits, *Experiment. Math.*, por aparecer.

[3] M. Benito y Juan L. Varona, Advances in aliquot sequences, *Math. Comp.* **68** (1999), 389–393.

[4] G. Martin, The smallest solution of $\phi(30n+1) < \phi(30n)$ is ..., *Amer. Math. Monthly* **106** (1999), 449–451.

[5] D. J. Newman, Euler's ϕ function on arithmetic progressions, *Amer. Math. Monthly* **104** (1997), 256–257.

[6] K. Ford, The distribution of totients, *Ramanujan J.* **2** (1998), 67–151.

[7] K. Ford, The number of solutions of $\phi(x) = m$, *Ann. of Math. (2)* **150** (1999), 283–311.

[8] H. Furstenberg, On the infinitude of primes, *Amer. Math. Monthly* **62** (1955), 353.

[9] S. Lang, Old and new conjectured Diophantine inequalities, *Bull. Amer. Math. Soc. (N.S.)* **23** (1990), 37–75.

[10] M. Nathanson, *Elementary methods in number theory*, Graduate Texts in Mathematics **195**, Springer-Verlag, Nueva York, 2000.

[11] P. Ribenboim, *The new book of prime number records*, Springer-Verlag, Nueva York, 1996.

[12] D. Zagier, Newman's short proof of the prime number theorem, *Amer. Math. Monthly* **104** (1997), 705–708.

Departamento de Matemáticas y Computación, Universidad de La Rioja, Edificio Vives, Calle Luis de Ulloa s/n, 26004 Logroño, Spain
Correo electrónico: aldaz@dmc.unirioja.es

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109-1109, USA
Correo electrónico: anabz@math.lsa.umich.edu