Un millón de casos no bastan: hace falta una demostración*

Juan Luis Varona

1. Introducción

El objetivo de este artículo es dar una recopilación de ejemplos de propiedades matemáticas que parece que van a ser ciertas siempre, pues hay muchos casos que así lo indican, pero que finalmente fallan. En la figura 1, cualquiera podría decir a simple vista que todos los números son pares, pero para darse cuenta de que es falso hay que tener mucho más cuidado.

90	24	10	70	80	40	36	88	88	72	56	86	74	66	66	84	56	50
44	84	62	66	60	80	92	56	26	32	16	74	76	70	68	50	96	16
46	80	88	10	42	10	42	72	18	36	14	46	74	38	76	44	70	20
54	94	16	94	74	18	36	42	92	62	52	98	98	94	12	60	30	48
84	50	88	62	20	94	70	36	92	10	50	78	32	76	12	98	10	54
18	88	44	96	98	46	84	98	84	60	78	80	98	46	80	52	62	82
90	72	58	10	10	82	46	54	80	16	86	12	98	14	22	94	22	26
54	26	28	42	14	34	12	38	86	56	12	30	69	86	56	66	48	58
54	40	50	16	36	68	74	96	66	78	36	96	42	82	32	52	86	68
72	46	40	12	46	94	76	46	60	54	34	90	88	40	92	90	14	10
92	18	22	52	16	18	52	18	68	96	94	38	58	80	98	28	38	90

Figura 1: Descubre el número impar.

Casi todos los ejemplos que veremos provienen de la teoría de números. A diferencia de lo que ocurre en otras partes de las matemáticas, en teoría de números hay numerosos problemas abiertos cuyo enunciado es fácil de comprender para los no especialistas; esto permite, a menudo, mostrar a los no matemáticos que las matemáticas no son una ciencia acabada, y que la investigación en matemáticas es claramente algo real. Del mismo modo, también es relativamente sencillo mostrar ejemplos no sofisticados de tendencias que, de pronto, se rompen. No podemos dejar de citar que, en palabras de Gauss, la teoría de números es la Reina de las

*Este artículo ha sido publicado (el 25 de septiembre de 2024) en *MATerials MATemàtics* **2024** (2024), no. 6, 35 pp.; `https://mat.uab.cat/web/matmat/wp-content/uploads/sites/23/2024/09/v2024n06.pdf`

Matemáticas; lamentablemente, casi ni existe en los planes de estudio actuales de las titulaciones de matemáticas en las universidades españolas.

No es difícil darse cuenta de que, en el mundo real, este tipo de cosas sólo nos preocupan a los matemáticos. Eso lo pone de manifiesto, de forma magistral, una de las tiras cómicas de *Spiked Math*. Estas tiras cómicas recuerdan a las de *xkcd*, que se pueden encontrar en `http://www.xkcd.com` y son bastante más conocidas. El lector puede disfrutar con ambas; lamentablemente, la página web de *Spiked Math* ya no funciona, pero sus tiras se pueden encontrar, reproducidas, en numerosos sitios.[1] A diferencia de *xkcd*, que es más general, todas las tiras de *Spiked Math* tienen temática matemática. Ambas tienen su propio patrón muy reconocible en cuanto al diseño gráfico de los personajes que intervienen. En *xkcd* los personajes son muy esquemáticos, figuras de palo (líneas sin grosor), y la cabeza un redonchel[2] sin nada dentro; en *Spiked Math*, los cuerpos de las personas siempre tienen forma triangular, y más detalles en el dibujo. Además, *xkcd* no usa colores, al contrario que las tiras de *Spiked Math* que sí están coloreadas.

Volviendo a la diferente concepción del rigor y los errores entre las distintas ciencias, en la figura 2 reproducimos la tira *World Annihilation*, aunque traducida al español. No vamos a cometer el error de explicar al lector su contenido.

Pero dejemos ya la introducción y vayamos a lo que nos interesa: mostrar ejemplos de que, en matemáticas, sin una demostración rigurosa nunca podemos estar seguros de que una propiedad sea cierta, por mucho que lo parezca. Sin una demostración, sólo tenemos un conjetura (de hecho, algunos de los ejemplos que aquí mostramos también aparecen en artículos con recopilaciones de conjeturas, como [13, § 10.1] y [14], aunque a nosotros nos interesan, fundamentalmente, las conjeturas que han sido resueltas en sentido negativo). A lo largo del artículo, a menudo nos iremos por las ramas de los diversos temas que tratemos, contando resultados relacionados.

2. Números primos y factorización de enteros

Vamos a comenzar viendo una serie de ejemplos relacionados con la búsqueda de números primos (en particular, primos de Fermat y primos de Mersenne), la factorización de números enteros y temas afines. Además, esto nos servirá como excusa para mostrar diversas propiedades relacionadas de indudable interés.

2.1. Primos de Fermat

No hace falta dar muchos detalles de quién era el francés Pierre de Fermat. Jurista de profesión y matemático por afición (lo cual no le impidió ser uno de los principales matemáticos de la primera mitad del siglo XVII), es muy conocido por

[1] Por ejemplo, la web completa de *Spiked Math* está archivada en `https://web.archive.org/web/20120628101305/http://spikedmath.com/`.

[2] Barriendo para casa: «redonchel» es un riojanismo que no aparece en el diccionario de la RAE. Si el lector no conocía la palabra, no le costará nada imaginarse su significado.

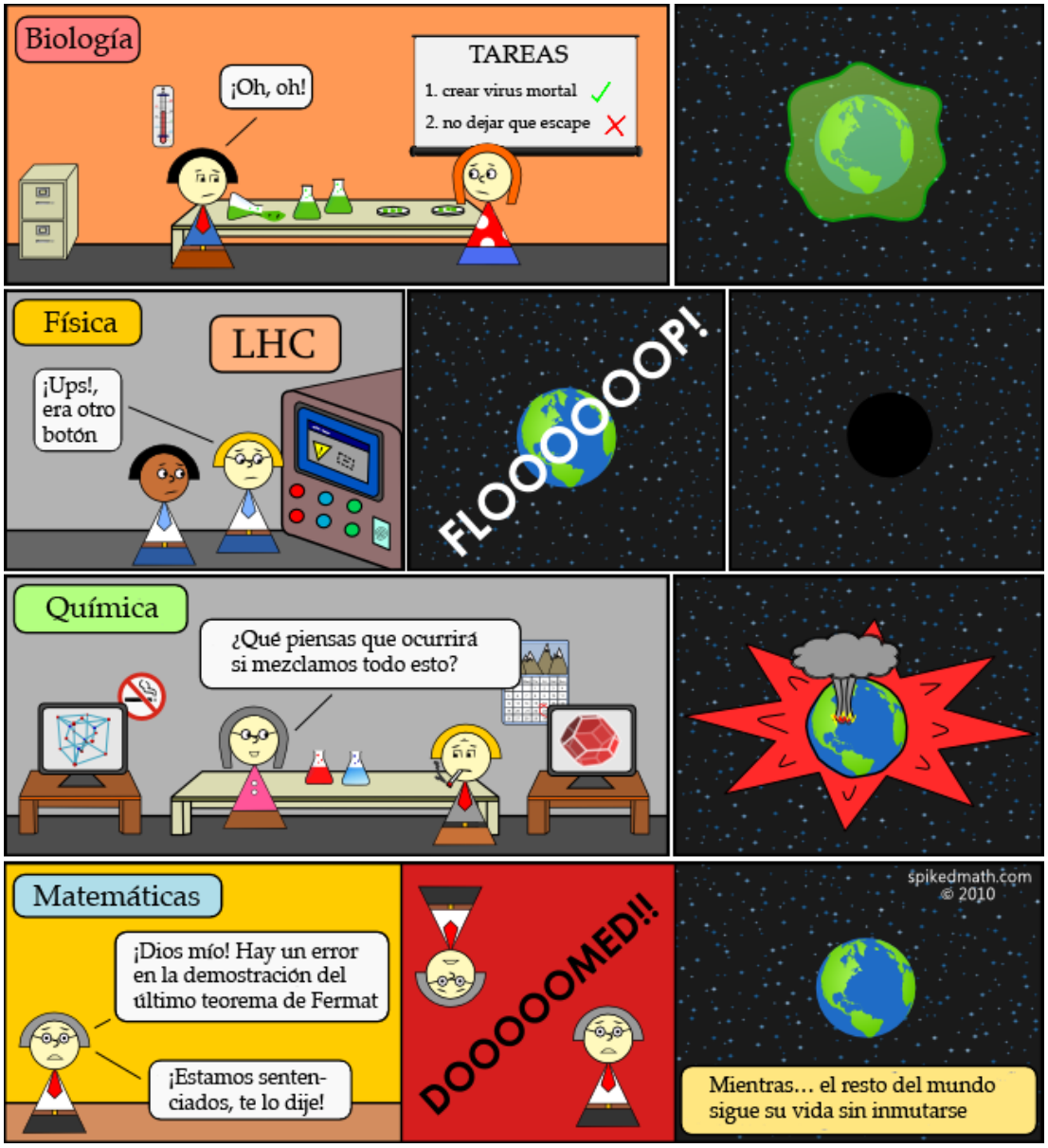


Figura 2: *World Annihilation* (Spiked Math, 183, 22 de febrero de 2010).

el denominado «último teorema de Fermat», que afirma que la ecuación $x^n + y^n = z^n$ no tiene soluciones enteras no nulas cuando el exponente n es un entero mayor o igual que 3. En 1637, en su ejemplar de la *Arithmetica* de Diofanto (editada por Claude Gaspard Bachet de Méziriac en 1621) que estaba leyendo, Fermat anotó en el margen que había encontrado una demostración maravillosa de ese hecho, pero que el margen era demasiado estrecho para escribirla. En realidad, ese resultado fue una conjetura abierta hasta 1995, que es cuando Andrew Wiles logró demostrarlo. En el intermedio, los intentos para probar la conjetura dieron lugar, en la práctica, a numerosos avances en diversos campos de las matemáticas.

Posiblemente ningún matemático actual piensa que la supuesta demostración de Fermat fuese correcta (él sí que proporcionó, años más tarde, una demostración

rigurosa del caso $n = 4$), pero no podemos estar seguros. Lo que sí es claro es que Fermat era demasiado optimista en algunas de sus afirmaciones, como vamos a ver a continuación.

Se llaman números de Fermat a los de la forma

$$F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, \ldots,$$

y si son primos se denominan primos de Fermat.

Es fácil demostrar que, para que $2^m + 1$ sea primo, forzosamente tiene que ser $m = 2^n$. En efecto, descompongamos

$$2^{rs} + 1 = (2^r)^s + 1 = x^s + 1$$

(donde hemos tomado $x = 2^r$); si s es impar, el polinomio $x^s + 1$ se anula con $x = -1$, luego es divisible por $x + 1$. En consecuencia, $2^m + 1$ no puede ser primo si m tiene un factor impar mayor que 1.

Los primeros números de Fermat son

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537,$$

y los cinco son primos. Ante esos ejemplos, Fermat conjeturó, en 1640, que todos los F_n eran primos (aunque admitió que no había conseguido probarlo).

Pasó casi un siglo hasta que se comprobó que la conjetura de Fermat no era cierta. En 1733, Leonhard Euler encontró la descomposición

$$F_5 = 2^{2^5} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417.$$

Hay que aclarar que no lo hizo dividiendo «a lo bruto» hasta encontrar un factor, sino que previamente probó algunos resultados matemáticos (condiciones necesarias para los posibles factores de los F_n) que le facilitaban el chequeo. Se pueden ver más detalles —tanto del procedimiento para factorizar F_5 como de lo que sigue en este apartado— en [35, § 3.4.1].

En realidad, no se conoce ningún F_n con $n > 4$ que sea primo, y muchos piensan que no habrá ninguno. Pero no hay ninguna seguridad al respecto.

Lo que sí hay es un test de primalidad «muy rápido» y sencillo para estos números, el denominado test de Pépin, desarrollado por el matemático (y sacerdote jesuita) francés Théophile Pépin en 1877. El test de Pépin afirma lo siguiente (su demostración, que aquí no vamos a abordar, usa la ley de reciprocidad cuadrática de Gauss):

Teorema. *Sea $F_n = 2^{2^n} + 1$ con $n \geq 1$. El número F_n es primo si y sólo si*

$$3^{(F_n - 1)/2} \equiv -1 \pmod{F_n}.$$

Con este test, y la ayuda de ordenadores, se ha conseguido demostrar, por ejemplo, que los números F_n no son primos para $5 \leq n \leq 32$ (ya hemos dicho que Euler encontró el factor 641 de F_5; además, Thomas Clausen encontró el factor

274 177 de F_6 en 1854, antes de que se conociera el test de Pépin). Se han encontrado algunos factores de muchos de estos F_n, pero actualmente no se conoce ningún factor de F_{20} o F_{24} (y sólo de F_5 a F_{11} se conoce la descomposición en factores completa). Encontrar factores de los números de Fermat es extremadamente complicado, pues $F_n = 2^{2^n} + 1$ crece muy rápido con n: el número de dígitos de F_n es

$$\left\lfloor \log_{10}\left(2^{2^n}+1\right)+1\right\rfloor \approx \left\lfloor \log_{10}\left(2^{2^n}\right)+1\right\rfloor = 1+\lfloor 2^n \log_{10}(2)\rfloor,$$

donde $\lfloor x \rfloor$ denota el mayor entero que es menor o igual que x. Pero hay algoritmos especializados para buscar factores primos de la forma $k \cdot 2^m + 1$. Hasta ahora, el mayor número de Fermat del que se ha encontrado un factor es $F_{18\,233\,954}$, y el factor es $7 \cdot 2^{18\,233\,956} + 1$; lo encontró R. Propper en 2020 con ayuda de *software* especializado desarrollado por Reynolds, Penné y Fougeron. Hay unas cuantas páginas web dedicadas en este tipo de retos.[3]

Quizás de manera sorprendente (de hecho, muy sorprendente si uno no ha oído hablar de ello), los números primos de Fermat están muy relacionados con la geometría. En efecto, se cumple lo siguiente:

Teorema. *Un polígono regular de M lados es construible con regla y compás si y sólo si*

$$M = 2^k p_1 p_2 \cdots p_n$$

con $k \geq 0$ y siendo los p_j primos de Fermat distintos.

Geométricamente, si sabemos construir un polígono regular, es inmediato construir otro con el doble de lados sin más que dividir un segmento por la mitad con regla y compás. Asimismo, si sabemos construir los polígonos regulares de r y s lados, con r y s primos entre sí, también es sencillo construir el de rs lados. En consecuencia, lo importante es discernir para qué primos p se puede construir —con regla y compás— el polígono regular de p lados. Los matemáticos de la Grecia clásica sabían construir los polígonos de 3 y 5 lados; desde entonces, no se había encontrado cómo construir ningún otro hasta que Carl Friedrich Gauss, en 1796 (con 19 años), encontró cómo construir el polígono regular de 17 lados.

Construir con regla y compás un polígono de M lados equivale a poder escribir $\cos(2\pi/M)$ (y $\operatorname{sen}(2\pi/M)$) mediante una combinación de sumas, restas, multiplicaciones, divisiones y raíces cuadradas de números enteros (ésas son las operaciones que se pueden realizar de manera exacta con regla y compás). En particular, y para el polígono regular de 17 lados, Gauss probó, en sus *Disquisitiones Arithmeticae* (escrito en 1798 y publicado por primera vez en 1801), que

$$\cos\left(\frac{2\pi}{17}\right) = \frac{-1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34-2\sqrt{17}} + \frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}.$$

[3]Por ejemplo, `http://www.prothsearch.com/fermat.html`.

En cuanto al teorema anterior tal como lo hemos enunciado, Gauss sólo demostró que la condición $M = 2^k p_1 p_2 \cdots p_n$ es suficiente. Que dicha condición también es necesaria lo probó Pierre Wantzel en 1836, utilizando técnicas de teoría de Galois. Con el mismo tipo de técnicas, Wantzel también probó la imposibilidad de la duplicación del cubo y de la trisección del ángulo, dos de los tres célebres problemas de la geometría clásica (el tercero, la cuadratura del círculo, no se resolvió, también en sentido negativo, hasta que Ferdinand von Lindemann probó la trascendencia de π en 1882).

2.2. Primos de Mersenne

Otros números «bonitos» cuya primalidad interesa a la comunidad matemática son los números de Mersenne, $M_n = 2^n - 1$. Para que M_n sea primo, el propio n tiene que ser primo, pues $2^{rs} - 1 = (2^r)^s - 1 = x^s - 1$ (estamos tomando $x = 2^r$), y el polinomio $x^s - 1$ es divisible por $x - 1$.

La primalidad de $2^p - 1$ para $p = 2$, 3, 5, 7 ya era conocida desde la época griega. Quizás se podría pensar que $2^p - 1$, con p primo, siempre es primo; pero esto es claramente falso, pues $2^{11} - 1 = 2047 = 23 \cdot 89$. La primalidad de $2^{13} - 1$ se conoce, al menos, desde 1456. Ya en 1588, Pietro Cataldi había verificado que $2^{17} - 1$ y $2^{19} - 1$ eran primos, y aventuró que lo mismo ocurría para $p = 23$, 29, 31 y 37. Se equivocó con 23, 29 y 37, como podemos ver sin más que dar sus descomposiciones en factores primos:

$$\begin{aligned} 2^{23} - 1 &= 8\,388\,607 = 47 \cdot 178\,481, \\ 2^{29} - 1 &= 536\,870\,911 = 233 \cdot 1103 \cdot 2089, \\ 2^{37} - 1 &= 137\,438\,953\,471 = 223 \cdot 616\,318\,177 \end{aligned}$$

(la primera y la tercera las encontró Fermat en 1640, y la segunda Euler en 1738, casi un siglo más tarde que las otras dos).

Es en 1644 cuando el monje francés Marin Mersenne entra en escena en relación a los números que ahora llevan su nombre. Mersenne afirmó que, para $p \leq 257$, el número $2^p - 1$ es primo si y sólo si $p = 2$, 3, 5, 7, 13, 17, 19, 31, 67, 127 o 257. Esa lista resultó incorrecta en ambos sentidos: algunos primos no están en ella, y algunos de los números que sí están no son primos. La lista correcta de primos de Mersenne para $p \leq 257$ no se completó hasta mediados del siglo XX, ya con ayuda de ordenadores: los valores de p para los que M_p es primo son $p = 2$, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 y 127 (el siguiente primo surge con $p = 521$).

Actualmente, se conocen 51 números de Mersenne primos y muchísimos más que se ha demostrado que no son primos, pero no se sabe si hay infinitos en ninguno de los dos casos. Con ayuda de ordenadores, se han encontrado primos de Mersenne enormes (de millones de dígitos). Y es que, como se puede ver en la figura 3, los números primos de Mersenne —y los primos grandes en general— tienen un halo misterioso que los hace muy atractivos.

Como ocurría con el test de Pépin para los números de Fermat, hay un test especializado y muy eficiente para comprobar si un número de Mersenne es pri-

Figura 3: Ejemplos de primos de Mersenne en un matasellos conmemorativo y en un sello.

mo. Es el donominado test de Lucas-Lehmer, que mostramos a continuación (se pueden ver más detalles en [35, § 3.4.3]):

Teorema. *Sea $M_p = 2^p - 1$ con p un primo impar, y definamos los números S_k de manera recurrente mediante*

$$S_0 = 4, \qquad S_{k+1} = S_k^2 - 4, \quad k \geq 0.$$

Entonces, el número M_p es primo si y sólo si $S_{p-2} \equiv 0 \pmod{M_p}$.

Fue Édouard Lucas, en 1876, el que ideó la versión original del test, y con él probó la primalidad de M_{127}. En la formulación dada por Lucas, el test estaba presentado de manera distinta a como se muestra ahora, que es un refinamiento posterior (de 1930) debido a Derrick Henry Lehmer.

La demostración del test de Lucas-Lehmer sólo es un poco más complicada que la del test de Pépin del apartado anterior, aunque sí requiere algunos requisitos técnicos adicionales. En lo que sí se diferencian es en que el de Lucas-Lehmer ha tenido mucho más éxito a la hora de encontrar números primos que el de Pépin. En realidad, esto no es muy sorprendente. El n-ésimo primo es, a grandes rasgos, del tamaño de $n\log(n)$ (aunque no necesitamos tanta precisión, que el cociente entre ambas cantidades tiende a 1 cuando $n \to \infty$ es equivalente al teorema de los números primos). Entonces, sin más que comparar el crecimiento de $n\log(n)$ con el de 2^n, nos damos cuenta de que, para un mismo tamaño de números (es decir, hasta el tamaño que los ordenadores y los algoritmos son capaces de manejar en cada momento), hay muchísimos más candidatos a ser primos entre los números de Mersenne que entre los números de Fermat.

Dado que el test de Lucas-Lehmer es muy rápido y efectivo, ha sido bastante habitual que, históricamente desde que Lucas probó el test en su primera versión, el mayor primo conocido casi siempre haya sido un M_p. Los primeros se encontraron efectuando operaciones con lápiz y papel. Pero, claro, desde que aparecieron los ordenadores, todos los récords de «el mayor primo conocido» han sido batidos con ayuda informática. Actualmente, hay páginas web dedicadas a ello, y que, en particular, proporcionan *software* altamente especializado.[4]

He aquí un esquema que resume algunos de los hitos históricos sobre el cálculo del mayor primo conocido en cada momento:

[4]Merece la pena destacar `https://www.mersenne.org/primes/`.

- Lucas, en 1876, demostró que $2^{127} - 1$ es primo. Tiene 39 dígitos, y fue el mayor primo conocido durante 75 años.

- En 1951, A. Ferrier, con la ayuda de una calculadora mecánica, probó que el número $(2^{148}+1)/17$ (con 44 dígitos) es primo; este número, el mayor que se ha encontrado sin ayuda electrónica, no es de Mersenne, y para probar que es primo utilizó el denominado test de Proth, que aquí no hemos enunciado pero es similar a los de Pépin o Lucas-Lehmer (véase [35, § 3.4.2]).

- Poco más tarde, ese mismo año, J. C. P. Miller y D. J. Wheeler inauguraron la extensa lista de primos encontrados con ordenador. Encontraron varios primos de la forma $k \cdot M_{127} + 1$ y un nuevo récord, $180M_{127}^2 + 1$, con 79 dígitos.

- El primer M_p primo encontrado con ordenador fue $2^{521}-1$ (con 157 dígitos). Lo halló Raphael Robinson en 1952, junto con M_{607}, M_{1279}, M_{2203} y M_{2281} (este último, con 687 dígitos).

- Desde entonces, salvo entre 1989 y 1992 con un primo de la forma $k \cdot 2^n - 1$ y 65 087 dígitos, el mayor primo conocido siempre ha sido un primo de Mersenne.

- Desde 1996 (ese año se probó la primalidad de $2^{1\,398\,269} - 1$, con 420 921 dígitos), todos los nuevos primos de Mersenne que se han encontrado (17 hasta ahora) lo han sido gracias al *Great Internet Mersenne Prime Search* (GIMPS), una búsqueda colaborativa desarrollada gracias a internet.[5]

- Actualmente, el último que se ha encontrado es $2^{82\,589\,933} - 1$ (tiene más de 24 millones de dígitos). Se halló con GIMPS en diciembre de 2018. Hasta entonces, se iban encontrado nuevos primos de Mersenne con un ritmo aproximado de uno anual, pero parece que este ritmo se ha interrumpido.

La Electronic Frontier Foundation ofrece recompensas económicas a los primeros individuos o grupos que descubran primos de determinados tamaños. Varios de estos premios han sido ya cobrados por participantes del GIMPS. Actualmente, están vigentes un premio de 150 mil dólares para los primeros que encuentren un primo de 100 millones de dígitos, y otro premio de 250 mil dólares por un primo de 1000 millones de dígitos.

Cuando hablábamos de números de Fermat, ya vimos que demostrar que un número no es primo no es lo mismo que encontrar un factor suyo (o que factorizarlo completamente como producto de primos). Salvo para números con divisores «pequeños», encontrar un factor de un número enorme es, en general, considerablemente más complicado que demostrar si el número es primo o no.

Por supuesto, lo mismo ocurre con los números de Mersenne y, a este respecto, resulta anecdótico el caso de M_{67}. Con el test de Lucas-Lehmer es sencillo probar que M_{67} es un número compuesto. Pero eso no proporciona sus divisores. En 1903,

[5] Dicha búsqueda está centralizada en `https://www.mersenne.org`.

Frank Cole, en una reunión de la American Mathematical Society (AMS), salió a la pizarra y, en silencio, se dedicó a efectuar multiplicaciones durante más de una hora hasta comprobar la siguiente igualdad:

$$193\,707\,721 \cdot 761\,838\,257\,287 = 2^{67} - 1;$$

la audiencia le premió con una gran ovación. Según él mismo explicó, había dedicado «tres años de domingos» a factorizar M_{67}. En memoria de Cole, y desde 1931, la AMS otorga el «Cole Prize in Number Theory»; actualmente, el premio se da cada tres años.

También para números enteros arbitrarios (no sólo para los números de formas especiales como los F_n o los M_p), factorizar enteros es —con lo que se sabe hacer hasta ahora— mucho más complicado que comprobar la primalidad, pero no hay ningún resultado que, de alguna forma, asegure cuánto. En 2002, Manindra Agrawal, Neeraj Kayal y Nitin Saxena encontraron un test de primalidad genérico en tiempo polinomial (polinomial en el número de dígitos), y que ahora se denomina test AKS, véase [2]. La publicación de ese artículo fue una enorme sorpresa para la comunidad matemática; en particular porque las matemáticas que utiliza el test AKS son mucho más sencillas que las que se utilizan en test genéricos previos cuya complejidad computacional es, asintóticamente, mayor que polinomial. No se conoce ningún algoritmo de factorización en tiempo polinomial, pero no se puede asegurar que no exista.

Por supuesto, esto tiene una importancia enorme en criptografía (la seguridad del método criptográfico RSA depende de la dificultad para factorizar enteros grandes), y el descubrimiento e implementación de un algoritmo rápido de factorización pondría en jaque una gran parte de la criptografía actual. Es lo que promete la computación cuántica, si alguna vez los ordenadores cuánticos de potencia adecuada llegan a existir. Pero dejemos este tema y volvamos a los primos de Mersenne.

En el apartado anterior vimos que los primos de Fermat estaban relacionados con los polígonos regulares construibles con regla y compas. Del mismo modo, los primos de Mersenne también tienen una relación inesperada; esta vez, con los números perfectos.

Un número se denomina perfecto cuando es la suma de sus divisores propios, por ejemplo:

$$6 = 1 + 2 + 3, \qquad 28 = 1 + 2 + 4 + 7 + 14.$$

Ya en los *Elementos* de Euclides (que fueron escritos a principios del siglo III a. C.) aparece un modo de encontrar números perfectos pares; y fue Euler quien demostró que todos surgen de esa manera. Como vemos a continuación, los números perfectos pares están íntimamente relacionados con los primos de Mersenne:

Teorema. *Un número n par es perfecto si y sólo si*

$$n = 2^{p-1}(2^p - 1)$$

con $M_p = 2^p - 1$ primo de Mersenne.

Que los números de esa forma son perfectos (lo que demostró Euclides) es bastante sencillo. En efecto, al ser $2^p - 1$ primo, los divisores de $n = 2^{p-1}(2^p - 1)$ (incluyendo el propio n) son 1, 2, 2^2, ..., 2^{p-1}, y $1 \cdot (2^p - 1)$, $2 \cdot (2^p - 1)$, $2^2 \cdot (2^p - 1)$, ..., $2^{p-1} \cdot (2^p - 1)$. Su suma (incluyendo n) es

$$\begin{aligned}\sigma(n) &= 1 + 2 + 2^2 + \cdots + 2^{p-1} + (1 + 2 + 2^2 + \cdots + 2^{p-1})(2^p - 1) \\ &= \frac{2^p - 1}{2 - 1} + \frac{2^p - 1}{2 - 1}(2^p - 1) = 2^p(2^p - 1) = 2n;\end{aligned}$$

así pues, la suma de los divisores propios de n es $\sigma(n) - n = n$, tal como queríamos comprobar. Que todos los números perfectos pares son de esa forma (lo que demostró Euler) es un poco más complicado. Se puede ver, por ejemplo, en [35, § 7.2].

No se sabe si hay números perfectos impares. Es, posiblemente, el problema abierto más antiguo de las matemáticas.

2.3. Funciones generadoras de primos

Todos conocemos que, para encontrar los números primos, basta usar la criba de Eratóstenes. Pero ¿hay alguna función que nos permita generar los números primos? Por supuesto, podríamos empaquetar el algoritmo de la criba de Eratóstenes en algo que podríamos denominar función, pero eso sería hacer trampas en un solitario. Así que, sin ser rigurosos respecto a lo que pretendemos, vamos a ser sensatos.

Lo que deseamos es encontrar alguna expresión que genere los primos. Y podemos pensar en ello con diferente grado de ambición. ¿Queremos algo que genere todos los números primos? ¿Una expresión que siempre genere números primos? (aunque no todos). Por supuesto, nos gustaría que fuese una expresión sencilla.

En 1772, Euler se dio cuenta de que el polinomio $x^2 + x + 41$ proporciona un número primo para $x = 0, 1, 2, \ldots, 39$. Pero ya no es un número primo si tomamos $x = 40$. Se pueden encontrar otros polinomios que dan más primos.

¿Existe un polinomio P tal que $P(n)$ sea primo para todo $n \in \mathbb{Z}$? (o para todo $n \geq n_0$). Sin duda, sería un polinomio muy bonito.

En 1752, Christian Goldbach se dio cuenta de que esto no era posible:

Teorema. *No existe ningún polinomio con coeficientes enteros P (no constante) tal que $P(n)$ sea primo para todo $n \in \mathbb{Z}$ (o para todo $n \geq n_0$).*

Goldbach es mucho más conocido por la «conjetura de Goldbach» (que enunció en 1742, en una carta dirigida a Euler): «Cada número par mayor que dos es suma de dos primos», que continúa abierta. Hasta donde se ha buscado con ordenador, la conjetura siempre se cumple, pero no existe ninguna demostración rigurosa.

Sí que se ha conseguido probar una versión más débil de dicha conjetura. En 2013, el matemático peruano Harald Helfgott probó que todos los impares mayores que 5 son suma de tres primos, lo que habitualmente se denominaba

«conjetura débil —o ternaria— de Goldbach». Se puede ver un esquema de su demostración en [18]. Como sus nombres sugieren, la conjetura «fuerte» implica la «débil»: si la conjetura fuerte estuviera probada, y tuviéramos un número n impar, $n-3$ sería par, luego suma de dos primos p y q por la conjetura fuerte; así que podríamos escribir $n = 3 + p + q$.

Volviendo al teorema anterior, y aunque ésta no es la demostración original de Goldbach, usando congruencias es fácil probar que tal polinomio $P(x)$ no puede existir:

Supongamos que ese polinomio $P(x)$ que genera primos para $n \geq n_0$ sí que existe. Elegimos un $a \in \mathbb{Z}$ (lo escogemos $\geq n_0$), y tomamos $p = P(a)$, que por hipótesis deberá ser primo. Cualquier $b \equiv a \pmod{p}$ verificará $P(b) \equiv P(a) \pmod{p}$, luego $P(b) \equiv p \pmod{p}$. Por hipótesis, $P(b)$ también es primo, así que forzosamente $P(b) = p$. Pero en la clase de a en $\mathbb{Z}_p$ existen infinitos elementos (todos los de la forma $b = a + kp$, $k \in \mathbb{Z}$, y son todos $\geq n_0$ cuando $k \geq 0$), luego el polinomio $Q(x) = P(x) - p$ tiene infinitas raíces, lo cual es imposible.

Dado que acabamos de ver que no hay polinomios que siempre generen números primos, ¿se puede conseguir de alguna otra manera? En este sentido, vamos a mostrar un par de resultados llamativos.

En 1951, Edward Maintland Wright probó lo siguiente:

Teorema. *Existe un número real $\alpha \in (1, 2)$ tal que los términos de la sucesión $\{\alpha_n\}_{n=0}^{\infty}$ definida —de manera recursiva— mediante*

$$\alpha_0 = \alpha, \quad \alpha_{n+1} = 2^{\alpha_n}, \quad n = 0, 1, 2, 3, \ldots$$

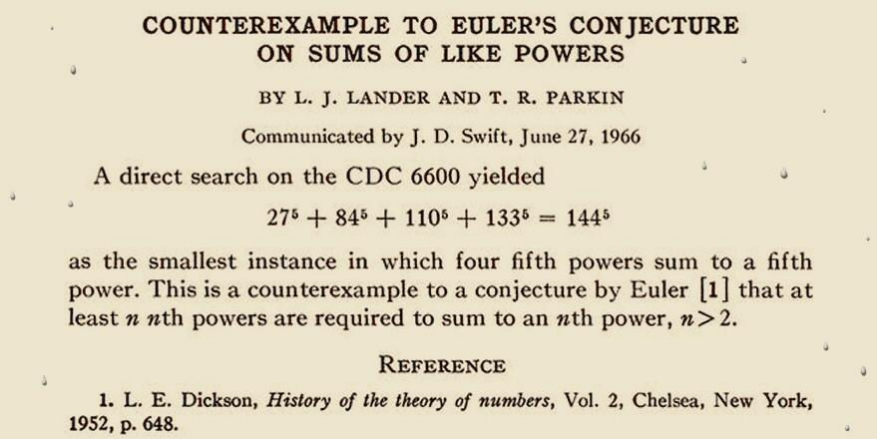
cumplen que $\lfloor \alpha_n \rfloor$ es primo para todo $n = 1, 2, 3, \ldots$ Dicho de manera más compacta, la parte entera de $2^{2^{\cdot^{\cdot^{\cdot^{2^{\alpha}}}}}}$ es un primo para cualquier número de iteraciones de la exponencial.

No vamos a dar la demostración de este teorema, que se consigue de manera bastante sencilla a partir del postulado de Bertrand (es decir, que «Para cada $n \in \mathbb{N}$ existe algún número primo p tal que $n < p \leq 2n$»). Se puede ver en [35, § 9.3.2].

Realmente, el resultado de Wright es una adaptación de este otro que probó William H. Mills en 1947, cuyo enunciado es más sencillo pero cuya demostración es menos elemental:

Teorema. *Existe un número real $\theta \in (1, \infty)$ tal que $\lfloor \theta^{3^n} \rfloor$ es primo para todo $n \in \mathbb{N}$.*

En la práctica, son dos resultados sólo de existencia: ni α (Wright) ni θ (Mills) se pueden encontrar. Y lo mismo ocurre con todas las demás constantes generadoras de primos —cada una con su método para generar los primos— que aparecen en la literatura matemática. Véase, por ejemplo, [36] y las referencias que contiene.



COUNTEREXAMPLE TO EULER'S CONJECTURE
ON SUMS OF LIKE POWERS

BY L. J. LANDER AND T. R. PARKIN

Communicated by J. D. Swift, June 27, 1966

A direct search on the CDC 6600 yielded

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

as the smallest instance in which four fifth powers sum to a fifth power. This is a counterexample to a conjecture by Euler [1] that at least n nth powers are required to sum to an nth power, $n>2$.

REFERENCE

1. L. E. Dickson, *History of the theory of numbers*, Vol. 2, Chelsea, New York, 1952, p. 648.

Figura 4: El contraejemplo de Lander y Parkin a una conjetura de Euler.

3. La conjetura de las sumas de potencias de Euler

En 1740, Euler había probado que la ecuación diofántica $x^3 + y^3 = z^3$ no tenía soluciones no nulas (es decir, que el último teorema de Fermat era cierto con exponente 3).

En 1769 conjeturó que, si para algún exponente entero $n \geq 2$ y un número de sumandos $k \geq 2$, se cumplía

$$a_1^n + a_2^n + \cdots + a_k^n = c^n$$

con $a_1, a_2, \ldots, a_k$ y c enteros positivos, forzosamente debía ser $k \geq n$. Es decir que, cuando $n \geq 2$, al menos se necesitan n potencias n-ésimas para obtener una suma que es también una potencia n-ésima.

La conjetura se demostró falsa en 1966, año en el que Leon J. Lander y Thomas R. Parkin [21, 22] realizaron una búsqueda por ordenador que les permitió encontrar el contraejemplo

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

El contraejemplo lo publicaron, en primer lugar, en [21], en lo que constituye uno de los artículos más cortos de la historia de las matemáticas (véase la figura 4). Posteriormente, en [22] dieron más detalles de cómo habían efectuado su búsqueda.

Aunque, en su tiempo —con la potencia de los ordenadores de entonces—, la búsqueda de Lander y Parkin resultó meritoria, resulta curioso observar lo fácil que resulta ahora realizar esa búsqueda desde el mismo LaTeX que estamos usado para escribir este artículo (en realidad, desde LuaLaTeX). El código Lua de la figura 5 está destinado a chequear si, dado m, hay alguna solución de la ecuación diofántica $a^5 + b^5 + c^5 + d^5 = e^5$ con $a, b, c, d \leq m$; y sólo mediante fuerza bruta, es decir, probando con todas las tuplas (a, b, c, d). Si, con LuaLaTeX, cargamos `\usepackage{luacode}` e insertamos el código de la figura en el preámbulo de

```
\begin{luacode*}

function LanderParkin(a,b,c,d)
  local s, t
  s = a^5 + b^5 + c^5 + d^5
  t = math.floor(s^0.2)
  if t^5 == s then
    return true
  else
    return false
  end
end

function buscarHasta(m)
  local t
  local x = os.clock()
  for a=1, m do
    for b=a, m do
      for c=b, m do
        for d=c, m do
          if LanderParkin(a,b,c,d) then
            tex.sprint("\\par Contraejemplo:\\ ")
            t = math.floor((a^5 + b^5 + c^5 + d^5)^0.2)
            tex.sprint("$", a,"^5 + ", b,"^5 + ",
                c,"^5 + ", d,"^5 = ", t,"^5$")
            tex.sprint("\\par")
          end
        end
      end
    end
  end
  tex.print(string.format(' Tiempo usado: %.2f seg.', os.clock() - x))
  tex.sprint("\\par\\medskip")
end

\end{luacode*}
```

Figura 5: Programa en Lua para buscar, con LuaLaTeX, el contraejemplo de Lander y Parkin a la conjetura de las sumas de potencias de Euler.

un archivo `.tex`, la orden `\directlua{buscarHasta(140)}` nos proporciona la solución de Lander y Parkin —en el ordenador personal que está usando el que esto escribe— en un par de segundos (en [26] hay más ejemplos de cómo hacer cálculos matemáticos directamente en LaTeX con LuaLaTeX).

Una vez comprobado que la conjetura era falsa al menos para exponente $n = 5$, faltaba conocer si era cierta o no para otros valores de n. Desde luego, el caso que más intrigaba era $n = 4$. ¿Podría ser cierto que no existieran enteros positivos x, y, z y t tales que $x^4 + y^4 + z^4 = t^4$? La respuesta a esta pregunta se resistió dos décadas. Fue en 1987 cuando Noam Elkies [9] probó —utilizando ciertas construcciones geométricas denominadas curvas elípticas y ayudado por potentes

ordenadores— que la conjetura era falsa también en este caso: encontró la solución

$$2\,682\,440^4 + 15\,365\,639^4 + 18\,796\,760^4 = 20\,615\,673^4$$

e incluso demostró que existía una clase infinita de soluciones. El año siguiente, Roger E. Frye [11] encontró

$$95\,800^4 + 217\,519^4 + 414\,560^4 = 422\,481^4$$

y demostró que era la menor solución posible de esa ecuación diofántica.

En contraposición al éxito en la búsqueda de soluciones para las potencias cuartas y quintas en la ecuación de Euler, aún no se sabe qué ocurre para potencias sextas o superiores. ¿Estaba Euler totalmente equivocado o había algo de cierto debajo de su conjetura? Aún no se sabe para ningún exponente mayor o igual que 6.

4. Algunos ejemplos adicionales

Presentamos a continuación cuatro ejemplos interesantes de propiedades que son ciertas para muchísimos valores de n, pero que, en un determinado momento, fallan. No tienen ninguna relación en común, más allá de que todos ellos son fáciles de explicar y no requieren ningún conocimiento matemático avanzado.

4.1. ¿Es $991n^2 + 1$ un cuadrado perfecto?

El ejemplo que ahora mostramos está extraído de [29, § 4.1, ejemplo 4.4(i), p. 53]. Parece que $991n^2 + 1$ no es un cuadrado perfecto para ningún $n \in \mathbb{N}$:

$$\begin{array}{rcl}
991 \cdot 1^2 + 1 = 992 & \text{y} & \sqrt{992} = 31.496031\ldots, \\
991 \cdot 2^2 + 1 = 3965 & \text{y} & \sqrt{3965} = 62.96824\ldots, \\
991 \cdot 3^2 + 1 = 8920 & \text{y} & \sqrt{8920} = 94.44575\ldots, \\
991 \cdot 4^2 + 1 = 15857 & \text{y} & \sqrt{15857} = 125.92458\ldots, \\
991 \cdot 5^2 + 1 = 24776 & \text{y} & \sqrt{24776} = 157.40394\ldots, \\
\multicolumn{3}{c}{\ldots} \\
\multicolumn{3}{c}{991 \cdot 12\,055\,735\,790\,331\,359\,447\,442\,538\,766^2 + 1 \neq a^2\ .}
\end{array}$$

Una vez comprobado para números de semejante tamaño, cualquiera podría suponer que eso iba a ser cierto siempre. Pero, finalmente,

$$\begin{aligned}
991 \cdot 12\,055\,735\,790\,331\,359\,447\,442\,538\,767^2 + 1 \\
= 379\,516\,400\,906\,811\,930\,638\,014\,896\,080^2,
\end{aligned}$$

luego el resultado que tanto habíamos observado acaba fallando.

4.2. Si dividimos 2^n entre n, ¿el resto nunca es 3?

Este otro ejemplo está extraído de [29, § 4.1, ejemplo 4.4(h), p. 53]. Si, para n entero positivo, dividimos 2^n entre n, el resto nunca es 3 para

$$n = 1, 2, 3, \ldots, 4\,700\,063\,496.$$

Sin embargo, el resto es 3 para $n = 4\,700\,063\,497$.

4.3. La sucesión de Shallit

Definamos la sucesión de enteros $\{a_n\}_{n=0}^{\infty}$ mediante

$$a_0 = 8, \qquad a_1 = 55, \qquad a_{n+1} = \left\lfloor \frac{a_{n-1}^2}{a_{n-2}} + 1 \right\rfloor, \quad n \geq 1.$$

Esta sucesión está relacionada con los números de Pisot (ahora no necesitamos saber qué es eso), y fue propuesta por Jeffrey Shallit en [33] (para más detalles, véase [4]).

Esta sucesión $\{a_n\}_{n=0}^{\infty}$ comienza con 8, 55, 379, 2612, 18002, ..., y parece que sus términos satisfacen la relación de recurrencia

$$a_n = 6a_{n-1} + 7a_{n-2} - 5a_{n-3} - 6a_{n-4}.$$

Pero no es cierto indefinidamente; la identidad anterior falla en $n = 11\,056$.

Si usamos $\{a'_n\}_{n=0}^{\infty}$ para denotar la segunda sucesión, realmente ocurre que

$$a_{11\,056} = a'_{11\,056} + 1.$$

Estos números tienen 9270 dígitos.

4.4. ¿Es $2^{p-1} - 1$ (con p primo) divisible por p^2?

El teorema pequeño de Fermat (o el teorema de Euler-Fermat) asegura que

$$p \mid (2^{p-1} - 1)$$

cuando p es un primo. ¿Es $2^{p-1} - 1$ divisible por p^2?

Los experimentos muestran que, para cualquier primo $p < 1093$,

$$2^{p-1} - 1 \text{ no es divisible por } p^2.$$

Sin embargo, para $p = 1093$,

$$\frac{2^{1093-1} - 1}{1093^2} \in \mathbb{Z}.$$

Éste es un número con 323 dígitos.

En realidad, una vez que sabemos que $(2^{p-1}-1)/p$ es un entero, no hay ningún indicio en contra de que ese entero sea divisible por p. Heurísticamente, un entero al azar debería ser divisible por p una de cada p veces. Así pues, parece sensato pensar que $2^{p-1}-1$ (con p primo) sea divisible por p^2 bastante a menudo. Pero no es eso lo que se ha observado.

Los primos p tales que $p^2 \mid (2^{p-1}-1)$ se denominan primos de Wieferich (los describió por primera vez Arthur Wieferich en 1909, en sus trabajos relativos al último teorema de Fermat). Además de 1093, otro primo de Wieferich es $p = 3511$. No se conoce ninguno más; de hecho, en [7] se comprobó que no hay ningún otro menor que $4 \cdot 10^{12}$, y esta cota se ha mejorado sustancialmente con posteridad. ¿Hay algo detrás de esta aparente escasez de primos de Wieferich? Poco se conoce a ciencia cierta; en particular, no se sabe si hay o no infinitos primos de Wieferich.

5. La ley fuerte de los números pequeños de R. K. Guy

Comenzaremos mostrando un ejemplo de un patrón que acaba rompiéndose y que, a la postre, será un ejemplo paradigmático de lo que, de manera informal, Richard K. Guy había denominado «leyes fuertes de los números pequeños», que veremos justo después.

5.1. Potencias quintas más cinco

¿Los números n^5+5 y $(n+1)^5+5$ son siempre primos entre sí? Aparentemente, es lo que se obtiene si vamos probando con $n = 1, 2, 3, \ldots$

El primer n para el que n^5+5 y $(n+1)^5+5$ no son coprimos es $n = 533\,360$, para el cual

$$\operatorname{mcd}(n^5+5, (n+1)^5+5) = 1\,968\,751.$$

Con n^5-5 y $(n+1)^5-5$, el primer contraejemplo es aún mayor:

$$\operatorname{mcd}(n^5-5, (n+1)^5-5) = 1 \quad \text{para} \quad 1 \leq n < 3\,404\,141,$$

y falla en el siguiente valor de n. Tanto en este caso como en el anterior, este hecho parece muy sorprendente.

Podemos dar un ejemplo similar con potencias 17. El primer fallo de

$$\gcd(n^{17}+9, (n+1)^{17}+9) = 1$$

es $n = 8\,424\,432\,925\,592\,889\,329\,288\,197\,322\,308\,900\,672\,459\,420\,460\,792\,433$. Esta vez, el primer n para el que los dos números no son coprimos es enorme.

Analicemos qué sucede. Por simplicidad, veámoslo primero con exponente 2: ¿Qué pasa con $\operatorname{mcd}(n^2+1, (n+1)^2+1)$?

Tomemos

$$a = n^2+1, \quad b = (n+1)^2+1.$$

Un número que divida a a y b debe dividir a

$$2(a+b) - (a-b)^2 = 5.$$

Así que $\mathrm{mcd}(n^2+1, (n+1)^2+1) = 1$ o 5. Con $n = 2$ sale 5.

Con argumentos similares (sencillos de entender pero, esta vez, difíciles de descubrir) se obtiene que

$$\mathrm{mcd}(n^5+5, (n+1)^5+5) = 1 \quad \text{o} \quad 1\,968\,751.$$

Y el segundo caso ocurre con

$$n = 533\,360 + 1\,968\,751\,k, \quad k = 0, 1, 2, \ldots$$

Vamos a comprobarlo.

Supongamos que $d \mid (n^5+5)$ y $d \mid ((n+1)^5+5)$; es decir, que d es un divisor común, aunque no necesariamente el mayor. Entonces,

$$d \mid \Big((n+1)^5 + 5 - (n^5+5)\Big) = 5n^4 + 10n^3 + 10n^2 + 5n + 1$$

y, de manera similar,

$$\begin{aligned}
d \mid & \Big(5(n^5+5) - (n-2)(5n^4+10n^3+10n^2+5n+1)\Big) \\
& \quad = 10n^3 + 15n^2 + 9n + 27, \\
d \mid & \Big(4(5n^4+10n^3+10n^2+5n+1) - (2n+1)(10n^3+15n^2+9n+27)\Big) \\
& \quad = 7n^2 - 43n - 23, \\
d \mid & \Big(98(10n^3+15n^2+9n+27) - (140n+1\,070)(7n^2-43n-23)\Big) \\
& \quad = 50\,112n + 27\,256, \\
d \mid & \Big(1\,569\,507\,840(7n^2-43n-23) - (219\,240n - 1\,466\,005)(50\,112n+27\,256)\Big) \\
& \quad = 3\,858\,751\,960 = 2^3 \cdot 5 \cdot 7^2 \cdot 1\,968\,751.
\end{aligned}$$

Además, se tiene lo siguiente: (a) Los números n^5+5 y $(n+1)^5+5$ tienen distinta paridad, luego su divisor común d no puede ser par. (b) Por inspección (o por el teorema pequeño de Fermat), $n^5 \equiv n \pmod 5$, luego d no puede ser múltiplo de 5. (c) Por inspección, $n^5 \not\equiv (n+1)^5 \pmod 7$, luego d tampoco puede ser múltiplo de 7. En consecuencia, sólo puede ocurrir $d = 1$ o $d = 1\,968\,751$. ¿Cuándo se da el segundo caso?

Por lo que hemos visto, d es un divisor común de $50\,112n + 27\,256$ y de $1\,968\,751$. Como $1\,968\,751$ es primo, si $50\,112n + 27\,256 \not\equiv 0 \pmod{1\,968\,751}$, forzosamente deberá ser $d = 1$. Eso no ocurrirá si

$$50\,112n + 27\,256 \equiv 0 \pmod{1\,968\,751}.$$

Esto es una ecuación modular que se puede resolver sin dificultad por procedimientos estándar, y su solución es $n \equiv 533\,360 \pmod{1\,968\,751}$. Así pues, es en este caso cuando el mcd vale $1\,968\,751$, tal como queríamos comprobar.

No queremos despedir este apartado sin comentar de dónde surge este tipo de interesantes problemas.

En 1995, en la columna *Math Investigations* de George Berzsenyi en la revista *Quantum* (véase [5]), se plantea el siguiente problema: dados dos enteros positivos m y k fijos, encontrar

$$G(m,k) = \text{máx}\{\text{mcd}(n^m + k, (n+1)^m + k) : n \in \mathbb{N}\}.$$

En particular, se menciona que sería interesante conocer para qué valores de m y k se cumple $G(m,k) = 1$. (Problemas similares, para valores de m y k concretos, habían sido previamente propuestos en algunas olimpiadas matemáticas.)

En los siguientes números de su columna, Berzsenyi vuelve a aludir al problema, y comenta soluciones que le envían los lectores. En particular, aparece el caso de $\text{mcd}(n^5+5, (n+1)^5+5)$, y se menciona que es una maravillosa ilustración de la ley fuerte de los números pequeños de R. K. Guy, que nosotros veremos en el siguiente apartado. Asimismo, Stan Wagon, en 1996, en su columna en internet *Problem of the Week* pregunta (en el problema 805) si es verdad o no que, para cada entero positivo n, los números n^5+5 y $(n+1)^5+5$ son coprimos,[6] lo cual ayudó a divulgar el problema.

Finalmente, el ejemplo $\text{mcd}(n^{17}+9, (n+1)^{17}+9)$ con potencias 17 está extraído de [29, § 4.1, ejemplo 4.4(j), p. 53].

5.2. Las leyes fuertes de los números pequeños

En 1988, en un artículo de la muy conocida revista *American Mathematical Monthly* [15], Richard K. Guy enunció lo que denominó «ley fuerte de los números pequeños» y propuso muchos ejemplos. El nombre es, obviamente, un guiño, por contraposición, a las leyes de los grandes números de la estadística, cuyo comportamiento es contrario a lo que aquí se expone, y desde bastantes años antes había estado circulando en un manuscrito suyo no publicado; de hecho, el nombre lo usó Martin Gardner en 1980 en su columna *Mathematical Games* de *Scientific American* [12], atribuyéndolo a R. K. Guy.

Ley fuerte de los números pequeños. *No hay suficientes números pequeños como para que puedan satisfacer todo lo que se les pide.*

En 1990, en otro artículo, esta vez en *Mathematics Magazine* [16], añadió una segunda ley (y muchos más ejemplos):

Segunda ley fuerte de los números pequeños. *Cuando dos números parecen iguales, ¡no es necesariamente así!*

La idea subyacente a todo esto es que, en numerosos problemas que dependen de n, los patrones que se observan para valores pequeños de n no son realmente ciertos siempre.

[6] Véase `https://stanwagon.com/potw/spring96/p805.html`.

Aunque no figura en el artículo de R. K. Guy, el caso de $\mathrm{mcd}(n^5+5, (n+1)^5+5)$ del apartado anterior es un ejemplo típico: como hemos visto, el máximo común divisor sólo puede ser 1 o 1 968 751. Y, claro, no se puede conseguir 1 968 751 con números pequeños.

Ejemplos (quizás muy exagerados) de la ley son los siguientes:

- El 10 % de los primeros 100 números son cuadrados perfectos.
- Un cuarto de los números menores que 100 son primos
- Excepto el 6, todos los números menores que 10 son potencias de primos.
- La mitad de los números menores que 10 son números de Fibonacci.

La ley fuerte de los números pequeños es enemiga del descubrimiento matemático. Si observas un patrón, ¿cómo saber que es real? En palabras del propio R. K. Guy:

- Semejanzas superficiales engendran declaraciones espurias.
- Coincidencias caprichosas causan conjeturas poco cuidadas.

Y, por otra parte, la ley también trabaja así:

- Excepciones tempranas eclipsan eventuales propiedades esenciales.
- Irregularidades iniciales inhiben la intuición.

6. La función ϕ de Euler en sucesiones

La denominada función ϕ de Euler, o función *totient*, que resulta importantísima en teoría de números, se define de la siguiente manera:

$$\phi(n) = \mathrm{card}\{\, k \in \mathbb{N} \,:\, 1 \leq k \leq n,\ \mathrm{mcd}(k,n) = 1 \,\}.$$

Ésta es una de las denominadas funciones aritméticas notables, que son funciones definidas sobre los naturales (pueden toman valores en $\mathbb{Z}$, $\mathbb{R}$ o $\mathbb{C}$, según el caso), y donde el adjetivo «notables» alude a que su definición tiene relación con alguna propiedad aritmética interesante. En [35, capítulo 7] podemos ver cuáles son las funciones a las que comúnmente se alude con este nombre, así como sus principales propiedades. Algunas de de estas funciones (en concreto, $\Omega(n)$, $\lambda(n)$ y $\mu(n)$) nos aparecerán, más adelante, en otros apartados de este artículo.

Volviendo a la función ϕ, como muestra de su importancia merece la pena señalar que, si hubiera un teorema con el nombre de «teorema fundamental de las congruencias», sin duda tendría que ser el teorema de Euler-Fermat que afirma que, si n es un entero positivo, y a cumple $\mathrm{mcd}(a,n) = 1$, entonces

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

En el caso $n = p$, un primo, entonces $\phi(p) = p - 1$ y se obtiene que $a^{p-1} \equiv 1$ (mód p) cuando $p \nmid a$, que se denomina teorema pequeño de Fermat. También es muy relevante el caso $n = pq$ (producto de dos primos distintos), donde se tiene $\phi(pq) = (p-1)(q-1)$ (y el correspondiente resultado se denomina teorema de la media de Fermat); esto interviene, de manera muy destacada, en la criptografía RSA. Pero no necesitamos nada de esto para lo que sigue, así que dejemos esta digresión y volvamos a donde estábamos.

Está claro que la función $\phi(n)$ no tiene un comportamiento regular (en particular, no es creciente ni decreciente). Pero, cuanto más grande sea n, más números $k \leq n$ hay, y muchos de esos k contribuirán a $\phi(n)$ por ser primos con n. Así, uno puede esperar que, por ejemplo,

$$\phi(210\,n) < \phi(6\,469\,693\,230\,n + 31), \quad n \geq 1$$

(el segundo argumento es siempre significativamente mayor que el primero, la diferencia crece al crecer n, y la desigualdad es cierta para n pequeño). ¿Será eso cierto siempre? Seguro que, a estas alturas, el lector ya puede imaginar que no, pese a que esa desigualdad sí que es cierta para una ingente cantidad de valores de n.

En 1997, D. J. Newman [27] demostró, usando el teorema de Dirichlet sobre primos en progresiones aritméticas, que, para a, b, c, d enteros no negativos con $a, c > 0$ y $ad - bc \neq 0$, las desigualdades

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

se invierten infinitas veces (en [1] se proporciona una prueba alternativa más elemental, que no utiliza el teorema de Dirichlet).

De manera más concreta, y para un ejemplo más sencillo que el anterior, Greg Martin [25] probó, en 1999, que la primera inversión de

$$\phi(30n) \leq \phi(30n + 1)$$

ocurre en cierto número n de 1116 dígitos que aparece explícitamente en su artículo.

7. El problema booleano de las ternas pitagóricas

¿Podemos separar los números naturales $\{1, 2, 3, \dots\}$ en dos partes de manera que ninguna de las partes contenga una terna (a, b, c) tal que $a^2 + b^2 = c^2$?

Si las dos partes se visualizan con dos colores, eso equivale a decir que ningún triángulo rectángulo tenga sus tres lados del mismo color.

El problema fue propuesto, en los años 80 del siglo XX, por Ronald Graham, quien ofreció 100 dólares al que lo resolviera. Es un ejemplo típico de la denominada teoría de Ramsey, un campo de las matemáticas —de la combinatoria—

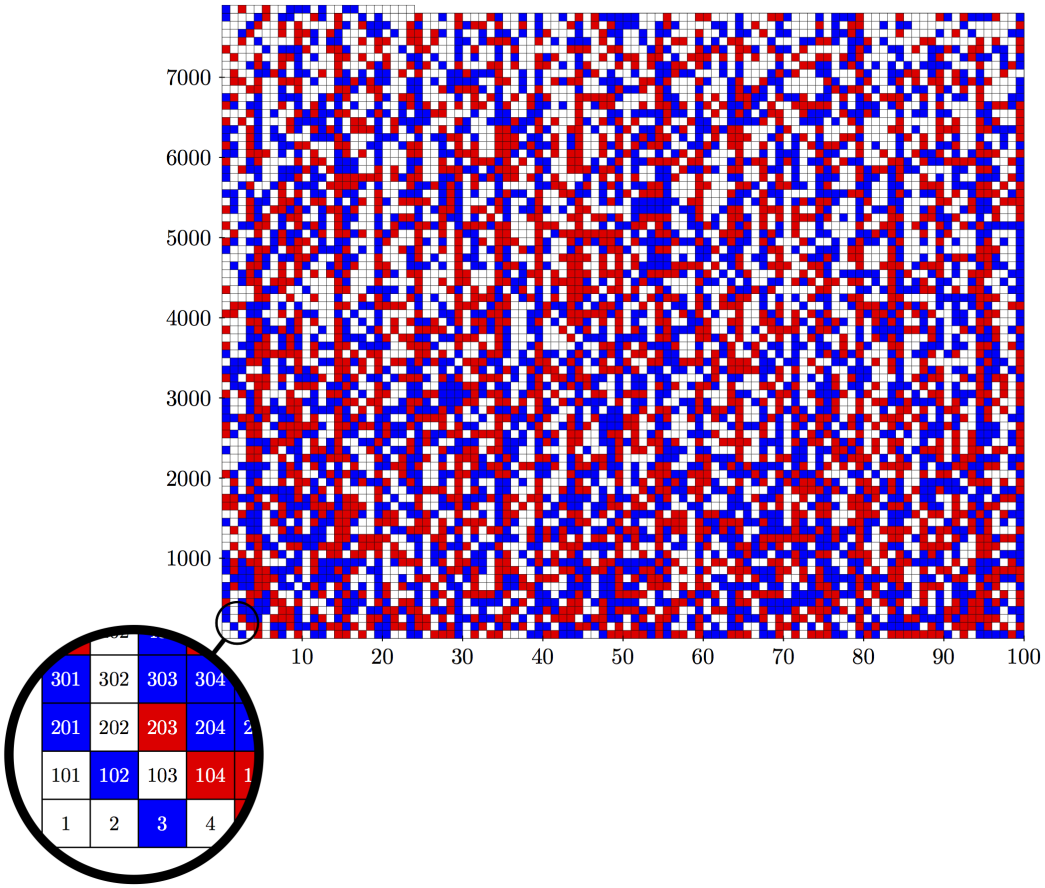


Figura 6: Coloración de la solución del problema booleano de las ternas pitagóricas para lados ≤ 7824.

que estudia las condiciones bajo las cuales, en una estructura de cierto tamaño, se cumple alguna propiedad preestablecida; en general, la dificultad de los problemas de Ramsey crece muchísimo con el tamaño del problema (en [10] se pueden ver más detalles y unos cuantos ejemplos).

Si vamos fijando n y se van haciendo pruebas con triángulos de lados $a, b, c \leq n$, parece que, en efecto, se va consiguiendo. Pero, según va a aumentando el valor de n, hay más formas de descomponer el conjunto $\{1, 2, \ldots, n\}$ en dos partes y, cuando n es suficientemente grande, resulta computacionalmente imposible probar con todas. No obstante, Joshua Cooper y Ralph Overstreet habían demostrado, en 2015, que el problema tenía solución para $\{1, 2, \ldots, 7664\}$. ¿Qué pasaba para n mayor?

El año siguiente, Marijn J. H. Heule, Oliver Kullmann y Victor W. Marek publicaron un artículo en el que mostraban que también era posible dar una coloración para lados $a, b, c \leq 7824$ de manera que ningún triángulo rectángulo tenga sus tres lados del mismo color. Una de las posibles formas de colorear de rojo o azul todos los números hasta el 7824, de modo que no haya ninguna terna pitagórica cuyos miembros sean todos del mismo color es la de la figura 6 (las casillas blancas se corresponden con los números que no apararen en ninguna terna

pitagórica, y por tanto pueden ser de cualquier color); el eje vertical representa las centenas y el horizontal las correspondientes decenas y unidades.

Y, lo más importante en cuanto a la solución del problema, en su artículo —publicado en *arXiv* el 3 de mayo de 2016 y noticia en *Nature* [19] el 26 de mayo (el artículo completo está en [20])— demostraron que, a partir del 7825, no resulta posible asignar dos colores a los números enteros sin que aparezcan ternas pitagóricas monocromáticas.

El resultado, de manera sorprendente, tuvo una enorme repercusión en la prensa generalista; por ejemplo, en España fue reseñado en las secciones de ciencia de *El País* y de *ABC*. Pero no fue por el resultado matemático en sí, sino por el reto computacional que supuso el hallazgo. La comprobación que descarta todas las posibilidades había sido realizada en el supercomputador Stampede de la Universidad de Texas, un clúster con 800 núcleos de cálculo en paralelo que tardó aproximadamente dos días en resolver el problema (en total, unas 35 000 horas de CPU); la figura 7 muestra una foto del ordenador.

Figura 7: El supercomputador Stampede de la Universidad de Texas en Autin.

Lo más relevante computacionalmente hablando —y esto es lo que atrajo la atención fuera del mundo de las matemáticas— fue que el fichero generado en el cálculo (la demostración, por así decirlo) ocupa 200 terabytes de información, y supuso un récord absoluto para el tamaño de la prueba de un problema matemático (el récord anterior era de 13 gigabytes). Así mismo, la prueba en sí estaba acompañada de un archivo descargable que se puede repasar en 30 000 horas de CPU.

8. La integral de Borwein

En 2001 (véase [3]), los hermanos David Borwein y Jonathan Borwein mostraron un bonito e ingenioso patrón —en una expresión integral que ahora se denomina «integral de Borwein»— que, inesperadamente, deja de ser cierto.

En su artículo, ellos probaron que

$$\int_0^\infty \frac{\operatorname{sen}(x)}{x}\,dx = \frac{\pi}{2},$$
$$\int_0^\infty \frac{\operatorname{sen}(x)}{x}\frac{\operatorname{sen}(x/3)}{x/3}\,dx = \frac{\pi}{2},$$
$$\int_0^\infty \frac{\operatorname{sen}(x)}{x}\frac{\operatorname{sen}(x/3)}{x/3}\frac{\operatorname{sen}(x/5)}{x/5}\,dx = \frac{\pi}{2},$$
$$\int_0^\infty \frac{\operatorname{sen}(x)}{x}\frac{\operatorname{sen}(x/3)}{x/3}\frac{\operatorname{sen}(x/5)}{x/5}\frac{\operatorname{sen}(x/7)}{x/7}\,dx = \frac{\pi}{2},$$
$$\dots$$
$$\int_0^\infty \frac{\operatorname{sen}(x)}{x}\frac{\operatorname{sen}(x/3)}{x/3}\frac{\operatorname{sen}(x/5)}{x/5}\cdots\frac{\operatorname{sen}(x/13)}{x/13}\,dx = \frac{\pi}{2}.$$

Pero, si añadimos un factor más,

$$\int_0^\infty \frac{\operatorname{sen}(x)}{x}\frac{\operatorname{sen}(x/3)}{x/3}\cdots\frac{\operatorname{sen}(x/15)}{x/15}\,dx = \frac{467\,807\,924\,713\,440\,738\,696\,537\,864\,469}{935\,615\,849\,440\,640\,907\,310\,521\,750\,000}\,\pi;$$

es un valor muy cercano a $\pi/2$ (difiere de él en, aproximadamente, $2.31 \cdot 10^{-11}$), pero ya no es lo que estábamos obteniendo.

También explican la razón de que eso ocurra (que no es obvia), y es que

$$\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{9}+\frac{1}{11}+\frac{1}{13} < 1$$

pero

$$\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{9}+\frac{1}{11}+\frac{1}{13}+\frac{1}{15} > 1.$$

El artículo [32] proporciona una demostración simplificada que permite comprender, de forma gráfica e intuitiva, por qué se produce el cambio en el valor de la integral cuando la suma es mayor que 1.

Con una integral muy similar, se puede conseguir que el patrón tarde mucho más en romperse. La identidad

$$\int_0^\infty \frac{\operatorname{sen}(x)}{x}\frac{\operatorname{sen}\left(\frac{x}{101}\right)}{\frac{x}{101}}\frac{\operatorname{sen}\left(\frac{x}{201}\right)}{\frac{x}{201}}\cdots\frac{\operatorname{sen}\left(\frac{x}{100n+1}\right)}{\frac{x}{100n+1}}\,dx = \frac{\pi}{2}$$

falla, por primera vez, para

$$n = 15\,341\,178\,777\,673\,149\,429\,167\,740\,440\,969\,249\,338\,310\,889.$$

Eso sucede porque ése es el primer n para el que

$$\sum_{k=1}^{n}\frac{1}{100k+1} > 1.$$

9. Coeficientes de polinomios ciclotómicos

Tomamos el polinomio

$$P_n(x) = x^n - 1, \qquad n \geq 1,$$

y queremos estudiar su factorización en $\mathbb{Z}[x]$. Como $P_n(1) = 0$, $P_n(x)$ es divisible por $x - 1$, pero puede haber más divisores en $\mathbb{Z}[x]$.

En las factorizaciones de $P_n(x)$ en polinomios irreducibles, todos los coeficientes parecen ser 0, +1 o −1. Los primeros casos son

$$\begin{aligned}
x^2 - 1 &= (x-1)(x+1),\\
x^3 - 1 &= (x-1)(x^2+x+1),\\
x^4 - 1 &= (x-1)(x+1)(x^2+1),\\
x^5 - 1 &= (x-1)(x^4+x^3+x^2+x+1),\\
x^6 - 1 &= (x-1)(x+1)(x^2+x+1)(x^2-x+1),\\
x^7 - 1 &= (x-1)(x^6+x^5+x^4+x^3+x^2+x+1).
\end{aligned}$$

Esos polinomios irreducibles se denominan «polinomios ciclotómicos».

Si seguimos, vamos obteniendo

$$\begin{aligned}
x^8 - 1 &= (x-1)(x+1)(x^2+1)(x^4+1),\\
x^9 - 1 &= (x-1)(x^2+x+1)(x^6+x^3+1),\\
x^{10} - 1 &= (x-1)(x+1)(x^4+x^3+x^2+x+1)(x^4-x^3+x^2-x+1),\\
&\cdots
\end{aligned}$$

Al menos hasta $x^{100} - 1$, sólo salen coeficientes 0, +1 o −1. Es fácil pensar que eso va a ocurrir siempre, es decir, que los polinomios ciclotómicos sólo van a tener coeficientes 0, +1 o −1.

En 1883, A. Migotti comprobó que eso no era cierto, sino que falla con $x^{105}-1$, uno de cuyos factores irreducibles es

$$\begin{aligned}
x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - \mathbf{2}x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34}\\
+ x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15}\\
+ x^{14} + x^{13} + x^{12} - x^9 - x^8 - \mathbf{2}x^7 - x^6 - x^5 + x^2 + x + 1
\end{aligned}$$

(los coeficientes de x^{41} y x^7, que aparecen destacados en la expresión anterior, son −2).

Más aún. En 1931, I. Schur envió una carta a Landau en la que demostraba que no hay ninguna cota para el tamaño de los coeficientes de los polinomios ciclotómicos, sino que existen coeficientes tan grandes como se quiera. La demostración se puede ver en [24]. De hecho, $105 = 3 \cdot 5 \cdot 7$ es el menor número que se obtiene como producto de tres primos diferentes, y se puede demostrar que la propiedad que se está comentando es cierta para todos los números que son producto de, como máximo, dos primos diferentes.

Los polinomios ciclotómicos tienen una rica estructura y muchas propiedades interesantes. A este respecto, recomendamos el artículo [6], que proporciona muchos detalles adicionales sobre lo que aquí hemos expuesto.

10. La conjetura de Pólya

Para un entero $n > 1$, sea $\Omega(n)$ el número de divisores primos de n (contando cada primo tantas veces como su multiplicidad); además, tomamos $\Omega(1) = 0$.

A partir de la función aritmética $\Omega(n)$, a los enteros positivos los podemos dividir en dos tipos:

- n se dice *de tipo par* si $\Omega(n)$ es par. Por ejemplo, $15 = 3 \cdot 5$ y $100 = 2^2 \cdot 5^2$ son de tipo par (también $n = 1$ es de tipo par).
- n se dice *de tipo impar* si $\Omega(n)$ es impar. Por ejemplo, $30 = 2 \cdot 3 \cdot 5$ y $75 = 3 \cdot 5^2$ son de tipo impar.

Asimismo, definimos estas dos funciones:

$$\text{Pares}(n) = \text{card}\left\{k : 1 \le k \le n,\ k \text{ de tipo par}\right\},$$
$$\text{Impares}(n) = \text{card}\left\{k : 1 \le k \le n,\ k \text{ de tipo impar}\right\}.$$

Por ejemplo,

$$\begin{aligned} \text{Pares}(10) &= 5, \quad \text{Impares}(10) = 5, \\ \text{Pares}(100) &= 49, \quad \text{Impares}(100) = 51, \\ \text{Pares}(1000) &= 493, \quad \text{Impares}(1000) = 507. \end{aligned}$$

En 1919, George Pólya se dio cuenta de que, para todos los n en los que lo comprobaba, siempre se cumplía que $\text{Impares}(n) \ge \text{Pares}(n)$. Además, demostró que el enunciado

$$\text{Impares}(n) \ge \text{Pares}(n) \quad \text{para todo } n > 1$$

implicaba la hipótesis de Riemann (más adelante explicaremos en qué consiste esto). Aparentemente, Pólya nunca conjeturó que esa propiedad fuera cierta, pero habitualmente se alude a ella con el nombre de conjetura de Pólya.

Podemos dar una descripción alternativa de la conjetura utilizando la función de Liovillle $\lambda(n)$ y, sobre todo, el sumatorio de la función de Liouville $L(n)$, que para n entero positivo se definen así:

$$\lambda(n) = (-1)^{\Omega(n)} \qquad \text{y} \qquad L(n) = \sum_{k=1}^{n} (-1)^{\Omega(k)}.$$

Con esta notación, podemos escribir

$$L(n) = \text{Pares}(n) - \text{Impares}(n) = \sum_{k=1}^{n} (-1)^{\Omega(k)}.$$

De este modo, la conjetura de Pólya equivale a afirmar que $L(n) \le 0$ para todo $n > 1$.

¿Qué ocurrió con esta conjetura?

En 1942, Albert E. Ingham ideó un ingenioso método que, según él suponía, podía servir para encontrar un contraejemplo. Usando métodos derivados de los de Ingham, pero ya con ayuda informática, C. Brian Haselgrove [17] refutó la conjetura en 1958, y estimó que debía existir un contraejemplo alrededor de $1.85 \cdot 10^{361}$, pero sin darlo explícitamente.

En 1960, R. Sherman Lehman [23] encontró un contraejemplo, $n = 906\,180\,359$. Finalmente, en 1960, Minoru Tanaka [34] demostró que el menor contraejemplo de la conjetura de Pólya es $n = 906\,150\,257$.

11. La función de Möbius y la conjetura de Mertens

Otra función aritmética notable es la función de Möbius, que se define así:

$$\mu(n) = \begin{cases} 1, & \text{si } n = 1, \\ (-1)^k, & \text{si } n \text{ es producto de } k \text{ primos distintos}, \\ 0, & \text{si } n \text{ tiene por divisor un primo al cuadrado.} \end{cases}$$

Aunque parece rara, surge de manera natural en muchos problemas de teoría de números. La definió y estudió August Möbius en 1832; pero, implícitamente, ya la usaba Euler en 1750.

En 1896, y de manera independiente, Jacques Hadamard y Charles de la Vallée-Poussin probaron el denominado «teorema de los números primos» (TNP), que sin duda es el resultado más importante de la teoría de números analítica:

Teorema de los números primos. *Para $x \geq 1$, sea $\pi(x)$ la función que cuenta cuántos primos menores o iguales que x hay, es decir,*

$$\pi(x) := \operatorname{card}\{p \text{ primo} : p \leq x\}.$$

Entonces,

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

Que $\lim_{x\to\infty} \pi(x) = \infty$ equivale a decir que existen infinitos primos, que ya era conocido desde la época de Euclides (el artículo [30] recoge bastantes demostraciones distintas de este resultado); pero, aproximadamente, y para cada $x > 1$, ¿cuántos hay en el intervalo $[1, x]$? Intentando estimar eso, el TNP había sido conjeturado, también independientemente, por Adrien Marie Legendre (1798) y Carl Friedrich Gauss (1849) a partir de sus observaciones en una tabla de primos. Pafnuty Chebyshev, en 1852, dio algunos resultados que se aproximaban bastante al TNP, pero no consiguió probarlo. Si el lector está interesado en los detalles sobre lo que probó Chebyshev, o quiere ver una demostración del TNP, puede hacerlo consultando [35, capítulos 9 y 10].

Actualmente se conocen varias formas de probar el TNP, pero ninguna es especialmente sencilla. El caso es que, en lo que respecta a lo que aquí estamos tratando, demostrar el TNP equivale a probar que

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\leq x} \mu(n) = 0;$$

éste es, de hecho, uno de los caminos habituales para atacar la demostración del TNP. Debemos aquí aclarar que, cuando se dice que dos problemas abiertos son equivalentes, nos referimos a que los dos resultados se implican mutuamente (es decir, que ambos son ciertos o ambos falsos), pues sabemos cómo demostrar cualquiera de los dos asumiendo el otro como cierto. En cambio, cuando se dice que dos resultados matemáticos ya demostrados son equivalentes (como es el caso anterior), eso alude a que, partiendo de uno de ellos, el otro se deduce de ése con argumentos relativamente sencillos (comparados con la demostración de los propios resultados); a menudo, esto se aplica a resultados que, antes de ser teoremas, eran problemas abiertos que desafiaron a la comunidad matemática durante bastante tiempo.

En 1897, Franz Mertens conjeturó que, para cada $x > 1$, se cumplía

$$M(x) := \sum_{n\leq x} \mu(n) < \sqrt{x}$$

(previamente, ya lo había conjeturado Thomas Joannes Stieltjes en 1885, en una carta a Charles Hermite). Eso es más de lo que se necesita para probar el TNP (y, de hecho, incluso implica la veracidad de la hipótesis de Riemann), pero los experimentos numéricos sugerían que podía ser cierto.

Pese a las numerosas evidencias computacionales a favor de la conjetura, Andrew Odlyzko y Herman te Riele [28] demostraron, en 1985, que

$$\limsup_{x\to\infty} M(x)x^{-1/2} > 1.06 \quad \text{y} \quad \liminf_{x\to\infty} M(x)x^{-1/2} < -1.009,$$

lo cual implica claramente que la conjetura de Mertens es falsa. Pero no encontraron ningún contraejemplo concreto, y estimaron que no iba a haber ninguno menor que 10^{20}. Actualmente hay más indicios de dónde puede estar el primer contraejemplo, pero se sigue sin conocer ninguno, y es uno de los retos más apasionantes de la teoría de números computacional.

Para concluir, merece la pena señalar que ahora se conjetura que

$$M(x) = o(x^{1/2+\varepsilon}) \quad \text{para todo } \varepsilon > 0$$

(recordemos que $f(x) = o(g(x))$ para $x \to \infty$, donde f y g son funciones positivas, significa que $f(x)/g(x) \to 0$ cuando $x \to \infty$), pero permanece sin confirmar ni refutar. Éste sería un resultado muy relevante, pues se sabe que su demostración equivaldría a la de la hipótesis de Riemann.

12. El tamaño de $\pi(x)$

En el apartado anterior hemos visto que teorema de los números primos (TNP) afirma que

$$\pi(x) := \operatorname{card}\{p \text{ primo} : p \leq x\} \sim \frac{x}{\log(x)}, \quad x \to \infty$$

(como es habitual, el símbolo $\sim$ alude a que el cociente tiende a 1 cuando $x \to \infty$).

Vamos a dar un enunciado alternativo, y para ello necesitamos definir el logaritmo integral:

$$\operatorname{li}(x) = \text{v. p.} \int_0^x \frac{dt}{\log(t)} = \lim_{\varepsilon \to 0^+} \left(\int_0^{1-\varepsilon} + \int_{1+\varepsilon}^x \right) \frac{dt}{\log(t)}, \qquad x > 1.$$

Obsérvese que estamos obligados a tomar el valor principal de la integral dado que, si no, la integral sería divergente en $t = 1$. Esto no tiene mucha importancia pues podíamos haber definido la función tomando 2 en el extremo inferior de integración en vez de 0, con lo cual no habríamos necesitado usar el valor principal (y la diferencia sería nimia, pues $\operatorname{li}(2) = 1.045\,163\ldots$), pero vamos a dejarlo tal como se define habitualmente.

Es relativamente sencillo probar que $\operatorname{li}(x) \sim \frac{x}{\log(x)}$, luego el TNP se puede enunciar de cualquiera de estas dos formas equivalentes:

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log(x)} = 1, \qquad \lim_{x \to \infty} \frac{\pi(x)}{\operatorname{li}(x)} = 1.$$

Cuando se presenta el TNP en entornos o en textos no especializados se suele hacer con $x/\log(x)$ (pues esa función es menos extraña que $\operatorname{li}(x)$), pero en las demostraciones del TNP aparece $\operatorname{li}(x)$ de forma natural, no $x/\log(x)$. Así que a partir de ahora nos centraremos, sobre todo, en $\operatorname{li}(x)$.

En el cuadro 1 se puede ver la aproximación de $\pi(x)$ con $x/\log(x)$, con $\operatorname{li}(x)$ y con otra función que hemos denotado $\operatorname{Ri}(x)$ y a la que volveremos más adelante. De momento, fijémonos en la columna $\operatorname{li}(x) - \pi(x)$. Para valores «pequeños» de x, siempre se cumple $\operatorname{li}(x) \geq \pi(x)$; incluso da la impresión de que, al crecer x, las diferencias $\operatorname{li}(x) - \pi(x)$ crecen continuamente hacia infinito.

Resulta razonable pensar en la posibilidad de que $\operatorname{li}(x) - \pi(x) \geq 0$ siempre. Pero es completamente falso. En 1914, y en contra de la opinión habitual de los matemáticos de la época, John Edensor Littlewood probó el siguiente resultado:

Teorema. *La diferencia* $\operatorname{li}(x) - \pi(x)$ *cambia de signo infinitas veces.*

Más precisamente, lo que Littlewood demostró es que, para una constante $K > 0$ conveniente, existen infinitos valores de x para los cuales

$$\operatorname{li}(x) - \pi(x) > K \frac{\sqrt{x}}{\log(x)} \log(\log(\log(x))),$$

y también infinitos valores de x tales que

$$\mathrm{li}(x) - \pi(x) < -K \frac{\sqrt{x}}{\log(x)} \log(\log(\log(x))).$$

Obviamente, esto prueba el teorema anterior tal como lo hemos enunciado, pero no muestra dónde están los cambios de signo de $\mathrm{li}(x) - \pi(x)$.

Encontrar el primer cambio de signo es un tema de indudable interés; pero, pese a los esfuerzos realizados, no se conoce ningún x que cumpla $\mathrm{li}(x) < \pi(x)$. Sí se sabe que existe alguno menor que ciertas cotas superiores concretas, pero son verdaderamente enormes. Por ejemplo, H. te Riele [31] probó que el primer cambio de signo ocurre para $x \leq 6.69 \cdot 10^{370}$.

x	$\pi(x)$	$\pi(x) - \frac{x}{\log(x)}$	$\mathrm{li}(x) - \pi(x)$	$\mathrm{Ri}(x) - \pi(x)$
10^2	25	3	5	1
10^3	168	23	10	0
10^4	1 229	143	17	−2
10^5	9 592	906	38	−5
10^6	78 498	6 116	130	29
10^7	664 579	44 158	339	88
10^8	5 761 455	332 774	754	97
10^9	50 847 534	2 592 592	1 701	−79
10^{10}	455 052 511	20 758 029	3 104	−1 828
10^{11}	4 118 054 813	169 923 159	11 588	−2 318
10^{12}	37 607 912 018	1 416 705 193	38 263	−1 476

Cuadro 1: Aproximación a $\pi(x)$ mediante $x/\log(x)$, $\mathrm{li}(x)$ y $\mathrm{Ri}(x)$ (valores redondeados al entero más cercano).

Vayamos ahora con la función $\mathrm{Ri}(x)$ de la cuarta columna, que se denomina función de Riemann (la introdujo Riemann en sus estudios sobre la distribución de los primos) y se define así:

$$\mathrm{Ri}(x) := \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \mathrm{li}(x^{1/n}) = 1 + \sum_{n=1}^{\infty} \frac{1}{n\zeta(n+1)} \frac{\log^n(x)}{n!}.$$

En realidad, la expresión de la derecha la dio J. P. Gram en 1884, y es útil porque converge muy rápido, aunque eso no nos preocupa para lo que ahora pretendemos; por supuesto, $\zeta(n+1)$ alude a la función zeta de Riemann, que para $s > 1$ se define mediante $\zeta(s) = \sum_{k=1}^{\infty} 1/k^s$.

Según vemos en el cuadro 1, parece que $\mathrm{Ri}(x)$ aproxima $\pi(x)$ mejor que $\mathrm{li}(x)$, es decir, que

$$|\,\mathrm{Ri}(x) - \pi(x)| \leq |\,\mathrm{li}(x) - \pi(x)|,$$

al menos para los valores de x que ahí se muestran. ¿Es verdad siempre?

Pues tampoco es cierto en general, sino que incluso puede ser $\mathrm{li}(x) = \pi(x)$ mientras $|\,\mathrm{Ri}(x) - \pi(x)|$ es bastante grande. De nuevo no se conocen valores de x concretos que violen la desigualdad anterior.

Ya que en este trabajo hemos mencionado la hipótesis de Riemann varias veces, y además nos acaba de aparecer la función zeta de Riemann, vamos a ver en qué consiste la hipótesis de Riemann, que es uno de los problemas abiertos más importantes de las matemáticas. Aunque hemos dicho que la función zeta de Riemann es $\zeta(s) = \sum_{k=1}^{\infty} 1/k^s$ para $s > 1$, en realidad esa expresión es válida para $s \in \mathbb{C}$ con $\mathrm{Re}(s) > 1$. Si $\mathrm{Re}(s) < 1$, esa serie ya no converge, así que no se puede usar esa definición. Pero, al igual que se puede hacer con muchas otras funciones de variable compleja, hay expresiones alternativas que son válidas en un rango más grande de valores de s y que proporcionan una función que coincide con la dada por la serie cuando $\mathrm{Re}(s) > 1$. Esto es lo que se denomina extensión analítica, y tal extensión es única, así que se usa la misma notación $\zeta(s)$ para denotar la función extensión.

Con la extensión analítica, es relativamente sencillo demostrar que $\zeta(-2k) = 0$ para k entero positivo; estos son los denominados «ceros triviales» de la zeta de Riemann. Se puede ver que el resto de los ceros están en la banda $0 < \mathrm{Re}(s) < 1$ y, por raro que parezca a quien no conozca el tema, están muy involucrados en la demostración del TNP. Es más, cuanto mejor se logre posicionar dónde están los ceros, más precisión se logra sobre la distribución de los números primos, en el sentido de que mejor se consigue acotar la diferencia $|\,\mathrm{li}(x) - \pi(x)|$. Lo mejor sería demostrar que todos los ceros están en el centro de la banda, es decir, cumplen $\mathrm{Re}(s) = 1/2$, y esto es lo que se denomina hipótesis de Riemann, formulada por primera vez por Bernhard Riemann en 1859.

El TNP nos dice que, cuando $x \to \infty$,

$$|\,\mathrm{li}(x) - \pi(x)| = o\left(\frac{x}{\log(x)}\right).$$

Si se lograra demostrar la hipótesis de Riemann, tendríamos mucha más precisión; en concreto que

$$|\,\mathrm{li}(x) - \pi(x)| \leq Cx^{1/2}\log(x)$$

para alguna constante C (válida para todo x suficientemente grande). Y hay más resultados que se saben probar si damos por cierta la hipótesis de Riemann, así que su demostración no sólo sería interesante por sí misma, sino que contribuiría de manera decisiva a agrandar el concimiento matemático. Pero, pese a que se ha conseguido encontrar ingentes cantidades de ceros en la recta crítica $\mathrm{Re}(s) = 1/2$, y ninguno fuera de ella (aparte de los ceros triviales antes mencionados), nada parece indicar que la demostración de la hipótesis de Riemann pueda estar cercana.

13. 200 años del retrato falso de Legendre

Queremos concluir con algo que ya no es una propiedad matemática que, tras muchos casos de éxito, falla, sino con un retrato que, tras ser la imagen utilizada para representar a un matemático durante aproximadamente dos siglos, finalmente se descubrió que no era él. Los detalles de la historia que ahora resumimos se pueden leer en [8].

Se trata del matemático francés Adrien-Marie Legendre (1752–1833), que hizo grandes contribuciones en análisis, teoría de números, mecánica celeste... Hasta que se descubrió el error, el retrato habitualmente asignado a Legendre se puede ver en la figura 8.

Figura 8: El falso retrato de Adrien-Marie Legendre.

En 2005, dos estudiantes de la Universidad of Estrasburgo descubrieron, sorprendidos, que ese retrato era el mismo que se usaba para representar al político francés Louis Legendre (1752–1797). En poco tiempo se confirmó que el retrato era, efectivamente, del político y no del matemático. El error proviene del hecho de que el retrato original estaba descrito con un simple «Legendre» (como se ve en la figura 8), y hay trazas de su atribución errónea al matemático desde, al menos, un libro de litografías publicado en 1833.

Faltaba encontrar una imagen que sí representara al matemático. En diciembre de 2008, un aficionado encontró, en la biblioteca el Instituto de Francia en París, un retrato suyo en el libro *Album de 73 portraits-charge aquarellés des membres de I'Institut*, una colección de 73 caricaturas de miembros de distintas *Académies*, y de algunos de sus alumnos, pintadas en 1820 por el artista francés Julien-Léopold Boilly. Allí aparece junto a Joseph Fourier, y es el único retrato conocido de Adrien-Marie Legendre. Puede verse en la figura 9.

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), no. 4, 364–367.

[2] M. Agrawal, N. Kayal y N. Saxena, PRIMES is in P, *Annals of Math. (2)* **160** (2004), 781–793.

[3] D. Borwein y J. M. Borwein, Some remarkable properties of sinc and related integrals, *Ramanujan J.* **5** (2001), 73–89.

[4] D. W. Boyd, Linear recurrence relations for some generalized Pisot sequences, *Advances in Number Theory (Kingston, ON, 1991)*, 333–340, Oxford Univ. Press, New York, 1993.

Figura 9: Caricaturas de Adrien-Marie Legendre (izquierda) y Joseph Fourier (derecha), por el artista francés Julien-Léopold Boilly.

[5] G. Berzsenyi, Math Investigations: Maximizing the greatest, *Quantum* **5** (1995), no. 5, 39.

[6] G. Brookfield, The coefficients of cyclotomic polynomials, *Math. Mag.* **89** (2016), 179–188.

[7] R. Crandall, K. Dilcher y C. Pomerance, A search for Wieferich and Wilson primes, *Math. Comp.* **66** (1997), 433–449.

[8] P. Duren, Changing faces: The mistaken portrait of Legendre, *Notices Amer. Math. Soc.* **56** (2009), no. 11, 1440–1443. También: portada del no. 11 y «About the cover», p. 1455.

[9] N. Elkies, On $A^4 + B^4 + C^4 = D^4$, *Math. Comput.* **51** (1988), 825–835.

[10] E. Fernández Moral y L. Roncal, Los números de Ramsey y el álgebra, *Gac. R. Soc. Mat. Esp.* **15** (2012), 651–674.

[11] R. E. Frye, Finding $95800^4+217519^4+414560^4 = 422481^4$ on the Connection Machine, *Supercomputing 88* (Proceedings of the 1988 ACM/IEEE Conference on Supercomputing, vol. II: Science and Applications, J. L. Martin y S. F. Lundstrom, eds.), 106–116, Orlando, FL, 1988.

[12] M. Gardner, Mathematical Games: patterns in primes are a clue to the strong law of small numbers, *Scientific American* **243** (dec. 1980), 18–28.

[13] A. Gasull, Gemmes matemàtiques, *Materials Matemàtics*, vol. 2019, treball no. 2, 88 pp.

[14] A. Gasull, Conjectures, *Butl. Soc. Catalana Mat.* 36 (2021), no. 1, 69–113.

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

[16] R. K. Guy, The second strong law of small numbers, *Math. Mag.* **63** (1990), 3–20.

[17] C. B. Haselgrove, A disproof of a conjecture of Pólya, *Mathematika* **5** (1958), 141–145.

[18] H. Helfgott, La conjetura débil de Goldbach, *La Gaceta de la RSME* **16** (2013), 709–726.

[19] M. J. H. Heule, O. Kullmann y V. W. Marek, Two-hundred-terabyte maths proof is largest ever, *Nature* **534** (2016), 17–18.

[20] M. J. H. Heule, O. Kullmann y V. W. Marek, Solving and verifying the Boolean Pythagorean triples problem via cube-and-conquer, *Theory and Applications of Satisfiability Testing – SAT 2016* (N. Creignou y D. Le Berre, eds.), 228–245, *Lecture Notes in Computer Science*, vol. 9710, Springer, Cham, 2016.

[21] L. J. Lander y T. R. Parkin, Counterexample to Euler's conjecture on sums of like powers, *Bull. Amer. Math. Soc.* **72** (1966), 1079.

[22] L. J. Lander y T. R. Parkin, A counterexample to Euler's sum of powers conjecture, *Math. Comp.* **21** (1967), 101–103.

[23] R. S. Lehman, On Liouville's function, *Math. Comp.* **14** (1960), 311–320.

[24] E. Lehmer, On the magnitude of the coefficients of the cyclotomic polynomials, *Bull. Amer. Math Soc.* **42** (1936), 389–392.

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

[26] J. I. Montijano, M. Pérez, L. Rández y J. L. Varona, Numerical methods with LuaLaTeX, *TUGboat* **35** (2014), 51–56.

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

[28] A. M. Odlyzko y H. J. J. te Riele, Disproof of the Mertens conjecture, *J. Reine Angew. Math.* **357** (1985), 138–160.

[29] V. Ponomarenko, *Mathematical Maturity via Discrete Mathematics*, Dover, 2019.

[30] D. Sadornil y J. L. Varona, Existen infinitos primos (desde Euclides hasta el siglo XXI), *Gac. R. Soc. Mat. Esp.* **24** (2021), 301–324.

[31] H. J. J. te Riele, On the sign of the difference $\pi(x) - \mathrm{li}(x)$, *Math. Comp.* **47** (1987), 323–328.

[32] H. Schmid, Two curious integrals and a graphic proof, *Elem. Math.* **69** (2014), 11–17.

[33] J. Shallit, Problem B-686, *Fib. Quart.* **29** (1991), 85.

[34] M. Tanaka, A numerical investigation on cumulative sum of the Liouville function, *Tokyo J. Math.* **3** (1980), 187–189.

[35] J. L. Varona, *Recorridos por la teoría de números*, 2.ª ed., Electolibris y Real Sociedad Matemática Española, Murcia, 2019. Disponible en `https://www.unirioja.es/cu/jvarona/libroTN.html`

[36] J. L. Varona, A couple of transcendental prime-representing constants, *Amer. Math. Monthly* **128** (2021), 922–928.

Juan Luis Varona
Departamento de Matemáticas y Computación
Universidad de La Rioja
`jvarona@unirioja.es`
`https://www.unirioja.es/cu/jvarona/`