Existen infinitos primos (desde Euclides hasta el siglo XXI)

por

Daniel Sadornil y Juan Luis Varona

Resumen. Hace bastante más de dos milenios, Euclides nos dejó escrito que existían infinitos números primos, con un lenguaje que no era el actual, pero con un rigor que prácticamente en nada difiere del de las matemáticas contemporáneas. Desde entonces han sido numerosos los matemáticos que han proporcionado otras pruebas del mismo resultado, a veces con ideas muy brillantes y aparentemente distantes del objetivo. En este artículo se recogen unas cuantas de estas demostraciones, agrupándolas por el tipo de técnicas que se han usado, que han sido de lo más variado, o por el camino que se ha seguido para probar la existencia de infinitos números primos. Como se pondrá de manifiesto a lo largo del artículo, se podría decir que «todos los caminos (salvo quizás un número finito) llevan... a la demostración».

Introducción

Si se le preguntase a una persona por algunos recuerdos de lo que aprendió de matemáticas en la escuela primaria, enseguida respondería con los números y las cuatro operaciones básicas del cálculo. Entre los no muchos conceptos matemáticos que se estudian a edad tan temprana, casi todos relacionados con la geometría y la aritmética, están los números primos. Si se hiciera la pregunta ¿qué es un número primo?, una posible respuesta sería ésta:

Definición. Un número primo es un número que sólo es divisible por el número uno y por él mismo.

Con esa definición, y centrándonos en los enteros positivos, el 1 sería un número primo. Esto tiene un pequeño inconveniente, y es que el teorema fundamental de la aritmética ya no se puede enunciar diciendo que «todo número mayor que 1 se puede escribir de forma única como producto de primos»; si 1 es primo, siempre podríamos añadir el factor 1^c con cualquier exponente c y se pierde la unicidad. Para enunciar el teorema de manera correcta, habría que precisarlo un poquito. Nada grave, pero, por eso y por alguna otra cosa que comentaremos un poco más adelante, actualmente se excluye al 1 de la definición de primos, simplemente añadiendo el requisito de que el número sea mayor que 1. Pero, históricamente, el 1 fue considerado como primo hasta el siglo xix, que es cuando se empezó a pensar que era más conveniente adoptar el criterio contrario (una buena referencia donde se trata la historia de la primalidad del 1 es el artículo de Caldwell y Xiong [5]).

De hecho, existen otras formas de definir número primo que directamente evitan que 1 sea un primo: «un número primo es un número que no es producto de dos números naturales más pequeños que él» o «un número primo es un número que tiene exactamente dos divisores». Desde luego, habría que comprobar la equivalencia entre las definiciones, pero no tiene ninguna dificultad.

Por otra parte, en matemáticas, el concepto de número primo se puede extender a contextos más generales que el de los números naturales. En ese sentido, se distingue entre números primos e irreducibles, que se definen así:

DEFINICIÓN. Sea p un entero mayor que 1. Entonces:

- Se dice que p es un número irreducible si no se puede descomponer en dos factores distintos de 1.
- Se dice que p es un número primo si, siempre que divide a un producto ab, divide a uno de los factores a o b.

De esta manera, ahora estamos llamando irreducibles a los números que antes llamábamos primos, y el concepto de número primo ya no es el mismo que antes. En los enteros positivos, esto no tiene relevancia, pues se demuestra con facilidad que ambos conceptos son equivalentes.

Pero, en contextos matemáticos más generales —en concreto, en teoría de anillos conmutativos—, ya no es lo mismo. Así, por ejemplo, en el anillo $\mathbb{Z}[\sqrt{-5}]$, el 3 es irreducible, pero no es primo puesto que divide a $(2+\sqrt{-5})(2-\sqrt{-5}) = 9$ y no divide a ninguno de los dos factores. Nos estamos saliendo de lo que aquí nos interesa —nosotros sólo vamos a hablar de primos «clásicos», es decir, considerando sólo los enteros positivos—, pero, realmente, todo esto es lo que ha dado la puntilla a la consideración o no del 1 como número primo. Al definir los conceptos de primo y de irreducible en el contexto de la teoría de anillos conmutativos, forzosamente hay que descartar las unidades (no vamos a aclarar qué es esto, pero, por supuesto, el 1 es una unidad, y también lo sería el -1 si no sólo habláramos de enteros positivos), y tener en cuenta la unicidad en la descomposición «salvo unidades». Este tipo de generalizaciones ha hecho que ya no exista ninguna controversia, y que las matemáticas actuales ya no consideren al 1 entre los primos.

Volviendo ya a los enteros positivos, una frase muy manida —pero no por ello menos cierta— es que los números primos son los ladrillos a partir de los cuales se construyen todos los números enteros y, por tanto, el estudio de los números enteros se reduce al de los primos. Uno de los resultados más básicos e importantes sobre los números primos es éste:

TEOREMA. *Existen infinitos números primos.*

Desde Euclides, alrededor del 300 a. C. hasta la actualidad, numerosos matemáticos han ideado diferentes demostraciones de este teorema. Tener demostraciones alternativas no sólo es bonito *per se*, sino que permite ver los resultados desde diferentes enfoques e incluso descubrir cómo áreas o partes de las matemáticas, en principio alejadas, se pueden cruzar en una demostración. Tal como afirmaba Sir Michael Atiyah (ver [40]):

> *«Cualquier buen teorema debe tener varias pruebas, cuantas más mejor. Por dos razones: generalmente, diferentes pruebas tienen diferentes fortalezas y debilidades, y se generalizan en diferentes direcciones, no son sólo repeticiones mutuas.»*

En este sentido, no se puede obviar a Erdős. Solía decir que no necesitas creer en Dios, pero, como matemático, deberías creer en *El Libro*, en cuyo interior están escritas las demostraciones más elegantes de todos los teoremas matemáticos, incluso los que todavía no están demostrados. Unas cuantas de estas demostraciones especialmente bellas están destinadas a probar la infinidad de los números primos.

Actualmente hay muchísimas formas de demostrar la existencia de infinitos primos, y el objetivo de este artículo es recoger un puñado de ellas. ¿Cuántas? Desde luego, si algún resultado matemático merece la pena de ser considerado como «perfecto» es éste, así que hemos optado por mostrar, de manera completa, un número perfecto de demostraciones (algunas otras, y pequeñas variantes, las comentaremos someramente). El número perfecto anterior al que hemos tomado es pequeño, y el siguiente demasiado grande; dejamos que el lector adivine cuántas demostraciones hemos incluido. La primera demostración que se muestra es, lógicamente, la que realiza Euclides en los *Elementos* —tal como la redactó él con un lenguaje geométrico y reinterpretada con lenguaje aritmético actual—, y la última es la propuesta por Lemmermeyer en 2020.

Por supuesto, la elección ha sido fruto del gusto personal de los autores. Si el lector lo desea, puede encontrar muchas otras. En concreto, los libros de Aigner y Ziegler [1, capítulo 1], Dickson [9, capítulo XVIII], Narkiewicz [32, capítulo 1], Pollack [38, capítulo 1] y Ribenboim [41, capítulo 1] hacen su propia selección de demostraciones. Así mismo hay un amplio abanico disponible en los artículos de Granville [17], Městrović [27] (contiene casi 200) y Yamada [52]. Hemos intentado citar las fuentes originales de las demostraciones que hemos presentado; pero, además, casi todas ellas están recogidas en una o varias de las recopilaciones anteriores.

Además de esta introducción, el artículo se divide en seis secciones dependiendo del método o la herramienta matemática usada para demostrar la infinitud de los números primos. En la sección 1, se muestra la demostración de Euclides y sus variantes en las que, a partir de un número finito de primos, se construye otro número que no es divisible por los primos anteriores. La sección 2 muestra las demostraciones que parten de la idea de Goldbach de construir sucesiones de enteros cuyos términos son primos entre sí. En la sección 3 se presentan algunas demostraciones que utilizan sumas infinitas, tal como hizo Euler. La sección 4 está dedicada a las demostraciones basadas en técnicas básicas de combinatoria y aritmética. La sección 5 recoge la prueba topológica de Furstenberg y dos versiones de ésta desde otro punto de vista. Finalmente, en la sección 6 se muestran otras demostraciones donde se usan técnicas diferentes a las anteriores, y se mencionan algunas muy recientes.

En todo el artículo, usaremos p, a veces con subíndices, para denotar primos. Además, cuando escribamos $\sum_p$ o $\prod_p$ nos estaremos refiriendo a que la correspondiente suma o producto se extiende sobre primos, quizás con alguna condición si es que se indica. Para abreviar, prescindiremos de usar mcd para indicar el máximo co-

mún divisor, y escribiremos simplemente $(a, b) = \mathrm{mcd}(a, b)$. No obstante, el mínimo común múltiplo lo denotaremos con $\mathrm{mcm}(a, b)$.

1. EUCLIDES (CONSTRUCCIÓN)

Como ya se ha mencionado, la primera demostración de la que se tiene constancia de la infinitud de los números primos se debe a Euclides, y es la Proposición 20 del Libro IX de los *Elementos* (estamos aquí siguiendo la numeración de [12], la edición moderna en español más conocida, en otras ediciones la numeración de las proposiciones puede variar ligeramente). No obstante, Euclides no usa el enunciado actual, pues no manejaba el concepto de «infinito». Su enunciado es

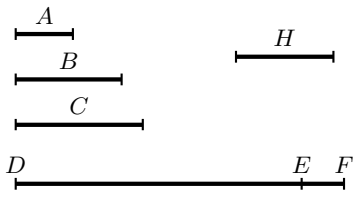
> «*Hay más números primos que cualquier cantidad propuesta de números primos*».

Para su demostración es necesario el concepto de medida entre números; es decir, un número es medido por otro número si el primero puede descomponerse en partes iguales, todas ellas iguales al segundo. Además, se define número primo como aquél que sólo es medido por la unidad. Por otra parte, la demostración de Euclides usa el hecho de que, dado un entero positivo mayor que 1, hay un primo que lo divide (el propio número si éste es primo). Este hecho se deduce de la Proposición 31 del Libro VII que afirma que «*Se mide cualquier número compuesto por algún número primo*».

El texto y los gráficos concretos que aparecen en los *Elementos* pueden variar ligeramente entre las distintas ediciones. Pero, aproximadamente, lo que escribe Euclides en la Proposición 20 del Libro IX es lo que sigue:

DEMOSTRACIÓN 1 (GEOMÉTRICA). Sean A, B y C los números primos propuestos. Digo que hay más números primos que A, B, C.

Pues tómese DE el número menor medido por A, B, C, y añádase a DE la unidad EF. Entonces DF es primo o no. Sea primo en primer lugar; entonces han sido hallados los números primos A, B, C, y DF, que son más que A, B, y C.



Consideremos ahora que DF no sea primo; entonces es medido por algún número primo: sea medido por el número primo H. Digo que H no es el mismo que ninguno de los números A, B, C. Pues si fuera posible, séalo. Pero A, B, C miden a DE, entonces H medirá también a DE. Pero mide asimismo a DF; y H, siendo un número, medirá también a la unidad restante EF; lo cual es absurdo. Luego H no es el mismo que ninguno de los números anteriores A, B, C. Y se ha supuesto que es primo. Por consiguiente, han sido hallados más números primos que la cantidad propuesta de los números A, B, C. □

En la demostración anterior, la expresión «tómese DE el número menor medido por A, B, C» equivale, tal como lo decimos ahora, a «tómese DE el mínimo común

Demostración de la existencia de infinitos primos en la edición de los *Elementos* de Euclides del impresor Erhard Ratdolt (Venecia, 1482); en esta edición, dicha demostración es la Proposición 21 del Libro IX. Ejemplar de la Biblioteca del Monasterio de San Millán de Yuso (La Rioja), cortesía de la Fundación San Millán de la Cogolla, `http://bibliotecavirtual.larioja.org/bvrioja/i18n/consulta/registro.do?id=3089`

múltiplo de A, B, C» (y, como A, B, C son primos distintos, DE sería su producto). Reescribiendo esta demostración en notación y lenguaje aritmético moderno se tiene la prueba que acostumbra a verse en numerosos textos:

Demostración 1 (Aritmética). Supongamos que existe una cantidad finita de números primos (distintos) $p_1, p_2, \ldots, p_r$. Sea $N = p_1 p_2 \cdots p_r + 1$. Si N es primo, N es un primo que no está en nuestra lista, ya que es mayor que todos los demás. Si N no es primo, existirá un primo p que lo divide, pero N tiene resto 1 al dividirlo por p_i para cada $1 \leq i \leq r$, por tanto p no puede ser ninguno de los primos p_i. En ambos casos, nuestra lista inicial es incompleta. □

Schaumberger (1985) [45] reinterpreta esta demostración usando el principio del palomar: como hay exactamente r primos, cualquier lista de $r + 1$ enteros distintos mayores que 1 contiene dos que comparten un divisor primo; ninguna pareja de enteros de la lista p_1, p_2,..., p_r y $p_1 \cdot p_2 \cdots p_r + 1$ comparte un divisor, así que necesariamente la lista inicial de r primos no es completa.

Merece la pena comentar que la demostración de Euclides sólo puede asegurar que $N = p_1 p_2 \cdots p_r + 1$ es divisible por algún número primo diferente de la lista inicial, pero no que el propio N sea un nuevo primo. Por ejemplo $715 = 2 \cdot 3 \cdot 7 \cdot 17 + 1$ no

es primo porque $715 = 5 \cdot 11 \cdot 13$. Tampoco ocurre así si se toman todos los números primos menores que uno dado, pues $30\,031 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 59 \cdot 509$ no es primo. De hecho, para $n < 100\,000$ sólo hay 19 valores de n tales que el número $N = \prod_{p \le n} p + 1$ es primo (se denominan «primos primoriales»).

La idea básica de la demostración de Euclides es, suponiendo que existe sólo una cantidad finita de primos, construir un nuevo número que no sea divisible por ninguno de los primos. Diferentes construcciones de este número dan lugar a variantes de la demostración. Posiblemente la variación más simple (atribuida a Hermite, [32, § 1.1.3]) consiste en tomar $N = n! + 1$; inmediatamente se sigue que, si p_n es el divisor primo más pequeño de N, necesariamente $p_n > n$ y, por tanto, se tiene así una sucesión infinita de números primos. También es sencilla la idea de Kummer (1878) [41, § 1.I], que parte del entero $N = p_1 p_2 \cdots p_r - 1$:

DEMOSTRACIÓN 2. Supongamos que existe una cantidad finita de números primos distintos $p_1 < p_2 < \cdots < p_r$, $r > 1$. Sea $N = p_1 p_2 \cdots p_r > 2$. Entonces, $N - 1$ debería tener un divisor primo p_i en común con N, pero esto es absurdo pues, si para algún $1 \le i \le r$, el primo p_i divide tanto a N como a $N - 1$, entonces divide a su diferencia, es decir, p_i divide a 1. En consecuencia, existe algún primo más. □

Así mismo, Stieltjes (1890) [32, § 1.1.3] propone una demostración a partir del entero $N = p_1 p_2 \cdots p_r$ factorizándolo en dos enteros.

DEMOSTRACIÓN 3. Supongamos que existe una cantidad finita de números primos distintos $p_1, p_2, \ldots, p_r$, y sea $N = p_1 p_2 \cdots p_r$. Este entero puede escribirse como $N = a \cdot b$ con a y b enteros positivos primos entre sí (pues cada factor primo p de N sólo lo divide una vez). Sea $M = a + b > 1$. Es claro que ningún número primo de la lista puede dividir a M, pues entonces a y b no serían primos entre sí. Entonces, o bien M es un primo diferente de los de la lista, o bien es divisible por otro primo que tampoco está en la lista. En ambos casos la lista inicial de primos es incompleta. □

La demostración original de Euclides es un caso particular de la de Stieltjes tomando uno de los factores igual a 1. Por otra parte, Boije af Gennäs (1893) [4] presenta una variante de la demostración anterior tomando $N = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ con $N = a \cdot b$ y $M = a - b > 1$. Si además $M < (p_r + 2)^2$, se puede demostrar que M es primo. La demostración de Kummer es un caso particular de ésta tomando todos los exponentes iguales a 1 y $b = 1$.

Braun (1899) [32, § 1.1.3] (y posteriormente, de manera similar, Métrod (1917) [28]) en lugar de tomar el producto de números primos considera la suma de inversos de primos:

DEMOSTRACIÓN 4. Supongamos que sólo hay una cantidad finita de números primos distintos $p_1, p_2, \ldots, p_r$, con $p_1 = 2$, $p_2 = 3$ y $p_3 = 5$ los tres primeros, y sea $N = p_1 p_2 \cdots p_r$. La suma de los inversos de los primos es mayor que 1, pues $\sum_{i=1}^{r} \frac{1}{p_i} = \frac{a}{N} \ge \frac{1}{2} + \frac{1}{3} + \frac{1}{5} = \frac{31}{30}$. Por tanto, el numerador a tendrá un factor primo p. Si existiese $1 \le k \le r$ con $p = p_k$, entonces, como $a = \sum_{i=1}^{r} \frac{N}{p_i}$, es claro que p_k

debería dividir a $\frac{N}{p_k}$, lo que resulta absurdo. Así pues, el primo p no puede ser uno de los de nuestra lista inicial. □

Euler, en 1736 (publicado póstumamente en 1862, [9, § XVIII, p. 413]), modifica ligeramente el argumento de Euclides usando la función multiplicativa $\varphi(n) = \text{card}\{a : 1 \leq a \leq n,\ (a, n) = 1\}$ que él mismo estudió.

Demostración 5. Suponemos que existe una cantidad finita de números primos distintos $p_1, p_2, \ldots, p_r$, y sea $N = p_1 p_2 \cdots p_r$. Entonces, el número de enteros menores que N y coprimos con él es

$$\varphi(N) = \prod_{i=1}^{r} (p_i - 1) \geq 2 \cdot 4 \cdots \geq 2.$$

Por tanto, debe existir al menos un número entero a perteneciente al intervalo $[2, N]$ coprimo con N. Y ese a tendrá un factor primo p diferente de todos los p_i, con lo que hemos llegado a un absurdo. □

Hay más construcciones que nos permiten determinar nuevos números primos a partir de una lista inicial; por ejemplo, utilizando el pequeño teorema de Fermat, Granville [18] prueba que si $p_1, p_2, \ldots, p_r$ es una lista finita de primos impares y tomamos $L = \prod_{i=1}^{r} (p_i - 1)$, los enteros $2^L + 1$ y $2^{L+1} - 1$ no son divisibles por ninguno de los primos iniciales.

La demostración de Euclides puede adaptarse para probar la existencia de infinitos primos con algunas características. Por ejemplo, para demostrar que existen infinitos primos $p \equiv 3 \bmod 4$: si $p_1, p_2, \ldots, p_r$ es una cantidad finita de números primos de la forma $4n + 3$, se toma $N = 4p_1 p_2 \cdots p_r - 1$ y se procede de manera similar. También para primos $p \not\equiv 1 \bmod m$, $m > 2$, considerando números de la forma $N = m p_1 p_2 \cdots p_r - 1$ con $p_1, p_2, \ldots, p_r$ una lista de dos o más primos de estas características. Tampoco es muy complicado probar la existencia de infinitos primos de la forma $4n+1$ (o algunas otras), pero se requiere algo más de trabajo que sólo las ideas de Euclides. Finalmente, hemos de destacar que, para progresiones aritméticas arbitrarias, Dirichlet, en 1837, demostró que si a, b son enteros positivos coprimos, entonces la sucesión $\{an+b\}_{n=1}^{\infty}$ contiene infinitos primos (por lo que siempre existen infinitos números de la forma $2020n + 2021$, por ejemplo).

2. Goldbach (sucesiones)

La idea de Goldbach (en una carta a Euler fechada en 1730, [41, § 1.II]) consiste en que cualquier sucesión infinita de enteros positivos $\{a_n\}_{n=0}^{\infty}$ tal que $(a_i, a_j) = 1$ si $i \neq j$ conduce a una prueba del teorema de Euclides. En efecto, cada elemento de la sucesión será divisible por un primo; más en concreto, a_1 será divisible por un primo p_1; como a_1 y a_2 son primos entre sí, cualquier primo p_2 que divida a a_2 será distinto de p_1, y así sucesivamente. Esta idea —que algunos textos atribuyen a Hurwitz o incluso a Pólya y Szegő— es, posiblemente, la primera que permitió dar una demostración esencialmente diferente de la de Euclides. En la práctica,

una demostración de este tipo se reduce a construir una sucesión con las características buscadas. La de Goldbach usa la sucesión determinada por los números de Fermat $2^{2^n}+1$:

DEMOSTRACIÓN 6. Sea $F_n = 2^{2^n}+1$. Por inducción, es fácil probar que $F_n - 2 = F_0F_1\cdots F_{n-1}$. Por tanto, si $n < m$ entonces F_n divide $F_m - 2$. Luego, si existe un primo que divide a ambos, dividirá a $F_m - (F_m - 2) = 2$, lo cual es absurdo pues todos los números de Fermat son impares. □

Esta demostración, además, determina también un cota superior (nada fina) para el primo n-ésimo p_n, concretamente $p_n \leq 2^{2^{n-1}}+1$.

Los números de Fermat pueden definirse recursivamente tomando $F_{-1} = 1$ y $F_n = 2 + \prod_{i=-1}^{n-1} F_i$. Sylvester (1880) [48] propone una generalización a partir de una relación de recurrencia donde $a_0 = 2$ y $a_n = 1 + \prod_{i=0}^{n-1} a_i$ (equivalentemente, $a_{n+1} = a_n^2 - a_n + 1$) que cumple también que dos términos cualesquiera de la sucesión son primos entre sí.

Pólya (1921) [39] demuestra, para una gran clase de sucesiones definidas mediante fórmulas de recurrencia lineales, que éstas contienen una subsucesión creciente infinita de términos coprimos dos a dos. La sucesión recurrente por excelencia es la sucesión de Fibonacci, $f_0 = 0$, $f_1 = 1$, $f_n = f_{n-1} + f_{n-2}$ que Wunderlich (1965) [51] usó para demostrar la infinitud de los números primos. En la demostración se usa una conocida propiedad de los números de Fibonacci: $(f_n, f_m) = f_{(n,m)}$ (es decir, los números de Fibonacci no siempre son coprimos dos a dos, al contrario de lo que ocurría con los números de Fermat).

DEMOSTRACIÓN 7. Supongamos que, además de $p = 2$, sólo hay una cantidad finita de primos $p_1, p_2, \ldots, p_r$. Los correspondientes números de Fibonacci $f_{p_1}, f_{p_2}, \ldots, f_{p_r}$ son mayores que 1 y coprimos dos a dos, pues $(f_{p_i}, f_{p_j}) = f_{(p_i,p_j)} = 1$ si $i \neq j$. Entonces, cada uno de los primos debe dividir a uno y sólo uno de los f_{p_j}, y cada uno de los f_{p_j} es divisible por un único número primo. Pero $f_{19} = 4181 = 37 \cdot 113$, que tiene dos factores. □

Hemminger (1966) [20] generaliza la idea anterior y muestra que, de igual forma, se pueden usar sucesiones $\{a_n\}_n$ que cumplan cuatro condiciones, a saber: que no existan elementos repetidos, que si p es primo entonces $a_p \neq 1$, que exista un número primo p tal que a_p no es primo, y que si $(n, m) = 1$ entonces $(a_n, a_m) = 1$. La sucesión $a_n = 2^n - 1$ (números de Mersenne si n es primo) cumple también $(2^n - 1, 2^m - 1) = 2^{(n,m)} - 1$, así que de nuevo permite probar la infinitud de los números primos, pues $2^4 - 1 = 15 = 3 \cdot 5$.

Pero, tal como ya habíamos visto antes con el ejemplo de Sylvester, no únicamente pueden usarse recurrencias lineales. Harris (1956) [19] prueba que si a_0, a_1, a_2 son enteros positivos coprimos dos a dos y se define $a_n = a_0a_1a_2\cdots a_{n-3}a_{n-1} + a_{n-2}$, la sucesión $\{a_n\}_n$ está formada por enteros coprimos dos a dos (no necesariamente positivos, pero una subsucesión suya sí tiene esta propiedad adicional).

Otros autores han dado ejemplos de sucesiones recurrentes no lineales de términos coprimos dos a dos. Por ejemplo, Edwards (1964) [10] define las sucesiones $a_n =$

$a_{n-1}(a_{n-1}-q)+q$ con $(a_1,q)=1$ y $a_1>q$, $b_n=b_{n-1}(b_{n-1}+q)-q$ con $(b_1,q)=1$ y $b_1>1$, o $c_n=2c_{n-1}^2-1$ con $c_1>1$; y Mohanty (1978) [30] usa la sucesión $a_n=a_n^2-ma_n+m$ con $a_0=a+m$ y $(a,m)=1$.

Por otra parte, si f es un polinomio con coeficientes enteros (en lo que sigue, f^n significa componer n veces el polinomio f) y r un entero, Lambek y Moser (1957) [22] demuestran que $f^n(r)$ es una sucesión de términos coprimos dos a dos si y sólo si $(f^k(0),f^n(r))=1$ para todo n,k, y determinan todos los polinomios $f(x)$ para los cuales se cumple esta condición para todo entero r. Dichos polinomios vienen dados por

$$1+x(x-1)g(x),\quad 1-x-x^2+x(x^2-1)g(x),\quad 1-2x^2+x(x^2-1)g(x),$$
$$-1+x(x+1)g(x),\quad x^2-x-1+x(x^2-1)g(x),\quad 2x^2-1+x(x^2-1)g(x),$$

con $g(x)$ cualquier polinomio con coeficientes enteros.

De forma diferente, Sierpiński (1970) [47, § III] prueba que existen progresiones aritméticas formadas por enteros positivos coprimos dos a dos tan largas como se desee (por supuesto, esto implica que existen tantos primos distintos como se desee):

Demostración 8. Para cada $k\geq 1$, sean los números $k!\,n+1$, $1\leq n\leq k$. Veamos que son coprimos dos a dos. Dados dos de ellos cualesquiera, $k!\,r+1$ y $k!\,s+1$ con $1\leq r<s\leq k$, sea $d=(k!\,r+1,k!\,s+1)$. Es claro que $d\mid \big(s(k!\,r+1)-r(k!\,s+1)\big)=s-r<k$, luego $1\leq d<k$ y $d\mid k!$. Como $d\mid(k!\,r+1)$, también $d\mid 1$, y por tanto $d=1$. □

Sierpiński [47, § II, problemas 42 y 43] también muestra que las sucesiones de los números triangulares $a_n=\frac{n(n+1)}{2}$ y de los números tetraédricos $a_n=\frac{n(n+1)(n+2)}{6}$ contienen una subsucesión infinita de enteros coprimos dos a dos.

Para concluir esta sección, la última demostración de la infinitud de los números primos a partir de sucesiones que presentamos es la de Saidak (2006) [43], que construye una sucesión de forma que cada nuevo término tiene, al menos, un factor primo más que el anterior:

Demostración 9. Sea $a_1=m>1$ entero y $a_2=m(m+1)$; como $(m,m+1)=1$, estos dos números no tienen factores primos en común, luego a_2 tiene, al menos, dos factores primos distintos. Sea ahora $a_3=a_2\cdot(a_2+1)$; igualmente $(a_2,a_2+1)=1$ y tienen factores primos distintos. Como a_2 tiene dos factores primos diferentes, a_3 tiene como mínimo tres factores primos distintos. Iterando este procedimiento, $a_n=a_{n-1}(a_{n-1}+1)$ es divisible por al menos n primos distintos. Luego deben existir infinitos números primos. □

Siguiendo esta idea, Maji (2015) [24] define la sucesión $a_1=m^{\alpha_{1,1}}$, $a_2=(m+1)^{\alpha_{2,1}}$ y, en general, $a_n=a_1^{\alpha_{n,1}}a_2^{\alpha_{n,2}}\cdots a_{n-2}^{\alpha_{n,n-2}}+a_{n-1}^{\alpha_{n,n-1}}$ con $\alpha_{i,j}$ enteros positivos, y demuestra que los términos de esta sucesión son coprimos dos a dos.

3. EULER (SUMAS INFINITAS)

En 1737 [13, teorema 19], Euler prueba que

$$\sum_{p \text{ primo}} \frac{1}{p} = \infty. \tag{1}$$

Por supuesto, esto proporciona una demostración de la existencia de infinitos primos, ya que, en otro caso, la suma sería finita.

Las demostraciones originales de Euler no se pueden analizar desde el punto de vista del rigor matemático actual. Él, y los matemáticos de su época, estaban interesados en descubrir, y las dosis de ingenio e intuición que desplegaron eran, ciertamente, envidiables. Pero en la matemática del siglo XVIII no se había instalado aún el rigor de las definiciones y de las demostraciones (de hecho, podríamos decir que dicho rigor se había «relajado», pues las matemáticas griegas sí lo tenían). Así pues, no veremos aquí los resultados de Euler tal como él los probó, sino con interpretaciones actuales bastante libres construidas sobre sus ideas.

Reinterpretado de manera suficientemente general, y con notación actual, podemos decir que del trabajo de Euler se desprende que, si f es una función completamente multiplicativa (es decir, si f no es la función nula y cumple $f(n \cdot m) = f(n)f(m)$), entonces

$$\sum_{n=1}^{\infty} f(n) = \prod_{p \text{ primo}} \frac{1}{1 - f(p)} \tag{2}$$

(en principio, esto requiere asumir que la serie sea convergente, pero con un poco de cuidado se puede prescindir de esa hipótesis); los detalles se pueden ver en [50, § 9.1]. Este resultado, que se conoce como identidad de Euler, es la clave de diversas demostraciones sobre la infinidad de los números primos; entre ellas, algunas de las que veremos en esta sección. En particular, y sin entrar en detalles, aplicando (2) a la función $f(n) = 1/n$ y usando que $\sum_{n=1}^{\infty} 1/n = \infty$ (esto lo había probado Nicolás de Oresme hacia 1360), se desprende la divergencia de la serie (1).

No vamos ahora a probar (2) con la generalidad que ahí se anuncia. Al contrario, y de momento, simplemente vamos a seguir el tipo de razonamientos que usa Euler sólo hasta el punto de conseguir probar que existen infinitos primos. De ese modo, se puede dar la siguiente demostración, tal como aparece en [41, § 1.III]:

DEMOSTRACIÓN 10. Observemos primero que, si p y q son dos primos distintos, al multiplicar las progresiones geométricas

$$\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1 - 1/p} \quad \text{y} \quad \sum_{k=0}^{\infty} \frac{1}{q^k} = \frac{1}{1 - 1/q}$$

obtenemos

$$1 + \frac{1}{p} + \frac{1}{q} + \frac{1}{p^2} + \frac{1}{pq} + \frac{1}{q^2} + \cdots = \frac{1}{1 - 1/p} \cdot \frac{1}{1 - 1/q},$$

de modo que en el lado izquierdo de esta expresión están los inversos de todos los números de la forma $p^h q^k$ con $h, k \geq 0$. Esto mismo se puede hacer si, en vez de dos, multiplicamos un número finito de series. En concreto, y si suponemos que sólo existe un número finito de primos $p_1, p_2, \ldots, p_r$, el producto de las r identidades

$$\sum_{k=0}^{\infty} \frac{1}{p_i^k} = \frac{1}{1-1/p_i}, \quad 1 \leq i \leq r,$$

es

$$\prod_{i=1}^{r} \left(\sum_{k=0}^{\infty} \frac{1}{p_i^k} \right) = \prod_{i=1}^{r} \frac{1}{1-1/p_i}. \tag{3}$$

Además, cada entero positivo n se puede escribir de manera única como producto de primos (en otras palabras, de los $p_1, p_2, \ldots, p_r$ cada uno elevado a una potencia ≥ 0), así que cada $1/n$ será uno de los sumandos que aparece al desarrollar el lado izquierdo de (3), es decir,

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{i=1}^{r} \frac{1}{1-1/p_i}.$$

Pero esto es imposible, puesto que $\sum_{n=1}^{\infty} 1/n = \infty$. □

Los argumentos de Euler para probar algo como (2) no están en [13], sino que requieren herramientas más potentes. Un parte importante de las herramientas que se usan están desarrolladas en el capítulo XV de su libro *Introductio in Analysin Infinitorum*, publicado en 1748 (ver la edición traducida y anotada [14]); en particular, allí aparece el desarrollo en potencias de la función $\log(1-x)$, que resulta clave en lo que mostraremos a continuación. De nuevo el razonamiento no es original de Euler, sino moderno.

Sin recurrir a la reducción al absurdo, empleada con éxito en la demostración anterior, si se pretende dar una demostración de (1) o (2) ya no estamos suponiendo que hay un número finito de primos, luego, haciendo lo mismo, ya no estaríamos multiplicando un número finito de series. En lugar de $\sum_{k=1}^{\infty} 1/p^k = 1/(1-1/p)$ conviene usar

$$\sum_{k=0}^{\infty} \frac{1}{p^{sk}} = \frac{1}{1-1/p^s}, \quad \text{con } s > 1.$$

Haciendo como en (3) pero con todos los primos, y utilizando de nuevo la unicidad de la descomposición de cada entero n como producto de primos, lo que tenemos es

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ primo}} \left(\sum_{k=0}^{\infty} \frac{1}{p^{sk}} \right) = \prod_{p \text{ primo}} \frac{1}{1-1/p^s}.$$

Tomando logaritmos,

$$\log \left(\sum_{n=1}^{\infty} \frac{1}{n^s} \right) = \log \left(\prod_{p \text{ primo}} \frac{1}{1-1/p^s} \right) = - \sum_{p \text{ primo}} \log(1-1/p^s).$$

Pero $x \leq -\log(1-x) \leq x + x^2$ cuando $0 \leq x \leq 1/2$, así que podemos poner $-\log(1-x) = x + R(x)$ para cierta función $R(x)$ que cumple $0 \leq R(x) \leq x^2$ cuando $0 \leq x \leq 1/2$. En consecuencia,

$$\log\left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right) = \sum_{p \text{ primo}} \frac{1}{p^s} + \sum_{p \text{ primo}} R\left(\frac{1}{p^s}\right). \tag{4}$$

Hagamos ahora tender $s \to 1$. El sumando de la derecha converge como consecuencia de la cota $|R(x)| \leq x^2$. En cambio, $\sum_{n=1}^{\infty} 1/n^s \to \infty$ cuando $s \to 1$, pues la serie armónica $\sum_{n=1}^{\infty} 1/n$ diverge. Así, la única manera de que (4) siga siendo cierta cuando $s \to 1$ es que $\sum_p 1/p = \infty$, tal como queríamos comprobar.

Realmente, existen otras maneras, numerosas incluso, de probar que $\sum_p 1/p = \infty$ (y, por tanto, la infinidad de los números primos) sin seguir los argumentos de Euler. Pero, por lo general, estas demostraciones utilizan técnicas menos elementales que las que se usan en la mayoría de las demostraciones de la infinitud de los números primos. Veremos aquí únicamente la prueba que dio Erdős en 1938 [11].

DEMOSTRACIÓN 11. Comprobaremos (1) por reducción al absurdo, así que comencemos suponiendo que la serie es convergente; en ese caso, existirá un entero b tal que $\sum_{p \geq b} 1/p < 1/2$. Para x entero positivo, sean los conjuntos

$$M_x = \{n \leq x : \text{todos sus divisores primos son} < b\},$$
$$N_x = \{n \leq x : \text{tiene un divisor primo} \geq b\},$$

cuyos cardinales cumplen $\text{card}(M_x) + \text{card}(N_x) = x$. La cantidad de números menores o iguales que x divisibles por p es $\lfloor x/p \rfloor$, así que

$$\text{card}(N_x) \leq \sum_{p \geq b} \left\lfloor \frac{x}{p} \right\rfloor \leq \sum_{p \geq b} \frac{x}{p} \leq \frac{x}{2},$$

y, por tanto, $\text{card}(M_x) \geq x/2$. Por otra parte, cualquier $n \in M_x$ lo podemos escribir como $n = k^2 m$ con $m \in M_x$ y libre de cuadrados. Pero esto implica que $k \leq \sqrt{n} \leq \sqrt{x}$ y, como la cantidad de números libres de cuadrados de M_x es $\leq 2^b$, de aquí se sigue que $\text{card}(M_x) \leq 2^b \sqrt{x}$. Así pues, $x/2 \leq \text{card}(M_x) \leq 2^b \sqrt{x}$, lo cual es falso sin más que tomar x suficientemente grande. □

Hay otros procedimientos para demostrar la divergencia de la suma de los inversos de los números primos que también tienen bastante interés. Por ejemplo, Niven, en 1971 [33], lo demuestra a partir de $e^x > 1 + x$ y de la divergencia de la suma de los inversos de enteros libres de cuadrados. Pinasco, en 2009 [37], usa los mismos argumentos que los de la demostración 17 que veremos más adelante, llevándolos un poco más lejos.

Pero dejemos ya las demostraciones de la divergencia de $\sum_p 1/p$, y sigamos con algunas demostraciones de la infinidad de los números primos basadas en series. Una de ellas es la atribuida a J. Hacks (a finales del siglo XIX) [38, § 1.4], que presentamos a continuación:

Demostración 12. Partimos de la igualdad $\prod_p 1/(1-1/p^2) = \pi^2/6$ (que es, simplemente, reescribir la suma $\sum_{k=1}^{\infty} 1/k^2 = \pi^2/6$ según la identidad de Euler (2)). Si hubiera sólo una cantidad finita de primos, el producto sería un número racional, así que π sería racional. Pero sabemos que π es irracional, luego forzosamente debe haber infinitos primos. □

Otra demostración que prueba la existencia de infinitos primos ayudándose de una serie es la que dio Perott (1881) [36]:

Demostración 13. Supongamos que hay un número finito de primos $p_1, p_2, \ldots, p_r$. Dado cualquier entero N mayor que todos esos primos, sea $\theta(N)$ la cantidad de enteros entre 1 y N que no son divisibles por un cuadrado, con lo cual $\theta(N) \geq N - \sum_{k=1}^{r} \lfloor N/p_k^2 \rfloor$ (pues el número de enteros menores o iguales que N divisibles por p_k^2 es, a lo sumo, N/p_k^2). Ahora, usando que $\sum_{k=1}^{\infty} 1/k^2 = \pi^2/6$, tenemos

$$\theta(N) \geq N\left(1 - \sum_{k=1}^{r} \frac{1}{p_k^2}\right) > N\left(1 - \sum_{k=2}^{\infty} \frac{1}{k^2}\right) > N\left(2 - \frac{\pi^2}{6}\right) > \frac{N}{3}$$

(en realidad, bastaría saber que $\sum_{k=1}^{\infty} 1/k^2 < 2$, una propiedad bastante sencilla, y a partir de aquí la demostración sigue de forma similar usando, en lugar del $N/3$, un aN con alguna constante positiva a).

Por otra parte, todos los números sin factor cuadrático entre 1 y N tendrán la forma $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ con exponentes $e_j = 0$ o 1, así que habrá, como mucho, 2^r de tales números; es decir, $\theta(N) \leq 2^r$. En consecuencia, $2^r \geq \theta(N) > N/3$. De aquí, $N < 3 \cdot 2^r$, así que $3 \cdot 2^r$ sería una cota superior para los números naturales, algo inexistente. □

Merece la pena comentar que la prueba de Perott que acabamos de ver acota el número de enteros positivos $\leq N$ no divisibles por un cuadrado por un procedimiento radical: excluye los conjuntos de enteros no divisibles por cada cuadrado k^2 y no sólo los divisibles por el cuadrado de un primo. Este argumento es, esencialmente, la base de las métodos de criba desarrollados para proporcionar estimaciones a la cantidad de enteros que satisfacen determinadas propiedades. De hecho, y tal como hace Kilford en [21], la propia demostración de Perott se puede adaptar fácilmente llamando $\theta_m(N)$, con $m \geq 2$, a la cantidad de enteros positivos que no se pueden dividir por alguna potencia m-ésima, y usando que $\sum_{k=1}^{\infty} 1/k^m \leq \sum_{k=1}^{\infty} 1/k^2 = \pi^2/6$.

Finalmente, podemos mencionar que a partir de la irracionalidad de e y del desarrollo de la función e^{-x} como un producto infinito que involucra la función de Möbius, Meštrović [27] determina también la infinitud de los números primos.

4. Combinatoria y Aritmética

En esta sección incluiremos varias demostraciones que, de alguna forma, emplean ideas de combinatoria. A menudo, se emplea el teorema fundamental de la aritmética para expresar cada entero, de manera única, como producto de primos, cada primo

elevado a un exponente, y la combinatoria entra en juego al contar el número de exponentes que satisfacen ciertos requisitos.

La primera demostración que presentamos que usa ideas combinatorias es una de Thue (1897), que se puede encontrar en [41, § 1.IV]:

DEMOSTRACIÓN 14. Sean n y k dos enteros positivos cualesquiera que satisfacen $(1+n)^k < 2^n$, y sean $p_1 = 2$, $p_2 = 3, \ldots$, p_r todos los primos $\leq 2^n$. Cada entero positivo $m \leq 2^n$ se puede escribir (de manera única) en la forma $m = 2^{e_1}3^{e_2}\cdots p_r^{e_r}$ para ciertos exponentes $e_i \geq 0$; asimismo se cumplirá $e_i \leq n$, ya que $m \leq 2^n$. En esas condiciones, puesto que el número de elecciones de los $e_1, e_2, \ldots, e_r$ que satisfacen $0 \leq e_i \leq n$ es $(n+1)^r$, tendremos $(1+n)^k < 2^n \leq (1+n)^r$; en particular, $r > k$. Pero cualquier $k \geq 1$ cumple $(1+2k^2)^k < 2^{2k^2}$, ya que $1 + 2k^2 < 2^{2k}$. Así que, sea cual sea el k, siempre ponemos tomar $n = 2k^2$. Y como el número de primos $\leq 2^n = 4^{k^2}$ es $r > k$, hemos probado que existen al menos $k+1$ primos $\leq 4^{k^2}$. Eso es válido para cada $k \geq 1$, luego deben existir infinitos primos. □

Otra demostración que utiliza argumentos de combinatoria es la de Auric (1915), que se puede encontrar en [41, § 1.V.B]:

DEMOSTRACIÓN 15. Supongamos que existe, sólo, una cantidad finita de primos, $p_1 < p_2 < \cdots < p_r$. Además, para cualquier entero $t > 1$, sea $N = p_r^t$. Cada entero $m \leq N$ se puede escribir como $m = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ para cierta r-tupla $(e_1, e_2, \ldots, e_r)$ definida de forma única. Tomemos ahora $E = (\log p_r)/(\log p_1)$, con lo cual $e_i \leq tE$ para cada i, ya que $p_1^{e_i} \leq p_i^{e_i} \leq N = p_r^t$. Pero N es, como mucho, el número de r-tuplas $(e_1, e_2, \ldots, e_r)$ con $0 \leq e_i \leq tE$, que es $N \leq (tE+1)^r$, así que

$$p_r^t = N \leq (tE+1)^r \leq t^r(E+1)^r,$$

y esto es imposible para t suficientemente grande. □

Las dos demostraciones anteriores tienen más de un siglo de antigüedad. Bastante más reciente es esta otra de Chernoff (1965) [8]:

DEMOSTRACIÓN 16. Supongamos que el número de primos es finito, $p_1, p_2, \ldots, p_r$, con lo cual cada entero positivo se podrá expresar de manera única en la forma $p_1^{e_1}p_2^{e_2}\ldots p_r^{e_r}$ con exponentes $e_i \geq 0$. Entonces, para cualquier entero positivo N, existirán exactamente N r-tuplas $(e_1, e_2, \ldots, e_r)$ de enteros no negativos que satisfacen la desigualdad $p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r} \leq N$, o, de manera equivalente,

$$e_1 \log p_1 + e_2 \log p_2 + \cdots + e_r \log p_r \leq \log N.$$

De esta forma, N, el número de tales r-tuplas, es el número de puntos de coordenadas enteras de la región r-dimensional

$$x_1 \log p_1 + x_2 \log p_2 + \cdots + x_r \log p_r \leq \log N, \quad x_i \geq 0.$$

El volumen de esta región es

$$\frac{(\log N)^r}{r! \log p_1 \log p_2 \cdots \log p_r},$$

y por tanto tendríamos que, para alguna constante c, $N \sim c\cdot(\log N)^r$ asintóticamente cuando $N \to \infty$, lo cual es falso, luego el número de primos tiene que ser infinito. □

Ya en este siglo, presentamos a continuación una demostración ideada por Pinasco (2009) [37]. Esta demostración utiliza una sucesión que se define recursivamente como sigue. Dada la sucesión de los primos $p_1, p_2, \ldots$, tomamos

$$a_0 = 0, \qquad a_{k+1} = a_k + \frac{1 - a_k}{p_{k+1}}, \quad k \geq 0$$

(en principio, esta sucesión podría ser finita si el número de primos fuese finito). Es sencillo comprobar que el n-ésimo término resulta ser

$$a_n = \sum_{1\leq i\leq n} \frac{1}{p_i} - \sum_{1\leq i<j\leq n} \frac{1}{p_i p_j} + \sum_{1\leq i<j<k\leq n} \frac{1}{p_i p_j p_k} + \cdots + (-1)^{n+1} \frac{1}{p_1 \cdots p_n};$$

además, esa expresión también puede escribirse como

$$a_n = 1 - \prod_{i=1}^{n} \Big(1 - \frac{1}{p_i}\Big).$$

De aquí se sigue que $0 < a_n < 1$ para todo n, ya que $0 < 1 - 1/p_i < 1$ para todos los primos p_i. Esto es todo lo que necesitamos para dar la siguiente demostración:

Demostración 17. Supongamos que sólo hay una cantidad finita de primos, y sean $p_1 < p_2 < \cdots < p_r$ todos ellos. Para cada $x \geq 1$, sea A_i el conjunto de los enteros en $[1, x]$ que son divisibles por p_i. Aplicando el principio de inclusión-exclusión al cálculo de la cardinalidad de $\cup_{i=1}^{r} A_i$ tenemos

$$\lfloor x \rfloor = 1 + \sum_i \left\lfloor \frac{x}{p_i} \right\rfloor - \sum_{i<j} \left\lfloor \frac{x}{p_i p_j} \right\rfloor + \sum_{i<j<k} \left\lfloor \frac{x}{p_i p_j p_k} \right\rfloor + \cdots + (-1)^{r+1} \left\lfloor \frac{x}{p_1 \cdots p_r} \right\rfloor.$$

Ahora, multipliquemos ambos términos de esta expresión por x^{-1}, tomemos límites cuando $x \to \infty$ y usemos que

$$\lim_{x\to\infty} x^{-1} \left\lfloor \frac{x}{t} \right\rfloor = \frac{1}{t},$$

con lo cual obtendríamos

$$1 = \sum_i \frac{1}{p_i} - \sum_{i<j} \frac{1}{p_i p_j} + \sum_{i<j<k} \frac{1}{p_i p_j p_k} + \cdots + (-1)^{r+1} \frac{1}{p_1 \cdots p_r} = a_r.$$

Pero esto es falso, pues ya hemos visto antes que todos los a_n son menores estrictamente que 1. □

Otra demostración basada en argumentos de combinatoria es la que presentó Sadhukhan en 2017 [42]:

DEMOSTRACIÓN 18. Por el teorema fundamental de la aritmética, cada entero $n > 1$ se puede escribir como $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ con los p_i primos distintos, y esta factorización es única salvo el orden; tomemos ahora $f(n) = e_1 + e_2 + \cdots + e_k$. De esta forma, podemos descomponer el conjunto de los enteros positivos en una serie de conjuntos disjuntos $S_0, S_1, S_2, \ldots$ definidos como

$$S_0 = \{1\}, \quad S_m = \{x \in \mathbb{N} : f(x) = m\}, \qquad m \geq 1.$$

Observemos que, si $x \in S_m$, forzosamente se cumplirá $x \geq 2^m$.

Supongamos ahora que sólo hay r primos distintos. El cardinal de S_m es el número de combinaciones con repetición de r elementos tomados m a m, es decir,

$$\operatorname{card}(S_m) = \binom{m+r-1}{m}.$$

Esto implica que existe una constante c tal que $\operatorname{card}(S_m) < cm^{r-1}$ para cada $m \geq 1$. Por otra parte, y dado que $\{1, 2, \ldots, 2^M - 1\} \subset \bigcup_{m=0}^{M-1} S_m$, se tiene

$$1 + \sum_{m=1}^{M-1} \operatorname{card}(S_m) = \operatorname{card}\left(\bigcup_{m=0}^{M-1} S_m \right) \geq 2^M - 1.$$

De aquí se sigue que $1 + \sum_{m=1}^{M-1} cm^{r-1} > 2^M - 1$ y, por tanto, $1 + c(M-1)^r > 2^M - 1$, lo cual es falso para M suficientemente grande. □

5. FURSTENBERG (TOPOLOGÍA)

Una de las demostraciones más atípicas de la infinidad de los números primos la dio Harry Furstenberg en 1955 [15], y está basada en la definición y propiedades de los espacios topológicos. No está de más comentar que Furstenberg recibió el premio Abel en 2020.

DEMOSTRACIÓN 19. Dotemos a los enteros $\mathbb{Z}$ de una topología, definiendo para ello una base de abiertos. Los abiertos de esta base son los conjuntos (sucesiones aritméticas indexadas en $\mathbb{Z}$)

$$S(a, b) = \{an + b : n \in \mathbb{Z}\} = a\mathbb{Z} + b \qquad (\text{con } a \geq 1),$$

y un conjunto $U \subseteq \mathbb{Z}$ es abierto si para cualquier elemento x de U existe un $S(a, b)$ tal que $x \in S(a, b) \subset U$.

Es fácil comprobar que se cumplen las propiedades que definen una topología: el vacío y $\mathbb{Z} = S(1, 0)$ son abiertos, la unión arbitraria de abiertos es un abierto, y la intersección finita de abiertos es un abierto (obsérvese que, si $x \in S(a_1, b_1) \cap S(a_2, b_2)$, $S(a_1, b_1) \cap S(a_2, b_2) = S(a_1, x) \cap S(a_2, x) = S(\operatorname{mcm}(a_1, a_2), x)$).

En esta topología, ningún conjunto abierto (salvo el vacío) es finito; en consecuencia, el complementario de un conjunto finito nunca puede ser cerrado. Además,

los subconjuntos $S(a,b)$ son abiertos (por definición) y cerrados, ya que podemos escribir $S(a,b)$ como el complementario de una unión de abiertos:

$$S(a,b) = \mathbb{Z} \setminus \bigcup_{j=1}^{a-1} S(a, b+j).$$

Los únicos enteros que no son múltiplos de primos son -1 y $+1$, y esto lo podemos plasmar como

$$\mathbb{Z} \setminus \{-1, +1\} = \bigcup_{p \text{ primo}} S(p,0). \tag{5}$$

Este conjunto (5) no puede ser cerrado, ya que su complementario es finito. Por otra parte, y para cada primo p, los conjuntos $S(p,0)$ son cerrados. Supongamos ahora que sólo existe una cantidad finita de primos p. En ese caso, la unión de todos los $S(p,0)$ sería un cerrado (unión finita de cerrados), con lo cual (5) sería un conjunto cerrado, y ya hemos visto que eso no es cierto. □

Realmente, se puede rehacer la demostración de Furstenberg prescindiendo de su lenguaje topológico. Eso es lo que hacen Cass y Wildenberg (2003) [7]:

Demostración 20. Dado un conjunto $A \subset \mathbb{Z}$, su función característica se define tomando $\chi_A(x) = 1$ si $x \in A$ y $\chi_A(x) = 0$ si $x \notin A$. Un conjunto de enteros se denomina periódico si su función característica es periódica.

Con esta notación, si S y T son conjuntos periódicos con periodos s y t, entonces $S \cup T$ es periódico con un periodo que divide a $\text{mcm}(s,t)$, y lo mismo se extiende a uniones finitas. Además, si un conjunto S es periódico, también lo es su complementario.

Para cada primo p, sea $S_p = \{n \cdot p : n \in \mathbb{Z}\}$. Si sólo hubiese una cantidad finita de primos, el conjunto $\mathcal{S} = \cup_p S_p$ sería una unión finita de conjuntos periódicos, así que $\mathcal{S}$ sería periódico, y también lo sería su complementario. Pero el complementario de $\mathcal{S}$ es $\{-1, 1\}$ que, como es finito, no puede ser periódico, y hemos llegado a un absurdo. □

También Mercer en 2009 [25] la reescribe despojándola de su sabor topológico, y lo hace como sigue:

Demostración 21. Para c y m enteros y $m \geq 1$, sea $c + m\mathbb{Z}$ el conjunto de los enteros congruentes con c módulo m; a estos conjuntos los llamamos «progresiones aritméticas» (indexadas en $\mathbb{Z}$, tal como decíamos en la demostración 19, donde usábamos $S(m,c)$). Con esta notación, para $m \geq 2$, el conjunto de los enteros no divisibles por m es

$$\text{NM}(m) = (1 + m\mathbb{Z}) \cup \cdots \cup ((m-1) + m\mathbb{Z})$$

(la abreviatura NM alude a «no múltiplos»).

Propiedad 1: Una intersección finita de progresiones aritméticas es, o bien vacía, o bien infinita. En efecto, si x pertenece a $c_i + m_i\mathbb{Z}$ para $1 \leq i \leq r$, lo mismo sucede con $x + y$ donde y es cualquier múltiplo común de los m_i.

Propiedad 2: Si $\mathcal{S}$ es cualquier colección de conjuntos, entonces una intersección finita de uniones finitas de conjuntos en $\mathcal{S}$ es también una unión finita de intersecciones finitas de conjuntos en $\mathcal{S}$. Esto es así ya que la intersección de conjuntos es distributiva sobre la unión; por ejemplo,

$$\begin{aligned}(R \cup S \cup T) \cap (U \cup V) \cap (W \cup X) \\ = (R \cap U \cap W) \cup (R \cap U \cap X) \cup (R \cap V \cap W) \cup (R \cap V \cap X) \\ \cup (S \cap U \cap W) \cup (S \cap U \cap X) \cup (S \cap V \cap W) \cup (S \cap V \cap X) \\ \cup (T \cap U \cap W) \cup (T \cap U \cap X) \cup (T \cap V \cap W) \cup (T \cap V \cap X).\end{aligned}$$

Con esto, ya podemos probar el teorema. Supongamos que sólo existiera una cantidad finita de primos, y sean $p_1, p_2, \ldots, p_r$ todos ellos. Entonces,

$$\{-1, +1\} = \mathrm{NM}(p_1) \cap \mathrm{NM}(p_2) \cap \cdots \cap \mathrm{NM}(p_r),$$

que es una intersección finita de uniones finitas de progresiones aritméticas, así que, por la propiedad 2, es también una unión finita de intersecciones finitas de progresiones aritméticas. Pero, por la propiedad 1, esto debería dar lugar a un conjunto vacío o infinito, así que hemos llegado a una contradicción. □

Finalmente, no está de más añadir que Carlson [6] muestra que, en realidad, estas demostraciones tienen una bonita relación, aunque oculta, con la tradicional de Euclides. En efecto, con la notación de la demostración anterior, y si p es un primo, lo que se tiene es $\mathrm{NM}(p) = \mathbb{Z} \setminus p\mathbb{Z}$. Entonces, si sólo hubiese una cantidad finita de primos $p_1, p_2, \ldots, p_k$, lo que podríamos escribir es que, para cualquier entero m,

$$mp_1p_2 \cdots p_k + 1 \in \bigcap_{i=1}^{k} (\mathbb{Z} \setminus p_i\mathbb{Z}) = \mathbb{Z} \setminus \bigcup_{i=1}^{k} p_i\mathbb{Z} = \{-1, 1\},$$

que es absurdo (incluso para $m = 1$), y $p_1p_2 \cdots p_k + 1$ es lo mismo que aparece en las demostraciones habituales «a lo Euclides».

6. Otros caminos llevan a la demostración

En las secciones anteriores se han expuesto demostraciones de la infinitud de los números primos hechas desde diferentes puntos de vista, y, dentro de cada sección, las demostraciones allí agrupadas tenían algún punto en común; por ejemplo, el esquema era similar o las herramientas o técnicas utilizadas podían englobarse dentro de un mismo contexto. No obstante, lo presentado hasta ahora no recoge todos los tipos de demostración, sino que se han usado muchas otras aproximaciones para llegar al resultado que nos interesa. En esta sección mostramos algunas de ellas, o, si no las incluimos, comentamos dónde las puede encontrar el lector interesado.

Una manera sencilla de probar la existencia de infinitos primos es usar el teorema de Lagrange que afirma que el orden —es decir, el cardinal— de un subgrupo de un grupo finito, y en particular el orden de cualquier elemento (que es el cardinal del subgrupo que genera), siempre divide al orden del grupo. Con esta idea, y tal como se muestra en [1, capítulo 1], tenemos lo siguiente:

Demostración 22. Supongamos que sólo hay un número finito de primos, y sea p el mayor. Vamos a ver que cualquier divisor primo q de $2^p - 1$ debe ser mayor que p, con lo cual habremos llegado a un absurdo.

Sea q un divisor primo de $2^p - 1$, es decir, $2^p \equiv 1 \bmod q$. Como p es primo, esto significa que el elemento 2 tiene orden p en el grupo multiplicativo $(\mathbb{Z}/q\mathbb{Z})^\star$ (dicho de otra forma, que el subgrupo generado por 2 tomando potencias sucesivas tiene orden p). El grupo $(\mathbb{Z}/q\mathbb{Z})^\star$ tiene $q-1$ elementos, así que, por el teorema de Lagrange, el orden de cualquier elemento debe dividir a $q-1$. En consecuencia, $p \mid (q-1)$ y, por tanto, $p < q$, tal como buscábamos. □

Washington, en 1980 [41, § 1.VI], proporciona una demostración hecha desde un punto de vista muy algebraico. En concreto, muestra un ejemplo de anillo de enteros cuadrático que no es dominio de ideales principales, para con ello probar que existen infinitos números primos.

Demostración 23. El conjunto $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{N}\}$ es un dominio de Dedekind pues es el anillo de enteros del cuerpo de números cuadrático $\mathbb{Q}(\sqrt{-5})$. Este anillo no es de factorización única, pues $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ y los elementos 2, 3, $1 + \sqrt{-5}$ o $1 - \sqrt{-5}$ son elementos primos de este anillo. Por tanto, $\mathbb{Z}[\sqrt{-5}]$ no es un anillo de ideales principales y, en consecuencia, tendrá un número infinito de ideales primos (pues todo dominio de Dedekind con un número finito de ideales primos es dominio de ideales principales). Por otra parte, como en un cuerpo de números de grado finito existe sólo un número finito de ideales primos que dividen a cada primo $p \in \mathbb{Z}$, no es posible que haya un número finito de primos $p \in \mathbb{Z}$. □

Otra técnica para mostrar la infinitud de los números primos consiste en dar una cota inferior para el número de primos menores que un entero dado N, de forma que esta cota tienda a infinito cuando N también tiende a infinito. Nair, en 1982 [31], demuestra, de una forma bastante ingeniosa, que el número de primos menores o iguales que N es mayor o igual que $cN/\log N$ para una cierta constante positiva. Su demostración puede simplificarse si sólo se requiere probar la infinitud de los primos:

Demostración 24. Para cada entero positivo n, sea $I_n = \int_0^1 x^n(1-x)^n\,dx$. Es claro que $I_n > 0$. Desarrollando e integrando, se tiene

$$I_n = \int_0^1 \sum_{r=0}^{n} (-1)^r \binom{n}{r} x^{n+r}\,dx = \sum_{r=0}^{n} (-1)^r \binom{n}{r} \frac{1}{n+r+1}. \tag{6}$$

Si denotamos $d_m = \operatorname{mcm}(1, 2, \ldots, m)$, como el denominador del lado derecho de (6) es a lo sumo $2n+1$, es claro que $d_{2n+1} I_n$ es un entero positivo. Además, si $x \in [0,1]$, entonces $x(1-x) \le 1/4$, así que $I_n \le 1/4^n$, con lo cual $1 \le d_{2n+1} I_n \le d_{2n+1}/4^n$ y $d_{2n+1} \ge 4^n$.

Por otra parte, para cada primo p, sea p^a la mayor potencia de p que divide a d_{2n+1}; entonces p^a divide a m para algún m menor que $2n+1$. De esta forma, $p^a \le 2n+1$ y $a \le \log(2n+1)/\log p$ (por simplicidad de lo que sigue, pensemos que el logaritmo es en base 2).

Con todo esto, si $p_1, p_2, \ldots, p_r$ fueran los únicos números primos, se tendría que

$$4^n \leq d_{2n+1} \leq \prod_{i=1}^{r} p_i^{\log(2n+1)/\log p_i} \leq \prod_{i=1}^{r} p_i^{\log(2n+1)} = N^{\log(2n+1)}$$

con $N = p_1 \cdot p_2 \cdots p_r$, que es claramente falso si n es suficientemente grande. □

Meštrović, además de recopilar en su artículo [27] casi 200 demostraciones de la infinitud de los números primos, es autor de varias. En una de ellas [26] utiliza el teorema fundamental de la aritmética y la representación en base n de un número racional para determinar la infinitud de los números primos.

DEMOSTRACIÓN 25. Observemos previamente que, dado un entero $n > 2$, la representación de $n/(n-1)$ en base n es

$$\frac{n}{n-1} = \frac{1}{1-1/n} = \sum_{i=0}^{\infty} \frac{1}{n^i} = (1.1111\ldots)_n. \tag{7}$$

Visto eso, supongamos que $p_1 = 2 < p_2 < \cdots < p_r$ son los únicos primos existentes, y sean a, b enteros positivos con $a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ y $b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$. Entonces, tomando $s = \max\{f_1, f_2, \ldots, f_r\}$, la fracción a/b puede escribirse como

$$\frac{a}{b} = \frac{p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}}{p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}} = \frac{p_1^{e_1+s-f_1} p_2^{e_2+s-f_2} \cdots p_r^{e_r+s-f_r}}{p_1^s p_2^s \cdots p_r^s} = \frac{c}{n^s}$$

con $n = p_1 p_2 \cdots p_r$ y $c = p_1^{e_1+s-f_1} p_2^{e_2+s-f_2} \cdots p_r^{e_r+s-f_r}$ enteros positivos. Como c es un número entero, tiene una representación finita en base n y, por tanto, la representación en base n de cualquier número racional positivo a/b tendrá un número finito de términos.

Si ahora tomamos $a/b = n/(n-1)$, este número tiene dos representaciones en base n, una infinita $(1.1111\ldots)_n$ y otra finita. Pero los únicos números que tienen una representación finita y otra infinita en base n son los que, a partir de un término, todos los dígitos de su representación infinita son k con $k = n-1$, y eso no es lo que ocurre con (7) ya que $n > 2$. □

Mixon, en 2012 [29], construye una aplicación que asigna a cada entero la lista de los exponentes que aparecen en su descomposición en factores primos. Demuestra que, si hubiera un número finito de primos, esta aplicación sería inyectiva, pero también prueba que no existe ninguna aplicación inyectiva entre los conjuntos indicados.

DEMOSTRACIÓN 26. Supongamos que $p_1 = 2 < p_2 < \cdots < p_r$ son todos los primos que existen. Fijado un entero positivo K se define

$$\begin{array}{rccc} f: & \{1, 2, \ldots, 2^K\} & \longrightarrow & \{0, 1, \ldots, K\}^r \\ & x = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} & \longmapsto & (e_1, e_2, \ldots, e_r) \end{array}$$

Esta aplicación f está bien definida, pues

$$K \geq \log_2(x) = \sum_{i=1}^{r} e_i \log_2(p_i) \geq \sum_{i=1}^{r} e_i \geq \text{máx}\{e_1, \ldots, e_r\}.$$

Por una parte, por el teorema fundamental de la aritmética, f es una aplicación inyectiva. Por otra parte es claro que, si K cumple $2^K > (K+1)^r$, no puede existir ninguna aplicación inyectiva entre ambos conjuntos. En consecuencia, hay una cantidad infinita de primos. □

Northshield es otro de los autores que han presentado varias demostraciones; la primera de ellas, en 2015 [34], es quizás la demostración más corta que existe, de hecho su publicación lleva por título «A one-line proof of the infinitude of primes» y sólo usa nociones básicas de trigonometría (para que el lector la siga fácilmente, aquí daremos algunos detalles que la hacen un poco más larga).

Demostración 27. Si sólo existe una cantidad finita de primos $p_1, p_2, \ldots, p_r$, entonces

$$0 < \prod_{i=1}^{r} \text{sen}\left(\frac{\pi}{p_i}\right) = \prod_{i=1}^{r} \text{sen}\left(\frac{\pi}{p_i} + 2\pi \prod_{p_j \neq p_i} p_j\right) = \prod_{i=1}^{r} \text{sen}\left(\frac{1 + 2\prod_{j=1}^{r} p_j}{p_i}\,\pi\right) = 0.$$

La primera desigualdad es cierta pues $0 < \pi/p_i \leq \pi/2$; y la última igualdad se cumple ya que $1 + 2\prod_{j=1}^{r} p_j$ es un número entero que será divisible por algún primo p_{i_0} de la lista de primos, y por tanto $(1 + 2\prod_{j=1}^{r} p_j)\pi/p_{i_0}$ es un múltiplo entero de π, de seno nulo. □

Otra demostración del propio Northshield [35] usa la teoría de probabilidades y la dificultad de definir de forma elemental qué es un entero aleatorio. Dicha dificultad consiste en que, para tomar un entero aleatorio con una distribución uniforme, cada entero debería tener la misma posibilidad de ser elegido; pero, entonces, como la suma de todas las probabilidades debe ser $\sum_n P(X = n) = 1$, es imposible que la probabilidad $P(X = n)$ asignada a cada número sea constante.

En 1976, Barnes [3] presentó una demostración que usaba fracciones continuas y su relación con las soluciones enteras de una ecuación de Pell. No obstante, en 2020, Lemmermeyer [23] evita esos contextos y simplifica notablemente la demostración:

Demostración 28. Supongamos que hay una cantidad finita de primos, $p = 2$ y $3 = p_1, \ldots, p_r$ los impares. Sea $q = p_1 \cdots p_r$ el producto de todos los primos impares. Es claro que $q^2 + 1$ no es divisible por ningún primo impar y, en consecuencia, debe ser una potencia de 2. Como 1 es el único resto cuadrático impar módulo 4, se tiene que $q^2 + 1 \equiv 2$ mód 4, luego deber ser $q^2 + 1 = 2$ y, por tanto, $q = 1$, que es absurdo pues $q > p_1 = 3$. □

Concluimos el artículo mencionando algunas demostraciones recientes hechas desde puntos de vista distintos de los que aquí hemos tratado. Presentarlas hubiera requerido adentrarnos un poco más en el contexto especializado que utiliza cada una

de ellas —a menudo alejado de la aritmética—, así que nos hemos conformado con citarlas para que el lector pueda buscarlas si lo desea. Una de estas demostraciones es la de Alpoge de 2015 [2], que deduce la infinitud de los números primos utilizando el teorema de van der Waerden; dicho teorema afirma que, si se asigna a cada entero un color entre m ($m \geq 2$), para cada $k \geq 3$ existen al menos k enteros en progresión aritmética con el mismo color. Pero las hay para todos los gustos. Así, por ejemplo, también podemos encontrar demostraciones realizadas en los últimos años que han usado lenguajes formales [49], teoría de valoraciones [46], dimensión fractal [44] o métricas p-ádicas [16]. Seguro que no son las últimas, y que el ingenio de los matemáticos descubre otros caminos sorprendentes para llegar al mismo destino.

Referencias

[1] M. Aigner y G. M. Ziegler, *Proofs from THE BOOK*, 6.ª edición, Springer, 2018.

[2] L. Alpoge, van der Waerden and the primes, *Amer. Math. Monthly* **122** (2015), 784–785.

[3] C. W. Barnes, The infinitude of primes; a proof using continued fractions, *Enseign. Math.* **22** (1976), 313–316.

[4] C. O. Boije af Gennäs, Trouver un nombre premier plus grand qu'un nombre premier donne, *Öfversigt K. Sv. Vetenskaps-Akad. Förhand.* **50** (1893), 469–471.

[5] C. K. Caldwell y Y. Xiong, What is the smallest prime?, *J. Integer Seq.* **15** (2012), Article 12.9.7.

[6] N. A. Carlson, A connection between Furstenberg's and Euclid's proofs of the infinitude of primes, *Amer. Math. Monthly* **121** (2014), 444.

[7] D. Cass y G. Wildenberg, Math Bite: A novel proof of the infinitude of primes, revisited, *Math. Mag.* **76** (2003), 203.

[8] P. R. Chernoff, A "Lattice Point" proof of the infinitude of primes, *Math. Mag.* **38** (1965), 208.

[9] L. E. Dickson, *History of the Theory of Numbers. Volume I: Divisibility and Primality*, Carnegie Institution of Washington, 1919. Reimpreso por Dover, 2005.

[10] A. W. F. Edwards, Infinite coprime sequences, *Math. Gaz.* **48** (1964), 416–422.

[11] P. Erdős, Über die Reihe $\sum 1/p$, *Math. Zutphen B* **7** (1938), 1–2.

[12] Euclides, *Elementos*, 3 vols., traducción y anotaciones de M. L. Puertas, Editorial Gredos, Madrid, 1991, 1994 y 1996.

[13] L. Euler, Variae observationes circa series infinitas, *Comment. Acad. Sci. Petropol.* **9** (escrito en 1737 y publicado en 1744), 160–188. Reimpreso en *Opera Omnia*, Series 1, Vol. 14, 216–244.

[14] L. Euler, *Introductio in Analysin Infinitorum* (Introducción al análisis de los infinitos), editado por A. J. Durán y F. J. Pérez, 2 vols. (facsímil y edición crítica), SAEM Thales y Real Sociedad Matemática Española, Sevilla, 2000.

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

[16] H. Göral, p-adic metrics and the infinitude of primes, *Math. Mag.* **93** (2020), 19–22.

[17] A. Granville, A panoply of proofs that there are infinitely many primes, *Lond. Math. Soc. Newsl.* **472** (2017), 23–27.

[18] A. Granville, Varias demostraciones aritméticas de la infinitud de los números primos, *La Gaceta de la RSME* **23** (2020), 324.

[19] V. C. Harris, Another proof of the infinitude of primes, *Amer. Math. Monthly* **63** (1956), 711.

[20] R. L. Hemminger, Classroom notes: More on the Infinite Primes Theorem, *Amer. Math. Monthly* **73** (1966), 1001–1002.

[21] L. J. P. Kilford, An infinitude of proofs of the infinitude of primes, arXiv:math/0610066v2 [math.NT], 2006.

[22] J. Lambek y L. Moser, On relatively prime sequences, *Math. Gaz.* **41** (1957), 287–288.

[23] F. Lemmermeyer, A simple proof of the infinitude of primes, *Elem. Math.* **75** (2020), 80.

[24] B. Maji, A new proof of the infinitude of primes, *Resonance* **20** (2015), 1128–1135.

[25] I. D. Mercer, On Furstenberg's proof of the infinitude of primes, *Amer. Math. Monthly* **116** (2009), 355–356.

[26] R. Meštrović, An elementary proof of the infinitude of primes, preprint, 2012. `https://sites.google.com/site/romeomestrovic/preprints`

[27] R. Meštrović, Euclid's theorem on the infinitude of primes: a historical survey of its proofs (300 B.C.–2017), arXiv:1202.3670v3 [math.HO], 2018.

[28] G. Métrod, Suite illimitée des nombres premiers, *L'Intermédiaire des Math.* **24** (1917), 39–40.

[29] D. G. Mixon, Another simple proof of the infinitude of primes, *Amer. Math. Monthly* **119** (2012), 811.

[30] S. P. Mohanty, The number of primes is infinite, *Fibonacci Quart.* **16** (1978), 381–384.

[31] M. Nair, On Chebyshev-type inequalities for primes, *Amer. Math. Monthly* **89** (1982), 126–129.

[32] W. Narkiewicz, *The Development of Prime Number Theory: From Euclid to Hardy and Littlewood*, Springer, 2000.

[33] I. Niven, A proof of the divergence of $\sum 1/p$, *Amer. Math. Monthly* **78** (1971), 272–273.

[34] S. Northshield, A one-line proof of the infinitude of primes, *Amer. Math. Monthly* **122** (2015), 466.

[35] S. Northshield, Two short proofs of the infinitude of primes, *College Math. J.* **48** (2017), 214–216.

[36] J. PEROTT, Sur l'infinité de la suite des nombres premiers, *Bull. des Sc. Math. et Astr. (2)* **5** (1881), 183–184.

[37] J. P. PINASCO, New proofs of Euclid's theorem and Euler's theorem, *Amer. Math. Monthly* **116** (2009), 172–173.

[38] P. POLLACK, *Not Always Buried Deep: A Second Course in Elementary Number Theory*, 2.ª edición, American Mathematical Society, 2009.

[39] G. PÓLYA, Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen, *J. Reine Angew. Math.* **151** (1921), 1–31.

[40] M. RAUSSEN Y C. SKAU, Interview with Michael Atiyah and Isadore Singer, *Eur. Math. Soc. Newsl.* **53** (2004), 24–30. Reproducido en *Notices Amer. Math. Soc.* **52** (2005), 225–233.

[41] P. RIBENBOIM, *The Little Book of Bigger Primes*, 2.ª edición, Springer, 2004.

[42] A. SADHUKHAN, Partitioning the natural numbers to prove the infinitude of primes, *College Math. J.* **48** (2017), 217–218.

[43] F. SAIDAK, A new proof of Euclid's theorem, *Amer. Math. Monthly* **113** (2006), 937–938.

[44] K. SAITO, A fractal proof of the infinitude of primes, *Lith. Math. J.* **59** (2019), 408–411.

[45] N. SCHAUMBERGER, A variation of the standard proof of the infinitude of primes, *Pi Mu Epsilon Journal* **8** (1985), 159.

[46] S. SEKI, Valuations, arithmetic progressions, and prime numbers, *Notes Number Theory Discrete Math.* **24** (2018), 128–132.

[47] W. SIERPIŃSKI, *250 Problems in Elementary Number Theory*, Elsevier, New York, 1970.

[48] J. J. SYLVESTER, On a point in the theory of vulgar fractions, *Amer. J. Math.* **3** (1880), 332–335.

[49] A. THAKKAR, Infinitude of primes using formal languages, *Amer. Math. Monthly* **125** (2018), 945–749.

[50] J. L. VARONA, *Recorridos por la Teoría de Números*, 2.ª edición, Electolibris y Real Sociedad Matemática Española, Murcia, 2019.

[51] M. WUNDERLICH, Classroom Notes: Another proof of the Infinite Primes Theorem, *Amer. Math. Monthly* **72** (1965), 305.

[52] T. YAMADA, *Proofs of the infinitude of primes*, 2018. `http://tyamada1093.web.fc2.com/math/files/infprime.pdf`

DANIEL SADORNIL, DPTO. DE MATEMÁTICAS, ESTADÍSTICA Y COMPUTACIÓN, UNIVERSIDAD DE CANTABRIA
Correo electrónico: `sadornild@unican.es`

JUAN LUIS VARONA, DPTO. DE MATEMÁTICAS Y COMPUTACIÓN, UNIVERSIDAD DE LA RIOJA
Correo electrónico: `jvarona@unirioja.es`
Página web: `https://www.unirioja.es/cu/jvarona/`