Épsilon - Revista de Educación Matemática 2013, Vol. 30(2), nº 84, 69-88

Demostraciones de la infinidad de los números primos

Enrique de Amo
Departamento de Matemáticas. Universidad de Almería

Manuel Díaz Carrillo
Departamento de Análisis Matemático. Universidad de Granada

Juan Fernández Sánchez
I.E.S. "Valle del Almanzora" (Cantoria), Almería

Resumen: *Es bien conocido, gracias a Euclides, desde hace ya más de veintitrés siglos, el hecho de que existen infinitos números primos, y a pesar de esto, sigue vigente el interés por conocer diferentes demostraciones de este resultado. El objetivo de este trabajo es presentar demostraciones conocidas sobre dos resultados principales acerca de los números primos (el de su infinitud y el de la divergencia de la serie de los recíprocos). Además, aportamos otras demostraciones nuevas, de modo que sirva tanto al edificio teórico de las matemáticas como a su didáctica, facilitando nuevos accesos a sus demostraciones, por otras vías.*
Palabras clave: *número primo, serie divergente, serie armónica*

Proofs of the infinity of prime numbers

Summary: *It is thanks to Euclid, that the existence of infinity prime numbers has been a well known fact for 23 centuries and never the less, there is still great interest in finding new evidence of this outcome. The aim of this paper is to present already known proofs of the main results concerning prime numbers (their infinity and the divergence of the reciprocal number series). Furthermore, we contribute new evidence that will support both the theoretical construction and the didactics of mathematics, providing new access to its evidence through other paths.*
Keywords: *prime number, divergent series, harmonic series*

INTRODUCCIÓN

Los números primos son, sin duda alguna, uno de los objetos de estudio que mayor fecundidad ha podido aportar al quehacer matemático a lo largo de toda su historia. Hoy en día se mantiene como un campo de plena vigencia por sus aplicaciones en ámbitos como son la criptografía o la teoría de códigos.

El objetivo de este trabajo es presentar demostraciones conocidas sobre dos resultados principales acerca de los números primos (el de su infinitud y el de la divergencia de la serie de los recíprocos). Además, en algunos casos, aportamos otras demostraciones nuevas, de modo que sirva tanto al edificio teórico de las matemáticas como a su didáctica, facilitando nuevos accesos a sus demostraciones, por otras vías. Es bien conocido, gracias a Euclides, desde hace ya más de veintitrés siglos, el hecho de que *existen infinitos números primos*, y a pesar de esto, sigue vigente el interés por conocer diferentes demostraciones de este resultado, ya que aportan un doble enriquecimiento: el científico y el educativo.

Desde una perspectiva científica, conocer y analizar nuevas demostraciones de un teorema facilita una mejor comprensión del resultado y permite estudiarlo desde distintos puntos de vista, analizando el papel y las características de las herramientas matemáticas que se han utilizado para tal fin.

El segundo de los motivos que hace que tenga gran interés el estudio de nuevas demostraciones de un resultado conocido es su potencial educativo y la posibilidad de utilizar estas herramientas en el aula. Dependiendo del nivel educativo y de los fines que se persigan en cada momento, si disponemos de diferentes demostraciones de un resultado, podemos presentarlas para su estudio y análisis o bien para mostrar la utilidad de los nuevos conocimientos que el alumnado va adquiriendo a la hora de abordar problemas estudiados anteriormente. También pueden ser utilizadas como un recurso al plantear al estudiante un problema conocido pidiéndole que ahora lo estudie desde perspectivas diferentes a las que ha tenido anteriormente, relacionando y conectando conceptos que pertenecen a ramas del conocimiento matemático aparentemente distantes o que han tenido un origen muy diferente.

En la primera sección hacemos una recopilación de diversas demostraciones de dicho resultado, aunque aquí no están recogidas todas las que hemos encontrado en la literatura. Por ejemplo, en los libros de Pollack y Ribenboim se encuentran dos de ellas, que no reproducimos porque las herramientas que utilizan hacen recomendable no añadirlas en el perfil de este trabajo. El lector interesado siempre puede consultar dichas referencias. También, hay varias demostraciones que, con el añadido "siguiendo a", no aparecen de forma explícita, pero se obtienen fácilmente siguiendo esas ideas.

Así mismo, debemos señalar que al final de esta primera sección aportamos tres demostraciones que, hasta donde nosotros conocemos, no han sido publicadas y presentan algunos aspectos novedosos, aunque los lectores familiarizados con la Teoría de Números encontrarán que, en todas ellas, hay ideas que aparecen en la literatura relativa a este campo.

Somos conscientes de que sería necesario demostrar algunas de las afirmaciones que se harán en algún momento, como pueden ser las relativas a ciertas convergencias, al

teorema de factorización única o la misma irracionalidad de π^2, entre otras. No se reproducen aquí esas demostraciones para no alargar el trabajo en exceso, de modo que evitamos lo que podría llevar a desviar la atención de la idea central que se persigue. No obstante, en la literatura sobre el tema se encuentran demostradas habitualmente esas afirmaciones que aquí no lo están.

Euler, en 1737, en un artículo que inició un nuevo camino en la Teoría de Números, demostró que *la serie de los inversos de los números primos es divergente*. Desde entonces hasta la actualidad han aparecido diferentes demostraciones de este teorema. En la segunda sección recogemos todas las demostraciones que hemos encontrado de dicho resultado; y, en particular, aportamos dos nuevas.

EL NÚMERO DE PRIMOS ES INFINITO

Notación y convenio. Supondremos, para las demostraciones que siguen en esta sección, que sólo existe un número finito r de números primos. A estos números los notaremos en orden creciente por $p_1, p_2, \ldots, p_r$. La letra p será reservada, habitualmente para primos, y si no se explicita el subíndice, designará a uno cualquiera de ellos. A veces, se utilizará p , sin lugar a confusión, como índice para sumatorias y productos.

Los siguientes convenios también los tendremos en cuenta en todo lo que sigue: C siempre designará a una constante. En ocasiones, aparecerá con subíndices o primas. Con la notación ya indicada arriba, $N := p_r!$ y $R := p_1, p_2, \ldots p_r$ Con $\lfloor x \rfloor$ notamos, como se acostumbra, al mayor de los enteros menor o igual que x. Aquí (m,n) es el máximo común divisor de m y n.

Demostración 1ª [Euclides, 300 A.C., aprox.]

Consideremos el valor $n = R + 1$. (En algunos textos podemos encontrar que el razonamiento se hace para $n = N + 1$.) Al dividir n entre cualquiera de los primos p_i resultará un resto igual a 1. Por tanto, n no es divisible por ningún primo. Como esto es absurdo, hemos de concluir que el número de primos ha de ser infinito.

Observemos que el número $m!+1$ no ha de ser necesariamente primo. El número primo más grande conocido de este tipo (cuando se escribe esta nota) es el $26951!+1$.

Si se representa por $m\#$ al producto de todos los primos menores o iguales a m

Euclides.

el número $m\# + 1$ puede ser un no primo. El mayor de los conocidos de este tipo es $392113\#+1$.

Demostración 2ª [Goldbach, 1730]

Sea $n_1 = 3$ y definamos por recurrencia,

$$n_j = 2 + \prod_{1 \le i < j} n_i,$$

para $j > 1$. Entonces, tenemos que:

1) Todo n_i es impar.
2) Cuando $j > i$, entonces $n_j \equiv 2 \bmod n_i$.
3) $(n_i, n_j) = 1$ para $i \neq j$.

En consecuencia, el número de primos es infinito.

Demostración 3ª [Euler, publicada póstumamente]

La función de Euler φ asigna a cada número entero n > 1 el número de primos relativos con él que son menores que n. Es conocida la fórmula

$$\varphi(n) = \prod_{p|n} (p - 1).$$

Aplicando esta expresión a R tenemos que

$$\varphi(R) = \prod_{i=1}^{r} (p_i - 1).$$

Como este producto es mayor que 1 , concluimos que hay un número primo distinto de los p_i. Por tanto, en cualquier conjunto finito de primos nunca están todos.

Euler.

Demostración 4ª [Euler, 1737]

La realizamos con la ayuda de la función ζ de Riemann, definida para los números complejos con parte real mayor que 1 mediante la fórmula

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

Por otra parte, se tiene

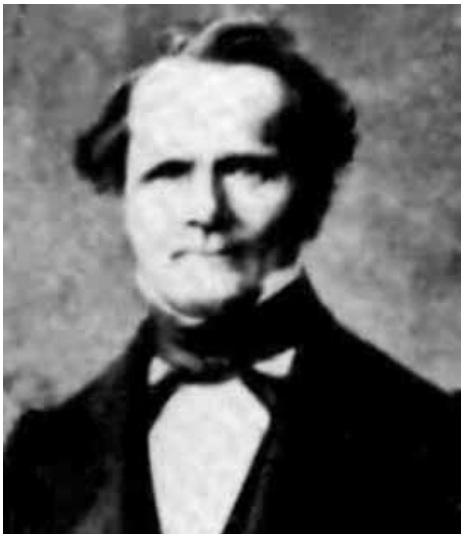
$$\zeta(s) = \prod_{p} (1 - 1/p^s)^{-1}.$$

Si el número de primos fuese finito, entonces la función de la izquierda sería analítica en el semiplano de los complejos con parte real positiva. Por tanto, existiría $\lim_{s \to 1^+} \sum_{n=1}^{\infty} \frac{1}{n^s}$ lo cual es absurdo, pues es bien conocido que la serie armónica diverge. Consecuentemente, el número de primos no puede ser finito.

Demostración 5ª [Kummer, 1878]

Consideremos los valores N y $N - 1$. Llamemos p_i a alguno de los primos que ha de dividir a $N - 1$. Puesto que p_i también divide a N, esto implica que p_i debe dividir a su diferencia: $N - (N - 1) = 1$. Esta conclusión es absurda, de donde se sigue que el número de primos ha de ser infinito.

Los mayores primos conocidos restando 1 son 103040! – 1 y 843301# – 1.



Kummer.

Demostración 6ª [Perrot, 1881]

Bajo las hipótesis de esta sección, hay 2^r números libres de cuadrados. Y dado un valor tenemos las desigualdades:

$$n \leq 2^r + \sum_{i=1}^{r} \frac{n}{p_i^2} < 2^r + n \sum_{i=2}^{\infty} \frac{1}{i^2} = 2^r + Cn$$

con $C < 1$. Pero, esto es absurdo para un valor suficientemente grande de n. Esta contradicción nos permite afirmar que el número de primos es infinito.

Demostración 7ª [Stieltjes, 1890]

Stieltjes.

Para una descomposición $R = bd$, cualquier p_i divide uno de los valores b o d. Pero no puede dividir ambos a la vez, por lo que p_i no divide a su suma; es decir, $b + d$ no es divisible por ningún primo. Esta última afirmación es absurda, y concluimos que existen infinitos números primos.

Demostración 8ª [Thue, 1897]

Sea m un entero positivo cualquiera. Siempre es posible descomponerlo en producto de potencias de primos en la forma $m = 2^{e_1}...p_r^{e_r}$ donde cada e_i depende de m. Si hacemos $e_i = 0, \ldots, n$, para $i = 1, \ldots, r$, obtenemos $(n + 1)^r$ posibilidades de expresarlo. Todos los valores menores o iguales a 2^n tienen, en su descomposición factorial, a lo sumo factores primos contando multiplicidades. Por tanto, $2^n < (n+1)^r$. Tomemos $n = 2k^2$ con k verificando la condición $1 + 2k^2 < 2^{2k}$, de donde $(1 + 2k^2)^k < (2^{2k})^k$. Si ahora unimos las dos desigualdades anteriores:

$$(1 + 2k^2)^k < 2^{2k^2} < (1 + 2k^2)^r.$$

Pero esto significa que $r > k$ para cualquier valor de k, lo que es absurdo. Por tanto, deducimos que el número de primos ha de ser infinito.

Demostración 9ª [Auric, 1915]

Siguiendo con la notación utilizada, hagamos $n = 2^{e_1}...p_r^{e_r}$. Si consideramos $v = p_r^t$ para los valores $n \leq v$ se verifica la desigualdad $e_i \leq t \log_2 p_r$. En consecuencia, la cantidad de estos números n es menor o igual que $(t \log_2 p_r + 1)^r$. Se tiene, por tanto, que

$$p_r^t = v \leq (t \log_2 p_r + 1)^r$$

Pero esto no puede ser cierto cuando t toma un valor suficientemente grande: contradicción; y en consecuencia, se sigue la infinitud del conjunto de los números primos.

Demostración 10ª [Braun, 1897; Metrod, 1917]

Sea $Q_i = R/p_i$ Por tanto, p_i no divide a Q_i pero sí a los demás Q_j Por esta razón, no divide a la suma de todos ellos. En consecuencia, $Q_1 + Q_2 + \ldots + Q_r$ no es divisible por ningún primo, lo cual es imposible. Volvemos a tener una contradicción que garantiza que el número de primos es infinito.

Demostración 11ª [Pólya]

Polya.

Consideremos el número de Fermat $F_n = 2^{2^n} + 1$. Estos números son primos entre sí. En efecto, puesto que $F_m - 2 = F_0 F_1 \cdots F_{m-1}$ si F_m y F_n no fuesen primos entre sí, habría un primo p, que dividiría a ambos. Si $n < m$ entonces p divide a $F_m - 2 = F_0 F_1 \cdots F_{m-1}$ y a F_m por lo que también dividirá su diferencia, que es 2. Por tanto, tenemos que $p = 2$. Pero F_m es impar y 2 no lo puede dividir, por lo que estos números son primos dos a dos; es decir, los divisores primos de cada uno de ellos no dividen a ninguno de los demás. En consecuencia, el número de primos es infinito. El lector habrá observado que esta demostración es la misma que la segunda. Su presencia aquí se debe a que la forma de presentarla es diferente y su autor la desconocía.

Demostración 12ª [Siguiendo a Erdös, 1938]

Erdös.

El número de números libres de cuadrados es 2^r. Por otra parte, el número de cuadrados menores que n es menor o igual que $\sqrt{n}$. Puesto que un número menor que n se puede expresar como el producto de un cuadrado inferior a n y un número libre de cuadrados, tenemos que $n \leq 2^r \sqrt{n}$. Esto no puede ocurrir para un valor de n suficientemente grande. Esta contradicción nos conduce a que no puede haber un número finito de primos.

Demostración 13ª [Fürstenberg, 1955]

Vamos a dotar al conjunto $\mathbb{Z}$ de una topología. Para ello, definamos $A_{m,n}$ como la progresión aritmética $m + n$ $\mathbb{Z}$ con $n \neq 0$ Tomemos como base de abiertos al conjunto de progresiones $A_{m,n}$ Evidentemente, $A_{m,n}$ es un abierto. También es un conjunto cerrado, al ser el complementario del abierto resultante de la unión de los $A_{d,n}$ con $d \neq m$. Ahora, bajo la

hipótesis de ser el número de primos finito, el conjunto $\bigcup_{i=1}^{r} A_{0,p_i}$ será un cerrado, y su

complementario será abierto. Pero esto no es posible, ya que se trata del conjunto $\{1,-1\}$ Esta contradicción nos permite deducir que el número de primos es infinito.

Demostración 14ª [Harris, 1956]

Elijamos dos valores tales que $(b_0,b_2)=1$ y definamos la fracción continua $b_0+\frac{1}{b_1+\frac{1}{b_2+\ldots+\frac{1}{b_k}}}$ donde $b_k=A_0A_1\cdots A_{k-3}$. Como las convergentes de una fracción continua vienen dadas por la relación $A_0=1$, $A_1=b_0$, $A_n=b_nA_{n-1}+A_{n-2}$ tenemos que $A_k=A_0A_1\cdots A_{k-3}A_{k-1}+A_{k-2}$ Demostraremos que los primeros valores de A_n son coprimos. Es cierto para $n=2$; lo suponemos cierto para $k-1$: será $(A_k, A_i)=1$, ya que A_i sólo divide a uno de los dos sumandos. Es decir, los divisores primos de cada uno de ellos no dividen a ninguno de los demás, por lo que el número de primos ha de ser infinito.

Se ha reproducido la demostración utilizando fracción continua como hace el autor, pero no se usa ninguna propiedad especial de esta expresión de los números reales. Por tanto, puede también hacerse la demostración utilizando la definición de b_k y A_k sin que aparezcan fracciones continuas.

Demostración 15ª [Wunderlich, 1965]

Esta demostración se basa en el uso de los números de Fibonacci. Como es bien conocido, se trata de la sucesión definida de forma recurrente por

$$F_0=F_1=1 \text{ y } F_n=F_{n-1}+F_{n-2};$$

(no confundir éstos con los números de Fermat de la demostración 11 ª) y la propiedad utilizada es

$$F_{(m,n)}=(F_m,F_n).$$

Si existiese un número finito de números primos, entonces los números $F_{p_1},\ldots,F_{p_r}$ habrían de ser primos dos a dos y, por tanto, primos. Pero, si tenemos en cuenta que $F_{19}=4181=113\times 37$ obtenemos una contradicción que nos lleva a afirmar que el número de primos no es finito.

De modo similar, se puede obtener la demostración de la infinitud de números primos utilizando otras sucesiones. A continuación, se proponen estas cuatro:

Propuesta 1. Utilizar la sucesión de números de Mersenne, esto es, los números de la forma 2^n-1 .

Propuesta 2. La sucesión definida recurrentemente por: $a_1=1, a_2=2$ y

$$\begin{cases} a_{2n}=a_2a_4\cdots a_{2n-2}+a_1a_3\cdots a_{2n-1} \\ a_{2n-1}=a_2a_4\cdots a_{2n-1}+a_1a_3\cdots a_{2n} \end{cases}$$

Propuesta 3. Una sucesión satisfaciendo: $a_1 > d \geq 1, \quad a_n - d = a_{n-1}(a_{n-1} - d)$ y $(a_1, d) = 1$.

Propuesta 4. La sucesión definida por: a_1 un número impar y $a_n = a_{n-1}^2 - 2$.

Demostración 16ª [Dressler, 1975] (Esencialmente, igual a la de Perrot)

Supongamos, como siempre, que sea *r* el cardinal finito de números primos. En consecuencia, el número total de números libres de cuadrados ha de ser 2^r. Para un valor *n,* el número de términos menores o iguales que él y divisibles por p_i^2 es menor o igual que n/p_i^2. Por tanto, $2^r \geq n\left(1-\sum_{i=1}^{r}\frac{1}{p_i^2}\right) = Cn$, con *C* positivo. Al ser *r* constante, la desigualdad $2^r > Cn$ sólo es posible para un número finito de valores de . Hemos llegado a un absurdo consecuencia de suponer finito el número de primos.

Demostración 17ª [Siguiendo a Nair, 1982]

Sea

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

$$= \sum_{r=0}^{n}(-1)^r \binom{n}{r} \frac{1}{n+r+1}.$$

Multiplicamos I_n por d_{2n+1} donde d_m es el mínimo común múltiplo de los *m* primeros números.

Como $x(1-x) \leq 1/4$ e $I_n > 0$ tenemos que $1 \leq (1/4)^n d_{2n+1}$, de donde

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

Pero, esta expresión sólo es cierta para un número finito de valores de *n*. Por tanto, obtenemos una contradicción al suponer que el número de primos sea finito.

Demostración 18ª [Hacks]

Puesto que tenemos la igualdad $\prod_p (1-1/p^2)^{-1} = \pi^2/6$, si el número de primos es finito, el producto inicial es racional. Sin embargo, es conocido que π^2 es irracional, por lo que deducimos que el número de primos ha de ser infinito.

Demostración 19ª [Pollack]

Haciendo uso de la célebre evaluación de Euler de las series $\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^{2k}}$ con k un entero positivo, podemos escribir la igualdad: $\frac{\zeta(2)^2}{\zeta(4)} = 5/2$. Por otra parte, utilizando la igualdad producto para ζ, escribimos $\frac{\zeta(2)^2}{\zeta(4)} = \prod_p \frac{p^2+1}{p^2-1}$

Suponiendo que el número de primos sea finito, tendremos que $\frac{5}{2} = \frac{5}{3}\frac{10}{8}\frac{26}{24}\cdots = \frac{M}{S}$. Puesto que 3 divide a *S,* debe hacerlo también con *M*, por lo que 3 divide a algún $p_i^2 + 1$ o, equivalentemente, $p_i^2 \equiv 2 \pmod 3$. Pero esto último no es posible ya que $0^2 \equiv 0 \pmod 3$; $1^2 \equiv 1 \pmod 3$; $2^2 \equiv 1 \pmod 3$. Esta contradicción nos muestra que el cardinal del conjunto de los números primos es infinito.

Demostración 20ª (Imitación)

A partir de la doble expresión:

$$\prod_p \frac{\zeta(8)}{\zeta(4)\zeta(2)^2} = 8/35, \quad \prod_p \frac{\zeta(8)}{\zeta(4)\zeta(2)^2} = \prod_p \frac{(p^2-1)^2}{p^4+1},$$

si el número de primos fuese finito, el último producto sería igual a un racional, digamos *M/S* (con *M* y *S* no necesariamente primos entre sí)**.** De ahí, deducimos que $35S = 8M$, por lo que 5 divide a algún p^4+1 o equivalentemente a $p^4 \equiv 4$. Pero esto, por el teorema pequeño de Fermat, no es posible. (También se puede comprobar directamente.) De este modo, volvemos a obtener una contradicción.

Damos a continuación tres demostraciones nuevas de la infinitud del número de primos.

Demostración 21ª

Combinando las fórmulas de Stirling, $n! \approx e^{n\ln n - n + \frac{1}{2}\ln(2\pi n)}$ y de Legendre, $n! = \prod_p p^{\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots}$ tenemos lo siguiente:

$$n^n e^{-n} < n! = \prod_p p^{\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots} \le \prod_p p^{\frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots}$$

$$= \left(\prod_p p^{\frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots} \right)^n \le C^n.$$

La desigualdad $n^n e^{-n} < C^n$ es equivalente a $\frac{n}{C} < e$. Esto último sólo es posible para un número finito de valores de *n*. Por ello, concluimos que el número de primos es infinito.

Demostración 22ª

Utilizando la fórmula de Legendre, tenemos:

$$\binom{2n}{n} = \frac{(2n)!}{n!n!} = \frac{\prod_p p^{\left\lfloor \frac{2n}{p} \right\rfloor + \left\lfloor \frac{2n}{p^2} \right\rfloor + \left\lfloor \frac{2n}{p^3} \right\rfloor + \cdots}}{\prod_p p^{2\left\lfloor \frac{n}{p} \right\rfloor + 2\left\lfloor \frac{n}{p^2} \right\rfloor + 2\left\lfloor \frac{n}{p^3} \right\rfloor + \cdots}}$$

$$= \prod_p p^{\left\lfloor \frac{2n}{p} \right\rfloor - 2\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{2n}{p^2} \right\rfloor - 2\left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{2n}{p^3} \right\rfloor - 2\left\lfloor \frac{n}{p^3} \right\rfloor + \cdots}$$

$$\leq \prod_p p^{\log_p(2n)} \leq \prod_p 2n = 2^r n^r$$

Si aplicamos la formula de Stirling al primer término, tenemos que para valores grandes de n, $2^n = O\left(n^r\right)$. Pero esto último sólo es posible para un número finito de valores de *n*. Concluimos entonces que el cardinal del conjunto de los números primos es infinito.

Demostración 23ª

Consideraremos el conjunto de los naturales *n* tales que $1 \leq n \leq R$. En él asignamos la probabilidad uniforme: todo elemento tiene la misma probabilidad 1/*R*. Tomamos el suceso P_i que consta de los múltiplos de p_i, y su probabilidad es $1/p_i$. Puesto que P_i y P_j son independientes entre sí cuando $i \neq j$, la probabilidad de no ser divisible por ningún primo es $\prod_p (1-1/p) = 1/R$ (el único valor que no es divisible por un primo es 1).

Repitiendo esta idea en el conjunto $1 \leq n \leq R^2$, tenemos la identidad $\prod_p (1-1/p) = 1/R^2$ Por tanto, $1/R = 1/R^2$. Pero esto es falso, salvo que sea $R = 1$. Como esto último no puede ocurrir, deducimos que existen infinitos números primos.

LA SUMA DE LA SERIE DE LOS INVERSOS DE LOS PRIMOS NO EXISTE

Antes de comenzar con las demostraciones que presentamos, es necesario recordar que si los términos a_n son todos del mismo signo, la convergencia a un número no nulo de un producto infinito de la forma $\prod_n (1+a_n)$ es equivalente a la convergencia de la serie $\sum_n a_n$. En particular, son equivalentes la convergencia de $\prod_p \left(1+\frac{1}{p}\right)$ y la de $\sum_p \frac{1}{p}$. Como es

usual, por $\pi(k)$ notaremos al cardinal del conjunto de los números primos menores o iguales que k.

Demostración 1ª [Euler, 1737]

Partiendo de la desigualdad $\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1} > \sum_{n\le x}\frac{1}{n} > \ln x$ se sigue la relación

$$-\sum_{p\le x}\ln(1-1/p) > \ln\ln x,$$

donde el término de la derecha diverge cuando $x \to \infty$. Como, además, se tiene $0 < \ln(1-1/p)+1/p < \frac{C}{p^2}$ tenemos la divergencia de la serie de los inversos de los primos.

Imitación. La convergencia de $2\sum_p \frac{1}{p}$ es equivalente a la de $\prod_p\left(1+\frac{2}{p}\right)$.

Podemos escribir las siguientes desigualdades:

$$\prod_{p\le p_n}\left(1+\frac{2}{p}\right) > \prod_{p\le p_n}\left(1+\frac{1}{p}+\frac{1}{p(p-1)}\right)$$
$$= \prod_{p\le p_n}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right) > 1+\frac{1}{2}+\cdots+\frac{1}{p_n}.$$

Pero, el último término es, aproximadamente, $\ln p_n$. Por tanto, la serie inversa de los primos no converge.

Demostración 2ª [Tras los pasos de Tschebyshev, 1851]

Esta es una demostración que aparece en muchos textos y está basada en una de las desigualdades de Tchebyshev: $\pi(k) > C_1 k/\ln k$.

Haciendo $k = p_n$, se deduce

$$\frac{p_n}{\ln p_n} < C_2 n \Rightarrow p_n \le C_2 n \ln p_n \qquad (a)$$

Si tenemos en cuenta que $\ln x < \sqrt{x}$ obtenemos $\ln p_n < C_3 \ln n$ Sustituyendo en la desigualdad (a), tenemos $p_n < C_4 n \ln n$ Ahora, puesto que $\sum \frac{1}{n\ln n}$ diverge, también lo hace $\sum \frac{1}{p_n}$

Demostración 3ª [Erdö s, 1938]

Si la serie $\sum_p \frac{1}{p}$ converge, podemos encontrar un número b, verificando $\sum_{p\ge b}\frac{1}{p} < 1/2$.

Para la demostración, introducimos los siguientes conjuntos:

$$M_x = \{n \leq x \ : \text{todos sus divisores primos son menores que } b\}$$

y

$$N_x = \{n \leq x \ : \text{admite un divisor primo mayor que } b\}.$$

Entre sus cardinales se da la siguiente relación $Card(N_x) = x - Card(M_x)$ Por otra parte, la cantidad de números menores o iguales que x divisibles por p es $\lfloor x/p \rfloor$. Puesto que $Card(N_x) \leq \sum_{p \geq b} \left\lfloor \frac{x}{p} \right\rfloor \leq \sum_{p \geq b} \frac{x}{p} \leq x/2$ deducimos que $x - Card(M_x) \leq x/2$; y, por tanto, $x/2 \leq \text{Card}(M_x)$.

Si $n \in M_x$, entonces $n = k^2 m$, con m libre de cuadrados y perteneciente a M_x. Puesto que $k \leq \sqrt{n} \leq \sqrt{x}$ y la cantidad de números libres de cuadrados de M_x es menor o igual que 2^b se sigue que $Card(M_x) \leq 2^b \sqrt{x}$ y, por tanto, $x/2 \leq 2^b \sqrt{x}$.

Esto último es falso para valores suficientemente grandes de x. Por tanto, $\sum_p \frac{1}{p}$ no converge.

Demostración 4ª [Bellman, 1943]

Si la suma de la serie fuese finita $\sum_p \frac{1}{p} < \infty$ existiría un valor b verificando $\sum_{p \geq b} \frac{1}{p} < \alpha < 1$; por esto, deducimos que $\left(\sum_{p \geq b} \frac{1}{p} \right)^2 < \alpha^2$ En general, tenemos que $\left(\sum_{p \geq b} \frac{1}{p} \right)^n < \alpha^n$ De esas acotaciones se sigue esta otra:

$$\sum_{n=1}^{\infty} \left(\sum_{p \geq b} \frac{1}{p} \right)^n < \sum_{n=1}^{\infty} \alpha^n.$$

Ahora bien, la última serie es una progresión geométrica convergente. Consecuentemente, también habrá de ser finita la expresión

$$\left(1 + \sum_{n=1}^{\infty} \left(\sum_{p \geq b} \frac{1}{p} \right)^n \right) \frac{1}{(1 - \frac{1}{2}) \cdots (1 - \frac{1}{s})},$$

donde el producto es sobre los primos y s es el mayor primo menor que b.

Sin embargo, este producto es, nuevamente, la serie $\sum_{n \in \mathbb{Z}^+} \frac{1}{n}$, que, como bien sabemos, diverge. Concluimos, por tanto, que la suposición inicial de convergencia no puede ser cierta.

Demostración 5ª [Dux, 1956]

Volvamos a suponer que $\sum_{p>b} \frac{1}{p} < \frac{1}{2}$ y definamos los conjuntos:

$$M = \{n : \text{todos sus divisores primos son menores que } b\}$$
$$S = \{n : \text{todos sus divisores primos son mayores que } b\}$$
$$Q = \{n : \text{admite divisores primos mayores y menores que } b\}$$

Tenemos dos series cuyas sumas son finitas:

$$\sum_{n\in M} \frac{1}{n} = \prod_{p\le b} \frac{1}{(1-\frac{1}{p})}$$

y

$$\sum_{m\in S} \frac{1}{m} \le \sum_{p>b} \frac{1}{p} + \left(\sum_{p>b} \frac{1}{p}\right)^2 + \cdots < 1.$$

Como consecuencia de que estas dos series sean convergentes, también lo habrá de ser:

$$\sum_{t\in Q} \frac{1}{t} = \sum_{n\in M} \frac{1}{n} \sum_{m\in S} \frac{1}{m}.$$

Finalmente, al ser las tres series anteriores convergentes, deducimos que lo es la serie armónica

$$\sum_{n\in\mathbb{Z}^+} \frac{1}{n} = 1 + \sum_{n\in Q} \frac{1}{n} + \sum_{n\in M} \frac{1}{n} + \sum_{n\in S} \frac{1}{n},$$

pero esto nos lleva a una contradicción; y, por tanto, debemos concluir que la serie de los inversos de los primos es divergente.

Demostración 6ª [Moser, 1958]

Usando la notación $R(x) = \sum_{p\le x} \frac{1}{p}$ la demostración se basa en el siguiente resultado: Si existe $\sum_p \frac{1}{p}$, entonces $\lim_{n\to\infty} \pi(x)/x = 0$.

Podemos hacer estos cálculos:

$$\pi(x) = 1(R(1) - R(2)) + 2(R(2) - R(3)) + \cdots + x(R(x) - R(x-1)),$$

de donde

$$\pi(x)/x = R(x) - ((R(0) + R(1) + \cdots + R(x-1))/x;$$

y, por la sumabilidad de Césaro, los dos términos de la derecha tienen el mismo límite.

Si la serie $\sum_p 1/p$ fuera convergente, tendrían que existir un n de modo que $\sum_{p>n} \frac{1}{p} < 1/2$ y un m tal que $\pi(n!m)/m < 1/2$. Con ellos, definamos $T_i = in! - 1$, para cada $i = 1, \ldots, m$. Los factores primos de T_i son mayores que n. Si p es un primo común a T_i y T_j entonces p divide $j - i$; y, por tanto, p habrá de dividir, como máximo, a $m/p + 1$ de los T_i. Pero, como cada T_i tiene, al menos, un primo entre n y $n!m$, deducimos la desigualdad $\sum_{n!m>p>n} \left(\frac{m}{p}+1\right) \geq m$ que, a su vez, implica $\sum_{p>n} \frac{1}{p} + \frac{\pi(n!m)}{m} \geq 1$. Ahora bien, esta última expresión es contradictoria con las dos primeras desigualdades.

Demostración 7ª [Clarkson, 1966]

Si la serie $\sum_p 1/p$ es convergente, al igual que antes, tomemos b verificando $\sum_{p>b} \frac{1}{p} < 1/2$ y definamos $Q = \prod_{p \leq b} p$. En estas condiciones podemos afirmar que los factores de $1 + iQ$ son todos mayores que b y, por tanto,

$$\sum_{i=1}^{r} \frac{1}{1+iQ} < \sum_{p>b} \frac{1}{p} + \left(\sum_{p>b} \frac{1}{p}\right)^2 + \left(\sum_{p>b} \frac{1}{p}\right)^3 + \cdots < \sum_{j=1}^{\infty} \frac{1}{2^j} = 1.$$

Pero esto no es posible, pues en ese caso $\sum_{i\geq 1} \frac{1}{1+iQ}$ sería una serie convergente, y en consecuencia, se tendría la convergencia de la serie armónica. Concluimos así que la serie $\sum_p \frac{1}{p}$ es divergente.

Demostración 8ª [Vanden Eynden, 1980]

Consideremos, nuevamente, el conjunto

$$M = \{n : \text{todos sus divisores primos son menores que } b\} \cup \{1\}.$$

Utilizando la igualdad

$$\prod_{p \leq b} \left(1 + \frac{1}{p}\right) \sum_{n \in M} \frac{1}{n^2} = \sum_{n \in M} \frac{1}{n},$$

si hacemos tender b a infinito y suponemos que el producto infinito es convergente, tenemos la identidad

$$\prod_p \left(1+\frac{1}{p}\right)\sum_{n\in Z^+}\frac{1}{n^2} = \sum_{n\in Z^+}\frac{1}{n}$$

Pero, ahora, la suposición de la convergencia de la serie $\sum_p \frac{1}{p}$ implicaría la de la serie armónica. Este absurdo nos lleva a afirmar que la serie de los inversos de los primos es divergente.

Las dos demostraciones siguientes son nuevas.

Demostración 9ª

Está basada en dos fórmulas para el factorial de un número. Se trata de las conocidas fórmulas de Stirling y de Legendre.

Con la ayuda de ellas podemos establecer que, para $n \geq 2$ existe $C_1 > 0$ verificando que

$$e^{C_1 n \ln n} \leq e^{n\ln n - n} \leq n! = \prod_p p^{\left\lfloor \frac{n}{p}\right\rfloor + \left\lfloor \frac{n}{p^2}\right\rfloor + \left\lfloor \frac{n}{p^3}\right\rfloor + \cdots}.$$

Utilizando lo anterior y sumando una serie geométrica tenemos

$$\begin{aligned} C_1 n\ln n &\leq \sum_{p\leq n} n\ln p\left(\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\cdots\right)\\ &\leq \sum_{p\leq n} n\frac{\ln p}{p} + n\sum_{p\leq n}\ln p\sum_{n=2}^{\infty}\frac{1}{p^n}\\ &= \sum_{p\leq n} n\frac{\ln p}{p} + n\sum_{p\leq n}\frac{1/p^2}{1-1/p}\ln p\\ &= \sum_{p\leq n} n\frac{\ln p}{p} + n\sum_{p\leq n}\frac{1}{p(p-1)}\ln p. \end{aligned}$$

Puesto que $\sum_{d=2}^{\infty}\frac{1}{d(d-1)}\ln d$ es convergente, la última suma está acotada por C_2. Esto nos conduce a la desigualdad

$$C_1 n\ln n \leq \sum_{p\leq n} n\frac{\ln p}{p} + C_2 n,$$

que la podemos reescribir así: $C_1 \ln n \leq \sum_{p\leq n}\frac{\ln p}{p} + C_2.$

Supongamos que $\sum_p \frac{1}{p}$ sea convergente. Entonces existirá un k tal que $\sum_{p\geq k} \frac{1}{p} < C_1/4$. Por tanto, ha de valer la relación:

$$\sum_{p\leq k} \frac{\ln p}{p} + \sum_{k<p\leq n} \frac{\ln p}{p} \leq C_3 + C_1 \frac{\ln n}{4}.$$

Ahora bien, dado que a partir de cierto valor de n se tiene que $C_2 + C_3 \leq C_1 \frac{\ln n}{4}$, se sigue que

$$C_1 \ln n \leq C_1 \frac{\ln n}{2} \Leftrightarrow C_1 \leq \frac{C_1}{2};$$

desigualdad evidentemente absurda que nos lleva a concluir que la serie $\sum_p \frac{1}{p}$ no es convergente.

Demostración 10ª

Suponiendo que exista $\sum_p \frac{1}{p} = k$, escribiremos

$$k_r = \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p_{r-1}} + \frac{1}{p_r} < k.$$

Vamos a estudiar e^{k_r}. Gracias al desarrollo en serie de la función exponencial, tenemos que

$$e^k > e^{k_r} = 1 + k_r + \frac{k_r^2}{2!} + \frac{k_r^3}{3!} + \cdots > \sum_{n<p_r}^{*} \frac{1}{n},$$

donde * indica que la suma está tomada en los números enteros positivos libres de cuadrados (esto es, que todos los números primos en su factorización tienen exponente uno). Haciendo tender r hacia infinito obtenemos que la suma de los inversos de los enteros positivos libres de cuadrados $\sum_n^{*} \frac{1}{n}$ es convergente.

Pero es conocido que esa serie es divergente: de no ser así, puesto que la suma de los inversos de los cuadrados es finita, existiría el producto

$$\sum_n^{*} \frac{1}{n} \sum_{n=1}^{\infty} \frac{1}{n^2},$$

lo que es equivalente a afirmar que la serie armónica converge. Por tanto, $\sum_p \frac{1}{p}$ ha de ser divergente.

Una bonita demostración, aunque errónea

La probabilidad de que un número no sea divisible por ningún primo es cero; pero también es $\prod_p \left(1-\frac{1}{p}\right)$ por lo que $\prod_p \left(1-\frac{1}{p}\right)=0$ y, equivalentemente, $\sum \frac{1}{p}$ diverge.

Es conocido que no es posible definir una probabilidad P en $\mathbb{Z}^+$ verificando que $P(n\mathbb{Z}^+) = 1/n$. Utilizando una variación de esta idea, sí que es posible dar una demostración correcta de la divergencia de la serie.

Demostración 11ª [Pinasco]

Dado un subconjunto A de $\mathbb{Z}^+$ definimos $A(n) := \sum_{\substack{1\le a\le n \\ a\in A}} 1$. Si existe $\lim_{n\to\infty} \frac{A(n)}{n}$, a este número lo llamaremos densidad de A.

Es sencillo comprobar que existe la densidad del conjunto de los números que no son múltiplos de los primeros primos y esta densidad es, exactamente, $\prod_{n=1}^{k}\left(1-\frac{1}{p_n}\right)$. Suponiendo que existiese $\sum \frac{1}{p}$ tendríamos que esa densidad estaría acotada por $\sum_{n=k+1}^{\infty} \frac{1}{p_n}$.

Con la suposición de la convergencia de $\sum \frac{1}{p}$ tendremos que:

a) $\prod_{n=1}^{k}\left(1-\frac{1}{p_n}\right) > \prod_p \left(1-\frac{1}{p}\right) > \varepsilon > 0$, y

b) es posible tomar k verificando que $\sum_{n=k+1}^{\infty} \frac{1}{p_n} < \varepsilon$.

Pero estas conclusiones nos conducen a que

$$\varepsilon < \prod_{n=1}^{k}\left(1-\frac{1}{p_n}\right) < \sum_{n=k+1}^{\infty} \frac{1}{p_n} < \varepsilon,$$

lo que, evidentemente, es absurdo y nos da, nuevamente, la divergencia de la serie $\sum \frac{1}{p}$ de los recíprocos de los primos.

AGRADECIMIENTOS

Este trabajo está financiado por el Ministerio de Ciencia e Innovación (España) bajo el Proyecto de Investigación número MTM2011-22394

REFERENCIAS

Aldaz, J.M. y Bravo, A. (2003). *Euclid's argument on the infinitude of primes. Amer. Math. Monthly,* 110(2), 141-142.

Abel, U. y Siebert, H. (1993). *Sequences with large numbers of prime values*. *Amer. Math. Monthly,* 100(2), 167-169.

Bellman, R. (1943) *A note on the divergence of a series*. *Amer. Math. Monthly, 50,* 318-319.

Bateman, P.T. y Horn, R.A. (1962). *A heuristic asymptotic formula concerning the distribution of prime numbers. Math. Comp.* 16, 363-367.

Chapman, R. (2003). *Evaluating* ζ(2). Recuperado de la dirección http://www.maths.ex.ac.uk/ rjc/rjc.html

Chebyshev, P.L. (1851) *Sur la fonction qui detérmine la totalité des nombres premiers inférieurs a une limite donnée. Mémoires présentés a l'Académie Impériale des Sciences de St. Petersbourg par divers Savants 6*, 141-157.

Chebyshev, P.L. (1852) *Mémoire sur les nombres premiers. Journal de Mathématique pures et appliqués, 17,* 366-390.

Clarkson, J.A. **(**1966). *On the series of prime reciprocals. Proc. Amer. Math. Soc.,* 17, 541.

Dressler, R.E. (1975). *A lower bound for* π (n). *Amer. Math. Monthly,* 82**,** 151-152.

Dux, E. (1956). *Ein kurzer Beweis der Divergenz der unendlichen Reihe* $\sum_{r=1}^{\infty} \frac{1}{Pr}$ *. Elem. Math.,* 11*,* 50-51.

Euler, L. (1737). *Variae observationes circa series infinites. Comm. Acad. Petropolitanae, 9,* 160-188.

Erdös, P. (1938). *Ü ber die Reihe* $\sum \frac{1}{p}$, *Mathematica Zutphen B,* **7***,* 1-2.

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

Golomb, S.W. (1959). *A connected topology for the integers. Amer. Math. Monthly,* **66***,* 663-665.

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

Hemminger, R. (1966). *More on the infinite primes theorem. Amer. Math. Monthly, 73,* 1001-1002

Hirschhorn, M.D. (2002). *There are infinitely many prime numbers*, *Austral. Math. Soc. Gaz., 29*(2), 103.

Mohanty, S.P. (1978). *The number of primes is infinite. Fibonacci Quart.,* **16**(4), 381-384.

Mohanty, S.P. (1979). *The number of primes is infinite. Bull. Math. Assoc. India,* **11**(1-2), 62-68.

Moser, L. (1958). *On the series* $\sum \frac{1}{P}$ *. Amer. Math. Monthly, 65,* 104-105.

Nair, M. (1982). *On Chebyshev-type inequalities for primes. Amer. Math. Monthly,* **89**(2), 126-129.

Pollack, P. (2004). *Not Always Buried Deep. Selections from Analytic and Combinatorial Number Theory 2003*. Recuperado de la dirección http://www.princeton.edu/~ppollack/notes/notes.pdf

Ribenboim, P. (1996). *The new book of prime number records*. New York: Springer-Verlag.

Rubinstein, M. (1993). *A formula and a proof of the infinitude of the primes. Amer. Math. Monthly, 100,* 388-392.

Sierpiński, W. (1964). *Les binômes* $x^2 + n$ *et les nombres premiers. Bull. Soc. Roy. Sci. Liége 33,* 259-260.

Vanden Eynden, Ch. (1980). *Proofs that* $\sum 1/p$ *diverges. Amer. Math. Monthly, 87*(5), 394-397.

Wunderlich, M. (1965). *Another proof of the infinite primes theorem. Amer. Math. Monthly, 72,* 305.