

Las demostraciones alternativas como recurso científico y didáctico. El caso de la infinitud de los números primos.

Vicente Vicario García

En este artículo pretendemos poner de relieve la importancia de las componentes científica y didáctica asociadas a las demostraciones alternativas de una misma proposición matemática. La pluralidad demostrativa nos permite interpretar las funciones de la demostración y enriquecer la comprensión de un determinado objeto matemático. Es esta gama de posibilidades y relaciones demostrativas la que nos ayuda a alcanzar la óptima comprensión significativa asociada a la demostración matemática y establecer conexiones, a veces inesperadas.

Introducción

Una manera de hacer más significativa la comprensión asociada al contenido de la demostración de una proposición matemática es abordar ésta desde diferentes vertientes. Desde el punto de vista científico, las demostraciones alternativas de una misma proposición brindan espléndidas garantías de poder interconectar y explorar un determinado objeto matemático a través de diversas ramas de la matemática, quizás remotas, para poder así llegar a un alto nivel de comprensión de la proposición demostrada y de todo su entorno asociado. Creemos que es muy conveniente poder utilizar, siempre que sea posible, distintas técnicas para demostrar una misma proposición, ya que nos permite intuir, clarificar, verificar y proporcionar, en muchos casos, pautas explicativas. Además, las diferentes demostraciones suelen aportar matices nuevos que pueden ser interesantes y que nos dan idea de qué camino escoger más acorde a la potencia demostrativa o explicativa que pretendemos en un determinado contexto.

Otra razón esencial para el estudio y análisis de las demostraciones alternativas es su aplicación en el campo de la didáctica de la matemática, y más concretamente, en el aula. Parece razonable pensar que si disponemos de algunas demostraciones alternativas de una proposición, podemos emplear éstas según los fines que se deseen y dependiendo del nivel del auditorio al que se destinan. Podemos también etiquetar y analizar cada demostración según el marco de las funciones más relevantes que muestre, como verificación, sistematización, y explicación, además de otras.[†] Cada nueva demostración debe hacernos reflexionar fundamentalmente sobre su alcance junto con el grado de interconexión y simplicidad que exhibe respecto de otras demostraciones.[‡]

El propósito de estas líneas es reflejar esta dinámica con un ejemplo paradigmático como el elegido: *“El caso de la infinitud de los números primos”*.

[†] Véanse el artículo iniciador *“El papel y la función de la demostración en matemáticas”* de M. de Villiers, Universidad de Stellenbosch, África del Sur, en Epsilon, N° 26, 1993. pp. 15-30. Este artículo es una versión traducida al castellano y adaptada del artículo aparecido en Pythagoras, 24 Nov, 1990, traducido y publicado con la correspondiente autorización.

[‡] Véase el artículo *“Concepciones del profesor de secundaria sobre la demostración matemática. El caso de la irracionalidad de $\sqrt{2}$ y las funciones de la demostración”* de Vicente Vicario García y José Carrillo Yáñez en IX simposio de la SEIEM, Córdoba, 2005, pp 145-152.

Creemos que la pluralidad demostrativa que se muestra en este trabajo habla por sí sola de la potente gama de ideas científico-didácticas y conclusiones que se pueden extraer del mismo.

A continuación, y después de un breve preámbulo sobre los números primos y sus caracterizaciones básicas, exponemos algunas demostraciones elementales de la infinitud de los números primos. En una parte de las mismas se asumen como previamente demostrados otros teoremas que se especifican, en otras, se escriben algunos comentarios históricos relativos a la demostración. Obviamente, existen versiones muy potentes relativas a la distribución de los números primos como el postulado de Bertrand o incluso el famoso teorema del número primo (*TNP*), pero nuestro objetivo aquí es sólo el análisis de demostraciones simples y relativamente breves.

La sucesión de los números primos 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,... extraída del conjunto de los números naturales nos es completamente familiar. Muchos problemas y muy profundos, algunos de los cuales son muy sencillos de enunciar y extraordinariamente complejos de demostrar, han sido planteados a cerca de esta serie de números que ha sido objeto de estudio y reflexión a lo largo de los últimos veinticinco siglos. Ya en 1751 el genial y prolífico matemático suizo Leonhard Euler (1707, 1783) expresaba lo siguiente:

“Los matemáticos han intentado en vano, hasta ahora, descubrir algún orden en la secuencia de los números primos y tenemos razones para creer que se trata de un misterio en el que nunca penetrará la mente humana”.

Es fácil construir mecánicamente una tabla de números primos hasta un límite moderado N , mediante un procedimiento conocido ya por los antiguos matemáticos griegos denominado “*Criba de Eratóstenes*”. Para ello se escriben todos los números naturales desde 2 hasta N . A partir de aquí, comenzamos con el 2 y tachamos en sucesión, de dos en dos, todos los números de la lista. El siguiente número no tachado, el 3, es primo, y comenzamos desde este número tachando todos los enteros de tres en tres, no tachados previamente. El siguiente número no tachado, el 5, es primo, y tachamos ahora todos los múltiplos de cinco no tachados previamente, contando para ello de cinco en cinco. Así proseguimos sucesivamente hasta considerar el último primo $p \leq \sqrt{N}$ y se detiene el proceso. Los números que quedan sin tachar, junto con los iniciales ya considerados, son todos los números primos hasta N . Este tipo de construcción nos muestra que los números primos son cada vez más escasos.

Por otra parte, es sencillo comprender que existen en la recta numérica bloques de enteros compuestos consecutivos tan grandes como queramos. El precio a pagar es que debemos utilizar números cada vez mayores. Basta observar que para cualquier $n > 1$, los números consecutivos $n!+2, n!+3, \dots, n!+n$ son todos compuestos. Nuestro objetivo ahora es demostrar, e intentar comprender, por qué existen infinitos números primos aunque estos se hagan cada vez más raros.

Veamos a continuación diversas demostraciones relativamente breves de la infinitud de los números primos:

Proposición: “El conjunto de los números primos contiene infinitos elementos”.

1ª Demostración (Euclides): Razonaremos por reducción al absurdo. Supongamos que el número de primos sea finito. Sean entonces los números primos los elementos del conjunto $\{p_1, p_2, p_3, \dots, p_n\}$. Construyamos el número $N = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n + 1$. Este número N , o bien es primo, o bien es divisible por algún número primo q necesariamente distinto a los p_i anteriores. Por tanto, en cualquier caso, hemos llegado a una contradicción que demuestra el teorema.[†]

2ª Demostración (Hermite): Sean $n = 1, 2, 3, \dots$ los números naturales y q_n el factor primo más pequeño de $n! + 1$ para cada valor de n . Como q_n tiene que ser necesariamente mayor que n , se deduce que esta sucesión contiene infinitos elementos distintos, y que por tanto existen infinitos números primos.

3ª Demostración (Saidak): Sea n un número natural arbitrario. Sabemos que puesto que n y $n + 1$ son números naturales consecutivos deben ser primos entre sí. Entonces el número $N_2 = n(n + 1)$ debe tener, como mínimo, dos factores primos distintos. Análogamente, los números naturales $n(n + 1)$ y $n(n + 1) + 1$, son consecutivos y, por tanto, primos entre sí. En consecuencia, el número $N_3 = n(n + 1) \cdot [n(n + 1) + 1]$ debe tener, como mínimo, tres factores primos diferentes. Este proceso puede ser continuado indefinidamente, así que el conjunto de los números primos es infinito.[#]

4ª Demostración (Odoni): Se considera la sucesión recurrente $e_{n+1} = e_1 \cdot e_2 \cdot e_3 \cdot \dots \cdot e_n + 1$ con $e_1 = 2$ y $n \geq 1$. Podemos observar que si $i \neq j$ entonces $m.c.d.(e_i, e_j) = 1$ ya que cualquier factor primo común a e_i y e_j debe dividir a 1. Sea ahora p_i el menor número primo que aparece en la descomposición en factores primos de e_i , entonces la sucesión $p_1, p_2, p_3, \dots, p_n, \dots$ es una sucesión infinita de primos distintos, lo que demuestra el teorema.[‡]

5ª Demostración (Stieltjes): Asumiremos (para abreviar la exposición) como lema previo en esta demostración la proposición siguiente debida a Euclides: “Sea p número primo que divide al producto de naturales ab . Entonces p divide a o p divide b ”. (esta proposición aparece en *Los Elementos* como Proposición 30 del libro VII, a veces denominada, lema de Euclides.

Razonaremos por reducción al absurdo. Supongamos que el número de primos es finito. Sea Q el producto de todos los números primos y sean $m > 1$ y $n > 1$ dos

[†] Esta demostración clásica aparece en el libro IX de *Los Elementos* como proposición 20. Puede reformularse trivialmente de manera que se transforme en una demostración directa, en lugar de la demostración indirecta dada. Para ello, basta considerar un conjunto de números primos consecutivos $\{p_1, p_2, p_3, \dots, p_n\}$ y construir el número $N = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n + 1$ que debe ser divisible por algún número primo distinto a los anteriores. Obsérvese que el razonamiento proporciona un método para construir o identificar, al menos teóricamente, nuevos números primos.

[#] Esta bellísima demostración es extraordinariamente reciente y apareció en un artículo de Filip Saidak con el título “*A new Proof of Euclid’s theorem*” en *American Mathematical Monthly*, December 2006, pp. 937-938.

[‡] Obsérvese que claramente se cumple la relación $e_{n+1} = e_n^2 - e_n + 1$.

enteros positivos con $Q = m \cdot n$. Se tiene entonces, según el lema de Euclides, que todo número primo p divide, o bien a m , o bien a n , pero no a ambos (m y n son primos entre sí). Entonces $m + n$ no puede tener ningún divisor primo, lo que es una contradicción.

6ª Demostración (Euler): El gran matemático Leonhard Euler llegó a descubrir relaciones sorprendentes entre la teoría de números y el análisis. En su artículo “*Variae observationes circa series infinitas*” de 1737, demostró que la divergencia de la serie armónica implica, de forma sorprendente, la existencia de infinitos números primos.

La demostración siguiente, por reducción al absurdo, se basa en el teorema fundamental de la aritmética y en la divergencia de la serie armónica.[†]

Supongamos que existen solamente k números primos distintos $\{p_1, p_2, p_3, \dots, p_k\}$. Aplicando el teorema fundamental de la aritmética, sabemos que todo número natural n es descomponible en forma única (salvo reordenaciones triviales) en la forma canónica $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k}$.

Partimos ahora de la siguiente relación, que es fácil de verificar, ya que en el miembro de la derecha aparecen todos los inversos de los números naturales:

[†] El comportamiento divergente de la serie armónica ya había sido detectado en el siglo XIV por Oresme. Agrupó los sucesivos términos de la serie armónica colocando el primer y segundo términos en un primer grupo, los dos términos siguientes en un segundo grupo, los cuatro términos que le siguen en un tercer grupo, y así sucesivamente, de manera que el grupo m -ésimo incluye 2^{m-1} términos. Entonces es claro que tenemos infinitos grupos de términos y que la suma de los términos relativos a cada grupo es mayor o igual que $1/2$, por lo que sumando una cantidad suficiente de términos podemos superar cualquier número dado.

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \dots = 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \dots + \frac{1}{8}\right) + \left(\frac{1}{9} + \dots + \frac{1}{16}\right) + \dots \geq$$

$$1 + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \left(\frac{1}{16} + \frac{1}{16} + \dots + \frac{1}{16}\right) + \dots \geq \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \dots$$

También el matemático Pietro Mengoli (1625,1686) redescubrió el resultado de Oresme sobre la divergencia de la serie armónica asociando términos, teorema que se suele atribuir a Jacques Bernouilli que en 1689 proporcionó en su *Tractatus de seriebus infinitis* una demostración especialmente elegante y rigurosa y que damos a continuación. En su demostración, Jacques afirma primero que, si $a > 1$, entonces $\frac{1}{a} + \frac{1}{a+1} + \frac{1}{a+2} + \dots + \frac{1}{a^2} \geq 1$.

Para ello basta considerar la clara desigualdad siguiente $\frac{1}{a+1} + \frac{1}{a+2} + \dots + \frac{1}{a^2} \geq (a^2 - a) \frac{1}{a^2} = 1 - \frac{1}{a}$ y a partir de aquí, llegamos a lo afirmado por Bernouilli. Por tanto, aplicando esta desigualdad sobre los términos de la serie armónica, llegamos a la relación siguiente:

$$\sum_{k=1}^{\infty} \frac{1}{k} = 1 + \left(\frac{1}{2} + \frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \dots + \frac{1}{25}\right) + \left(\frac{1}{26} + \frac{1}{27} + \dots + \frac{1}{676}\right) + \dots \geq 1 + 1 + 1 + 1 + \dots$$

de la que se deduce que la serie armónica crece más que cualquier número prefijado. Otra demostración radicalmente diferente de la divergencia de la serie armónica fue dada por su hermano Jean Bernouilli. El propio Euler proporcionó otra demostración en su *Introductio in Analisin Infinitorum* de 1748, pero resultó poco rigurosa bajo el prisma actual, ya que en ella se omitían conceptos como convergencia/divergencia de una serie.

$$\sum_{n=1}^{\infty} \frac{1}{n} = \left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \dots\right) \cdot \left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \dots\right) \cdots \left(1 + \frac{1}{p_k} + \frac{1}{p_k^2} + \dots\right) \quad [1]$$

Además, a partir del valor de la suma de los infinitos términos de una serie geométrica convergente, tenemos que

$$\sum_{n=1}^{\infty} \frac{1}{n} = \frac{1}{1 - \frac{1}{p_1}} \cdot \frac{1}{1 - \frac{1}{p_2}} \cdots \frac{1}{1 - \frac{1}{p_k}} \quad [2]$$

lo que es absurdo, ya que la serie armónica $\sum_{n=1}^{\infty} \frac{1}{n}$, como es sabido, es divergente.

7ª Demostración (Euler): Esta es otra demostración debida a Euler. Demostraremos que la suma de los inversos de los números primos es divergente utilizando los recursos del análisis matemático, lo cual, como corolario evidente, nos proporciona la infinitud de los números primos. Obsérvese que en esta demostración volvemos a emplear el teorema fundamental de la aritmética y la divergencia de la serie armónica. Ciertamente demostramos mucho más que la infinitud de los números primos.

Demostración: Denotaremos p_n el n -ésimo número primo. Sea m un número natural $m \geq 2$. Cada número natural $n \leq m$ es un producto único (salvo reordenaciones triviales) de potencias de números primos p con $p \leq n \leq m$. Por otra parte, para cada número primo p se tiene

$$\sum_{j=0}^{\infty} \frac{1}{p^j} = \frac{1}{1 - \frac{1}{p}} \quad [3]$$

Es claro que se tiene la desigualdad siguiente

$$\sum_{n=1}^m \frac{1}{n} \leq \prod_{p \leq m} \left(\sum_{j=0}^{\infty} \frac{1}{p^j} \right) = \prod_{p \leq m} \left(\frac{1}{1 - \frac{1}{p}} \right) \quad [4]$$

donde el producto está extendido a los números primos $p \leq m$. De la desigualdad anterior y del desarrollo de $\ln(1 - x)$ se deduce que

$$\ln \left(\sum_{n=1}^m \frac{1}{n} \right) \leq - \sum_{p \leq m} \ln \left(1 - \frac{1}{p} \right) = \sum_{p \leq m} \sum_{j=1}^{\infty} \frac{1}{jp^j} = \sum_{p \leq m} \left(\frac{1}{p} + \frac{1}{p^2} \sum_{j=2}^{\infty} \frac{1}{jp^{j-2}} \right) \leq$$

$$\begin{aligned} &\leq \sum_{p \leq m} \frac{1}{p} + \sum_{p \leq m} \left(\frac{1}{p^2} \sum_{j=2}^{\infty} \frac{1}{p^{j-2}} \right) = \sum_{p \leq m} \frac{1}{p} + \sum_{p \leq m} \left(\frac{1}{p^2} \cdot \frac{1}{1 - \frac{1}{p}} \right) = \\ &= \sum_{p \leq m} \frac{1}{p} + \sum_{p \leq m} \frac{1}{p(p-1)} \leq \sum_{p \leq m} \frac{1}{p} + \sum_{n=2}^m \frac{1}{n(n-1)} \leq 1 + \sum_{p \leq m} \frac{1}{p} \end{aligned} \quad [5]$$

ya que $\sum_{n=2}^m \frac{1}{n(n-1)} \leq \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = \sum_{n=2}^{\infty} \left(\frac{1}{n-1} - \frac{1}{n} \right) = 1$ puesto que esta última serie es una serie telescópica. Ahora bien, como m es arbitrario, a partir de la divergencia de la serie armónica, se deduce entonces que

$$\lim_{m \rightarrow \infty} \sum_{p \leq m} \frac{1}{p} = +\infty^\dagger \quad [6]$$

Observemos también, a partir de este breve análisis, que el crecimiento de la serie de los inversos de los números primos hacia infinito es extremadamente lento, pero existen otras series de crecimiento todavía más lento. ‡

8ª Demostración (Erdős): La siguiente demostración fue dada por el genial y muy prolífico matemático húngaro P. Erdős en el siglo XX. Supongamos que $2, 3, 5, \dots, p_j$ son los primeros j números primos y sea $N(x)$ el número de naturales menores o iguales que x que no son divisibles por ningún primo $p > p_j$.

Podemos expresar cualquier n en la forma $n = n_1^2 \cdot m$ donde m es un número natural libre de cuadrados y entonces no divisible por el cuadrado de ningún número primo. Entonces $m = 2^{b_1} \cdot 3^{b_2} \cdot \dots \cdot p_j^{b_j}$ donde b_j es 0 ó 1. Por otra parte, existen 2^j posibles cambios para los exponentes y por tanto, no más de 2^j diferentes valores de m .

† Obtener el carácter asintótico de $\sum_{n=1}^n \frac{1}{p_n}$ supone otra serie de estimaciones más complejas que también Euler obtuvo, pero no con el debido rigor. En realidad, refinando el argumento anterior, se puede obtener

la expresión $\sum_{p \leq n} \frac{1}{p} = \ln \ln n + B + O\left(\frac{1}{\ln n}\right)$ donde B es una constante caracterizada por la expresión

$$B = \gamma + \sum_p \left[\ln\left(1 - \frac{1}{p}\right) + \frac{1}{p} \right] \approx 0.26149\dots \quad \text{donde } \gamma \text{ es la famosa constante de Euler.}$$

‡ Piénsese en la llamada escala logarítmica de series, todas ellas divergentes, con ritmo de divergencia cada vez más lento: $\sum_{n=1}^N \frac{1}{n}$, $\sum_{n=1}^N \frac{1}{n \ln n}$, $\sum_{n=1}^N \frac{1}{n \ln n \ln n}$, $\sum_{n=1}^N \frac{1}{n \ln n \ln n \ln n}$, ... respectivamente asintóticas a $\ln n$, $\ln \ln n$, $\ln \ln \ln n$, $\ln \ln \ln \ln n$, ...

Además $n_1 \leq \sqrt{n} \leq \sqrt{x}$ y entonces no existen más de \sqrt{x} diferentes valores de n_1 teniéndose que $N(x) \leq \sqrt{x} \cdot 2^j$.

Ahora, si el número de primos fuese finito, sean estos los números $2, 3, 5, \dots, p_j$. En este caso $N(x) = x$ para todos los valores de x y entonces $x \leq 2^j \cdot \sqrt{x}$, que es lo mismo que $x \leq 2^{2j}$, lo que es absurdo para $x \geq 2^{2j} + 1$.[†]

9ª Demostración (Goldbach): Consideraremos los denominados números de Fermat $F_n = 2^{2^n} + 1$ con $n \geq 0$.[‡] Demostremos por inducción que se verifica la siguiente relación $\prod_{k=0}^{n-1} F_k = F_n - 2$ entre los números de Fermat. Para $n = 1$, tenemos que $F_0 = 3$ y $F_1 - 2 = 3$. Aplicando la hipótesis inductiva, tenemos que

$$\prod_{k=0}^n F_k = \left(\prod_{k=0}^{n-1} F_k \right) \cdot F_n = (F_n - 2) \cdot F_n = (2^{2^n} - 1) \cdot (2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2 \quad [7]$$

Por tanto, de la relación: $\prod_{k=0}^{n-1} F_k = F_n - 2$, podemos observar que dos cualesquiera números de Fermat son primos entre sí, y se deduce la existencia de infinitos números primos.

10ª Demostración (Schorn): Para la demostración observemos que si $1 \leq i < j \leq n$, entonces $m.c.d.[(n!)i + 1, (n!)j + 1] = 1$. De hecho, escribiendo $j = i + d$, entonces $1 \leq d < n$ y $m.c.d.[(n!)i + 1, (n!)j + 1] = m.c.d.[(n!)i + 1, (n!)d] = 1$, porque todo primo p dividiendo $(n!)d$ es a lo sumo igual a n . Ahora, si el número de primos fuese m , tomemos $n = m + 1$. Lo anterior implica que los $m + 1$ enteros $(m + 1)!i + 1$ con $1 \leq i \leq m + 1$ son primos entre sí, dos a dos, así que existen como mínimo $m + 1$ distintos primos en contra de la hipótesis.

[†] Este mismo razonamiento de Erdős se puede emplear para demostrar de forma indirecta la divergencia de los inversos de los números primos. Véase la clásica "Introduction to the Theory of Numbers", de Hardy and Wright, fifth edition, Clarendon Press, Oxford, pag 17.

[‡] Entre los muchos resultados de Fermat relativos a la teoría de números primos, surge uno especialmente relevante relacionado con una inducción *precipitada*. Creía haber determinado una solución al viejo problema de construir una fórmula que diese sólo números primos para todos los valores de la variable. No es difícil demostrar que $2^m + 1$ no puede ser primo a no ser que m sea una potencia de 2 y engañado esta vez por su intuición, pensaba que los números de la forma $F_n = 2^{2^n} + 1$ (números de Fermat F_n) eran primos para todo valor de n . En 1732 Euler tras un intenso cálculo y probando con unos determinados candidatos a divisores, demostró que $F_5 = 2^{2^5} + 1 = 4.294.967.297$ es divisible por 641 con lo que la conjetura de Fermat resultaba errónea. Actualmente esta conjetura está tan *devaluada* que los matemáticos se inclinan más bien a la opinión contraria, es decir, la de que no hay ningún número primo de Fermat a partir de F_4 . Se conoce actualmente que para todos los n tales que $5 \leq n \leq 22$ y otros valores de n mucho mayores los números de Fermat F_n son todos compuestos. Sin embargo, no se sabe actualmente si existe un número finito o infinito de números primos de Fermat.

11ª Demostración (Euler): Asumiremos (para abreviar la exposición) como lema previo en esta demostración la proposición siguiente debida a Euler: “Sean a y n números naturales tales que $m.c.d.(a,n)=1$, entonces en el lenguaje de las congruencias se tiene que $a^{\varphi(n)} \equiv 1 \pmod{n}$, donde $\varphi(n)$ es la famosa función indicador de Euler que representa el número de los números $1,2,\dots,n$ que son primos con n . Aquí tomamos por definición $\varphi(1) = 1$ ”.[†]

Sean a y n números naturales tales que $m.c.d.(a,n) = 1$. El menor número natural d tal que $a^d \equiv 1 \pmod{n}$ se denomina el orden de $a \pmod{n}$. Por el anterior teorema el orden d existe y además divide a $\varphi(n)$. En efecto, d divide a todo entero k tal que $a^k \equiv 1 \pmod{n}$ porque por el algoritmo de la división $k = dq + r$ con $0 \leq r < d$ y de aquí $a^r \equiv 1 \pmod{n}$ y por consiguiente, puesto que d es mínimo, se deduce que $r = 0$.

Para demostrar la infinitud de los números primos consideremos los números de la forma $2^p - 1$ con p número primo (denominados números de Mersenne) y demostremos que cualesquiera de sus factores primos q han de ser de la forma $2kp + 1$ que obviamente son mayores que p . En efecto, sea q cualquier factor primo de $2^p - 1$. Entonces, en virtud del teorema de Euler, se tiene que $2^{q-1} \equiv 1 \pmod{q}$ y como el orden de $2 \pmod{q}$ es claramente p se tiene que p divide a $q-1$ y de aquí se concluye la demostración.

12ª Demostración: Sean p_1, p_2, \dots, p_j números primos consecutivos. Consideremos ahora los números de Mersenne asociados $2^{p_1} - 1, 2^{p_2} - 1, \dots, 2^{p_j} - 1$. Es fácil ver, a partir del argumento utilizado en la demostración anterior, que estos números son primos entre sí, dos a dos, y en consecuencia, existen infinitos números primos.

13ª Demostración (Vinogradov): En esta *exótica* demostración se asume que se ha demostrado previamente la irracionalidad de un valor particular de la función zeta de Riemann, en particular de $\zeta(2)$ (Euler demostró que $\zeta(2) = \frac{\pi^2}{6}$) sin recurrir, obviamente, a la infinitud de los números primos, salvando así un argumento circular.

Supongamos que el número de primos sea finito. Sean entonces los números primos los elementos del conjunto $\{p_1, p_2, p_3, \dots, p_k\}$. Por las relaciones ya comentadas entre la función zeta y los números primos tenemos que

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \left(1 + \frac{1}{p_1^2} + \frac{1}{p_1^4} + \dots\right) \cdots \left(1 + \frac{1}{p_k^2} + \frac{1}{p_k^4} + \dots\right) \quad [8]$$

lo que es absurdo, ya que el primer miembro de la igualdad es un número irracional y el segundo es racional.

[†] Se puede deducir la siguiente expresión para la función indicador $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$ donde el producto se refiere a todos los primos de la descomposición de n .

14ª Demostración (basada en la sucesión de Fibonacci): En esta demostración utilizaremos la conocida sucesión de Fibonacci definida en la forma $F_n = F_{n-1} + F_{n-2}$ con $F_1 = F_2 = 1$. Para demostrar la infinitud de los números primos, necesitamos obtener dos relaciones importantes entre los números de Fibonacci. Inicialmente demostraremos, por inducción, que se cumple la siguiente relación:

Teorema: “Siendo F_n el n -ésimo número de Fibonacci definido por $F_1 = F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$ entonces se cumple que $F_{n+m} = F_n F_{m+1} + F_{n-1} F_m$, $\forall m, n \geq 1$ ”.

Demostración: La demostración la efectuaremos por inducción sobre m . Para $m = 1$, tenemos la relación $F_{n+1} = F_n \cdot 1 + F_{n-1} \cdot 1 = F_n F_2 + F_{n-1} F_1$. Así que la expresión es cierta $\forall n$ con $m = 1$. Asumiremos que la expresión es cierta $\forall n$ con $m = M$ y demostraremos que la expresión también es cierta con $m = M + 1$.

$$\begin{aligned} F_{n+M+1} &= F_{n+M} + F_{(n-1)+M} = F_n F_{M+1} + F_{n-1} F_M + F_{n-1} F_{M+1} + F_{n-2} F_M = \\ &= F_n F_{M+1} + (F_{n-1} + F_{n-2}) F_M + F_{n-1} F_{M+1} = F_n (F_M + F_{M+1}) + F_{n-1} F_{M+1} = \\ &= F_n F_{M+2} + F_{n-1} F_{M+1} \end{aligned} \quad [9]$$

y por tanto la proposición dada es cierta $\forall n$ con $m = M + 1$ y el teorema queda demostrado. Por otra parte, surge ahora fácilmente un importante corolario asociado a este resultado, que también se demuestra fácilmente por inducción.

Corolario1: “ F_n divide a F_{nm} $\forall m, n \geq 1$ ”.

Demostración: La demostración la efectuaremos por inducción sobre m . Para $m = 1$, F_n ciertamente es divisible por sí mismo. Supongamos que la proposición es cierta $\forall n$ con $m = M$. Entonces para $m = M + 1$, tenemos utilizando la proposición anterior

$$F_{n(M+1)} = F_{nM+n} = F_{nM} F_{n+1} + F_{nM-1} F_n \quad [10]$$

Por la hipótesis de inducción F_n divide a F_{nM} y entonces la última expresión es divisible por F_n . Esto implica que F_n divide a $F_{n(M+1)}$ así que el resultado es cierto para $m = M + 1$ y el corolario está demostrado.

El segundo importante resultado sobre la sucesión de Fibonacci que nos interesa aquí es el siguiente:

$$m.c.d.(F_a, F_b) = F_{m.c.d.(a,b)} \quad [11]$$

Para demostrarlo es útil recordar las etapas del algoritmo de Euclides junto con el corolario anterior. Supongamos $a \geq b > 0$. Recordemos que sus etapas son las siguientes:

$$\begin{aligned} a &= bq_1 + r_1 & 0 \leq r_1 < b \\ b &= q_2 r_1 + r_2 & 0 \leq r_2 < r_1 \end{aligned}$$

$$\begin{aligned}
r_1 &= q_3 r_2 + r_3 & 0 \leq r_3 < r_2 \\
\text{.....} & \\
r_{n-2} &= q_n r_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n. & & [12]
\end{aligned}$$

Denotemos ahora por d al $m.c.d.(a, b)$. Como d/a (d divide a) y d/b (d divide b) se deduce que d/r_1 (d divide r_1). Continuando las etapas del algoritmo, se obtiene que d/r_s para cada s . Así tenemos que d/r_n y por tanto $d \leq r_n$. Por otra parte, recorriendo las etapas del algoritmo en sentido inverso tenemos la secuencia $r_n/r_{n-1}, \dots, r_n/b, r_n/a$ luego r_n/d y por tanto $d \geq r_n$. Se deduce pues, una doble desigualdad, que implica $d = r_n$. Tenemos pues, las relaciones siguientes:

$$m.c.d.(F_a, F_b) = m.c.d.(F_a, F_{aq_1+r_1}) = m.c.d.(F_a, F_{aq_1} \cdot F_{r_1+1} + F_{aq_1-1} \cdot F_{r_1}) \quad [13]$$

y como F_a divide a $F_{aq_1} \cdot F_{r_1+1}$ por el corolario anterior, entonces se tiene

$$m.c.d.(F_a, F_b) = m.c.d.(F_a, F_{aq_1-1} \cdot F_{r_1}) \quad [14]$$

Además, es claro que dos números de Fibonacci consecutivos son primos entre sí. Por tanto, tenemos que $m.c.d.(F_{aq_1}, F_{aq_1-1}) = 1$ y llegamos a la relación

$$m.c.d.(F_a, F_{aq_1-1} \cdot F_{r_1}) = m.c.d.(F_a, F_{r_1}) = m.c.d.(F_a, F_b) \quad [15]$$

Repitiendo el mismo razonamiento obtenemos

$$m.c.d.(F_{r_1}, F_a) = m.c.d.(F_{r_2}, F_{r_1}) = \dots = m.c.d.(F_{r_n}, F_{r_{n-1}}) \quad [16]$$

y como $r_n/r_{n-1} \Rightarrow F_{r_n}/F_{r_{n-1}}$ (por el corolario anterior) $\Rightarrow m.c.d.(F_{r_n}, F_{r_{n-1}}) = F_{r_n}$. De aquí se deduce la relación buscada

$$m.c.d.(F_a, F_b) = F_{r_n} = F_{m.c.d.(a,b)} \quad [17]$$

De esta última relación deducimos inmediatamente como corolario la existencia de infinitos números primos. Basta observar la secuencia de números de Fibonacci $\{F_{p_1}, F_{p_2}, \dots, F_{p_n}\}$ que está formada por números primos entre sí, dos a dos.[†]

[†] Obsérvese que se cumple la relación más fuerte $m.c.d.(n, m) = 1 \Rightarrow m.c.d.(F_n, F_m) = 1$.

COMENTARIOS

Hemos podido observar una gran diversidad en las demostraciones que se han presentado sobre la infinitud de los números primos. Todas ellas se han escogido por su naturaleza de demostraciones elementales. Entre ellas hay demostraciones relativamente breves en las que sobresale su carácter puramente verificativo, como las demostraciones de Euclides, Hermite, Saidak, Odoni y Schorn. Podemos observar que estas demostraciones se limitan a verificar la infinitud de los números primos pero no aportan esencialmente mucho más a la comprensión de la distribución de los mismos. Algunas de ellas se dan en su versión de demostración indirecta, aunque como hemos notado, las cuatro se pueden reformular trivialmente hasta convertirlas en demostraciones directas.

Las demostraciones de Euclides y Hermite son muy similares. Las dos son demostraciones elementales que no recurren a otros resultados previos como a la unicidad de la descomposición de un número natural en factores primos o a otros teoremas *sofisticados*, únicamente se basan en que el menor divisor de un número natural es un número primo. La demostración de Saidak es incluso conceptualmente más simple que las dos citadas. En su argumentación, Euclides se limita a demostrar que si $\{p_1, p_2, p_3, \dots, p_n\}$ es un conjunto de números primos consecutivos, entonces en el intervalo $(p_n, p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n + 1]$ existe siempre un número primo. De hecho, se pueden hacer ligeras modificaciones del argumento de Euclides para obtener más precisión. En realidad, si $r \geq 2$ entonces el intervalo $(p_r, \prod_1^r p_r + 1]$ contiene dos números primos ya que un mismo número primo q no puede dividir simultáneamente a $\prod_1^r p_r + 1$ y a $\prod_1^r p_r - 1$ puesto que entonces tendría que dividir a su diferencia 2.[†]

La demostración de Euclides es muy ingeniosa y aplicable a la demostración de la infinitud de los números primos de otras clases como los números primos de la forma $4n - 1$, $6n + 1$, $6n + 5$ y otras. A modo de ejemplo, para demostrar que existen infinitos números primos de la forma $4n - 1$ podemos razonar por reducción al absurdo y suponer que existe un número finito de tales primos siendo p el mayor de ellos. Ahora

[†] Si $r \geq 3$, entonces el intervalo $(p_r, \prod_2^r p_i)$ contiene como mínimo $\lfloor \log_2(2r) \rfloor + 1$ números primos. Observemos que para $r = 3$ o $r = 4$ el resultado puede obtenerse directamente. Supongamos que $r \geq 5$. Observemos que $p_5 = 11 > 2 \cdot 5$ y que sólo son naturales consecutivos los primos 2 y 3, por tanto, $2r < p_r$. Entonces $\forall j/1 \leq j \leq \lfloor \log_2(2r) \rfloor + 1$, los números $\prod_2^r p_i - 2^j$ pertenecen al intervalo $(p_r, \prod_2^r p_i)$ y son primos entre sí dos a dos. Claramente $2^j \leq 4r < 2p_r$ y de aquí se sigue que $\prod_2^r p_i - 2^j > 3p_r - 2^j > p_r$. Además $\prod_2^r p_i - 2^j$ no es divisible por p_i para $1 \leq i \leq r$ así que existe un primo $q_j > p_r$ con $q_j \mid \prod_2^r p_i - 2^j$. Si $j \neq k$, entonces $q_j \neq q_k$ para j ya que si $q_j \mid \prod_2^r p_i - 2^k \Rightarrow q_j \mid (2^j - 2^k)$ lo que absurdo, ya que 2 y $2^{j-k} - 1$ son estrictamente menores que p_r , que a su vez es menor que q_j y por tanto este último no puede dividir a $2^k(2^{j-k} - 1)$.

consideremos el número $N = 2^2 \cdot 3 \cdot 5 \cdots p - 1$. Como N es de la forma $4k - 1$, no puede ser primo ya que p era el mayor de todos. Es claro que ningún número primo menor o igual que p divide N y por tanto sus factores primos son mayores que p . Por otra parte, no todos los factores primos de N pueden ser de la forma $4k + 1$, puesto que en ese caso, su producto claramente también lo sería y evidentemente N , no lo es. Por lo tanto, algún factor primo de N ha de ser de la forma $4k - 1$, lo que es absurdo. Esta contradicción demuestra el teorema. De nuevo, debemos indicar que se puede trivialmente reformular esta demostración para convertirla en una demostración de carácter directo.[‡]

Desgraciadamente la demostración de la infinitud de los números primos de la forma $4n + 1$ no se puede efectuar mediante una extensión sencilla del argumento de Euclides. Existen varias formas elementales alternativas de demostración para este caso. A continuación expondremos brevemente una de ellas.

Para demostrar la infinitud de los números primos de la forma $4n + 1$, supondremos dado un $N > 1$, y en el lenguaje de las congruencias, siempre se podrá encontrar un número primo de la forma $p \equiv 1 \pmod{4}$ y mayor que N . Para ello consideremos el número $M = (N!)^2 + 1$ y sea p el factor primo menor de M que necesariamente debe ser mayor que N , puesto que claramente ninguno de los números $\{2, 3, 4, \dots, N\}$ puede ser divisor de M . Entonces tenemos que $(N!)^2 \equiv -1 \pmod{p}$ lo que nos lleva a la relación $(N!)^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$ que junto con el teorema de Euler (ya comentado anteriormente en este artículo) produce $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ y esto implica que $p \equiv 1 \pmod{4}$. Esto concluye la demostración.

En realidad, existen otros casos más generales de progresiones aritméticas para las que podemos encontrar demostraciones relativamente sencillas “ad hoc”.

Por otra parte, las demostraciones de Odoni y Schorn son también elementales y relativamente breves, pero su estructura es radicalmente diferente a las demostraciones de Euclides y Hermite. Las demostraciones de Odoni y Schorn se basan en construir secuencias infinitas de números naturales que sean primos dos a dos, lo que es bastante más que demostrar la infinitud de los números primos. Observemos que tampoco se basan en otros teoremas previos.

La demostración de Goldbach, también se basa en generar una secuencia infinita de números naturales primos, dos a dos, tal como la secuencia que forman los números de Fermat. En esta demostración se explicita ya la propia secuencia y no aparece de forma recursiva como en la demostración de Odoni.

[‡] P. G. Dirichlet demostró en 1834 el profundo teorema que establece que si $m.c.d.(a, b) = 1$ entonces la progresión aritmética $\{an + b\}$ contiene infinitos números primos. La demostración aportada por Dirichlet exigía importantes herramientas del análisis matemático. La demostración muestra que la serie

$$\sum_{p \equiv a \pmod{m}} \frac{1}{p} \text{ es divergente.}$$

Incluso la demostración basada en la sucesión de Fibonacci se basa en generar también otra secuencia infinita de números naturales primos entre sí, tal como la secuencia de los números de Fibonacci que tengan como subíndices dos números naturales que sean primos.

REFERENCIAS BIBLIOGRÁFICAS

- [1] Aparicio, E. (1993). *Teoría de los números*. Servicio editorial. Universidad del País Vasco.
- [2] Baker, A. (1984). *Breve introducción a la teoría de los números*. Alianza Universidad. Versión española de Alejandro Salinero Galán.
- [3] Boyer, C. B. (1992). *Historia de la Matemática*. Alianza Universidad Textos. Alianza editorial.
- [4] Cilleruelo, J. & Córdoba, A. (1992). *La teoría de los números*. Biblioteca Mondadori.
- [5] Collete, J. P. (1985). *Historia de las Matemáticas*. Siglo XXI de España ediciones. S.A.
- [6] Davis, P.J. & Hersh, R. (1983). *Experiencia Matemática*. Madrid. Labor.
- [7] Guzman de, M. (2003). *Cómo hablar, demostrar y resolver en Matemáticas*. Iniciación al método matemático. Base Universitaria. Anaya.
- [8] Hardy, G. H. & Wright, E. M. (1978). *An Introduction to the Theory of Numbers*. Fifth edition. Clarendon Press. Oxford.
- [9] Ibañes, M. & Ortega, T. (1997). *La demostración matemática. Clasificación y ejemplos en el marco de la Educación Secundaria*. Educación Matemática, 9(2), 65-104.
- [10] Kline, M. (1992). *El pensamiento matemático de la Antigüedad a nuestros días*. Tres volúmenes. Alianza editorial.
- [11] Lakatos, I. (1978). *Pruebas y refutaciones*. Madrid. Alianza.
- [12] López, F. & Tena, J. (1990). *Introducción a la teoría de los números primos. (Aspectos algebraicos y analíticos)*. Instituto de ciencias de la educación. Universidad de Valladolid.
- [13] Sáenz, C. (2001). *Sobre conjeturas y demostraciones en la enseñanza de las Matemáticas*. En M. F. Moreno et al. (eds). Investigación en educación matemática. Universidad de Almería.

[14] Vicario, V. & Carrillo, J. (2005). *Concepciones del profesor de secundaria sobre la demostración matemática. El caso de la irracionalidad de $\sqrt{2}$* . Simposio de la SEIEM en Córdoba, 2005. pp. 145-152.

[15] Villiers de, M. (1993). *El papel y la función de la demostración en Matemáticas*. Revista Epsilon 26, 15-30. Artículo aparecido en Pythagoras, 24 Nov, 1990. Traducido y publicado con la correspondiente autorización.

[16] Vinogradov, I. (1977). *Fundamentos de la teoría de números*. Editorial MIR. Moscú. Traducido del ruso.

---oooOooo---

Revista Escolar de la Olimpiada Iberoamericana de Matemática

<http://www.campus-oei.org/oim/revistaoim/>

Edita:

