Dos demostraciones sobre la infinitud de los números primos

Teorema.- Existen infinitos números primos.

1.- Una de ellas es consecuencia directa de la relación establecida por Euler entre la función zeta de Riemman y el producto de Euler:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - p^{-s}\right)^{-1}$$

Es un hecho conocido que la serie armónica $\sum_{n=1}^{\infty} \frac{1}{n}$ es divergente. Se podría escribir $\sum_{n=1}^{\infty} \frac{1}{n} = \infty$, para expresar dicha divergencia. Por tanto, haciendo $s \to 1$, tendríamos que:

$$\lim_{s \to 1} \zeta(s) = \zeta(1) = \sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p} \left(1 - p^{-1}\right)^{-1}$$

donde $\prod_p$ indica un producto sobre los número primos, de la forma:

$$\prod_{p} \left(1 - p^{-1}\right)^{-1} = \left(1 - p_1^{-1}\right)^{-1} \cdot \left(1 - p_2^{-1}\right)^{-1} \cdot \ldots \cdot \left(1 - p_n^{-1}\right)^{-1} \cdot \ldots$$

Pues bien, si existiese un número finito de números primos, pongamos $\{p_1, p_2, \ldots, p_k\}$, entonces:

$$\prod_{p} \left(1 - p^{-1}\right)^{-1} = \left(1 - p_1^{-1}\right)^{-1} \cdot \left(1 - p_2^{-1}\right)^{-1} \cdot \ldots \cdot \left(1 - p_k^{-1}\right)^{-1} = m$$

donde m sería un número real (finito, pues). De este modo, por un lado tendríamos que:

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

y por otro

$$\prod_p \left(1-p^{-1}\right)^{-1} = \left(1-p_1^{-1}\right)^{-1} \cdot \left(1-p_2^{-1}\right)^{-1} \ldots \left(1-p_k^{-1}\right)^{-1} = m < \infty$$

lo que es absurdo, pues estaría en contradicción con la igualdad establecida en el producto de Euler:

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

que es válido para $Re(s) > 1$, y si $s \to 1$ tiene perfectamente sentido el argumento empleado (pues no se desmentiría que $Re(s) > 1$).

De este modo debe haber infinitos números primos.

Esta es una de las demostraciones más elegantes y sencillas, pero requiere del empleo de conceptos de matemáticas avanzadas como es el producto de Euler o la función zeta de Riemann

2.- Esta segunda forma también se hace por reducción al absurdo y requiere de un mínimo conocimiento de teoría de números. En ella se tiene en cuenta el teorema fundamental de la aritmética, que dice algo así: *Todo número mayor que 1 es o bien un número primo o bien un producto de números primos.* Para proceder por reducción al absurdo es necesario suponer, pues, que hay un número finito de números primos: $p_1, p_2, \ldots, p_k$, con $k \geq 2$. Bajo estas hipótesis consideremos el producto de todos ellos:

$$N = p_1 \cdot p_2 \cdot \ldots \cdot p_k$$

cuyo resultado produce un número N que no es un número primo (por ser producto de primos). Por tanto, se puede poner de la forma $N = m \cdot n$, donde m y n se podrían expresar como producto de primos, a elección, del conjunto $\{p_1, p_2, \ldots, p_k\}$. Sea ahora un primo $p \in \{p_1, p_2, \ldots, p_k\}$. Pues bien, como $N = m \cdot n$ o bien $p|m$ ($p|m$ significa que p divide

a m, por ejemplo, 3 divide a 6) o bien $p|n$. Supongamos, por ejemplo, que $p|m$ (se podría suponer que $p|n$, pero es exactamente el mismo razonamiento; es decir, da igual suponer que $p|n$ o $p|m$, indistintamente). No obstante, si $p|m$ entonces p no divide a n (y si $p|n$ entonces p no dividiría a m). Así que... Notar además que, si $p|m$ y $p|n$, entonces también p dividiría a $m+n$ (si $p=2$ y p divide a 4 y p divide 6, entonces $p=2$ también divide 10=6+4; se puede probar con $p=3$ y razonar con 9 y 12, por ejemplo; así sucesivamente para convencerse). Es decir, si $p|m$ y $p|n$ (algo en nuestro caso no posible), entonces $p|(m+n)$. Por tanto, si ahora nos ceñimos a nuestro caso, por lo razonado se tiene que si $p|m$, entonces p no divide a n y, por tanto, p no divide a $m+n$ (porque si $p|m$ y $p|n$, acabamos de ver que $p|(m+n)$; así con que no divida a uno, m o n, es suficiente para concluir que p no divide a $m+n$, porque si lo hiciese todo sería mentira y nada sería lo que parece, al menos en matemáticas). No obstante, $m+n \in \mathbb{N}$ (no primo), y por el teorema fundamental de la aritmética $m+n$ admite una factorización en números primos. Como el conjunto de números primos $\{p_1, p_2, \ldots, p_k\}$ es finito y $p \in \{p_1, p_2, \ldots, p_k\}$, una de las dos siguientes no puede ser: o bien el teorema fundamental de la aritmética, y sería mentira que todo número es primo o bien un producto de primos; o bien la hipótesis inicial de que el conjunto $\{p_1, p_2, \ldots, p_k\}$ es finito. Supongo que con esto se concluye la demostración.

En consecuencia, debe haber infinitos números primos.