# Los números primos son infinitos

Felipe Riquelme

Una de las principales razones del porqué me convertí en matemático es debido al uso extremo del ingenio. ¿Cómo resolver un problema que está ligado a la existencia de un número infinito de elementos?. ¿Cómo resolver un problema que nos afirme que existen infinitos elementos que satisfacen una propiedad dada?. En cualquier caso, uno estaría tentado a intentarlo considerando un elemento a la vez. Una vez escogido podemos verificar si este satisface la propiedad buscada. Si la satisface, entonces lo agregamos a la lista de elementos que satisface la propiedad. Si no la satisface, lo desechamos. Pero este tipo de algoritmo tiene un problema. Si verificamos uno por uno, siempre nos quedarán infinitos elementos por verificar, ¡NUNCA TERMINAREMOS!. Inclusive si un computador nos hiciera todo el trabajo, por más rápido que este procese la información, siempre tendrá infinitos elementos a verificar.

El problema de infinitud de números primos me maravilló desde el día que pude entenderlo a cabalidad, y es por cierto a modo personal de ver, el ejemplo clave en que el ingenio de las matemáticas se hace presente. El problema nos habla de la existencia de infinitos elementos, pero el argumento utilizado para probarla es hermoso pues no cae en la trampa de verificación. Evita ese problema. Se las ingenia para sacar adelante un resultado impresionante.

**Definición 1.** *Un número entero positivo se dice número primo si los únicos factores que lo definen son* 1 *y sí mismo.*

Sin mucho trabajo podemos verificar que $2, 3$ y $5$ son números primos. Pero $4, 6$ y $8$ no lo son pues se escriben respectivamente como $2 \cdot 2$, $2 \cdot 3$ y $2 \cdot 2 \cdot 2$. En la actualidad, el número primo más grande conocido tiene una cantidad impresionante de digitos; un total de 17.425.170. Pero gracias a Euclides, en una demostración que consta de más de dos mil años de antigüedad, sabemos que podemos encontrar números primos más grandes aún, y que encontrarlos de manera explícita dependerá esencialmente de qué tan grande sea el procesador de un computador.

**Teorema 2.** *[Euclides, $\sim$ 300 a.c.] El conjunto de números primos es infinito.*

Para entender la demostración debemos hablar primero de la lógica matemática. Más precisamente del argumento de *reducción al absurdo*. Este argumento consiste en suponer que el resultado es falso. En el caso del Teorema de Euclides esto significaría suponer que solo existen finitos números primos. Luego, en una cadena de argumentos lógicos, intentar llegar a alguna contradicción lógica. Encontrar en cierta medida una falla en el mundo de las matemáticas. En otras palabras, estaríamos demostrando que lo que estamos suponiendo como real, NO PUEDE SUCEDER.

**Demostración:** Sea $P$ el conjunto de números primos. Supongamos que $P$ solo contiene una cantidad finita de elementos. Como son finitos, los podemos nombrar. A saber, $P = \{p_1, p_2, ..., p_n\}$. En base a este conjunto construiremos un nuevo número que llamaremos $N$. Sea $N$ entonces el número entero definido como el producto de todos los elementos de $P$ más 1, es decir,

$$N = (p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_{n-1} \cdot p_n) + 1.$$

Como ya dijimos, $N$ es un número entero. La clave en la demostración recae en la pregunta siguiente...

¿Es $N$ un número primo?.

Todo número entero es o no es un número primo. Si $N$ es un número primo entonces este debiera estar en el conjunto $P$, pues $P$ por definición consiste de *todo* número primo. Pero por construcción de $N$, este es estrictamente más grande que cualquier número en el conjunto $P$, por lo que por definición $N$ no está en $P$. De esto concluímos que $N$ no es un número primo. Como $N$ no es un número primo este se descompone como el producto de dos números enteros distintos de 1 y $N$. Estos factores o son números primos o no lo son. Si no lo son entonces estos a su vez se descomponen como producto de factores distintos de 1 y de sí mismos. Eventualmente, en un número finito de pasos, obtendremos algún número primo $p$ que divida a $N$ (de hecho todo número entero se descompone como producto de números primos, resultado conocido como *Teorema Fundamental de la Aritmética*). El número primo $p$ debe estar en $P$. Entonces $p = p_i$ para algún $i$ comprendido entre 1 y $n$. Lamentablemente, al dividir $N$ por $p_i$ el resto es siempre 1 por definición de $N$. Esto significa que $p$ divide a $N$ y a su vez no lo divide. Una contradicción lógica.

Hemos demostrado entonces por reducción al absurdo que el conjunto $P$ de números primos debe ser infinito. De no serlo, siempre podemos construir un número primo que no esté en $P$.

■

Daré un ejemplo concreto del funcionamiento de esta demostración. Sea $P = \{2, 3, 5\}$ el conjunto de los primeros 3 números primos. En este caso el número $N$ que definimos en la demostración sería $N = 2 \cdot 3 \cdot 5 + 1 = 31$. Si somos pacientes y verificamos número por número, nos damos cuenta que 31 es un número primo. Así hemos construído un número primo que no está en $P$. Si ahora $P = \{2, 3, 5, 7\}$, entonces $N = 211$ y si llegamos a ser más pacientes aún, podemos verificar que $N$ es también un número primo. Finalmente, si $P = \{2, 3, 5, 7, 11, 13\}$ entonces $N = 30031$. En este caso $N$ no es un número primo. En efecto, se escribe como $N = 59 \cdot 509$, siendo ambos factores números primos. Ninguno de ellos se encuentra en $P$.

Para finalizar, como los matemáticos somos obsesivos creandonos problemas de la nada, ya que conocemos que existen infinitos números primos, nos gustaría saber cómo estos se distribuyen en los enteros. En cierto modo nos preguntamos cuántos números primos hay proporcionalmente hablando en el conjunto de enteros positivos. Uno podría intentar ser increíblemente explícito en este sentido, y sacarle el jugo al problema. Y sinceramente, a partir de este tipo de obsesividades es que se ha desarrollado exponencialmente la teoría de números. Uno de los resultados más conocidos en este aspecto corresponde al *Teorema de los Números Primos*, conjeturado por Gauss y demostrado de manera independiente por Hadamard y Poussin.

**Teorema 3.** *[Hadamard/Poussin, 1896] Sea $x$ un real positivo. Denotamos por $\pi(x)$ a todos los números primos entre 1 y $x$. Entonces*

$$\pi(x) \sim \frac{x}{\ln(x)}.$$

El Teorema de los Números Primos nos dice que para valores muy grandes de $x$, la función contadora de primos $\pi(x)$ se comporta como la función $\frac{x}{\ln(x)}$. Este resultado implica la infinitud de los numeros primos, pues si $x$ tiende a infinito entonces $x/\ln(x)$ tiende a infinito.