

¿Existe un número primo mayor que todos los demás?

Juan Segurola · Todos los derechos reservados

QUE · Artículo 043 · Preguntas sencillas, respuestas profundas · Versión 0.1 ES

Ningún número primo es el último. Esta respuesta no depende de hasta dónde haya buscado un ordenador, y descubrir otro primo muy grande no reforzaría el argumento subyacente. La afirmación se refiere a toda lista finita posible de primos, incluidas aquellas cuyos elementos nadie ha escrito.

La distinción está entre ampliar una colección y demostrar que no puede estar completa. El cálculo puede establecer las propiedades de enteros concretos. Una demostración puede explicar por qué ninguna colección finita los contiene a todos. Los Elementos de Euclides, libro IX, proposición 20, ofrecen un argumento según el cual los números primos superan cualquier multitud finita dada. [1]

1. ¿Qué es un primo?

Aquí, un primo es un entero mayor que uno cuyos únicos divisores positivos son uno y él mismo. Así, dos y tres son primos, mientras que seis no lo es: dos y tres lo dividen. El número uno queda excluido por la definición. La pregunta se refiere a esta clase precisa de enteros positivos, no a lo grande que pueda ser un numeral escrito.

Un hecho preliminar hace funcionar el argumento: todo entero mayor que uno tiene un divisor primo. Para ver por qué, elijamos su divisor más pequeño mayor que uno. Si ese divisor fuera compuesto, tendría a su vez un divisor más pequeño mayor que uno, que también dividiría al número original. Esto contradice la elección del divisor más pequeño. Por tanto, el divisor elegido debe ser primo.

La demostración usa el orden de los enteros positivos y la divisibilidad ordinaria. No requiere que ya sepamos factorizar eficientemente un número enorme. La existencia de un divisor y un método práctico para encontrarlo con rapidez son cuestiones distintas.

2. Tomemos cualquier lista que se proponga como completa

Supongamos que alguien nos da una lista finita de todos los primos, desde p_1 hasta p_n . Multiplicamos todos sus elementos para obtener P y formamos $N = P + 1$. Cada primo de la lista divide exactamente a P . Por tanto, al dividir N por cualquiera de ellos queda resto uno.

En consecuencia, ningún primo de la lista divide a N . Sin embargo, N es mayor que uno y, por el argumento preliminar, tiene un divisor primo. Ese divisor no está en la lista propuesta como completa. La lista no podía estar completa.

Nada del razonamiento dependía de la lista finita con la que empezáramos. Eso es lo que da alcance a la demostración. No comprueba las primeras mil posibilidades y conjetura que el patrón continúa; proporciona una contradicción para cualquier afirmación finita de completitud. La construcción mediante el producto es una presentación moderna habitual del argumento de divisibilidad. [1]

3. El número que construimos no tiene por qué ser primo

Este es el punto donde a menudo falla una explicación por lo demás convincente. La demostración no dice que multiplicar primos consecutivos y sumar uno produzca siempre un primo. Dice que el resultado tiene un divisor primo que no está en la lista inicial.

Para la lista 2, 3 y 5, la construcción da 31, que es primo. Pero al usar 2, 3, 5, 7, 11 y 13 se obtiene 30 031, y $30\,031 = 59 \times 509$. Este ejemplo es compuesto y, aun así, hace exactamente lo que exige la demostración. Ni 59 ni 509 están entre los seis primos iniciales.

Un resultado compuesto no es una comprobación fallida del teorema. Es uno de los dos casos que admite el argumento. Confundir el entero construido con el nuevo divisor primo convierte una demostración válida en una receta inválida. La diferencia es pequeña en palabras y decisiva en lógica.

4. ¿El nuevo primo tiene que ser mayor?

Si la lista inicial contiene realmente todos los primos hasta cierta cota, un divisor primo ausente debe superar esa cota. Si la lista es simplemente una selección arbitraria, el divisor ausente podría ser un primo menor que se omitió. Ambos casos son compatibles con la demostración.

Por tanto, el teorema refuta la existencia de un primo máximo del siguiente modo. Si existiera un primo máximo, todo primo estaría entre los enteros, en número finito, desde dos hasta ese valor. Podríamos enumerarlos y la construcción mostraría que la lista está incompleta. Esto contradice el supuesto.

Un ejercicio útil es distinguir «no está en esta lista» de «es mayor que todos los elementos de esta lista». Solo coinciden cuando la lista tiene la propiedad de completitud adecuada. Tener presente esa condición evita un paso oculto habitual en las presentaciones divulgativas.

5. Lo que aún puede aportar el cálculo

El teorema no proporciona un procedimiento general eficiente para encontrar un primo de un tamaño deseado. Construir P puede requerir un entero enorme, y extraer un factor de $P + 1$ puede ser computacionalmente difícil. Una demostración de existencia sin cota superior y el tiempo de ejecución de un algoritmo son logros diferentes.

Del mismo modo, hablar del mayor primo conocido es hacer una afirmación sobre un cuerpo de conocimiento verificado en un momento concreto. Hablar de un primo máximo sería hacer una afirmación sobre los propios enteros. Actualizar un récord puede cambiar la primera afirmación y no puede cambiar el teorema que descarta la segunda. No hace falta ningún récord numérico para entender la distinción.

No hay incertidumbre científica sobre la conclusión dentro de la aritmética ordinaria de enteros y las definiciones indicadas. Las cautelas pertinentes se refieren al alcance de la demostración, a la validez de cada paso y al error de sustituirla por una tendencia experimental. Otras preguntas sobre cómo se distribuyen los primos o con qué eficiencia pueden encontrarse no se resuelven simplemente mostrando que hay infinitos.

La respuesta es exacta: no existe un primo máximo porque puede demostrarse que cualquier lista finita supuestamente completa omite un divisor primo de un entero construido específicamente. La fuerza del resultado reside en su argumento general, no en el tamaño de algún número que hayamos calculado.

Referencias

[1] Euclid. Elements, libro IX, proposición 20. Edición electrónica y comentarios de David E. Joyce, Clark University. <https://mathcs.clarku.edu/~djoyce/elements/bookIX/propIX20.html>

Lectura relacionada

Artículo 044: ¿Cómo podemos saber que un nudo no se puede deshacer?