EL TEOREMA FUNDAMENTAL DE LA ARITMETICA

¿Porqué no es una afirmación obvia la unicidad de la descomposición en primos de un número natural?

Oscar A. Cámpoli

En cualquier curso de aritmética elemental se hace, muy al comienzo, una demostración larga y complicada de lo que se llama Teorema Fundamental de la Aritmética y que dice que si descomponemos un número natural de dos maneras distintas como producto de números primos, éstas dos descomposiciones solo pueden diferir en el orden de los factores.

En ésta nota quisiera hablar acerca de las razones de la necesidad de la demostración, y de algunos de los motivos de su interés.

Dado un número natural, si es primo está ya expresado como producto de primos (uno solo) y si no es primo se puede expresar como producto de dos números menores a los que se aplican las mismas posibilidades y seguimos descomponiendo hasta obtener un producto de números primos.

Ahora bien, la unicidad de ésta descomposición salvo reordenamientos puede parecer obvia y/o irrelevante. Quisiera mencionar primero una razón por la cual ya a los griegos no les parecía irrelevante. Según algunas referencias, es un teorema que demostró Euclides usando una idea de Tetetus y que fue trascendente en la discusión que llevaron a cabo los griegos de los números irracionales, el hecho de que si p es un número primo entonces $\sqrt{p}$ es un número irracional.

La demostración por el absurdo sería suponer que existen números naturales m y n tales que $\sqrt{p} = m/n$ de donde sigue que $p\ n^2 = m^2$. Está claro que cualquier descomposición en producto de primos del número m^2 produce una cantidad par de factores y a su vez, una descomposición de $p\ n^2$ en producto de primos produce un número impar de factores. Esto es absurdo si estamos seguros de la validez del Teorema Fundamental de la Aritmética antes mencionado.

A continuación quisiera dar algunos ejemplos que pueden convencernos de que la afirmación no es obvia.

Consideremos la siguiente sucesión de números naturales

1, 6, 11, 16, 21, 26, 31, ...

Esta es la sucesión formada sumando 1 a todos los números naturales múltiplos de 5.

Para un tal número, decimos que es *primitivo* si no se puede escribir como producto de dos números menores de la misma sucesión (notar la similitud con la definición de natural primo).

Por ejemplo, 6 es primitivo ya que el único que lo precede es 1. También 11 es primitivo ya que los únicos que lo preceden son 6 y 1 y ninguno de sus productos es 11. Para uso posterior, digamos que cualquier lector puede convencerse rápidamente por inspección de los números que los preceden que 21, 26, y 91 también son primitivos (¡podemos usar el Teorema Fundamental de la Aritmética para abreviar la inspección!).

Probablemente a esta altura convenga convencerse que si multiplicamos dos números cualesquiera en la sucesión, obtenemos otro de la sucesión. En efecto, escribamos que $5r + 1$ y $5s + 1$ son dos de dichos elementos en la sucesión. Al multiplicarlos obtenemos $5(5rs + r + s) + 1$ que está entonces en la sucesión.

Repitiendo ahora el razonamiento anterior, es inmediato mostrar que todo número de la sucesión se puede escribir como producto de números primitivos de la sucesión. En efecto, un número de la sucesión es primitivo o no. Si es primitivo ya estamos y si no lo es, será producto de dos menores en la sucesión, etc. ¿La unicidad es entonces obvia de nuevo como en el caso del Teorema Fundamental de la aritmética?.

A poco andar notamos que la unicidad es falsa ya que por ejemplo

$5 \times 109 + 1 = 546 = 21 \times 26 = 6 \times 91$

Ejercicios

1) Hacer un razonamiento como el de arriba para la sucesión que se obtiene sumando 1 a los múltiplos de 3 y dar un ejemplo de no unicidad en éste caso también.

2) Siguiendo el esquema anterior, definir lo que sería un número impar primitivo. Mostrar a continuación que un número impar primitivo es necesariamente primo.

3) ¿Qué otros números primos o no podemos usar para formar sucesiones adonde podamos encontrar ejemplos de no unicidad? ¿Puede caracterizarlos?

4) ¿Qué otros números podemos usar para sumar a los múltiplos de uno dado para formar sucesiones (¡cerradas por productos!) con ejemplos de no unicidad?

Facultad de Matemática, Astronomía y Física (IMAF),
Universidad Nacional de Córdoba