Los átomos de la matemática

José Ángel Cid

Diario Jaén, 23 de abril de 2009

EL RINCÓN MATEMÁTICO

Los átomos de la matemática

José Ángel Cid Araujo
Departamento de Matemáticas de la Universidad de Jaén

El filósofo griego Demócrito propuso que la materia estaba formada por unidades mínimas e indivisibles llamadas átomos. Hoy en día, el átomo ha sido escindido en componentes más pequeños (electrones, quarks, muones…), pero la idea de Demócrito sigue vigente y se cree que, tanto la materia como la energía, existen en unidades mínimas. En el mundo abstracto de la aritmética el papel de los átomos lo desempeñan los números primos, es decir, aquellos números distintos de 1 que sólo son divisibles por 1 y por sí mismos. Por ejemplo 2, 3, 5, 7, 11… son primos, mientras que 1, 4, 6, 8, 9, 10… no lo son. El Teorema Fundamental de la Aritmética afirma que cualquier número se descompone de forma única como producto de primos, y, por tanto, éstos constituyen los bloques numéricos básicos.

Los números primos parecen captar la atención del ser humano de una forma casi mística. Carl Sagan imagina en su novela "Contacto" (llevada al cine con Jodie Foster como protagonista) una civilización extraterrestre que se comunica con la humanidad mediante señales de radio que representan la secuencia de los números primos. En "El hombre que confundió a su mujer con un sombrero" el neurólogo Oliver Sacks relata el caso de dos gemelos autistas que hallaban un gran placer en comunicarse números primos (¡de hasta 20 cifras!). Los gemelos eran incapaces de realizar incluso el cálculo más sencillo, por lo que se supone que poseían una "sensibilidad" especial que les permitía distinguir directamente los números primos.

Euclides ya probó en "Los elementos" la existencia de una infinitud de números primos. La demostración es tan elegante (según los lectores de "Mathematical Intelligencer" es el tercer teorema matemático más bello) que no me resisto a incluirla: Si disponemos de un conjunto finito de primos *p1, p2… pN*, el número *P=p1 x p2 x … pN +1* no es divisible exactamente por ninguno de ellos (pues el resto de la división es 1) y entonces ha de ser el mismo primo o divisible por un primo distinto de *p1, p2…, pN*. Obtenemos, de esta forma, un nuevo número primo y, como podemos repetir este proceso indefinidamente, el conjunto de los números primos es infinito. Los primos con un gran número de cifras son necesarios actualmente, por ejemplo, para encriptar de forma segura la información que se envía a través de internet.

El filósofo griego Demócrito propuso que la materia estaba formada por unidades mínimas e indivisibles llamadas átomos. Hoy en día el átomo ha sido escindido en componentes más pequeños (electrones, quarks, muones...) pero la idea de Demócrito sigue vigente y se cree que tanto la materia como la energía existen en unidades mínimas. En el mundo abstracto de la aritmética el papel de los átomos lo desempeñan los números primos, es decir, aquellos números distintos de 1 que solo son divisibles por si mismos y por 1. Por ejemplo 2, 3, 5, 7, 11,... son primos mientras que 1, 4, 6, 8, 9, 10... no lo son. El Teorema Fundamental de la Aritmética afirma que cualquier número se descompone de forma única como producto de primos, y por tanto éstos constituyen los bloques numéricos básicos.

Los números primos parecen captar la atención del ser humano de una forma casi mística. Carl Sagan imagina en su novela "Contacto"(llevada al cine con Jodie Foster como protagonista) una civilización extraterrestre que se comunica con la humanidad mediante señales de radio que representan la secuencia de los números primos. En "El hombre que confundió a su mujer con un sombrero"el neurólogo Oliver Sacks relata el caso de dos gemelos autistas que hallaban un gran placer en comunicarse números primos (¡de hasta 20 cifras!). Los gemelos eran incapaces de realizar incluso el cálculo más sencillo, por lo que se supone que poseían una "sensibilidad" especial que les permitía distinguir directamente los números primos.

Euclides ya probó en "Los elementos" la existencia de una infinitud de números primos. La demostración es tan elegante (según los lectores de "Mathematical Intelligencer" es el tercer teorema matemático más bello) que no me resisto a incluirla: si disponemos de un conjunto finito de primos $p_1, p_2, \ldots, p_n$ entonces el número $p = p_1 p_2 \ldots p_n + 1$ no es divisible exactamente por ninguno de ellos (pues el resto de la división es 1) y entonces ha de ser él mismo primo o divisible por un primo distinto de $p_1, p_2, \ldots, p_n$. Obtenemos de esta forma un nuevo número primo y, como podemos repetir este proceso indefinidamente, el conjunto de los números primos es infinito. Los primos con un gran número de cifras son necesarios actualmente, por ejemplo, para encriptar de forma segura la información que se envía a través de internet.

Para saber más:

- C. Sagan, *Contacto*, Planeta, (2001).

- O. Sacks, *El hombre que confundió a su mujer con un sombrero*, Anagrama, 2004.

- D. Wells, *Are These the Most Beautiful?*, The Mathematical Intelligencer 12, no. 3, (1990), 37–41.

- M. Gardner, *Mosaicos de Penrose y escotillas cifradas*, Labor, (1990). En los capítulos 11 y 12 hay una discusión sobre el sistema de clave pública RSA, que se basa en determinadas propiedades de los números primos.