MARZO,
MES DE LAS
MATEMÁTICAS

Números naturales: de contar a encriptar información

Texto **Manuel de León Rodríguez**
Aplicaciones interactivas **José Luís Álvarez García y Javier Cayetano Rodríguez**

“Contar fue la primera actividad matemática desarrollada por el ser humano: los días, las cabezas de ganado, los miembros de la tribu. E inmediatamente surge la necesidad de registrar los datos”.

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN
FECYT FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

Contar nos ha llevado a la invención de los números, uno de nuestros mayores logros. Nuestros números nacen en India, y los árabes los traen a Europa en el siglo X.

El hueso de Ishango
Hace más de 20000 años, unos hombres o mujeres tallaron una serie de muescas en un peroné de un babuino en Ishango, en el lago Eduardo, cerca del nacimiento del Nilo. Esas columnas de muescas representan cantidades que nos han intrigado desde hace más de 50 años tras su descubrimiento. Surge así la necesidad no solo de contar sino también de registrar los resultados de los cómputos.

¿Era este hueso una primitiva regla de cálculo con la que nuestros ancestros medían las estaciones y el paso de los astros?

¿Fue una creación de las mujeres para llevar un calendario lunar relacionado con la menstruación?

El cero: un elemento demoníaco
El cero causa una revolución cuando Fibonacci (Leonardo de Pisa) lo introduce en Europa en el siglo XII, en su *Liber abaci* (Libro del ábaco); Fibonacci lo aprendió de los árabes en sus viajes acompañando a su padre por el norte de África. El nuevo sistema decimal, con el cero incluido, simplificaba de una manera casi mágica los cálculos de los comerciantes, acostumbrados al ábaco, que no precisa del cero. La lucha entre ambos sistemas fue tremenda, y el cero fue acusado de elemento demoníaco.

Los números primos

En realidad, no serían necesarios todos los números naturales, porque todos los podemos construir a partir de los números primos.

¿Cuántos números primos existen?
Sabemos que hay infinitos, tal y como probó Euclides hace 2300 años en Los Elementos. Supongamos que solo hay un número finito de números primos: $p_1, p_2, \ldots, p_n$; el número

$$q = (p_1 \cdot p_2 \cdot \ldots \cdot p_n) + 1$$

es un nuevo número primo, ya que ninguno de los p_k puede ser divisor de q. Llegamos a una contradicción. Esta es una prueba por reducción al absurdo.

Pero no se conoce un patrón que nos diga cómo están distribuidos.

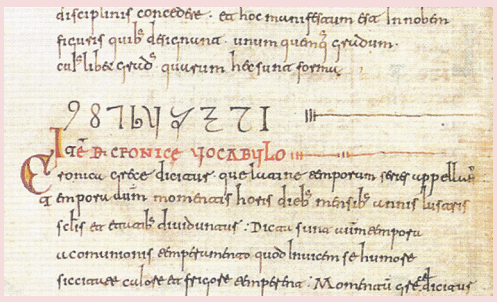
¿Cómo encontrar los números primos entre 1 y 100?
La *Criba de Eratóstenes* es un procedimiento para determinar todos los números primos hasta cierto número natural dado. Si queremos conocer los primos entre 1 y 100, comenzamos por el 2 y tachamos sus múltiplos, luego los múltiplos de 3, así hasta que sea posible; los números que quedan son primos. Eratóstenes de Cirene fue un matemático griego famoso por haber calculado la longitud de la circunferencia de la Tierra.

La hipótesis de Riemann
La hipótesis de Riemann, formulada por primera vez por Bernhard Riemann en 1859, es una conjetura sobre la distribución de los ceros de la función zeta de Riemann ζ (s).

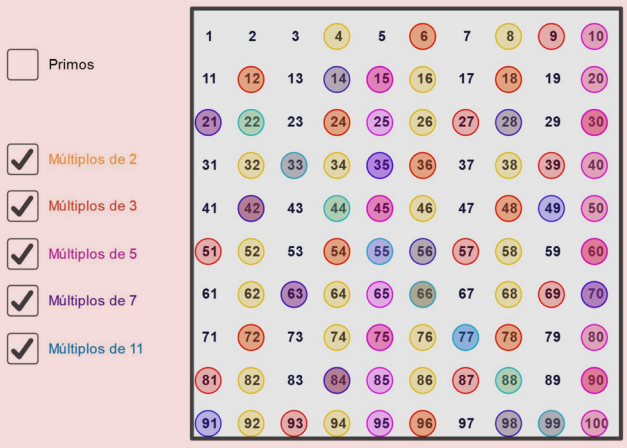
La hipótesis afirma que la parte real de todo cero no trivial de la función zeta de Riemann es ½.

Demostrarla nos permitiría descubrir la distribución que siguen los números primos. Es uno de los *Siete Problemas del Milenio* de la Fundación Clay y una manera matemática de ganar un millón de dólares.

El origen de los números
Los números del 9 al 1, tal y como los representamos hoy en día, aparecen por primera vez en España, en el *Codex Vigilanus* o *Codex Albeldensis*, compuesto por el monje Vigila en el siglo X en la Rioja.



Un número primo es el que solo se puede dividir por 1 y por sí mismo (el 1 no se considera un número primo, pero si el 2, 3, 5, 7, 11, ...



$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Saber si un número es primo o no es fácil para números pequeños, pero puede ser una tarea ardua o casi imposible para números muy grandes.

Cazadores matemáticos de fantasmas
Hasta ahora solo se conocen 51 primos de Mersenne, y de ellos, $2^{82.589.933} - 1$ es el mayor número primo conocido, con 24.862.048 dígitos.

Actualmente existe una red de 'cazadores de números primos', la *Great Internet Mersenne Prime Search* (*GIMPS*) que busca primos nuevos desde 1996.

¿Por qué es importante conocer más y más números primos?
Encriptar es transformar un mensaje en otro que solo nosotros y nuestro destinatario somos capaces de descifrar. Para ello, tenemos que conocer la clave. Como todo mensaje se puede traducir en números, reducimos el problema a transmitir números. Si conocemos dos primos muy grandes y los multiplicamos, obtendremos un número enorme. Si transmitimos ese número, nadie será capaz de descomponerlo en sus factores originales.

Un problema es transmitir la clave al destinatario. Se habla de encriptación simétrica cuando la clave para encriptar es la misma que para desencriptar; en otro caso, se dice asimétrica. Esto es lo que pasa con las claves basadas en la descomposición de un número en sus factores primos.

Aritmética modular
La aritmética modular se basa en la idea de números congruentes.

Se conoce también como 'aritmética del reloj', ya que superado el módulo, vuelven a repetirse las clases de congruencia. Por ejemplo 5 y 17 son congruentes módulo 12, por eso las 17 horas son las 5 de la tarde.

La aritmética modular fue introducida en 1801 por Carl Friedrich Gauss en su libro *Disquisitiones Arithmeticae.*

¿Cómo funciona la encriptación con números primos?

- Se eligen dos números, p y q, y se multiplican, $n = p \cdot q$
- Se calcula este número $z = (p-1) \cdot (q-1)$
- Se elige un número primo k, tal que k sea coprimo (sin divisores comunes) con z
- La clave pública es el par (n,k)
- La clave privada es un número j tal que $k \cdot j = 1 \pmod z$
- El mensaje convertido en un número P lo ciframos usando esta ecuación $P^k = E \pmod n$
- Enviamos E. El destinatario conoce la clave privada, j y hace el siguiente cálculo, $E^j = P \pmod n$

La razón de que funcione está en el llamado *Teorema de Euler-Fermat:*
Si a y n son enteros coprimos, entonces

$$a^{\Phi(n)} \equiv 1 \pmod n$$

donde $\Phi(n)$ es la llamada función de Euler ($\Phi(n)$ es el número de enteros positivos menores o iguales a n y coprimos con n).

Más razones para buscar números primos
Los números primos se usan también para evaluar el rendimiento bruto de los modernos procesadores y permiten saber si estos chips son capaces de soportar cargas de trabajo muy elevadas durante largos periodos de tiempo.

Un primo de Mersenne es un número de la forma $2^p - 1$, donde p también es un número primo.

Marin Mersenne (1588 –1648) fue un sacerdote, matemático y filósofo francés del siglo XVII, muy activo en su época comunicando entre sí y con él a los intelectuales europeos.

En 1978, **Ted Rivest**, **Adi Shamir** y **Leonard Adleman**, inventaron el algoritmo *RSA* (llamado así por sus iniciales) y que usa este procedimiento.

Dos números enteros a y b son congruentes módulo n, si ambos dejan el mismo resto al dividirlos por n, o lo que es lo mismo, si a – b es un múltiplo de n

Retrato de **Carl Friedrich Gauss**

Retrato de **Leonhard Euler**