El Mundo, 28 de Agosto de 2002
COMPUTACIÓN DISTRIBUIDA
-
ELMUNDO.ES MADRID.- ¿Cómo es posible identificar un número primo cuando éste tiene cientos de dígitos? Es la pregunta sin solución que muchos matemáticos se preguntaron y pocos se atrevieron a contestar. Un matemático indio fue el valiente que se planteó solucionarlo y que lo ha conseguido: Manindra Agrawal, profesor del Instituto tecnológico de La India ha descubierto una fórmula matemática en forma de algoritmo que reconoce los números primos. Ahora las mentes más brillantes del mundo se enfrentan a un nuevo reto: mejorar el enorme algoritmo y acabar con su margen de error.

Los números primos están entre los fenómenos matemáticos más complejos porque éstos no tienen un patrón definido, no aparecen de un modo fácilmente reconocible. Números primos como el 2, el 5 ó el 7 sí se pueden identificar como números primos, porque no son divisibles por ningún otro número, excepto por el 1 y por sí mismos. Pero, ¿qué sucede con los números más grandes? Es muy fácil determinar si un número razonablemente pequeño es primo, pero no es tan sencillo si se habla de un número con, por ejemplo, 300 dígitos.

Los números primos muy largos son esenciales en el software informático para la seguridad de las aplicaciones y su encriptación. Pero, aparte de las aplicaciones comerciales, estos números siempre han fascinado a los matemáticos. Después de varios comienzos en falso durante los tres últimos años, Agrawal y otros dos de sus estudiantes, Neeraj Kayal y Nitin Saxena, resolvieron finalmente el enigma: un algoritmo es la clave para reconocer los números primos.

Estos problemas ya los resuelven los ordenadores, mucho más rápido que las mentes más privilegiadas del planeta. Pero los ordenadores también se estropean y se equivocan.

El llamamiento de Agrawal

La proeza de Agrawal fue descubrir que un algoritmo puede identificar un número primo muy largo y sin errores. Nadie sabía nada de la ingeniosa solución de este matemático indio hasta que Agrawal envió su informe por correo electrónico a otros matemáticos para pedirles ayuda. Necesitaba pulir y mejorar su hallazgo.

Hendrik Lenstra, profesor de matemáticas en la Universidad de California, Berkeley, (EEUU) fue uno de los científicos que recibió el correo. Lenstra ha reconocido a algunas publicaciones científicas que al principio creía que el descubrimiento de un desconocido matemático de La India no tenía sentido. Unos minutos de recapacitación hicieron que Lenstra empezara a tomarse el e-mail muy en serio.

En un par de días, Lenstra envió a Agrawal una versión simplificada de su algoritmo. El problema del algoritmo original era su reducido margen de error. Aunque las ideas de Lenstra conseguían reducir el margen, Agrawal llegó a la conclusión de que el algoritmo mejorado era "impracticable".

Estos algoritmos, mejorados, ofrecen grandes posibilidades ya que reconocen los números primos mucho más rápido y sin posibilidad de errores. Pero la versión simplificada de Lenstra todavía es prematura. Tiene que corregirse.

Muchos otros matemáticos están trabajando en el problema. Agrawal cree que, con la actividad de los numerosos científicos que se han implicado en este gran enigma, en menos de un año se podrán ver algunas mejoras. Desde el momento que distribuyó su informe, Agrawal recibió el reconocimiento y el aplauso de muchos compañeros de diferentes países.

El hecho de que este descubrimiento pueda tener o no valor en el mercado no le preocupa a Agrawal, porque ha dado renovadas esperanzas a los estudiosos de los misterios matemáticos. El número primo más largo conocido tiene cuatro millones de dígitos. Su fórmula puede ser clave para acabar con un problema matemático como éste al que nadie encontraba solución. Ya ha empezado la competición mundial para mejorar el algoritmo original. ¿Quién ganará?