

[Sociedad](#) | Jueves, 7 de febrero de 2013

Primos

Un profesor de matemática de la Universidad de Missouri, Estados Unidos, acaba de descubrir el número primo más grande conocido hasta el momento. Tiene más de 17 millones de dígitos. Las aplicaciones de los números primos.

Por Adrián Paenza

Curtis Cooper es profesor de matemática en una universidad muy pequeña, en el centro de Estados Unidos, la Universidad de Missouri. Cooper se dedica desde hace muchos años a una rama de la matemática que se llama Teoría de Números. Hace dos días, el 5 de febrero del 2013, anunció al mundo que acababa de encontrar el número primo más grande que se conozca hasta hoy. Para tener una idea, este número tiene más de ¡17 millones de dígitos!

Es difícil imaginarse un número tan grande y, por otro lado, ¿para qué? ¿Qué utilidad podría tener para la vida cotidiana descubrir un número de semejante longitud? ¿Qué hay detrás de esa búsqueda? ¿Y qué significa haberlo encontrado? ¿Es que acaso mejora la calidad de vida de la ciudadanía? ¿Nos hace mejores? En definitiva... ¿para qué sirve?

Quiero ofrecer una sola –potencial– respuesta: los números primos están asociados a su vida cotidiana mucho más allá de lo que usted advierte. El único problema es que son totalmente transparentes para un ciudadano común, y obviamente me incluyo. Pero cada vez que usted retira dinero de un cajero automático, cada vez que hace cualquier transacción por Internet, cada vez que usted abre su correo electrónico y luego de poner su identidad agrega su contraseña o password, cada vez que usted usa su tarjeta de crédito (o débito) por Internet, está usando algunas propiedades de los números primos. La criptografía moderna se basa esencialmente en los números primos.

Es obvio que ninguna persona necesita saber esto, de la misma forma que una persona que conduce un automóvil no necesita saber ni cómo ni por qué funciona. Sólo le alcanza con saber manejar. Todo aquel que es diabético, sabe que necesita –eventualmente– usar insulina. El diabético la usa y no se cuestiona ni cómo se produce ni por qué funciona. Uno vive en un edificio o en una casa, y no necesita ser ni ingeniero ni arquitecto ni albañil. De hecho, usted está leyendo un diario y no necesita saber cuáles fueron los pasos que mediaron entre que yo estoy escribiendo estas líneas y usted que las está leyendo. La vida fluye de esa forma para todos en todas las actividades. La única diferencia es que cuando se produce algún acontecimiento en el mundo de la matemática, es como si el mundo entero cuestionara: ¿y ESO para qué sirve?

Como recordatorio: un número primo es un número entero positivo [1] que solamente se puede dividir exactamente por uno y por él mismo. Por ejemplo, el número dos es primo, el tres también, el cinco, el siete, el once son todos números primos. El seis no, porque no sólo es divisible por sí mismo y por uno, sino que también se puede dividir exactamente por dos y por tres. El 36 tampoco, porque es divisible exactamente por 1, 2, 3, 4, 6, 9, 12, 18 y 36. En resumen, uno podría decir que un número positivo diferente de uno es primo si solamente tiene dos divisores: uno y él mismo.

Dicho esto, algunos datos más, muy importantes:

a) se sabe que hay infinitos números primos. Lo demostró Euclides hace 2400 años;

b) todo número entero positivo (salvo el uno) o bien es primo, o bien se escribe como producto de números primos. Además, esta descomposición es única, salvo el orden. Este hecho es tan relevante que se conoce con el nombre de



Teorema Fundamental de la Aritmética.

Y ahora, un dato esencial: es muy fácil multiplicar números. No importa cuán grandes sean, las computadoras multiplican números con una velocidad alucinante. Sin embargo, lo que no pueden hacer las computadoras en un tiempo razonable es descubrir cuáles son los números primos en los que se descompone un número.

Por ejemplo, el número 15 se escribe como tres por cinco (o cinco por tres), y no hay otra forma de descomponerlo. En este caso, es muy fácil. También es fácil descomponer al número 100. Se escribe así: $100 = 2 \times 2 \times 5 \times 5$.

Pero si yo le dijera que encuentre los factores primos del número 237.598.000.273.154.151.515.515.027, quizás usted me entienda que es un poco más complicado. Es decir, cuando los números tienen muchos dígitos, encontrar los números primos que lo componen es muy difícil.

La criptografía aprovecha esta dificultad técnica para poder generar claves o contraseñas que son virtualmente inviolables. En realidad, no lo son, si uno tuviera suficiente tiempo (por ejemplo diez mil años), pero a los efectos prácticos, es como si lo fueran. Y acá me quiero permitir una licencia para exagerar: la lucha entre computadoras y el hallazgo de números primos cada vez más grandes se transforma en una suerte de carrera contra reloj: por un lado, las computadoras son cada vez más rápidas y por otro, los números primos que se encuentran son cada vez más de mayor longitud.

Una última palabra respecto de esto: si se pudiera encontrar una forma razonable (en tiempo) para encontrar los factores primos que tiene un número, ¡colapsaría el sistema financiero internacional! Así de sencillo: todas las transacciones conocidas, cuya "invulnerabilidad" pareciera estar asegurada, se resquebrajaría y caería como un castillo de naipes.

Una vuelta a Cooper

Para encontrar el número primo anunciado el 5 de febrero, Cooper trabajó junto a 98.980 personas y 574 equipos. Sí, casi 100 mil personas unidas detrás de un proyecto común que se llama GIMPS, por sus siglas en inglés: Great Internet Mersenne Prime Search (La Gran Búsqueda por Internet de Primos de Mersenne). Así como hay gente que se junta en el proyecto SETI buscando señales extraterrestres, hay más de 730 mil procesadores (computadoras) tratando de encontrar números primos (en este caso, se llaman primos de Mersenne por la forma particular que tienen).

El número encontrado por Cooper es dos multiplicado por sí mismo 57.885.161 veces y luego hay que restarle uno. Es decir: $257.885.161 - 1$.

Este número resulta tener 17.425.170 dígitos. Si uno quisiera escribirlo, necesitaría casi 84 kilómetros para poder hacerlo.

Claramente no fue dinero el móvil ni de Cooper ni del resto de los que participaron, ya que solamente conseguirá algo así como el equivalente de tres mil dólares por su hallazgo. Sin embargo, la primera persona que consiga un número primo con más de 100 millones de dígitos, obtendrá 150 mil dólares y el que llegue al número primo con más de 1000 millones de dígitos recibirá 250 mil dólares.

El primo más grande que se conocía hasta acá fue descubierto en el año 2008 (hace casi cinco años) y tenía 13 millones de dígitos. Cooper ya había encontrado otro, pero que no llegaba a los diez millones de dígitos. Por último: está claro que la vida cotidiana no cambia ni para usted ni para mí con este hallazgo. Sin embargo, hacer ciencia básica, empujar la frontera del conocimiento, tiene siempre el atractivo extra de no saber en qué momento de la evolución del ser humano, algo que parecía intrascendente o irrelevante, puede cambiar la vida de las personas. Y más allá de eso, lo que motoriza todas estas búsquedas es el deseo del hombre de conquistar lo desconocido, descubrir lo ignorado y contestar las preguntas que nadie pudo hasta acá.

[1] A los efectos prácticos, solamente hablo de números positivos, pero en realidad, la definición sobre la primalidad de un número se extiende a todos los números enteros. Eso sí: los números uno y menos uno (+1 y -1) están excluidos de la lista: no son números primos.