Ladrillos, candados y progresiones

El fabuloso mundo de los números primos

Agustín Rayo

No hay nada más hermoso que un número primo; el 19, por ejemplo, o el 101, o el 512.927.357, o el $2^{43.112.609} - 1$.

Lo que distingue a los números primos de los números naturales comunes y corrientes es que tienen exactamente dos divisores: 1 y ellos mismos. El número 7, por ejemplo, es primo porque los únicos números que lo dividen (sin resto) son el 1 y el 7. El número 12, en cambio, no es primo porque puede ser dividido (sin resto) por el 2, el 3, el 4 y el 6, además del 1 y el 12. (El número 1 no cuenta como primo porque tiene un solo divisor: él mismo.)

Los números primos son tan hermosos porque son las piezas básicas —los ladrillos— a partir de las cuales están construidos todos los números naturales mayores que 1. El número 6, por ejemplo, está construido a partir de los primos 2 y 3 (porque $6 = 2 \times 3$), y el número 12 está construido a partir de dos copias del 2 y una del 3 (porque $12 = 2 \times 2 \times 3$) (*véase la ilustración*). (El teorema fundamental de la aritmética es una versión precisa de esta idea; nos dice que todo número natural mayor que 1 tiene una descomposición única en números primos.)

Criptografía

Supongamos que usted y yo nos vemos obligados a comunicarnos a través de un mensajero. Sabemos que el mensajero entregará nuestros mensajes, pero no queremos que descubra sus contenidos. ¿Cómo podríamos evitar que nuestra información caiga en manos del mensajero? Una manera de hacerlo sería ponernos de acuerdo para utilizar un código secreto: un código que conozcamos nosotros, pero no el mensajero.

Este método funciona siempre y cuando podamos reunirnos sin que esté presente el mensajero para decidir qué código secreto utilizar. Pero supongamos que no tenemos manera de ponernos de acuerdo de antemano. Toda nuestra correspondencia —incluida la correspondencia en la que nos ponemos de acuerdo acerca de cómo transmitir nuestros secretos— pasará a través del mensajero. ¿Hay alguna manera de mantener seguros nuestros secretos?

He aquí un método posible. Yo voy a la tienda y me compro un candado. Me quedo con la llave, y le mando a usted el candado abierto, junto con una nota solicitándole que ponga su mensaje en una caja y asegure la caja con el candado. Aun cuando el mensajero se entere de todo lo que está sucediendo, nuestro secreto estará seguro, porque una vez que el candado esté cerrado, sólo yo podré abrirlo.

Los números primos nos dan una manera de obtener resultados similares sin tener que ir a la ferretería. El método del candado funciona porque los candados gozan de una asimetría: son fáciles de cerrar, aunque difíciles de abrir. Pues resulta que los números primos también gozan de una cierta asimetría. Es fácil multiplicar números primos para obtener un número compuesto, pero a la fecha no se conoce ningún método eficiente para descomponer un número compuesto en los primos que lo constituyen.

Esto hace posible que usted y yo aseguremos nuestros secretos utilizando el método siguiente. Yo escojo dos números primos p y q, y me cercioro de que sean grandes. (Se conocen métodos eficientes para hacer esto.) El resultado de multiplicar p y q será nuestro 'candado'. Le mando a usted ese número a través del mensajero, junto con instrucciones acerca de cómo codificar su mensaje secreto sobre la base del 'candado'. Con el proceso de codificación correcto, el mensaje sólo podrá ser decodificado por quien tenga la 'llave': un número que puede ser derivado eficientemente por quien conozca p y q, pero no por quien conozca sólo el producto. Si el mensajero estuviera en posición de descomponer el candado en p y q, se hallaría capacitado para dar con la llave. Pero cuando p y q son suficientemente grandes, no se conoce ninguna manera de hacerlo en un tiempo razonable.

Muchos de los métodos criptográficos que se utilizan hoy en día —y, en particular, muchos de los que se utilizan para transmitir información de manera segura a través de Internet— están basados en variaciones de esta idea.

Un nuevo resultado sobre números primos

A pesar de su papel fundamental en la teoría de números —y de su importancia práctica— se sabe sorprendentemente poco acerca de los números primos.

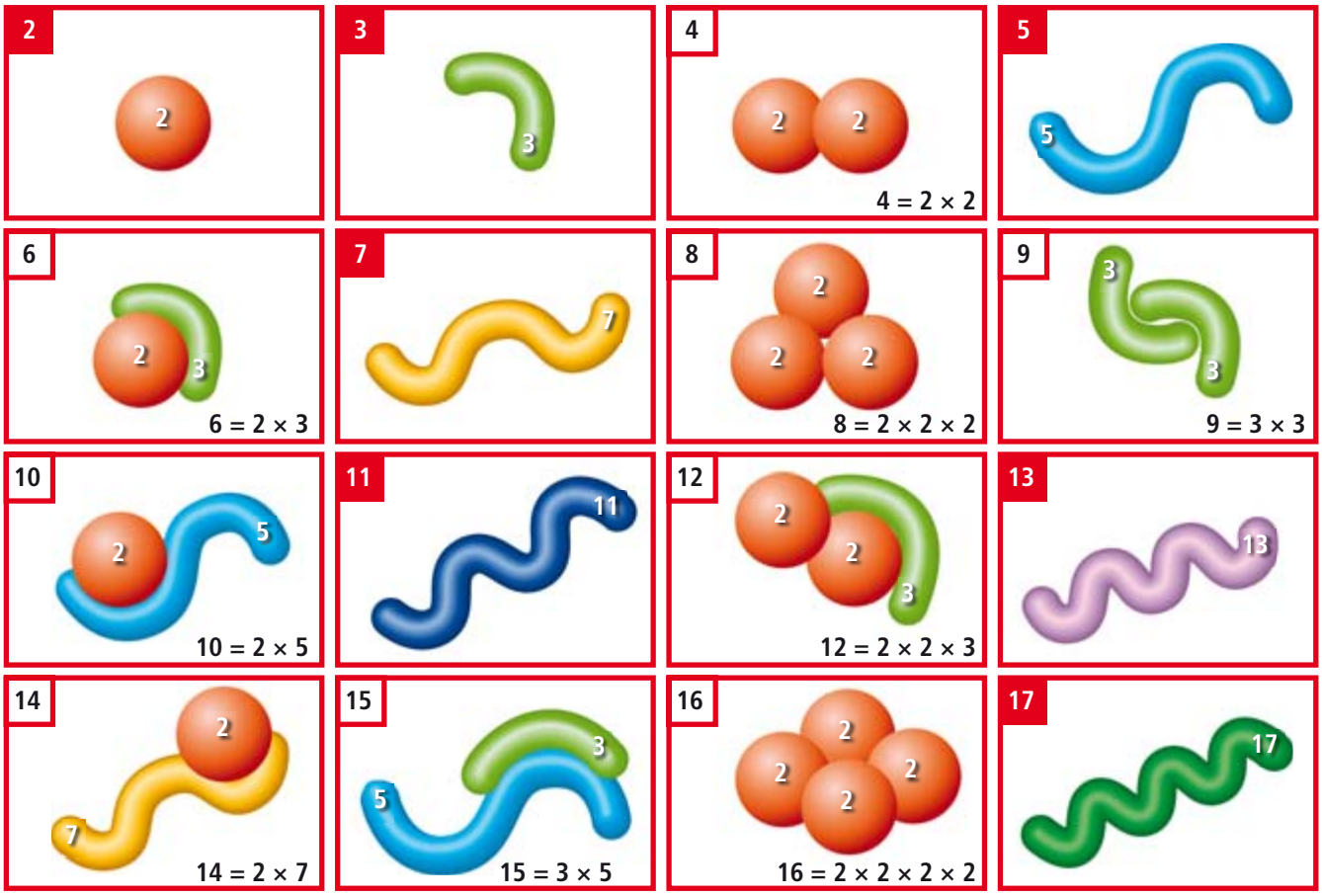
Algo que sí sabemos es que la secuencia de números primos es infinita. (*Prueba:* Supongamos que la secuencia de primos es finita: $p_1, p_2, \ldots, p_k$. Entonces existe un número $P = p_1 \times p_2 \times \ldots \times p_k$, que resulta de multiplicar a todos los números primos. Pero el número $P + 1$ tiene que ser primo. Si no lo fuera, tendría que poderse dividir entre uno de los $p_1, p_2, \ldots, p_k$, pero ningún número mayor que 1 puede dividir a un número y su sucesor. Hemos, pues, encontrado un número primo mayor que $p_1, p_2, \ldots, p_k$, contradiciendo el supuesto de que todos los primos están en $p_1, p_2, \ldots, p_k$.)

Otra cosa que sabemos es que los primos son cada vez más escasos. El teorema de los números primos nos dice que

¿Quiere saber más?

Un método criptográfico basado en las ideas que describí arriba es el RSA. (Se llama así, por los nombres de sus autores: Ron Rivest, Adi Shamir y Leonard Adleman.) Aunque hay métodos más elaborados, el RSA es especialmente elegante y fácil de describir. Hay una buena discusión en <http://es.wikipedia.org/wiki/RSA>.

Ben Green escribió una nota breve en la que explica las ideas fundamentales detrás de su teorema. Puede encontrarse en <http://smf.emath.fr/en/Publications/Gazette/2007/112/smf_gazette_112_26-27.pdf>.



Los números primos son los ladrillos a partir de los cuales están construidos los números naturales mayores que 1.

cuanto mayor sea N, menor será la proporción de primos entre 1 y N. Por ejemplo, el 40 % de los números entre 1 y 10 son primos, pero sólo el 25 % de los números entre 1 y 100 son primos, y sólo el 16,8 % de los números entre 1 y 1000 son primos. (En el caso general, la proporción de números entre 1 y N que son primos es aproximadamente $1/\ln(N)$, donde $\ln(N)$ es el 'logaritmo natural' de N, es decir, el número x tal que $N = e^x$.) Sabemos también que hay límites a cuán grande puede ser una secuencia de números sin contener al menos un número primo. El teorema de Bertrand-Chebyshev implica que, para todo N mayor que 1, hay al menos un número primo entre N y $2N$.

Por desgracia, no sabemos mucho más. Se desconoce si hay infinitos 'primos gemelos' (es decir, números p y $p + 2$, tales que ambos son primos). También se desconoce si todo número par mayor que 2 es la suma de dos primos. Este problema, denominado conjetura de Goldbach, ha estado abierto desde 1742, cuando el matemático prusiano Christian Goldbach le escribió a Euler sugiriendo que podría ser verdad. En julio del 2008, Tomás Oliveira e Silva utilizó un programa de cómputo para mostrar que la conjetura es verdad para cualquier número menor que 12×10^{17}, pero nadie ha conseguido demostrar que no podría haber algún número mayor a 12×10^{17} que no sea la suma de dos primos. (Si a usted se le ocurre alguna manera de probar alguna de estas conjeturas —y si tiene menos de 40 años— seguramente sería honrado con una Medalla Fields, el más alto honor que un matemático puede recibir.)

En vista de lo poco que se sabe sobre la distribución de los números primos, cada nuevo resultado es motivo de alegría. Y en 2004 Ben Green (profesor de la Universidad de Cambridge) y Terry Tao (profesor de la Universidad de California en Los Angeles, y ganador de la Medalla Fields) probaron un teorema fabuloso.

Digamos que una 'progresión' de números primos es una secuencia de primos tal que miembros consecutivos de la secuencia están siempre igualmente espaciados. La secuencia de primos 5, 11, 17, 23, 29, por ejemplo, es una progresión porque la diferencia entre un número y su sucesor es siempre 6. (En mayo de 2009, Raanan Chermoni y Jaroslaw Wroblewski utilizaron un programa de cómputo para encontrar una progresión de 25 números primos: $6.171.054.912.832.631 + 366.384 \times 223.092.870 \times n$, para n de 0 a 24. Que yo sepa, nadie ha logrado identificar una progresión de más de 25 números primos.)

El resultado de Green y Tao es que, *dado cualquier número N*, existe una progresión de números primos de al menos tamaño N. Existe, por ejemplo, una progresión de al menos $10^{10^{10^{10}}}$ números primos, aunque nadie haya logrado identificarla. (El teorema nos asegura que existen progresiones de primos de longitudes arbitrariamente grandes, pero no nos da un método eficiente para construirlas.)

Pocas veces se encuentra uno con un resultado tan hermoso.

Agustín Rayo es profesor de filosofía en el Instituto de Tecnología de Massachusetts.