

# Los Números Primos: de Euclides a Internet

Miguel Ángel Abánades Astudillo  
Ingeniería Técnica en Informática de Sistemas  
Centro de Estudios Superiores Felipe II (UCM)  
C/ Capitán 39, 28300 Aranjuez, Madrid

## Introducción

Al oír la palabra *números* lo que primero nos viene a la cabeza es la lista 1, 2, 3, 4, 5,...etc. Éstos son los que se conocen como *números naturales*. El estudio de los números naturales conforma lo que se llama *Teoría de Números*, una de las ramas más interesantes y complejas de las Matemáticas. Carl Fiedrich Gauss, considerado por muchos el matemático más importante de la historia, se refería a ella como la *Reina de las Matemáticas*.

Entre los números naturales hay algunos que se pueden escribir como el producto de dos números más pequeños. Por ejemplo, el número 10 se puede escribir como el producto de 2 y de 5. Éstos son los números *compuestos*. Aquellos números que no son compuestos se denominan números *primos*. Es decir, los números primos son los números naturales formados por una sola pieza. Por ejemplo, el número 7 es primo ya que no podemos encontrar dos números naturales más pequeños que él de modo que multiplicándolos se obtenga 7. A esto hay que añadir una excepción, la del número 1. Al ser el primer número natural no hay ninguno más pequeño que él y por consiguiente no es compuesto. Considerando lo dicho anteriormente, deberíamos decir que el número 1 es primo. Sin embargo, el número 1 presenta un comportamiento muy diferente al resto de los números primos debido a su condición de elemento neutro de la multiplicación (multiplicar por 1 es como no hacer nada). Esto hace que no consideremos el número 1 ni como primo ni como compuesto.

La lista de los números primos empieza por tanto así: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, etc. Y aunque es posible escribir números primos muy grandes, la lista completa de *todos* los primos es aún un misterio. En esta breve nota queremos ilustrar la fascinación por los números primos de matemáticos, profesionales y aficionados por igual, desde la antigüedad hasta nuestros días. Veremos que en las últimas décadas, con la revolución digital y el acceso generalizado a los ordenadores, esta fascinación se ha visto, si cabe, acentuada.

## Teorema Fundamental de la Aritmética

La propiedad más importante de los números primos es que constituyen las piezas básicas en las que se descompone cualquier número natural. Más exactamente, el *Teorema Fundamental de la Aritmética* dice que todo número natural mayor o igual que 2 puede ser expresado, de manera única, como producto de números primos. Por ejemplo, el número 90 podemos escribirlo como  $2 \times 3 \times 3 \times 5$ . Es importante recalcar que el teorema no sólo nos dice que podemos escribir 90 como producto de números primos, sino que además nos dice que hay una *única* manera de hacerlo. Por supuesto, se consideran iguales todas las maneras que se obtienen cambiando el

orden de los números primos; en el caso de 90, consideramos como iguales los productos  $2 \times 3 \times 3 \times 5$  y  $3 \times 2 \times 3 \times 5$ . Obsérvese que si considerásemos el número 1 como número primo, la descomposición de un número natural como producto de números primos no sería única, ya que podríamos escribir, por ejemplo,  $6 = 2 \times 3$ ,  $6 = 2 \times 3 \times 1$ ,  $6 = 2 \times 3 \times 1 \times 1$ , etc.

El Teorema Fundamental de la Aritmética aparece en el libro IX de *Los Elementos* de Euclides, texto del siglo IV antes de nuestra era considerado por muchos como el primer libro de Matemáticas *modernas* de la historia. Resulta interesante observar el lenguaje que usa Euclides en este contexto. En vez de decir que un número *divide* a otro, Euclides usa la expresión *mide a*, considerando conceptos geométricos: 3 *mide a* 15 porque podemos dividir un segmento de longitud 15 en 5 segmentos de longitud 3. Esta percepción geométrica es coherente con la mentalidad de la época que consideraba la palabra Matemáticas como un sinónimo de Geometría.

Con el Teorema Fundamental de la Aritmética en mente podemos pensar en los números primos como un análogo numérico de los átomos en Química, que son irreducibles y además generan, mediante distintas combinaciones, todas las moléculas. Esto hace que los números primos tengan estrechas relaciones con aspectos de las Matemáticas que aparentemente no están directamente relacionados con ellos.

### **Irracionalidad de $\sqrt{2}$**

Consideramos ahora todos los números *reales*, es decir, los números *con decimales*. Si pensamos en los primos como números formados por una sola pieza, podríamos decir que lo más alejado de esta idea es la de *número irracional*. Veremos que, a pesar de las diferencias conceptuales iniciales, estas dos ideas están muy relacionadas. Pero antes, vamos a explicar con algo más de detalle qué entendemos por número irracional. Decimos que un número real positivo es *racional* si se puede escribir como la división de dos números naturales (racional viene del latín *ratio*, proporción). Por ejemplo, el número 3,75 es racional porque es igual a  $15/4$ , y el número 0,1353535353535... (repetiéndose 35 indefinidamente) también es racional porque es igual a  $134/990$ . Los números que no se pueden escribir como un cociente de este tipo se llaman *irracionales*. La diferencia se encuentra en las cifras decimales: un número real es racional si tiene una cantidad finita de decimales o si, como en el ejemplo anterior, tiene una cantidad infinita de cifras decimales pero de manera que a partir de un punto la lista de decimales repite indefinidamente las mismas cifras. Los números irracionales, por el contrario, son aquellos con una lista de cifras decimales infinita *de verdad*, es decir, que no se *estabiliza* con la repetición de algunas cifras. Esto hace que la escritura *normal* (con las cifras del 0 al 9) de los números irracionales sea imposible. Esta es la razón por la que a veces usamos símbolos especiales para referirnos a algunos números. Esto pasa, por ejemplo, con  $\pi$ , el más famoso de todos los números irracionales. Otros símbolos usados para escribir indirectamente algunos números son las *raíces*. Estamos acostumbrados a tratar con el número  $\sqrt{2}$ , y nos olvidamos de

que no estamos escribiendo el número en sí, sino un símbolo que significa *el número positivo cuyo cuadrado es 2*.

En el caso particular de  $\sqrt{2}$  tenemos que, como  $\pi$ , también es irracional. Vamos a esbozar una demostración de este hecho que sólo usa la escasa teoría sobre los números primos que hemos comentado. Esto es sorprendente si tenemos en cuenta que la idea de irracional se corresponde con números infinitamente *divididos* en trozos y la idea de primo se corresponde con números *indivisibles*. En la demostración de la irracionalidad de  $\sqrt{2}$  que vamos a ver se usa el método de *reducción al absurdo*. Este método dice que si, partiendo de una suposición, llegamos a una situación imposible, es que la suposición de la que partimos es falsa. En nuestro caso particular, como queremos demostrar que  $\sqrt{2}$  es irracional, partiremos de la suposición de que esto es falso, esto es, de que  $\sqrt{2}$  es racional. Si a partir de esto logramos llegar a una situación imposible, deduciremos que la suposición de que  $\sqrt{2}$  es racional es falsa y por tanto habremos demostrado que  $\sqrt{2}$  es irracional. Para empezar la demostración suponemos pues que  $\sqrt{2}$  es racional, es decir, que podemos escribir  $\sqrt{2} = m/n$ , donde  $m$  y  $n$  son números naturales. De esta ecuación se deduce  $n \times \sqrt{2} = m$  y elevando ambos miembros al cuadrado obtenemos  $n^2 \times 2 = m^2$ . Si consideramos ahora la descomposición en producto de primos de ambos miembros de la ecuación obtenemos

$$(p_1 \times p_2 \times \dots \times p_r)^2 \times 2 = (q_1 \times q_2 \times \dots \times q_s)^2,$$

donde escribimos entre paréntesis los primos que aparecen en la descomposición en factores primos de  $n$  y  $m$  respectivamente. Como los paréntesis están elevados al cuadrado, los números primos de dentro quedan a su vez elevados al cuadrado, dando lugar a la ecuación

$$p_1 \times p_1 \times p_2 \times p_2 \times \dots \times p_r \times p_r \times 2 = q_1 \times q_1 \times q_2 \times q_2 \times \dots \times q_s \times q_s,$$

en la cual los primos procedentes de la descomposición de  $m$  y  $n$  aparecen una cantidad par de veces. Ahora bien, en la ecuación tenemos un número 2 *desemparejado*. De esto se deduce que el número primo 2 aparece un número impar de veces en el miembro de la izquierda y un número par de veces en el miembro de la derecha. Pero esto es imposible ya que, como hemos comentado, el Teorema Fundamental de la Aritmética dice que la descomposición de un número en producto de primos es única. De esta manera llegamos a la contradicción que buscábamos y por tanto se deduce que  $\sqrt{2}$  es irracional.

## Números primos y criptografía

El Teorema Fundamental de la Aritmética es un resultado de existencia. Nos dice que para cada número *existe* una manera de escribirlo como producto de números primos pero no nos dice cómo hacerlo. Si consideramos un número natural “pequeño”, digamos 3.780, podemos *descomponerlo* fácilmente en producto de primos haciendo divisiones sencillas:

$$3.780 = 2 \times 2 \times 3 \times 3 \times 3 \times 5 \times 7.$$

Uno pensaría que esta operación, ejercicio habitual en la escuela primaria, se puede hacer con cualquier número. Esto no es así ni mucho menos. En general, encontrar los números primos que dividen a un número dado es un problema muy difícil, y no sólo desde un punto de vista teórico, sino también computacional. Es decir, que ni el ordenador más potente puede encontrar,

en un tiempo razonable, los divisores primos de un número un poco “grande”. Tanto es así que muchos métodos de codificación de información usan este hecho.

Los primeros sistemas de transmisión de mensajes secretos se basaban en el intercambio de una clave entre el emisor y el receptor con un contacto directo previo. Esto, en comunicaciones a grandes distancias no era muy práctico ya que hacía necesario que emisor y receptor se juntasen cada vez que motivos de seguridad obligaban a cambiar la clave. En 1977, Rivest, Shamir y Adleman, científicos del MIT (*Masachussets Institute of Technology*) en EEUU, idearon un esquema de *cifrado de clave pública*. Según este método, llamado RSA por las iniciales de los apellidos de sus creadores, el receptor hace público un número natural “grande”, del cual conoce su descomposición en factores primos. Este número es usado por el emisor para cifrar sus mensajes. La idea es que aunque todo el mundo tiene acceso a la clave pública y al mensaje cifrado, éste sólo pueden ser descifrado si se conocen los números primos que dividen al número clave. Para que nos hagamos una idea de qué significa “grande”, actualmente se considera segura una clave pública dada por un número natural de más de 300 cifras. Por supuesto, a medida que evolucionan las capacidades de los ordenadores, la idea de lo que es un número “grande” va cambiando. Por ejemplo, los creadores del esquema RSA predijeron que un mensaje encriptado por ellos usando un número de 129 cifras como clave, tardaría en descifrarse 40 trillones de años. Sin embargo, a principios de los años noventa, mediante la colaboración de 1.600 ordenadores durante 8 meses, se consiguió descifrar. Esto, a pesar del error en las predicciones de sus creadores, más que restar validez al método RSA, muestra su fortaleza e ilustra la dificultad de un problema tan aparentemente sencillo como es la descomposición de un número como producto de primos.

Estas aplicaciones de los números primos en el campo de la criptografía muestran cómo las Matemáticas más abstractas pueden tener relación directa con actividades tan mundanas como el uso de un cajero automático.

### **Infinitos números primos**

Una vez vistos algunos ejemplos de las propiedades de los números primos, volvemos a la pregunta más básica posible: ¿cuáles son los números primos? Como ya hemos comentado, ésta es una pregunta que todavía no tiene respuesta; no se conoce la lista completa de los números primos. Consideramos entonces una pregunta aparentemente similar: ¿cuántos números primos hay? En otras palabras: ¿la lista de los números primos es infinita o *se acaba*? Sorprendentemente ésta es una pregunta mucho más fácil de contestar. La respuesta es que hay una cantidad infinita de números primos. La demostración de esta propiedad se remonta de nuevo a Euclides y a sus enciclopédicos *Elementos*. Éste es un ejemplo de tipo de resultado matemático que mucha gente encuentra sorprendente: somos capaces de decir cuántos primos hay sin verlos. De una simplicidad de alguna manera ingenua, pero con una claridad rotunda, la demostración de este resultado es un buen ejemplo de belleza en las Matemáticas. Siga también el esquema de reducción al absurdo: supongamos que hay una cantidad finita de

números primos, digamos que 18. Esto quiere decir que podemos escribir una lista con todos los números primos:  $p_1, p_2, p_3, \dots, p_{18}$ . Consideramos ahora el producto de todos los primos y le sumamos 1. Es decir, consideramos el número

$$N = (p_1 \times p_2 \times p_3 \times \dots \times p_{18}) + 1.$$

Este número no está en la lista  $p_1, p_2, p_3, \dots, p_{18}$  de todos los primos porque es mayor que cualquiera de ellos, así que  $N$  no es primo. Tenemos entonces que  $N$  es compuesto y por tanto se puede dividir por algún número primo. Es decir, que  $(p_1 \times p_2 \times p_3 \times \dots \times p_{18}) + 1$  se puede dividir por alguno de los primos en la lista  $p_1, p_2, p_3, \dots, p_{18}$  dando de resto cero. Pero esto es imposible ya que, por la manera que hemos construido  $N$ , al dividirlo por cualquiera de los números primos de la lista siempre obtenemos de resto el número 1. De esta contradicción se deduce por tanto que la lista de todos los números primos es infinita.

### Primos de Mersenne. Primos-récords

Han sido muchos los matemáticos que han dedicado esfuerzos al estudio de los números primos, encomendándose a su búsqueda como si del mismísimo Santo Grial se tratara. Esto ha hecho que ciertos tipos de números primos se conozcan con el nombre del matemático que más los estudió. Éste es el caso de Marin Mersenne, fraile francés de la orden de los mínimos que en el siglo XVII convirtió la habitación de su convento en París en un centro de reunión de matemáticos de la talla de Fermat o Pascal. Mersenne estudió especialmente los números primos de la forma  $2^p - 1$ . Se puede probar que si  $p$  no es primo entonces  $2^p - 1$  tampoco es primo, con lo que sólo tienen interés los números  $2^p - 1$  con  $p$  primo. Antes de Mersenne, otros matemáticos habían establecido ya que ciertos números del tipo  $2^p - 1$  eran primos. En particular, se sabía que  $2^p - 1$  era primo para  $p = 2, 3, 5, 7, 13, 17$  y  $19$ , y que  $2^p - 1$  no era primo para  $p = 11$ . Entonces Mersenne en 1644, en el prólogo de su libro *Cogitata Physica-Mathematica*, escribe que considerando un primo  $p$  entre 2 y 257, el número  $2^p - 1$  es primo sólo para los números  $p$  siguientes: 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 y 257. Toda la comunidad matemática opinaba que era imposible que Mersenne hubiese estudiado tal cantidad de números, pero tampoco había nadie capaz de probar que su enunciado era incorrecto. La afirmación estaba tan por encima de las posibilidades de la época que tuvieron que pasar más de 100 años para que alguien hiciese un avance real en su estudio: finalmente se logró probar que efectivamente el número  $2^{31} - 1$  es un número primo. Éste es sólo uno de la cantidad ingente de resultados matemáticos asociados al nombre del matemático más prolífico de la historia, el suizo Leonhard Euler. El estudio del resultado anunciado por Mersenne no se completó hasta 1947, estableciéndose que la lista correcta es: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 y 127. Al final resultó que Mersenne había puesto dos números de más y tres de menos en su lista original. A pesar de todo, los primos de la forma  $2^p - 1$  conservan el nombre de Mersenne. Quedaban así entonces establecidos los 12 primeros primos de Mersenne. Merece la pena escribir en su totalidad la representación decimal del duodécimo primo de Mersenne:

$$2^{127} - 1 = 170.141.183.460.469.231.731.687.303.715.884.105.727.$$

Este número, que se mantuvo con el récord del primo más grande conocido durante 75 años, muy probablemente pase a la historia como el número primo más grande descubierto con

métodos manuales. Fue descubierto por Lucas en 1876 usando un resultado que actualmente se conoce como el *test de Lucas-Lehmer* por haber sido simplificado por Lehmer alrededor de 1930. Este test nos dice que para ver si  $2^p-1$  es primo basta ver que divide a una cierta cantidad definida *recursivamente*. En 1951 Ferrier dio un salto cualitativo en el estudio de los números primos y superó el récord de Lucas en 5 cifras usando una calculadora mecánica. No duró sin embargo mucho este nuevo récord ya que ese mismo año se supera el récord en 35 cifras con el uso de un computador. Así empieza la era de la electrónica y el test de Lucas-Lehmer para primos de Mersenne toma todavía más relevancia. Este test se adapta especialmente bien a la tecnología digital debido a que en sistema binario la división por  $2^p-1$  se reduce a sumas y rotaciones de cifras. Esto ha hecho que todos los récords de tamaño en primos los hayan ostentado desde entonces primos de Mersenne. Con los nuevos computadores el número de cifras de los nuevos primos-récords se dispara. Si en 1951 el primo conocido más grande tenía 79 cifras, al año siguiente ya tiene 687, y once años más tarde, 3.376. El número de cifras de estos récords aumenta según se incrementa la potencia de los nuevos computadores. En 1996 el super computador Cray T94 determina que el número  $2^{1.257.787}-1$  es primo. Es el trigésimocuarto primo de Mersenne y tiene 378.632 cifras.

## GIMPS

En la última década del siglo de la ciencia un avance tecnológico revoluciona el mundo de las telecomunicaciones: *Internet*. Nacida a partir de una idea del ejército americano apenas 20 años antes, la *red de redes* pasa rápidamente al ámbito universitario y el fenómeno es entonces imparable. Pronto las instituciones de todo el mundo están *conectadas* y el número de hogares con acceso a Internet crece de manera exponencial. Con millones de ordenadores conectados entre sí, el siguiente paso natural en la búsqueda de primos-récords es la colaboración en Internet. George Woltman, programador y entusiasta de la teoría de números, empieza a finales de 1995 a recopilar toda la información existente relativa a los primos-récords. También crea un programa optimizado para la búsqueda de primos de Mersenne y lo *cuelga* en la red. Así empieza el proyecto GIMPS (*Great Internet Mersenne Prime Search*). La idea es que colaboradores de todo el mundo operen sobre una base de datos central. La automatización final del proceso de participación es realizada a finales de 1997 por Scott Kurowski.

Desde entonces, basta con un ordenador personal y un modem para participar en la histórica búsqueda de los números primos. No hay más que conectar con la página WEB de GIMPS ([www.mersenne.org](http://www.mersenne.org)) y descargar el software necesario. Automáticamente, la base de datos central te asigna una serie de cálculos. Esta tarea la realiza el ordenador con los recursos que no están siendo utilizados en cada momento, no interfiriendo así en su actividad normal. Una vez obtenidos los resultados, el mismo ordenador contacta automáticamente con la base de datos central, actualizándola. Si el ordenador no está conectado continuamente a Internet, espera a estar conectado para hacer la transferencia de datos. Esto hace posible el uso de los nuevos resultados por otros colaboradores. Así, desde 1996, los cinco números que han ostentado el récord del número primo más grande conocido han sido primos de Mersenne obtenidos por

GIMPS. Estos fueron *descubiertos* por voluntarios en Francia en 1996, Inglaterra en 1997, Estados Unidos en 1998 y 1999 y Canadá en 2001.

Más exactamente, el número primo más grande conocido en la actualidad fue anunciado el 5 de Diciembre de 2001 y su descubridor fue Michael Cameron de Ontario. Este estudiante de 20 años usó un ordenador personal de 800 MHz durante 45 días. En la literatura científica, Cameron comparte autoría con Woltman y Kurowski, creadores de GIMPS, aunque a decir verdad, los verdaderos descubridores son los 130.000 voluntarios que colaboraron a lo largo de 27 meses con sus 205.000 ordenadores personales. El primo-récord actual es el  $2^{13.466.917}-1$ . Tiene 4.053.946 cifras y es el primo de Mersenne número 39 que se conoce. En total, todos los cálculos realizados para su detección equivalen al trabajo de un sólo ordenador personal durante más de 13.000 años. Para que nos hagamos una idea de su tamaño, si escribiésemos todas sus cifras decimales con un tamaño de fuente de 11 puntos, tendría una longitud de más de 14 kilómetros. A pesar de poner su nombre en la historia de los números primos, Michael Cameron no fue tan afortunado como Nayan Hajratwala, el descubridor en 1999 del primer primo-récord con más de un millón de cifras. Éste se llevó un premio de más de 44.000 euros dado por la *Electronic Frontier Foundation*. Esta misma institución ha ofrecido un premio de 90.000 euros para el descubridor del primer número primo con más de 10 millones de cifras.

### Conjeturas famosas

La espectacularidad los datos anteriores contrasta con el desconocimiento de algunas cuestiones sobre los números primos aparentemente muy sencillas. Algunos resultados sobre los números primos se *intuye* que son verdad, pero por ahora son tan sólo conjeturas, enunciados plausibles sin demostración. Algunas de estas conjeturas llevan abiertas durante cientos de años. Este es el caso de la *Conjetura de Golbach*.

El 7 de Julio 1742, Christian Golbach, profesor de San Petesburgo que acabó en Moscú como tutor de la familia del zar Pedro II, escribe una carta a Euler donde le comenta que, a pesar de no haber encontrado una demostración, está seguro de que todo número natural mayor o igual que 6 se puede escribir como suma de tres números primos. Euler le contesta que el resultado es equivalente a que todo número natural *par* mayor o igual que 3 es la suma de *dos* primos. Este último enunciado es el que pasa a la historia con el nombre de Conjetura de Golbach, uno de los problemas abiertos más famosos de las Matemáticas. No se duda de su veracidad, como además sugieren los cálculos hechos con algunos de los ordenadores más potentes, pero nadie ha sido capaz de dar una demostración general. El último avance en la comprobación directa del resultado mediante ordenador asegura que el resultado es cierto para todo número par hasta 400 billones.

Otra de las conjeturas más interesantes es la relativa a la cantidad de números primos *gemelos*. Dos números primos  $p$  y  $q$  se dice que son *gemelos* si  $p = q + 2$ . Como ningún número primo puede ser par, dos primos son gemelos si están todo lo cerca que dos primos pueden llegar a

estar. Primos gemelos son, por ejemplo, las parejas (17, 19), (29, 31) y (1.000.000.000.061, 1.000.000.000.063). La *Conjetura de los primos gemelos* dice que hay infinitas parejas de primos gemelos. Aunque esta afirmación parezca muy similar al resultado que hemos demostrado sobre la existencia de una cantidad infinita de números primos, todavía nadie ha sido capaz de determinar si es cierta o no. Esta conjetura puede sugerir que los primos se encuentran cerca unos de otros. Sin embargo, es fácil ver que hay listas de números naturales consecutivos no primos de cualquier longitud.

La historia de las Matemáticas está llena de resultados que en algún momento parecían retos inalcanzables. El enigma de la distribución de los números primos es posible que algún día se resuelva. Mientras tanto, seguirá despertando interés en matemáticos de todos los niveles, desde los investigadores en Teoría de Números en las universidades, hasta los niños que aprenden a dividir en las escuelas.

En otros campos de la ciencia, las aplicaciones directas marcan los caminos a seguir. En Matemáticas, sin embargo, es la fascinación por lo desconocido, por el conocimiento *en estado puro*, lo que guía, por lo general, las investigaciones. El gran Newton decía que se veía a sí mismo como “*un niño jugando a la orilla del mar, recogiendo aquí y allá una piedra más o menos lisa, o una concha de rara belleza, mientras el gran océano de la verdad permanece completamente invisible ante mis ojos*”. Sirva como ejemplo esta breve ilustración de la historia de los primos, que en último caso son sencillamente unos números “un poco especiales”.

### **Más información**

**<http://www.mersenne.org>**

Página de GIMPS (en inglés).

**<http://www.utm.edu/research/primes>**

Página con información diversa sobre los números primos (en inglés).

**<http://www.geocities.com/CapeCanaveral/Launchpad/2208/index.html>**

Página con información variada sobre los números primos (en español).

**<http://www.cs.unb.ca/~alopez-o/math-faq/node27.html>**

Página con información variada sobre los números primos (en inglés).

**<http://www-history.mcs.st-andrews.ac.uk/history/Mathematicians/Mersenne.html>**

Breve biografía de Marin Mersenne en la página de historia de las Matemáticas de la Universidad de Saint Andrews en Escocia (en inglés).

**<http://www.mathacademy.com>**

Página con diversa información matemática (en inglés).

**<http://www.times-archive.co.uk/news/pages/tim/2000/03/16/timfeafea02004.html>**

Artículo sobre la conjetura de Golbach aparecido en el *Sunday Times* el 16 de Marzo de 2000 (en inglés).

**[http://news.bbc.co.uk/hi/english/sci/tech/newsid\\_1693000/1693364.stm](http://news.bbc.co.uk/hi/english/sci/tech/newsid_1693000/1693364.stm)**

Artículo sobre el descubrimiento de un nuevo primo-récord aparecido en *BBC News* el 5 de Diciembre de 2001 (en inglés).