La frase más excitante que se puede oír en ciencia,
la que anuncia nuevos descubrimientos, no es "¡Eureka!"
sino "qué extraño" .

Número primo de Marin Mersenne

Se dice que un número *M* es un número de Mersenne si es una unidad menor que una potencia de 2. $M_n = 2^n - 1$.

Un número primo de Mersenne es un número de Mersenne que es primo. Se denominan así en memoria del filósofo del siglo XVII Marin Mersenne quien en su *Cognitata Physico-Mathematica* realizó una serie de postulados sobre ellos que sólo pudo refinarse tres siglos después. También compiló una lista de números primos de Mersenne con exponentes menores o iguales a 257, y conjeturó que eran los únicos números primos de esa forma. Su lista sólo resultó ser parcialmente correcta, ya que por error incluyó M_{67} y M_{257}, que son compuestos, y omitió M_{61}, M_{89}, y M_{107}, que son primos; y su conjetura se revelaría falsa con el descubrimiento de números primos de Mersenne más grandes. No proporcionó ninguna indicación de cómo dio con esa lista, y su verificación rigurosa sólo se completó más de dos siglos después.

Actualmente (abril de 2011), sólo se conocen 47 números primos de Mersenne, siendo el mayor de ellos $M_{43.112.609} = 2^{43.112.609}-1$, un número de casi trece millones de cifras. El número primo más grande que se conocía en una fecha dada casi siempre ha sido un número primo de Mersenne: desde que empezó la era electrónica en 1951 siempre ha sido así salvo en 1951 y entre 1989 y 1992.

Cuando Marin Mersenne contaba con 56 años de edad publicó un libro titulado *Cogitata Physico-Mathematica* en cuyo prefacio comentaba que los primeros primos de la forma $2^p - 1$eran los que correspondían a *p=2, 3, 5, 7, 13, 17, 19, 31, 67, 127 y 257*. Las comprobaciones hasta *p=19* no fueron demasiado problemáticas, pero a partir de ahí los cálculos tenían ya cierta entidad.

En 1774, **Euler** probó que $M_{31} = 2^{31} - 1$era un número primo, por lo que Mersenne iba bien en su *predicción*. Más adelante, en 1876, **Lucas** demostraba que $M_{127} = 2^{127} - 1$también era un número primo. No iba mal Marin Mersenne.

Pero poco después la predicción de Mersenne se torció un poco, ya que en 1883 **Pervushin** demostraba que $M_{61} = 2^{61} - 1$era primo, hecho que significaba que Mersenne se había dejado un primo por el camino. Pero bueno, al parecer había acertado en todos los que había calificado como números primos… ¡Un momento, faltaba el M_{67}! ¿Qué pasó con él?

En 1903, en una de las reuniones de la *American Mathematical Society*, un matemático desconocido hasta la fecha llamado **Frank Nelson Cole** presentó un trabajo titulado *Sobre la factorización de grandes números*. Cuando el Presidente de la AMS llamó a Cole para que expusiera su trabajo, éste se colocó delante de una pizarra y comenzó a calcular a mano *2 elevado a 67* (vamos, multiplicó 2 por sí mismo 67 veces) sin pronunciar ni una palabra. Cuando terminó restó 1 al número obtenido, dejando escrito el resultado final. Después se dirigió a una zona de la pizarra que no estaba utilizada y, todavía sin decir palabra ni frase alguna, realizó a mano la siguiente operación:

Frank Nelson Cole

$$193707721 \cdot 761838257287$$

Cuando concluyó la multiplicación se pudo comprobar que el resultado coincidía con el obtenido anteriormente. Esto es, Cole había probado que M_{67}**no era un número primo**. Hecho esto, Cole se volvió a sentar sin decir absolutamente nada y los asistentes a su presentación le dedicaron una calurosa ovación.

Por cierto, más adelante Cole comentó que encontrar esos dos factores le había llevado *"tres años de domingos"*.

Actualmente, el mayor primo de Mersenne que se conoce es $M_{43.112.609} = 2^{43.112.609} - 1$, que tiene 12.978.189 cifras. Se trata del 47º primo de Mersenne conocido y su descubrimiento se anunció el 23 de agosto de 2008. De momento no se conocen más. Esta es la Tabla de primos de Mersenne conocidos hasta el momento, con los datos de su descubridor y año de descubrimiento.

Lista de los números primos de Mersenne conocidos

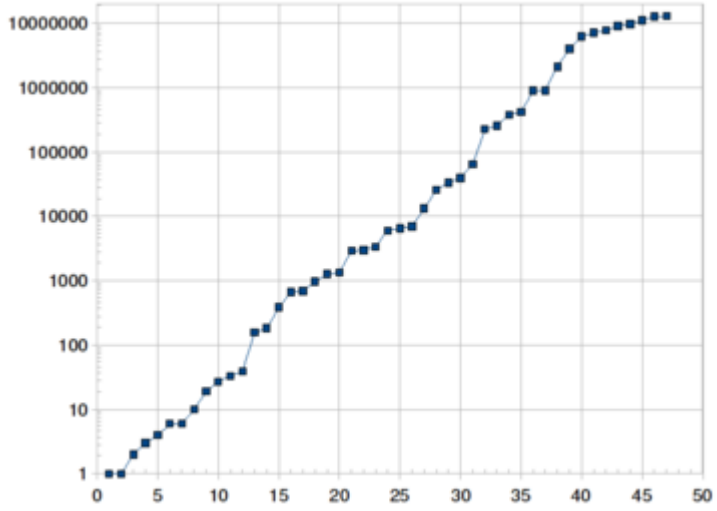


Gráfico que representa el número de cifras de cada uno de los primos de Mersenne conocidos. Nótese que la escala vertical es logarítmica.

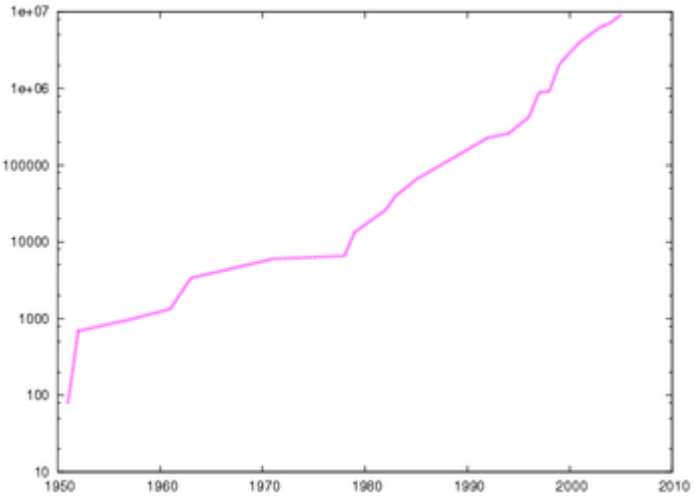


Gráfico del número de dígitos del primo de Mersenne más grande que se conocía cada año (era electrónica). La escala vertical es logarítmica.

La siguiente tabla muestra los números primos de Mersenne conocidos:

#	n	M_n	Nº de cifras de M_n	Fecha del descubrimiento	Descubridor
1	2	3	1	*antigüedad*	*desconocido*
2	3	7	1	*antigüedad*	*desconocido*
3	5	31	2	*antigüedad*	*desconocido*
4	7	127	3	*antigüedad*	*desconocido*
5	13	8191	4	1456	*anónimo*
6	17	131071	6	1588	Cataldi
7	19	524287	6	1588	Cataldi
8	31	2147483647	10	1772	Euler
9	61	2305843009213693951	19	1883	Pervushin
10	89	618970019…449562111	27	1911	Powers
11	107	162259276…010288127	33	1914	Powers
12	127	170141183…884105727	39	1876	Lucas

13	**521**	**686479766…115057151**	**157**	**30-01-1952**	**Robinson (SWAC)**
14	**607**	**531137992…031728127**	**183**	**30-01-1952**	**Robinson (SWAC)**
15	**1.279**	**104079321…168729087**	**386**	**25-06-1952**	**Robinson (SWAC)**
16	**2.203**	**147597991…697771007**	**664**	**07-10-1952**	**Robinson (SWAC)**
17	**2.281**	**446087557…132836351**	**687**	**09-10-1952**	**Robinson (SWAC)**
18	**3.217**	**259117086…909315071**	**969**	**08-09-1957**	**Riesel**
19	**4.253**	**190797007…350484991**	**1.281**	**03-11-1961**	**Hurwitz**
20	**4.423**	**285542542…608580607**	**1.332**	**03-11-1961**	**Hurwitz**
21	**9.689**	**478220278…225754111**	**2.917**	**11-05-1963**	**Gillies**
22	**9.941**	**346088282…789463551**	**2.993**	**16-05-1963**	**Gillies**
23	**11.213**	**281411201…696392191**	**3.376**	**02-06-1963**	**Gillies**
24	**19.937**	**431542479…968041471**	**6.002**	**04-03-1971**	**Tuckerman**
25	**21.701**	**448679166…511882751**	**6.533**	**30-10-1978**	**Noll y Nickel**
26	**23.209**	**402874115…779264511**	**6.987**	**09-02-1979**	**Noll**
27	**44.497**	**854509824…011228671**	**13.395**	**08-04-1979**	**Nelson y Slowinski**

28	**86.243**	**536927995…433438207**	**25.962**	**25-09-1982**	**Slowinski**
29	**110.503**	**521928313…465515007**	**33.265**	**28-01-1988**	**Colquitt y Welsh**
30	**132.049**	**512740276…730061311**	**39.751**	**20-09-1983**	**Slowinski**
31	**216.091**	**746093103…815528447**	**65.050**	**06-09-1985**	**Slowinski**
32	**756.839**	**174135906…544677887**	**227.832**	**19-02-1992**	**Slowinski y Gage**
33	**859.433**	**129498125…500142591**	**258.716**	**10-01-1994**	**Slowinski y Gage**
34	**1.257.787**	**412245773…089366527**	**378.632**	**03-09-1996**	**Slowinski y Gage**
35	**1.398.269**	**814717564…451315711**	**420.921**	**13-11-1996**	**GIMPS / Joel Armengaud**
36	**2.976.221**	**623340076…729201151**	**895.932**	**24-08-1997**	**GIMPS / Gordon Spence**
37	**3.021.377**	**127411683…024694271**	**909.526**	**27-01-1998**	**GIMPS / Roland Clarkson**
38	**6.972.593**	**437075744…924193791**	**2.098.960**	**01-06-1999**	**GIMPS / Nayan Hajratwala**
39	**13.466.917**	**924947738…256259071**	**4.053.946**	**14-11-2001**	**GIMPS / Michael Cameron**
40[*]	**20.996.011**	**125976895…855682047**	**6.320.430**	**17-11-2003**	**GIMPS / Michael Shafer**
41[*]	**24.036.583**	**299410429…733969407**	**7.235.733**	**15-05-2004**	**GIMPS / Josh Findley**

42[*]	**25.964.951**	**122164630…577077247**	**7.816.230**	**18-02-2005**	**GIMPS / Martin Nowak**
43[*]	**30.402.457**	**315416475…652943871**	**9.152.052**	**15-12-2005**	**GIMPS / Curtis Cooper y Steven Boone**
44[*]	**32.582.657**	**124575026…053967871**	**9.808.358**	**04-09-2006**	**GIMPS / Curtis Cooper y Steven Boone**
45[*]	**37.156.667**	**202254406…308220927**	**11.185.272**	**06-09-2008**	**GIMPS / Hans-Michael Elvenich**
46[*]	**42.643.801**	**169873516…562314751**	**12.837.064**	**12-04-2009**	**GIMPS / Odd M. Strindmo**
47[*]	**43.112.609**	**316470269…697152511**	**12.978.189**	**23-08-2008**	**GIMPS / Edson Smith**

***No se conoce si existen más números primos de Mersenne entre el 39 ($M_{13.466.917}$) y el 47 ($M_{43,112,609}$) por lo tanto, esta tabla es provisional. Por poner un ejemplo histórico, el 29º número primo de Mersenne fue descubierto *después* del 30º y el 31º.**

Si n es compuesto, entonces M_n es compuesto.

Demostración
Si *n* es un número natural, por el teorema binomial se tiene:

$$c^n - d^n = (c-d)\sum_{k=0}^{n-1} c^k d^{n-1-k}$$

,

Tomando *c* = 2, *d* = 1 y *n* = *ab* (*a*, *b* > 1), se tiene:

$$M_n = M_{ab} = 2^{ab}-1 = (2^a)^b-1^b = (2^a-1)\sum_{k=0}^{b-1}(2^a)^k 1^{b-1-k} = (2^a-1)\cdot\left(1+2^a+2^{2a}\right.$$

$2^a - 1$ es mayor que 1 porque se ha procurado que *a* es estrictamente mayor que 1, y la suma $1 + 2^a + 2^{2a} + 2^{3a} + \ldots + 2^{(b-1)a}$ también lo es. Por tanto, se tiene una factorización de M_n, así que M_n es compuesto.

***Observación*: Por <u>contraposición</u>, si M_n es primo, entonces *n* es primo. Esto facilita la búsqueda de nuevos números primos de Mersenne M_n, ya que sólo hay que comprobar la primalidad de aquellos para los que *n* es primo.**

> **Si *p* es un número primo distinto de 2, cualquier primo *q* que divida a 2^p-1 debe ser uno más que un múltiplo de 2*p*. Esta proposición también se cumple si $2^p - 1$ es primo.**

- **Ejemplo I: $2^5 - 1 = 31$ es primo, y 31 es igual a 1 más un múltiplo de 2·5.**
- **Ejemplo II: $2^{11} - 1 = 23 \cdot 89$, siendo:**

  $23 = 1 + 2 \cdot 11$
  $89 = 1 + 8 \cdot 11$
  $23 \cdot 89 = 1 + 186 \cdot 11$

Demostración

Si *q* divide 2*p* - 1, entonces $2p \equiv 1 \pmod{q}$. Por el <u>Pequeño Teorema de Fermat</u>, $2(q-1) \equiv 1 \pmod{q}$. Supongamos que existe un *p* que no divida *q* − 1. Entonces, como *p* y *q* − 1 deben ser <u>primos entre sí</u>, una nueva aplicación del Pequeño Teorema de Fermat muestra que $(q-1)(p-1) \equiv 1 \pmod{p}$. Por tanto, existe un número $x \equiv (q-1)(p-2)$ tal que $(q-1)\cdot x \equiv 1 \pmod{p}$, y por tanto un número *k* tal que $(q-1)\cdot x - 1 = kp$.

Como $2(q-1) \equiv 1 \pmod{q}$, al elevar ambos lados de la <u>congruencia</u> a la potencia *x* resulta $2(q-1)x \equiv 1$, y como $2p \equiv 1 \pmod{q}$, al elevar de nuevo ambos lados de la congruencia a la potencia *k* resulta $2kp \equiv 1$. Por tanto, $2(q-1)x \div 2kp = 2(q-1)x - kp \equiv 1 \pmod{q}$. Pero por definición $(q-1)x - kp = 1$, lo que implica que $21 \equiv 1 \pmod{q}$; en otras palabras, que *q* divide 1. Con esto, la premisa inicial de que *p* no divide *q* − 1 es insostenible.

> **Si *p* es un número primo distinto de 2, cualquier primo *q* que divida $2^p - 1$ es congruente con $\pm 1 \pmod{8}$.**

Demostración

$2^{p+1} = 2 \pmod{q}$, así que $2^{(p+1)/2}$ es una raíz cuadrada de 2 módulo *q*. Por reciprocidad cuadrática, cualquier módulo primo del cual 2 tenga raíz cuadrada es congruente con $\pm 1 \pmod 8$

Desmentida la conjetura original de Mersenne (que establecía una lista de números primos de Mersenne menores o iguales que M_{257} y afirmaba que no existían más que esos), han surgido otras preguntas abiertas relacionadas con la caracterización de estos números. En particular, la conjetura de Bateman, Selfridge and Wagstaff (1989) también recibe el nombre de "Nueva conjetura de Mersenne".

Nueva conjetura de Mersenne

La Nueva conjetura de Mersenne o Conjetura de Bateman, Selfridge y Wagstaff (Bateman et al. 1989) establece que para cada número natural impar *p*, si se cumplen dos de las siguientes condiciones, también se cumple la tercera:

1. **$p = 2^k \pm 1$ o $p = 4^k \pm 3$ para algún número natural *k*.**
2. **$2^p - 1$ es primo (un número primo de Mersenne).**
3. **$(2^p + 1) / 3$ es primo (un número primo de Wagstaff).**

Si *p* es un número compuesto impar, entonces tanto $2^p - 1$ como $(2^p + 1)/3$ son compuestos. Por tanto, sólo es necesario examinar números primos para verificar esta conjetura.

Se puede pensar que la nueva conjetura de Mersenne es un intento de rescatar la centenaria conjetura original de Mersenne, que se demostró falsa. Sin embargo, según Robert D. Silverman, John Selfridge declaró que la *NCM* es "obviamente cierta" ya que fue elegida con el fin de encajar en los datos conocidos y los contraejemplos más allá de esos casos son progresivamente más improbables. Se puede considerar más como una observación que como una pregunta abierta en busca de respuesta. Su página web contiene la verificación de los resultados obtenidos hasta este número.

Conjetura de Lenstra–Pomerance–Wagstaff

Lenstra, Pomerance y Wagstaff han conjeturado que no sólo existe un número infinito de primos de Mersenne, sino que el número de primos de Mersenne con exponente *p* menor que *x* se puede aproximar asintóticamente por

$$e^\gamma \cdot \log_2(x),$$

donde γ es la constante de Euler-Mascheroni y $e^\gamma = 1.781072417990197\ldots$

Relación con otras categorías de números

Números perfectos

Euclides, muchos siglos antes que Mersenne, ya conocía estos números y encontró una fuerte relación entre ellos y los números perfectos. Si *M* es un número primo de Mersenne, entonces *M*·(*M*+1)/2 es un número perfecto. Asimismo, Euler demostró en el siglo XVIII que todos los números perfectos pares son de la forma *M*·(*M*+1)/2. No se conocen en la actualidad números perfectos impares, y se sospecha que no existe ninguno.

Números dobles de Mersenne

Un número doble de Mersenne se define como:

$$M_{M_p} = 2^{2^p-1} - 1$$

donde *p* es el exponente de un número primo de Mersenne.

Números repunit

Los números repunit (del inglés *repeated unit*, "unidad repetida") son los que, en una base dada, se representan como una cadena de unos. Los números de Mersenne son los números repunit en el sistema binario.

Otras curiosidades.

Golbach, propuso una famosa conjetura, conjetura que se conoce precisamente como "conjetura de Golbach", que la suma de dos números primos es siempre un número par.

Es precisamente una conjetura, porque ningún matemático ha podido demostrar esta proposición.

Pero, ¡Funciona!

Probemos: 7 + 5=12

23+ 31= 54

¡Inténtelo con otro par de números primos.

El monje Francés Mensenne (1588-1648) , advirtió que hay muchos números primos que tienen la forma: $2^p - 1$, donde p es un numero primo.

Durante muchos años se creyó que $2^{67} - 1$ era primo, pero el matemático Cole (1861-1927) en una reunión de la American Mathematical Society , en 1903 calculo el valor en un extremo de una pizarra y en el otro extremo efectuó la multiplicación 193.707.721 x 761.838.257.287. ¡Los resultados eran los mismos!

En 1985, se detectó el 23º primo de Mersenne, esto es: $2^{116.091} - 1$, este número en esta oportunidad se incluyó en un matasello postal (estampilla)

El último número primo de Mersenne obtenido recientemente corresponde a $2^{1.398.269} - 1$, este numero contiene 420.921 dígitos. Si este número se escribe con la separación acostumbrada tendría una longitud de ¡600 metros!

Algunas curiosidades de los números primos:

Todo número primo es un múltiplo de seis más/menos la unidad. Esto es: $\dot{6} \pm 1$ (exceptuando los números primos 2 y 3)

Probemos:

17= 6 x 3 -1

23 = 6 x 4-1

31 = 6x 5 +1

Primos gemelos: cuando la diferencia entre dos números primos es exactamente 2, se dice que estos números son "primos gemelos"

Ejemplo: 7 y 5 son primos gemelos

Divisores de un número: conjunto de números que dividen exactamente a un número.

Ejemplo, los divisores de 18 son: 1 , 2 , 3 6, 9 y 18

Numero perfecto: si la suma de los divisores, exceptuando el propio número como divisor, da el propio número, se dice que el número es ¡Perfecto!

Ejemplo 6 , porque los divisores de 6 , a excepción del 6, son 1 , 2 y 3, cuya suma es : 1+2+3 =6

Números amigos: cuando la suma de los divisores de uno de ellos (exceptuando el propio número) corresponde al otro número, y la suma de los divisores de este (exceptuando el propio número) corresponde al primero.

Ejemplo 220 y 284 son amigos, porque

Divisores de 220, son: 1, 2 , 4 ,5 , 10 , 11, 20 , 110 y 220 , cuya suma : 1+2+4+5+11+20+110 =

Divisores de 284, son:

MCM (máximo común múltiplo de un conjunto de números) corresponde al menor de los números que es divisible por un conjunto de otros números)

Ejemplo el MCM(60 y 48) es 12, pues 60 es divisible por 12 y también 48 lo es. Y este es el mayor de los múltiplos.

Lo curioso es que el producto del MCD por el MCM de un par de número corresponde al producto de los números, esto es:

Ejemplo: MCD(18, 12) = 6

MCM(18,12) =36

Entonces 6 x 36 = 216

Que coincide con el producto de 18 x 12 = (18+2)=20 x 10 = 200 + 16 = 216

¡Otra que funciona!

Y continúa la historia de los números primos:

EL MAYOR NÚMERO PRIMO CONOCIDO

Número primo es aquel número natural mayor que uno que sólo es divisible por él mismo y por la unidad. Por ejemplo, los primeros números primos son: 2, 3, 5, 7, 11, 13, 17, 19, …

El Teorema Fundamental de la Aritmética afirma que cualquier número no primo (compuesto) puede escribirse de una única manera como producto de números primos. Por ejemplo: 70 = 2.5.7 . Los números primos son, por tanto, los cimientos sobre los que se construye todo el edificio de la Aritmética, razón por la cual constituyen el objeto central de su estudio.

´

Ya Euclides, en el siglo III a.C., demostró de un modo sencillo y elegante que hay infinitos números primos, es decir, siempre hay uno mayor que cualquiera que encontremos por muy grande que sea. A partir de entonces ha atraído en gran manera a los matemáticos y aficionados a esta disciplina la idea de obtener una fórmula que nos permita expresarlos todos o al menos un conjunto indefinido de ellos, algo que no se ha conseguido.

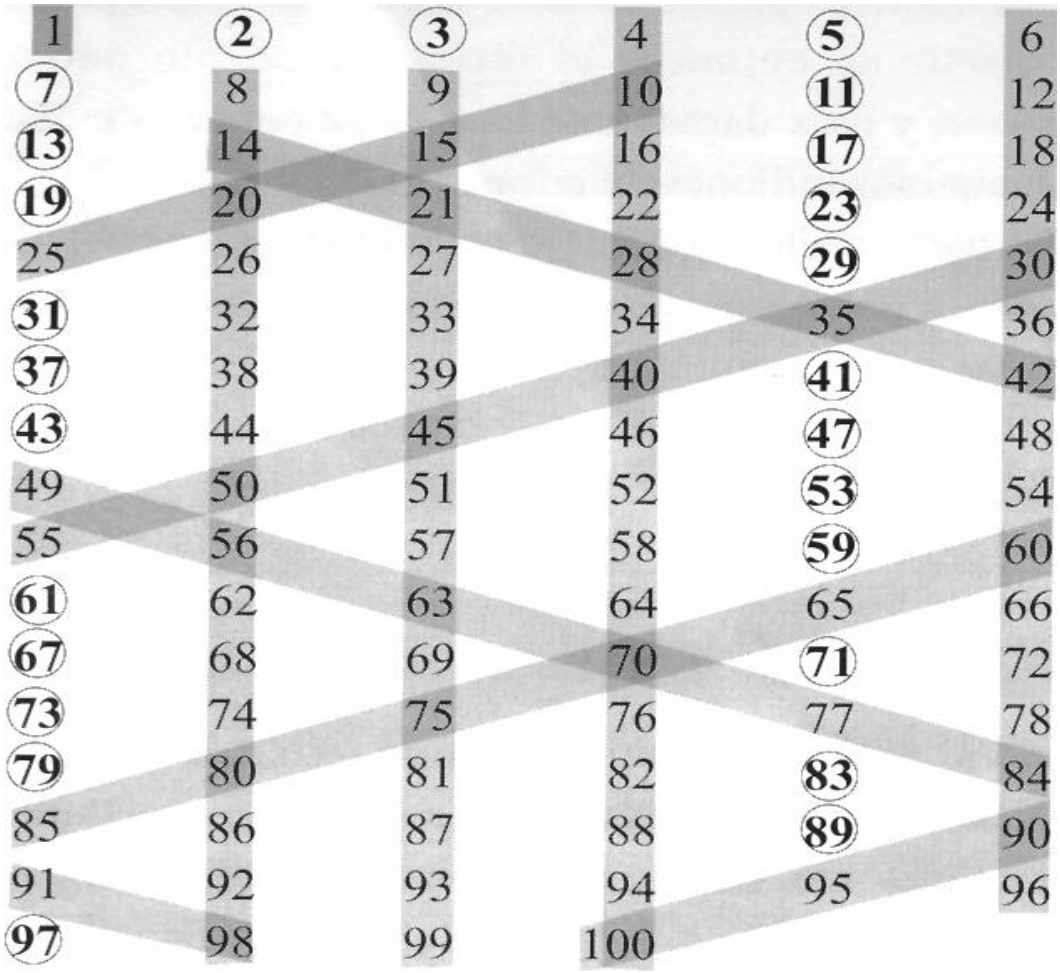
Sí que hay métodos para ir formando ordenadamente la sucesión de los números primos y actualmente con la ayuda del ordenador se puede ir generando estos números con una enorme rapidez, pero no existe un procedimiento de cálculo que nos diga cuál es el número primo que ocupa un determinado lugar en la sucesión. Sí que sabemos que entre los más grandes cada vez son más escasos los números primos. Hay 25 entre los 100 primeros naturales, 21 entre los 100 siguientes, etc..

El primer método de construcción de los números primos que se conoce es el debido al matemático griego Eratóstenes de Cirene, quien en el siglo III a.C. dio un método para seleccionar números primos, que consistía en ir tachando los números que no son primos de la sucesión ordenada de los números naturales.

Si cogemos los 100 primeros números naturales y aplicamos lo anterior tenemos lo que se conoce como Criba de Eratóstenes. Para su construcción ordenamos dichos números formando seis columnas. A continuación procedemos del siguiente modo:

- ***Se tacha el 1, que no es primo.***
- ***Eliminamos los múltiplos de 2, excepto el 2, es decir los números de las columnas 2^a , 4^a y 6^a .***
- ***Se eliminan los múltiplos de 3, salvo el 3 (columna 3^a , pues la 6^a ya está eliminada).***
- ***Quitamos los múltiplos de 5, salvo el 5, y los múltiplos de 7, excepto el 7. Tanto unos como otros se encuentran formando diagonales.***

Los que van quedando son los que constituyen la sucesión de los números primos, que como podemos observar en el gráfico presentan una cierta regularidad, aunque no lo suficiente como para encontrar una expresión matemática que nos permita su construcción.


1 2 3 4 5 6
7 8 9 10 11 12
13 14 15 16 17 18
19 20 21 22 23 24
25 26 27 28 29 30
31 32 33 34 35 36
37 38 39 40 41 42
43 44 45 46 47 48
49 50 51 52 53 54
55 56 57 58 59 60
61 62 63 64 65 66
67 68 69 70 71 72
73 74 75 76 77 78
79 80 81 82 83 84
85 86 87 88 89 90
91 92 93 94 95 96
97 98 99 100

Si que existen algunas fórmulas que nos dan un número finito de números primos como la descubierta por Euler en el siglo XVIII, , que da números primos desde hasta . El récord actual de polinomios cuadráticos que dan números primos para valores consecutivos de n lo ostenta el polinomio de Ruby: , que da 45 primos para n = 0, 1, 2, ..., 44, pero es compuesto para n = 45. **$41_2++nn0=n39=n|275381036|_2+-nn$**

Goldbach probó en 1752 que ningún polinomio (y Legendre que ningún cociente de polinomios) en una variable y de coeficientes enteros es primo para todo n. En otras palabras, no existe ninguna "fórmula sencilla" que genere sólo números primos.

Podemos decir que antes de la llegada de los ordenadores el mayor de los números primos conocidos era el número de Mersenne 2^{127}-1, que posee 39 cifras. Los números de Mersenne (monje francés que desarrolló sus estudios sobre números primos en la primera mitad del siglo XVII) son de la forma $12-_P$. Para que estos números sean primos es necesario que p también lo sea, pero no es suficiente.

A partir de entonces el récord se ha ido batiendo continuamente hasta llegar a diciembre de 2005 en el que se obtuvo el que hasta la fecha es el mayor número primo conocido. Este ha sido descubierto por una pareja de científicos norteamericanos, los doctores Curtis Cooper y Steven Boone, y posee un total de 9.152.052 cifras, con lo que se han acercado enormemente a los diez millones de cifras que es la meta para ganar los 100.000 $ destinados a quienes lo consigan. El número encontrado es el 43º primo de Mersenne conocido hasta ahora y viene dado por: $2^{30402457}-1$.

Actualmente, los números primos se usan en la creación de sistemas de seguridad para computadoras: cuanto más altos son, más seguridad ofrecen. La dificultad de encontrarlos es que entre un número primo y otro no existe un intervalo previsible, por lo cual la búsqueda de los mismos ha intrigado a matemáticos de todas las épocas. Sin embargo, este reciente descubrimiento no podría ser utilizado por una computadora casera actual, que necesitaría cientos de años para poder calcularlo. Cooper y Boone pertenecen a un grupo virtual mundial conocido como GIMPS (Great Internet Mersenne Prime Search o gran búsqueda de primos Mersenne por Internet) que convoca a unos 200.000 informáticos independientes, dispuestos a donar el tiempo libre de sus computadoras para realizar este tipo de cálculos.