Escola Secundária da Sé-Lamego

Ficha de Trabalho de Matemática

26/10/99 ***Números primos e a Internet*** **7.º Ano**

Nome: _____ N.º:____ Turma: ___

O Trabalho

1. Verifica se o número primo $2^{2976221}-1$, referido no livro de texto como o maior número primo conhecido até 24 de Agosto de 1997, é presentemente o maior número primo conhecido.

2. Na nota histórica do livro de texto é referido que «Euclides (séc. III ª C.) provou que há uma infinidade de números primos». Descobre essa demonstração e tenta compreendê-la.

3. Refere algumas curiosidades acerca dos números primos.

Algumas pistas para o desenvolvimento do trabalho

1.

Chris Caldwell (caldwell@utm.edu) from chris-caldwell.utm.edu at 06/03/99 02:57PM
URL
www.mersenne.org
comment
New Mersenne Prime found!! Not yet verified
(Quoted from a note posted by George Woltman to the Mersenne list on june 1, 1999)
The 38th Mersenne prime was *probably* discovered today. The exponent is in the 6,000,000s (the prime is in the neighborhood of 2,000,000 digits). The discoverer is a member of the top 200 contributors according to http://www.mersenne.org/top.htm
As was agreed after the last prime was discovered, I'm announcing the news to this mailing list immediately. When the prime is properly verified and published, then I'll announce the exact exponent. This process was agreed to as a compromise in keeping everyone informed, yet minimizing any chance of the news prematurely leaking to the press. And now the bad news. Since the EFF award requires publication of the result in a refereed academic journal, the publication process will take longer than normal. It could be a few months.

http://www.utm.edu/cgi-bin/caldwell/bubba/research/primes/cgi/news/

GIMPS Finds First Multi-Million-Digit Prime, Stakes Claim to $50,000 EFF Award. $2^{6,972,593}$-1 is now the Largest Known Prime.

ORLANDO, Florida, June 30, 1999 -- Nayan Hajratwala, a participant in the Great Internet Mersenne Prime Search (GIMPS), has discovered the first known 2 million-digit prime number using software written by George Woltman and the distributed computing technology and services of Scott Kurowski's company, Entropia.com, Inc. The prime number, $2^{6,972,593}$-1, contains 2,098,960 digits qualifying for the $50,000 prize offered by the Electronic Frontier Foundation (EFF). An article is being submitted to an academic journal for consideration.

The new prime number, discovered on June 1st, is one of a special class of prime numbers called Mersenne primes. This is only the 38th known Mersenne prime. Nayan used a 350 MHz Pentium II IBM Aptiva computer running part-time for 111 days to prove the number prime. Running uninterrupted it would take about three weeks to test the primality of this number. Richard Crandall, whose faster algorithms helped prove the number prime, has a poster that displays this huge number for sale at http://www.perfsci.com.

http://www.utm.edu/research/primes/notes/6972593/PressAnnouncement.html

The Oregonian
THE FULL STORY

Prime-number coup let's consultant pocket another number: $50,000

Nayan Hajratwala gets a prize after his computer discovers the 38th Mersenne
Wednesday, July 7, 1999

By Ruth Bennett of The Oregonian staff
Call it the rewards of time management.

Nayan Hajratwala, a technology consultant at PricewaterhouseCoopers in Plymouth, Mich., parlayed the microseconds between mouse clicks and the dull moments that others trickle away unprofitably in screen savers into $50,000 -- or, as he puts it, into a nice home theater system. And just in time for his 26th birthday.

Hajratwala's computer, a 350 MHz Pentium II IBM Aptiva, discovered the 38th Mersenne prime number on June 1, using an algorithm developed by Reed College professor Richard Crandall. The identity of the number, confirmed three weeks later, has now been released: at 2 to the 6,972,593 power -1, it contains 2,098,960 digits.

"It didn't require any effort on my part," Hajratwala said. His computer is hooked up to PrimeNet, a server operated by Entropia.com, which transforms the idle time of more than 21,500 personal and business machines into usable computing power for various projects. The volunteer network performs 720 billion calculations per second, according to Entropia.com's founder, Scott Kurowski. If the computing time had to be purchased commercially, he estimates it would cost between $182,000 and $486,000 a day.

Hajratwala has participated in the Great Internet Mersenne Prime Search (GIMPS), one of PrimeNet's projects, since February 1998. PrimeNet sends his home computer large numbers, which his machine sets about factoring in its spare time. It took 111 days of part-time processing to discover that the winning candidate had no other factors besides itself and one -- in other words, it was prime.

The prize money is donated by the Electronic Frontier Foundation, an Internet civil liberties group promoting the type of distributed or cooperative computing network offered by Entropia.com. The next award the foundation will give is $100,000, to be claimed by the discoverer of a 10 million digit prime number, a task that Kurowski characterizes as 125 times more difficult than finding the current record-holding number.

No prize had been offered when Hajratwala began his part in the search. Mainly, he says, it was something to do for fun. Although, he said, "prime numbers are somewhat interesting," the foremost draw was the distributed computing concept, related to Hajratwala's professional interests. The money, he said "is just a nice bonus."

Hajratwala downplays his role in mathematical history. "I just happened to be the right one. It's almost like a lottery."

Such modesty, however, doesn't diminish his enthusiasm for the hunt for the next large prime.

"The machine is running as we speak," he said.

---

http://www.oregonlive.com/news/99/07/st070731.html

On 1 June 1999, the team of Nayan Hajratwala, George Woltman, Scott Kurowski et. al. discovered a new record prime: $2^{6972593}-1$. This is the 38th *known* Mersenne prime (there may be smaller ones as not all previous exponents have been checked). This is GIMPS fourth record in four year!

Hajratwala found this prime using a program written by Woltman linked to the GIMPS internet database via Scott Kurowski's PrimeNet. Hajratwala, a Price Waterhouse employee in Plymouth, Michigan, is one of about 12000 individuals involved in GIMPS: the **G**reat **I**nternet **M**ersenne **P**rime **S**earch launched by Woltman in early 1996. GIMPS offers free software (and source code) for personal computer owners to use in searching for big prime numbers.

Hajratwala's home machine, a 350 MHz Aptiva, took 111 days of idle time to find this prime. His machine could have found it in 3 weeks if run full time. The primality of this number was first verified by David Willmore using a program written by Ernst Mayer on a 500 MHz Alpha workstation (the computation took two weeks). See our page on this number for more information.

prime	digits	who	when	reference
$2^{6972593}-1$	2098960	Hajratwala, Woltman, Kurowski & GIMPS	1999	(notes)
$2^{3021377}-1$	909526	Clarkson, Woltman, Kurowski & GIMPS	1998	(notes)
$2^{2976221}-1$	895932	Spence, Woltman & GIMPS	1997	(notes)
$2^{1398269}-1$	420921	Armengaud, Woltman & GIMPS	1996	(notes)
$2^{1257787}-1$	378632	Slowinski & Gage	1996	(notes)
$2^{859433}-1$	258716	Slowinski & Gage	1994	
$2^{756839}-1$	227832	Slowinski & Gage	1992	[Peterson92]
$302627325\cdot2^{530101}+1$	159585	Nash, Dunaieff, Burrowes, Jobling & Gallot	1999	
$481899\cdot2^{481899}+1$	145072	Morii & Gallot	1998	
$3\cdot2^{382449}+1$	115130	Cosgrave & Gallot	1999	

http://www.utm.edu/research/primes/largest.html#lists

2.

Um pouco sobre números primos

Nem precisamos dizer que primos são números que só são divisíveis, com resultado, inteiro, por si mesmo e pela unidade.
O interessante é observar que os números primos não são igualmente distribuídos, ou melhor, quanto mais se sobe em valor, mais raros vão ficando os mesmos. Assim, alguém poderia pensar que haverá um ponto limite, isto é, o *maior primo*.
Entretanto, pode-se demonstrar que os primos também são infinitos. Segue a prova mais comum (por absurdo):
Suponhamos que o tal do *maior primo* exista. Então haverá um número **n** finito de primos e podemos representá-los por: **P1, P2, P3 ..... Pn-1, Pn** onde **Pn** seria o maior primo e **P1 = 2**.
Agora, multiplicamos todos eles e chamamos o resultado de **M**, isto é:
M = P1 . P2 . P3 ..... Pn-1 . Pn
Como **Pn** é o maior primo, qualquer número maior que ele não será primo. Assim **M** e **M-1** não serão primos. Portanto deverá haver um determinado primo **Pi** que divide **M-1** e, então, podemos escrever:
(M-1) / Pi = M/Pi + 1/Pi e, nesta equação, temos o absurdo:
(M-1)/Pi é inteiro, conforme já dito
M/Pi é inteiro, pois **M** é o produto dos primos
1/Pi é fracionário, pois **Pi >= 2**
Ora, um número inteiro não pode ser igual à soma de outro inteiro mais uma fração. Então a hipótese do maior primo é falsa.
Que achou? Notou que, para esta demonstração, é preciso supor que todo número não primo tem, pelo menos, um divisor primo maior do que 1? Você pode provar isto? Então escreva-nos.

http://users.provider.com.br/mas/Algomais.htm#Primos

Demostración de Euclides de que hay infinitos primos...

La demostración de que hay una infinidad de primos se remonta a Euclides, y es uno de los argumentos clásicos de la matemática. Inicialmente, Euclides asume que hay una lista finita de números primos conocidos, y entonces demuestra que tiene que existir un número infinito de adiciones a esta lista. Hay N números primos en la lista finita de Euclides, los cuales son etiquetados P1, P2, P3, ... Pn. Euclides entonces puede generar un nuevo número Qa tal que:

Qa=(P1 x P2 x P3 x ... x Pn) + 1

Este nuevo número, Qa, o bien es primo o bien no es primo. Si es primo, entonces hemos conseguido de generar otro primo más grande, y por tanto nuestra lista original de primos no era completa. De otro modo, si Qa no es primo, entonces será perfectamente divisible por algún primo. Y este número primo no puede ser ninguno de los primos anteriores conocidos, porque la división de Qa por cualquiera de los primos conocidos anteriormente inevitablemente dejará como resta 1. Por tanto, es necesario que haya otro primo, que podemos etiquetar Pn+1.

Ahora hemos llegado a la situación en la cual o bien Qa es un nuevo primo o bien tenemos otro primo nuevo, Pn+1. En cualquier de los dos casos hemos añadido otro número primo en nuestra lista. Ahora podemos de repetir el proceso, añadiendo nuestro nuevo primo (Pn+1 o Qa) en nuestra lista, y generar otro número Qb. O bien este nuevo número volverá a ser otro nuevo primo, o hay otro número

primo, Pn+2, que no es de nuestra lista de primos conocidos. El resultado de este argumento es que, por larga que sea nuestra lista de números primos, siempre es posible encontrar otro nuevo. Por tanto, la lista de primos es inacabable e infinita.

http://www.geocities.com/CapeCanaveral/Launchpad/2208/curiositats.html#Demo

Prime Numbers

One of the most important and beautiful fields of mathematics is number theory - the study of numbers and their properties. Despite the fact that mathematicians have been studying numbers for as long as humans have been able to count, the field of number theory is far from being outdated; some of the most exciting and important problems in mathematics today have to do with the study of numbers. In particular, prime numbers are of great interest.

Definition: A number p is prime if it is a positive integer greater than 1 and is divisible by no other positive integers other than 1 and itself.

Positive integers that aren't prime are called composite integers.

Examples: 2,3, and 5 are prime. 6 is composite.

All positive integers n have at least one prime divisor: if n is prime, then it is its own prime divisor. If n is composite, and one factors it completely, one will have reduced n to prime factors.

Examples: 6=3*2, 18=3*3*2, 48=6*8=2*3*2*2*2

The following theorem was proved eloquently by Euclid.

Theorem: There are infinitely many prime numbers.

Proof:
Suppose the opposite, that is, that there are a finite number of prime numbers. Call them p_1, p_2, p_3, p_4,....,p_n. Now consider the number

$(p_1*p_2*p_3*...*p_n)+1$

Every prime number, when divided into this number, leaves a remainder of one. So this number has no prime factors (remember, by assumption, it's not prime itself). This is a contradiction. Thus there must, in fact, be infinitely many primes.

So, that proves that we'll never find all of the prime numbers because there's an infinite number of them. But that hasn't stopped mathematicians from looking for them, and for asking all kinds of neat questions about prime numbers.

http://forum.swarthmore.edu/~isaac/problems/prime1.html

3.

iWorld - miércoles, 4 de febrero de 1998

2^3021377-1: Nuevo récord para el procesamiento distribuido en Internet

El número 2 elevado a 3.021.377, menos uno [2^3021377-1] ha pasado a la lista de los récords como el mayor número primo conocido en la actualidad (sólo divisible por sí mismo y la unidad). Este hecho no pasaría de ser una anécdota matemática si no fuera porque para encontrarlo se han usado, en vez de superordenadores, miles de ordenadores personales conectados a través de Internet en lo que se denomina «procesamiento distribuido».

Un Pentium 200 MHz, perteneciente a Roland Clarkson, un estudiante de 19 años de Norwalk, California, encontró el trigesimoséptimo número primo de Mersenne (una forma especial de estos números, relativamente fáciles de computar). Es el mayor conocido hasta la fecha, con 909.526 dígitos de longitud.

Lo importante es que el Pentium de Clarkson no estaba solo. Empleando el software de cálculo y conectividad desarrollado por George Woltman y Scott Kurowski, esa máquina formaba parte de un grupo global de más de 4.000 voluntarios que participaban en el proyecto GIMPS (Great Internet Mersenne Prime Search, Gran Búsqueda de Primos de Mersenne mediante Internet). GIMPS es un proyecto (entre otros similares) que hace uso de un sistema de procesamiento distribuido gracias a la potencia de Internet para conectar ordenadores personales con una finalidad común: generar una enorme potencia de cálculo para realizar una tarea concreta.

Un servidor denominado PrimeNet distribuye el trabajo a toda la Red, y recoge los cálculos de las miles de copias del programa que corren en los ordenadores personales de usuarios de todo el mundo, operando en la práctica como un superordenador masivamente paralelo. En un día normal, PrimeNet tiene la misma potencia de cálculo que un PC convencional funcionando durante todo un año. La potencia de PrimeNet crece cada vez que alguien se añade al grupo. El servidor controla los diferentes estados de las pruebas, el tiempo empleado y las personas y ordenadores que lo realizan. Internet hace posible que estas complejas tareas sean transparentes para los usuarios, que ejecutan el programa en ratos libres, cuando no usan las máquinas, como tarea de fondo e incluso como salvapantallas, lo que no afecta a su rendimiento normal.

Descubrir números primos del tamaño de 2^3021377-1 hubiera sido imposible hace unos años. GIMPS es un ejemplo de lo que se puede conseguir cuando un gran número de personas, usando Internet, se coordinan en pro de una tarea. El nuevo primo de Mersenne, el número 37 de la lista, fue verificado posteriormente de forma independiente en un superordenador Cray por David Slowinski, descubrir de siete de estos números entre 1979 y 1996.

La búsqueda de nuevos números primos de Mersenne continúa: puede haber algunos más pequeños y muchos más grandes todavía por descubrir. Cualquiera que tenga un ordenador personal razonablemente potente puede unirse al proyecto GIMPS para participar. En la página web del grupo se encuentran todas las instrucciones y software (gratuito) necesario para ponerse en marcha.

Utilidad del procesamiento distribuido en Internet

Mucha gente se pregunta para qué sirven este tipo de hazañas computacionales, aparentemente poco prácticas. En realidad son los efectos colaterales los que realmente importan, más que los números primos en sí o el mérito de encontrarlos. En el caso de GIMPS, como en el de otros proyectos distribuidos similares (por ejemplo, Distributed.net) se han realizado algunos avances significativos.

- Avances en procesamiento distribuido. Se ha demostrado que Internet es un buen entorno para sacar partido a la potencia no utilizada (tiempo libre) de miles de máquinas conectadas a la Red. Se cree que algún día será posible llevar a cabo proyectos que hoy en día requieren superordenadores, reemplazándolos por un gran número de pequeños ordenadores convencionales en red.

- Perfeccionamiento de métodos matemáticos. Al buscar la optimización en los cálculos a realizar para comprobar los números primos, Richard Crandall descubrió un método que duplica la velocidad de cálculo de algunas transformadas rápidas de Fourier, técnica que se usa en multitud de aplicaciones científicas y dispositivos electrónicos.

- Los profesores de escuelas elementales y de enseñanza primaria usan proyectos como GIMPS para llamar la atención de los estudiantes por la matemática. Los estudiantes, usando software gratuito, contribuyen a la investigación matemática de una forma concreta.

- Históricamente, la búsqueda de números primos de Mersenne (al igual que otras como el cálculo de los dígitos decimales de Pi) se ha empleado para comprobar el hardware de los nuevos ordenadores. El software del proyecto GIMPS ha identificado problemas de hardware en muchos PC. Intel actualmente usa partes del software GIMPS para encontrar defectos de fabricación en sus Pentium II y Pentium Pro antes de ponerlos a la venta.

GIMPS (www.mersenne.org/prime.htm)

Distributed.net (www.distributed.net)

http://www.idg.es/iworld/actualidad/19980204y.asp

Early History

Many early writers felt that the numbers of the form 2^n-1 were prime for *all* primes *n*, but in 1536 Hudalricus Regius showed that 2^{11}-1 = 2047 was not prime (it is 23·89). By 1603 Pietro Cataldi had correctly verified that 2^{17}-1 and 2^{19}-1 were both prime, but then incorrectly stated 2^n-1 was also prime for 23, 29, 31 and 37. In 1640 Fermat showed Cataldi was wrong about 23 and 37; then Euler in 1738 showed Cataldi was also wrong about 29. Sometime later Euler showed Cataldi's assertion about 31 was correct.
Enter French monk Marin Mersenne (1588-1648). Mersenne stated in the preface to his *Cogitata Physica-Mathematica* (1644) that the numbers 2^n-1 were prime for

n = 2, 3, 5, 7, 13, 17, 19, **31, 67, 127 and 257**

and were composite for all other positive integers $n < 257$. Mersenne's (incorrect) conjecture fared only slightly better than Regius', but still got his name attached to these numbers.

Definition: When 2^n-1 is prime it is said to be a **Mersenne prime**

It was obvious to Mersenne's peers that he could not have tested all of these numbers (in fact he admitted as much), but they could not test them either. It was not until over 100 years later, in 1750, that Euler verified the next number on Mersenne's and Regius' lists, 2^{31}-1, was prime. After another century, in 1876, Lucas verified 2^{127}-1 was also prime. Seven years later Pervouchine showed 2^{61}-1 was prime, so Mersenne had missed this one. In the early 1900's Powers showed that Mersenne had also missed the primes 2^{89}-1 and 2^{107}-1. Finally, by 1947 Mersenne's range, $n \leq 258$, had been completely checked and it was determined that the correct list is:

n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 and 127.

http://www.utm.edu/research/primes/mersenne.shtml

Why do people look for these big primes?

"Why?" we are often asked, "why would anyone want to find a prime that big?"" I often now answer with "did you ever collect anything?"" or "did you ever try to win a competition?"" Much of the answer for why we collect large primes is the same as why we might collect other rare items. Below I will present a more complete answer divided into several parts.

1. Tradition!
2. For the by-products of the quest
3. People collect rare and beautiful items

4. For the glory!
5. To test the hardware
6. To learn more about their distribution

This does not exhaust the list of reasons, for example some might be motivated by primary research or a need for publication. Many others just hate to see a good machine wasting cycles (sitting idle or running an inane screen saver). Perhaps these arguments will not convince you. If not, just recall that the eye may not see what the ear hears, but that does not reduce the value of sound. There are always melodies beyond our grasp. (*)

.....

http://www.utm.edu/research/primes/notes/faq/why.html

How long is the prime $2^{6972593}$-1?

[Home Page || Largest | Mersenne | FAQ | Proofs | Lists | Proving]

If we were to print all of the 2098960 decimal digits of the prime $2^{6972593}$-1 in a single line of type, how long would it be? Obviously it depends on the size of the font. You select the font size and I'll tell you how long. 10 and 12 point fonts are standard size fonts in books and articles.

10 | How Long?

If you use a 10 point font then the prime is...		
	without commas	with commas
(US)	4 miles 3173 feet and 6 inches	6 miles 711 feet and 4 inches
(metric)	7404 meters	9872 meters
...and the associated perfect number is...		
(US)	9 miles and 1067 feet	12 miles 1422 feet and 8 inches
(metric)	14809 meters	19745 meters

http://www.utm.edu/cgi-bin/caldwell/primes/HowLong.cgi/6972593/

$2^{6972593}$-1

The complete decimal expansion

- text file (2 meg) alternate sites:
- New perfect number's complete expansion alternate sites:
- Curt Noll's site which has the expansion in decimal (in three forms) as well as the English name!

http://www.utm.edu/research/primes/notes/6972593/

$2^{6972593}$-1 is prime

$2^{6972593}$-1 is a Mersenne prime.

Landon Curt Noll computed the decimal value of this prime was using calc and the English name for this prime using number.

4.370.757.441.270.813.788.333.232.912.069.460.708.676.247.705.748.

516.066.310.181.318.151.923.248.225.070.653.865.555.856.672.485.830.590.030.

270.826.993.209.390.672.909.069.784.256.394.631.416.264.579.463.761.570.844.

689.139.643.362.319.751.312.366.709.949.001.656.294.573.733.085.918.183.620.

876.126.580.313.766.242.613.708.591.473.816.297.933.199.276.751.723.653.303.

.....

FALTA UMA IMENSIDÃO de dígitos!

.....

http://reality.sgi.com/chongo/tech/math/prime/merdigit/m6972593/prime-c-e.html

Prime numbers

Prime numbers and their properties were first studied extensively by the ancient Greek mathematicians.

The mathematicians of Pythagoras's school (500 BC to 300 BC) were interested in numbers for their mystical and numerological properties. They understood the idea of primality and were interested in *perfect* and *amicable* numbers.
(A *perfect number* is one whose proper divisors sum to the number itself. e.g. The number 6 has proper divisors 1, 2 and 3 and 1 + 2 + 3 = 6, 28 has divisors 1, 2, 4, 7 and 14 and 1 + 2 + 4 + 7 + 14 = 28.
A *pair of amicable numbers* is a pair like 220 and 284 such that the proper divisors of one number sum to the other and vice versa.)

By the time Euclid's *Elements* appeared in about 300 BC, several important results about primes had been proved. In Book IX of the *Elements*, Euclid proves that there are infinitely many prime numbers. This is one of the first proofs known which uses the method of contradiction to establish a result. Euclid also gives a proof of the Fundamental Theorem of Arithmetic: Every integer can be written as a product of primes in an essentially unique way.

Euclid also showed that if the number 2 - 1 is prime then the number 2 (2 - 1) is a perfect number. The mathematician Euler (much later in 1747) was able to show that *all* even perfect numbers are of this form. It is not known to this day whether there are any *odd* perfect numbers.

In about 200 BC the Greek Eratosthenes devised an *algorithm* for calculating primes called the *Sieve of Eratosthenes*.

There is then a long gap in the history of prime numbers during what is usually called the Dark Ages.

The next important developments were made by Fermat at the beginning of the 17th Century. He proved a speculation of Albert Girard that every prime number of the form 4 n + 1 can be written in a unique way as the sum of two squares and was able to show how any number could be written as a sum of four squares.
He devised a new method of factorising large numbers which he demonstrated by factorising the number 2027651281 = 44021 x 46061.
.....
.....
http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Prime_numbers.html

The First 1,000 Primes

(the 1,000th is 7919)
For more information on primes see http://www.utm.edu/research/primes

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167
173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347
349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503 509 521 523
541 547 557 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691 701 709 719 727
733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937
941 947 953 967 971 977 983 991 997 1009 1013 1019 1021 1031 1033 1039 1049 1051 1061 1063 1069 1087 1091 1093 1097
1103 1109 1117 1123 1129 1151 1153 1163 1171 1181 1187 1193 1201 1213 1217 1223 1229 1231 1237 1249 1259 1277 1279
1283 1289 1291 1297 1301 1303 1307 1319 1321 1327 1361 1367 1373 1381 1399 1409 1423 1427 1429 1433 1439 1447 1451
1453 1459 1471 1481 1483 1487 1489 1493 1499 1511 1523 1531 1543 1549 1553 1559 1567 1571 1579 1583 1597 1601 1607
1609 1613 1619 1621 1627 1637 1657 1663 1667 1669 1693 1697 1699 1709 1721 1723 1733 1741 1747 1753 1759 1777 1783
1787 1789 1801 1811 1823 1831 1847 1861 1867 1871 1873 1877 1879 1889 1901 1907 1913 1931 1933 1949 1951 1973 1979
1987 1993 1997 1999 2003 2011 2017 2027 2029 2039 2053 2063 2069 2081 2083 2087 2089 2099 2111 2113 2129 2131 2137
2141 2143 2153 2161 2179 2203 2207 2213 2221 2237 2239 2243 2251 2267 2269 2273 2281 2287 2293 2297 2309 2311 2333
2339 2341 2347 2351 2357 2371 2377 2381 2383 2389 2393 2399 2411 2417 2423 2437 2441 2447 2459 2467 2473 2477 2503
2521 2531 2539 2543 2549 2551 2557 2579 2591 2593 2609 2617 2621 2633 2647 2657 2659 2663 2671 2677 2683 2687 2689
2693 2699 2707 2711 2713 2719 2729 2731 2741 2749 2753 2767 2777 2789 2791 2797 2801 2803 2819 2833 2837 2843 2851
2857 2861 2879 2887 2897 2903 2909 2917 2927 2939 2953 2957 2963 2969 2971 2999 3001 3011 3019 3023 3037 3041 3049
3061 3067 3079 3083 3089 3109 3119 3121 3137 3163 3167 3169 3181 3187 3191 3203 3209 3217 3221 3229 3251 3253 3257
3259 3271 3299 3301 3307 3313 3319 3323 3329 3331 3343 3347 3359 3361 3371 3373 3389 3391 3407 3413 3433 3449 3457
3461 3463 3467 3469 3491 3499 3511 3517 3527 3529 3533 3539 3541 3547 3557 3559 3571 3581 3583 3593 3607 3613 3617
3623 3631 3637 3643 3659 3671 3673 3677 3691 3697 3701 3709 3719 3727 3733 3739 3761 3767 3769 3779 3793 3797 3803
3821 3823 3833 3847 3851 3853 3863 3877 3881 3889 3907 3911 3917 3919 3923 3929 3931 3943 3947 3967 3989 4001 4003
4007 4013 4019 4021 4027 4049 4051 4057 4073 4079 4091 4093 4099 4111 4127 4129 4133 4139 4153 4157 4159 4177 4201

4211 4217 4219 4229 4231 4241 4243 4253 4259 4261 4271 4273 4283 4289 4297 4327 4337 4339 4349 4357 4363 4373 4391 4397 4409 4421 4423 4441 4447 4451 4457 4463 4481 4483 4493 4507 4513 4517 4519 4523 4547 4549 4561 4567 4583 4591 4597 4603 4621 4637 4639 4643 4649 4651 4657 4663 4673 4679 4691 4703 4721 4723 4729 4733 4751 4759 4783 4787 4789 4793 4799 4801 4813 4817 4831 4861 4871 4877 4889 4903 4909 4919 4931 4933 4937 4943 4951 4957 4967 4969 4973 4987 4993 4999 5003 5009 5011 5021 5023 5039 5051 5059 5077 5081 5087 5099 5101 5107 5113 5119 5147 5153 5167 5171 5179 5189 5197 5209 5227 5231 5233 5237 5261 5273 5279 5281 5297 5303 5309 5323 5333 5347 5351 5381 5387 5393 5399 5407 5413 5417 5419 5431 5437 5441 5443 5449 5471 5477 5479 5483 5501 5503 5507 5519 5521 5527 5531 5557 5563 5569 5573 5581 5591 5623 5639 5641 5647 5651 5653 5657 5659 5669 5683 5689 5693 5701 5711 5717 5737 5741 5743 5749 5779 5783 5791 5801 5807 5813 5821 5827 5839 5843 5849 5851 5857 5861 5867 5869 5879 5881 5897 5903 5923 5927 5939 5953 5981 5987 6007 6011 6029 6037 6043 6047 6053 6067 6073 6079 6089 6091 6101 6113 6121 6131 6133 6143 6151 6163 6173 6197 6199 6203 6211 6217 6221 6229 6247 6257 6263 6269 6271 6277 6287 6299 6301 6311 6317 6323 6329 6337 6343 6353 6359 6361 6367 6373 6379 6389 6397 6421 6427 6449 6451 6469 6473 6481 6491 6521 6529 6547 6551 6553 6563 6569 6571 6577 6581 6599 6607 6619 6637 6653 6659 6661 6673 6679 6689 6691 6701 6703 6709 6719 6733 6737 6761 6763 6779 6781 6791 6793 6803 6823 6827 6829 6833 6841 6857 6863 6869 6871 6883 6899 6907 6911 6917 6947 6949 6959 6961 6967 6971 6977 6983 6991 6997 7001 7013 7019 7027 7039 7043 7057 7069 7079 7103 7109 7121 7127 7129 7151 7159 7177 7187 7193 7207 7211 7213 7219 7229 7237 7243 7247 7253 7283 7297 7307 7309 7321 7331 7333 7349 7351 7369 7393 7411 7417 7433 7451 7457 7459 7477 7481 7487 7489 7499 7507 7517 7523 7529 7537 7541 7547 7549 7559 7561 7573 7577 7583 7589 7591 7603 7607 7621 7639 7643 7649 7669 7673 7681 7687 7691 7699 7703 7717 7723 7727 7741 7753 7757 7759 7789 7793 7817 7823 7829 7841 7853 7867 7873 7877 7879 7883 7901 7907 7919 end.

http://www.utm.edu/research/primes/lists/small/1000.txt

Números primos

Los números primos siempre han sido unos números muy discutidos. Algunos matemáticos han intentado estudiar el por qué del orden que siguen, sin llegar a conclusiones. Aquí pretendemos hacer un exhaustivo estudio de los números primos hasta el 2.000.000, contando los porcentajes que salen de sus terminaciones.

Para esto hemos calculado, en primicia mundial, todos los números primos hasta el 2.000.000 (148.933) y los porcentajes de los que acaban en 1, 3, 7, 9 (a parte de estos hay el 2 y el 5).

Carles Pina i Estany (cpina@linuxfan.com)
Manresa, Barcelona, España

Menú

¿Será primo?

Si te interesa el tema, pon esta página en los bookmarks y envia la URL por mail a tus amigos, te lo agradecerán.
Si tienes alguna duda, comentario, crítica, etc. no dudes en escribirme a cpina@linuxfan.com

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

Finding Very Small Primes

For finding all the small primes, say all those less than 10,000,000; one of the most efficient ways is by using **the Sieve of Eratosthenes** (ca 240 BC):

> Make a list of all the integers less than or equal to n (greater than one) and strike out the multiples of all primes less than or equal to the square root of n, then the numbers that are left are the primes. (See also our glossary page.)

For example, to find all the odd primes less than or equal to 100: list the odd numbers from 3 to 100 (why even list the evens?) The first number is 3 so it is the first odd prime--cross out all of its multiples. Now the first number left is 5, the second odd prime--cross out all of its multiples. Repeat with 7 and then since the first number left, 11, is larger than the square root of 100, all of the numbers left are primes. This method is so fast that there is no reason to store a large list of

primes on a computer--an efficient implementation can find them faster than a computer can read from a disk. Bressoud has a pseudocode implementation of this algorithm [Bressoud89, p19] and Riesel a PASCAL implementation [Riesel94, p6]. We also have a page of implementations.
To find individual small primes **trial division** works okay. Just divide by all the primes less than the square root. For example, to show is 211 is prime, just divide by 2, 3, 5, 7, 11, and 13. (Pseudocode [Bressoud89, pp21-22], PASCAL [Riesel94, pp7-8].)
Rather than divide by just the primes, it is sometimes more practical to divide by 2, 3 and 5; then by all the numbers congruent to 1, 7, 11, 13, 17, 19, 23, and 29 modulo 30--again stopping when you reach the square root. This type of factorization is sometimes called **wheel factorization**.
Suppose *n* has twenty digits, then it is getting impractical to divide by the primes less than its square root, and it is impossible if *n* has two hundred digits--so we need much faster tests. We discuss several such tests below.

http://www.utm.edu/research/primes/prove/prove2.html

Chris Caldwell (caldwell@utm.edu) from chris-caldwell.utm.edu at 06/01/99 10:44AM
Title
First occurence of a prime gap larger than 1000
comment
Subject
Thomas R. Nicely and Bertil Nyman have just submitted a new paper on prime gaps to the Mathematics of Computation. From their abstract:

> The interval from 10^15 to 3 x 10^15 is analyzed for first occurrence prime gaps and maximal prime gaps. Thirty-four new first occurrences are found, including three new maximal gaps. The first occurrence of a prime gap of 1000 or greater is found to be the maximal gap of 1132 following the prime 1693182318746371.

The paper can be found at Thomas Nicely's homepage.

http://www.utm.edu/cgi-bin/caldwell/bubba/research/primes/cgi/news/

Chris K Caldwell (caldwell@utm.edu) from ob129.iswt.com at 02/02/98 10:30PM
Title
New Mersenne, 37th and largest yet!
News Item
GIMPS has triumphed again!!!! See this page for more information!!

http://www.utm.edu/cgi-bin/caldwell/bubba/research/primes/cgi/news/

The Great Internet Mersenne Prime Search

http://www.entropia.com/http://www.entropia.com/

Make Math History!!

You could discover one of the most coveted finds in all of Mathematics - a new Mersenne prime number. Join in on this fun, yet serious research project. All you need is a personal computer and a lot of luck.
In addition to the joy of making a mathematical discovery, you **might** win some cash. The Electronic Frontier Foundation is offering a $100,000 award to the first person to discover a ten million digit prime number! See what GIMPS will do if we are lucky enough to find a ten million digit prime.

.....

Last updated: October 4, 1999

http://www.mersenne.org/prime.htm

FREE Software!

Free - you can't beat that price! You need a Pentium computer with Windows 3.1, Windows 95, Windows 98, Windows NT, OS/2, Linux, of FreeBSD. PowerPC owners can also participate. C and Fortran code is available for UNIX users. The FAQ page answers many questions you may have before downloading the software. In case of downloading difficulties, European, Russian, Canadian, and U.S. mirror sites are available.

http://www.mersenne.org/freesoft.htm

The Electronic Frontier Foundation (EFF), the first civil liberties group dedicated to protecting the health and growth of the Internet, is sponsoring cooperative computing awards, with over half a million dollars in prize money, to encourage ordinary Internet users to contribute to solving huge scientific problems.

Through the EFF Cooperative Computing Awards, EFF will confer prizes of:

$50,000 to the first individual or group who discovers
a prime number with at least 1,000,000 decimal digits

$100,000 to the first individual or group who discovers
a prime number with at least 10,000,000 decimal digits

$150,000 to the first individual or group who discovers
a prime number with at least 100,000,000 decimal digits

$250,000 to the first individual or group who discovers
a prime number with at least 1,000,000,000 decimal digits

http://www.eff.org/coop-awards/

O Professor