Els Secrets dels Nombres Primers

El primer més gran del Món!

$$2^{57885161}-1$$

El nombre més gran el qual sabem demostrar que és primer

$$2^{57885161}-1$$

El nombre més gran el qual sabem demostrar que és primer

581887266232246442175100212113232368636370852325421589325781704480584492761707442316428281349423376942979071335489886655517752224731316967316601101080371457923021838436917492197333394648729851218665756323673512565202964097437803696250542088744968273344617858384022131920787583935917496283612402707082209797985800006635414921583881775901175855244421937156984065294070824916668433336287290654803493450648643707818608236480157480359745219707507173734977384814523731184368200564270648717597756654478727288872431916344358766382062118229667496087869810535788260544601094919298182471920835982201714594800354914858410693177101697773656631281661229484707215557966266854716941055601329650332927448761752400534090665613215981324295363545348287526775794185616611330163046727522053003794315781916734410811689902077426244905522416405144627121004481430624576881550456735283818183504195396520995731249226377913834034798484811398338429561975738169909795719648312120188779924256666579294440399570664183761039922888206552449492372168896516376792875366121320482328712573315076376604535941261564769293342771929543146519802037551978248144126543026556679084137083659849957039763812411301935060208612469375104539563868543051406863437928977878036686713967121684883313087697822841916169287312199626810610158398639559691029439851779239402729921189380970540576088779968142355964715311250969549166558947742393502579357098104425910862032972128219793306441515423911098991939979427886345975192725641201184650333340676148782573998479038371240312700333447509945455946437852136913945748122077796193478763163066731335847021918439577616802120061247377392853400841817699231403447635855770653563026194153409946766192861670496579960888267204960758019384784218949053456295699099877089643134340870697323126938069845802671443205595983681514576908873828905683297986620636176211498476939389889353860479590210009108390139929244978462210255274781427403296107975987454098551521592861106597567595475288750192297317589058417805081631684523271610955684657578488603527048636481360738154098160985140027267737061112918416723801649835396499341746978315057896776236721816498126253027402790865019847348177754303185964895031476662136171535912727008563784507197606344663531432323425342607325102341242812572932271391617827771280215924710272482400776920577631166808152141531528142934919630354071454929389638644023323247019498710363335662341775472107388977813647059852864120239575594407334637623354075517360012123250340004310387632655722008052260735884424569576168825458333903596129095161099601952070814924327059656253677571057631264561138164258597051912042362107951507623924738643276079018719892536274884723023844338923508948316548987142560897050867400305312979992267484319349783508312698215233694618637666829074713926175767765539685103941901776771510015052220964026463375177095832062210878945887710951433481731180049461420775486585722243219794969799752974898322476437297618185551060980301879054967333487991621777727038599886744808243314069910187761640920383352895407535183008282726171291463795952657074783078702009434200166180222053283682048232057366819031674789531215940430760964906294297159409961364527227095084236325465587196186021964223959834597554425029281820887488334305329294282242708622122281397257639235936242739008998375867851514611787277117481007475769637027213910738552270680363266487889306634188196964400898981891179715830393827598062506665259086044516822494937745410942833323095203705645658725746141988071724285951

El nombre més gran el qual sabem demostrar que és primer

$1111....^{(57.885.161\ \text{dígits})}...1111$

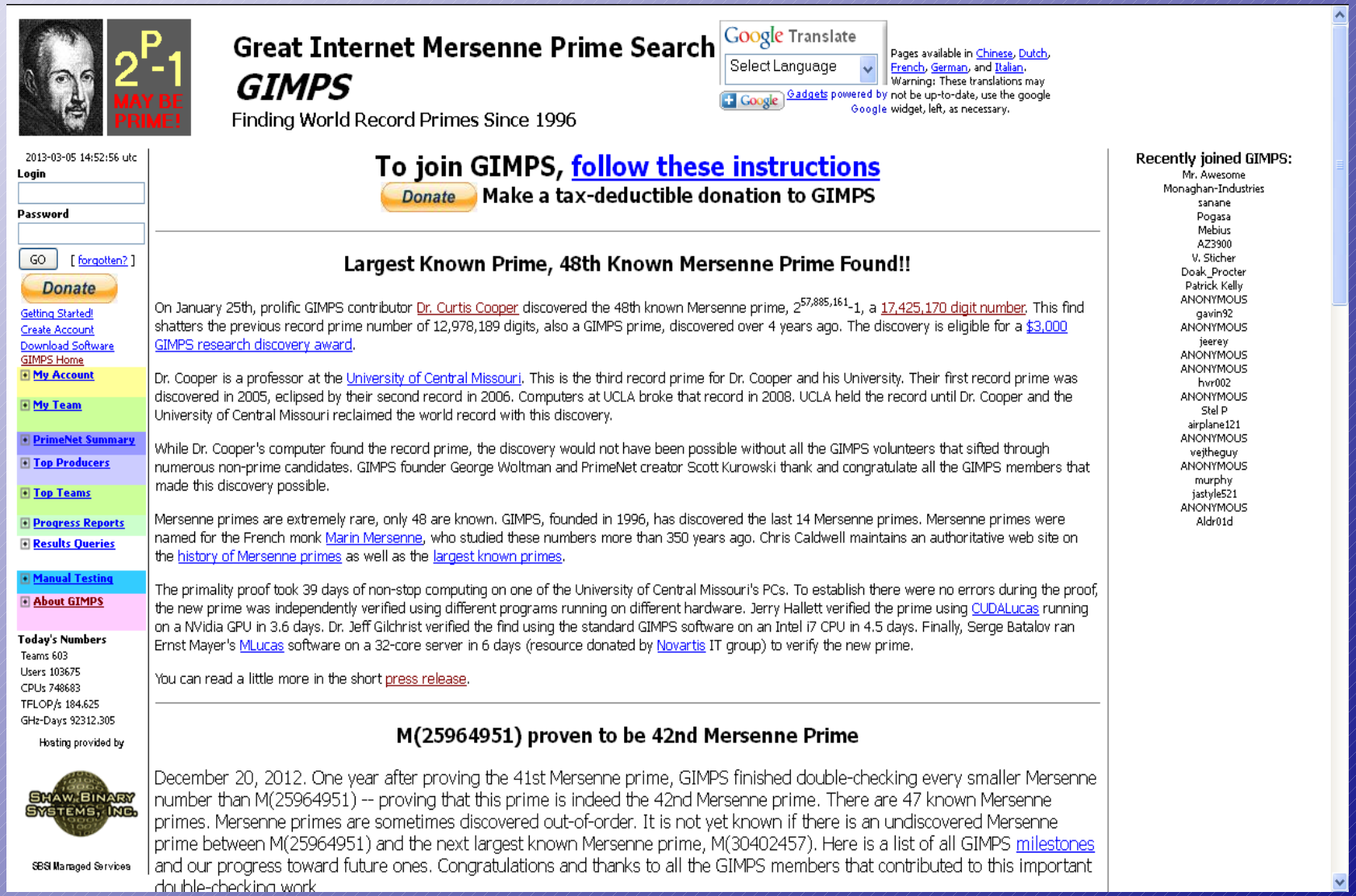
(en base dos)

El nombre més gran el qual sabem demostrar que és primer

Curtis Cooper

Trobat el 25 de Gener a les 23:30:26 UTC

GIMPS


Great Internet Mersenne Prime Search
GIMPS
Finding World Record Primes Since 1996
Google Translate
Select Language
Pages available in Chinese, Dutch, French, German, and Italian.
Warning: These translations may not be up-to-date, use the google Google widget, left, as necessary.
2013-03-05 14:52:56 utc
Login
Password
GO
[forgotten?]
Donate
Getting Started!
Create Account
Download Software
GIMPS Home
My Account
My Team
PrimeNet Summary
Top Producers
Top Teams
Progress Reports
Results Queries
Manual Testing
About GIMPS
Today's Numbers
Teams 603
Users 103675
CPUs 748683
TFLOP/s 184.625
GHz-Days 92312.305
Hosting provided by
SBSI Managed Services
To join GIMPS, follow these instructions
Donate
Make a tax-deductible donation to GIMPS
Largest Known Prime, 48th Known Mersenne Prime Found!!
On January 25th, prolific GIMPS contributor Dr. Curtis Cooper discovered the 48th known Mersenne prime, 2^57,885,161-1, a 17,425,170 digit number. This find shatters the previous record prime number of 12,978,189 digits, also a GIMPS prime, discovered over 4 years ago. The discovery is eligible for a $3,000 GIMPS research discovery award.
Dr. Cooper is a professor at the University of Central Missouri. This is the third record prime for Dr. Cooper and his University. Their first record prime was discovered in 2005, eclipsed by their second record in 2006. Computers at UCLA broke that record in 2008. UCLA held the record until Dr. Cooper and the University of Central Missouri reclaimed the world record with this discovery.
While Dr. Cooper's computer found the record prime, the discovery would not have been possible without all the GIMPS volunteers that sifted through numerous non-prime candidates. GIMPS founder George Woltman and PrimeNet creator Scott Kurowski thank and congratulate all the GIMPS members that made this discovery possible.
Mersenne primes are extremely rare, only 48 are known. GIMPS, founded in 1996, has discovered the last 14 Mersenne primes. Mersenne primes were named for the French monk Marin Mersenne, who studied these numbers more than 350 years ago. Chris Caldwell maintains an authoritative web site on the history of Mersenne primes as well as the largest known primes.
The primality proof took 39 days of non-stop computing on one of the University of Central Missouri's PCs. To establish there were no errors during the proof, the new prime was independently verified using different programs running on different hardware. Jerry Hallett verified the prime using CUDALucas running on a NVidia GPU in 3.6 days. Dr. Jeff Gilchrist verified the find using the standard GIMPS software on an Intel i7 CPU in 4.5 days. Finally, Serge Batalov ran Ernst Mayer's MLucas software on a 32-core server in 6 days (resource donated by Novartis IT group) to verify the new prime.
You can read a little more in the short press release.
M(25964951) proven to be 42nd Mersenne Prime
December 20, 2012. One year after proving the 41st Mersenne prime, GIMPS finished double-checking every smaller Mersenne number than M(25964951) -- proving that this prime is indeed the 42nd Mersenne prime. There are 47 known Mersenne primes. Mersenne primes are sometimes discovered out-of-order. It is not yet known if there is an undiscovered Mersenne prime between M(25964951) and the next largest known Mersenne prime, M(30402457). Here is a list of all GIMPS milestones and our progress toward future ones. Congratulations and thanks to all the GIMPS members that contributed to this important double-checking work.
Recently joined GIMPS:
Mr. Awesome
Monaghan-Industries
sanane
Pogasa
Mebius
AZ3900
V. Sticher
Doak_Procter
Patrick Kelly
ANONYMOUS
gavin92
ANONYMOUS
jeerey
ANONYMOUS
ANONYMOUS
hvr002
ANONYMOUS
Stel P
airplane121
ANONYMOUS
vejtheguy
ANONYMOUS
murphy
jastyle521
ANONYMOUS
Aldr01d

Nombres Primers

Un nombre $p>1$ enter és primer si no és divisible per cap nombre $1<d<p$.

Si un nombre primer p divideix $a \cdot b$, aleshores divideix a o divideix b.

Teorema Fonamental

Tot nombre enter més gran que 1 és producte de nombres primers de manera única.

Primers menors que 1000

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 ...

Hi ha infinits nombres primers

Euclides 300 ac -???

Si $p_1,p_2,\ldots,p_r$ són primers,

el nombre

$N=p_1 \cdot p_2 \cdots p_r+1$

no és divisible per cap dels p_i

Per tant hi ha algun altre primer q dividint N

Com veure si un nombre és primer

Eratòstenes 276 aC-195aC

<u>Garbell d'Eratòstenes</u>

p>1 és primer si no és divisible per cap nombre (primer) menor que $\sqrt{p}$.

(Idea: si $p=a\cdot b$, a i $b<p$, aleshores o $a<\sqrt{p}$ o $b<\sqrt{p}$)

Exemple

97 és primer.

$\sqrt{97}=9'84886...$

2 no divideix 97

3 no divideix 97

5 no divideix 97

7 no divideix 97

109379 és primer

$\sqrt{109379}=330.72496...$

No és divisible per cap dels 66 primers <330.

Un altre exemple

2^{521}-1 és primer

(Robinson, 1952)

Té 157 dígits.

L'arrel quadrada té 78 dígits.

Si fem 1 milió de divisions cada segon, trigaríem 10^{64} anys en acabar.

L'univers té menys de 10^{12} anys.

Impossible

Primers de Mersenne

Martin Mersenne 1588-1648

Primers de la forma $p=2^n-1$.

Condició necessària
Si p és primer, n és primer.

Exemples:n=2,3,5,13,17,...

$2^{11}-1=23\times89$

m nombre perfecte parell

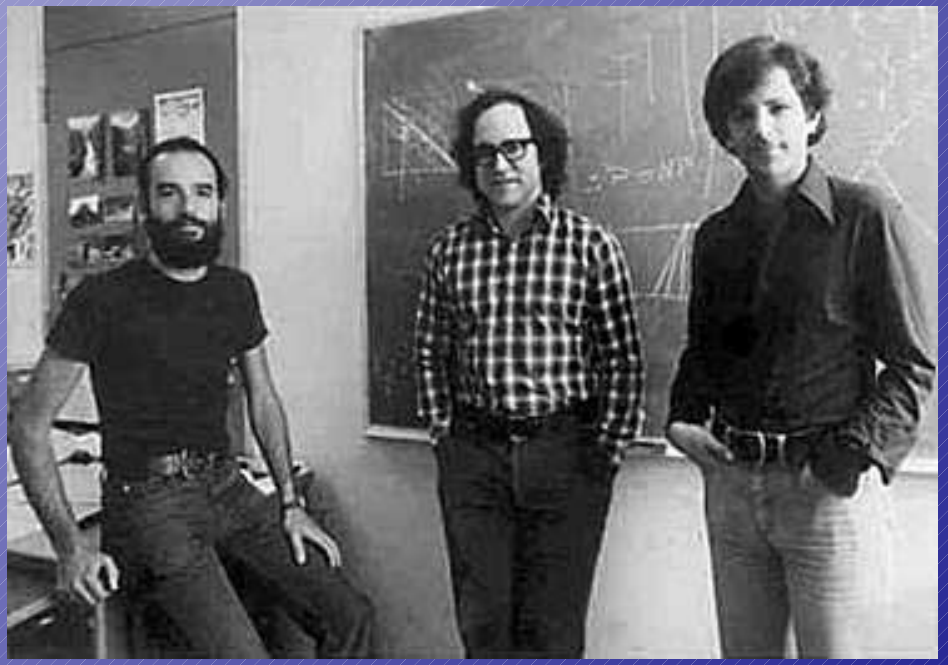
$\updownarrow$

$m=2^{n-1}(2^n-1)$

$2^{3-1}(2^3-1)=28=1+2+4+7+14$

RSA

Quan ens connectem a una pàgina segura fem servir normalment RSA.



RSA=Ron Rivest, Adi Shamir and Leonard Adleman

Utilitza primers amb 500 bits com a mínim.

Com saber que un nombre no és primer

<u>Petit Teorema de Fermat</u>

Si $p>1$ és un nombre primer,

i a és un nombre enter no divisible per p,

aleshores

$a^{p-1}-1$ és divisible per p

Pierre de Fermat 1601-1665

Exemple

$p=2^{523}-1$ no és primer

Prenem $a=3$.

Calculem el residu de dividir $a^{p-1}-1$ entre p.

No és 0. *(0.17 segons)*

Compte! a=2 no funciona

El mètode no ens diu els factors.

Cal saber calcular de manera ràpida i eficient el reste de dividir $a^{p-1}-1$ entre p.

p=160188778313202118610543685368878688932828701136501444932217468039063·
17141769186124919812831709653432211647616505671863034509489662036786000648697710185950408 9

L'aritmètica dels rellotges

Per calcular el reste de dividir $a \cdot b$ entre n,

podem calcular els restes r_a i r_b de dividir a i b entre n,

multiplicar-los $c=r_a \cdot r_b$,

i calcular el reste r de dividir c entre n.

Exemple

a=97, b=117, n=17

$r_a=12$ $r_b=15$

$c=180$

$r=10$

L'exponenciació binaria

$p=2^{523}-1$ $a=3$

Volem calcular el residu de dividir

$a^{p-1}-1$ entre p

Idea:

$p+1=2^{523}$

$a^{p+1}=(\ldots(((a^2)^2)^2)^2\ldots^{(523\ vegades)}\ldots)^2$

(cada operació $(-)^2$ després calculem el residu)

Ho fem amb unes 1000 "operacions"

1000 ≈ dos vegades el nombre de xifres.

Temps exponencial i polinomial

- Temps polinomial
- Un algorisme aplicat a un número que triga un temps que és funció polinomial de les xifres del número.
- Si doblem el número de xifres, es multiplica el temps per una constant

- Temps exponecial
- Un algorisme aplicat a un número que triga un temps que és funció polinomial del número.
- Si doblem el número de xifres, s'eleva el temps per una constant

Què fa el RSA

És un algorisme de clau pública.

Clau pública≡Candau

Es basa en que hi ha funcions que són fàcils de fer i difícils de desfer.

Clau privada≡Clau.

Multiplicar↔Factoritzar

RSA i els secrets

RSA funciona gràcies a que

Multiplicar és polinomial.

Factoritzar "sembla" exponecial.

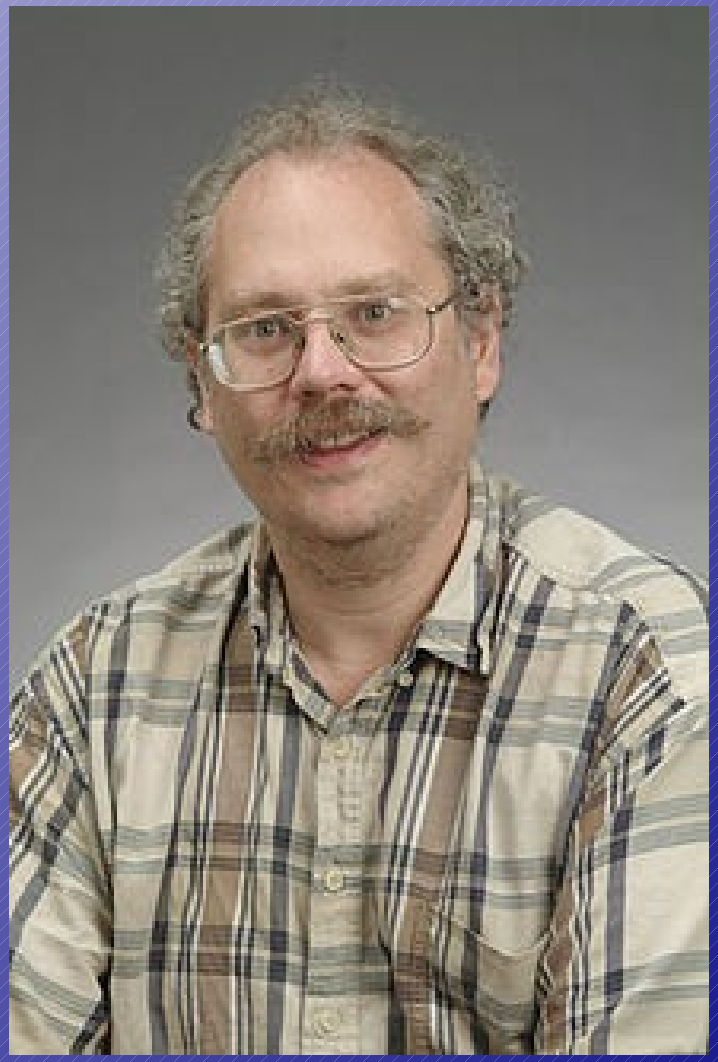
(fins ara ningú ha trobat un algorisme polinomial)

La primalitat és polinomial.

(demostrat el 6 d'agost del 2002)

RSA i la Física Quàntica

- Si poden construir ordinadors quàntics prou grossos, es pot factoritzar en temps polinomial.
- Peter Shor (1994)
- 2012: factorització de 21 en un ordinador quàntic.



Teoremes sobre Primers

Teorema d'Euler: Hi ha infinits nombres primers "acabats en 1" (en qualsevol base).

Postulat de Bertrand-Txevitxev: Per a tot nombre n>2, hi ha algun nombre primer p tal que n<p<2n.

Teorema de Dirichlet: Hi ha infinits nombres primers amb reste *a* al dividir per *b*, si *a*<*b* i són primers entre si.

Teorema dels nombres primers: Hi ha "aproximadament" *x/log(x)* primers menor que *x*.

Conjectures de Nombres Primers

Conjectura de Goldbach: Tot nombre parell >2 és suma de dos nombres primers.

Conjectura dels Primers Bessons: Hi ha infinits primers p tals que $p+2$ és primer.

(3 i 5, 5 i 7, 11 i 13, 17 i 19, 29 i 31, 41 i 43,...)

Conjectura d'Euler: Hi ha infinits primers de la forma n^2+1.

($1^2+1=2$, $2^2+1=5$, $4^2+1=17$, $6^2+1=37$, $10^2+1=101$, $14^2+1=197$...)

Conjectura d'Opperman: Per a tot $n>1$ hi ha un nombre primer p tal que $n^2<p<(n+1)^2$