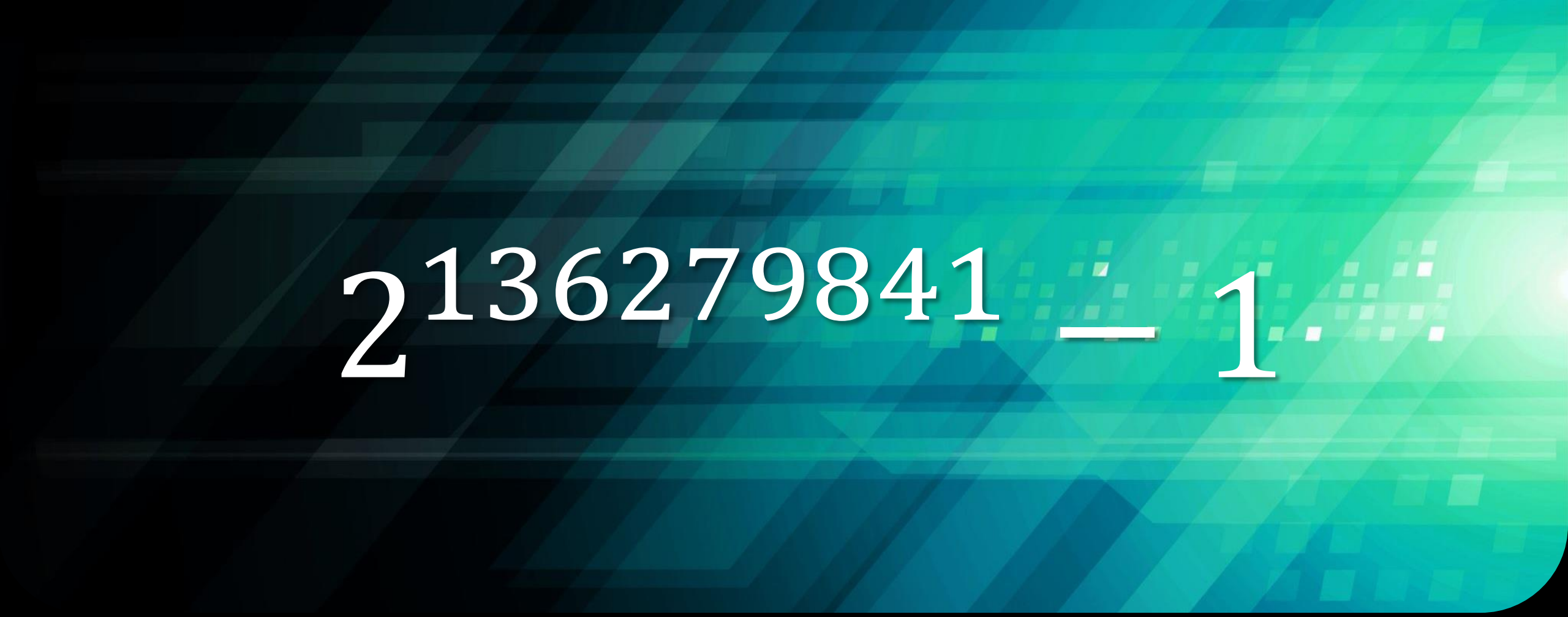


Praštevilo, dolgo 41 milijonov števk

Boštjan Kuzman

Great Internet Mersenne Prime Search
GIMPS
Finding World Record Primes Since 1996

Username
Password
Log In | Register | Forgot password?

Welcome to GIMPS
the Great Internet Mersenne Prime Search

Join GIMPS | Downloads | Known Primes | Progress Overview | Milestones | History

What is GIMPS?

GIMPS is a collaborative project of volunteers who search for Mersenne prime numbers.

Find out how it works, create an account, download software, start searching!

Ask questions on the Mersenne Forum.

All exponents below 70 578 077 have been tested and verified.
All exponents below 124 817 431 have been tested at least once.

Previous Day Stats		Today's Numbers	
Newly Factored	258	GFLOP/s	5 751 392
First Prime Tests	133	GHz-Days	2 875 696
Verified Prime Tests	538	CPUs & GPUs	2 846 014

$2^{136279841}-1$ is the New Largest Known Prime Number

October 21, 2024 — The Great Internet Mersenne Prime Search (GIMPS) has discovered a new Mersenne prime number, $2^{136279841}-1$. At 41,024,320 digits, it eclipses by more than 16 million digits the previous largest known prime number found by GIMPS nearly 6 years ago.

Luke Durant, GIMPS most prolific contributor using free GIMPS software, proved the number prime on October 12. After notifying the GIMPS server, GIMPS began a rigorous process of independently confirming the prime number on several different hardware platforms using several different programs. This process concluded on October 19th.

This prime ends the 28 year reign of ordinary PCs finding the largest known prime. In 2017, Mihai Preda authored Mersenne prime search software that runs on GPUs. GPUs were primarily used in PCs as video cards or for mining cryptocurrency. Nowadays, video cards are also used to power the AI revolution. Durant's idea was to use these powerful GPUs that are now available in the cloud and heavily discounted when they are being under-utilized. Luke organized these cloud GPUs creating a kind of "cloud supercomputer" spanning 17 countries. After nearly a year of testing, Luke finally struck paydirt. On October 11, an NVIDIA A100 GPU in Dublin, Ireland, reported that M136279841 is probably prime. On October 12, an NVIDIA H100 in San Antonio, Texas, USA, confirmed primality with a Lucas-Lehmer test.

Luke, a 36 year-old researcher from San Jose, CA, and former NVIDIA employee, is one of thousands of GIMPS volunteers contributing spare CPU and GPU time in hopes of making a little bit of history. Mihai Preda, and later George Woltman, wrote the GPU software. Aaron Blosser keeps the GIMPS server running smoothly. This discovery is also made possible by the combined effort of each

Števila oblike $2^n - 1$ imenujemo **Mersennova števila.**

n	1	2	3	4	5	6	7	8	9	10	...
$2^n - 1$	1	3	7	15	31	63	127	255	511	1023	...

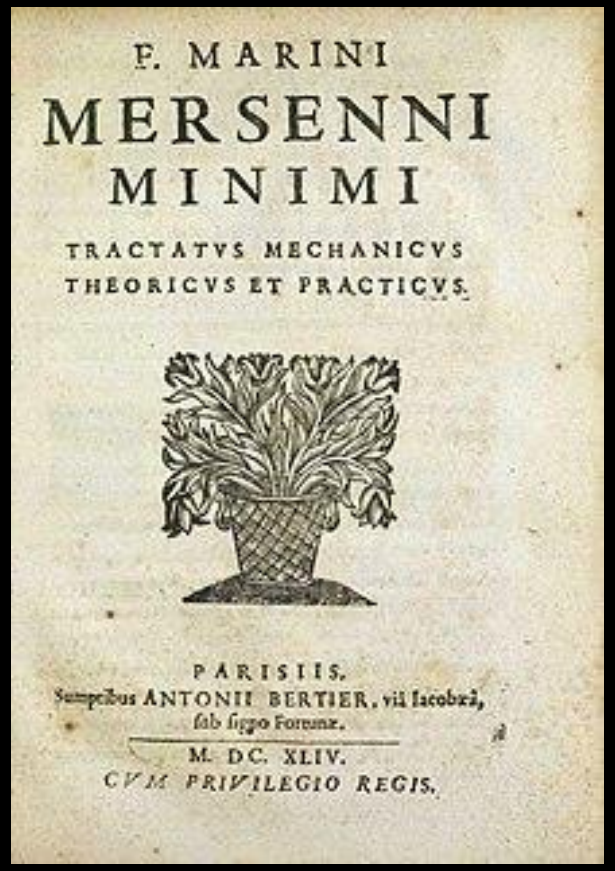
Marin Mersenne (1588-1648)

HARMONIE
VNIVERSELLE,
CONTENANT LA THEORIE
ET LA PRATIQVE
DE LA MVSIQVE.

Où il est traité de la Nature des Sons, & des Mouuemens, des Consonances, des Dissonances, des Genres, des Modes, de la Composition, de la Voix, des Chants, & de toutes sortes d'Instrumens Harmoniques.

Par F. MARIN MERSENNE de l'Ordre des Minimes.

A PARIS,
Chez SEBASTIEN CRAMOISY, Imprimeur ordinaire du Roy, rue S. Iacques, aux Cicognes.
M. DC. XXXVI.
Auec Priuilege du Roy, & Approbation des Docteurs.



F. MARINI
MERSENNI
MINIMI

TRACTATVS MECHANICVS
THEORICVS ET PRACTICVS.

PARISIIS,
Sumptibus ANTONII BERTIER, viâ Iacobæâ,
sub signo Fortunæ.
M. DC. XLIV.
CVM PRIVILEGIO REGIS.

IZREK: Če je $2^n - 1$ praštevilo, potem je n praštevilo.

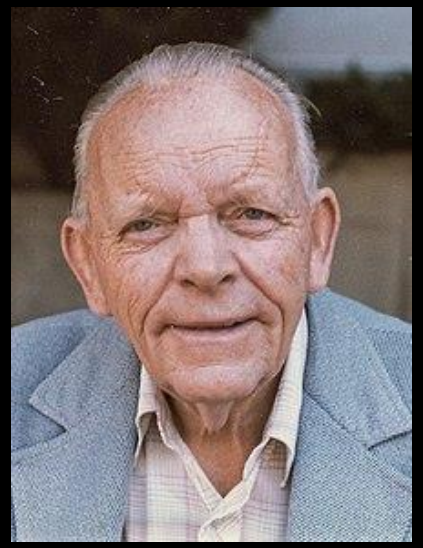
DOKAZ:
Recimo, da je n sestavljeno.
Torej je $n = ab$, kjer je $1 < a, b < n$.
Sledi
$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)((2^a)^{b-1} + \cdots + 2^a + 1)$.
Faktorja na desni sta večja od 1, torej $2^n - 1$ ni praštevilo.

OPOMBA: Obrat ne velja. Če je n praštevilo, $2^n - 1$ ni nujno praštevilo.
Protiprimer je recimo $2^{11} - 1 = 2047 = 23 \cdot 89$.

Če torej želimo najti novo zelo veliko praštevilo, vzamemo že znano praštevilo p in preverimo, ali je $2^p - 1$ praštevilo. V splošnem je problem preverjanja praštevilskosti računsko zelo požrešen. Za števila oblike $2^p - 1$ pa obstaja bistveno hitrejši test.

LUCAS-LEHMERJEV TEST:
Naj bo p znano praštevilo.
Testirati želimo število $M_p = 2^p - 1$.
Definiramo $s_0 = 4$ in $s_i = s_{i-1}^2 - 2 \pmod{M_p}$ za $i \geq 1$.
Če je $s_{p-2} = 0$, potem je M_p praštevilo.


Edouard Lucas (1842-1891)


Derrick Lehmer (1905-1991)

Zgled: Naj bo $p = 5$. Testirati želimo $M_5 = 2^5 - 1 = 31$.
Dobimo
$s_0 = 4$,
$s_1 = 4^2 - 2 \ (mod\ 31) = 14$,
$s_2 = 14^2 - 2 \ (mod\ 31) = 8$,
$s_3 = 8^2 - 2 \ (mod\ 31) = 0$.
Torej je 31 praštevilo.

Mersennova praštevila so povezana s popolnimi števili.

Naravno število je **popolno**, če je enako vsoti svojih pravih deliteljev.

Zgledi:
$6 = 1 + 2 + 3 \ = 2 \cdot 3 = \ 2^1(2^2 - 1)$
$28 = 1 + 2 + 4 + 7 + 14 = 4 \cdot 7 = 2^2(2^3 - 1)$
$496 = \cdots = 16 \cdot 31 = 2^4(2^5 - 1)$
$8128 = \cdots = 64 \cdot 127 = 2^6(2^7 - 1)$

EVKLIDOV IZREK (250 PNŠ):
Če je $2^p - 1$ praštevilo, potem je $2^{p-1}(2^p - 1)$ popolno število.
Dokaz: Vsota vseh deliteljev je $(1 + 2 + \cdots + 2^{p-1}) \cdot ((2^p - 1) + 1) = (2^p - 1) \cdot 2^p$.

EULERJEV IZREK (okoli 1730): Vsa soda popolna števila so te oblike.

Doslej je znanih 52 popolnih števil.
Ni znano, ali je popolnih števil neskončno.
Ni znano, ali obstaja kako liho popolno število.