Mersenne Primes and GIMPS

Curtis Cooper
University of Central Missouri

October 21, 2019

Prime Numbers

- A **prime number** is a positive integer which has exactly two factors, itself and one.

Prime Numbers

- A **prime number** is a positive integer which has exactly two factors, itself and one.
- Prime Numbers Less Than 100:

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,$$
$$43,\ 47,\ 53,\ 59,\ 61,\ 67,\ 71,\ 73,\ 79,\ 83,\ 89,\ 97$$

Mersenne Numbers

- A **Mersenne number** is a number of the form $2^p - 1$, where p is a prime number.

Mersenne Numbers

- A **Mersenne number** is a number of the form $2^p - 1$, where p is a prime number.
- Examples of Mersenne numbers are:

$$M2 = 2^2 - 1 = 3$$
$$M3 = 2^3 - 1 = 7$$
$$M5 = 2^5 - 1 = 31$$
$$M7 = 2^7 - 1 = 127$$
$$M11 = 2^{11} - 1 = 2047$$

Mersenne Primes

- A **Mersenne prime** is a Mersenne number that is prime.

Mersenne Primes

- A **Mersenne prime** is a Mersenne number that is prime.
- Examples of Mersenne primes are:

$$3 = 2^2 - 1$$
$$7 = 2^3 - 1$$
$$31 = 2^5 - 1$$
$$127 = 2^7 - 1$$
$$8191 = 2^{13} - 1$$

Mersenne Primes

- A **Mersenne prime** is a Mersenne number that is prime.
- Examples of Mersenne primes are:

$$3 = 2^2 - 1$$
$$7 = 2^3 - 1$$
$$31 = 2^5 - 1$$
$$127 = 2^7 - 1$$
$$8191 = 2^{13} - 1$$

- $2047 = 2^{11} - 1 = 23 \times 89$.

Marin Mersenne

- Mersenne primes are named after a 17th-century French monk and mathematician

Marin Mersenne (1588-1648)

Marin Mersenne

- Mersenne compiled what was supposed to be a list of Mersenne primes with exponents up to 257.

Marin Mersenne

- Mersenne compiled what was supposed to be a list of Mersenne primes with exponents up to 257.
- 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257

Marin Mersenne

- Mersenne compiled what was supposed to be a list of Mersenne primes with exponents up to 257.
- 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257
- His list was largely incorrect, as Mersenne mistakenly included M67 and M257 (which are composite), and omitted M61, M89, and M107 (which are prime).

Marin Mersenne

- Mersenne compiled what was supposed to be a list of Mersenne primes with exponents up to 257.
- 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257
- His list was largely incorrect, as Mersenne mistakenly included M67 and M257 (which are composite), and omitted M61, M89, and M107 (which are prime).
- A correct list of all Mersenne primes in this number range was completed and rigorously verified only about three centuries after Mersenne published his list.

Marin Mersenne

- Mersenne compiled what was supposed to be a list of Mersenne primes with exponents up to 257.
- 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257
- His list was largely incorrect, as Mersenne mistakenly included M67 and M257 (which are composite), and omitted M61, M89, and M107 (which are prime).
- A correct list of all Mersenne primes in this number range was completed and rigorously verified only about three centuries after Mersenne published his list.
- 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127

Edouard Lucas

Edouard Lucas (1816-1882)

Edouard Lucas

Edouard Lucas (1816-1882)

- Lucas proved in 1876 that M127 is indeed prime, as Mersenne claimed. This was the largest known prime number for 75 years, and the largest ever calculated by hand.

Edouard Lucas

Edouard Lucas (1816-1882)

- Lucas proved in 1876 that M127 is indeed prime, as Mersenne claimed. This was the largest known prime number for 75 years, and the largest ever calculated by hand.
- Without finding a factor, Lucas demonstrated that M67 is actually composite.

List of Known Mersenne Primes

- List of 51 Known Mersenne Primes - https://en.wikipedia.org/wiki/Mersenne_prime

M82589933

- $2^{82589933} - 1$ is prime!

M82589933

- $2^{82589933} - 1$ is prime!
- Largest Known Prime Number

M82589933

- $2^{82589933} - 1$ is prime!
- Largest Known Prime Number
- 24,862,048 decimal digits

M82589933

- $2^{82589933} - 1$ is prime!
- Largest Known Prime Number
- 24,862,048 decimal digits
- Discovered on December 7, 2018 by GIMPS and Patrick Laroche using a machine with an Intel i5-4590T CPU.

M82589933

- $2^{82589933} - 1$ is prime!
- Largest Known Prime Number
- 24,862,048 decimal digits
- Discovered on December 7, 2018 by GIMPS and Patrick Laroche using a machine with an Intel i5-4590T CPU.
- The primality proof took twelve days of non-stop computing using Prime95.

M82589933

- $2^{82589933} - 1$ is prime!
- Largest Known Prime Number
- 24,862,048 decimal digits
- Discovered on December 7, 2018 by GIMPS and Patrick Laroche using a machine with an Intel i5-4590T CPU.
- The primality proof took twelve days of non-stop computing using Prime95.
- Patrick is a 35 year old I.T. professional living in Ocala, Florida.

M82589933

- $2^{82589933} - 1$ is prime!
- Largest Known Prime Number
- 24,862,048 decimal digits
- Discovered on December 7, 2018 by GIMPS and Patrick Laroche using a machine with an Intel i5-4590T CPU.
- The primality proof took twelve days of non-stop computing using Prime95.
- Patrick is a 35 year old I.T. professional living in Ocala, Florida.
- For many years, Patrick had used GIMPS software as a free "stress test" for his computer builds.

M82589933

- $2^{82589933} - 1$ is prime!
- Largest Known Prime Number
- 24,862,048 decimal digits
- Discovered on December 7, 2018 by GIMPS and Patrick Laroche using a machine with an Intel i5-4590T CPU.
- The primality proof took twelve days of non-stop computing using Prime95.
- Patrick is a 35 year old I.T. professional living in Ocala, Florida.
- For many years, Patrick had used GIMPS software as a free "stress test" for his computer builds.
- Recently, he started prime hunting on his media server to "give back" to the project.

M82589933

- $2^{82589933} - 1$ is prime!
- Largest Known Prime Number
- 24,862,048 decimal digits
- Discovered on December 7, 2018 by GIMPS and Patrick Laroche using a machine with an Intel i5-4590T CPU.
- The primality proof took twelve days of non-stop computing using Prime95.
- Patrick is a 35 year old I.T. professional living in Ocala, Florida.
- For many years, Patrick had used GIMPS software as a free "stress test" for his computer builds.
- Recently, he started prime hunting on his media server to "give back" to the project.
- After less than 4 months and on just his fourth try, he discovered the new prime number.

News About 51th Mersenne Prime

- Official Press Release
  https://www.mersenne.org/primes/?press=M82589933

UCM's Four Mersenne Primes

- M30402457
  https://www.mersenne.org/primes/?press=M30402457

UCM's Four Mersenne Primes

- M30402457
  https://www.mersenne.org/primes/?press=M30402457
- M32582657
  https://www.mersenne.org/primes/?press=M32582657

UCM's Four Mersenne Primes

- M30402457
  https://www.mersenne.org/primes/?press=M30402457
- M32582657
  https://www.mersenne.org/primes/?press=M32582657
- M57885161
  https://www.mersenne.org/primes/?press=M57885161

UCM's Four Mersenne Primes

- M30402457
  https://www.mersenne.org/primes/?press=M30402457
- M32582657
  https://www.mersenne.org/primes/?press=M32582657
- M57885161
  https://www.mersenne.org/primes/?press=M57885161
- M74207281
  https://www.mersenne.org/primes/?press=M74207281

The Great Internet Mersenne Prime Search

- GIMPS is a collaborative project of volunteers who are searching for Mersenne prime numbers. The software used by GIMPS volunteers is Prime95. This software can be downloaded from the Internet for free.

The Great Internet Mersenne Prime Search

- GIMPS is a collaborative project of volunteers who are searching for Mersenne prime numbers. The software used by GIMPS volunteers is Prime95. This software can be downloaded from the Internet for free.
- George Woltman founded GIMPS in January 1996 and wrote the prime testing software.

The Great Internet Mersenne Prime Search

- GIMPS is a collaborative project of volunteers who are searching for Mersenne prime numbers. The software used by GIMPS volunteers is Prime95. This software can be downloaded from the Internet for free.
- George Woltman founded GIMPS in January 1996 and wrote the prime testing software.
- Scott Kurowski wrote the PrimeNet server that supports GIMPS. In 1997 he founded Entropia, a distributed computing software company.

GIMPS Statistics

- Woltman's program uses a special algorithm, discovered in the early 1990's by Richard Crandall. Crandall found ways to double the speed of what are called convolutions – essentially big multiplication operations.

GIMPS Statistics

- Woltman's program uses a special algorithm, discovered in the early 1990's by Richard Crandall. Crandall found ways to double the speed of what are called convolutions – essentially big multiplication operations.
- As of October 19, 2019, GIMPS had a sustained throughput of approximately 654 trillion floating-point operations per second.

GIMPS Statistics

- Woltman's program uses a special algorithm, discovered in the early 1990's by Richard Crandall. Crandall found ways to double the speed of what are called convolutions – essentially big multiplication operations.
- As of October 19, 2019, GIMPS had a sustained throughput of approximately 654 trillion floating-point operations per second.
- The GIMPS project consists of 216,343 users, 1368 teams, and 1,962,206 computers.

GIMPS Statistics

- Woltman's program uses a special algorithm, discovered in the early 1990's by Richard Crandall. Crandall found ways to double the speed of what are called convolutions – essentially big multiplication operations.
- As of October 19, 2019, GIMPS had a sustained throughput of approximately 654 trillion floating-point operations per second.
- The GIMPS project consists of 216,343 users, 1368 teams, and 1,962,206 computers.
- UCM has over 650 computers performing LL-tests on Mersenne numbers.

Woltman, Kurowski, and Crandall

Woltman

Kurowski

Crandall

GIMPS Links

- The GIMPS home page can be found at: https://www.mersenne.org

GIMPS Links

- The GIMPS home page can be found at: https://www.mersenne.org
- A Mersenne Prime discussion forum can be found at: http://www.mersenneforum.org

Lucas-Lehmer Test

- The **Lucas-Lehmer Test** is one way to test whether or not Mersenne numbers are Mersenne primes.

Lucas-Lehmer Test

- The **Lucas-Lehmer Test** is one way to test whether or not Mersenne numbers are Mersenne primes.

Definition

Let $S_1 = 4$ and

$$S_{n+1} = S_n^2 - 2 \text{ for } n \geq 1.$$

Lucas-Lehmer Test

- The **Lucas-Lehmer Test** is one way to test whether or not Mersenne numbers are Mersenne primes.

Definition

Let $S_1 = 4$ and

$$S_{n+1} = S_n^2 - 2 \text{ for } n \geq 1.$$

- The first few terms of the S sequence are:

$$4,\ 14,\ 194,\ 37634,\ 1416317954,\ 2005956546822746114,$$
$$4023861667741036022825635656102100994, \ldots$$

Lucas-Lehmer Test

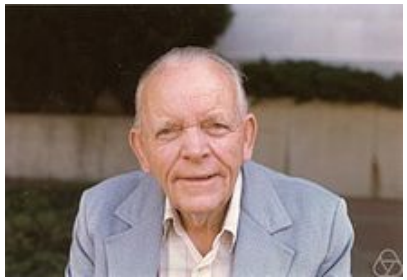
Lucas-Lehmer Test

Let p be a prime number. Then

$$M_p = 2^p - 1 \text{ is prime}$$
$$\text{if and only if}$$
$$S_{p-1} \bmod M_p = 0.$$

Lucas and Lehmer

Lucas



Lehmer

$2^{11} - 1$ is not prime

Theorem

$M_{11} = 2^{11} - 1 = 2047$ is not prime.

$2^{11} - 1$ is not prime

Theorem

$M_{11} = 2^{11} - 1 = 2047$ *is not prime.*

Proof

i	$S_i \bmod 2047$

$2^{11} - 1$ is not prime

Theorem

$M_{11} = 2^{11} - 1 = 2047$ is not prime.

Proof

i	$S_i \bmod 2047$
1	4

$2^{11} - 1$ is not prime

Theorem

$M_{11} = 2^{11} - 1 = 2047$ is not prime.

Proof

i	$S_i \bmod 2047$
1	4
2	$(4^2 - 2) = 14 \bmod 2047 = 14$

$2^{11} - 1$ is not prime

Theorem

$M_{11} = 2^{11} - 1 = 2047$ *is not prime.*

Proof

i	$S_i \bmod 2047$
1	4
2	$(4^2 - 2) = 14 \bmod 2047 = 14$
3	$(14^2 - 2) = 194 \bmod 2047 = 194$

$2^{11} - 1$ is not prime

Theorem

$M_{11} = 2^{11} - 1 = 2047$ *is not prime.*

Proof

i	$S_i \bmod 2047$
1	4
2	$(4^2 - 2) = 14 \bmod 2047 = 14$
3	$(14^2 - 2) = 194 \bmod 2047 = 194$
4	$(194^2 - 2) = 37634 \bmod 2047 = 788$

$2^{11} - 1$ is not prime

Theorem

$M_{11} = 2^{11} - 1 = 2047$ *is not prime.*

Proof

i	$S_i \bmod 2047$
1	4
2	$(4^2 - 2) = 14 \bmod 2047 = 14$
3	$(14^2 - 2) = 194 \bmod 2047 = 194$
4	$(194^2 - 2) = 37634 \bmod 2047 = 788$
5	$(788^2 - 2) = 620942 \bmod 2047 = 701$

$2^{11} - 1$ is not prime

Proof cont.

i	$S_i \bmod 2047$

$2^{11} - 1$ is not prime

Proof cont.

i	$S_i \bmod 2047$
6	$(701^2 - 2) = 491399 \bmod 2047 = 119$

$2^{11} - 1$ is not prime

Proof cont.

i	$S_i \bmod 2047$
6	$(701^2 - 2) = 491399 \bmod 2047 = 119$
7	$(119^2 - 2) = 14159 \bmod 2047 = 1877$

$2^{11} - 1$ is not prime

Proof cont.

i	$S_i \bmod 2047$
6	$(701^2 - 2) = 491399 \bmod 2047 = 119$
7	$(119^2 - 2) = 14159 \bmod 2047 = 1877$
8	$(1877^2 - 2) = 3523127 \bmod 2047 = 240$

$2^{11} - 1$ is not prime

Proof cont.

i	$S_i \bmod 2047$
6	$(701^2 - 2) = 491399 \bmod 2047 = 119$
7	$(119^2 - 2) = 14159 \bmod 2047 = 1877$
8	$(1877^2 - 2) = 3523127 \bmod 2047 = 240$
9	$(240^2 - 2) = 57598 \bmod 2047 = 282$

$2^{11} - 1$ is not prime

Proof cont.

i	$S_i \bmod 2047$
6	$(701^2 - 2) = 491399 \bmod 2047 = 119$
7	$(119^2 - 2) = 14159 \bmod 2047 = 1877$
8	$(1877^2 - 2) = 3523127 \bmod 2047 = 240$
9	$(240^2 - 2) = 57598 \bmod 2047 = 282$
10	$(282^2 - 2) = 79522 \bmod 2047 = 1736$

$2^{31} - 1$ is prime

Theorem

$M_{31} = 2^{31} - 1 = 2147483647$ *is prime.*

$2^{31} - 1$ is prime

Theorem

$M_{31} = 2^{31} - 1 = 2147483647$ is prime.

Proof.

i	$S_i \bmod (2^{31} - 1)$

$2^{31} - 1$ is prime

Theorem

$M_{31} = 2^{31} - 1 = 2147483647$ *is prime.*

Proof.

i	$S_i \bmod (2^{31} - 1)$
1	4

$2^{31} - 1$ is prime

Theorem

$M_{31} = 2^{31} - 1 = 2147483647$ *is prime.*

Proof.

i	$S_i \bmod (2^{31} - 1)$
1	4
2	14

$2^{31} - 1$ is prime

Theorem

$M_{31} = 2^{31} - 1 = 2147483647$ *is prime.*

Proof.

i	$S_i \bmod (2^{31} - 1)$
1	4
2	14
3	194

$2^{31} - 1$ is prime

Theorem

$M_{31} = 2^{31} - 1 = 2147483647$ *is prime.*

Proof.

i	$S_i \bmod (2^{31} - 1)$
1	4
2	14
3	194
4	37634

$2^{31} - 1$ is prime

Theorem

$M_{31} = 2^{31} - 1 = 2147483647$ *is prime.*

Proof.

i	$S_i \bmod (2^{31} - 1)$
1	4
2	14
3	194
4	37634
5	1416317954

$2^{31} - 1$ is prime

Theorem

$M_{31} = 2^{31} - 1 = 2147483647$ *is prime.*

Proof.

i	$S_i \bmod (2^{31} - 1)$
1	4
2	14
3	194
4	37634
5	1416317954
6	669670838

$2^{31} - 1$ is prime

Theorem

$M_{31} = 2^{31} - 1 = 2147483647$ *is prime.*

Proof.

i	$S_i \bmod (2^{31} - 1)$
1	4
2	14
3	194
4	37634
5	1416317954
6	669670838
7	1937259419

$2^{31} - 1$ is prime

Theorem

$M_{31} = 2^{31} - 1 = 2147483647$ *is prime.*

Proof.

i	$S_i \bmod (2^{31} - 1)$
1	4
2	14
3	194
4	37634
5	1416317954
6	669670838
7	1937259419
8	425413602

$2^{31} - 1$ is prime

i	$S_i \bmod (2^{31} - 1)$
9	842014276
10	12692426
11	2044502122
12	1119438707
13	1190075270
14	1450757861
15	877666528
16	630853853
17	940321271
18	512995887
19	692931217

$2^{31} - 1$ is prime

i	$S_i \bmod (2^{31} - 1)$
20	1883625615
21	1992425718
22	721929267
23	27220594
24	1570086542
25	1676390412

$2^{31} - 1$ is prime

i	$S_i \bmod (2^{31} - 1)$
20	1883625615
21	1992425718
22	721929267
23	27220594
24	1570086542
25	1676390412
26	1159251674

$2^{31} - 1$ is prime

i	$S_i \bmod (2^{31} - 1)$
20	1883625615
21	1992425718
22	721929267
23	27220594
24	1570086542
25	1676390412
26	1159251674
27	211987665

$2^{31} - 1$ is prime

i	$S_i \bmod (2^{31} - 1)$
20	1883625615
21	1992425718
22	721929267
23	27220594
24	1570086542
25	1676390412
26	1159251674
27	211987665
28	1181536708

$2^{31} - 1$ is prime

i	$S_i \bmod (2^{31} - 1)$
20	1883625615
21	1992425718
22	721929267
23	27220594
24	1570086542
25	1676390412
26	1159251674
27	211987665
28	1181536708
29	65536

$2^{31} - 1$ is prime

i	$S_i \bmod (2^{31} - 1)$
20	1883625615
21	1992425718
22	721929267
23	27220594
24	1570086542
25	1676390412
26	1159251674
27	211987665
28	1181536708
29	65536
30	0

5 Fun Facts

5 Fun Facts on GIMPS

5 Fun Facts

5 Fun Facts on GIMPS

- 1. The largest known prime as of October 21, 2019 is:

$$2^{82,589,933} - 1.$$

It was discovered by Patrick LaRoche, George Woltman, Aaron Blosser, et al. (GIMPS) on December 7, 2018 and has 24,862,048 decimal digits.

2nd Fact

- 2. The Great Internet Mersenne Prime Search (GIMPS) is a volunteer organization devoted to the search for large Mersenne primes. George Woltman founded GIMPS in 1996 and created the software used to search for large Mersenne primes. The group has found 17 world-record prime numbers over its 23 years of existence. The software can be freely downloaded at:

www.mersenne.org

3rd Fact

- 3. Marin Mersenne and Eduoard Lucas are mathematicians who researched Mersenne primes. Mersenne was a 17th century French monk. In 1876, Lucas discovered and proved that $2^{127} - 1$ is prime. This prime is the largest prime proved without the use of a computer. His method of proof, using the Lucas-Lehmer Test, is essentially the technique used today to prove Mersenne numbers are prime.

4th Fact

- 4. The University of Central Missouri has found 4 Mersenne primes as a participant in GIMPS. They are:

$$2^{30,402,457} - 1,$$
$$2^{32,582,657} - 1,$$
$$2^{57,885,161} - 1,$$
$$2^{74,207,281} - 1.$$

They were found in 2005, 2006, 2013, and 2016, respectively. At the time, each of them was the largest known prime number.

5th Fact

- 5. The Electronic Frontier Foundation (EFF) has offered a $150,000 prize for the discovery of the first one-hundred million digit prime number. EFF's motivation is to encourage research in computational number theory related to large primes.

Email Address and Talk URL

- Curtis Cooper's Email: cooper@ucmo.edu

Email Address and Talk URL

- Curtis Cooper's Email: cooper@ucmo.edu
- Talk: cs.ucmo.edu/∼cnc8851/talks/cs2400/mpandgimps.pdf