Mersenne Primes, GIMPS, and the LL Test

Curtis Cooper
University of Central Missouri

June 11, 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:

$$
\begin{aligned}
3 &= 2^2 - 1 \\
7 &= 2^3 - 1 \\
31 &= 2^5 - 1 \\
127 &= 2^7 - 1 \\
8191 &= 2^{13} - 1
\end{aligned}
$$

Mersenne Primes

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

$$
\begin{aligned}
3 &= 2^2 - 1 \\
7 &= 2^3 - 1 \\
31 &= 2^5 - 1 \\
127 &= 2^7 - 1 \\
8191 &= 2^{13} - 1
\end{aligned}
$$

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

1. Mersenne Primes
   - Primes
   - Mersenne Primes
2. History
   - Marin Mersenne
   - Edouard Lucas
   - Computer Era
3. 51st MP
   - M82589933
   - News on 51th Mersenne Prime
4. GIMPS
   - GIMPS
   - GIMPS People
   - GIMPS Links
5. LL Test
   - Lucas-Lehmer Test

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).

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 (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.

Franklin Nelson Cole's Talk

- No factor was found until a famous talk by Cole in 1903.

Franklin Nelson Cole's Talk

- No factor was found until a famous talk by Cole in 1903.
- Without speaking a word, he went to a blackboard and computed $2^{67} - 1$:

Franklin Nelson Cole's Talk

- No factor was found until a famous talk by Cole in 1903.
- Without speaking a word, he went to a blackboard and computed $2^{67} - 1$:
- $$2^{67} - 1 = 147,573,952,589,676,412,927.$$

Franklin Nelson Cole's Talk

- No factor was found until a famous talk by Cole in 1903.
- Without speaking a word, he went to a blackboard and computed $2^{67} - 1$:
- $$2^{67} - 1 = 147,573,952,589,676,412,927.$$
- On the other side of the board, he computed $193,707,721 \times 761,838,257,287$:

Franklin Nelson Cole's Talk

- No factor was found until a famous talk by Cole in 1903.
- Without speaking a word, he went to a blackboard and computed $2^{67} - 1$:
- $$2^{67} - 1 = 147,573,952,589,676,412,927.$$
- On the other side of the board, he computed $193,707,721 \times 761,838,257,287$:
- $$\begin{array}{r} 193,707,721 \\ \times 761,838,257,287 \\ 147,573,952,589,676,412,927. \end{array}$$

List of Mersenne Primes

- He returned to his seat without speaking and with the audience's applause.

List of Mersenne Primes

- He returned to his seat without speaking and with the audience's applause.
- 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.

List of Mersenne Primes

- He returned to his seat without speaking and with the audience's applause.
- 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

Noll and Nickel

- The search for Mersenne primes was revolutionized by the introduction of the electronic digital computer.

Noll and Nickel

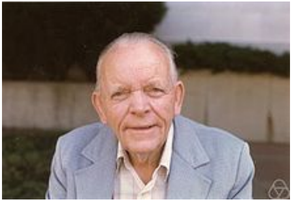
- The search for Mersenne primes was revolutionized by the introduction of the electronic digital computer.
- Landon Curt Noll and Laura Nickel, 18 year-old high school students, discovered M21701 (1978). They were both studying number theory under Dr. Lehmer. This is the 25th Mersenne prime.

Noll and Nickel

- The search for Mersenne primes was revolutionized by the introduction of the electronic digital computer.
- Landon Curt Noll and Laura Nickel, 18 year-old high school students, discovered M21701 (1978). They were both studying number theory under Dr. Lehmer. This is the 25th Mersenne prime.
- Later Landon Curt Noll found M23209 (1979).

Noll and Lehmer

Landon Curt Noll



Derrick Henry Lehmer

Edson Smith

- On August 23, 2008, Edson Smith at UCLA, participating in GIMPS, discovered the Mersenne prime M43112609 with almost 13 million decimal digits.

Edson Smith

- On August 23, 2008, Edson Smith at UCLA, participating in GIMPS, discovered the Mersenne prime M43112609 with almost 13 million decimal digits.
- He claimed the 100,000 dollar prize, awarded by the Electronic Frontier Foundation, for the first known prime with at least 10 million decimal digits.

Edson Smith

- On August 23, 2008, Edson Smith at UCLA, participating in GIMPS, discovered the Mersenne prime M43112609 with almost 13 million decimal digits.
- He claimed the 100,000 dollar prize, awarded by the Electronic Frontier Foundation, for the first known prime with at least 10 million decimal digits.
- The prime was found on a Dell OptiPlex 745. This is the eighth Mersenne prime discovered at UCLA.

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.

- $2^{82589933} - 1$ 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.

- $2^{82589933} - 1$ 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

News About 51th Mersenne Prime

- Official Press Release
  https://www.mersenne.org/primes/?press=M82589933
- John D. Cook
  https://www.johndcook.com/blog/2018/12/22/51st-mersenne-prime/

Digits of M82589933 by Landon Curt Noll

- Digits of M82589933 http://lcn2.github.io/mersenne-english-name/m82589933/prime-c.html

Digits of M82589933 by Landon Curt Noll

- Digits of M82589933 http://lcn2.github.io/mersenne-english-name/m82589933/prime-c.html
- Pronunciation of M82589933 http://lcn2.github.io/mersenne-english-name/m82589933/prime.html

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

More About 49th Mersenne Prime

- Standupmaths
  https://www.youtube.com/watch?v=q5ozBnrd5Zc

More About 49th Mersenne Prime

- Standupmaths
  https://www.youtube.com/watch?v=q5ozBnrd5Zc
- Standupmaths2
  https://www.youtube.com/watch?v=jNXAMBvYe-Y

More About 49th Mersenne Prime

- Standupmaths
  https://www.youtube.com/watch?v=q5ozBnrd5Zc
- Standupmaths2
  https://www.youtube.com/watch?v=jNXAMBvYe-Y
- Jimmy Fallon
  https://www.facebook.com/kshbtv/videos/10153315475526190

Mersenne Buttons

- M30402457 Button
  cs.ucmo.edu/∼cnc8851/images/9.jpg

Mersenne Buttons

- M30402457 Button
  cs.ucmo.edu/∼cnc8851/images/9.jpg
- M32582657 Button
  cs.ucmo.edu/∼cnc8851/images/11.jpg

Mersenne Buttons

- M30402457 Button
  cs.ucmo.edu/∼cnc8851/images/9.jpg
- M32582657 Button
  cs.ucmo.edu/∼cnc8851/images/11.jpg
- M57885161 Button
  cs.ucmo.edu/∼cnc8851/images/7.jpg

Mersenne Buttons

- M30402457 Button
  cs.ucmo.edu/∼cnc8851/images/9.jpg
- M32582657 Button
  cs.ucmo.edu/∼cnc8851/images/11.jpg
- M57885161 Button
  cs.ucmo.edu/∼cnc8851/images/7.jpg
- M74207281 Button
  cs.ucmo.edu/∼cnc8851/images/0.jpg

Jumping GIFS

- 3 Primes GIF
  http://cs.ucmo.edu/∼cnc8851/images/6.gif

Jumping GIFS

- 3 Primes GIF
  http://cs.ucmo.edu/∼cnc8851/images/6.gif
- UCM GIF
  http://cs.ucmo.edu/∼cnc8851/images/14.gif

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 June 7, 2019, GIMPS had a sustained throughput of approximately 435 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 June 7, 2019, GIMPS had a sustained throughput of approximately 435 trillion floating-point operations per second.
- The GIMPS project consists of 211,680 users, 1338 teams, and 1,899,133 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 June 7, 2019, GIMPS had a sustained throughput of approximately 435 trillion floating-point operations per second.
- The GIMPS project consists of 211,680 users, 1338 teams, and 1,899,133 computers.
- UCM has over 700 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

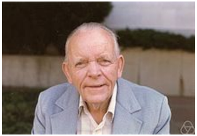
Lucas-Lehmer Test

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 mod 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

Sign of Penultimate Term

- Let p be an odd prime and S_i be the Lucas-Lehmer sequence for M_p.

Sign of Penultimate Term

- Let p be an odd prime and S_i be the Lucas-Lehmer sequence for M_p.
- If $S_{p-1} = 0 \pmod{M_p}$, then the penultimate term is

$$S_{p-2} = \pm 2^{(p+1)/2} \pmod{M_p}.$$

Sign of Penultimate Term

- Let p be an odd prime and S_i be the Lucas-Lehmer sequence for M_p.
- If $S_{p-1} = 0 \pmod{M_p}$, then the penultimate term is

$$S_{p-2} = \pm 2^{(p+1)/2} \pmod{M_p}.$$

- The sign of this penultimate term is call the Lehmer symbol

$$\varepsilon(4, p).$$

Sign of Penultimate Term

- Let p be an odd prime and S_i be the Lucas-Lehmer sequence for M_p.
- If $S_{p-1} = 0 \pmod{M_p}$, then the penultimate term is

$$S_{p-2} = \pm 2^{(p+1)/2} \pmod{M_p}.$$

- The sign of this penultimate term is call the Lehmer symbol

$$\varepsilon(4, p).$$

- The OEIS sequence A123271 shows $\varepsilon(4, p)$ for each Mersenne prime M_p.

Sign of $\varepsilon(4, p)$

p	$\varepsilon(4,p)$	p	$\varepsilon(4,p)$	p	$\varepsilon(4,p)$
3	1	127	1	9941	1
5	1	521	-1	$11,213$	-1
7	-1	607	-1	$19,937$	1
13	1	1279	-1	$21,701$	-1
17	-1	2203	1	$23,209$	1
19	-1	2281	-1	$44,497$	-1
31	1	3217	-1	$86,243$	1
61	1	4253	1	$110,503$	1
89	-1	4423	-1	$132,049$	1
107	-1	9689	-1	$216,091$	-1

Sign of $\varepsilon(4, p)$ cont.

p	$\varepsilon(4, p)$
$25,964,951$	1
$30,402,457$	-1
$32,582,657$	-1
$37,156,667$	1
$42,643,801$	-1
$43,112,609$	1
$57,885,161$	-1
$74,207,281$	-1
$77,232,917$	1
$82,589,933$	-1

M127

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

M127

- Lucas proved in 1876 that M127 is prime. This was the largest known prime number for 75 years, and the largest ever calculated by hand.
- Based on some theorems Lucas discovered and properties of Fibonacci numbers, his hand calculations boiled down to showing that if $r_1 = 3$, and

$$r_{k+1} = r_k^2 - 2 \text{ for } k \geq 1,$$

then if

$$r_{126} \bmod M127 = 0,$$

then M127 is prime.

M127

- Therefore, Lucas had to perform 125 squaring operations and 125 divide operations on 39 digit numbers.

M127

- Therefore, Lucas had to perform 125 squaring operations and 125 divide operations on 39 digit numbers.
- To do this, Lucas turned these calculations into a game. He used a 127×127 chessboard to do the calculations.

M127

- Therefore, Lucas had to perform 125 squaring operations and 125 divide operations on 39 digit numbers.
- To do this, Lucas turned these calculations into a game. He used a 127×127 chessboard to do the calculations.
- To see how Lucas did this, we will reduce the problem.

M127

- Therefore, Lucas had to perform 125 squaring operations and 125 divide operations on 39 digit numbers.
- To do this, Lucas turned these calculations into a game. He used a 127×127 chessboard to do the calculations.
- To see how Lucas did this, we will reduce the problem.
- We will show that $M7 = 2^7 - 1 = 127$ is prime.

M127

- Therefore, Lucas had to perform 125 squaring operations and 125 divide operations on 39 digit numbers.
- To do this, Lucas turned these calculations into a game. He used a 127×127 chessboard to do the calculations.
- To see how Lucas did this, we will reduce the problem.
- We will show that $M7 = 2^7 - 1 = 127$ is prime.
- For our reduced problem, we will play Lucas' game on a 7×7 chessboard.

M7

- The calculations we need to do to show $M7 = 2^7 - 1 = 127$ is prime are the following.

M7

- The calculations we need to do to show $M7 = 2^7 - 1 = 127$ is prime are the following.
- $r_1 = 3$

M7

- The calculations we need to do to show $M7 = 2^7 - 1 = 127$ is prime are the following.
- $r_1 = 3$
- $r_2 = 3^2 - 2 = 7$

M7

- The calculations we need to do to show $M7 = 2^7 - 1 = 127$ is prime are the following.
- $r_1 = 3$
- $r_2 = 3^2 - 2 = 7$
- $r_3 = 7^2 - 2 = 47$

M7

- The calculations we need to do to show $M7 = 2^7 - 1 = 127$ is prime are the following.
- $r_1 = 3$
- $r_2 = 3^2 - 2 = 7$
- $r_3 = 7^2 - 2 = 47$
- $r_4 = (47^2 - 2) \bmod 127 = 48$

M7

- The calculations we need to do to show $M7 = 2^7 - 1 = 127$ is prime are the following.
- $r_1 = 3$
- $r_2 = 3^2 - 2 = 7$
- $r_3 = 7^2 - 2 = 47$
- $r_4 = (47^2 - 2) \bmod 127 = 48$
- $r_5 = (48^2 - 2) \bmod 127 = 16$

M7

- The calculations we need to do to show $M7 = 2^7 - 1 = 127$ is prime are the following.
- $r_1 = 3$
- $r_2 = 3^2 - 2 = 7$
- $r_3 = 7^2 - 2 = 47$
- $r_4 = (47^2 - 2) \bmod 127 = 48$
- $r_5 = (48^2 - 2) \bmod 127 = 16$
- $r_6 = (16^2 - 2) \bmod 127 = 0.$

M7

- The calculations we need to do to show $M7 = 2^7 - 1 = 127$ is prime are the following.
- $r_1 = 3$
- $r_2 = 3^2 - 2 = 7$
- $r_3 = 7^2 - 2 = 47$
- $r_4 = (47^2 - 2) \bmod 127 = 48$
- $r_5 = (48^2 - 2) \bmod 127 = 16$
- $r_6 = (16^2 - 2) \bmod 127 = 0.$
- Therefore, M7 is prime.

Chessboard

- The 7×7 chessboard will store the calculations in base 2 (modulo 127). Columns on the board will represent powers of 2 and the rows will store the product of a single base 2 digit in r_k times the base 2 number r_k. Lucas used a pawn or no pawn to represent a 1 or 0 on the board, respectively.

Chessboard

- The 7×7 chessboard will store the calculations in base 2 (modulo 127). Columns on the board will represent powers of 2 and the rows will store the product of a single base 2 digit in r_k times the base 2 number r_k. Lucas used a pawn or no pawn to represent a 1 or 0 on the board, respectively.
- Initially, the top row will contain $r_1 = 3$.

Chessboard

- If the top row contained r_k, Lucas would square r_k with the following moves.

Chessboard

- If the top row contained r_k, Lucas would square r_k with the following moves.
- He would do standard multiplication to populate the board with pawns. Each row corresponds to putting a shift of the top row in the row or having no pawns in the row, depending on whether there is a pawn in the corresponding column of the top row or not. Because Lucas is doing the calculations modulo 127, the columns wrap around the chessboard.

Pawn Moves

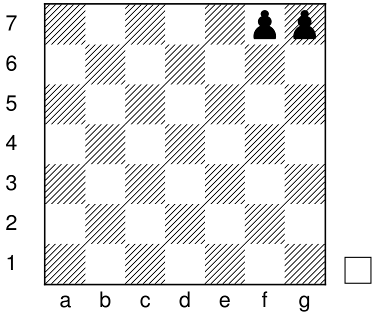
- He would then subtract 2 (once), usually by taking a pawn away from Column f. In the game, two pawns in the same column would be equivalent to removing those two pawns and replacing them by one pawn in the next column to the left. The column to the left of the left-most column is the right-most column.

Pawn Moves

- He would then subtract 2 (once), usually by taking a pawn away from Column f. In the game, two pawns in the same column would be equivalent to removing those two pawns and replacing them by one pawn in the next column to the left. The column to the left of the left-most column is the right-most column.
- Lucas kept this game going until he didn't have two pawns in any column. Then he would slide each pawn in a column to the top row. This would be his r_{k+1}.

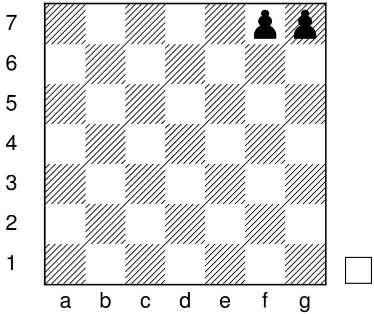
Lucas Game

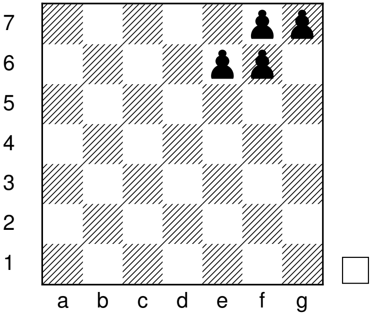
Lucas started the game with $r_1 = 3$.
On the chessboard, that would be:



Lucas Game

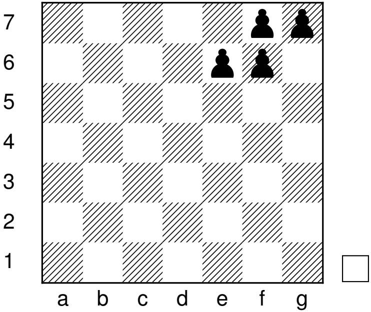
Squaring $r_1 = 3$ would result in the following chessboard.

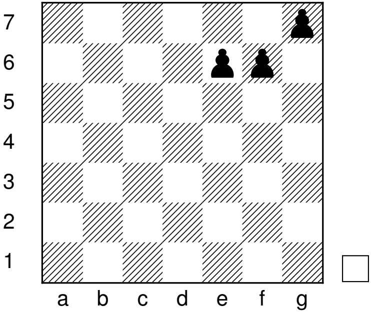




Lucas Game

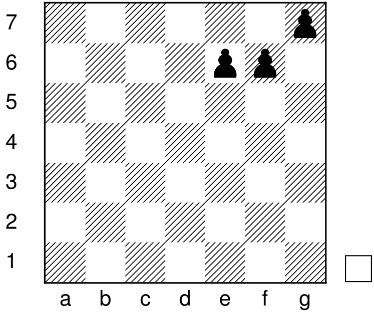
We can subtract 2 by removing a pawn from Column f. That would result in the following chessboard.

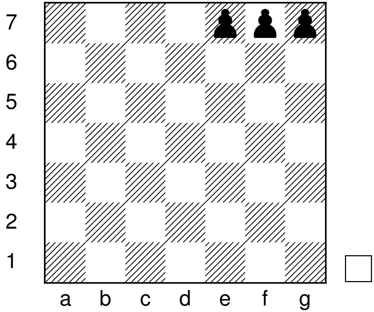




Lucas Game

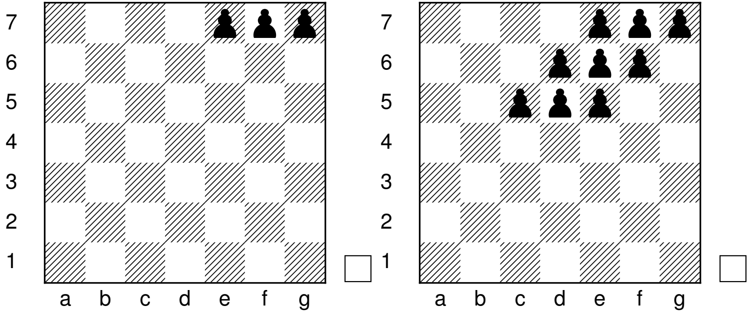
Pushing all the pawns to the top row would result in the following chessboard which is $r_2 = 7$.





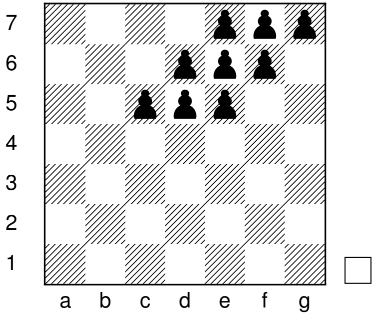
Lucas Game

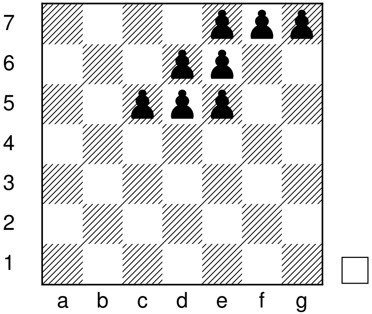
Now we need to square $r_2 = 7$. This would result in the following chessboard.



Lucas Game

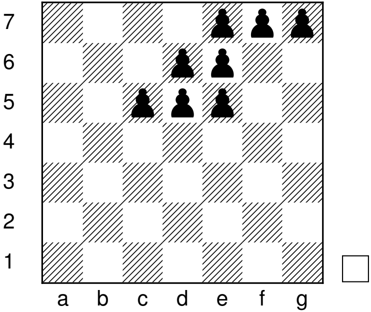
Subtracting 2 would result in the following chessboard.

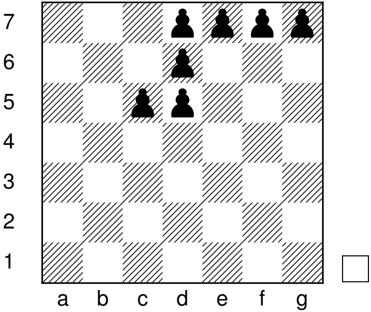




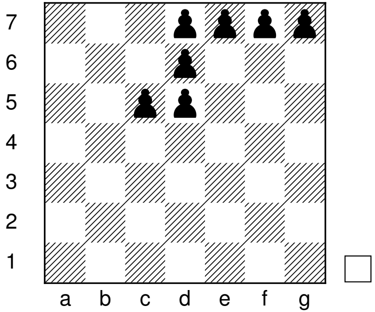
Lucas Game

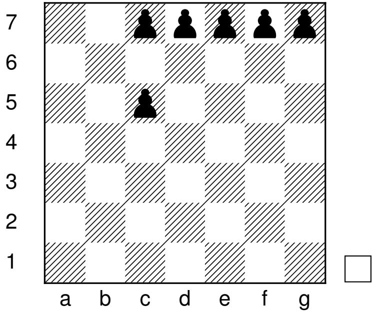
We now do the game moves where we replace two pawns in a column by one pawn in the column to the left. Here are the steps in the game.



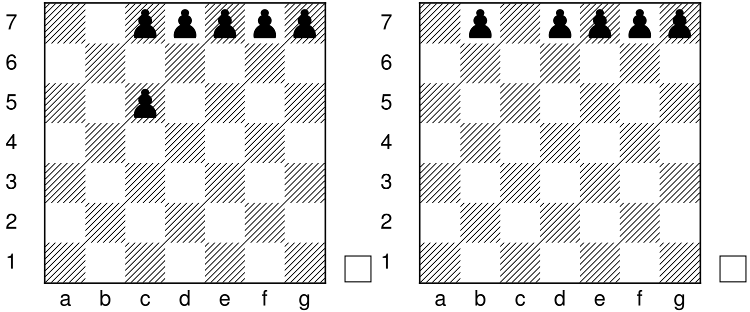


Lucas Game



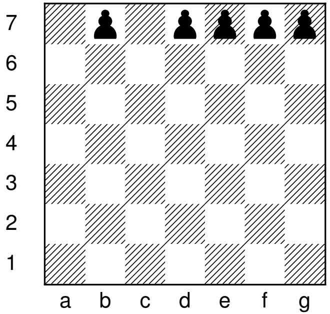


Lucas Game



Lucas Game

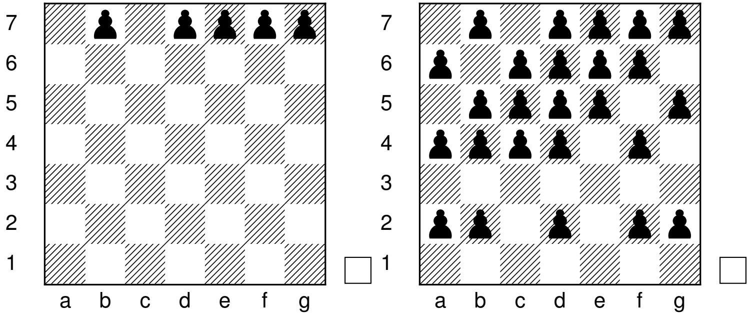
The final chessboard with $r_3 = 47$ would be the following.



$\square$

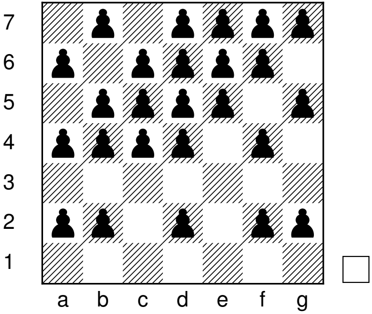
Lucas Game

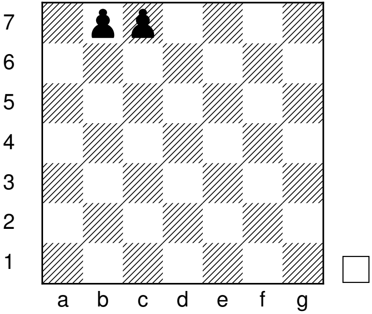
Squaring $r_3 = 47$, we obtain the following chessboard.



Lucas Game

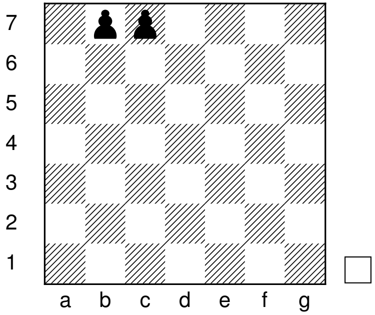
Subtracting 2 and reducing, we obtain the following chessboard.

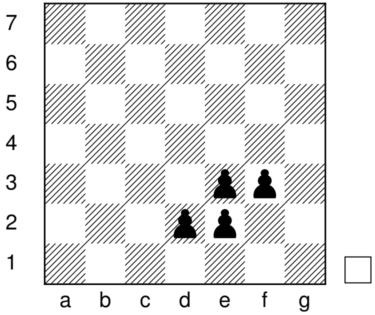




Lucas Game

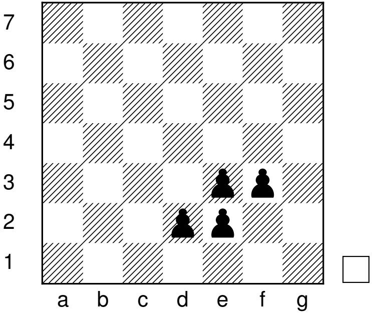
Squaring $r_4 = 48$, we obtain the following chessboard.

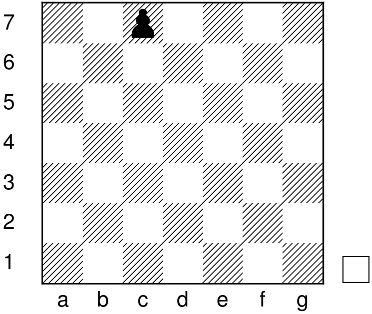




Lucas Game

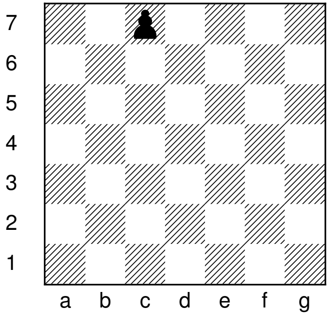
Subtracting 2 and reducing, we obtain the following chessboard.

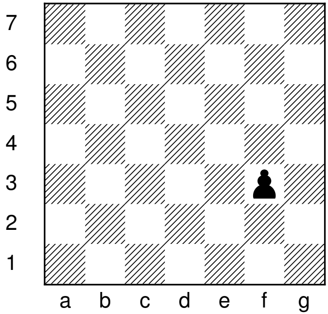




Lucas Game

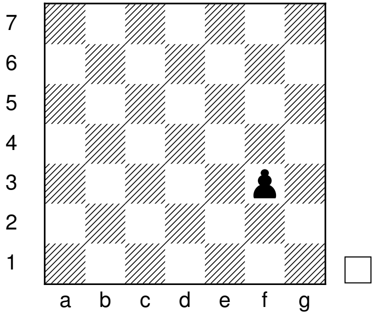
Squaring $r_5 = 16$, we obtain the following chessboard.

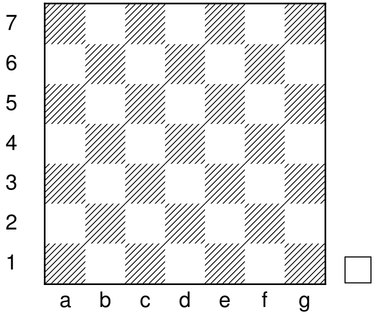




Lucas Game

Subtracting 2 from the result gives $r_6 = 0$.





Lucas Game

Thus, $r_6 = 0$.

Lucas Game

Thus, $r_6 = 0$.
Therefore, $M7 = 2^7 - 1 = 127$ is a Mersenne prime.

5 Fun Facts

5 Fun Facts on GIMPS

5 Fun Facts

5 Fun Facts on GIMPS

- 1. The largest known prime as of June 11, 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/gimpsmsa5/gimpsmsa5.pdf