Mersenne Primes, GIMPS, and the LL Test

Curtis Cooper
University of Central Missouri

June 13, 2018

1. **Mersenne Primes**
   - Primes
   - Mersenne Primes
2. **History of Mersenne Primes**
   - Marin Mersenne
   - Edouard Lucas
   - Computer Era
3. **50th Mersenne Prime**
   - M77232917
   - News on 50th Mersenne Prime
4. **GIMPS**
   - GIMPS
   - GIMPS People
   - GIMPS Links
5. **Lucas-Lehmer Test and Lucas Game**
   - Lucas-Lehmer Test

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:

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

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

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

Edouard Lucas

Edouard Lucas

- 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

- 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.

Edouard Lucas

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

- No factor was found until a famous talk by Cole in 1903.
- Without speaking a word, he went to a blackboard and raised 2 to the 67th power, then subtracted one.

- No factor was found until a famous talk by Cole in 1903.
- Without speaking a word, he went to a blackboard and raised 2 to the 67th power, then subtracted one.
- On the other side of the board, he multiplied 193,707,721 times 761,838,257,287 and got the same number, then returned to his seat (to applause) without speaking.

- No factor was found until a famous talk by Cole in 1903.
- Without speaking a word, he went to a blackboard and raised 2 to the 67th power, then subtracted one.
- On the other side of the board, he multiplied 193,707,721 times 761,838,257,287 and got the same number, then returned to his seat (to applause) without speaking.
- 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.

Edouard Lucas

- No factor was found until a famous talk by Cole in 1903.
- Without speaking a word, he went to a blackboard and raised 2 to the 67th power, then subtracted one.
- On the other side of the board, he multiplied 193,707,721 times 761,838,257,287 and got the same number, then returned to his seat (to applause) without speaking.
- 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

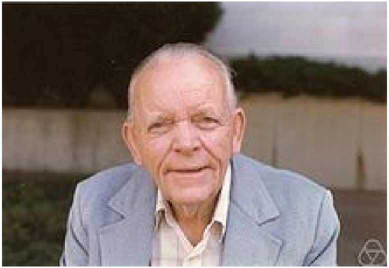
Computer Era

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

- 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. They were both studying number theory under Dr. Lehmer. This is the 25th Mersenne prime.

- 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. They were both studying number theory under Dr. Lehmer. This is the 25th Mersenne prime.
- Later Landon Curt Noll found M23209.

- 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. They were both studying number theory under Dr. Lehmer. This is the 25th Mersenne prime.
- Later Landon Curt Noll found M23209.



Derrick Henry Lehmer

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

Computer Era

- 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.

- 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 50 Known Mersenne Primes - https://en.wikipedia.org/wiki/Mersenne_prime

M77232917

- $2^{77232917} - 1$ is prime!

M77232917

- $2^{77232917} - 1$ is prime!
- Largest Known Prime Number

M77232917

- $2^{77232917} - 1$ is prime!
- Largest Known Prime Number
- 23,249,425 decimal digits

M77232917

- $2^{77232917} - 1$ is prime!
- Largest Known Prime Number
- 23,249,425 decimal digits
- Discovered on December 26, 2017 by GIMPS and Jonathan Pace using the LLT / Prime95 on a quad-core Intel i5-6600 CPU.

M77232917

- $2^{77232917} - 1$ is prime!
- Largest Known Prime Number
- 23,249,425 decimal digits
- Discovered on December 26, 2017 by GIMPS and Jonathan Pace using the LLT / Prime95 on a quad-core Intel i5-6600 CPU.
- The primality proof took six days of non-stop computing.

M77232917

- $2^{77232917} - 1$ is prime!
- Largest Known Prime Number
- 23,249,425 decimal digits
- Discovered on December 26, 2017 by GIMPS and Jonathan Pace using the LLT / Prime95 on a quad-core Intel i5-6600 CPU.
- The primality proof took six days of non-stop computing.
- Jon, a GIMPS volunteer for over 14 years, is a 51-year old Electrical Engineer living in Germantown TN.

M77232917

- $2^{77232917} - 1$ is prime!
- Largest Known Prime Number
- 23,249,425 decimal digits
- Discovered on December 26, 2017 by GIMPS and Jonathan Pace using the LLT / Prime95 on a quad-core Intel i5-6600 CPU.
- The primality proof took six days of non-stop computing.
- Jon, a GIMPS volunteer for over 14 years, is a 51-year old Electrical Engineer living in Germantown TN.
- He is a long-time math enthusiast who is working for FedEx and is active in community charities.

M77232917

- $2^{77232917} - 1$ is prime!
- Largest Known Prime Number
- 23,249,425 decimal digits
- Discovered on December 26, 2017 by GIMPS and Jonathan Pace using the LLT / Prime95 on a quad-core Intel i5-6600 CPU.
- The primality proof took six days of non-stop computing.
- Jon, a GIMPS volunteer for over 14 years, is a 51-year old Electrical Engineer living in Germantown TN.
- He is a long-time math enthusiast who is working for FedEx and is active in community charities.
- As SysAdmin for his charities, he runs Prime95 on all PCs and servers.

News About 50th Mersenne Prime

- Official Press Release https://www.mersenne.org/primes/press/M77232917.html

News About 50th Mersenne Prime

- Official Press Release
  https://www.mersenne.org/primes/press/M77232917.html
- Science Daily
  https://www.sciencedaily.com/release/2018/01/180104164507.htm

News About 50th Mersenne Prime

- Official Press Release
  https://www.mersenne.org/primes/press/M77232917.html
- Science Daily
  https://www.sciencedaily.com/release/2018/01/180104164507.htm
- John D. Cook
  https://www.johndcook.com/blog/2018/01/04/new-prime-number-record-50th-mersenne-prime/

Digits of M77232917 by Landon Curt Noll

- Digits of M77232917 http://lcn2.github.io/mersenne-english-name/m77232917/prime-c.html

Digits of M77232917 by Landon Curt Noll

- Digits of M77232917 http://lcn2.github.io/mersenne-english-name/m77232917/prime-c.html
- Pronunciation of M77232917 http://lcn2.github.io/mersenne-english-name/m77232917/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

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

1. Mersenne Primes
   - Primes
   - Mersenne Primes
2. History of Mersenne Primes
   - Marin Mersenne
   - Edouard Lucas
   - Computer Era
3. 50th Mersenne Prime
   - M77232917
   - News on 50th Mersenne Prime
4. **GIMPS**
   - GIMPS
   - GIMPS People
   - GIMPS Links
5. Lucas-Lehmer Test and Lucas Game
   - Lucas-Lehmer Test

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.

- 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.

- 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 11, 2018, GIMPS had a sustained throughput of approximately 308 trillion floating-point operations per second.

- 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 11, 2018, GIMPS had a sustained throughput of approximately 308 trillion floating-point operations per second.
- The GIMPS project consists of 194,134 users, 1229 teams, and 1,711,236 computers.

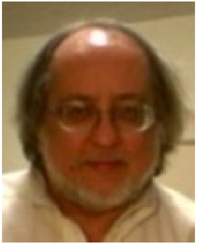
GIMPS

- 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 11, 2018, GIMPS had a sustained throughput of approximately 308 trillion floating-point operations per second.
- The GIMPS project consists of 194,134 users, 1229 teams, and 1,711,236 computers.
- UCM has over 700 computers performing LL-tests on Mersenne numbers.

GIMPS People

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.

- 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 **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

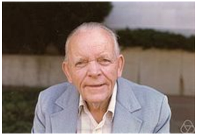
$$M_p = 2^p - 1 \text{ is prime}$$

if and only if

$$S_{p-1} \bmod M_p = 0.$$

Lucas-Lehmer Test

Lucas



Lehmer

Theorem

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

Theorem

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

Proof

i	$S_i \bmod 2047$

Theorem

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

Proof

i	$S_i \bmod 2047$
1	4

Theorem

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

Proof

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

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	$(14^2 - 2) = 194 \bmod 2047 = 194$

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	$(194^2 - 2) = 37634 \bmod 2047 = 788$

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	$(282^2 - 2) = 79522 \bmod 2047 = 1736$

Theorem

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

Theorem

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

Proof.

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

Theorem

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

Proof.

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

Theorem

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

Proof.

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

Theorem

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

Proof.

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

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

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

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

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

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

- 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.

- 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

$$r_{k+1} = r_k^2 - 2,$$

then if

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

then M127 is prime.

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

- 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.

- 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.

- 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.

- 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.

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

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

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

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

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

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

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

- 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.

- 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.

- 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 $r_1 = 3$.

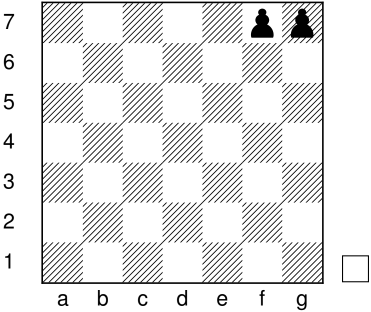
- If the top row contained r_k, Lucas would square r_k with the following moves.

- 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.

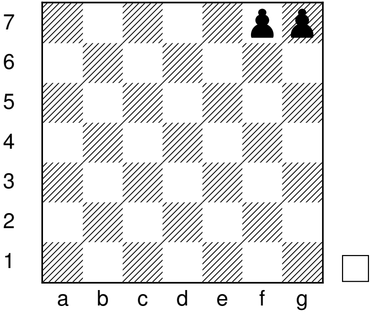
- He would then subtract 2 (once), usually by taking a pawn away from Column f. In the game, two pawns in the same column would be equivalent to removing those two pawns and replacing them by one pawn in the next column to the left. The column to the left of the left-most column is the right-most column.

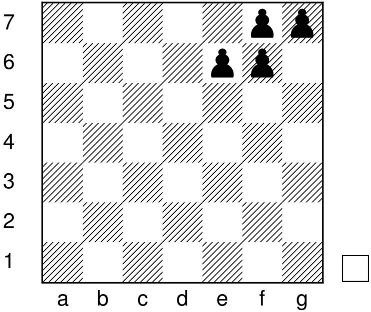
- He would then subtract 2 (once), usually by taking a pawn away from Column f. In the game, two pawns in the same column would be equivalent to removing those two pawns and replacing them by one pawn in the next column to the left. The column to the left of the left-most column is the right-most column.
- 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 started the game with $r_1 = 3$.
On the chessboard, that would be:

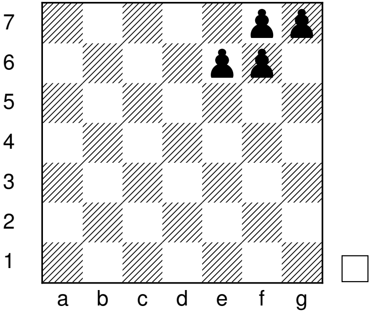


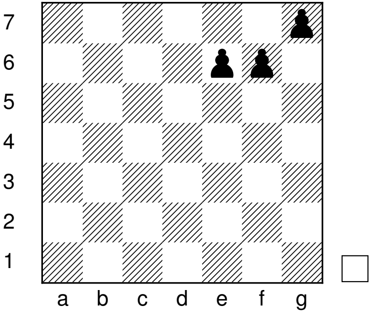
Squaring $r_1 = 3$ would result in the following chessboard.



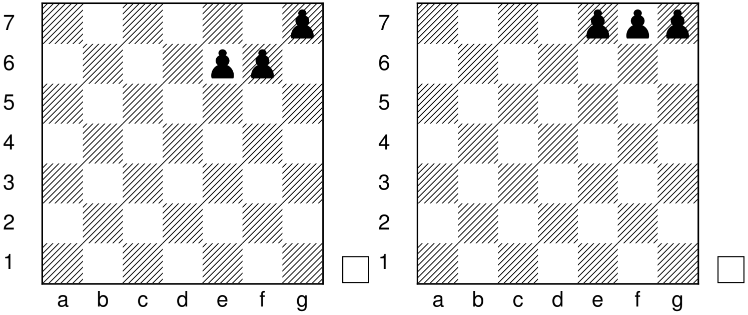


We can subtract 2 by removing a pawn from Column f. That would result in the following chessboard.

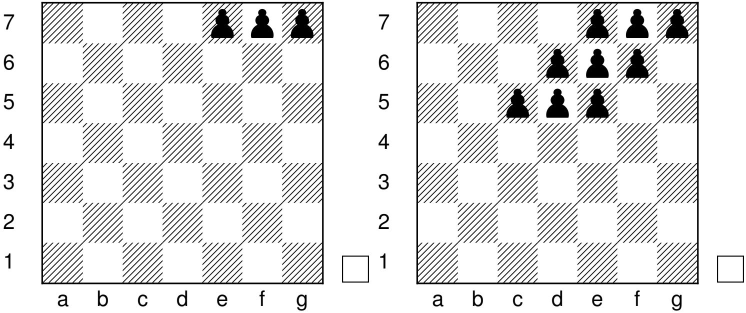




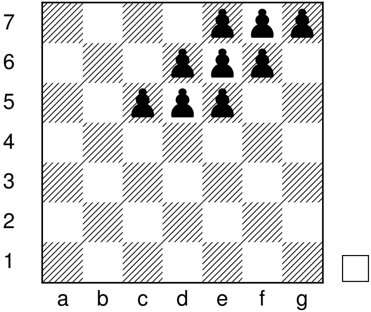
Pushing all the pawns to the top row would result in the following chessboard which is $r_2 = 7$.

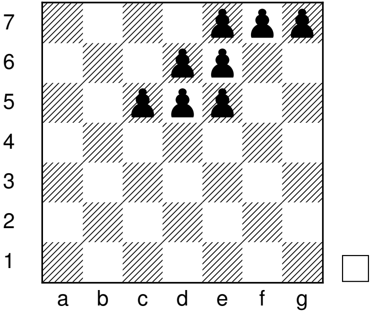


Now we need to square $r_2 = 7$. This would result in the following chessboard.

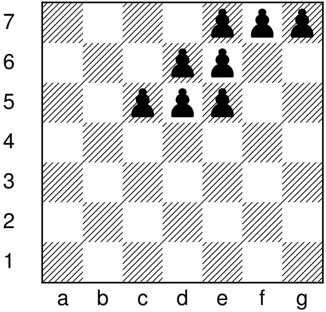


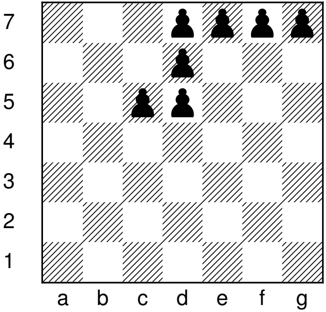
Subtracting 2 would result in the following chessboard.

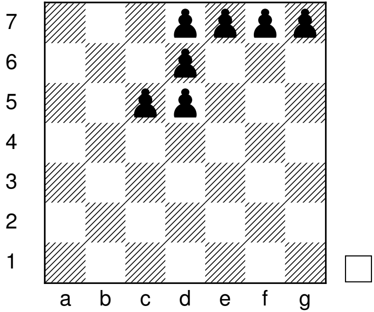


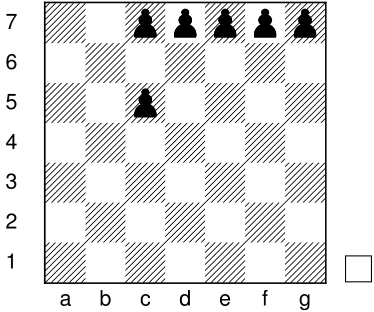


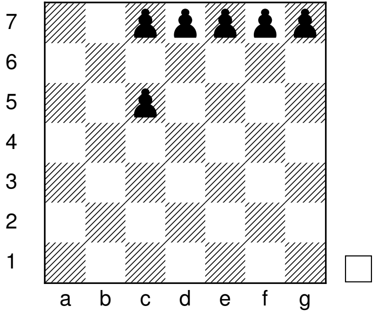
We now do the game moves where we replace two pawns in a column by one pawn in the column to the left. Here are the steps in the game.

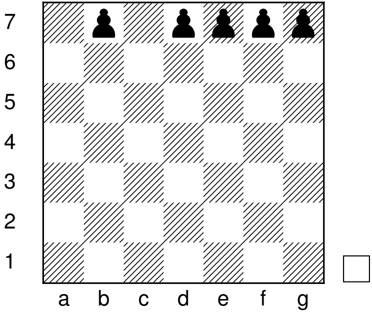




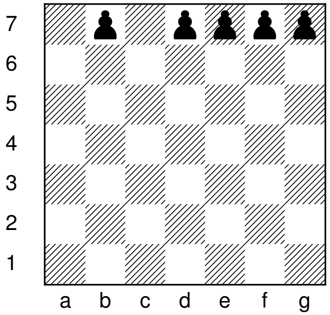

7
6
5
4
3
2
1
a b c d e f g


7
6
5
4
3
2
1
a b c d e f g


7
6
5
4
3
2
1
a b c d e f g

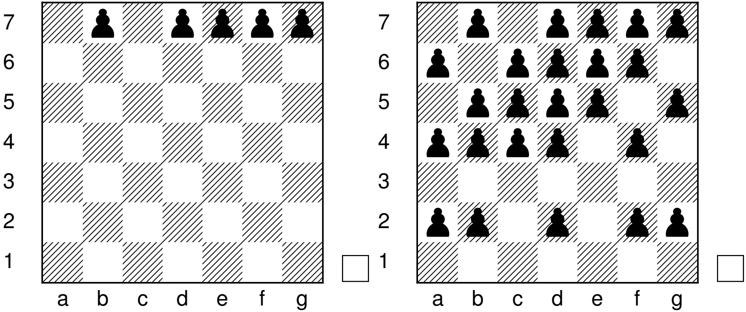

7
6
5
4
3
2
1
a b c d e f g

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



$\square$

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



Continuing this game, we have $r_4 = 48$, $r_5 = 16$, and $r_6 = 0$.

Continuing this game, we have $r_4 = 48$, $r_5 = 16$, and $r_6 = 0$. Therefore $M7 = 2^7 - 1 = 127$ is a Mersenne prime.

1. Mersenne Primes
   - Primes
   - Mersenne Primes
2. History of Mersenne Primes
   - Marin Mersenne
   - Edouard Lucas
   - Computer Era
3. 50th Mersenne Prime
   - M77232917
   - News on 50th Mersenne Prime
4. GIMPS
   - GIMPS
   - GIMPS People
   - GIMPS Links
5. Lucas-Lehmer Test and Lucas Game
   - Lucas-Lehmer Test

Top 10

Top 10 Reasons to Search for Large Mersenne Primes

Top 10

Top 10 Reasons to Search for Large Mersenne Primes

10. Because Mersenne primes are rare and beautiful.

Top 10

Top 10 Reasons to Search for Large Mersenne Primes

10. Because Mersenne primes are rare and beautiful.

9. To continue the mathematics and computer science tradition of Euler, Fermat, Mersenne, Lucas, Lehmer, etc.

Top 10

Top 10 Reasons to Search for Large Mersenne Primes

10. Because Mersenne primes are rare and beautiful.

9. To continue the mathematics and computer science tradition of Euler, Fermat, Mersenne, Lucas, Lehmer, etc.

8. To discover new number theory theorems as a by-product of the quest.

Top 10

Top 10 Reasons to Search for Large Mersenne Primes

10. Because Mersenne primes are rare and beautiful.

9. To continue the mathematics and computer science tradition of Euler, Fermat, Mersenne, Lucas, Lehmer, etc.

8. To discover new number theory theorems as a by-product of the quest.

7. To discover new and more efficient algorithms for testing the primality of large numbers.

Top 10

6. To help detect hardware problems (fan and CPU/bus problems) on individual computers at UCM.

Top 10

6. To help detect hardware problems (fan and CPU/bus problems) on individual computers at UCM.

5. To put to good use the idle CPU cycles of hundreds of computers in labs and offices across UCM's campus.

Top 10

6. To help detect hardware problems (fan and CPU/bus problems) on individual computers at UCM.

5. To put to good use the idle CPU cycles of hundreds of computers in labs and offices across UCM's campus.

4. To learn more about the distribution of Mersenne primes.

Top 10

3. To discover something to number theorists and computer scientists that is comparable to an astronomer discovering a new planet or a chemist discovering a new element.

Top 10

3. To discover something to number theorists and computer scientists that is comparable to an astronomer discovering a new planet or a chemist discovering a new element.

2. To produce much favorable press for UCM and demonstrate that the University of Central Missouri is a first-class research and teaching institution.

Top 10

3. To discover something to number theorists and computer scientists that is comparable to an astronomer discovering a new planet or a chemist discovering a new element.

2. To produce much favorable press for UCM and demonstrate that the University of Central Missouri is a first-class research and teaching institution.

1. To win the $150,000 offered by the Electronic Frontier Foundation (EFF) 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

Talk:
cs.ucmo.edu/∼cnc8851/talks/gimpsmsa4/mersennemsa4.pdf