The 48th Mersenne Prime, GIMPS, the LL Test, and Perfect Numbers

Curtis Cooper
University of Central Missouri

April 22, 2013

1. **Mersenne Primes**
   - Primes
   - Mersenne Primes
2. **48th Mersenne Prime**
   - News on 48th Mersenne Prime
3. **GIMPS**
   - GIMPS
   - GIMPS People
   - GIMPS Links
4. **Lucas-Lehmer Test**
   - Lucas-Lehmer Test
     - $2^{11} - 1$ is not prime
     - $2^{31} - 1$ is prime
5. **Two Theorems**

Prime Numbers

- A **prime number** is an integer, greater than 1, which has exactly two factors, itself and one.

Prime Numbers

- A **prime number** is an integer, greater than 1, 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:

$$
\begin{aligned}
3 &= 2^2 - 1 \\
7 &= 2^3 - 1 \\
31 &= 2^5 - 1 \\
127 &= 2^7 - 1 \\
2047 &= 2^{11} - 1
\end{aligned}
$$

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:

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

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

Marin Mersenne

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

Marin Mersenne (1588-1648)

News About 48th Mersenne Prime

- Official Press Release
  http://www.mersenne.org/various/57885161.htm

News About 48th Mersenne Prime

- Official Press Release
  http://www.mersenne.org/various/57885161.htm
- Huffington Post Story
  http://www.math-cs.ucmo.edu/ curtisc/M57885161.html

News About 48th Mersenne Prime

- Official Press Release
  http://www.mersenne.org/various/57885161.htm
- Huffington Post Story
  http://www.math-cs.ucmo.edu/ curtisc/M57885161.html
- New York Times Story
  http://www.math-cs.ucmo.edu/ curtisc/M57885161.html

More About 48th Mersenne Prime

- Fox 4 Kansas City News Story http://fox4kc.com/2013/02/08/ucm-professors-big-prime-number-discovery-has-bragging-rights/

More About 48th Mersenne Prime

- Fox 4 Kansas City News Story http://fox4kc.com/2013/02/08/ucm-professors-big-prime-number-discovery-has-bragging-rights/
- Lee Judge Cartoon http://www.cartoonistgroup.com/subject/The-Judge-Comics-and-Cartoons.php

More About 48th Mersenne Prime

- Fox 4 Kansas City News Story
  http://fox4kc.com/2013/02/08/ucm-professors-big-prime-number-discovery-has-bragging-rights/
- Lee Judge Cartoon
  http://www.cartoonistgroup.com/subject/The-Judge-Comics-and-Cartoons.php
- Digits of M57885161
  http://www.isthe.com/chongo/tech/math/digit/m57885161/prime-c.html

More About 48th Mersenne Prime

- Fox 4 Kansas City News Story
  http://fox4kc.com/2013/02/08/ucm-professors-big-prime-number-discovery-has-bragging-rights/
- Lee Judge Cartoon
  http://www.cartoonistgroup.com/subject/The-Judge-Comics-and-Cartoons.php
- Digits of M57885161
  http://www.isthe.com/chongo/tech/math/digit/m57885161/prime-c.html
- Pronunciation of M57885161
  http://www.isthe.com/chongo/tech/math/digit/m57885161/prime-d.html

1. Mersenne Primes
   - Primes
   - Mersenne Primes
2. 48th Mersenne Prime
   - News on 48th Mersenne Prime
3. **GIMPS**
   - GIMPS
   - GIMPS People
   - GIMPS Links
4. Lucas-Lehmer Test
   - Lucas-Lehmer Test
     - $2^{11} - 1$ is not prime
     - $2^{31} - 1$ is prime
5. Two Theorems

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

- 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 February 5, 2013, GIMPS had a sustained throughput of approximately 129 trillion floating-point operations per second).

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 February 5, 2013, GIMPS had a sustained throughput of approximately 129 trillion floating-point operations per second).
- The GIMPS project consists of 98,980 users, 574 teams, and 730,562 CPUs.

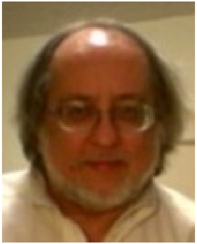
GIMPS

- 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 February 5, 2013, GIMPS had a sustained throughput of approximately 129 trillion floating-point operations per second).
- The GIMPS project consists of 98,980 users, 574 teams, and 730,562 CPUs.
- UCM has over 1000 computers performing LL-tests on Mersenne numbers.

GIMPS People

Woltman

Kurowski



Crandall

GIMPS Links

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

GIMPS Links

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

1. Mersenne Primes
   - Primes
   - Mersenne Primes
2. 48th Mersenne Prime
   - News on 48th Mersenne Prime
3. GIMPS
   - GIMPS
   - GIMPS People
   - GIMPS Links
4. **Lucas-Lehmer Test**
   - Lucas-Lehmer Test
     - $2^{11} - 1$ is not prime
     - $2^{31} - 1$ is prime
5. Two Theorems

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

Let p be a prime number. Then

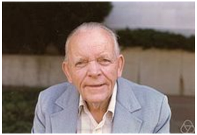
$$M_p = 2^p - 1 \text{ is prime}$$

$$\text{if and only if}$$

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

Lucas-Lehmer Test

Lucas



Lehmer

Theorem

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

Lucas-Lehmer Test

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

Lucas-Lehmer Test

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

Lucas-Lehmer Test

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

Theorem

If M_p is prime, then p is prime.

Theorem

If M_p is prime, then p is prime.

Proof

By contradiction. Suppose p is composite. Then $p = ab$ for some $a, b > 1$. But then

$$\begin{aligned} 2^p - 1 = 2^{ab} - 1 &= (2^a)^b - 1 \\ &= (2^a - 1) \cdot (2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1). \end{aligned}$$

Since the last two factors are both greater than 1, $2^p - 1$ is composite, a contradiction.

Perfect Numbers

- A **perfect number** is a positive integer that is equal to the sum of its proper positive divisors, that is the sum of its positive divisors excluding the number itself.

Perfect Numbers

- A **perfect number** is a positive integer that is equal to the sum of its proper positive divisors, that is the sum of its positive divisors excluding the number itself.
- First Eight Perfect Numbers:

$$\begin{aligned} 6 &= 1+2+3 \\ 28 &= 1+2+4+7+14 \\ 496 &= 1+2+4+8+16+31+62+124+248 \end{aligned}$$

$$8128,\ 33550336,\ 8589869056,$$
$$137438691328,\ 2305843008139952128$$

Perfect Number Theorem

Theorem

An even positive integer n is perfect if and only if there exists a positive integer p such that $2^p - 1$ is prime and $n = 2^{p-1} \cdot (2^p - 1)$.

Proof

($\Leftarrow$) Let $n = 2^{p-1} \cdot (2^p - 1)$, where $2^p - 1$ is prime. Since 2^{p-1} and $2^p - 1$ are relatively prime, the sum of the divisors of n is equal to the sum of the divisors of 2^{p-1} times the sum of the divisors of $2^p - 1$. But the sum of the divisors of 2^{p-1} is

$$1 + 2 + \cdots + 2^{p-2} + 2^{p-1} = 2^p - 1$$

and the sum of the divisors of $2^p - 1$ is 2^p, since $2^p - 1$ is prime. And the product is

$$(2^p - 1) \cdot 2^p = 2 \cdot 2^{p-1}(2^p - 1) = 2n.$$

So the sum of the proper divisors of n is n and n is perfect.

Proof

($\Rightarrow$) The proof is left to the reader.

Email Address and Talk URL

Curtis Cooper's Email:
cooper@ucmo.edu

Talk:
http://www.math-cs.ucmo.edu/∼curtisc/talks/gimpskme/mersennekme.pdf