The Discovery of the 43rd and 44th Mersenne Primes at UCM

Curtis Cooper
University of Central Missouri

August 10, 2012

1. **Mersenne Primes**
2. Lucas-Lehmer Test
3. GIMPS
   - GIMPS
   - GIMPS People
   - GIMPS Links
4. 43rd, 44th, and 47th Mersenne Primes
   - $2^{30402457} - 1$
   - $2^{32582657} - 1$
   - $2^{43112609} - 1$
5. Top 10

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:

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

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)

1. Mersenne Primes
2. **Lucas-Lehmer Test**
3. GIMPS
   - GIMPS
   - GIMPS People
   - GIMPS Links
4. 43rd, 44th, and 47th Mersenne Primes
   - $2^{30402457} - 1$
   - $2^{32582657} - 1$
   - $2^{43112609} - 1$
5. Top 10

- 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

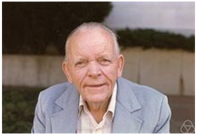
Let p be a prime number. Then

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

if and only if

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

Lucas



Lehmer

Theorem

$M_7 = 2^7 - 1 = 127$ *is prime.*

Theorem

$M_7 = 2^7 - 1 = 127$ is prime.

Proof

i	$S_i \bmod 127$

Theorem

$M_7 = 2^7 - 1 = 127$ *is prime.*

Proof

i	$S_i \bmod 127$
1	4

Theorem

$M_7 = 2^7 - 1 = 127$ *is prime.*

Proof

i	$S_i \bmod 127$
1	4
2	$(4^2 - 2) = 14 \bmod 127 = 14$

Theorem

$M_7 = 2^7 - 1 = 127$ is prime.

Proof

i	$S_i \bmod 127$
1	4
2	$(4^2 - 2) = 14 \bmod 127 = 14$
3	$(14^2 - 2) = 194 \bmod 127 = 67$

Theorem

$M_7 = 2^7 - 1 = 127$ *is prime.*

Proof

i	$S_i \bmod 127$
1	4
2	$(4^2 - 2) = 14 \bmod 127 = 14$
3	$(14^2 - 2) = 194 \bmod 127 = 67$
4	$(67^2 - 2) = 4487 \bmod 127 = 42$

Theorem

$M_7 = 2^7 - 1 = 127$ *is prime.*

Proof

i	$S_i \bmod 127$
1	4
2	$(4^2 - 2) = 14 \bmod 127 = 14$
3	$(14^2 - 2) = 194 \bmod 127 = 67$
4	$(67^2 - 2) = 4487 \bmod 127 = 42$
5	$(42^2 - 2) = 1762 \bmod 127 = 111$

Theorem

$M_7 = 2^7 - 1 = 127$ is prime.

Proof

i	$S_i \bmod 127$
1	4
2	$(4^2 - 2) = 14 \bmod 127 = 14$
3	$(14^2 - 2) = 194 \bmod 127 = 67$
4	$(67^2 - 2) = 4487 \bmod 127 = 42$
5	$(42^2 - 2) = 1762 \bmod 127 = 111$
6	$(111^2 - 2) = 12319 \bmod 127 = 0$

1. Mersenne Primes
2. Lucas-Lehmer Test
3. **GIMPS**
   - GIMPS
   - GIMPS People
   - GIMPS Links
4. 43rd, 44th, and 47th Mersenne Primes
   - $2^{30402457} - 1$
   - $2^{32582657} - 1$
   - $2^{43112609} - 1$
5. Top 10

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.

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 July 25, 2012, GIMPS had a sustained throughput of approximately 83.9 teraflops (a teraflop is 10^{12} 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 July 25, 2012, GIMPS had a sustained throughput of approximately 83.9 teraflops (a teraflop is 10^{12} floating-point operations per second).
- The GIMPS project consists of 88,074 users, 539 teams, and 642,683 CPUs.

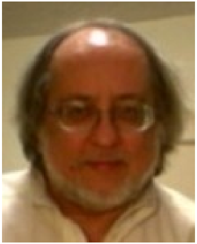
GIMPS

- 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 July 25, 2012, GIMPS had a sustained throughput of approximately 83.9 teraflops (a teraflop is 10^{12} floating-point operations per second).
- The GIMPS project consists of 88,074 users, 539 teams, and 642,683 CPUs.
- UCM has over 1000 computers performing LL-tests on Mersenne numbers.

GIMPS People

Woltman

Kurowski



Crandall

GIMPS Links

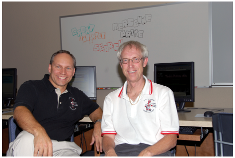
- The GIMPS home page can be found at: http://www.mersenne.org

GIMPS Links

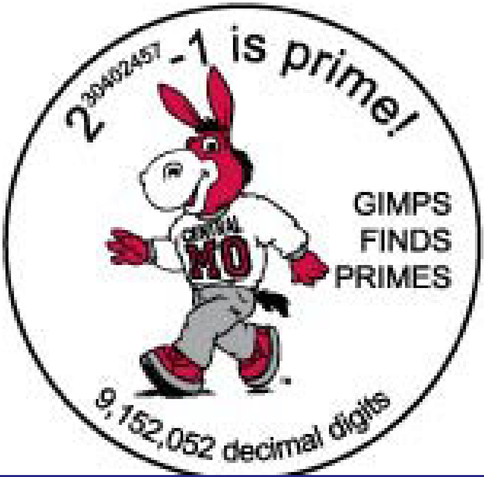
- The GIMPS home page can be found at: http://www.mersenne.org
- A Mersenne Prime discussion forum can be found at: http://www.mersenneforum.org

43rd, 44th, and 47th Mersenne Primes

	exponent	Digits in M_p	year	discoverer
43?	30402457	9152052	2005	Cooper, Boone, UCM, GIMPS
44?	32582657	9808358	2006	Cooper, Boone, UCM, GIMPS
47?	43112609	12978189	2008	Smith, UCLA, GIMPS



$2^{30402457}-1$ Button



News About $2^{30402457} - 1$

- On December 15, 2005 at 8:46:58 am (CST), computer commwd102–07l in the Communications Lab (Wood 102) proved that $2^{30402457} - 1$ is prime.

News About $2^{30402457} - 1$

- On December 15, 2005 at 8:46:58 am (CST), computer commwd102–07l in the Communications Lab (Wood 102) proved that $2^{30402457} - 1$ is prime.
- News items on the web regarding M30402457 can be found at: http://www.math-cs.ucmo.edu/∼curtisc/M30402457.html

$2^{32582657} - 1$ Button

News About $2^{32582657} - 1$

- On September 4, 2006 at 12:33:48 pm (CST), computer commwd102–04l in the Communications Lab (Wood 102) proved that $2^{32582657} - 1$ is prime.

News About $2^{32582657} - 1$

- On September 4, 2006 at 12:33:48 pm (CST), computer commwd102–04l in the Communications Lab (Wood 102) proved that $2^{32582657} - 1$ is prime.
- News items on the web regarding M32582657 can be found at: http://www.math-cs.ucmo.edu/~curtisc/M32582657.html

News About $2^{32582657} - 1$

- On September 4, 2006 at 12:33:48 pm (CST), computer commwd102–04l in the Communications Lab (Wood 102) proved that $2^{32582657} - 1$ is prime.
- News items on the web regarding M32582657 can be found at: http://www.math-cs.ucmo.edu/∼curtisc/M32582657.html
- Comments about M30402457 and M32582657 can be found at: http://primes.utm.edu/bios/code.php?code=G9

News About $2^{43112609} - 1$

- On August 23, 2008 in a computer lab in the Mathematics Department at UCLA, Edson Smith and his UCLA team proved that $2^{43112609} - 1$ is prime.

News About $2^{43112609} - 1$

- On August 23, 2008 in a computer lab in the Mathematics Department at UCLA, Edson Smith and his UCLA team proved that $2^{43112609} - 1$ is prime.
- Information about M43112609 can be found at: http://www.math.ucla.edu/∼edson/prime/

More News About $2^{43112609} - 1$

Because M43112609 was the first known ten million digit prime number, the Electronic Frontier Foundation (EFF) awarded \$100,000 to GIMPS for this discovery. According to the agreement of GIMPS volunteers, \$50,000 went to Edson Smith and the Mathematics Department at UCLA. \$25,000 went to a charity designated by George Woltman. And the remaining \$25,000 was split among the GIMPS individuals/groups who had found Mersenne primes between one and ten million digits. Since UCM had found two such primes, we received \$6,666 from GIMPS. The UCM money was distributed to colleges and units at UCM based on the percentage of computers running the Mersenne prime program in the college or unit.

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:
http://www.math-cs.ucmo.edu/~curtisc/talks/gimps3/Mersenne6.pdf