Mersenne Primes and GIMPS

Curtis Cooper and Steven Boone
ITV

April 21, 2006
Mersenne Primes

Mod Arithmetic

Lucas-Lehmer Test

FT

43 Mersenne Primes

Before Computers

Mainframe and Supercomputer Era

GIMPS Era

2^{30402457} - 1

GIMPS

GIMPS People

GIMPS Links

Top 10

Curtis Cooper and Steven Boone ITV

Mersenne Primes and GIMPS
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:

One way to generate primes is by using the Sieve of Eratosthenes. An explanation of the Sieve of Eratosthenes can be found at:

One way to generate primes is by using the Sieve of Eratosthenes. An explanation of the Sieve of Eratosthenes can be found at:


Demonstrations of the Sieve of Eratosthenes are found at:

http://www.math.utah.edu/~alfeld/Eratosthenes.html

and

http://www.faust.fr.bw.schule.de/mhb/eratosiv.htm
Marin Mersenne

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

Marin Mersenne (1588-1648)
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:

  $$3 = 2^2 - 1$$
  $$7 = 2^3 - 1$$
  $$31 = 2^5 - 1$$
  $$127 = 2^7 - 1$$
  $$2047 = 2^{11} - 1$$
A Mersenne prime is a Mersenne number that is prime.
Mersenne Primes

- A **Mersenne prime** is a Mersenne number that is prime.
- Examples of Mersenne primes are:
  
  \[3 = 2^2 - 1\]
  \[7 = 2^3 - 1\]
  \[31 = 2^5 - 1\]
  \[127 = 2^7 - 1\]
  \[8191 = 2^{13} - 1\]
Mersenne Primes

- A Mersenne prime is a Mersenne number that is prime.
- Examples of Mersenne primes are:
  
  \[ 3 = 2^2 - 1 \]
  
  \[ 7 = 2^3 - 1 \]
  
  \[ 31 = 2^5 - 1 \]
  
  \[ 127 = 2^7 - 1 \]
  
  \[ 8191 = 2^{13} - 1 \]
  
  \[ 2047 = 2^{11} - 1 = 23 \times 89. \]
<table>
<thead>
<tr>
<th>Rank</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mersenne Primes</td>
</tr>
<tr>
<td>2</td>
<td>Mod Arithmetic</td>
</tr>
<tr>
<td>3</td>
<td>Lucas-Lehmer Test</td>
</tr>
<tr>
<td>4</td>
<td>FT</td>
</tr>
<tr>
<td>5</td>
<td>43 Mersenne Primes</td>
</tr>
<tr>
<td></td>
<td>Before Computers</td>
</tr>
<tr>
<td></td>
<td>Mainframe and Supercomputer Era</td>
</tr>
<tr>
<td></td>
<td>GIMPS Era</td>
</tr>
<tr>
<td>6</td>
<td>$2^{30402457} - 1$</td>
</tr>
<tr>
<td>7</td>
<td>GIMPS</td>
</tr>
<tr>
<td></td>
<td>GIMPS</td>
</tr>
<tr>
<td></td>
<td>GIMPS People</td>
</tr>
<tr>
<td></td>
<td>GIMPS Links</td>
</tr>
<tr>
<td>8</td>
<td>Top 10</td>
</tr>
</tbody>
</table>

**Curtis Cooper and Steven Boone ITV**

**Mersenne Primes and GIMPS**
“Modulus” or Mod is Latin for “Remainder”. We are looking for the integer that occurs as a remainder when one integer is divided by another.
“Modulus” or Mod is Latin for “Remainder”. We are looking for the integer that occurs as a remainder when one integer is divided by another.

Examples

- 7 divided by 3 goes 2 times with a remainder of 1. Thus, $7 \mod 3 = 1$. 

“Modulus” or Mod is Latin for “Remainder”. We are looking for the integer that occurs as a remainder when one integer is divided by another.

**Examples**

- 7 divided by 3 goes 2 times with a remainder of 1. Thus, $7 \mod 3 = 1$.

- 8 divided by 3 goes 2 times with a remainder of 2. Thus, $8 \mod 3 = 2$. 
“Modulus” or Mod is Latin for “Remainder”. We are looking for the integer that occurs as a remainder when one integer is divided by another.

**Examples**

- 7 divided by 3 goes 2 times with a remainder of 1. Thus, \(7 \mod 3 = 1\).
- 8 divided by 3 goes 2 times with a remainder of 2. Thus, \(8 \mod 3 = 2\).
- 9 divided by 3 goes 3 times with a remainder of 0. Thus, \(9 \mod 3 = 0\).
A Mod Calculator can be found at:
http://www.antilles.k12.vi.us/math/cryptotut/mod_arithmetic.htm
A Mod Calculator can be found at:
http://www.antilles.k12.vi.us/math/cryptotut/mod_arithmetic.htm

Mod arithmetic is like clock arithmetic.

\[ a \mod b \]

is computed by starting with a clock with \( b \) hours, from 0 to \( b - 1 \).
A Mod Calculator can be found at: http://www.antilles.k12.vi.us/math/cryptotut/mod_arithmetic.htm

Mod arithmetic is like clock arithmetic.

\[ a \mod b \]

is computed by starting with a clock with \( b \) hours, from 0 to \( b - 1 \).

Counting \( a \) units on the \( b \) clock, the resulting hour we end-up at is \( a \mod b \).
More Examples

- $10 \mod 12 = 10$
More Examples

- $10 \mod 12 = 10$
- $14 \mod 12 = 2$
More Examples

- $10 \mod 12 = 10$
- $14 \mod 12 = 2$
- $22 \mod 8 = 6$
More Examples

- $10 \mod 12 = 10$
- $14 \mod 12 = 2$
- $22 \mod 8 = 6$
- $45 \mod 11$
More Examples

- $10 \mod 12 = 10$
- $14 \mod 12 = 2$
- $22 \mod 8 = 6$
- $45 \mod 11 = 1$
More Examples

- $10 \mod 12 = 10$
- $14 \mod 12 = 2$
- $22 \mod 8 = 6$
- $45 \mod 11 = 1$
- $46 \mod 7$
More Examples

- $10 \mod 12 = 10$
- $14 \mod 12 = 2$
- $22 \mod 8 = 6$
- $45 \mod 11 = 1$
- $46 \mod 7 = 4$
More Examples

- 10 mod 12 = 10
- 14 mod 12 = 2
- 22 mod 8 = 6
- 45 mod 11 = 1
- 46 mod 7 = 4
- 32 mod 5
More Examples

- $10 \text{ mod } 12 = 10$
- $14 \text{ mod } 12 = 2$
- $22 \text{ mod } 8 = 6$
- $45 \text{ mod } 11 = 1$
- $46 \text{ mod } 7 = 4$
- $32 \text{ mod } 5 = 2$
More Examples

- $10 \mod 12 = 10$
- $14 \mod 12 = 2$
- $22 \mod 8 = 6$
- $45 \mod 11 = 1$
- $46 \mod 7 = 4$
- $32 \mod 5 = 2$
- $23 \mod 9$
More Examples

- $10 \mod 12 = 10$
- $14 \mod 12 = 2$
- $22 \mod 8 = 6$
- $45 \mod 11 = 1$
- $46 \mod 7 = 4$
- $32 \mod 5 = 2$
- $23 \mod 9 = 5$
More Examples

- $10 \mod 12 = 10$
- $14 \mod 12 = 2$
- $22 \mod 8 = 6$
- $45 \mod 11 = 1$
- $46 \mod 7 = 4$
- $32 \mod 5 = 2$
- $23 \mod 9 = 5$
- $56 \mod 4$
More Examples

- \(10 \mod 12 = 10\)
- \(14 \mod 12 = 2\)
- \(22 \mod 8 = 6\)
- \(45 \mod 11 = 1\)
- \(46 \mod 7 = 4\)
- \(32 \mod 5 = 2\)
- \(23 \mod 9 = 5\)
- \(56 \mod 4 = 0\)
More Examples

- $10 \mod 12 = 10$
- $14 \mod 12 = 2$
- $22 \mod 8 = 6$
- $45 \mod 11 = 1$
- $46 \mod 7 = 4$
- $32 \mod 5 = 2$
- $23 \mod 9 = 5$
- $56 \mod 4 = 0$
- $24 \mod 11$
More Examples

- $10 \mod 12 = 10$
- $14 \mod 12 = 2$
- $22 \mod 8 = 6$
- $45 \mod 11 = 1$
- $46 \mod 7 = 4$
- $32 \mod 5 = 2$
- $23 \mod 9 = 5$
- $56 \mod 4 = 0$
- $24 \mod 11 = 2$
Mod Calculations are demonstrated at the website:
http://www.shodor.org/interactivate/activities/clock1/
• Mod Calculations are demonstrated at the website: http://www.shodor.org/interactivate/activities/clock1/

• We can do Modular Arithmetic using the following website. http://www.math.csusb.edu/faculty/susan/modular/modcalc.html
Mersenne Primes

Mod Arithmetic

Lucas-Lehmer Test

FT

43 Mersenne Primes

Before Computers

Mainframe and Supercomputer Era

GIMPS Era

GIMPS

GIMPS People

GIMPS Links

Top 10

Curtis Cooper and Steven Boone ITV

Mersenne Primes and GIMPS
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, ...
Let $p$ be a prime number. Then

$$M_p = 2^p - 1$$

is prime if and only if

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

\[ M_5 = 2^5 - 1 = 31 \text{ is prime.} \]
**Theorem**

\[ M_5 = 2^5 - 1 = 31 \] is prime.

**Proof**

\[ \begin{array}{c|c}
  i & S_i \mod 31 \\
  \hline
  1 & 4 \\
  2 & 2 \\
  3 & 14 \\
  4 & 194 \\
  5 & 62 \\
\end{array} \]
**Theorem**

\[ M_5 = 2^5 - 1 = 31 \text{ is prime.} \]

**Proof**

\[
\begin{array}{c|c}
  i & S_i \mod 31 \\
  1 & 4 \\
\end{array}
\]
Theorem

\[ M_5 = 2^5 - 1 = 31 \text{ is prime.} \]

Proof

<table>
<thead>
<tr>
<th>( i )</th>
<th>( S_i \mod 31 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>((4^2 - 2) = 14 \mod 31 = 14)</td>
</tr>
</tbody>
</table>
# Theorem

\[ M_5 = 2^5 - 1 = 31 \text{ is prime.} \]

## Proof

<table>
<thead>
<tr>
<th>( i )</th>
<th>( S_i \mod 31 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>((4^2 - 2) = 14 \mod 31 = 14)</td>
</tr>
<tr>
<td>3</td>
<td>((14^2 - 2) = 194 \mod 31 = 8)</td>
</tr>
</tbody>
</table>
Theorem

\( M_5 = 2^5 - 1 = 31 \) is prime.

Proof

\[
\begin{array}{ccc}
   i & S_i \mod 31 \\
   1 & 4 \\
   2 & (4^2 - 2) = 14 \mod 31 = 14 \\
   3 & (14^2 - 2) = 194 \mod 31 = 8 \\
   4 & (8^2 - 2) = 62 \mod 31 = 0 \\
\end{array}
\]
Theorem

\[ M_7 = 2^7 - 1 = 127 \text{ is prime.} \]
Theorem

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

Proof

$$i \quad S_i \mod 127$$
Theorem

\( M_7 = 2^7 - 1 = 127 \) is prime.

Proof

\[
\begin{array}{c|c}
    i & S_i \mod 127 \\
    
    1 & 4 \\
\end{array}
\]

Curtis Cooper and Steven Boone ITV
Mersenne Primes and GIMPS
**Theorem**

\[ M_7 = 2^7 - 1 = 127 \text{ is prime.} \]

**Proof**

<table>
<thead>
<tr>
<th>( i )</th>
<th>( S_i \mod 127 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>((4^2 - 2) = 14 \mod 127 = 14)</td>
</tr>
</tbody>
</table>
Theorem

\[ M_7 = 2^7 - 1 = 127 \text{ is prime.} \]

Proof

<table>
<thead>
<tr>
<th>( i )</th>
<th>( S_i \mod 127 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>((4^2 - 2) = 14 \mod 127 = 14)</td>
</tr>
<tr>
<td>3</td>
<td>((14^2 - 2) = 194 \mod 127 = 67)</td>
</tr>
</tbody>
</table>
Theorem

\[ M_7 = 2^7 - 1 = 127 \text{ is prime}. \]

Proof

\[
\begin{array}{ccc}
    i & S_i \mod 127 & \\
    1 & 4 & \\
    2 & (4^2 - 2) = 14 \mod 127 = 14 & \\
    3 & (14^2 - 2) = 194 \mod 127 = 67 & \\
    4 & (67^2 - 2) = 4487 \mod 127 = 42 & \\
\end{array}
\]
Theorem

\[ M_7 = 2^7 - 1 = 127 \] is prime.

Proof

\[
\begin{array}{c|c}
 i & S_i \mod 127 \\
\hline
 1 & 4 \\
 2 & (4^2 - 2) = 14 \mod 127 = 14 \\
 3 & (14^2 - 2) = 194 \mod 127 = 67 \\
 4 & (67^2 - 2) = 4487 \mod 127 = 42 \\
 5 & (42^2 - 2) = 1762 \mod 127 = 111 \\
\end{array}
\]
**Theorem**

\[ M_7 = 2^7 - 1 = 127 \text{ is prime.} \]

**Proof**

<table>
<thead>
<tr>
<th>( i )</th>
<th>( S_i \mod 127 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>((4^2 - 2) = 14 \mod 127 = 14)</td>
</tr>
<tr>
<td>3</td>
<td>((14^2 - 2) = 194 \mod 127 = 67)</td>
</tr>
<tr>
<td>4</td>
<td>((67^2 - 2) = 4487 \mod 127 = 42)</td>
</tr>
<tr>
<td>5</td>
<td>((42^2 - 2) = 1762 \mod 127 = 111)</td>
</tr>
<tr>
<td>6</td>
<td>((111^2 - 2) = 12319 \mod 127 = 0)</td>
</tr>
</tbody>
</table>
Theorem

\[ M_{11} = 2^{11} - 1 = 2047 \text{ is not prime.} \]
Theorem

\[ M_{11} = 2^{11} - 1 = 2047 \] is not prime.

Proof

\[
i \\
S_i \mod 2047
\]
Theorem

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

Proof

<table>
<thead>
<tr>
<th>$i$</th>
<th>$S_i \mod 2047$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>
Theorem

\[ M_{11} = 2^{11} - 1 = 2047 \text{ is not prime}. \]

Proof

\[
\begin{array}{cccc}
 i & S_i \text{ mod } 2047 \\
 1 & 4 \\
 2 & (4^2 - 2) = 14 \text{ mod } 2047 = 14 \\
\end{array}
\]
Theorem

\[ M_{11} = 2^{11} - 1 = 2047 \text{ is not prime.} \]

Proof

\[
\begin{array}{c|c}
 i & S_i \mod 2047 \\
1 & 4 \\
2 & (4^2 - 2) = 14 \mod 2047 = 14 \\
3 & (14^2 - 2) = 194 \mod 2047 = 194 \\
\end{array}
\]
**Theorem**

\[ M_{11} = 2^{11} - 1 = 2047 \text{ is not prime.} \]

**Proof**

<table>
<thead>
<tr>
<th>( i )</th>
<th>( S_i \mod 2047 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>((4^2 - 2) = 14 \mod 2047 = 14)</td>
</tr>
<tr>
<td>3</td>
<td>((14^2 - 2) = 194 \mod 2047 = 194)</td>
</tr>
<tr>
<td>4</td>
<td>((194^2 - 2) = 37634 \mod 2047 = 788)</td>
</tr>
</tbody>
</table>
Theorem

\[ M_{11} = 2^{11} - 1 = 2047 \text{ is not prime.} \]

Proof

\[
\begin{array}{c|c}
  i & S_i \mod 2047 \\
  \hline
  1 & 4 \\
  2 & (4^2 - 2) = 14 \mod 2047 = 14 \\
  3 & (14^2 - 2) = 194 \mod 2047 = 194 \\
  4 & (194^2 - 2) = 37634 \mod 2047 = 788 \\
  5 & (788^2 - 2) = 620942 \mod 2047 = 701 \\
\end{array}
\]
Proof cont.

\[ i \quad S_i \mod 2047 \]
Proof cont.

\[
i \quad S_i \mod 2047
\]

\[
6 \quad (701^2 - 2) = 491399 \mod 2047 = 119
\]
Proof cont.

<table>
<thead>
<tr>
<th>i</th>
<th>$S_i \mod 2047$</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>$(701^2 - 2) = 491399 \mod 2047 = 119$</td>
</tr>
<tr>
<td>7</td>
<td>$(119^2 - 2) = 14159 \mod 2047 = 1877$</td>
</tr>
</tbody>
</table>
Proof cont.

\[
i \quad S_i \mod 2047
\]

6 \quad (701^2 - 2) = 491399 \mod 2047 = 119

7 \quad (119^2 - 2) = 14159 \mod 2047 = 1877

8 \quad (1877^2 - 2) = 3523127 \mod 2047 = 240
### Proof cont.

<table>
<thead>
<tr>
<th>$i$</th>
<th>$S_i \mod 2047$</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>$(701^2 - 2) = 491399 \mod 2047 = 119$</td>
</tr>
<tr>
<td>7</td>
<td>$(119^2 - 2) = 14159 \mod 2047 = 1877$</td>
</tr>
<tr>
<td>8</td>
<td>$(1877^2 - 2) = 3523127 \mod 2047 = 240$</td>
</tr>
<tr>
<td>9</td>
<td>$(240^2 - 2) = 57598 \mod 2047 = 282$</td>
</tr>
</tbody>
</table>
Proof cont.

\[
i \quad \quad \quad \quad \quad \quad S_i \ mod \ 2047
\]

6 \quad (701^2 - 2) = 491399 \ mod \ 2047 = 119

7 \quad (119^2 - 2) = 14159 \ mod \ 2047 = 1877

8 \quad (1877^2 - 2) = 3523127 \ mod \ 2047 = 240

9 \quad (240^2 - 2) = 57598 \ mod \ 2047 = 282

10 \quad (282^2 - 2) = 79522 \ mod \ 2047 = 1736
Theorem

\[ M_{31} = 2^{31} - 1 = 2147483647 \text{ is prime.} \]
Theorem

\[ M_{31} = 2^{31} - 1 = 2147483647 \] is prime.

Proof

\[
i \quad S_i \mod 2^{31} - 1
\]
**Theorem**

\[ M_{31} = 2^{31} - 1 = 2147483647 \text{ is prime}. \]

**Proof**

<table>
<thead>
<tr>
<th>i</th>
<th>( S_i \mod 2^{31} - 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>
Theorem

\[ M_{31} = 2^{31} - 1 = 2147483647 \text{ is prime.} \]

Proof

<table>
<thead>
<tr>
<th>i</th>
<th>( S_i \mod 2^{31} - 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>14</td>
</tr>
</tbody>
</table>
Theorem

\[ M_{31} = 2^{31} - 1 = 2147483647 \text{ is prime.} \]

Proof

<table>
<thead>
<tr>
<th>i</th>
<th>( S_i \mod 2^{31} - 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>14</td>
</tr>
<tr>
<td>3</td>
<td>194</td>
</tr>
</tbody>
</table>
**Theorem**

\[ M_{31} = 2^{31} - 1 = 2147483647 \text{ is prime.} \]

**Proof**

<table>
<thead>
<tr>
<th>( i )</th>
<th>( S_i \mod 2^{31} - 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>14</td>
</tr>
<tr>
<td>3</td>
<td>194</td>
</tr>
<tr>
<td>4</td>
<td>37634</td>
</tr>
</tbody>
</table>
Theorem

\[ M_{31} = 2^{31} - 1 = 2147483647 \text{ is prime.} \]

Proof

<table>
<thead>
<tr>
<th>( i )</th>
<th>( S_i \mod 2^{31} - 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>14</td>
</tr>
<tr>
<td>3</td>
<td>194</td>
</tr>
<tr>
<td>4</td>
<td>37634</td>
</tr>
<tr>
<td>5</td>
<td>1416317954</td>
</tr>
</tbody>
</table>
**Theorem**

\[ M_{31} = 2^{31} - 1 = 2147483647 \text{ is prime.} \]

**Proof**

<table>
<thead>
<tr>
<th>( i )</th>
<th>( S_i \mod 2^{31} - 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>14</td>
</tr>
<tr>
<td>3</td>
<td>194</td>
</tr>
<tr>
<td>4</td>
<td>3,763,4</td>
</tr>
<tr>
<td>5</td>
<td>14,163,179,54</td>
</tr>
<tr>
<td>6</td>
<td>66,967,083,8</td>
</tr>
</tbody>
</table>
### Theorem

\[ M_{31} = 2^{31} - 1 = 2147483647 \text{ is prime.} \]

### Proof

<table>
<thead>
<tr>
<th>(i)</th>
<th>(S_i \mod 2^{31} - 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>14</td>
</tr>
<tr>
<td>3</td>
<td>194</td>
</tr>
<tr>
<td>4</td>
<td>37634</td>
</tr>
<tr>
<td>5</td>
<td>1416317954</td>
</tr>
<tr>
<td>6</td>
<td>669670838</td>
</tr>
<tr>
<td>7</td>
<td>1937259419</td>
</tr>
</tbody>
</table>
Theorem

\[ M_{31} = 2^{31} - 1 = 2147483647 \] is prime.

Proof

<table>
<thead>
<tr>
<th>( i )</th>
<th>( S_i \mod 2^{31} - 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>14</td>
</tr>
<tr>
<td>3</td>
<td>194</td>
</tr>
<tr>
<td>4</td>
<td>37634</td>
</tr>
<tr>
<td>5</td>
<td>1416317954</td>
</tr>
<tr>
<td>6</td>
<td>669670838</td>
</tr>
<tr>
<td>7</td>
<td>1937259419</td>
</tr>
<tr>
<td>8</td>
<td>425413602</td>
</tr>
</tbody>
</table>
Proof cont.

<table>
<thead>
<tr>
<th>( i )</th>
<th>( S_i \mod 2^{31} - 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>842014276</td>
</tr>
<tr>
<td>10</td>
<td>12692426</td>
</tr>
<tr>
<td>11</td>
<td>2044502122</td>
</tr>
<tr>
<td>12</td>
<td>1119438707</td>
</tr>
<tr>
<td>13</td>
<td>1190075270</td>
</tr>
<tr>
<td>14</td>
<td>1450757861</td>
</tr>
<tr>
<td>15</td>
<td>877666528</td>
</tr>
<tr>
<td>16</td>
<td>630853853</td>
</tr>
<tr>
<td>17</td>
<td>940321271</td>
</tr>
<tr>
<td>18</td>
<td>512995887</td>
</tr>
<tr>
<td>19</td>
<td>692931217</td>
</tr>
</tbody>
</table>
### Proof cont.

<table>
<thead>
<tr>
<th>$i$</th>
<th>$S_i \mod 2^{31} - 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>1883625615</td>
</tr>
<tr>
<td>21</td>
<td>1992425718</td>
</tr>
<tr>
<td>22</td>
<td>721929267</td>
</tr>
<tr>
<td>23</td>
<td>27220594</td>
</tr>
<tr>
<td>24</td>
<td>1570086542</td>
</tr>
<tr>
<td>25</td>
<td>1676390412</td>
</tr>
</tbody>
</table>
## Proof cont.

<table>
<thead>
<tr>
<th>$i$</th>
<th>$S_i \mod 2^{31} - 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>1883625615</td>
</tr>
<tr>
<td>21</td>
<td>1992425718</td>
</tr>
<tr>
<td>22</td>
<td>721929267</td>
</tr>
<tr>
<td>23</td>
<td>27220594</td>
</tr>
<tr>
<td>24</td>
<td>1570086542</td>
</tr>
<tr>
<td>25</td>
<td>1676390412</td>
</tr>
<tr>
<td>26</td>
<td>1159251674</td>
</tr>
</tbody>
</table>
### Proof cont.

<table>
<thead>
<tr>
<th>$i$</th>
<th>$S_i \mod 2^{31} - 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>1883625615</td>
</tr>
<tr>
<td>21</td>
<td>1992425718</td>
</tr>
<tr>
<td>22</td>
<td>721929267</td>
</tr>
<tr>
<td>23</td>
<td>27220594</td>
</tr>
<tr>
<td>24</td>
<td>1570086542</td>
</tr>
<tr>
<td>25</td>
<td>1676390412</td>
</tr>
<tr>
<td>26</td>
<td>1159251674</td>
</tr>
<tr>
<td>27</td>
<td>211987665</td>
</tr>
</tbody>
</table>
## Proof cont.

<table>
<thead>
<tr>
<th>$i$</th>
<th>$S_i \mod 2^{31} - 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>1883625615</td>
</tr>
<tr>
<td>21</td>
<td>1992425718</td>
</tr>
<tr>
<td>22</td>
<td>721929267</td>
</tr>
<tr>
<td>23</td>
<td>27220594</td>
</tr>
<tr>
<td>24</td>
<td>1570086542</td>
</tr>
<tr>
<td>25</td>
<td>1676390412</td>
</tr>
<tr>
<td>26</td>
<td>1159251674</td>
</tr>
<tr>
<td>27</td>
<td>211987665</td>
</tr>
<tr>
<td>28</td>
<td>1181536708</td>
</tr>
</tbody>
</table>
Proof cont.

<table>
<thead>
<tr>
<th>$i$</th>
<th>$S_i \mod 2^{31} - 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>1883625615</td>
</tr>
<tr>
<td>21</td>
<td>1992425718</td>
</tr>
<tr>
<td>22</td>
<td>721929267</td>
</tr>
<tr>
<td>23</td>
<td>27220594</td>
</tr>
<tr>
<td>24</td>
<td>1570086542</td>
</tr>
<tr>
<td>25</td>
<td>1676390412</td>
</tr>
<tr>
<td>26</td>
<td>1159251674</td>
</tr>
<tr>
<td>27</td>
<td>211987665</td>
</tr>
<tr>
<td>28</td>
<td>1181536708</td>
</tr>
<tr>
<td>29</td>
<td>65536</td>
</tr>
</tbody>
</table>
### Proof cont.

<table>
<thead>
<tr>
<th>$i$</th>
<th>$S_i \mod 2^{31} - 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>1883625615</td>
</tr>
<tr>
<td>21</td>
<td>1992425718</td>
</tr>
<tr>
<td>22</td>
<td>721929267</td>
</tr>
<tr>
<td>23</td>
<td>27220594</td>
</tr>
<tr>
<td>24</td>
<td>1570086542</td>
</tr>
<tr>
<td>25</td>
<td>1676390412</td>
</tr>
<tr>
<td>26</td>
<td>1159251674</td>
</tr>
<tr>
<td>27</td>
<td>211987665</td>
</tr>
<tr>
<td>28</td>
<td>1181536708</td>
</tr>
<tr>
<td>29</td>
<td>65536</td>
</tr>
<tr>
<td>30</td>
<td>0</td>
</tr>
</tbody>
</table>
Mersenne Primes
Mod Arithmetic
Lucas-Lehmer Test
FT

43 Mersenne Primes

Before Computers
Mainframe and Supercomputer Era
GIMPS Era

GIMPS

GIMPS
GIMPS People
GIMPS Links

Top 10

Curtis Cooper and Steven Boone ITV
Mersenne Primes and GIMPS
Multiply two $N$-digit numbers $A$ and $B$

- In grammar school, we multiply each digit of $B$ by the rightmost digit of $A$. 
Multiply two $N$-digit numbers $A$ and $B$

- In grammar school, we multiply each digit of $B$ by the rightmost digit of $A$.
- Then shift $B$ to the left one place (add a 0 at the right end) and multiply that by the next higher-order digit of $A$ and so forth.
Multiply two $N$-digit numbers $A$ and $B$

- In grammar school, we multiply each digit of $B$ by the rightmost digit of $A$.
- Then shift $B$ to the left one place (add a 0 at the right end) and multiply that by the next higher-order digit of $A$ and so forth.
- Then sum all the $N$ intermediate products.
Multiply two $N$-digit numbers $A$ and $B$

- In grammar school, we multiply each digit of $B$ by the rightmost digit of $A$.
- Then shift $B$ to the left one place (add a 0 at the right end) and multiply that by the next higher-order digit of $A$ and so forth.
- Then sum all the $N$ intermediate products.
- The operation count is on the order of $N^2$ digit multiplications and a similar number of digit additions.
Multiply two $N$-digit numbers $A$ and $B$

- In grammar school, we multiply each digit of $B$ by the rightmost digit of $A$.
- Then shift $B$ to the left one place (add a 0 at the right end) and multiply that by the next higher-order digit of $A$ and so forth.
- Then sum all the $N$ intermediate products.
- The operation count is on the order of $N^2$ digit multiplications and a similar number of digit additions.
- This is called a discrete convolution.
Fourier Transform

- The Fourier Transform allows us to do discrete convolutions very fast.
Fourier Transform

- The Fourier Transform allows us to do discrete convolutions very fast.
- Treat each of the numbers $A$ and $B$ as a vector with $N$ components (the digits of the number).
Fourier Transform

- The Fourier Transform allows us to do discrete convolutions very fast.
- Treat each of the numbers $A$ and $B$ as a vector with $N$ components (the digits of the number).
- Do a FT on each of the two vectors to get a pair of vectors $A^{FT}$ and $B^{FT}$. 
Fourier Transform

- The Fourier Transform allows us to do discrete convolutions very fast.
- Treat each of the numbers $A$ and $B$ as a vector with $N$ components (the digits of the number).
- Do a FT on each of the two vectors to get a pair of vectors $A^{FT}$ and $B^{FT}$.
- In this Fourier space, a convolution looks just like digit-by-digit multiplication.
Fourier Transform

- The Fourier Transform allows us to do discrete convolutions very fast.
- Treat each of the numbers $A$ and $B$ as a vector with $N$ components (the digits of the number).
- Do a FT on each of the two vectors to get a pair of vectors $A^{FT}$ and $B^{FT}$.
- In this Fourier space, a convolution looks just like digit-by-digit multiplication.
- (That is, if we multiply each individual component (just a number) of $A^{FT}$ with the corresponding one in $B^{FT}$, the result is the Fourier Transformed version of the convolution of $A$ and $B$.)
In Fourier space, a convolution costs $N$ operations.
Fourier Transform

- In Fourier space, a convolution costs $N$ operations.
- To get back the result we want, we do an inverse Fourier transform on the single vector resulting from the digit-by-digit multiply of $A^{FT}$ and $B^{FT}$. 
Fourier Transform Costs

- The Fourier transform costs $O(N \log_2(N))$. 
Fourier Transform Costs

- The Fourier transform costs $O(N \log_2(N))$.
- The constant in the big-Oh term is about 5.
Fourier Transform Costs

- The Fourier transform costs $O(N \log_2(N))$.
- The constant in the big-Oh term is about 5.
- Since we need to do two such transforms, an estimate of the FT cost is about $10N \log_2(N)$. 

Curtis Cooper and Steven Boone ITV
Mersenne Primes and GIMPS
Fourier Transform Costs

- The Fourier transform costs $O(N \log_2(N))$.
- The constant in the big-Oh term is about 5.
- Since we need to do two such transforms, an estimate of the FT cost is about $10N \log_2(N)$.
- For $N$ sufficiently large, this is faster than the grammar school way.
Fourier Transform Costs

- The Fourier transform costs $O(N \log_2(N))$.
- The constant in the big-Oh term is about 5.
- Since we need to do two such transforms, an estimate of the FT cost is about $10N \log_2(N)$.
- For $N$ sufficiently large, this is faster than the grammar school way.
- One final thing, if we FT-multiply two numbers with $N$ digits, we expect the product to have as many as $2N$ digits.
The Fourier transform costs $O(N \log_2(N))$.

The constant in the big-Oh term is about 5.

Since we need to do two such transforms, an estimate of the FT cost is about $10N \log_2(N)$.

For $N$ sufficiently large, this is faster than the grammar school way.

One final thing, if we FT-multiply two numbers with $N$ digits, we expect the product to have as many as $2N$ digits.

Thus, we need to do FTs of length $2N$ to leave room for the digits at the high end.
The numbers 12 and 23 are represented as

\[ A = \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 3 \\ 2 \\ 0 \\ 0 \end{pmatrix}. \]
FT Example - $12 \times 23 = 276$

The numbers 12 and 23 are represented as

$$A = \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 3 \\ 2 \\ 0 \\ 0 \end{pmatrix}.$$

We use the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix},$$

where $i = \sqrt{-1}$ to find the Fourier transform of $A$ and $B$. 
Fourier Transform of Vectors

We next multiply the above matrix by $A$ and $B$ to find their Fourier transforms.
Fourier Transform of Vectors

We next multiply the above matrix by $A$ and $B$ to find their Fourier transforms. Therefore,

$$A^{FT} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 2 + i \\ 1 \\ 2 - i \end{pmatrix}.$$
Fourier Transform of Vectors

We next multiply the above matrix by $A$ and $B$ to find their Fourier transforms. Therefore,

$$A^{FT} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \begin{bmatrix} 2 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \cdot i \\ 1 \\ 2 - i \end{bmatrix}. \quad \text{And}$$

$$B^{FT} = \begin{bmatrix} 5 \\ 3 + 2i \\ 1 \\ 3 - 2i \end{bmatrix}. $$
FT Discrete Convolution of A and B

Doing component-by-component multiplication, $A^{FT} \ast B^{FT}$ gives

$$\begin{pmatrix} 3 \\ 2 + i \\ 1 \\ 2 - i \end{pmatrix} \ast \begin{pmatrix} 5 \\ 3 + 2i \\ 1 \\ 3 - 2i \end{pmatrix} = \begin{pmatrix} 15 \\ 4 + 7i \\ 1 \\ 4 - 7i \end{pmatrix}.$$
Inverse Fourier Transform of Vector

The inverse Fourier transform of this vector uses the Fourier transform matrix, but the signs on the $i$-terms are switched and a factor of $1/4$ multiplying the whole matrix.

$$
\frac{1}{4} \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & -i & -1 & i \\
1 & -1 & 1 & -1 \\
i & 1 & -1 & -i
\end{pmatrix}.
$$
Inverse Fourier Transform of Vector

The inverse Fourier transform of this vector uses the Fourier transform matrix, but the signs on the \( i \)-terms are switched and a factor of \( 1/4 \) multiplying the whole matrix.

\[
\frac{1}{4} \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & -i & -1 & i \\
1 & -1 & 1 & -1 \\
1 & i & -1 & -i
\end{pmatrix}.
\]

Multiplying this matrix by our vector gives

\[
\begin{pmatrix}
6 \\
7 \\
2 \\
0
\end{pmatrix}.
\]
Inverse Fourier Transform of Vector

The inverse Fourier transform of this vector uses the Fourier transform matrix, but the signs on the $i$-terms are switched and a factor of $\frac{1}{4}$ multiplying the whole matrix.

$$\frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}.$$

Multiplying this matrix by our vector gives

$$\begin{pmatrix} 6 \\ 7 \\ 2 \\ 0 \end{pmatrix}.$$
43 Mersenne Primes

- Before Computers
- Mainframe and Supercomputer Era
- GIMPS Era

$2^{30402457} - 1$

GIMPS

- GIMPS
- GIMPS People
- GIMPS Links

Top 10

Curtis Cooper and Steven Boone ITV

Mersenne Primes and GIMPS
### Before Computers

<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>55</td>
<td>1642</td>
<td>anonymous</td>
</tr>
<tr>
<td>2</td>
<td>33</td>
<td>1644</td>
<td>Cataldi</td>
</tr>
<tr>
<td>3</td>
<td>43</td>
<td>1652</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>58</td>
<td>1664</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>67</td>
<td>1669</td>
<td>anonymous</td>
</tr>
<tr>
<td>6</td>
<td>83</td>
<td>1679</td>
<td>Cataldi</td>
</tr>
<tr>
<td>7</td>
<td>89</td>
<td>1681</td>
<td></td>
</tr>
</tbody>
</table>

Curtis Cooper and Steven Boone: ITV

Mersenne Primes and GIMPS
### Before Computers

<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>1</td>
<td>—</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>1</td>
<td>—</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>2</td>
<td>—</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>3</td>
<td>—</td>
</tr>
</tbody>
</table>
### Before Computers

<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>1</td>
<td>—</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>1</td>
<td>—</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>2</td>
<td>—</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>3</td>
<td>—</td>
</tr>
<tr>
<td>5</td>
<td>13</td>
<td>4</td>
<td>1456</td>
</tr>
</tbody>
</table>
Before Computers

<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>1</td>
<td>—</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>1</td>
<td>—</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>2</td>
<td>—</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>3</td>
<td>—</td>
</tr>
<tr>
<td>5</td>
<td>13</td>
<td>4</td>
<td>1456 anonymous</td>
</tr>
<tr>
<td>6</td>
<td>17</td>
<td>6</td>
<td>1588 Cataldi</td>
</tr>
<tr>
<td>7</td>
<td>19</td>
<td>6</td>
<td>1588 Cataldi</td>
</tr>
</tbody>
</table>
Before Computers

<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>31</td>
<td>10</td>
<td>1772 Euler</td>
</tr>
</tbody>
</table>

Curtis Cooper and Steven Boone ITV
Mersenne Primes and GIMPS
### Before Computers

<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>31</td>
<td>10</td>
<td>1772 Euler</td>
</tr>
<tr>
<td>9</td>
<td>61</td>
<td>19</td>
<td>1883 Pervushin</td>
</tr>
</tbody>
</table>
### Before Computers

<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>31</td>
<td>10</td>
<td>1772</td>
</tr>
<tr>
<td>9</td>
<td>61</td>
<td>19</td>
<td>1883</td>
</tr>
<tr>
<td>10</td>
<td>89</td>
<td>27</td>
<td>1911</td>
</tr>
<tr>
<td>11</td>
<td>107</td>
<td>33</td>
<td>1914</td>
</tr>
</tbody>
</table>
### Before Computers

Below are details of the most notable Mersenne primes discovered before the advent of computers:

<table>
<thead>
<tr>
<th>Exponent</th>
<th>Digits in $M_p$</th>
<th>Year</th>
<th>Discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>127</td>
<td>39</td>
<td>1876</td>
</tr>
</tbody>
</table>

Curtis Cooper and Steven Boone ITV

**Mersenne Primes and GIMPS**
## Mainframe and Supercomputer Era

<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>521</td>
<td>1952</td>
<td>Robinson</td>
</tr>
<tr>
<td>14</td>
<td>607</td>
<td>1952</td>
<td>Robinson</td>
</tr>
<tr>
<td>15</td>
<td>1279</td>
<td>1952</td>
<td>Robinson</td>
</tr>
<tr>
<td>16</td>
<td>2203</td>
<td>1952</td>
<td>Robinson</td>
</tr>
<tr>
<td>17</td>
<td>2281</td>
<td>1952</td>
<td>Robinson</td>
</tr>
</tbody>
</table>
## Mainframe and Supercomputer Era

<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>3217</td>
<td>969</td>
<td>1957</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Riesel</td>
</tr>
</tbody>
</table>
### Mainframe and Supercomputer Era

<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>3217</td>
<td>969</td>
<td>1957</td>
</tr>
<tr>
<td>19</td>
<td>4253</td>
<td>1281</td>
<td>1961</td>
</tr>
<tr>
<td>20</td>
<td>4423</td>
<td>1332</td>
<td>1961</td>
</tr>
</tbody>
</table>
### Mainframe and Supercomputer Era

<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>3217</td>
<td>969</td>
<td>1957</td>
</tr>
<tr>
<td>19</td>
<td>4253</td>
<td>1281</td>
<td>1961</td>
</tr>
<tr>
<td>20</td>
<td>4423</td>
<td>1332</td>
<td>1961</td>
</tr>
<tr>
<td>21</td>
<td>9689</td>
<td>2917</td>
<td>1963</td>
</tr>
<tr>
<td>22</td>
<td>9941</td>
<td>2993</td>
<td>1963</td>
</tr>
<tr>
<td>23</td>
<td>11213</td>
<td>3376</td>
<td>1963</td>
</tr>
</tbody>
</table>
## Mainframe and Supercomputer Era

<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>3217</td>
<td>969</td>
<td>1957 Riesel</td>
</tr>
<tr>
<td>19</td>
<td>4253</td>
<td>1281</td>
<td>1961 Hurwitz</td>
</tr>
<tr>
<td>20</td>
<td>4423</td>
<td>1332</td>
<td>1961 Hurwitz</td>
</tr>
<tr>
<td>21</td>
<td>9689</td>
<td>2917</td>
<td>1963 Gillies</td>
</tr>
<tr>
<td>22</td>
<td>9941</td>
<td>2993</td>
<td>1963 Gillies</td>
</tr>
<tr>
<td>23</td>
<td>11213</td>
<td>3376</td>
<td>1963 Gillies</td>
</tr>
<tr>
<td>24</td>
<td>19937</td>
<td>6002</td>
<td>1971 Tuckerman</td>
</tr>
</tbody>
</table>
### Mainframe and Supercomputer Era

<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>21701</td>
<td>6533</td>
<td>1978</td>
</tr>
<tr>
<td>26</td>
<td>23209</td>
<td>6987</td>
<td>1979</td>
</tr>
</tbody>
</table>

Curtis Cooper and Steven Boone ITV

Mersenne Primes and GIMPS
### Mersenne Primes

#### 43 Mersenne Primes

<table>
<thead>
<tr>
<th>Exponent</th>
<th>Digits in $M_p$</th>
<th>Year</th>
<th>Discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>21701</td>
<td>1978</td>
<td>Noll and Nickel</td>
</tr>
<tr>
<td>26</td>
<td>23209</td>
<td>1979</td>
<td>Noll</td>
</tr>
<tr>
<td>27</td>
<td>44497</td>
<td>1979</td>
<td>Nelson and Slowinski</td>
</tr>
<tr>
<td>exponent</td>
<td>Digits in $M_p$</td>
<td>year</td>
<td>discoverer</td>
</tr>
<tr>
<td>----------</td>
<td>----------------</td>
<td>------</td>
<td>---------------------</td>
</tr>
<tr>
<td>25</td>
<td>21701</td>
<td>1978</td>
<td>Noll and Nickel</td>
</tr>
<tr>
<td>26</td>
<td>23209</td>
<td>1979</td>
<td>Noll</td>
</tr>
<tr>
<td>27</td>
<td>44497</td>
<td>1979</td>
<td>Nelson and Slowinski</td>
</tr>
<tr>
<td>28</td>
<td>86243</td>
<td>1982</td>
<td>Slowinski</td>
</tr>
</tbody>
</table>

Mainframe and Supercomputer Era

Curtis Cooper and Steven Boone ITV
Mersenne Primes and GIMPS
<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>21701</td>
<td>6533</td>
<td>1978 Noll and Nickel</td>
</tr>
<tr>
<td>26</td>
<td>23209</td>
<td>6987</td>
<td>1979 Noll</td>
</tr>
<tr>
<td>27</td>
<td>44497</td>
<td>13395</td>
<td>1979 Nelson and Slowinski</td>
</tr>
<tr>
<td>28</td>
<td>86243</td>
<td>25962</td>
<td>1982 Slowinski</td>
</tr>
<tr>
<td>29</td>
<td>110503</td>
<td>33265</td>
<td>1988 Colquitt and Welsh</td>
</tr>
</tbody>
</table>
### Mainframe and Supercomputer Era

<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>132049</td>
<td>39751</td>
<td>1983 Slowinski</td>
</tr>
<tr>
<td>31</td>
<td>216091</td>
<td>65050</td>
<td>1985 Slowinski</td>
</tr>
</tbody>
</table>
### Mersenne Primes and GIMPS

#### Mainframe and Supercomputer Era

<table>
<thead>
<tr>
<th>Exponent</th>
<th>Digits in $M_p$</th>
<th>Year</th>
<th>Discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>132049</td>
<td>1983</td>
<td>Slowinski</td>
</tr>
<tr>
<td>31</td>
<td>216091</td>
<td>1985</td>
<td>Slowinski</td>
</tr>
<tr>
<td>32</td>
<td>756839</td>
<td>1992</td>
<td>Slowinski and Gage</td>
</tr>
<tr>
<td>33</td>
<td>859433</td>
<td>1994</td>
<td>Slowinski and Gage</td>
</tr>
<tr>
<td>34</td>
<td>1257787</td>
<td>1996</td>
<td>Slowinski and Gage</td>
</tr>
</tbody>
</table>
## GIMPS (Woltman, Kurowski, et al.) Era

<table>
<thead>
<tr>
<th>Exponent</th>
<th>Digits in $M_p$</th>
<th>Year</th>
<th>Discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>1398269</td>
<td>1996</td>
<td>Armengaud, GIMPS</td>
</tr>
</tbody>
</table>
GIMPS (Woltman, Kurowski, et al.) Era

<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>1398269</td>
<td>1996</td>
<td>Armengaud, GIMPS</td>
</tr>
<tr>
<td>36</td>
<td>2976221</td>
<td>1997</td>
<td>Spence, GIMPS</td>
</tr>
</tbody>
</table>
### GIMPS (Woltman, Kurowski, et al.) Era

<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>1398269</td>
<td>1996</td>
<td>Armengaud, GIMPS</td>
</tr>
<tr>
<td>36</td>
<td>2976221</td>
<td>1997</td>
<td>Spence, GIMPS</td>
</tr>
<tr>
<td>37</td>
<td>3021377</td>
<td>1998</td>
<td>Clarkson, GIMPS</td>
</tr>
</tbody>
</table>
### GIMPS (Woltman, Kurowski, et al.) Era

<table>
<thead>
<tr>
<th>Exponent</th>
<th>Digits in $M_p$</th>
<th>Year</th>
<th>Discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>1398269</td>
<td>1996</td>
<td>Armengaud, GIMPS</td>
</tr>
<tr>
<td>36</td>
<td>2976221</td>
<td>1997</td>
<td>Spence, GIMPS</td>
</tr>
<tr>
<td>37</td>
<td>3021377</td>
<td>1998</td>
<td>Clarkson, GIMPS</td>
</tr>
<tr>
<td>38</td>
<td>6972593</td>
<td>1999</td>
<td>Hajratwala, GIMPS</td>
</tr>
</tbody>
</table>

Curtis Cooper and Steven Boone ITV

Mersenne Primes and GIMPS
<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>39?</td>
<td>13466917</td>
<td>2001</td>
<td>Cameron, GIMPS</td>
</tr>
<tr>
<td></td>
<td>4053946</td>
<td></td>
<td></td>
</tr>
<tr>
<td>exponent</td>
<td>Digits in $M_p$</td>
<td>year</td>
<td>discoverer</td>
</tr>
<tr>
<td>----------</td>
<td>----------------</td>
<td>------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>39?</td>
<td>13466917</td>
<td>2001</td>
<td>Cameron, GIMPS</td>
</tr>
<tr>
<td>40?</td>
<td>20996011</td>
<td>2003</td>
<td>Shafer, GIMPS</td>
</tr>
</tbody>
</table>
### GIMPS Era

<table>
<thead>
<tr>
<th>exponent</th>
<th>Digits in $M_p$</th>
<th>year</th>
<th>discoverer</th>
</tr>
</thead>
<tbody>
<tr>
<td>41?</td>
<td>24036583</td>
<td>2004</td>
<td>Findley, GIMPS</td>
</tr>
<tr>
<td>42?</td>
<td>25964951</td>
<td>2005</td>
<td>Nowak, GIMPS</td>
</tr>
<tr>
<td>43?</td>
<td>30402457</td>
<td>2005</td>
<td>Cooper, Boone, CMSU, GIMPS</td>
</tr>
<tr>
<td>exponent</td>
<td>Digits in $M_p$</td>
<td>year</td>
<td>discoverer</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
<td>------</td>
<td>---------------------</td>
</tr>
<tr>
<td>41?</td>
<td>24036583</td>
<td>2004</td>
<td>Findley, GIMPS</td>
</tr>
<tr>
<td>42?</td>
<td>25964951</td>
<td>2005</td>
<td>Nowak, GIMPS</td>
</tr>
<tr>
<td>exponent</td>
<td>Digits in $M_p$</td>
<td>year</td>
<td>discoverer</td>
</tr>
<tr>
<td>----------</td>
<td>----------------</td>
<td>------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>41?</td>
<td>24036583</td>
<td>2004</td>
<td>Findley, GIMPS</td>
</tr>
<tr>
<td>42?</td>
<td>25964951</td>
<td>2005</td>
<td>Nowak, GIMPS</td>
</tr>
<tr>
<td>43?</td>
<td>30402457</td>
<td>2005</td>
<td>Cooper, Boone, CMSU, GIMPS</td>
</tr>
</tbody>
</table>

Curtis Cooper and Steven Boone ITV

Mersenne Primes and GIMPS
Mersenne Primes

Mod Arithmetic

Lucas-Lehmer Test

FT

43 Mersenne Primes

Before Computers

Mainframe and Supercomputer Era

GIMPS Era

$2^{30402457} - 1$

GIMPS

GIMPS People

GIMPS Links

Top 10

Curtis Cooper and Steven Boone ITV

Mersenne Primes and GIMPS
$2^{30402457} - 1$ Button

Curtis Cooper and Steven Boone ITV
Mersenne Primes and GIMPS
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.cmsu.edu/~curtisc/M30402457.html
**Digits of** $2^{30402457} - 1$

The digits of M30402457 can be found at:
http://mersenneforum.org/txt/43.txt
Digits of $2^{30402457} - 1$

- The digits of M30402457 can be found at: http://mersenneforum.org/txt/43.txt
- Comments about M30402457 can be found at: http://primes.utm.edu/bios/code.php?code=G9
Mersenne Primes
Mod Arithmetic
Lucas-Lehmer Test
FT
43 Mersenne Primes

Before Computers
Mainframe and Supercomputer Era
GIMPS Era

GIMPS
GIMPS
GIMPS People
GIMPS Links

Top 10

Curtis Cooper and Steven Boone ITV
Mersenne Primes and GIMPS
GIMPS is a collaborative project of volunteers who are searching for Mersenne prime numbers. The software used by GIMPS volunteers is Prime 95 and Mprime. 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 Prime 95 and Mprime. This software can be downloaded from the Internet for free.

- George Woltman founded GIMPS in January 1996 and wrote the prime testing software.
GIMPS is a collaborative project of volunteers who are searching for Mersenne prime numbers. The software used by GIMPS volunteers is Prime 95 and Mprime. 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 February 4, 2005, GIMPS had a sustained throughput of approximately 20 trillion calculations 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 February 4, 2005, GIMPS had a sustained throughput of approximately 20 trillion calculations per second.

• The GIMPS project consists of 70,000 networked computers.
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 4, 2005, GIMPS had a sustained throughput of approximately 20 trillion calculations per second.

The GIMPS project consists of 70,000 networked computers.

CMSU has over 850 computers performing LL-tests on Mersenne numbers.
GIMPS People

Curtis Cooper and Steven Boone ITV
Mersenne Primes and GIMPS
Mersenne Primes

Mod Arithmetic

Lucas-Lehmer Test

FT

43 Mersenne Primes

\[ 2^{30402457} - 1 \]

GIMPS

Top 10

GIMPS People

Woltman

Curtis Cooper and Steven Boone ITV

Mersenne Primes and GIMPS
Mersenne Primes

Mod Arithmetic

Lucas-Lehmer Test

FT

43 Mersenne Primes

$2^{30402457} - 1$

GIMPS

Top 10

GIMPS People

Woltman

Kurowski

Curtis Cooper and Steven Boone ITV

Mersenne Primes and GIMPS
GIMPS People

Woltman  Kurowski  Crandall
Tony Reix of Bull S.A. in Grenoble, France, using 16 Itanium2 1.5 GHz CPUs of a Bull NovaScale 6160 HPC at Bull Grenoble Research Center, double-checked M30402457 in 5 days.
Tony Reix of Bull S.A. in Grenoble, France, using 16 Itanium2 1.5 GHz CPUs of a Bull NovaScale 6160 HPC at Bull Grenoble Research Center, double-checked M30402457 in 5 days.

T.Rex ran the Glucas program by Guillermo Ballester Valor of Granada, Spain.
Tony Reix of Bull S.A. in Grenoble, France, using 16 Itanium2 1.5 GHz CPUs of a Bull NovaScale 6160 HPC at Bull Grenoble Research Center, double-checked M30402457 in 5 days.

T.Rex ran the Glucas program by Guillermo Ballester Valor of Granada, Spain.

Jeff Gilchrist of Elytra Enterprises Inc. in Ottawa, Canada, using fourteen days of time on 14 CPUs of a Compaq Alpha GS160 1.2 GHz CPU server at SHARCNET, triple-checked M30402457.
Mersenne Primes

Mod Arithmetic

Lucas-Lehmer Test

FT

43 Mersenne Primes

2^{30402457} - 1

GIMPS

Top 10

GIMPS People

Curtis Cooper and Steven Boone ITV

Mersenne Primes and GIMPS
Mersenne Primes

GIMPS People

T. Rex

Valor

Curtis Cooper and Steven Boone ITV

Mersenne Primes and GIMPS
Mersenne Primes and GIMPS

GIMPS People

T. Rex
Valor
Gilchrist
The GIMPS home page can be found at: http://www.mersenne.org
The GIMPS home page can be found at:
http://www.mersenne.org

Team Prime Rib’s home page can be found at:
http://www.teamprimerib.com/
GIMPS Links

- The GIMPS home page can be found at: http://www.mersenne.org
- Team Prime Rib’s home page can be found at: http://www.teamprimerib.com/
- A Mersenne Prime discussion forum can be found at: http://www.mersenneforum.org
The GIMPS home page can be found at:
http://www.mersenne.org

Team Prime Rib’s home page can be found at:
http://www.teamprimerib.com/

A Mersenne Prime discussion forum can be found at:
http://www.mersenneforum.org

The GIMPS at CMSU home page can be found at:
http://www.math-CS.cmsu.edu/~gimps/index.html
Mersenne Primes
Mod Arithmetic
Lucas-Lehmer Test
FT
43 Mersenne Primes
2^{30,402,457} - 1
GIMPS
GIMPS People
GIMPS Links

Top 10

Before Computers
Mainframe and Supercomputer Era
GIMPS Era

Curtis Cooper and Steven Boone ITV
Mersenne Primes and GIMPS
Top 10 Reasons to Search for Large Mersenne Primes

1. Because Mersenne primes are rare and beautiful.
2. To continue the mathematics and computer science tradition of Euler, Fermat, Mersenne, Lucas, Lehmer, etc.
3. To discover new number theory theorems as a by-product of the quest.
4. To discover new and more efficient algorithms for testing the primality of large numbers.
5. To expand the database of known primes, which is useful in cryptography and other fields.
6. To challenge the limits of computational technology and push the boundaries of what is possible.
7. To inspire and educate the public about mathematics and the importance of prime numbers.
8. To contribute to the advancement of mathematical research and knowledge.
9. To foster a sense of community and collaboration among mathematicians and computer scientists.
10. To celebrate the beauty and mystery of mathematics.
Top 10 Reasons to Search for Large Mersenne Primes

10. Because Mersenne primes are rare and beautiful.
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 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 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.
6. To help detect hardware problems (fan and CPU/bus problems) on individual computers at CMSU.
6. To help detect hardware problems (fan and CPU/bus problems) on individual computers at CMSU.

5. To put to good use the idle CPU cycles of hundreds of computers in labs and offices across CMSU’s campus.
6. To help detect hardware problems (fan and CPU/bus problems) on individual computers at CMSU.

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

4. To learn more about the distribution of Mersenne primes.
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 CMSU and demonstrate that Central Missouri State University 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 CMSU and demonstrate that Central Missouri State University is a first-class research and teaching institution.

1. To win the $100,000 offered by the Electronic Frontier Foundation (EFF) for the discovery of the first ten million digit prime number. EFF’s motivation is to encourage research in computational number theory related to large primes.