Mersenne Primes and GIMPS

Curtis Cooper
University of Central Missouri

July 24, 2014

Prime Numbers

- A **prime number** is a positive integer that has exactly two factors.

Prime Numbers

- A **prime number** is a positive integer that has exactly two factors.
- 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:

$$3 = 2^2 - 1$$
$$7 = 2^3 - 1$$
$$31 = 2^5 - 1$$
$$127 = 2^7 - 1$$
$$8191 = 2^{13} - 1$$

Mersenne Primes

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

$$3 = 2^2 - 1$$
$$7 = 2^3 - 1$$
$$31 = 2^5 - 1$$
$$127 = 2^7 - 1$$
$$8191 = 2^{13} - 1$$

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

Marin Mersenne

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

Marin Mersenne (1588-1648)

- Mersenne compiled what was supposed to be a list of Mersenne primes with exponents up to 257. His list of numbers n where $2^n - 1$ is prime is

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257.$$

- Mersenne compiled what was supposed to be a list of Mersenne primes with exponents up to 257. His list of numbers n where $2^n - 1$ is prime is

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257.$$

- Mersenne mistakenly included M67 and M257 (which are composite), and omitted M61, M89, and M107 (which are prime).

Edouard Lucas

Edouard Lucas

- In 1876 Lucas, using a test he developed, showed that M67 is composite without finding a factor.

- In 1876 Lucas, using a test he developed, showed that M67 is composite without finding a factor.
- No factor was found until a famous talk by Frank Cole at an AMS meeting in 1903. Cole devoted 20 years of Sunday afternoon computations to discover that

$$2^{67} - 1 = 193700721 \times 761838257287.$$

- In 1876 Lucas, using a test he developed, showed that M67 is composite without finding a factor.
- No factor was found until a famous talk by Frank Cole at an AMS meeting in 1903. Cole devoted 20 years of Sunday afternoon computations to discover that

$$2^{67} - 1 = 193700721 \times 761838257287.$$

- Without speaking a word, he went to a blackboard and raised 2 to the 67th power, then subtracted one.

- The base 2 representation of 67 is 1000011.

- The base 2 representation of 67 is 1000011.
- 1: $1^2 \times 2 = 2$.

- The base 2 representation of 67 is 1000011.
- 1: $1^2 \times 2 = 2$.
- 0: $2^2 = 4$.

- The base 2 representation of 67 is 1000011.
- 1: $1^2 \times 2 = 2$.
- 0: $2^2 = 4$.
- 0: $4^2 = 16$.

- The base 2 representation of 67 is 1000011.
- 1: $1^2 \times 2 = 2$.
- 0: $2^2 = 4$.
- 0: $4^2 = 16$.
- 0: $16^2 = 256$.

- The base 2 representation of 67 is 1000011.
- 1: $1^2 \times 2 = 2$.
- 0: $2^2 = 4$.
- 0: $4^2 = 16$.
- 0: $16^2 = 256$.
- 0: $256^2 = 65536$.

- The base 2 representation of 67 is 1000011.
- 1: $1^2 \times 2 = 2$.
- 0: $2^2 = 4$.
- 0: $4^2 = 16$.
- 0: $16^2 = 256$.
- 0: $256^2 = 65536$.
- 1: $65536^2 \times 2 = 8589934592$.

- The base 2 representation of 67 is 1000011.
- 1: $1^2 \times 2 = 2$.
- 0: $2^2 = 4$.
- 0: $4^2 = 16$.
- 0: $16^2 = 256$.
- 0: $256^2 = 65536$.
- 1: $65536^2 \times 2 = 8589934592$.
- 1: $8589934592^2 \times 2 = 147573952589676412928$.

- The base 2 representation of 67 is 1000011.
- 1: $1^2 \times 2 = 2$.
- 0: $2^2 = 4$.
- 0: $4^2 = 16$.
- 0: $16^2 = 256$.
- 0: $256^2 = 65536$.
- 1: $65536^2 \times 2 = 8589934592$.
- 1: $8589934592^2 \times 2 = 147573952589676412928$.
- $2^{67} - 1 = 147573952589676412927$.

- On the other side of the board, he multiplied 193,707,721 times 761,838,257,287 and got the same number.

- On the other side of the board, he multiplied 193,707,721 times 761,838,257,287 and got the same number.
- $193707721 \times 761838257287 = 147573952589676412927$.

- On the other side of the board, he multiplied 193,707,721 times 761,838,257,287 and got the same number.
- $193707721 \times 761838257287 = 147573952589676412927$.
- He returned to his seat (to applause) without speaking.

- 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

$$r_{126} \equiv 0 \pmod{M127}$$

then M127 is prime.

- Therefore, Lucas had to perform about 120 squaring operations and about 120 divide operations on 39 digit numbers.

- Therefore, Lucas had to perform about 120 squaring operations and about 120 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 about 120 squaring operations and about 120 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 about 120 squaring operations and about 120 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 about 120 squaring operations and about 120 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.
- $r_1 = 3$
- $r_2 = 3^2 - 2 = 7$
- $r_3 = 7^2 - 2 = 47$
- $r_4 = 47^2 - 2 \equiv 48 \pmod{127}$

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

- The calculations we need to do to show $M7 = 2^7 - 1 = 127$ is prime are the following.
- $r_1 = 3$
- $r_2 = 3^2 - 2 = 7$
- $r_3 = 7^2 - 2 = 47$
- $r_4 = 47^2 - 2 \equiv 48 \pmod{127}$
- $r_5 = 48^2 - 2 \equiv 16 \pmod{127}$
- $r_6 = 256 - 2 \equiv 0 \pmod{127}$.

- The calculations we need to do to show $M7 = 2^7 - 1 = 127$ is prime are the following.
- $r_1 = 3$
- $r_2 = 3^2 - 2 = 7$
- $r_3 = 7^2 - 2 = 47$
- $r_4 = 47^2 - 2 \equiv 48 \pmod{127}$
- $r_5 = 48^2 - 2 \equiv 16 \pmod{127}$
- $r_6 = 256 - 2 \equiv 0 \pmod{127}$.
- 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 $r_1 = 3$.

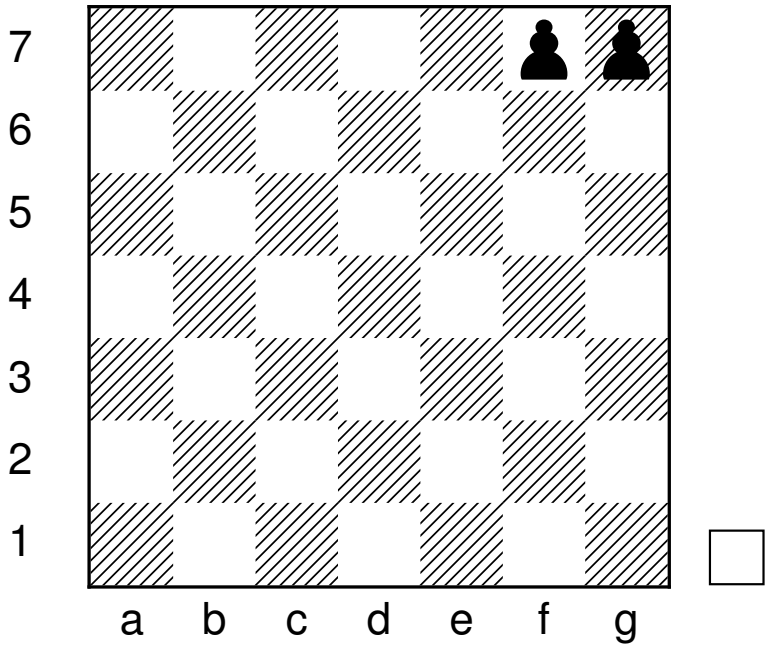
- If the top row contained r_k, Lucas would square r_k with the following moves.

- 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.

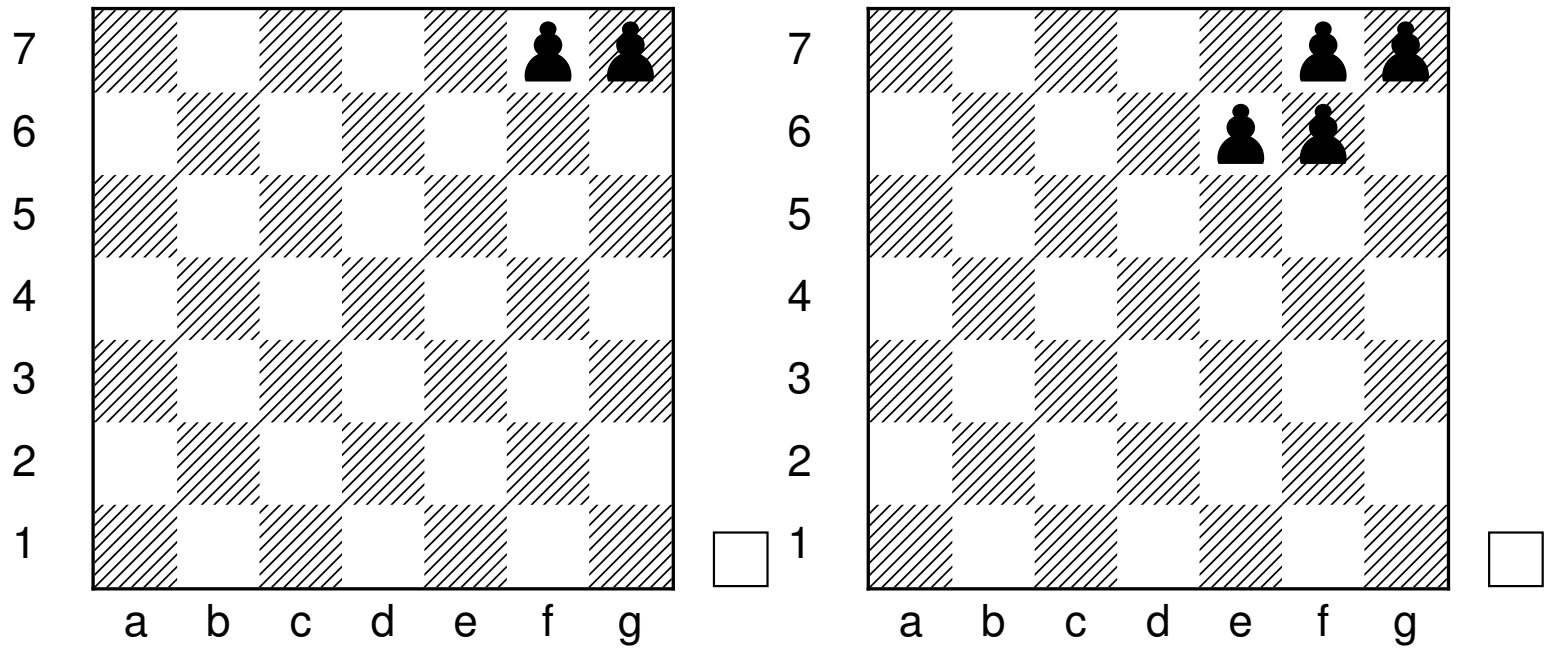
- He would then subtract 2 (once), usually by taking a pawn away from Column f. In the game, two pawns in the same column would be equivalent to removing those two pawns and replacing them by one pawn in the next column to the left. The column to the left of the left-most column is the right-most column.

- 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}.

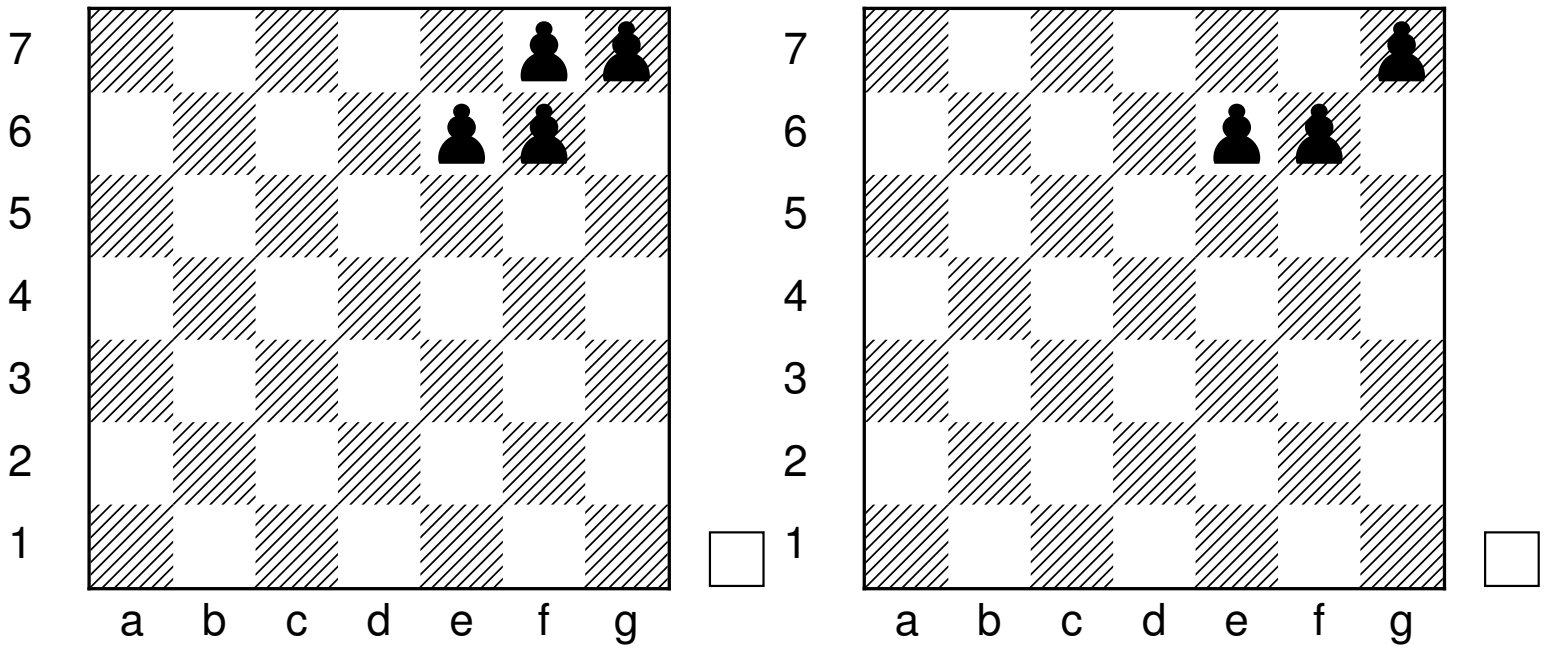
Lucas started the game with $r_1 = 3$.
On the chessboard, that would be:



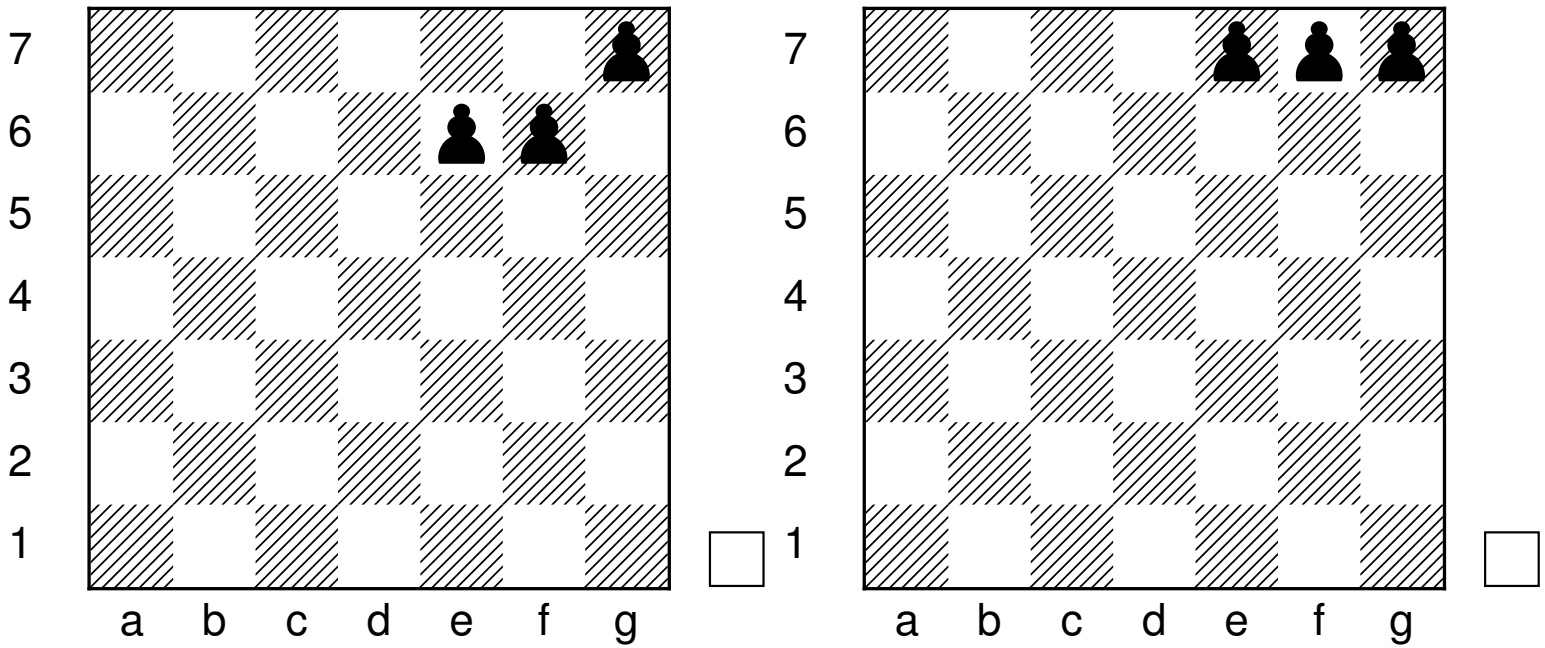
Squaring $r_1 = 3$ would result in the following chessboard.



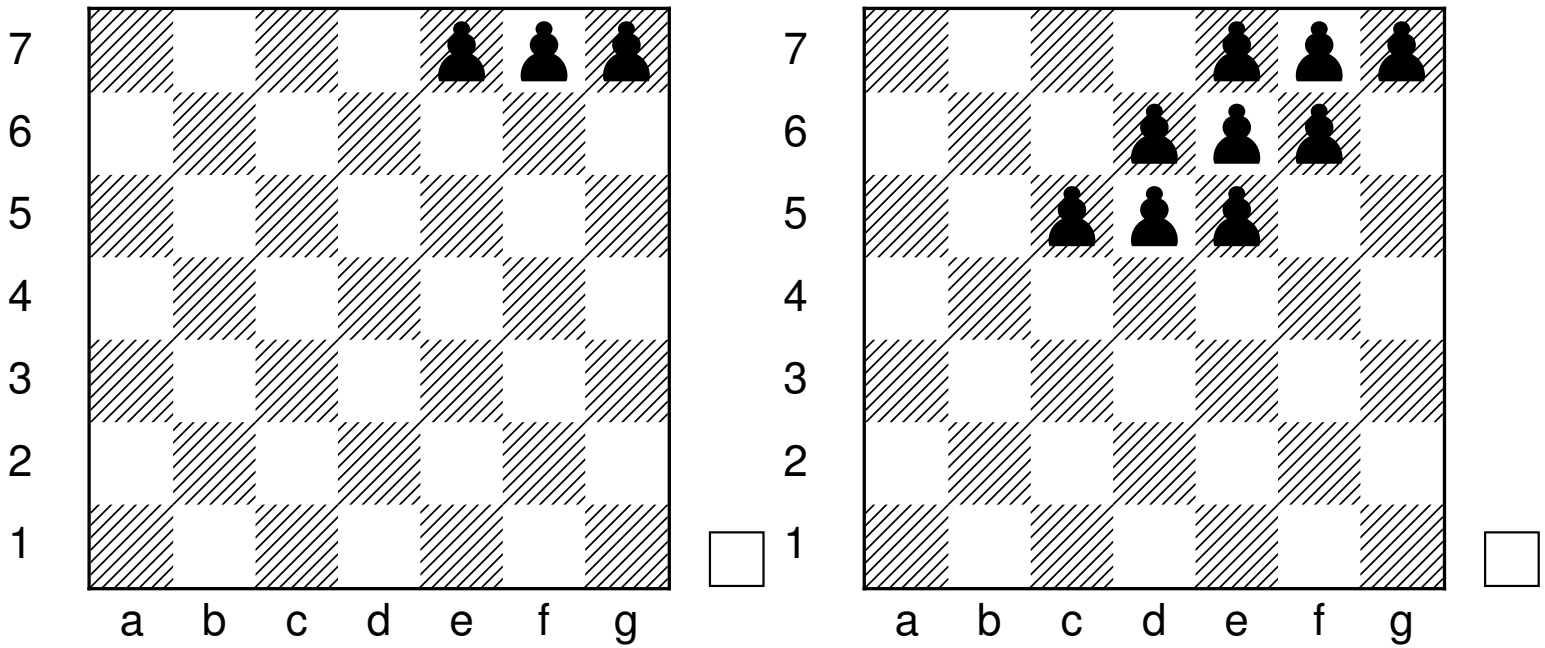
We can subtract 2 by removing a pawn from Column f. That would result in the following chessboard.



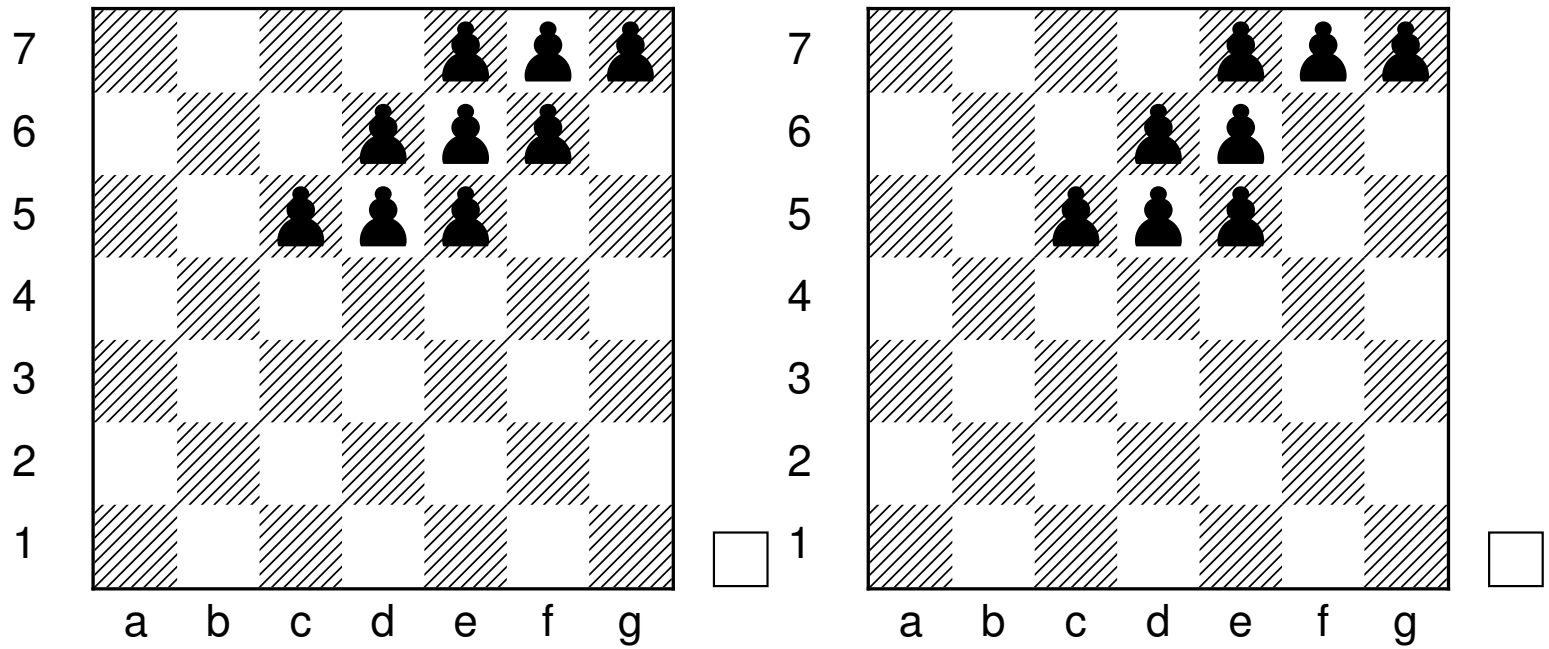
Pushing all the pawns to the top row would result in the following chessboard which is $r_2 = 7$.



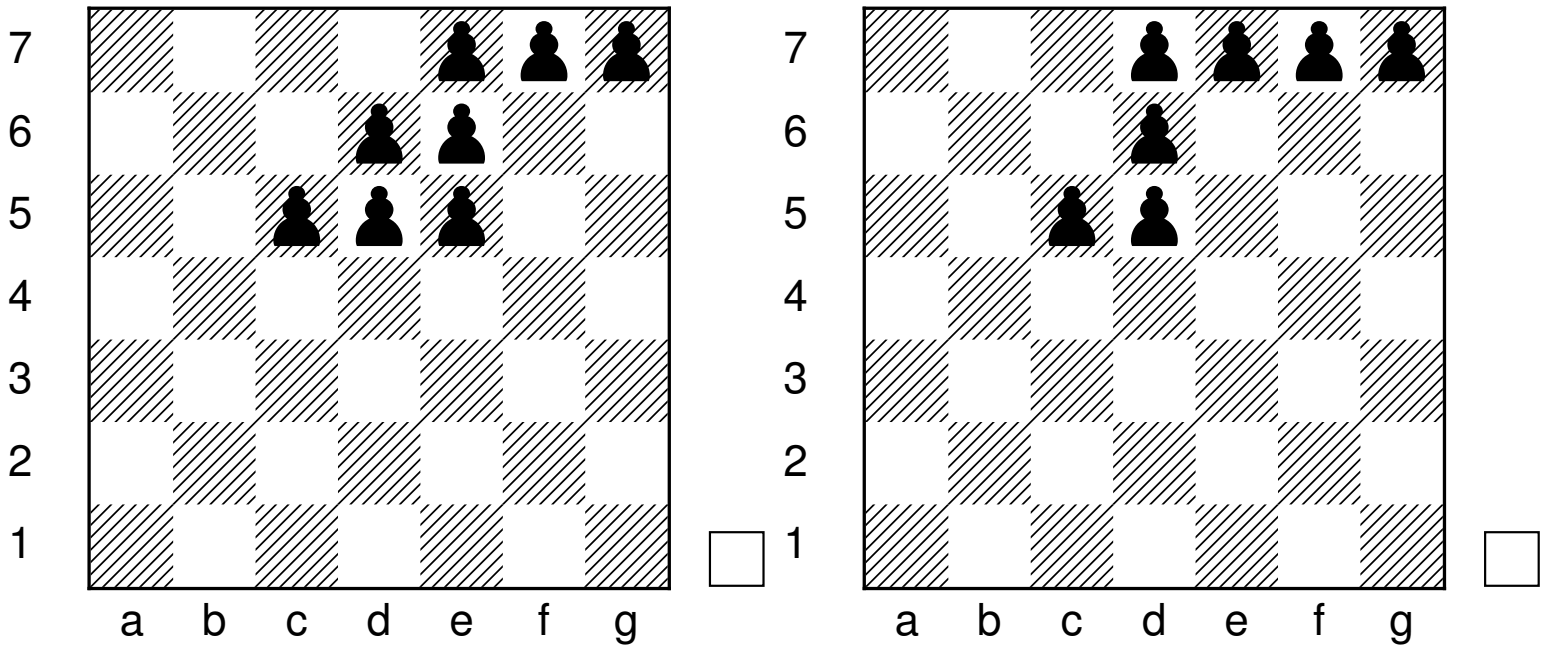
Now we need to square $r_2 = 7$. This would result in the following chessboard.

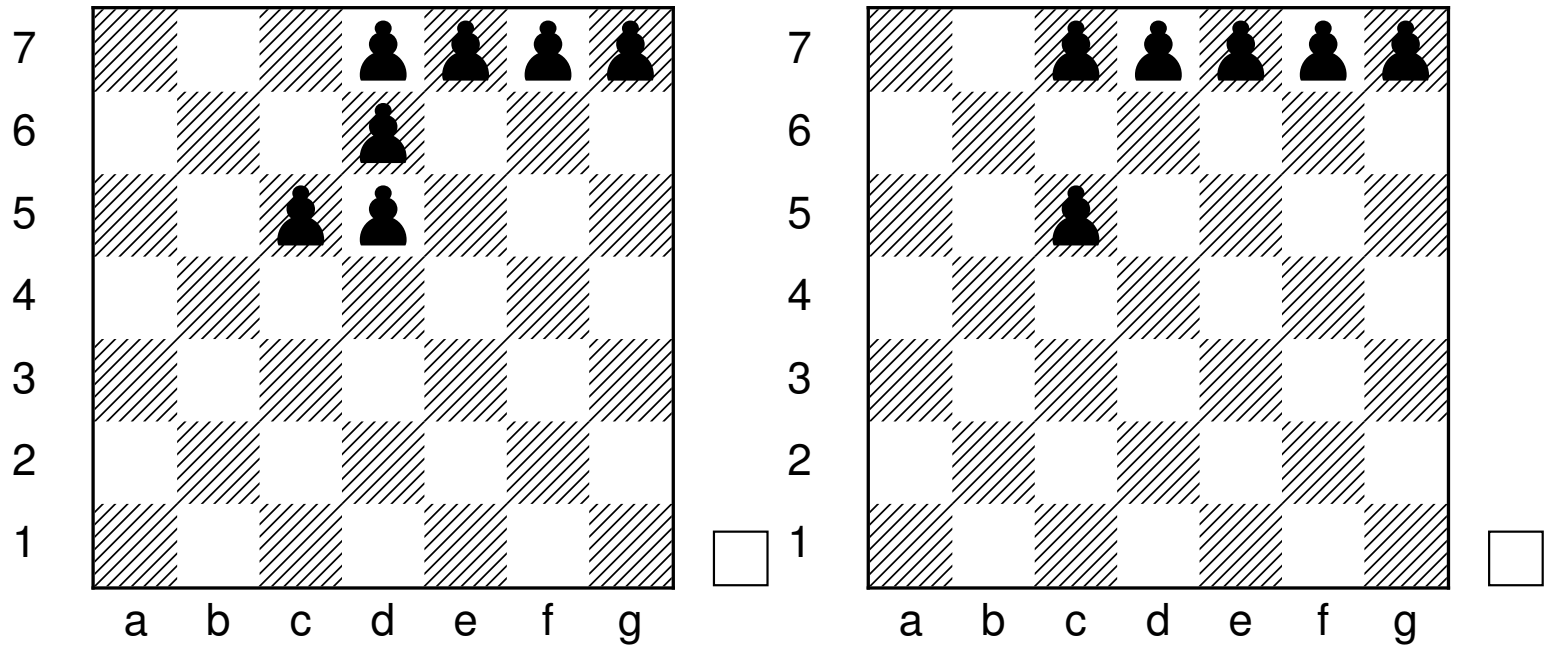


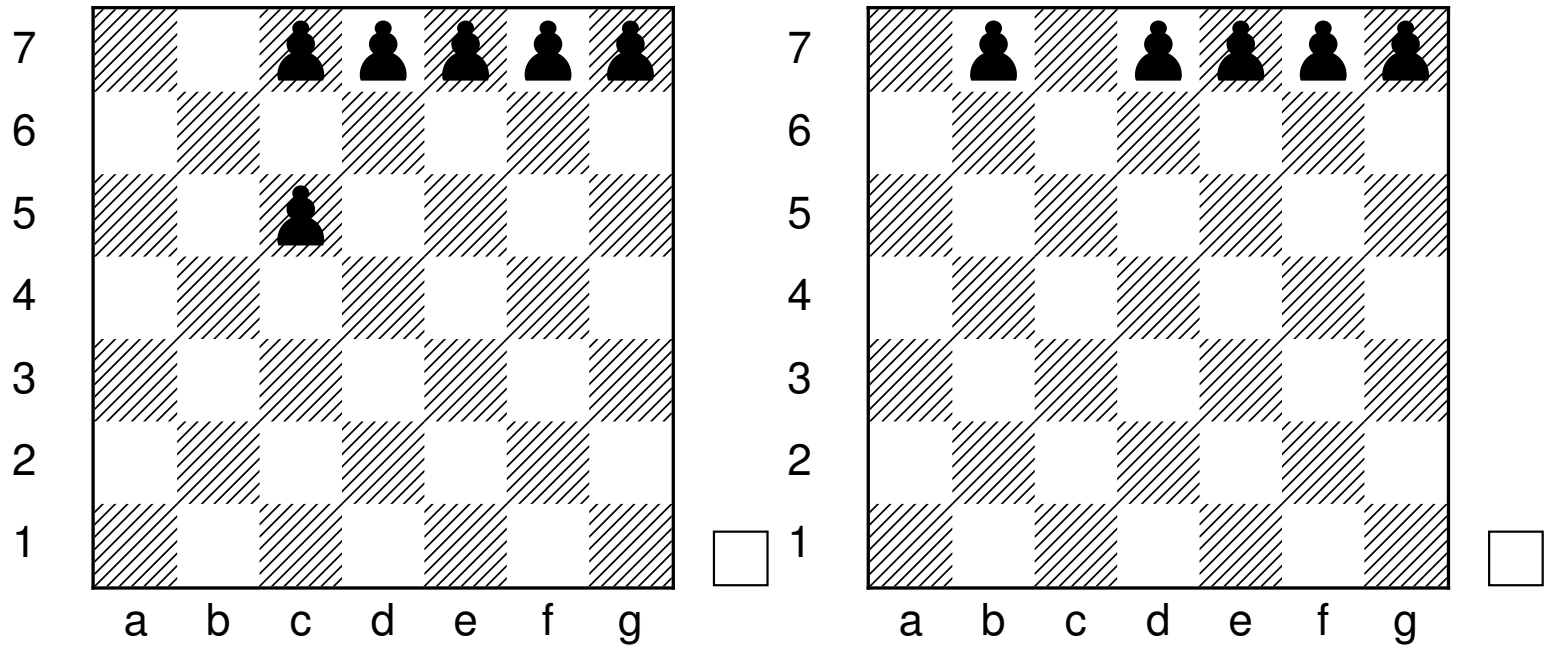
Subtracting 2 would result in the following chessboard.



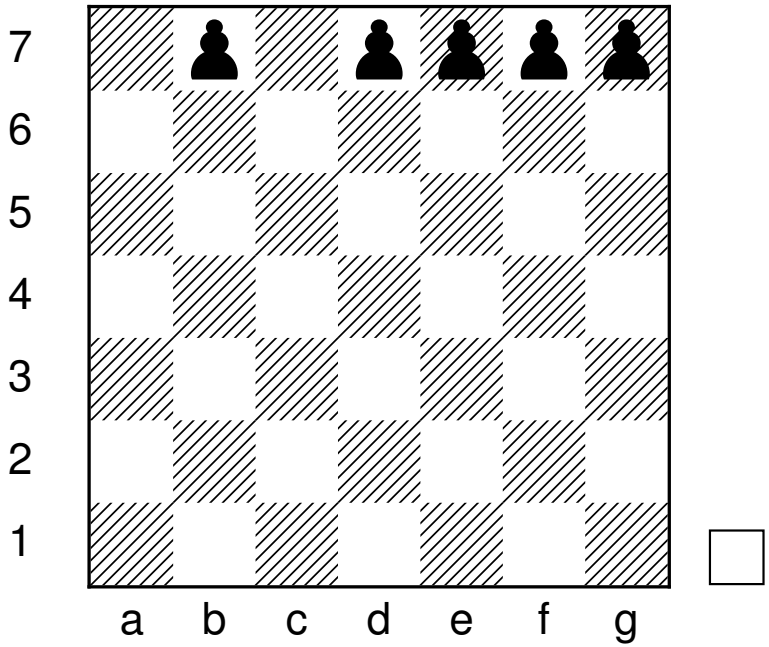
We now do the game moves where we replace two pawns in a column by one pawn in the column to the left. Here are the steps in the game.



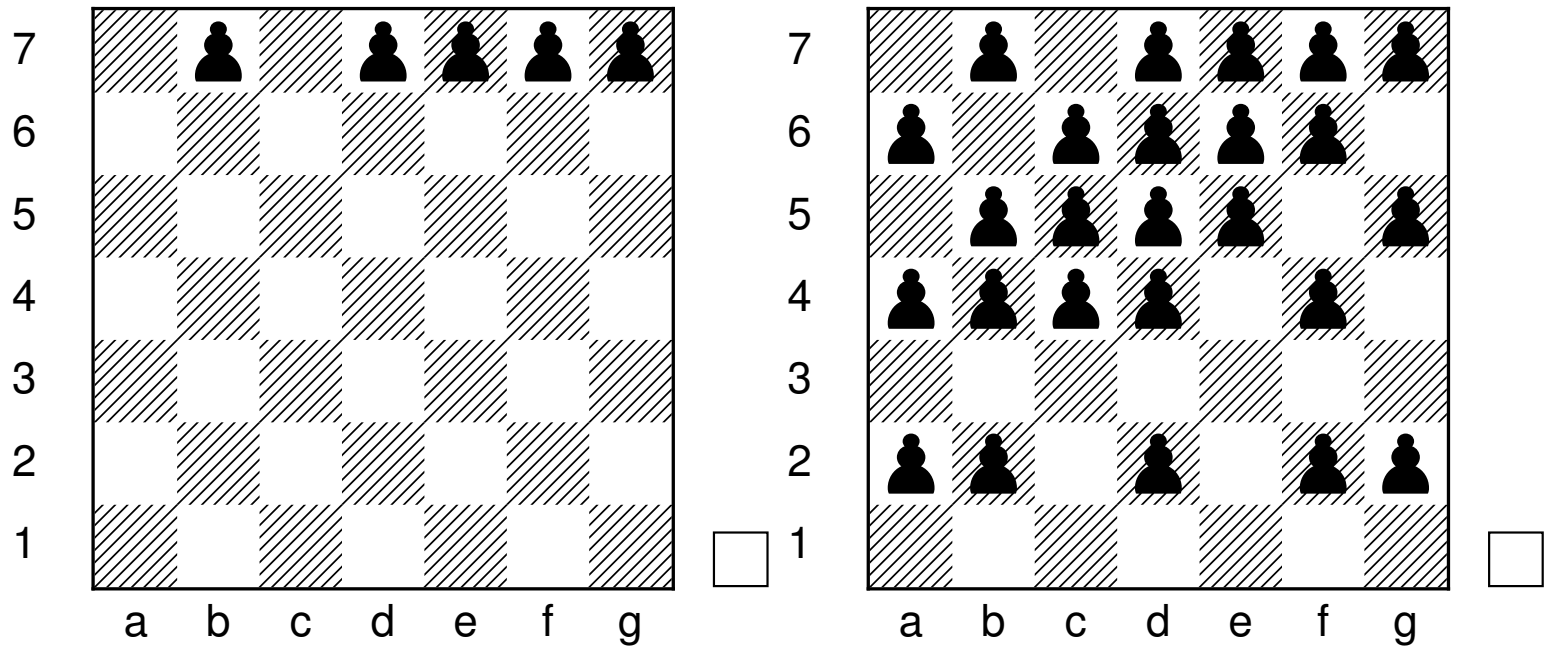

7
6
5
4
3
2
1
a b c d e f g
7
6
5
4
3
2
1
a b c d e f g


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.



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.

- Lucas played this game on a 127×127 chessboard. It is estimated that it must have taken him between 170 and 300 hours to complete the calculations. At the end, Lucas got $r_{126} \equiv 0 \pmod{M127}$.

- Lucas played this game on a 127×127 chessboard. It is estimated that it must have taken him between 170 and 300 hours to complete the calculations. At the end, Lucas got $r_{126} \equiv 0 \pmod{M127}$.
- A correct list of all Mersenne primes in the exponent range up to 257 was completed and rigorously verified in 1947.

- Lucas played this game on a 127×127 chessboard. It is estimated that it must have taken him between 170 and 300 hours to complete the calculations. At the end, Lucas got $r_{126} \equiv 0 \pmod{M127}$.
- A correct list of all Mersenne primes in the exponent range up to 257 was completed and rigorously verified in 1947.
- That list is:

$$2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 61,\ 89,\ 107,\ 127.$$

- 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.

- M4253 is the first Mersenne prime with more that 1000 digits.

- M4253 is the first Mersenne prime with more that 1000 digits.
- M44497 is the first with more than 10,000 digits.

- M4253 is the first Mersenne prime with more that 1000 digits.
- M44497 is the first with more than 10,000 digits.
- M6972593 was the first prime with at least 1,000,000 digits.

- M4253 is the first Mersenne prime with more that 1000 digits.
- M44497 is the first with more than 10,000 digits.
- M6972593 was the first prime with at least 1,000,000 digits.
- All three were the first known primes of any kind of that size.

- On August 23, 2008, Edson Smith at UCLA, participating in GIMPS, discovered M43112609, a 12.9-million-digit Mersenne prime.

- On August 23, 2008, Edson Smith at UCLA, participating in GIMPS, discovered M43112609, a 12.9-million-digit Mersenne prime.
- Since this prime was the first known prime with at least 10 million digits, the Electronic Frontier Foundation (EFF) awarded GIMPS 100,000 dollars. Part of the 100,000 dollars went to UCLA.

- On August 23, 2008, Edson Smith at UCLA, participating in GIMPS, discovered M43112609, a 12.9-million-digit Mersenne prime.
- Since this prime was the first known prime with at least 10 million digits, the Electronic Frontier Foundation (EFF) awarded GIMPS 100,000 dollars. Part of the 100,000 dollars went to UCLA.
- The prime was found on a Dell OptiPlex 745 and is the eighth Mersenne prime discovered at UCLA.

- List of 48 Known Mersenne Primes - http://en.wikipedia.org/wiki/Mersenne_prime

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.

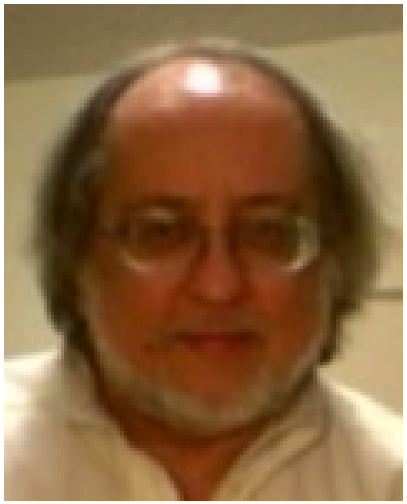
- Woltman's program uses a special algorithm, discovered in the early 1990's by Richard Crandall. Crandall found ways to double the speed of what are called convolutions – essentially big multiplication operations.
- As of February 5, 2013, GIMPS had a sustained throughput of approximately 129 trillion 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 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 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

- On January 25, 2013, Curtis Cooper, as a participant in GIMPS, discovered the 48th known Mersenne prime,

$$2^{57885161} - 1,$$

a 17,425,170 digit number.

- On January 25, 2013, Curtis Cooper, as a participant in GIMPS, discovered the 48th known Mersenne prime,

$$2^{57885161} - 1,$$

  a 17,425,170 digit number.
- The first and last digits of this prime are:

$$58188726623 \quad \ldots \quad 071724285951$$

- On January 25, 2013, Curtis Cooper, as a participant in GIMPS, discovered the 48th known Mersenne prime,

$$2^{57885161} - 1,$$

  a 17,425,170 digit number.
- The first and last digits of this prime are:

$$58188726623 \ \ldots \ 071724285951$$

- This is the 14th Mersenne prime found by GIMPS.

- On January 25, 2013, Curtis Cooper, as a participant in GIMPS, discovered the 48th known Mersenne prime,

$$2^{57885161} - 1,$$

  a 17,425,170 digit number.
- The first and last digits of this prime are:

$$58188726623 \quad \ldots \quad 071724285951$$

- This is the 14th Mersenne prime found by GIMPS.
- The new prime was independently verified using different programs running on different hardware.

- Serge Batalov ran Ernst Mayer's MLucas software on a 32-core server in 6 days (resource donated by Novartis IT group) to verify the new prime.

- Serge Batalov ran Ernst Mayer's MLucas software on a 32-core server in 6 days (resource donated by Novartis IT group) to verify the new prime.
- Jerry Hallett verified the prime using the CUDALucas software running on a NVidia GPU in 3.6 days.

- Serge Batalov ran Ernst Mayer's MLucas software on a 32-core server in 6 days (resource donated by Novartis IT group) to verify the new prime.
- Jerry Hallett verified the prime using the CUDALucas software running on a NVidia GPU in 3.6 days.
- Finally, Dr. Jeff Gilchrist verified the find using the GIMPS software on an Intel i7 CPU in 4.5 days and the CUDALucas program on a NVidia GTX 560 Ti in 7.7 days.

- This is the third Mersenne prime found at the University of Central Missouri.

- This is the third Mersenne prime found at the University of Central Missouri.
- The first Mersenne prime is $2^{30402457} - 1$ and was found on December 15, 2005. It has 9.125 million digits.

- This is the third Mersenne prime found at the University of Central Missouri.
- The first Mersenne prime is $2^{30402457} - 1$ and was found on December 15, 2005. It has 9.125 million digits.
- The second Mersenne prime is $2^{32582657} - 1$ and was found on September 4, 2006. It has 9.8 million digits.

- All of these Mersenne primes were the largest known prime at the time of their discovery.

- All of these Mersenne primes were the largest known prime at the time of their discovery.
- The new Mersenne prime was found in the Modern Language Lab at UCM. It was on the computer named: ml–wd-210–22l (Wood Building 210, Computer Number 22).

- All of these Mersenne primes were the largest known prime at the time of their discovery.
- The new Mersenne prime was found in the Modern Language Lab at UCM. It was on the computer named: ml–wd-210–22l (Wood Building 210, Computer Number 22).
- This computer was a 3 GHz Intel Core2 Duo E8400

- The exponent was assigned by the PrimeNet server on December 12, 2012 and started work on the exponent 5 days later.

- The exponent was assigned by the PrimeNet server on December 12, 2012 and started work on the exponent 5 days later.
- The computer ran George Woltman's program, implementing the Lucas-Lehmer test with Fast Fourier Transforms, for 39 days.

- The exponent was assigned by the PrimeNet server on December 12, 2012 and started work on the exponent 5 days later.
- The computer ran George Woltman's program, implementing the Lucas-Lehmer test with Fast Fourier Transforms, for 39 days.
- Interesting enough, the exponent which resulted in this Mersenne prime was assigned to two other users before we were assigned the number to test. Both times, the exponent was reclaimed by the PrimeNet server after 60 days because of inactivity in the computations.

- The exponent was assigned by the PrimeNet server on December 12, 2012 and started work on the exponent 5 days later.
- The computer ran George Woltman's program, implementing the Lucas-Lehmer test with Fast Fourier Transforms, for 39 days.
- Interesting enough, the exponent which resulted in this Mersenne prime was assigned to two other users before we were assigned the number to test. Both times, the exponent was reclaimed by the PrimeNet server after 60 days because of inactivity in the computations.
- We have over 1000 computers at UCM participating in the GIMPS project.

- My primary job as a participant in GIMPS is making sure all the computers are running Woltman's program. I basically install and start George Woltman's program on UCM's lab computers.

- My primary job as a participant in GIMPS is making sure all the computers are running Woltman's program. I basically install and start George Woltman's program on UCM's lab computers.
- The administration has been a great help to me, giving me administrator access to many computers in UCM's labs.

- My primary job as a participant in GIMPS is making sure all the computers are running Woltman's program. I basically install and start George Woltman's program on UCM's lab computers.
- The administration has been a great help to me, giving me administrator access to many computers in UCM's labs.
- In recent years, I have been able to access these lab computers from home.

- My primary job as a participant in GIMPS is making sure all the computers are running Woltman's program. I basically install and start George Woltman's program on UCM's lab computers.
- The administration has been a great help to me, giving me administrator access to many computers in UCM's labs.
- In recent years, I have been able to access these lab computers from home.
- Because of our 17 years of work in GIMPS and the 3 Mersenne primes we have discovered, there is great interest in GIMPS at UCM and a level of support and trust by our IT department and UCM administrators.

[Tue Dec 11 02:00:14 2012]
Iteration 44973837 / 54575267
Iteration 37543183 / 58588867
[Mon Dec 17 08:16:13 2012]
UID: curtisc/wd-210--22l, M54575267 is not prime.
Res64: FFF410C4C187CF11.
We5: 945B96CB,3369298,00000000,
AID: 63EFFFA1029B57A64A682FFA291D53A6
[Tue Dec 18 02:00:16 2012]
Iteration 1089622 / 57885161
Iteration 48128946 / 58588867
[Tue Dec 25 03:16:34 2012]
UID: curtisc/wd-210--22l, M58588867 is not prime.
Res64: 3CFF03A4A83FADD3.
We5: 1D5DE55D,31377919,00000000,

```
AID: C46BE4ABC4961A1321154AC11BD4FCC8
[Tue Jan 15 10:58:07 2013]
Iteration 31953531 / 56419513
Iteration 42813818 / 57885161
[Thu Jan 17 02:00:15 2013]
Iteration 34393427 / 56419513
Iteration 45189954 / 57885161
[Thu Jan 17 06:27:33 2013]
Iteration 45461248 / 57885161
Iteration 34661902 / 56419513
[Fri Jan 25 17:30:25 2013]
UID: curtisc/wd-210--22l, M57885161 is prime!
We5: 58BF09CF,00000000,
AID: CC2B2E16DC6B11B028899C3088AB7745
```

- Email from George Woltman

- Email from George Woltman
- Stephen Colbert

News About M57885161

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

News About M57885161

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

News About M57885161

- 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 M57885161

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

More About M57885161

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

Mersenne Buttons

- M30402457 Button http://www.math-cs.ucmo.edu/∼curtisc/photos/M30402457.jpg

Mersenne Buttons

- M30402457 Button http://www.math-cs.ucmo.edu/∼curtisc/photos/M30402457.jpg
- M32582657 Button http://www.math-cs.ucmo.edu/∼curtisc/photos/M32582657.jpg

Mersenne Buttons

- M30402457 Button http://www.math-cs.ucmo.edu/∼curtisc/photos/M30402457.jpg
- M32582657 Button http://www.math-cs.ucmo.edu/∼curtisc/photos/M32582657.jpg
- M57885161 Button http://www.math-cs.ucmo.edu/∼curtisc/images/1.jpg

Jumping GIFS

- 3 Primes GIF
  http://www.math-cs.ucmo.edu/∼curtisc/images/6.gif

Jumping GIFS

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

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

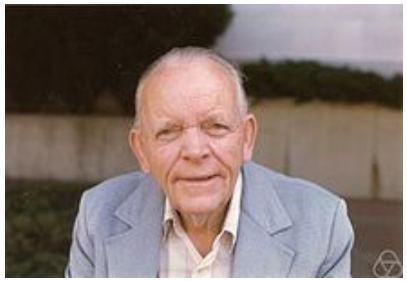
$$M_p = 2^p - 1 \text{ is prime}$$

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

Reasons

Reasons to Search for Large Mersenne Primes

Reasons

Reasons to Search for Large Mersenne Primes

1. To help in the discovery of new Mersenne primes.

Reasons

Reasons to Search for Large Mersenne Primes

1. To help in the discovery of new Mersenne primes.

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

Reasons

Reasons to Search for Large Mersenne Primes

1. To help in the discovery of new Mersenne primes.

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

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

Reasons

Reasons to Search for Large Mersenne Primes

Reasons

Reasons to Search for Large Mersenne Primes

4. To obtain favorable press for UCM for their support of our efforts to discover new Mersenne primes.

Reasons

Reasons to Search for Large Mersenne Primes

4. To obtain favorable press for UCM for their support of our efforts to discover new Mersenne primes.

5. 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/mersennegimps/mersennegimps.pdf