$2^{2976221}-1$ *is prime!*

THE GREAT INTERNET MERSENNE PRIME SEARCH

GIMPS

Modern Analysis of Mersenne Primes before Computers

Mersenne made a detailed study of Mersenne numbers. He claimed to know exactly which of the first 257 Mersenne numbers were prime and which were not. His work did not include proofs of these results. So mathematicians continued to investigate Mersenne's claims. In 1876 Édouard Lucas (French mathematician; 1842 - 1891) proved that

$$M_{127} = 170{,}141{,}183{,}460{,}469{,}231{,}731{,}687{,}303{,}715{,}884{,}105{,}727$$

was prime, as Mersenne claimed. This was the largest prime known to humankind for over 75 years!

But Mersenne made a few mistakes. One of these was with M_{67} which Mersenne claimed was prime. The story surrounding this number is rich:

Edouard Lucas worked a test whereby he was able to prove that the Mersenne number´ M_{67} was composite; but he could not produce the actual factors. At the October 1903 meeting of the American Mathematical Society, the American mathematician Frank Nelson Cole had a paper on the program with the somewhat unassuming title *On the Factorization of Large Numbers*. When called upon to speak, Cole walked to a [chalk] board and, saying nothing, proceeded to raise the integer 2 to the 67th power; then he carefully subtracted 1 from the resulting number and let the figure stand. Without a word he moved to a clean part of the board and multiplied, longhand, the product

$$193{,}707{,}721 \times 761{,}838{,}257{,}287.$$

The two calculations agreed. The story goes that, for the first and only time on record, this venerable body rose to give the presenter of a paper a standing ovation. Cole took his seat without having uttered a word, and no one bothered to ask him a question. (Later, he confided to a friend that it took him 20 years of Sunday afternoons to find the factors of M_{67}.)

1. About how many digits does M_{67} have?

2. How long do you think it might take you to calculate M_{67}, from its definition, by hand?

3. Describe the mathematics Cole was likely doing in these 20 years of Sunday afternoons to uncover this secret.

4. Do you think that Cole's time in determining a factorization of M_{67} was well spent? Explain.

Modern Analysis of Mersenne Primes with Computers

With the advent of desk calculators and early computers, by 1947 the primality of all 257 numbers on Mersenne's list were determined. Mersenne made only five mistakes out of 257 numbers - a remarkable accomplishment since these numbers grow so fast, as you have already seen.

The growth in the size of the largest know prime has been remarkable over the last 70 years. The term "exponential growth" is often used in everyday speech as a generic way to describe large rates of growth. This is inappropriate as the term has a precise and important meaning. Its use in this context is appropriate. The number of digits in the largest known primes has increased by a factor of 10 about every twelve years since 1945.[1] Lucas' prime, the enormous number above, has *only* 39 digits. In 1961, the record was a 1,332 digit number. In 1979, the record 13,395 digits. In 1992, the record 227,832 digits. In 1999, the record 2,098,960 digits. In fact, since 1996 *all* of the largest known prime numbers have been Mersenne primes and they have been discovered by volunteers of the Great Internet Mersenne Prime Search (GIMPS).

As part of GIMPS, volunteers run sophisticated computer analysis on pieces of data while their computers are idle. Called *distributed computing*, volunteers essentially loan their idle, unused computer time to a scientific effort. If you would like to be part of the GIMPS search, and maybe become famous, you can download software at www.mersenne.org. This software runs in background in the lowest priority on your computer, using your computer's capabilities when you are not actively using them.

Discovered on December 5, 2001, by 20 year-old **Michael Cameron** running GIMPS software on his PC, was the primality of the Mersenne number $2^{13466917} - 1$, an almost five-fold increase in the number of digits of the largest known prime from just three years earlier. There have been seven new prime number records since then, three by **Curtis Cooper,** a professor of mathematics and computer science at the University of Central Missouri who keeps GIMPS running on all of his campus' computers. His discoveries include the current record:

$$M^{57,885,161} = 2^{57,885,161} - 1$$

which is a 17,425,170 digit number.

[1] See http://primes.utm.edu/notes/by_year.html for the largest known primes by year and an interesting discussion about the use of *linear regression* to quantify the growth.

The initial digits of this number are:
581,887,266,232,246,442,175,100,212,113,232,368,636,370,852,325,421,589,325... and the final digits are:
937,745,410,942,833,323,095,203,705,645,658,725,746,141,988,071,724,285,951.
In between these 104 digits are 17,425,66 digits that have been *removed*.

5. If this page were filled with digits in this way, 35 lines to a page, how many digits could fit on the page?

6. How many pages would it take to write out the digits to Cooper's Mersenne prime in the way just described? Explain.

7. Does this help you appreciate how large this prime is and how remarkable it is that we know deductively that this number is prime? Explain.

The Twins

A moving story of arithmetical insight is told by **Oliver Sacks** (British-American neurologist and author; 1933 -) in the chapter "The Twins" from *The Man Who Mistook His Wife for a Hat*[2] This story involves two autistic twins who had extraordinary abilities to recognize numbers and number relationships in many everyday things around them. For example:

> A box of matches on their table fell, and discharged its contents on the floor: "111," they both cried simultaneously; and then, in a murmur, John said "37". Michael repeated this, John said it a third time and stopped. I counted the matches – it took some time – and there were 111.

8. What does 37 have to do with 111?

9. Why did the twins repeat 37 as they did?

10. What is the mathematical importance of 37 to 111?

[2] HarperPerrenial edition, 1990, pp. 195 - 213.

This storyline was adapted as one of the pivotal scenes in the movie Rain Man when the character Charlie Babbitt (played by **Tom Cruise** (American actor; 1962 -) begins to realize the remarkable power of brother Raymond, an autistic savant (played by **Dustin Hoffman** (1937; -)). In this adapted scene[3] Raymond wants toothpicks to eat his pancakes. When the waitress accidentally spills the box of toothpicks on the floor, Raymond says “82, 82, 82.” Charlie tells him he’s “not even close.” Raymond replies “246 total.” The waitress says that there are 250 in the box and then realizes there are exactly 4 left in the box.

In real life, Sacks spent a long time sitting in the company of the twins to gain their trust. After a great many visits the twins became comfortable and one day began speaking in numbers. Sacks secretly recorded these numbers and later determined they were all eight digit prime numbers. Subsequently he snuck a book of primes into their “meetings”. One day he participated in the conversation. After a period of shock, the twins welcomed him into the prime conversation. When Sacks later contributed a nine digit prime, the twins were shocked. But they responded with nine digit primes of their own. And then ten digit primes. And then numbers with more and more digits. Sacks assumed they must be primes, but was uncertain as his book did not include numbers this large and this was well before handheld technology put this information at our immediate disposal.

What is remarkable is that there is no know algorithm for generating primes and no efficient way to determine whether a given number is prime. These problems are holy grails to number theorists. As the great Euler said:

> Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate.

Yet, these two twins, whose arithmetic abilities were essentially nonexistent, somehow knew how to communicate with the prime numbers. Is it possible that the secret of the primes was

[3] Which can be found on YouTube by searching “Autism Tootpick Count”.

known to these twins? Perhaps. But if it was it has been lost. The twins were separated to help prevent their “unhealthy communication together... in an appropriate, socially acceptable way.” They subsequently seemed to lose their special abilities with primes.