

Perfect Numbers

A positive integer is said to be *perfect* if it is the sum of its proper divisors.

The first four perfect numbers are 6, 28, 496, and 8128, and these numbers have been known since the time of Euclid (300 BC).

Perfect numbers were an object of fascination and mystery for the early Greeks. However, despite occasional efforts, another perfect number was not discovered until 1536 AD!!!

In this presentation, we will determine the fifth perfect number.

Mersenne Primes

We began by looking for the fifth perfect number, and in our investigation, we discovered a beautiful connection to Mersenne primes.

Specifically, we proved that if $M_k = 2^k - 1$ is a prime number (for some integer k), then the number $n = 2^{k-1} \cdot M_k$ is perfect.

The great mathematician Leonhard Euler proved the converse, namely, that an even perfect number *must* be of the form $2^{k-1} \cdot M_k$, where M_k is a Mersenne prime.

We've shown that the first five Mersenne primes are M_2 , M_3 , M_5 , M_7 , and M_{13} . It turns out that the next two Mersenne primes are M_{17} and M_{19} .

So it seems that for most primes p , the integer M_p is prime. Right?

A Theorem of Fermat

Recall that $M_{11} = 23 \times 89$. Do you notice anything interesting?

I claim that $M_{23} = 2^{23} - 1 = 8388607$ is composite. If you were to hazard a guess for a prime factor of M_{23} , what would you pick?

It turns out that $M_{23} = 47 \times 178481$, and both 47 and 178481 are primes numbers congruent to 1 mod 23.

Fermat proved the following amazing theorem:

If p is prime, and q is a prime divisor of $M_p = 2^p - 1$, then q must be of the form $pk + 1$.

Illustrating Le Théorème De Fermat

Let's illustrate Fermat's theorem for $p = 19$. We will check that M_{19} is prime.

Without this theorem, checking for the primality of $2^{19} - 1$ would require manually checking all the primes up to $\sqrt{M_{19}} \approx 724$. That's a lot of busy work!

But with this theorem, we just need to check the primes less than 724 that are congruent to 1 mod 19. And there are only six of them, namely 191, 229, 419, 457, 571, and 647. We can quickly check that none of these six primes divide M_{19} , and so we conclude that M_{19} is prime.

To see if M_{29} is prime, we just need to check all the primes q for which $q \equiv 1 \pmod{29}$. And we find that $q = 233$ divides M_{29} , so this number is not prime.

We can quickly show that $M_{29} = 233 \times 1103 \times 2089$. By Fermat's theorem, we know that each of the numbers 233, 1103, and 2089 is congruent to 1 mod 29.

The next Mersenne prime is M_{31} , and the next one after that is M_{61} .

How Did He Come Up With That?

In the old days, there were no calculators or computers, and so determining the primality of M_p was very time-consuming. Even with Fermat's theorem, checking the primality of M_{61} would have taken several lifetimes – note that $\sqrt{M_{61}}$ is approximately one and a half billion. So we need something more sophisticated than Fermat's theorem.

In 1878, the French mathematician Lucas found the following stunning result that simplified the process of finding Mersenne primes:

Define $L_0 = 4$, and recursively define $L_{n+1} = L_n^2 - 2$.

Then, Lucas' Theorem states that for a prime number p ,

M_p is prime iff L_{p-2} is divisible by M_p .

How on earth did he come up with that?

Illustrating Lucas' Theorem

Let's demonstrate Lucas' Theorem for $p = 7$. We want to prove that L_5 is divisible by $M_7 = 2^7 - 1 = 127$.

$$L_0 = 4 \equiv 4 \pmod{127}$$

$$L_1 = 4^2 - 2 \equiv 14 \pmod{127}$$

$$L_2 = 14^2 - 2 = 194 \equiv 67 \pmod{127}$$

$$L_3 = 67^2 - 2 = 4487 \equiv 42 \pmod{127}$$

$$L_4 = 42^2 - 2 = 1762 \equiv 111 \pmod{127}$$

$$L_5 = 111^2 - 2 = 12319 \equiv 0 \pmod{127}$$

Using this theorem, Lucas proved that M_{61} is the next Mersenne prime after M_{31} .

GIMPS

Surprisingly, Mersenne primes occur extremely rarely, even though each of M_2 , M_3 , M_5 , M_7 , M_{13} , M_{17} , and M_{19} is prime.

So far, all the primes up to 14 million have been checked, and only 39 Mersenne primes have been found!

In 1996, George Woltman, a programmer in Orlando, started **GIMPS**, which stands for the Great Internet Mersenne Prime Search.

The latest Mersenne prime (the 39th) was found in December 2001 by Michael Cameron, a 20 year old from Owen Sound, Ontario. He joined GIMPS in mid-2001. For his discovery, he became very famous and very rich!

The 39th Mersenne prime is $M_{13466917} = 2^{13466917} - 1$, which has over four million digits!

You too can join GIMPS. For more info, see

<http://www.utm.edu/research/primes/mersenne.shtml>

Do you think the following conjecture is true or false?

There exist infinitely many Mersenne primes.

Odd Perfect Numbers

Euler proved that an even number n is perfect iff $n = 2^{k-1} \cdot M_k$, where M_k is a Mersenne prime.

For this result, and others, he was bestowed with many honours. For example, the city of Edmonton named their hockey name the Edmonton “Eulers”, in his honour.

However, no one has solved the problem of classifying the odd perfect numbers. To date, not a single odd perfect number has been found! Although many people conjecture that no odd perfect number exists, no one has been able to find a proof. Currently, the best known result is:

If n is an odd perfect number, then n must have at least eight distinct prime factors, have at least one prime divisor greater than 10^6 , and have at least 300 digits.

This problem is one of the “crown jewels” in number theory.