Final Project

Morgan Keeton

November 2021

An Introduction

For many years, Mersenne Primes have been used in cryptography, statistics and other mathematical fields to explore the cardinality and arithmetic features of prime numbers. Because of their relationship with perfect numbers, mathematicians have been searching for various properties relating to both Mersenne Primes and Perfect Numbers. A Mersenne Prime is a number of the form $2^p - 1$, where both p and $2^p - 1$ are prime (Srinath, et al.). Often, these Mersenne Primes are denoted as M_P, where M stands for Mersenne and p, the prime number, respectively. A perfect number is a number of the form $n = M_P\,(2^{p-1})$ or equivalently, $n = (2^p - 1)\,(2^{p-1})$. For example, the first Mersenne Prime that was discovered is 3. We can easily compute this as follows: $3 = 2^2 - 1$. Because of this, the correlating perfect number is 6, because $6 = (2^2 - 1)(2^{2-1}) = (4 - 1)(2^1) = 3 * 2 = 6$.

Throughout this paper, we will explore the idea and relationship between Mersenne Primes and Perfect Numbers, as well as the various properties that lie within this relationship. There are a multitude of theorems that could be explored, but these have been limited to the relationship between Gaussian and Eisenstein Mersenne Primes, the Lucas-Lehmer Test, Fermat's Last Theorem, and Arithmetical Progressions.

Mersenne Primes

As aforementioned, Mersenne Primes are numbers of the form $2^p - 1$, where both $2^p - 1$ and p are prime numbers. This group of numbers are named after the French Mathematician Marin Mersenne, respectively (Srinath, et al.). The first group of Mersenne Primes have been known in the field of mathematics since around 1876, when mathematician Lucas discovered $2^{127} - 1$, the twelfth Mersenne Prime, was indeed a Mersenne Prime (Robinson 842). We can prove that since $a^p - 1$ is prime, then k is prime and $a = 2$, hence proving that Mersenne Primes exist.

Proof. Let $a^k - 1$ be prime. We will show that $a = 2$ and k is prime.
We will first show that $a = 2$. Let's consider a while working $\pmod{a-1}$.
Since $a - 1 | a^k - 1$, we know that $a \equiv 1 \pmod{a-1}$. Similarly, $a^k \equiv 1 \pmod{a-1}$
So, $a - 1 \equiv 0 \pmod{a-1}$ and $a^k - 1 \equiv 0 \pmod{a-1}$ (as shown previously).
Recall however that $a^k - 1$ is prime. So, we have that $a^k - 1 = a - 1$ or $a - 1 = 1$ since

the only factors of a prime are one and itself. If $a - 1 = a^k - 1$, then $a = a^k$ which is a contradiction as this would not be prime [since $k > 1$, $a = 0$ or $a = 1$, and neither are prime]. So it must be that $a - 1 = 1$ which would lend that $a = 2$, as desired. Since $a = 2$, we now know that $2^k - 1$ is prime. To prove that k is prime, we will prove this by contrapositive. Let k be composite. Then by definition, k can be factored as $k = ab$ for some $a, b \in \mathbb{P}$.
So, $2^k - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)[(2^a)^{b-1} + \cdots + a + 1]$, so $2^k - 1$ is composite.
Thus by contrapositive, if k is prime,. $2^k - 1$ is also prime. □

So we have shown that Mersenne Primes M_P exist. Furthermore, there are a multitude of theorems within the exposition written by Srinath, et. al that explore certain properties within Mersenne Primes themselves. These theorems explore congruence properties of Mersenne Primes themselves when working different groups of primes and different sets of modulo n using the Chinese Remainder Theorem and Arithmetical Primes.

An Arithmetical Prime is a prime according to Dirichlet's Theorem, which states that for $a, b \in \mathbb{P}$ with $\gcd(a, b) = 1$, the set $\{an + b, n >= 1\}$ will have infinitely many primes. For example, consider $a = 3, b = 4$. The set $\{3n + 4, n >= 1\} = \{3 + 4 = 7, 9 + 4 = 13, \dots\}$ (Srinath, et al.). A new theorem proposed on the relationship between arithmetical progression and Mersenne primes states: "Every Mersenne Prime, M_P, is a prime number of the form $4n + 3$, for some integer 'n'" (Srinath, et al). The proof is fairly straight forward using induction, and also provided in the text. Based on this relationship, further conjectures were made about the congruence relationships of Mersenne Primes, and the proofs were left to the reader. There were nine given theorems, but we will explore three of them.

Let p be an odd prime and M_P be a Mersenne Prime. Then, the following hold:

1. $M_P \equiv 1 \pmod 2$
2. $M_P \equiv 1 \pmod 3$
3. $M_P \equiv 3 \pmod 4$ (Srinath et al).

Proof. Let p be an odd prime and M_P be a Mersenne Prime.

1. We will first show that $M_P \equiv 1 \pmod 2$. Since M_P is a Mersenne Prime, $M_P = 2^p - 1$. So, we will show that $2^P - 1 \equiv 1 \pmod 2$. This is trivial, since $2^p \equiv 0 \pmod 2 \implies 2^p - 1 \equiv -1 \pmod 2 \implies 2^p - 1 \equiv 1 \pmod 2$.
2. We will now show that $M_P \equiv 1 \pmod 3$. Consider $2^p - 1$, while working modulo 3. We know that $2^p - 1 \not\equiv 2 \pmod 3$, because $2^p - 1$ would be even and thus composite. If $2^p - 1 \equiv 0 \pmod 3$, then $2^p \equiv 1 \pmod 3$ and thus $p = 2$, which is a contradiction against our hypothesis. Thus, $2^p - 1 \equiv 1 \pmod 3$.
3. We will lastly prove that $M_P \equiv 3 \pmod 4$. Since $M_P = 2^P - 1$, we know that $2^p \equiv \pmod 4 \implies 2^p - 1 \equiv -1 \pmod 4 \implies 2^p - 1 \equiv 3 \pmod 4$.

□

These first three theorems were quite trivial to prove, but we can look at other theorems regarding M_P that are more exhaustive, less intuitive proofs.

Fermat's Little Theorem is especially important in proving various theorems about Mersenne Primes. As a reminder so that we can use the theorem later, Fermat's Little Theorem states: Let p be a any prime number and $a \in \mathbb{Z}$, with $p \not| a$. Then, $a^{p-1} \equiv 1 \pmod{p}$. The proof approach and conclusions of Fermat's Little Theorem are especially important in proving ideas about the cardinality of both Mersenne Primes and Perfect Numbers. While Mersenne Primes are certainly able to be calculated by hand using the Lucas-Lehmer Test, it is important to note that in recent years, computers have been integral in finding Mersenne Primes. For this reason, a chunk (albeit small) of code provided below shows computational ideas on how to search for Mersenne Primes and their corresponding perfect numbers less than $1,000,000$:

```
%creates an array of primes less than the specified number
p = primes(10^6);
candidates = [];
exponents = [];
perfect = [];

 %this for loop creates a different array to intersect
 %the primes that are of the form 2^n - 1
 for x = 1:20
     candidates(end+1) = sym(2)^x-1;
     if isprime(sym(2)^x-1);
         exponents(end+1) = x;
     end
 end

%intersecting these two arrays gives us a list of Mersenne Primes
m = intersect(p, candidates);

%finding the correlating perfect numbers
%these are of the form 2^(p-1)((2^p) - 1)
for q = exponents
    perfect(end+1) = sym(2)^(q-1)*(sym(2)^(q)-1);
end

disp(sym(m));
disp(sym(perfect));
```

Further we can prove the relationship between M_P and other whole numbers with respect to modulo arithmetic. For example, the following theorems are given.
Let p be an odd prime and M_P be a Mersenne Prime. Then the following hold:

1. $M_P \equiv 1 \pmod{9}$ if $p \equiv 1 \pmod{3}, p > 3$
   $M_P \equiv 4 \pmod{9}$ if $p \equiv 2 \pmod{3}$

2. $M_P \equiv 1 \pmod{10}$ if $p \equiv 1 \pmod 4$
   $M_P \equiv 7 \pmod{10}$ if $p \equiv 3 \pmod 4$ (Srinath et al).

(Note, this guideline was used to prove the following: every Mersenne Prime M_P is a number of the form $4n + 3$ with respect to arithmetic numbers. We have modified it to prove the above.):

Proof. 1. Let p be an odd prime and M_P be a Mersenne Prime. For (1), we are looking to show that $T_n = 9k+1$ for $p \equiv 1 \pmod 3, p > 3$ and $T_n = 9k+4$ for $p \equiv 2 \pmod 3$. Equivalently, if $p = 3s+1$, then $T_n = 9k+1$ and if $p = 3s+2$, then $T_n = 9k+4$. Using induction, we prove the base case first.

Base Case

For $p \equiv 1 \pmod 3$, $p > 3$, the base case is $p = 7$. So, $2^7 - 1 = 128 - 1 = 127 = 9*14+1$. So, $2^7 - 1 = 127 \equiv 1 \pmod 9$.

For $p \equiv 2 \pmod 3$, the base case is $p = 5$. So, $2^5 - 1 = 32 - 1 = 31 \equiv 4 \pmod 9$.

Inductive Steps

Assume that it holds for k. That is, $2^k - 1 \equiv 1 \pmod 9$, with $k \equiv 1 \pmod 3$
$2^k - 1 \equiv 4 \pmod 9$, with $k \equiv 2 \pmod 3$. We will show it holds for $k + 1$.

Case One: $k \equiv 1 \pmod 3$

We want $2^n - 1$ of the form $9n + 1$. We assume that $T_k = 9k_0 + 1$. So, for $k_0 + 1$ we have $2^{k_0+1} - 1 = 2_0^k * 2 - 1 = 2_0^k(2) - 1 = 2(9k_0 + 2) - 1 = 18k_0 + 4 - 1 = 18k_0 + 3 = 9(2k_0\frac{2}{9}) + 1 = 9k' + 1$ for $k' = 2k_0 + \frac{2}{9}$, so we have our desired result.

Case Two: $k \equiv 2 \pmod 3$

We want $T_k = 9k + 4$. We assume that $T_k = 9k_0 + 4$. So, for $k_0 + 1$, we have $2^{k+1} - 1 = 2^k(2) - 1 = (9k+8)2 - 1 = 18k + 16 - 1 = 18k + 15 = 9(2k_0 + \frac{11}{9}) + 4 = 9k' + 4$, for $k' = 2k_0 + \frac{11}{9}$.

Overall, using induction we have proved that (1) holds for all values of M_p.

2. For (2), we are looking to show that $T_k = 10k + 1$ for $p \equiv 1 \pmod 4$ and $M_p \equiv 7 \pmod{10}$, for $p \equiv 3 \pmod 4$.

Base Case

For $p \equiv 1 \pmod 4$, our base case if $p = 5$. So, $2^5 - 1 = 31 \equiv 1 \pmod{10}$.

For $p \equiv 3 \pmod 4$, our base case is $p = 4$, which we showed above $2^3 - 1 = 7 \equiv 7 \pmod{10}$.

Inductive Steps

We assume that it holds for k.

Case One: $p \equiv 1 \pmod 4$

We want T_N of the form $10k + 1$. We assume that $T_k = 10k + 1$. So for $k + 1$, we have $2^{k-1} = 2^k(2) - 1 = (10k + 2)2 - 1 = 20k + 4 - 1 = 20k + 3 = 10(2k + \frac{1}{5}) + 1 = 10k' + 1$, with $k' = 2k + \frac{1}{5}$.

Case Two: $p \equiv 7 \pmod{10}$

We want T_n of the form $10k + 7$. We assume that $T_k = 10k + 7$, so for $k + 1$ we have $2^{k+1} - 1 = 2^k 2 - 1 = (10k+8)2 - 1 = 20k + 16 - 1 = 20k + 15 = 10(2k + \frac{4}{5}) + 7 = 10k' + 7$, with $k' = 2k + \frac{4}{5}$

□

Recall that the Chinese Remainder Theorem is integral in proving relationships between Mersenne Primes and other whole numbers. For a reminder, the Chinese Remainder Theorem (CRT) states the following: "Given pairwise coprime positive integers $n_1, n_2, \ldots, n_k$ and arbitrary integers $a_1, a_2, \ldots, a_k$, the system of simultaneous congruences $x \equiv a_1 \pmod{n_1}, x \equiv a_2 \pmod{n_2}, \ldots, x \equiv a_k \pmod{n_k}$ has a solution and the solution is unique modulo $N = n_1 n_{2k}$." (Clement, et al). So, if we wanted to compute $M_P \equiv x \pmod{12}$, we could use the CRT and our equivalence relations less than ten (Srinath et al).

Perfect Numbers

As we begin investigating various theorems and relationships about Perfect Numbers, let's first revisit the core definition of a perfect number. According to the Euclid-Euler formula, a perfect number n is a perfect number if $n = 2^{k-1}(2^k - 1)$, where $2^k - 1$ is a Mersenne Prime (Pomerance 195). Further, we should define the σ function, which is the sum of all of the divisors of n, $\sum_{d|n} d$. With respect to perfect numbers, it was discovered that for $n = 2^{k-1}(2^k - 1)$ a perfect number, $\sigma(n) = 2n$. Now, one of the more profound and oldest unsolved mathematical problems or theories is the idea of having an odd perfect number. We know that the first few perfect numbers by small computations are 6 and 28, but mathematicians have since struggled to find any odd perfect numbers. Two well-known theorems have been found with regards to odd perfect numbers, which stated that for N an odd perfect number, $N \equiv 1 \pmod{9}$ or $N \equiv 9 \pmod{36}$ (Voight 293). No such odd perfect numbers have been discovered, but mathematicians have been able to develop upper and lower bounds for these such numbers.

Given the σ function, other types of perfect numbers have been discovered. Quasi-perfect numbers are of the form $\sigma(n) = 2n + 1$, but no such quasi-perfect numbers have been discovered (Cohen 372). While these respective numbers have yet to be discovered, it is known that for these to exist, $N > 10^{20}$ and N must have at least six distinct prime factors (Cohen 370). Furthermore, while perfect numbers are of the form $\sigma(n) = 2n$, multi-perfect numbers are of the form $\sigma(n) = kn, k \geq 2$. We will investigate tri-perfect numbers which are of the form $\sigma(n) = 3n$.

According to research, there are only a handful of discovered tri-perfect numbers. The first is 120 and the rest follow: $672, 523776, 459818240, 1476304896$, and 51001180160. Below is a program that not only compute $\sigma(n)$, but also returns whether n is a perfect or tri-perfect number.

```
%The following program computes the sigma function for the input
%It then tells you if it is a perfect or tri-perfect number

function [m] = sigma(n)
    d = divisors(n);
    q = [];

    for x = d
        q(end+1) = x;
```

```
 end
 m = sum(q);
if 2n == m
    disp("This is a perfect number");
end
if 3n == m
        disp("This is a tri-perfect number");
end
```

In continuation, interestingly enough it has been proven that if n is a perfect number, $8n+1$ is a perfect square (or equivalently, n a perfect number implies that n is a triangular number. The proof was given, but we will share it below:

Proof. Let n be a perfect number and $m \in \mathbb{P}$. Then,

$$n = \frac{m+1}{m} \implies 8n+1 = 4m(m+1)+1 = 4m^2+4m+1 = (2m+1)^2$$

□

'("The Mathematical Magic of Perfect Numbers").

Concluding Thoughts

Overall it would appear that there is a great deal more research out there on the idea of Mersenne Primes, rather than on perfect numbers. This seemed surprising given the multitude of conclusions that seemingly could be drawn given this relationship. However, it is important to recognize that we touched only on a glimpse of the various ideas and theorems surrounding this relationship. Additionally, the relationship between mathematics and computer science has been seemingly integral in the discover of large Mersenne Primes, Perfect Numbers, and multiply perfect numbers as well. While the idea of having an odd perfect number is still unsolved, it would appear that using lower and upper bounds, as well as programming would be imperative to this discovery. Additionally, we have the Chinese Remainder Theorem to thank for allowing mathematicians to investigate the modulo relationships within Mersenne Primes and whole numbers. Further, several of Fermat's Theorems (namely his little theorem and last theorem) were used to prove some of the fundamental aspects regarding Mersenne Primes and Perfect Numbers.

References

[Srinath et al] Srinath, M. S., Murthy, G. R., Chandrasekharan, V. (2011). *Congruence Properties of Mersenne Primes.*

[Robinson 842] Robinson, R. M. (1954). Mersenne and Fermat Numbers. *Proceedings of the American Mathematical Society*, 5(5), 842–846. https://doi.org/10.2307/2031878

[Pomerance 195] Pomerance, C. (1997). *Multiply Perfect Numbers, Mersenne Primes, and Effective Computability.* https://math.dartmouth.edu/ carlp/PDF/paper13.pdf

[Voight 293] Katok, S., amp; Voight, J. (2003). On the Existence of Odd Perfect Numbers. In *Mass Selecta: Teaching and learning advanced undergraduate mathematics* (pp. 293–300). essay.

[n.d] *Chinese Remainder Theorem* Brilliant Math amp; Science Wiki. (n.d.). Retrieved December 8, 2021, from https://brilliant.org/wiki/chinese-remainder-theorem/.

[n.d] *The Mathematical Magic of Perfect Numbers*, *Gerogia Journal of Science*, Vol. 66, No. 2, Article 4. Retrieved from https://digitalcommons.gaacademy.org/gjs/vol66/iss2/4