On the Cardinality of Mersenne Primes

Garimella Rama Murthy,
Associate Professor,
International Institute of Information Technology (IIIT),
Gachibowli, Hyderabad-32, AP, INDIA

ABSTRACT

In this research paper, it is shown that every Mersenne prime is a prime of the form \( 4n + 3 \), for some integer \( n \). Based on this result, approaches to determine the cardinality of Mersenne primes are discussed.

1. Introduction:

With the advent of the concept of “counting”, homo-sapien civilization in various parts of the planet began a systematic study of the properties of whole numbers (integers). Prime numbers were identified as those whole numbers which have the numbers “one” and “itself” as the divisors. Mathematicians became interested in determining the cardinality of prime numbers. Euclid provided an elegant proof that the prime numbers are infinite ("countably") (Har). Also, the fundamental theorem of arithmetic was proved by the Greek mathematicians. It states that every integer can be written as the product of powers of finitely many primes (below the integer). Euclid also provided an algorithm for computing the Greatest Common Divisor (GCD) of two whole numbers/integers. Also few books in Euclid’s Elements were devoted to number-theoretic investigations. Diophantus formulated the problem of solving algebraic equations in integers. For instance, it was proved that the sides of a right angle triangle satisfy an interesting quadratic Diophantine equation (named as the Pythagorean Theorem).

For quite a few centuries, there were only scattered mathematical results in number theory. Modern number theory began with the efforts of Fermat who recorded several interesting theorems (related to whole numbers) in the margins of his copy of “Arithmetica” (written by Diophantus) (Dun). For instance, the following theorem is the famous little theorem of Fermat:

**Theorem 1:** If “\( p \)” is a prime and “\( a \)” is a whole number which does not have “\( p \)” as a factor, then “\( p \)” divides evenly into \( a^{p-1} - 1 \). Equivalently, in the number theoretic notation we have \( a^{p-1} \equiv 1 \pmod{p} \).

Euler provided proofs for several theorems recorded by Fermat in his copy of “Arithmetica”. As time progressed, generations of mathematicians became interested in the following (so called) arithmetical function (kan):

\[ \pi(n) : \text{Total number of prime numbers until } 'n'. \]
Gauss conjectured the so-called “Prime Number Theorem” on empirical evidence. The formal proof was given by Hadamard et al. using the mathematical tools of analytic number theory. The Theorem states that

$$\lim_{n \to \infty} \frac{\pi(n)}{\frac{n}{\log n}} = 1.$$ 

Ever since, Euclid provided the elegant proof of the infinitude of the primes, mathematicians were interested in identifying special structured classes of primes and their cardinality. For instance, Fermat conjectured that

$$F_n = 2^{2^n} + 1$$

is a prime number for all \( n \geq 1 \). Euler refuted the conjecture by proving that \( F_5 \) is composite. In fact, so far, for no other value of ‘n’ (\( \geq 5 \)), \( F_n \) was found to be a prime number.

Mathematicians became interested in the problem of determining the cardinality of primes in arithmetical progressions like \{ 4n + 1, n \geq 1 \} and \{ 4m + 3, m \geq 1 \}. It was shown that Euclid’s proof argument can be naturally extended to prove that there are infinitely many primes in the arithmetical progression \{ 4n + 1, n \geq 1 \}. This approach did not directly work for determining the cardinality of primes in the arithmetical progression of the form \{ 4m + 3, m \geq 1 \}. Using the tools of analytic number theory, Dirichlet showed that there are infinitely many primes in every arithmetic progression of the form \{ an + b, n \geq 1 \} with \((a,b)=1\) i.e. “a” and “b” are relatively prime.

French father Marin Mersenne, defined primes of the form

$$M_p = 2^p - 1 \text{ for p a prime number}.$$ 

An interesting open problem is to determine the cardinality of Mersenne primes. There are several such open research problems. For instance, determination of cardinality of primes in the sequence \{ n^2 + 1, n \geq 1 \} is also an open research problem. An interesting general result is the following:

“No polynomial can generate primes for all integral values of the independent variable”.

In this technical report, we attempt the problem of determining the cardinality of Mersenne primes. This technical report is organized as follows. In Section 2, we summarize the Dirichlet Theorem on arithmetical primes. In Section 3, we explore the relationship between Mersenne primes and arithmetical primes. We prove an interesting theorem. In Section 4, our efforts at determining the cardinality of Mersenne primes (and thus that of even perfect numbers) are summarized. In Section 5, we conclude the technical report.

2. Arithmetical Primes: Dirichlet’s Theorem:

In view of the infinitude of primes of the form \{ 4n + 1, n \geq 1 \}, mathematicians were interested in the most general result regarding the cardinality of primes generated through an arithmetical progression. In this connection, the following observation follows readily:

- Suppose the Greatest Common Divisor (G.C.D) of \( a,b \) be \( D > 1 \).

Then it is easy to see that the arithmetic progression
\{ an + b, \ n \geq 1 \} \text{ will contain no prime numbers. Thus, let us consider the non-trivial case i.e} \\
\text{G.C.D. of } a, b = (a, b) = 1 \text{ i.e. } a, b \text{ are relatively prime.}

Using the tools of analytic number theory, Dirichlet proved the following interesting Theorem:

\textbf{Theorem 2:} Suppose ‘a’, ‘b’ are relatively prime numbers. Then the arithmetical progression \{ an + b, \ n \geq 1 \} \text{ will contain infinitely many prime numbers.}

In view of the above Dirichlet’s theorem, mathematicians are interested in determining the cardinality of prime numbers generated by a quadratic, cubic and higher degree polynomial (with the independent variable assuming integer values). The author is currently investigating this problem.

3. Relationship between Mersenne Primes and Arithmetic Primes:

On numerical (empirical) evidence, the author expected a relationship between Mersenne primes and arithmetical primes. Specifically Mersenne primes are related to the primes of the form \{ 4n + 3, \ n \geq 1 \}. The following Theorem is an interesting result in this direction:

\textbf{Theorem 3:} Every Mersenne prime, \( M_p \) is a prime number of the form \( 4n + 3 \) for some integer “n”.

\textbf{Proof:} First we consider the integers 
\[ T_n = 2^n - 1 \text{ for all integer values of } n. \]

We show that \( T_n = 4k + 3 \) for some integral value of \( k \). The proof approach is based on mathematical induction. It is easy to see that for \( n=2 \),
\[ T_2 = 3 = 4(0) + 3. \text{ Thus } k = 0. \]

Also, for \( n=3 \), we have that \[ T_3 = 7 = 4(1) + 3. \text{ Thus } k = 1. \]

Further, for \( n=4 \), we have that \[ T_4 = 15 = 4(3) + 3. \text{ Thus } k = 3. \]

\textbullet \ Now, let us assume that
\[ T_n = 4(k_0) + 3 \text{ for some integer } k_0. \]

It is easy to see that
\[ T_{n+1} = 2^{n+1} - 1 = (2^n)2 - 1 = 4k_0 + 4 \]
\[ = (4k_0 + 4)2 - 1 = 8k_0 + 7 = 4(2k_0 + 1) + 3 = 4k' + 3 \text{ for } k' = 2k_0 + 1. \]

Thus, by mathematical induction the claim holds true for \( n+1 \). Since, we are only interested in prime exponents, the claim still holds true. Thus

\textbullet \ Every Mersenne prime \( M_p \) is a prime of the form \( 4n +3 \) for some integer \( n. \)

Q.E.D.
**Corollary:** No Mersenne prime can be written as the sum of squares of two Integers

**Proof:** The corollary follows from the celebrated Theorem of Fermat on the primes of the form \( \{ 4n + 3 \mid n \geq 1 \} \). Q.E.D

**Note:** Not every prime of the form \( \{ 4n + 3 \mid \text{for some integer 'n'} \} \) is a Mersenne prime. For example, 19, 23.

- The above Theorem enables us to invoke results related to arithmetical primes of the form \( \{ 4n + 3 \mid n \geq 1 \} \) in association with the Mersenne primes. Details are discussed in the following section.

- As a generalization of Theorem 3, we expect the following result. It is trivial to see that \( a^p - 1 \) is never a prime number for \( a \geq 3 \). It will be an odd/even number when ‘a’ is even/odd number.

**Claim:** (i) If ‘p’ is a prime number and ‘a’ is an even number such that \( p \geq a \), then \( a^{p-1} \equiv 3 \pmod{4} \). (why not \( a^{p-1} \equiv 1 \pmod{4} \)).

(ii) If ‘p’ is a prime number and ‘a’ is odd number such that \( p \geq a \), then \( a^{p-1} \equiv 0 \pmod{4} \). (why not \( a^{p-1} \equiv 2 \pmod{4} \)).

### 4. Cardinality of Mersenne Primes and Perfect Numbers:

For a long time, determination of cardinality (finiteness or countably infiniteness) of Mersenne primes has been an open problem. It has been well known that this problem is directly related to the determination of cardinality of even perfect numbers (in view of the result of Euler on the structure of even perfect numbers). Specifically, we have the following Theorem:

**Theorem 4:** An even number, \( N \) is a perfect number if and only if

\[
N = 2^{p-1} M_p, \text{ where}
\]

‘p’ is a prime number and \( M_p \) is the associated Mersenne prime number.

- Another interesting problem is to determine whether there are any odd perfect numbers or not. Equivalently, it is to be determined whether all perfect numbers are just even numbers only.

Based on the Theorem 3, we attempt the problem of determination of cardinality of Mersenne primes. The following definition is utilized.

**Definition:** A Diophantine equation is called a “primal Diophantine equation” if all the integral solutions are required to be the prime numbers.

Based on the Theorem 3, we need to find the cardinality of solutions of the following “primal” Diophantine equation:

\[
M_p = 2^p - 1 = q = 4k + 3,
\]
where 'p', 'q' are prime numbers and 'k' is an integer.
i.e. The problem effectively boils down to the answer to the following question:

Q: Are there infinitely many arithmetic primes of the form \{ 4k + 3, k \geq 1 \} that
are also Mersenne primes?

- The following Lemma directly follows as a special case of Fermat's Little Theorem:

**Lemma 1:** If 'p' is a prime other than 2 and \( M_p = 2^p - 1 \) is the corresponding
Mersenne prime, then we have

\[ M_p = 2^p k + 1 \text{ for some integer 'k'}. \]

- The following Lemmas/ Theorems readily follow from the approach
to prove the Fermat's Little Theorem.

**Theorem 5:** If 'p' is a prime and 'a' is a whole number, then
\((a + 1)^p - (a^p + 1)\) is evenly divisible by 'p'.

**Theorem 6:** If 'p' is a prime and if \( a^p - a \) is evenly divisible by 'p', then so is
\((a + 1)^p - (a + 1)\).

**Theorem 7:** If 'p' is a prime and 'a' is any whole number, then 'p' divides
evenly into \( a^p - a \).

- Using the above Theorem with a=2, we readily have that

\[ M_p = p^k + 1 \text{ for some integer 'k'}. \]

- Special cases of Theorems 5 and 6 with a=2 can easily be derived.
They are avoided here for brevity.

The following approaches are currently attempted to determine the
cardinality of Mersenne primes:

**Approach 1:** Utilize the essential idea of Euclid's proof and the fact that the
product of finitely many Mersenne primes is a product of finitely many geometric progressions

**Approach 2:** Again utilize the idea of Euclid's proof along with the following fact:

\[ M_p = (1 + 1)^p - 1 = \binom{p}{1} + \binom{p}{2} + \ldots + \binom{p}{p} = 1 + 2p + \binom{p}{2} + \ldots + \binom{p}{p-2}. \]

**Approach 3:** Utilize the powerful tools of analytic number theory (as in the case
of proof of Dirichlet's Theorem) along with Theorem 3, proved in
this research paper.

**5. Conclusions:**

In this research paper, it is proved that every Mersenne prime
is a prime of the form \{ 4n + 3, for some integer 'n' \}. Generalizations
of this result are briefly discussed. Some special cases of the Fermat's Little
Theorem are briefly considered. Approaches to establish the cardinality of
Mersenne primes are summarized.
References:

