

On the number of prime factors of Mersenne numbers

Abílio Lemos and Ady Cambraia Junior

Departamento de Matemática
Universidade Federal de Viçosa
Viçosa-MG 36570-900

Brazil

abiliolemos@ufv.com.br
ady.cambraia@ufv.br

August 28, 2017

Abstract

Let $(M_n)_{n \geq 0}$ be the Mersenne sequence defined by $M_n = 2^n - 1$. Let $\omega(n)$ be the number of distinct prime divisors of n . In this short note, we present a description of the Mersenne numbers satisfying $\omega(M_n) \leq 3$. Moreover, we prove that the inequality, for $\epsilon > 0$, $\omega(M_n) > 2^{(1-\epsilon) \log \log n} - 3$ holds almost all positive integer n .

2010 *Mathematics Subject Classification*: 11A99, 11K65, 11A41.

Keywords: Mersenne numbers, arithmetic functions, prime divisors.

1 Introduction

Let $(M_n)_{n \geq 0}$ be the *Mersenne sequence* (sequence [A000225](#) in the OEIS) given by $M_0 = 0, M_1 = 1, M_2 = 3, M_3 = 7, M_4 = 15$ and $M_n = 2^n - 1$, for $n \geq 0$. A simple calculation shows that if M_n is a prime number, then n is a prime number. When M_n is a prime number, it is called Mersenne prime. Throughout history, many researchers sought to find Mersenne primes. Some tools are very important for the search for Mersenne primes, mainly the Lucas-Lehmer test. There are papers (see for example [\[1, 3, 11\]](#)) that seek to describe the prime factors of M_n , where M_n is a composite number and n is a prime number.

Besides, some papers seek to describe prime divisors of Mersenne number M_n , where n cannot be a prime number (see for example [\[4, 6, 8, 9, 10\]](#)). In this paper, we propose to investigate the function $\omega(n)$, which refers to the number of distinct prime divisors of n , applied to M_n .

2 Preliminary results

If n is a positive integer, write $\omega(n)$ for the number of distinct prime divisors of n . Some well known facts are presented below as lemmas.

The first Lemma is the well-know Theorem XXIII of [2], obtained by Carmichael.

Lemma 1. *If $n \neq 1, 2, 6$, then M_n has a prime divisor which does not divide any M_m for $0 < m < n$. Such prime is called a primitive divisor of M_n .*

We also need the following results:

$$d = \gcd(m, n) \Rightarrow \gcd(M_m, M_n) = M_d \quad (1)$$

Proposition 2. *If $1 < m < n$, $\gcd(m, n) = 1$ and $mn \neq 6$, then $\omega(M_{mn}) > \omega(M_m) + \omega(M_n)$.*

Proof. As $\gcd(m, n) = 1$, it follows that $\gcd(M_m, M_n) = 1$ by (1). Now, according to Lemma 1, we have a prime number p such that p divides M_{mn} and p does not divide $M_m M_n$. Therefore, the proof of proposition is completed. \square

Mihăilescu [7] proved the following result.

Lemma 3. *The only solution of the equation $x^m - y^n = 1$, with $m, n > 1$ and $x, y > 0$ is $x = 3, m = 2, y = 2, n = 3$.*

For $x = 2$, the Lemma 3 ensures that there is no $m > 1$, such that $2^m - 1 = y^n$ with $n > 1$.

Lemma 4. *Let p, q be prime numbers. Then,*

$$(i) \quad M_p \nmid (M_{pq}/M_p), \text{ if } 2^p - 1 \nmid q.$$

$$(ii) \quad M_p \nmid (M_{p^3}/M_p).$$

Proof. (i) We noticed that $M_{pq} = (2^p - 1)(\sum_{k=0}^{q-1} 2^{kp})$. Thus, if $(2^p - 1) | (\sum_{k=0}^{q-1} 2^{kp})$, then

$$(2^p - 1) \left| \left(\sum_{k=0}^{q-1} 2^{kp} + 2^p - 1 \right) \right. = 2^{p+1} (2^{pq-2p-1} + \dots + 2^{p-1} + 1),$$

i.e., $(2^p - 1) | ((q - 2)2^{p-1} + 1)$, where $(q - 2)2^{p-1} + 1$ is the rest of the euclidean division of $2^{pq-2p-1} + 2^{pq-3p-1} + \dots + 2^{pq-(q-2)p-1} + 2^{p-1} + 1$ by $2^p - 1$, i.e.,

$$(2^p - 1) | ((q - 2)2^{p-1} + 1 + (2^p - 1)) = 2^{p-1}q,$$

i.e., $2^p - 1 | q$. Therefore, the proof of (i) is completed.

(ii) We noticed that $M_{p^3} = (2^p - 1)(\sum_{k=0}^{p^2-1} 2^{kp})$. Thus, if $(2^p - 1) | (\sum_{k=0}^{p^2-1} 2^{kp})$, then

$$(2^p - 1) \left| \left(\sum_{k=0}^{p^2-1} 2^{kp} + 2^p - 1 \right) \right. = 2^{p+1} (2^{p^3-2p-1} + \dots + 2^{p-1} + 1),$$

i.e., $(2^p - 1) \mid ((p^2 - 2)2^{p-1} + 1)$, where $(p^2 - 2)2^{p-1} + 1$ is the rest of the euclidean division of $2^{p^3-2p-1} + 2^{p^2-3p-1} + \dots + 2^{p^3-(p^2-2)p-1} + 2^{p-1} + 1$ by $2^p - 1$, i.e.,

$$(2^p - 1) \mid ((p^2 - 2)2^{p-1} + 1 + (2^p - 1)) = 2^{p-1}p^2,$$

i.e., $2^p - 1 \mid p^2$. But, for $p = 2$ or $p = 3$, $2^p - 1 \nmid p^2$ and for $p \geq 5$, we have $2^p - 1 > p^2$. Therefore, the proof of (ii) is completed. \square

Remark 5. It is known that all divisors of M_p have the form $q = 2lp + 1$, where p, q are prime numbers and $l \equiv 0$ or $-p \pmod{4}$.

3 Mersenne numbers with $\omega(M_n) \leq 3$

Theorem 6. *The only solutions of the equation*

$$\omega(M_n) = 1$$

are given by n , where n is a prime number for which M_n is a prime number of the form $2lp + 1$, where $l \equiv 0$ or $-p \pmod{4}$.

Proof. The case $n = 2$ is obvious. The equation implied in $M_n = q^m$, with $m \geq 1$. However, according to Lemma 3, $M_n \neq q^m$, with $m \geq 2$. Thus, if there is a unique prime number q that divides M_n , then $M_n = q$, and $q = 2lp + 1$, where $l \equiv 0$ or $-p \pmod{4}$, according to Remark 5. \square

Proposition 7. *Let p_1, p_2, \dots, p_s be distinct prime numbers and n a positive integer such that $n \neq 2, 6$. If $p_1^{\alpha_1} \cdots p_s^{\alpha_s} \mid n$, where the α_i 's are positive integers and $\sum_{i=1}^s \alpha_i = t$, then $\omega(M_n) \geq t + 1$.*

Proof. According to Lemma 1, we have

$$\omega(M_{p_i^{\alpha_i}}) > \omega(M_{p_i^{\alpha_i-1}}) > \dots > \omega(M_{p_i}) \geq 1,$$

for each $i \in \{1, \dots, s\}$. Therefore, $\omega(M_{p_i^{\alpha_i}}) \geq \alpha_i$. Now, according to Proposition 2, we have

$$\omega(M_n) > \sum_{i=1}^s \omega(M_{p_i^{\alpha_i}}) \geq \sum_{i=1}^s \alpha_i = t.$$

Therefore, $\omega(M_n) \geq t + 1$. \square

To facilitate the proof of the next two theorems, we present two specific cases of Proposition 7.

Proposition 8. *Let $n \neq 6$ and*

(i) $p_1^3|n$, where p_1 is a prime number or

(ii) $p_1p_2|n$ or $2p_1|n$, where p_1, p_2 are distinct odd prime numbers.

Then, $\omega(M_n) \geq 3$.

Proof. For $p_1^3|n$, we apply the first part of the proof Proposition 7, with $s = 1$ and $\alpha_1 = 3$. For $p_1p_2|n$ and $2p_1|n$, we apply the Proposition 7, with $s = 2$ and $\alpha_1 = \alpha_2 = 1$. □

Proposition 9. *Let*

(i) $p_1^4|n$, where p_1 is a prime number or

(ii) $p_1p_2p_3|n$, where p_1, p_2, p_3 are distinct prime numbers or

(iii) $p_1p_2^2|n$, where p_1, p_2 are distinct prime numbers.

Then, $\omega(M_n) > 3$.

Proof. For $p_1^4|n$, we apply the first part of the proof Proposition 7, with $s = 1$ and $\alpha_1 = 4$. For $p_1p_2p_3|n$, we apply the Proposition 7, with $s = 3$ and $\alpha_1 = \alpha_2 = \alpha_3 = 1$. For $p_1p_2^2|n$, we apply the Proposition 7, with $s = 2$, $\alpha_1 = 1$ and $\alpha_2 = 2$. □

Theorem 10. *The only solutions of the equation*

$$\omega(M_n) = 2$$

are given by $n = 4, 6$ or $n = p_1$ or $n = p_1^2$, for some odd prime number p_1 . Furthermore,

(i) if $n = p_1^2$, then $M_n = M_{p_1}q^t$, $t \in \mathbb{N}$.

(ii) if $n = p_1$, then $M_n = p^sq^t$, where p, q are distinct odd prime numbers and $s, t \in \mathbb{N}$ with $\gcd(s, t) = 1$. Moreover, p, q satisfy $p = 2l_1p_1 + 1$, $q = 2l_2p_1 + 1$, where l_1, l_2 are distinct positive integers and $l_i \equiv 0$ or $-p \pmod{4}$.

Proof. This first part is an immediate consequence of Proposition 8.

(i) If $\omega(M_n) = 2$, with $n = p_1^2$, then on one hand $M_n = p^sq^t$, with $t, s \in \mathbb{N}$. On the other hand, by Lemma 1 $\omega(M_{p_1^2}) > \omega(M_{p_1}) \geq 1$, i.e., $M_{p_1} = p$, by Lemma 3. Thus, according to Lemma 4, $M_n = M_{p_1}q^t = pq^t$, with $t \in \mathbb{N}$.

(ii) If $\omega(M_n) = 2$, with $n = p_1$, then $M_n = p^sq^t$, with $t, s \in \mathbb{N}$. However, according to Lemma 3, we have $\gcd(s, t) = 1$. The remainder of the conclusion is a direct consequence of Remark 5. □

Theorem 11. *The only solutions of the equation*

$$\omega(M_n) = 3$$

are given by $n = 8$ or $n = p_1$ or $n = 2p_1$ or $n = p_1p_2$ or $n = p_1^2$ or $n = p_1^3$, for some distinct odd prime numbers $p_1 < p_2$. Furthermore,

- (i) if $n = 2p_1$, then $M_n = 3M_{p_1}k^r$, $r \in \mathbb{N}$, if $p_1 \neq 3$ and k is a prime number.
- (ii) if $n = p_1p_2$, then $M_n = M_{p_1}(M_{p_2})^tk^r$ and $\gcd(t, r) = 1$, with $t, r \in \mathbb{N}$, and k is a prime number.
- (iii) if $n = p_1^2$, then $M_n = M_{p_1}q^tk^r$ or $M_n = p^sq^tk^r$, with $M_{p_1} = p^sq^t$ and $(s, t) = 1$, and p, q, k are prime numbers.
- (iv) if $n = p_1^3$, then $M_n = M_{p_1}q^tk^r$ and $\gcd(t, r) = 1$, with $t, r \in \mathbb{N}$, and q, k are prime numbers.
- (v) if $n = p_1$, then $M_n = p^sq^tk^r$ and $p = 2l_1p_1 + 1, q = 2l_2p_1 + 1, k = 2l_3p_1 + 1$, where l_1, l_2, l_3 are distinct positive integers and $l_i \equiv 0$ or $-p \pmod{4}$, and $\gcd(s, t, r) = 1$, with $s, t, r \in \mathbb{N}$.

Proof. This first part is an immediate consequence of the Proposition 9.

(i) If $\omega(M_n) = 3$, with $n = 2p_1$, then on one hand $M_n = p^sq^tk^r$, with $t, s, r \in \mathbb{N}$. On the other hand, according to Proposition 2, $\omega(M_{2p_1}) > \omega(M_{p_1}) + \omega(M_2)$, i. e., $M_{p_1} = q$, according to Lemma 3. We noticed that $M_{2p_1} = (2^{p_1} - 1)(2^{p_1} + 1)$ and q does not divide $2^{p_1} + 1$, because if $q|(2^{p_1} + 1)$, then $q|2^{p_1} + 1 - (2^{p_1} - 1) = 2$. This is a contradiction, since q is odd prime. Thus, $M_n = (M_2)^sM_{p_1}w^r = 3^sq^tk^r$. Moreover, according to Lemma 4, we have $s = 1$ if $p_1 \neq 2^2 - 1 = 3$. Therefore, $M_n = M_2M_{p_1}w^r = 3qk^r$.

(ii) If $\omega(M_n) = 3$, with $n = p_1p_2$, then on one hand $M_n = p^sq^tk^r$, with $t, s, r \in \mathbb{N}$. On the other hand, according to Proposition 2, $\omega(M_{p_1p_2}) > \omega(M_{p_1}) + \omega(M_{p_2})$, i. e., $M_{p_1} = p$ and $M_{p_2} = q$, according to Lemma 3. Thus, $M_n = (M_{p_1})^s(M_{p_2})^tk^r = p^sq^tk^r$ and $\gcd(s, t, r) = 1$ if $s, t, r > 1$, according to Lemma 3. However, if $2^{p_1} - 1 \nmid p_2$, then $t = 1$ according to Lemma 4 and clearly, $2^{p_2} - 1 \nmid p_1$, because $p_1 < p_2$, i.e., according to Lemma 4, again, we have $s = 1$. Thus, $M_n = M_{p_1}M_{p_2}k^r = pqk^r$.

(iii) If $\omega(M_n) = 3$, with $n = p_1^2$, then on one hand $M_n = p^sq^tk^r$, with $t, s, r \in \mathbb{N}$. On the other hand, according to Lemma 4, we have $M_{p_1} = p^sq^t$, with $(s, t) = 1$ or $M_{p_1} = p$.

(iv) If $\omega(M_n) = 3$, with $n = p_1^3$, then on one hand $M_n = p^sq^tk^r$, with $t, s, r \in \mathbb{N}$. On the other hand, according to Lemma 1, $\omega(M_{p_1^3}) > \omega(M_{p_1^2}) > \omega(M_{p_1}) \geq 1$, i.e., $M_{p_1} = p$, according to Lemma 3. Thus, $M_n = M_{p_1}q^tk^r = pq^tk^r$ according to Lemma 4 and, $\gcd(t, r) = 1$ according to Lemma 3.

(v) If $n = p_1$, then $M_n = p^sq^tk^r$, with $t, s, r \in \mathbb{N}$. However, according to Lemma 3, $\gcd(s, t, r) = 1$. The form of p, q and k is given by Remark 5. \square

We present some examples of solutions for Theorems 6, 10 and 11.

- (i) $\omega(M_n) = 1$, where n is a prime number: $M_2 = 3, M_3 = 7, M_5 = 31, M_7 = 127, \dots$
- (ii) $\omega(M_n) = 2$, where n is a prime number: $M_{11} = 2047 = 23 \times 89, M_{23} = 8388607 = 47 \times 178481, \dots$ and $M_6 = (M_2)^2M_3$; with $n = p^2$, where p is a prime number: $M_4 = 15 = M_2 \times 5, M_9 = 511 = M_3 \times 73, M_{49} = M_{27} \times 4432676798593, \dots$

(iii) $\omega(M_n) = 3$, where n is a prime number: $M_{29} = 536870911 = 233 \times 1103 \times 2089$, $M_{43} = 8796093022207 = 431 \times 9719 \times 2099863, \dots$; with $n = 2p$, where p is a prime number: $M_{10} = M_2 \times M_5 \times 11$, $M_{14} = M_2 \times M_7 \times 43 \dots$; with $n = p^3$, p is a prime number: $M_8 = 255 = M_2 \times 5 \times 17$, $M_{27} = M_3 \times 73 \times 262657, \dots$; with $n = p_1 p_2$, where p_1 and p_2 are prime numbers: $M_{15} = M_3 \times M_5 \times 151$, $M_{21} = (M_3)^2 \times M_7 \times 337, \dots$; with $n = p^2$, where p is a prime number: $M_{25} = M_5 \times 601 \times 1801, \dots$

4 Mersenne numbers rarely have few prime factors.

We observe, that by Proposition 7, we have $\omega(M_n) \geq t + 1$, where t is the number of prime divisors of n , counting the multiplicity. Of course, this lower bound depends on n , but it is necessary to obtain the factorization of n . The theorem below proved a lower bound that depends directly on n . To prove this theorem, we need the following lemma.

Lemma 12 (Theorem 432, [5]). *Let $d(n)$ be the total number of divisors of n . If ϵ is a positive number, then*

$$2^{(1-\epsilon) \log \log n} < d(n) < 2^{(1+\epsilon) \log \log n}$$

for almost all positive integer n .

Theorem 13. *Let ϵ be a positive number. The inequality*

$$\omega(M_n) > 2^{(1-\epsilon) \log \log n} - 3$$

holds for almost all positive integer n .

Proof. According to Lemma 1, we know that if $h|n$ and $h \neq 1, 2, 6$, then M_h has a prime primitive factor. This implies that

$$\omega(M_n) \geq d(n) - 3$$

Consequently, by Lemma 12, we have

$$\omega(M_n) > 2^{(1-\epsilon) \log \log n} - 3$$

for almost all positive integer n . □

References

- [1] J. Brillhart, On the factors of certain Mersenne numbers. II, *Math. Comp.* **18** (1964), no. 87–92.
- [2] R. D. Carmichael, On the numerical factors of arithmetic forms $\alpha^n \pm \beta^n$, *Ann. of Math.* **15** (2) (1913/14), no. 1–4, 30–48.

- [3] J. R. Ehrman, The number of prime divisors of certain Mersenne numbers, *Math. Comp.* **21** (1967), no. 700–704.
- [4] K. Ford, F. Luca, I. E. Shparlinski, On the largest prime factor of the Mersenne numbers, *Bull. Austr. Math. Soc.* **79 (3)** (2009), 455–463.
- [5] G. H. Hardy and E. M. Wright, Editors (D. R. Heath-Brown, Joseph H. Silverman). An Introduction to the Theory of Numbers, Sixth Edition, *Oxford University Press* (2008).
- [6] L. Murata, C. Pomerance, On the largest prime factor of a Mersenne number, *Number Theory* **36** (2004), 209–218.
- [7] P. Mihăilescu, Primary Cyclotomic Units and a Proof of Catalan’s Conjecture. *J. Reine Angew. Math.* **572** (2004), 167–195.
- [8] C. Pomerance, On primitive divisors of Mersenne numbers, *Acta Arith.* **46** (1986), 355–367.
- [9] A. Schinzel, On primitive prime factors of $a^n - b^n$, *Proc. Cambridge Philos. Soc.* **58** (1962), 555–562.
- [10] C. L. Stewart, The greatest prime factor of $a^n - b^n$, *Acta Arith.* **26** (1974/75), 427–433.
- [11] S. S. Wagstaff, Jr., Divisors of Mersenne numbers. *Math. Comp.* **40** (1983), 385–397.