Prime factors of Mersenne numbers

Ady Cambraia Jr*, Michael P. Knapp†, Abílio Lemos*,
B. K. Moriya* and Paulo H. A. Rodrigues‡
ady.cambraia@ufv.br
mpknapp@loyola.edu
abiliolemos@ufv.br
bhavinkumar@ufv.br
paulo_rodrigues@ufg.br

February 1, 2021

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, given $\epsilon > 0$, $\omega(M_n) > 2^{(1-\epsilon)\log\log n} - 3$ holds for almost all positive integers n. Besides, we present the integer solutions (m, n, a) of the equation $M_m + M_n = 2p^a$ with $m, n \geq 2$, p an odd prime number and a a positive integer.

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 a 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, 12]) that seek to describe the prime factors of M_n, where M_n is a composite number and n is a prime number.

*Departamento de Matemática, Universidade Federal de Viçosa, Viçosa-MG 36570-900, Brazil
†Department of Mathematics and Statistics, Loyola University Maryland, 4501 North Charles Street, Baltimore MD 21210-2699, USA
‡Instituto de Matemática e Estatística, Campus Samambaia, CP 131, CEP 74001-970, Goiânia, Brazil

Besides, some papers seek to describe prime divisors of Mersenne number M_n, where n cannot be a prime number (see for example [4, 8, 9, 10, 11]). 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. Moreover, for a given odd prime p, we study the solutions of $M_m + M_n = 2p^a$, which as per our knowledge has not been studied anywhere in the literature.

2 Preliminary results

We start by stating some well-known facts. The first result is the well-known Theorem XXIII of [2], obtained by Carmichael.

Theorem 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:

$$d = \gcd(m, n) \Rightarrow \gcd(M_m, M_n) = M_d \tag{1}$$

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 Theorem 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. □

Mihăilescu [7] proved the following result.

Theorem 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 $x = 2$, Theorem 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) $M_p \nmid (M_{pq}/M_p)$, *if* $2^p - 1 \nmid q$;

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

Proof. (i) We note 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

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

Since $2^{pq-2p-1} + \cdots + 2^{p-1} + 1 \equiv (q-2)2^{p-1} + 1 \pmod{2^p - 1}$, we have $(2^p - 1)|\left((q-2)2^{p-1} + 1\right)$. Therefore,

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

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

□

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

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

In this section, we will characterize n for given value of $\omega(M_n)$. Moreover, as a consequence of Manea's Theorem – which we shall state next – we shall get the multiplicity $v_q(M_n)$ for a given odd prime q and a positive integer n.

Definition 6. Let n be a positive integer. The q-adic order of n, denoted by $v_q(n)$, is defined to be the natural l such that $q^l \mid\mid n$, i. e., $n = q^l m$ with $\gcd(q, m) = 1$.

Theorem 7 (Theorem 1 [6])**.** *Let a and b be two distinct integers, p be a prime number that does not divide ab, and n be a positive integer. Then*

1. *if $p \neq 2$ and $p|a-b$, then*

$$v_p(a^n - b^n) = v_p(n) + v_p(a-b);$$

2. *if n is odd, $a + b \neq 0$ and $p|a+b$, then*

$$v_p(a^n + b^n) = v_p(n) + v_p(a+b).$$

Theorem 8. *Let $q \neq 2$ be a prime number. Define $m = ord_q(2)$ and $w = v_q(2^m - 1)$. Let $n \in \mathbb{N}$, and write $n = q^l n_0$, with $\gcd(q, n_0) = 1$. Then*

$$v_q(M_n) = v_q(2^n - 1) = \begin{cases} 0 & \text{if } m \nmid n \\ l + w & \text{if } m|n. \end{cases}$$

Proof. By elementary number theory, we know that $2^n \equiv 1 \pmod{q}$ if and only if $\mathrm{ord}_q(2)|n$. This proves the first line of the formula.

Now, suppose that $m|n$ and write $n = mt$. Then we have

$$M_n = (2^m)^t - 1^t.$$

By Theorem 7 (with $a = 2^m$ and $b = 1$), we have

$$\begin{aligned} v_q(M_n) &= v_q(t) + v_q(2^m - 1) \\ &= l + w. \end{aligned}$$

This completes the proof. □

Theorem 9. *The only solutions of the equation*

$$\omega(M_n) = 1$$

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

Proof. The case $n = 2$ is obvious. For n odd, the equation implied is $M_n = q^m$, with $m \geq 1$. However, according to Theorem 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 $q = 2ln + 1$, where $l \equiv 0$ or $-n \pmod 4$, according to Remark 5. ☐

Proposition 10. *Let $p_1, p_2, \ldots, p_s$ be distinct prime numbers and n a positive integer such that $n \neq 2, 6$. If $p_1^{\alpha_1} \cdots p_s^{\alpha_s} | n$, where the $\alpha_i' s$ are positive integers and $\sum_{i=1}^{s} \alpha_i = t$, then*

$$\omega(M_n) \geq \begin{cases} t, & \text{if} \quad s = 1 \\ t + \displaystyle\sum_{i=2}^{s} \binom{s}{i}, & \text{if} \quad s > 1 \end{cases}.$$

Proof. According to Theorem 1, we have

$$\omega\left(M_{p_i^{\alpha_i}}\right) > w\left(M_{p_i^{\alpha_i - 1}}\right) > \cdots > \omega\left(M_{p_i}\right) \geq 1,$$

for each $i \in \{1, \ldots, s\}$. Therefore, $\omega(M_{p_i^{\alpha_i}}) \geq \alpha_i$ and this proves the case $s = 1$. Now, we observe that $\gcd\left(\prod_{i \in I} p_i, \prod_{j \in J} p_j\right) = 1$, for each pair $\emptyset \neq I, J \subset \{1, \ldots, s\}$ with $I \cap J = \emptyset$. Then follows from Theorem 1 and Proposition 2 that

$$\omega(M_n) \geq \sum_{i=2}^{s} \binom{s}{i} + t, \text{ if } s > 1.$$

☐

Now we are ready to prove some theorems.

Theorem 11. *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 $M_n = p^s q^t$, where p, q are distinct odd prime numbers and $s, t \in \mathbb{N}$ with $\gcd(s, t) = 1$. Moreover, p, q satisfy $p = 2l_1 p_1 + 1, q = 2l_2 p_1 + 1$, where l_1, l_2 are distinct positive integers and $l_i \equiv 0$ or $-p_1 \pmod 4$.

Proof. This first part is an immediate consequence of Proposition 10.

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

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

☐

Theorem 12. *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 $n = 2p_1$ and $p_1 \neq 3$, then $M_n = 3M_{p_1}k^r = 3qk^r$, $r \in \mathbb{N}$ and q, k are prime numbers.

(ii) if $n = p_1p_2$, then $M_n = (M_{p_1})^s M_{p_2} k^r = p^s q k^r$, with $s, r \in \mathbb{N}$ and p, q, k are prime numbers.

(iii) if $n = p_1^2$, then $M_n = M_{p_1} q^t k^r$ or $M_n = p^s q^t k^r$, with $M_{p_1} = p^s q^t$ and $(s, t) = 1$, and p, q, k are prime numbers.

(iv) if $n = p_1^3$, then $M_n = M_{p_1} q^t k^r = pq^t k^r$, with $t, r \in \mathbb{N}$ and p, q, k are prime numbers.

(v) if $n = p_1$, then $M_n = p^s q^t k^r$ 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 $-p_1 \pmod 4$, and $\gcd(s, t, r) = 1$, with $s, t, r \in \mathbb{N}$.

Proof. This first part is an immediate consequence of the Proposition 10.

(i) If $\omega(M_n) = 3$, with $n = 2p_1$, then on one hand $M_n = p^s q^t k^r$, 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 Theorem 3. We noted 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 an odd prime. Thus, $M_n = (M_2)^s M_{p_1} w^r = 3^s qk^r$. Moreover, according to Lemma 4, we have $s = 1$ if $p_1 \neq 2^2 - 1 = 3$. Therefore, $M_n = M_2 M_{p_1} w^r = 3qk^r$.

(ii) If $\omega(M_n) = 3$, with $n = p_1p_2$, then on one hand $M_n = p^s q^t k^r$, 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 Theorem 3. Thus, $M_n = (M_{p_1})^s (M_{p_2})^t k^r = p^s q^t k^r$ and $\gcd(s, t, r) = 1$ if $s, t, r > 1$, according to Theorem 3. However, $2^{p_2} - 1 \nmid p_1$, because $p_1 < p_2$. According to Lemma 4, we have $t = 1$. Thus, $M_n = M_{p_1}^s M_{p_2} k^r = p^s qk^r$.

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

(iv) If $\omega(M_n) = 3$, with $n = p_1^3$, then on one hand $M_n = p^s q^t w^r$, with $t, s, r \in \mathbb{N}$. On the other hand, according to Theorem 1, $\omega(M_{p_1^3}) > \omega(M_{p_1^2}) > \omega(M_{p_1}) \geq 1$, i.e., $M_{p_1} = p^s$. According to Theorem 3, we have $s = 1$. Thus, $M_n = M_{p_1} q^t k^r = pq^t k^r$.

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

We present some examples of solutions for Theorems 9, 11 and 12.

(i) $\omega(M_n) = 1$, where n is a prime number: $M_2 = 3, M_3 = 7, M_5 = 31, M_7 = 127, \ldots$

(ii) $\omega(M_n) = 2$, where n is a prime number: $M_{11} = 2047 = 23 \times 89, M_{23} = 8388607 = 47 \times 178481, \ldots$ and $M_6 = (M_2)^2 M_3$; with $n = p^2$, where p is a prime number: $M_4 = 15 = M_2 \times 5, M_9 = 511 = M_3 \times 73, M_{49} = M_7 \times 4432676798593, \ldots$.

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

Remark 13. Using Theorem 8 together with Theorem 11, 12, one can say something more about the structure of n.

4 Mersenne numbers rarely have few prime factors.

We observe that Proposition 10 provides a lower bound for $\omega(M_n)$. Of course, this lower bound depends on n, but it is necessary to obtain the factorization of n. The theorem below provided a lower bound that depends directly on n. To prove this theorem, we need the following lemma.

Theorem 14 (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 15. *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 Theorem 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 Theorem 14, we have

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

for almost all positive integer n. $\square$

5 Study of the Equation $M_m + M_n = 2p^a$

We consider the equation $M_m + M_n = 2p^a$ with $m, n \geq 2$, p an odd prime number and a a positive integer. We present two results on the solutions to this equation.

Lemma 16. *For every* $p \equiv 1 \pmod 4$ *we have* $p^a + 1 = 2k$, *where* $\gcd(k, 2) = 1$

Proof. We have

$$\begin{aligned} p \equiv 1 \pmod 4 \quad &\Rightarrow \quad p^a \equiv 1 \pmod 4 \\ &\Rightarrow \quad p^a + 1 \equiv 2 \pmod 4 \\ &\Rightarrow \quad p^a + 1 = 4a + 2, \quad \text{for some } a \in \mathbb{Z} \\ &\Rightarrow \quad p^a + 1 = 2k;\ \gcd(k, 2) = 1. \end{aligned}$$

□

Theorem 17. *Let* p *be a prime number with* $p \equiv 1 \pmod 4$. *Then*

$$M_m + M_n = 2p^a \tag{2}$$

has an integer solution only if $p = 2^{2^b} + 1$. *More precisely, such solutions are given by* $(m, n, a) = (2, 2^b + 1, 1)$.

Proof. Suppose that (2) has a solution, say (m, n, a). Without loss of generality, we can assume $m \leq n$. Notice that

$$2^m + 2^n = 2p^a + 2 = 4k,$$

by Lemma 16.

From which one can observe that $m = 2$ or $n = 2$, since otherwise k would be even.

Case 1. If $n = 2$ then $m \in \{1, 2\}$. Hence we get $4 + 2 = 4k$ or $4 + 4 = 4k$. Since 6 is not a multiple of 4, we are left with the later case, which implies $k = 2$. Therefore, $2k = 4 = p^a + 1$, which is absurd, since $p^a + 1 \geq 5$.

Case 2. $m = 2$ and $n > 2$. By definition of Mersenne numbers we have the following

$$\begin{aligned} 4(1 + 2^{n-2}) &= 2p^a + 2 = 4k \\ 2(1 + 2^{n-2}) &= p^a + 1 = 2k \\ p^a + 1 &= 2^{n-1} + 2. \end{aligned}$$

Subcase 1. $a = 1$. So we have, $p = 2^{n-1} + 1$. We know that if $2^N + 1$ is a prime number then N is a power of 2. Hence there exists b such that $n - 1 = 2^b$, i. e., $2 + 2^{2^b} = 2k$. Hence, if $(m, n, 1)$ is a solution of (2) then $m = 2$ and $n = 2^b + 1$ such that $2^{2^b} + 1$ is a prime number.

Subcase 2. $a \geq 2$. Suppose that there exists $a \geq 2$ satisfying the equation (2). This implies that $p^a = 2^{n-1} + 1$. Let us study when a is even and odd separately:

Subcase 2.1. a is even. The equation $p^a = 2^{n-1} + 1$ implies

$$\left(p^{\frac{a}{2}} - 1\right)\left(p^{\frac{a}{2}} + 1\right) = 2^{n-1}. \tag{3}$$

Let x and y be positive integers such that $p^{\frac{a}{2}} - 1 = 2^x$ and $p^{\frac{p}{2}} + 1 = 2^y$, then $y > x$ and $x + y = n - 1$. Thus $2^y - 2^x = 2^x(2^{y-x} - 1) = 2$ which implies $x = 1, y = 2$, and consequently $n = 4$. Therefore $p^a = 9$, i.e., $p = 3$ and $a = 2$, which is absurd, because $3 \not\equiv 1 \pmod 4$.

Subcase 2.2. a is odd. There exists a natural number l such that $a = 2l + 1$. Thus

$$p^a = 2^{n-1} + 1 \Rightarrow p^a - 1 = 2^{n-1} \Rightarrow (p-1)\left(1 + p + p^2 + \cdots p^{2l-1} + p^{2l}\right) = 2^{n-1}.$$

Thus, there exist positive integers x and y such that $p - 1 = 2^x$ and $1 + p + p^2 + \cdots p^{2l-1} + p^{2l} = 2^y$. Clearly $y > x$ and $x + y = n - 1$. Notice that $2^y - 2^x = 2 + p^2 + \cdots + p^{2l-1} + p^{2l} = k$, where k is odd, since $p \equiv 1 \pmod 4$. This only occurs when $x = 0$, that is a contradiction. □

Observation 18. *Since we know that Fermat primes are very rare, from Theorem 17 we can conclude that solutions are also very rare.*

The Theorem 17 explores solution in case prime $p \equiv 1 \pmod 4$. The next theorem will explore the solutions in case $p \equiv 3 \pmod 4$.

Theorem 19. *Let p be a prime number with $p \equiv 3 \pmod 4$. Then*

$$M_m + M_n = 2p^a \tag{4}$$

has an integer solution only if $p^a = 2^k(1 + 2^{n-(k+1)}) - 1$ with $2^k \mid\mid (p^a + 1)$. More precisely, such solutions are given by

(i) $(m, n, a) = (2, 4, 2)$;

(ii) $(m, n, a) = (k, k, 1)$ *if* $2^k = p^a + 1$. *In that case $M_k = p$ is a Mersenne prime;*

(iii) $(m, n, a) = (k + 1, n, a)$ *if* $p^a + 1 > 2^k$.

Proof. Since $p \equiv 3 \pmod 4$, there exists $k \in \mathbb{N}, k \geq 2$ such that $2^k \mid\mid (p^a + 1)$. Note that, if a is even, then $k = 1$. If a is odd, then $k \geq 2$, since $4 \mid (p^a + 1)$. Suppose (m, n, a) is a solution of (4). Without loss of generality we can assume $m \leq n$

Case 1. a is even.

As mentioned earlier, we can write $p^a + 1 = 2b$; where b is an odd integer. Since $p \geq 3$, we have $b \geq 5$. Observe that,

$$\begin{aligned} M_m + M_n &= 2p^a \\ 2^m + 2^n &= 2(p^a + 1) \\ 2^m + 2^n &= 2^2 b \end{aligned}$$

Hence, $m = 2$, which together with the fact that $b \geq 5$ implies, $n \geq 3$. Therefore, we have

$$\begin{aligned} 4(1 + 2^{n-2}) &= 2^2 b \\ 1 + 2^{n-2} &= b \end{aligned}$$

Therefore, we can conclude that, $b = 1 + 2^{n-2}$, which in turn implies $p^a + 1 = 2(1 + 2^{n-2})$ iff $(m, n, a) = (2, n, a)$ is the only solution of the equation (4). But, $p^a + 1 = 2(1 + 2^{n-2})$, then $p^a - 2^{n-1} = 1$. According to Theorem 3, the only solution, with a an even number is $n = 4$ and $a = 2$. Hence $p = 3$.

Case 2. a is odd. As mentioned earlier, we can write $p^a + 1 = 2^k b$; where b is an odd integer and $k \geq 2$. Observe that,

$$\begin{aligned} M_m + M_n &= 2p^a \\ 2^m + 2^n &= 2(p^a + 1) \\ 2^m + 2^n &= 2^{k+1} b. \end{aligned}$$

Note that, $b = 1$ iff $m = n = k$. Therefore, $p^a + 1 = 2^k$ iff $(m, n, a) = (k, k, a)$ is the only solution. But, if $p^a + 1 = 2^k$, then $2^k - p^a = 1$. By Theorem 3 $a = 1$. Thus the only solution is $(m, n, a) = (k, k, 1)$, where $M_k = p$ is a Mersenne prime.

From here on let us assume $b \geq 3$. Since $2^m + 2^n = 2^{k+1} b, b \geq 3$ we get $m = k + 1$. Since b is odd $n \geq k + 2$. Therefore,

$$\begin{aligned} 2^{k+1}(1 + 2^{n-(k+1)}) &= 2^{k+1} b \\ 1 + 2^{n-(k+1)} &= b \end{aligned}$$

Therefore, we conclude that, $b = 1 + 2^{n-(k+1)}$, which in turn implies $p^a + 1 = 2^k(1 + 2^{n-(k+1)})$ iff $(m, n, a) = (k + 1, n, a)$. □

Observation 20. *Theorem 19 tells us that the equation* (4) *has solution only for the primes of the form* $p^a + 1 = 2^k(1 + 2^{n-(k+1)})$. *For example* (4) *with* $p = 3, a = 4$ *has no solution.*

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] M. Manea, Some $a^n \pm b^n$ problems in number theory. *Mathematics Magazine* **79**, no. 2 (2006), 140–145.

[7] P. Mihăilescu, Primary Cyclotomic Units and a Proof of Catalan's Conjecture. *J. Reine Angew. Math.* **572** (2004), 167–195.

[8] L. Murata, C. Pomerance, On the largest prime factor of a Mersenne number, *Number Theory* **36** (2004), 209–218.

[9] C. Pomerance, On primitive dvivisors of Mersenne numbers, *Acta Arith.* **46** (1986), 355–367.

[10] A. Schinzel, On primitive prime factors of $a^n - b^n$, *Proc. Cambridge Philos. Soc.* **58** (1962), 555–562.

[11] C. L. Stewart, The greatest prime factor of $a^n - b^n$, *Acta Arith.* **26** (1974/75), 427–433.

[12] S. S. Wagstaff, Jr., Divisors of Mersenne numbers. *Math. Comp.* **40** (1983), 385–397.