Journal of Integer Sequences, Vol. 26 (2023),
Article 23.3.8

Jakóbczyk's Hypothesis on Mersenne Numbers and Generalizations of Skula's Theorem

Jiří Klaška
Institute of Mathematics
Faculty of Mechanical Engineering
Brno University of Technology
Technická 2
CZ – 616 69 Brno
Czech Republic
klaska@fme.vutbr.cz

Abstract

Recently Skula published an interesting article on the divisibility of Mersenne numbers $2^n - 1$ by powers of primes. His main result is closely related to Jakóbczyk's hypothesis. We generalize Skula's result for the numbers $a^n \pm 1$ where $a \in \mathbb{N}$, $a \geq 2$.

1 Introduction

In 1951, Polish priest and mathematician Franciszek Jakóbczyk [9, p. 127] published two remarkable hypotheses concerning Mersenne [23, A000225] and Fermat [23, A000215] numbers. These hypotheses can be formulated as follows.

Hypothesis 1. Every Mersenne number $M_n = 2^n - 1$ with a prime exponent n is of the form $M_n = p_1 \cdots p_k$ where $p_1, \ldots, p_k$ are distinct odd primes and $k \geq 1$.

Hypothesis 2. Every Fermat number $F_n = 2^{2^n} + 1$ with $n \in \mathbb{N} \cup \{0\}$ is of the form $F_n = p_1 \cdots p_k$ where $p_1, \ldots, p_k$ are distinct odd primes and $k \geq 1$.

Hypotheses 1 and 2 are currently among the well-known unresolved number theory problems. See, for example, [21, p. 92], [5, pp. 14–16] and, [13, p. 160]. A more detailed examination of the divisibility of Mersenne and Fermat numbers led to the discovery of a link between Jakóbczyk's hypotheses and the Wieferich primes [23, A001220]. Recall that a prime p is called Wieferich if $2^{p-1} \equiv 1 \pmod{p^2}$. Wieferich primes were first introduced in 1909 in relation to the first case of Fermat's last theorem. In the paper [27] Wieferich proved that, if p is an odd prime and $x^p + y^p + z^p = 0$ has a solution in integers x, y, z with $p \nmid xyz$, then $2^{p-1} \equiv 1 \pmod{p^2}$. Only two Wieferich primes have been discovered so far. The first Wieferich prime, 1093, was found by Meissner [17] in 1913 and the second Wieferich prime, 3511, was found by Beeger [2] in 1922. Whether the set W of all Wieferich primes is a finite or infinite set is another unanswered question. Recent calculations (March 2021) made under the PrimeGrid project [19] have shown that, if a third Wieferich prime exists, then its value must be greater than 3.15×10^{18}. In the following section, we give a summary of all known results related to Wieferich primes and Jakóbczyk's hypotheses. Details of the life and work of Franciszek Jakóbczyk (1905–1992) can be found in [18].

2 Jakóbczyk's hypotheses and Wieferich primes

In 1964, Schinzel [21, p. 102] posed the following problem: *Do there exist infinitely many natural numbers n for which the number $M_n = 2^n - 1$ is not divisible by any square of natural number > 1?* A partial answer to Schinzel's question is a result proved by Rotkiewicz [20, p. 79].

Theorem 3. (Rotkiewicz, 1965) *If there are infinitely many square-free Mersenne numbers, then there are infinitely many primes p satisfying $2^{p-1} \not\equiv 1 \pmod{p^2}$.*

In 1967, Warren and Bray [24, p. 563] proved the following implications:

Theorem 4. (Warren and Bray, 1967) *Let $n \in \mathbb{N}$, $n \neq 1$ and let p, q be odd primes. Then*

(i) *If $p \mid M_q$, then $2^{(p-1)/2} \equiv 1 \pmod{M_q}$.*

(ii) *If $p \mid F_n$, then $2^{(p-1)/2} \equiv 1 \pmod{F_n}$.*

The below corollary can be obtained easily from Theorem 4.

Corollary 5. *Let $n \in \mathbb{N}$ and let p, q be odd primes. Then* (i) *and* (ii) *hold.*

(i) *If $p^2 \mid M_q$, then $2^{p-1} \equiv 1 \pmod{p^2}$.*

(ii) *If $p^2 \mid F_n$, then $2^{p-1} \equiv 1 \pmod{p^2}$.*

The results presented by Warren and Bray can be extended as follows.

Theorem 6. *Let $n \in \mathbb{N}$ and let p, q be odd primes. Then* (i) *and* (ii) *hold.*

(i) *If $p \mid M_q$, then $p^2 \mid M_q$ if and only if $2^{p-1} \equiv 1 \pmod{p^2}$.*

(ii) *If $p \mid F_n$, then $p^2 \mid F_n$ if and only if $2^{p-1} \equiv 1 \pmod{p^2}$.*

See [13, p. 68] and, [13, p. 217]. Theorem 6 provides the basic link between Jakóbczyk's hypotheses and Wieferich primes. Finally, part (i) of Theorem 6 was generalized by Skula [22] in 2019. Before formulating Skula's result, it may be appropriate to recall some concepts and definitions. Let $k \in \mathbb{N}$ and let p be a Wieferich prime. By Definition 1.4 in the paper [22], p is called a Wieferich prime of order k if $q(2, p^k) \equiv 0 \pmod{p^k}$ or, equivalently, $2^{p^{k-1}(p-1)} \equiv 1 \pmod{p^{2k}}$. Here, $q(2, p^k)$ means the Euler quotient of p^k with base 2. See [1, Definition 1.2]. Hence, a prime p is Wieferich if and only if p is a Wieferich prime of order 1. Furthermore, note that, by [1, Definition 1.3], p is a Wieferich prime of order k if and only if p^k is a Wieferich number with base 2. See also [23, A077816]. Finally, let $a, m \in \mathbb{N}$, $m \geq 2$ and let $\gcd(a, m) = 1$. The smallest positive integer h for which $a^h \equiv 1 \pmod{m}$ is called the multiplicative order of a modulo m, which we write as $h = \operatorname{ord}_m(a)$. See [15, p. 55] or [13, p. 17]. It is clear from Euler's theorem [1, p. 55] that $\operatorname{ord}_{p^k}(2)$ exists for every odd prime p and $k \in \mathbb{N}$.

Now we can formulate the main result proved in [22].

Theorem 7. (Skula, 2019) *Let $k \in \mathbb{N}$ and let p, q be odd primes. If $p^k \mid M_q$, then the following statements* (i), (ii) *and* (iii) *are equivalent:*

(i) $p^{k+1} \mid M_q$.

(ii) *p is a Wieferich prime of order k.*

(iii) $\operatorname{ord}_{p^{k+1}}(2) = q$.

For an alternative proof of Theorem 7 see [12]. We conclude this section by recalling some known properties of $\operatorname{ord}_m(a)$ needed for proving our results.

Proposition 8. *Let $a, m \in \mathbb{N}$, $m \geq 2$ and let $\gcd(a, m) = 1$. Then* (i) – (vii) *hold.*

(i) *Let $k \in \mathbb{N}$. Then $a^k \equiv 1 \pmod{m}$ if and only if $\operatorname{ord}_m(a) \mid k$.*

(ii) $\operatorname{ord}_m(a) \mid \varphi(m)$. *Consequently, if p is an odd prime, then $\operatorname{ord}_p(2) \mid p - 1$. Here, φ means the Euler function.*

(iii) *Let $m = p_1^{k_1} \cdots p_s^{k_s}$ be a prime factorization of m. Then*

$$\operatorname{ord}_m(a) = \operatorname{lcm}(\operatorname{ord}_{p_1^{k_1}}(a), \ldots, \operatorname{ord}_{p_s^{k_s}}(a)).$$

(iv) *Let $a, k, s \in \mathbb{N}$ and let p be an odd prime satisfying $p \nmid a$. Further, let $\operatorname{ord}_p(a) = h$ and let $p^s \parallel a^h - 1$. Then*

$$\operatorname{ord}_{p^k}(a) = \begin{cases} h, & \text{for } k \leq s; \\ p^{k-s}h, & \text{for } k > s. \end{cases}$$

Here, $p^s \parallel a^h - 1$ means that $p^s \mid a^h - 1$ but $p^{s+1} \nmid a^h - 1$.

(v) *Let* $a, k \in \mathbb{N}$ *and let* p *be an odd prime satisfying* $p \nmid a$. *If* $\operatorname{ord}_{p^k}(a) = h$, *then* $\operatorname{ord}_{p^{k+1}}(a) \in \{h, ph\}$. *Consequently,* $\operatorname{ord}_{p^k}(a) \mid \operatorname{ord}_{p^{k+1}}(a)$.

(vi) *Let* $k \in \mathbb{N}$, p *be an odd prime and let* $p \nmid a$. *Then* $\operatorname{ord}_{p^{k+1}}(a) = p^s \operatorname{ord}_p(a)$ *for some* $s \in \{0, \ldots, k\}$.

(vii) *Let* $k, s \in \mathbb{N}$, p *be an odd prime and let* $p \nmid a$. *If* $\operatorname{ord}_p(a) = \cdots = \operatorname{ord}_{p^k}(a) \neq \operatorname{ord}_{p^{k+1}}(a)$, *then* $\operatorname{ord}_{p^{k+s}}(a) = p^s \operatorname{ord}_p(a)$.

The proof of (i) and (ii) can be found in [16, p. 43]. For (iii) see [4, p. 30]. Part (iv) is Theorem 4.4 proved by LeVeque in [15, pp. 80–81]. See also [16, pp. 52–53]. Finally, (v), (vi) and (vii) immediately follow from (iv).

3 Some arithmetic properties of the numbers $a^n \pm 1$

In this section, we will study in more detail the arithmetic properties of the numbers $M_n(a) = a^n - 1$ and $L_n(a) = a^n + 1$ where $a \in \mathbb{N}$, $a \geq 2$, $n \in \mathbb{N} \cup \{0\}$. First, we can observe that the sequences $(M_n(a))_{n=0}^{\infty}$ and $(L_n(a))_{n=0}^{\infty}$ are determined by the same linear second-order recurrence formula

$$H_{n+2} = (a+1)H_{n+1} - aH_n, \tag{1}$$

with suitable initial conditions $H_0, H_1 \in \mathbb{N} \cup \{0\}$. To see this, consider the characteristic equation (1). We have $x^2 - (a+1)x + a = (x-1)(x-a) = 0$. Hence, it follows that Binet's formula for H_n has the form $H_n = c_1 + c_2 a^n$ where $H_0 = c_1 + c_2$ and $H_1 = c_1 + ac_2$. After short calculation, we obtain

$$H_n = \frac{aH_0 - H_1}{a-1} + \frac{H_1 - H_0}{a-1}\, a^n. \tag{2}$$

If $[H_0, H_1] = [0, a-1]$, then $H_n = M_n(a)$ by (2). If $[H_0, H_1] = [2, a+1]$, then $H_n = L_n(a)$. Let $m \in \mathbb{N}$, $m \geq 2$ and let $\gcd(a, m) = 1$. We define

$$\begin{aligned}
M(a,m) &= \min\{n \in \mathbb{N} : [M_n(a), M_{n+1}(a)] \equiv [0, a-1] \pmod{m}\},\\
L(a,m) &= \min\{n \in \mathbb{N} : [L_n(a), L_{n+1}(a)] \equiv [2, a+1] \pmod{m}\},\\
\mu(a,m) &= \min\{n \in \mathbb{N} : M_n(a) \equiv 0 \pmod{m}\},\\
\lambda(a,m) &= \min\{n \in \mathbb{N} : L_n(a) \equiv 0 \pmod{m}\}.
\end{aligned}$$

Following the customary notation of the theory of linear recurrences, we call the numbers $M(a,m)$ and $L(a,m)$ primitive periods of the sequences

$$(M_n(a) \bmod m)_{n=0}^{\infty} \text{ and } (L_n(a) \bmod m)_{n=0}^{\infty}.$$

The numbers $\mu(a,m)$ and $\lambda(a,m)$ will then be called the rank of appearance of m in $(M_n(a))_{n=0}^{\infty}$ and $(L_n(a))_{n=0}^{\infty}$ respectively. In the following Theorem 9, the basic properties of the numbers $M(a,m)$, $L(a,m)$, $\mu(a,m)$ and $\lambda(a,m)$ will be given.

Theorem 9. *Let $a, m \in \mathbb{N}$, $a, m \geq 2$ and let $\gcd(a, m) = 1$. Then*

(A) *The numbers $M(a, m)$, $L(a, m)$ and $\mu(a, m)$ exist and we have*

$$M(a, m) = L(a, m) = \mu(a, m) = \operatorname{ord}_m(a). \tag{3}$$

(B) *Let $m \neq 2$ and let $\operatorname{ord}_m(a)$ be odd. Then $\lambda(a, m)$ does not exist.*
Let $m = 2$. Then $\lambda(a, 2) = 1$.

(C) *Let $m \neq 2$ and let $\operatorname{ord}_m(a) = 2t$ for some $t \in \mathbb{N}$. If $\lambda(a, m)$ exists, then*

$$\lambda(a, m) = \frac{\operatorname{ord}_m(a)}{2} = t. \tag{4}$$

(D) *Let $k, t \in \mathbb{N}$, p be an odd prime and let $p \nmid a$. Then*

$$\operatorname{ord}_{p^k}(a) = 2t \textit{ if and only if } \lambda(a, p^k) = t.$$

Proof. We prove (A). First, observe that $\operatorname{ord}_m(a)$ exists. Next, it is clear that $\mu(a, m) = \min\{n \in \mathbb{N} : a^n \equiv 1 \pmod{m}\} = \operatorname{ord}_m(a)$, which means that $\mu(a, m)$ exists. Let $r = \mu(a, m)$. Applying $\gcd(a, m) = 1$, we obtain $a^r - 1 \equiv 0 \pmod{m}$ if and only if $a^{r+1} - 1 \equiv a - 1 \pmod{m}$. Hence, $M(a, m) = r$ and, thus, $M(a, m) = \mu(a, m) = \operatorname{ord}_m(a)$. Finally, $[a^r - 1, a^{r+1} - 1] \equiv [0, a - 1] \pmod{m}$ if and only if $[a^r + 1, a^{r+1} + 1] \equiv [2, a + 1] \pmod{m}$. Hence, $M(a, m) = L(a, m)$. This proves (3).

We prove (B). Let $m \neq 2$ and suppose that $\lambda(a, m) = s$ for some $s \in \mathbb{N}$. Then $a^s \equiv -1 \pmod{m}$ and, $a^{2s} \equiv 1 \pmod{m}$ follows. Hence, $\operatorname{ord}_m(a) \mid 2s$. Since $\operatorname{ord}_m(a)$ is odd, there exists a $t \in \mathbb{N} \cup \{0\}$ satisfying $\operatorname{ord}_m(a) = 2t + 1$. This means that $2t + 1 \mid 2s$. Thus, there exists an $u \in \mathbb{N}$, $u \neq 1$ such that $2s = u(2t + 1)$. Hence, we see that $u = 2v$ for some $v \in \mathbb{N}$ and, thus, $s = v(2t + 1)$. Therefore, $a^s = (a^{2t+1})^v \equiv 1^v \equiv 1 \pmod{m}$. Since $a^s \equiv -1 \pmod{m}$, we have $2 \equiv 0 \pmod{m}$. Hence, $m = 2$, a contradiction.

Let $m = 2$. Then, it follows from $\gcd(a, 2) = 1$ that a is odd and, thus, $2 \mid a^n + 1$ for every $n \in \mathbb{N} \cup \{0\}$. Hence, $\lambda(a, m) = 1$. This proves (B).

We prove (C). Assume that $\lambda(a, m)$ exists and that $\lambda(a, m) = s$ for some $s \in \mathbb{N}$. Then $a^s \equiv -1 \pmod{m}$ and $a^{2s} \equiv 1 \pmod{m}$ follows. Hence, $\operatorname{ord}_m(a) \mid 2s$. Since, $\operatorname{ord}_m(a) = 2t$ we get $t \mid s$. Suppose that $t < s$. Then there is a $u \in \mathbb{N}$, $u \neq 1$ such that $s = tu$. First, suppose that u be even. Then we have $u = 2v$ for some $v \in \mathbb{N}$. Hence, $a^s = (a^{2t})^v \equiv 1^v \equiv 1 \pmod{m}$. On the other hand, $a^s \equiv -1 \pmod{m}$. Hence, $2 \equiv 0 \pmod{m}$. Since $m \neq 2$, we have a contradiction. Next, suppose that u be odd. Then $u = 2v + 1$ for some $v \in \mathbb{N} \cup \{0\}$. Hence, $a^s = a^{t(2v+1)} = (a^{2t})^v a^t \equiv a^t \pmod{m}$. This, together with $a^s \equiv -1 \pmod{m}$, yields $a^t \equiv -1 \pmod{m}$. Since $s = \min\{n \in \mathbb{N} : a^n \equiv -1 \pmod{m}\}$, we get $t \geq s$, which is a contradiction with $t < s$. Hence, $s = t$ and (4) follows.

We prove (D). (i) First, assume that $\operatorname{ord}_{p^k}(a) = 2t$. Therefore,

$$a^{2t} - 1 = (a^t - 1)(a^t + 1) \equiv 0 \pmod{p^k}. \tag{5}$$

Let $k > 1$. Suppose that $a^t - 1 \equiv 0 \pmod{p}$ and $a^t + 1 \equiv 0 \pmod{p}$. Then $2 \equiv 0 \pmod{p}$. As $p \neq 2$, we get a contradiction. Consequently, we have either $a^t - 1 \equiv 0 \pmod{p^k}$ or $a^t + 1 \equiv 0 \pmod{p^k}$. Since the case $a^t - 1 \equiv 0 \pmod{p^k}$ leads to a contradiction with $\operatorname{ord}_{p^k}(a) = 2t$, we have $a^t + 1 \equiv 0 \pmod{p^k}$. Similarly, if $k = 1$, then (5) together with $\operatorname{ord}_p(a) = 2t$ yields $a^t + 1 \equiv 0 \pmod{p}$. Hence, $t \in \{n \in \mathbb{N} : a^n + 1 \equiv 0 \pmod{p^k}\}$ for every $k \in \mathbb{N}$. This means that $\lambda(a, p^k)$ exists. Applying part (C) of Theorem 9, we now obtain $\lambda(a, p^k) = t$.

(ii) Conversely, assume that $\lambda(a, p^k)$ exists and that $\lambda(a, p^k) = t$. Then it follows from part (B) of Theorem 9 that $\operatorname{ord}_{p^k}(a)$ is even. Therefore, there is an $s \in \mathbb{N}$ such that $\operatorname{ord}_{p^k}(a) = 2s$. Hence, $a^{2s} \equiv 1 \pmod{p^k}$, which yields $(a^s - 1)(a^s + 1) \equiv 0 \pmod{p^k}$. Using the same reasoning as in (i), we conclude that $a^s \equiv -1 \pmod{p^k}$. Suppose that $s \neq t$. Since $\lambda(a, p^k) = t$, we have $s > t$. On the other hand, from $a^t \equiv -1 \pmod{p^k}$, we get $a^{2t} \equiv 1 \pmod{p^k}$, which means that $\operatorname{ord}_{p^k}(a) \mid 2t$. Since $\operatorname{ord}_{p^k}(a) = 2s$, we have $s \mid t$, which is a contradiction with $s > t$. Hence, $s = t$. This proves (D). $\square$

In the remaining part of this section, we will study the properties of the numbers $\lambda(a, m)$ in more detail.

Theorem 10. *Let $a, m \in \mathbb{N}$, $a, m \geq 2$, $2 \nmid m$ and let $\gcd(a, m) = 1$. Further, let $\operatorname{ord}_m(a) = 2t$ for some $t \in \mathbb{N}$ and let $m = p_1^{k_1} \cdots p_s^{k_s}$ be a prime factorization of m. Then $\lambda(a, m)$ exists if and only if* (i) *and* (ii) *hold.*

(i) *$\lambda(a, p_i^{k_i})$ exists for $i \in \{1, \ldots, s\}$.*

(ii) *For $i \in \{1, \ldots, s\}$, there is an odd $w_i \in \mathbb{N}$ satisfying $t = \lambda(a, p_i^{k_i}) w_i$.*

In addition, if $\lambda(a, m)$ exists, then

$$\lambda(a, m) = \operatorname{lcm}(\lambda(a, p_1^{k_1}), \ldots, \lambda(a, p_s^{k_s})) = t. \tag{6}$$

Proof. First, assume that $\lambda(a, m)$ exists. Then it follows that $\lambda(a, p_i^{k_i})$ exists for every $i \in \{1, \ldots, s\}$. Let $t_i = \lambda(a, p_i^{k_i})$. Applying part (D) of Theorem 9, we obtain $\operatorname{ord}_{p_i^{k_i}}(a) = 2t_i$. Next, using part (iii) of Proposition 8 , we get

$$2t = \operatorname{ord}_m(a) = \operatorname{lcm}(\operatorname{ord}_{p_1^{k_1}}(a), \ldots, \operatorname{ord}_{p_s^{k_s}}(a)) = 2 \operatorname{lcm}(t_1, \ldots, t_s). \tag{7}$$

Hence, $t_i \mid t$ for $i \in \{1, \ldots, s\}$. This means that $t = t_i w_i$ for some $w_i \in \mathbb{N}$.

Suppose that there is an $j \in \{1, \ldots, s\}$ such that $2 \mid w_j$. Using $a^{t_j} \equiv -1 \pmod{p_j^{k_j}}$, we find $a^t = (a^{t_j})^{w_j} \equiv (-1)^{w_j} \equiv 1 \pmod{p_j^{k_j}}$. Suppose now that $p_j^{k_j} \mid a^t + 1$. Then $a^t \equiv -1 \pmod{p_j^{k_j}}$. This, together with $a^t \equiv 1 \pmod{p_j^{k_j}}$, yields $2 \equiv 0 \pmod{p_j^{k_j}}$. Since p_j is an odd prime, we have a contradiction. Hence $p_j^{k_j} \nmid a^t + 1$, which implies $m \nmid a^t + 1$. Therefore, $\lambda(a, m) \neq t$. Since $\operatorname{ord}_m(a) = 2t$, by part (C) of Theorem 9, we conclude that $\lambda(a, m)$ does not exist, which is a contradiction.

For $i \in \{1, \dots, s\}$, let w_i be odd. Then $a^t = (a^{t_i})^{w_i} \equiv (-1)^{w_i} \equiv -1 \pmod{p_i^{k_i}}$. Hence, $p_i^{k_i} \mid a^t + 1$. If w_i is odd for $i \in \{1, \dots, s\}$, then $m = p_1^{k_1} \cdots p_s^{k_s} \mid a^t + 1$ and $t \in \{n \in \mathbb{N} : a^n + 1 \equiv 0 \pmod{m}\}$. This means that $\lambda(a, m)$ exists, and, using part (C) of Theorem 9, we get $\lambda(a, m) = t$. This, together with (7), yields (6).

Conversely, assume that (i) and (ii) hold. If $t_i = \lambda(a, p_i^{k_i})$, we have $a^{t_i} \equiv -1 \pmod{p_i^{k_i}}$. Now we can find $a^t = (a^{t_i})^{w_i} \equiv (-1)^{w_i} \equiv -1 \pmod{p_i^{k_i}}$. We now see that $p_i^{k_i} \mid a^t + 1$ for every $i \in \{1, \dots, s\}$ and, thus, $m = p_1^{k_1} \cdots p_s^{k_s} \mid a^t + 1$. Hence, $t \in \{n \in \mathbb{N} : a^n + 1 \equiv 0 \pmod{m}\}$, which means that $\lambda(a, m)$ exists. By part (C) of Theorem 9, we obtain $\lambda(a, m) = t$. The proof is complete. □

Remark 11. In [15, p. 57], LeVeque published the following Problem 19.

$$\textit{Show that, if } m > 1 \textit{ is odd and } \operatorname{ord}_m(a) = 2t, \textit{ then } a^t \equiv -1 \pmod{m}. \tag{8}$$

We now prove, using a counterexample, that LeVeque's implication is not true. Let $m = 91 = 7 \cdot 13$ and let $a = 5$. Then $\operatorname{ord}_{91}(5) = 12$, which means, by (8), that $t = 6$. Hence, $5^6 \equiv 64 \not\equiv -1 \pmod{91}$. It is evident that LeVeque's erroneous claim is closely related to the existence of the numbers $\lambda(a, m)$. By part (iii) of Proposition 8, we have

$$\operatorname{ord}_{91}(5) = \operatorname{lcm}(\operatorname{ord}_7(5), \operatorname{ord}_{13}(5)) = \operatorname{lcm}(6, 4) = 12.$$

Hence, using part (D) of Theorem 9, we obtain $\lambda(5, 7) = \operatorname{ord}_7(5)/2 = 3$ and $\lambda(5, 13) = \operatorname{ord}_{13}(5)/2 = 2$. Next, applying Theorem 10, we get $w_1 = 6/\lambda(5, 7) = 2$ and $w_2 = 6/\lambda(5, 13) = 3$. Because w_1 is not odd, $\lambda(5, 91)$ does not exist. In other words, $91 \nmid L_6(5) = 5^6 + 1 = 2 \cdot 13 \cdot 601$.

Let $a \in \mathbb{N}$, $a > 1$ and let a be odd. Then $2 \mid a + 1$ and thus $\{k \in \mathbb{N} : 2^k \mid a + 1\} \neq \emptyset$. Put $\nu(a) = \max\{k \in \mathbb{N} : 2^k \mid a + 1\}$. In the following Lemma 12, we show that there is a close connection between the numbers $\nu(a)$ and $\lambda(a, 2^k)$.

Lemma 12. *Let $a, k, n \in \mathbb{N}$, $a > 1$ and let a be odd. Then*

(A) *If $2 \mid n$, then $2 \parallel a^n + 1$.*

(B) *If $2 \nmid n$, then $2^{\nu(a)} \parallel a^n + 1$.*

(C) *$\lambda(a, 2^k)$ exist if and only if $k \leq \nu(a)$. In this case, $\lambda(a, 2^k) = 1$.*

Proof. We prove (A). Let $2 \mid n$. Since $a > 1$ is odd, there is an $\alpha \in \mathbb{N}$ such that $a = 2\alpha + 1$. Hence, using the assumption $2 \mid n$ and the binomial theorem, we get

$$a^n + 1 = (2\alpha + 1)^n + 1 \equiv 2 \pmod{4}. \tag{9}$$

By (9), $2 \parallel a^n + 1$ for an even n.

We prove (B). Let $2 \nmid n$. Then $a^n + 1 = (a + 1)(a^{n-1} - a^{n-2} + \cdots - a + 1)$. Since a is odd, we have $2 \nmid (a^{n-1} - a^{n-2} + \cdots - a + 1)$. Hence, $2^s \mid a^n + 1$ if and only if $2^s \mid a + 1$ for every $s \in \mathbb{N}$. This means that $2^{\nu(a)} \parallel a^n + 1$ for any odd n.

Combining (A) and (B), (C) follows immediately. □

Lemma 12 will be useful in proving Theorem 13.

Theorem 13. *Let $a, M \in \mathbb{N}$, $a, M \geq 2$, $\gcd(a, M) = 1$ and let $2 \nmid a$, $2 \mid M$. Further, let $M = 2^{\alpha} p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ be a prime factorization of M and let $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Then* (A) *and* (B) *hold.*

(A) *Let $\alpha = 1$. Then $\lambda(a, M)$ exists if and only if $\lambda(a, m)$ exists. Moreover, if $\lambda(a, M)$ exists, then $\lambda(a, M) = \lambda(a, m)$.*

(B) *Let $\alpha > 1$. Then $\lambda(a, M)$ exists if and only if $\lambda(a, 2^{\alpha})$ and $\lambda(a, m)$ exist and, $2 \nmid \lambda(a, m)$. Moreover, if $\lambda(a, M)$ exists, then $\lambda(a, M) = \lambda(a, m)$.*

Proof. We prove (A). Assume that $\lambda(a, M)$ exists and that $\lambda(a, M) = U$. Then $M \mid a^U + 1$. Since $M = 2m$ and $\gcd(2, m) = 1$, we get $m \mid a^U + 1$, which implies that $\lambda(a, m)$ exists and that $\lambda(a, m) \leq U = \lambda(a, M)$.

Conversely, assume that $\lambda(a, m)$ exists and that $\lambda(a, m) = u$. Then $m \mid a^u + 1$. Since a is odd, we have $2 \mid a^n + 1$ for every $n \in \mathbb{N}$. Hence and from $\gcd(2, m) = 1$, we obtain $M = 2m \mid a^u + 1$. This means that $\lambda(a, M)$ exists and that $\lambda(a, M) \leq u = \lambda(a, m)$. This proves (A).

We prove (B). Let $\alpha > 1$. First, assume that $\lambda(a, M)$ exists and that $\lambda(a, M) = U$. Then $M = 2^{\alpha} m \mid a^U + 1$. Hence and from $\gcd(2^{\alpha}, m) = 1$, we obtain $2^{\alpha} \mid a^U + 1$ and $m \mid a^U + 1$. This means that $\lambda(a, 2^{\alpha})$ and $\lambda(a, m)$ exist. Next, by part (C) of Lemma 12, we have $\alpha \leq \nu(a)$ and, from $m \mid a^U + 1$, we get $\lambda(a, m) \leq U = \lambda(a, M)$.

Let $\lambda(a, m) = u$. Suppose that $2 \mid u$. Then, by part (A) of Lemma 12, we have $2 \parallel a^u + 1$. This means that $2^{\alpha} \nmid a^u + 1$. Hence, $M = 2^{\alpha} m \nmid a^u + 1$ and, thus, $\lambda(a, M) \neq u = \lambda(a, m)$. This, together with $u = \lambda(a, m) \leq U$, yields $u < U$. Hence, $U = u + k$ for some $k \in \mathbb{N}$. From $2^{\alpha} m \mid a^{u+k} + 1$ and $\gcd(2^{\alpha}, m) = 1$, we can deduce that $m \mid a^{u+k} + 1$, or equivalently, $a^u a^k \equiv -1 \pmod{m}$. Using $a^u \equiv -1 \pmod{m}$, we now obtain $a^k \equiv 1 \pmod{m}$. Hence, $\operatorname{ord}_m(a) \mid k$. Suppose that $\operatorname{ord}_m(a)$ is odd. Then, by part (B) of Theorem 9, $\lambda(a, m)$ does not exist, which is a contradiction. Hence, $2 \mid \operatorname{ord}_m(a)$ and, $2 \mid k$ follows. Therefore, $2 \mid u + k = U$. By part (A) of Lemma 12, we now obtain $2 \parallel a^U + 1$. Hence and from $\alpha > 1$, we get $2^{\alpha} \nmid a^U + 1$, which means $2^{\alpha} m = M \nmid a^U + 1$, a contradiction.

Let $2 \nmid u$. Then, by part (B) of Lemma 12, we have $2^{\nu(a)} \mid a^u + 1$. As $\alpha \leq \nu(a)$, we also have $2^{\alpha} \mid a^u + 1$. Hence and from $m \mid a^u + 1$, we obtain $2^{\alpha} m = M \mid a^u + 1$, and $U = \lambda(a, M) \leq u$ follows. This, together with $u = \lambda(a, m) \leq U$, yields $\lambda(a, M) = \lambda(a, m)$.

Conversely, assume that $\lambda(a, 2^{\alpha})$ and $\lambda(a, m)$ exist and that $\lambda(a, m)$ is odd. First, observe that, if $\alpha > 1$ and $\lambda(a, 2^{\alpha})$ exists, then, by part (C) of Lemma 12, we have $\alpha \leq \nu(a)$ and, by part (B) of Lemma 12, we have $2^{\alpha} \mid a^n + 1$ for any odd $n \in \mathbb{N}$. Let $\lambda(a, m) = u$. Then $m \mid a^u + 1$. Since u is odd, we get $2^{\alpha} \mid a^u + 1$. Hence and from $\gcd(2^{\alpha}, m) = 1$, we now obtain $M = 2^{\alpha} m \mid a^u + 1$, which means that $\lambda(a, M)$ exists and that $\lambda(a, M) \leq u$. Put $\lambda(a, M) = U$. Then we can write $M = 2^{\alpha} m \mid a^U + 1$. Since $\gcd(2^{\alpha}, m) = 1$, we get $m \mid a^U + 1$, which yields $\lambda(a, m) \leq U$. Finally, combining $U = \lambda(a, M) \leq u$ with $u = \lambda(a, m) \leq U$, we get $\lambda(a, M) = \lambda(a, m)$. This proves (B). $\square$

Remark 14. Let us note for completeness sake that the case of $\lambda(a,m)$, where $2 \mid a$ and $2 \mid m$, is trivial. Since $a^n + 1$ is odd for all $n \in \mathbb{N}$, $\lambda(a,m)$ does not exist.

Let us conclude this section with an illustrative example.

Example 15. Let $a = 11$, $m = 1769 = 29 \cdot 61$ and let $M = 7076 = 2^2 m$. First, observe that $\mathrm{ord}_{29}(11) = 28$, $\mathrm{ord}_{61}(11) = 4$ and, $\mathrm{ord}_{1769}(11) = 28$. Applying part (D) of Theorem 9, we obtain $\lambda(11,29) = \mathrm{ord}_{29}(11)/2 = 14$ and, $\lambda(11,61) = \mathrm{ord}_{61}(11)/2 = 2$. Next, using Theorem 10, we get $t = \mathrm{ord}_{1769}(11)/2 = 14$, $w_1 = 14/\lambda(11,29) = 1$ and, $w_2 = 14/\lambda(11,61) = 7$. Since w_1 and w_2 are odd numbers, $\lambda(11,1769)$ exists and, by (6), we have $\lambda(11,1769) = 14$. Further, observe that $2^2 \mid a+1 = 12$. Hence, by Lemma 12, $\lambda(11,2^2)$ exists and $\lambda(11,2^2) = 1$. Because $\lambda(11,1769)$ is an even number, by Theorem 13, we conclude that $\lambda(11,7076)$ does not exist.

4 Mersenne numbers with base a

In this section, we generalize Skula's result presented in Theorem 7. Let $a, k \in \mathbb{N}$, $a \geq 2$ and let p be a prime satisfying $p \nmid a$. We will call p a *Wieferich prime of order k with base a* if p^k is a Wieferich number with base a. That is, p is a Wieferich prime of order k with base a if and only if

$$q(a,p^k) \equiv 0 \pmod{p^k}, \text{ or equivalently, } a^{p^{k-1}(p-1)} \equiv 1 \pmod{p^{2k}}.$$

See [1, Definition 1.3].

Proposition 16. *Let $a, k \in \mathbb{N}$, $a \geq 2$, p be a prime and let $p \nmid a$. Then*

(A) $a^{p^{k-1}(p-1)} \equiv 1 \pmod{p^{2k}}$ *if and only if* $a^{p-1} \equiv 1 \pmod{p^{k+1}}$.

(B) $a^{p-1} \equiv 1 \pmod{p^{k+1}}$ *if and only if* $\mathrm{ord}_{p^{k+1}}(a) = \mathrm{ord}_p(a)$.

(C) *p is a Wieferich prime of order k with base a if and only if* $\mathrm{ord}_{p^{k+1}}(a) = \mathrm{ord}_p(a)$.

Proof. First, we prove (A). Assume that $a^{p^{k-1}(p-1)} \equiv 1 \pmod{p^{2k}}$. Then, by part (i) of Proposition 8,

$$\mathrm{ord}_{p^{2k}}(a) \mid p^{k-1}(p-1). \tag{10}$$

Suppose that $a^{p-1} \not\equiv 1 \pmod{p^{k+1}}$. Then $\mathrm{ord}_{p^{k+1}}(a) \neq \mathrm{ord}_p(a)$ and, by part (vi) of Proposition 8, there exists an $r \in \{1,\ldots,k\}$ such that $\mathrm{ord}_{p^{k+1}}(a) = p^r \mathrm{ord}_p(a)$. Hence, by part (vii) of Proposition 8, we have

$$\mathrm{ord}_{p^{2k}}(a) = p^k \mathrm{ord}_{p^{k+1}}(a) = p^{k+r} \mathrm{ord}_p(a). \tag{11}$$

Since $r \in \{1,\ldots,k\}$ and $\mathrm{ord}_p(a) \mid p-1$, we get a contradiction by relations (10) and (11).

Conversely, assume that $a^{p-1} \equiv 1 \pmod{p^{k+1}}$. Then $\mathrm{ord}_{p^{k+1}}(a) \mid p-1$, which yields $\mathrm{ord}_p(a) = \mathrm{ord}_{p^{k+1}}(a)$. Hence, by part (vi) of Proposition 8, there exists an $s \in \{0, \dots, k-1\}$ such that $\mathrm{ord}_{p^{2k}}(a) = p^s \,\mathrm{ord}_{p^{k+1}}(a) = p^s \,\mathrm{ord}_p(a)$. Since $s \leq k-1$, we get $\mathrm{ord}_{p^{2k}}(a) \mid p^{k-1} \,\mathrm{ord}_p(a)$, which, together with $\mathrm{ord}_p(a) \mid p-1$, yields $\mathrm{ord}_{p^{2k}}(a) \mid p^{k-1}(p-1)$. Hence, $a^{p^{k-1}(p-1)} \equiv 1 \pmod{p^{2k}}$. This proves (A).

We prove (B). Let $a^{p-1} \equiv 1 \pmod{p^{k+1}}$. Then $\mathrm{ord}_{p^{k+1}}(a) \mid p-1$. Using part (vi) of Proposition 8, we obtain $\mathrm{ord}_{p^{k+1}}(a) = p^t \,\mathrm{ord}_p(a)$ for some $t \in \{0, \dots, k\}$. If $t \neq 0$, then $p^t \,\mathrm{ord}_p(a) \mid p-1$, which is a contradiction. Hence, $\mathrm{ord}_{p^{k+1}}(a) = \mathrm{ord}_p(a)$.

Conversely, let $\mathrm{ord}_{p^{k+1}}(a) = \mathrm{ord}_p(a) = u$. Then $u \mid p-1$, which means that there exists a $v \in \mathbb{N}$ such that $p-1 = uv$. Since $a^u \equiv 1 \pmod{p^{k+1}}$, we have $a^{p-1} = a^{uv} = (a^u)^v \equiv 1 \pmod{p^{k+1}}$ as required.

Finally, combining (A) and (B), we obtain (C). The proof is complete.

□

Remark 17. The conclusion (A) in Proposition 16 also holds if $p \mid a$. In this case, of course, we have $a^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{2k}}$, $a^{p-1} \not\equiv 1 \pmod{p^{k+1}}$ for every $a, k \in \mathbb{N}$, $a \geq 2$. The conclusion (B) in Proposition 16 also holds for $k = 0$.

Now we can to prove Theorem 18.

Theorem 18. *Let $a, k \in \mathbb{N}$, $a \geq 2$, p, q be odd primes and let $p \nmid a$, $p \nmid a-1$. If $p^k \mid M_q(a)$, then the following statements are equivalent:*

(A) *$p^{k+1} \mid M_q(a)$.*

(B) *p is a Wieferich prime with base a of order k.*

(C) *$\mathrm{ord}_{p^{k+1}}(a) = q$.*

Proof. First, we show that (A) implies (B). Let $p^{k+1} \mid M_q(a)$. Then $a^q \equiv 1 \pmod{p^{k+1}}$, which yields $\mathrm{ord}_{p^{k+1}}(a) \mid q$. Since q is a prime, we have $\mathrm{ord}_{p^{k+1}}(a) \in \{1, q\}$. If $\mathrm{ord}_{p^{k+1}}(a) = 1$, then $\mathrm{ord}_p(a) = 1$, which means $p \mid a-1$, a contradiction. Hence, $\mathrm{ord}_{p^{k+1}}(a) = q$. Suppose that $p = q$. Then $\mathrm{ord}_{p^{k+1}}(a) = p$ and, using part (vi) of Proposition 8, we get $\mathrm{ord}_p(a) = 1$. Hence, $p \mid a-1$, a contradiction. Let $p \neq q$. Then, by part(vi) of Proposition 8, $\mathrm{ord}_{p^{k+1}}(a) = p^s \,\mathrm{ord}_p(a)$ for some $s \in \{0, \dots, k\}$. Since $p \neq q$, we get $s = 0$ and $\mathrm{ord}_{p^{k+1}}(a) = \mathrm{ord}_p(a) = q$. This means, by Proposition 16, that p is a Wieferich prime of order k with base a.

Next, we show that (B) implies (C). Assume that p is a Wieferich prime of order k with base a. Then, by Proposition 16, we have $2^{p-1} \equiv 1 \pmod{p^{k+1}}$ and, using part (i) of Proposition 8, we get $\mathrm{ord}_{p^{k+1}}(a) \mid p-1$. Next, from the basic assumption $p^k \mid M_q(a)$, we obtain $a^q \equiv 1 \pmod{p^k}$ and $\mathrm{ord}_{p^k}(a) \mid q$ follows. Hence, $\mathrm{ord}_{p^k}(a) \in \{1, q\}$. Suppose that $\mathrm{ord}_{p^k}(a) = 1$. Then $p^k \mid a-1$, which yields $p \mid a-1$, a contradiction. Hence, $\mathrm{ord}_{p^k}(a) = q$. Now, by part (v) of Proposition 8, we have $\mathrm{ord}_{p^{k+1}}(a) = pq$ or $\mathrm{ord}_{p^{k+1}}(a) = q$. Suppose that $\mathrm{ord}_{p^{k+1}}(a) = pq$. Since $\mathrm{ord}_{p^{k+1}}(a) \mid p-1$, we get $pq \mid p-1$, a contradiction. Hence, (C).

Finally, we show that (C) implies (A). If $\mathrm{ord}_{p^{k+1}}(a) = q$, then $a^q \equiv 1 \pmod{p^{k+1}}$, which yields $p^{k+1} \mid M_q(a)$. The proof is complete. □

Another generalization of Theorem 7 provide Theorem 19.

Theorem 19. *Let $a, k \in \mathbb{N}$, $a \geq 2$, p, q be primes and let $p \nmid a$. Then we have $p^{k+1} \mid M_q(a)$ if and only if at least one of the below conditions* (A), (B), (C) *holds.*

(A) $\mathrm{ord}_p(a) = 1$, $\mathrm{ord}_{p^{k+1}}(a) = p$, $p = q$.

(B) $\mathrm{ord}_p(a) = \mathrm{ord}_{p^{k+1}}(a) = 1$.

(C) $\mathrm{ord}_p(a) = \mathrm{ord}_{p^{k+1}}(a) = q$.

Proof. (i) If $p^{k+1} \mid M_q(a)$, then $a^q \equiv 1 \pmod{p^{k+1}}$, which yields $\mathrm{ord}_{p^{k+1}}(a) \mid q$. Since q is a prime, we have $\mathrm{ord}_{p^{k+1}}(a) \in \{1, q\}$. If $\mathrm{ord}_{p^{k+1}}(a) = 1$, then $\mathrm{ord}_p(a) = 1$ and (B) follows. If $\mathrm{ord}_{p^{k+1}}(a) = q$, then, by part (vi) of Proposition 8, we have $\mathrm{ord}_{p^{k+1}}(a) = p^s \,\mathrm{ord}_p(a)$ for some $s \in \{0, \dots, k\}$. Hence, $p^s \,\mathrm{ord}_p(a) = q$. Since $\mathrm{ord}_p(a) \in \mathbb{N}$ and p, q are primes, only two following cases can occur.

Case 1: $s = 1$, $\mathrm{ord}_p(a) = 1$, $p = q$. Hence, (A).
Case 2: $s = 0$, $\mathrm{ord}_p(a) = q$. Hence, (C).

(ii) The proof of a converse implication consists of three simple parts. Assume (A). Then $\mathrm{ord}_{p^{k+1}}(a) = p$ implies $a^p \equiv 1 \pmod{p^{k+1}}$, which means $p^{k+1} \mid a^p - 1$. Since $p = q$, we have $p^{k+1} \mid a^q - 1 = M_q(a)$. Assume (B). Then $\mathrm{ord}_{p^{k+1}}(a) = 1$ implies $a \equiv 1 \pmod{p^{k+1}}$, thus, $p^{k+1} \mid a - 1$. Hence, $p^{k+1} \mid (a-1)(a^{q-1} + \cdots + a + 1) = a^q - 1 = M_q(a)$. Assume (C). Then $\mathrm{ord}_{p^{k+1}}(a) = q$ implies $a^q \equiv 1 \pmod{p^{k+1}}$. Hence, $p^{k+1} \mid a^q - 1 = M_q(a)$. □

Applying Theorem 19 for $a = 2$, we obtain Corollary 20.

Corollary 20. *Let $k \in \mathbb{N}$, p, q be primes and let $p \neq 2$. Then $p^{k+1} \mid M_q$ if and only if $\mathrm{ord}_{p^{k+1}}(2) = \mathrm{ord}_p(2) = q$. Consequently,*

$$p^2 \mid M_q \text{ if and only if } p \in W \text{ and } \mathrm{ord}_p(2) = q. \tag{12}$$

Proof. If p is a prime satisfying $\mathrm{ord}_p(2) = 1$, then $2 \equiv 1 \pmod{p}$, which is a contradiction. Hence, the cases (A) and (B) in Theorem 19 never occur. Part (C) in Theorem 19 yields $\mathrm{ord}_{p^{k+1}}(2) = \mathrm{ord}_p(2) = q$. If $k = 1$, (12) follows immediately. □

We now show some examples demonstrating part (C) of Theorem 19.

Example 21. (i) Let $k = 1$, $a = 53$, $p = 47$. Then

$$\mathrm{ord}_{47}(53) = \mathrm{ord}_{47^2}(53) = 23 \text{ and, } 47^2 \mid M_{23}(53) = 53^{23} - 1.$$

(ii) Let $k = 2$, $a = 6619$, $p = 383$. Then

$$\mathrm{ord}_{383}(6619) = \mathrm{ord}_{383^3}(6619) = 191 \text{ and, } 383^3 \mid M_{191}(6619) = 6619^{191} - 1.$$

(iii) Let $k = 3$, $a = 2819$, $p = 19$. Then

$$\mathrm{ord}_{19}(2819) = \mathrm{ord}_{19^4}(2819) = 3 \text{ and, } 19^4 \mid M_3(2819) = 2819^3 - 1.$$

(iv) Let $k = 3$, $a = 15384$, $p = 71$. Then

$$\mathrm{ord}_{71}(15384) = \mathrm{ord}_{71^4}(15384) = 7 \text{ and, } 71^4 \mid M_7(15384) = 15384^7 - 1.$$

5 Landry numbers with base a

In this section we will refer to *Landry numbers with base a* as the numbers

$$L_n(a) = a^n + 1 \text{ where } a \in \mathbb{N}, a \geq 2, n \in \mathbb{N} \cup \{0\}.$$

In particular, to numbers $L_n = L_n(2) = 2^n + 1$, we will refer as *Landry numbers*. The term of Landry numbers we will introduce in honor of the French mathematician Fortuné Landry (1799–1895), who successfully dealt with prime factorizations of the numbers $2^n \pm 1$. This designation has been inspired by a note presented by Williams [26, p. 463]. Here, Williams mentions that some of Landry's results have not received due attention being largely ignored. For details see [26].

The main aim of this section is to show that results analogous to Theorem 7 can also be proved for Landry numbers. The following Lemma 22 will be useful in proving Theorem 23.

Lemma 22. *Let $k \in \mathbb{N}$, p, q be primes and let $p \neq 2$. Then* (i) – (iv) *hold.*

(i) $\operatorname{ord}_{p^k}(2) \neq 1$.

(ii) $\operatorname{ord}_{p^k}(2) = 2$ *if and only if* $p = 3$ *and* $k = 1$.

(iii) $\operatorname{ord}_{p^{k+1}}(2) \neq 2$.

(iv) *If* $\operatorname{ord}_{p^{k+1}}(2) = 2q$ *then,* $\operatorname{ord}_p(2) \neq q$.

The proof of Lemma 22 can be left to the reader.

Theorem 23. *Let $k \in \mathbb{N}$, p, q be odd primes and let $p > 3$. If $p^k \mid L_q$, then the following statements are equivalent:*

(A) $p^{k+1} \mid L_q$.

(B) *p is a Wieferich prime of order k.*

(C) $\operatorname{ord}_{p^{k+1}}(2) = 2q$.

Proof. First, we prove that (A) implies (B). Let $p^{k+1} \mid L_q$. Then we have $2^q \equiv -1 \pmod{p^{k+1}}$, which yields $2^{2q} \equiv 1 \pmod{p^{k+1}}$. Hence, $\operatorname{ord}_{p^{k+1}}(2) \mid 2q$. By Lemma 22, we now obtain $\operatorname{ord}_{p^{k+1}}(2) = 2q$. Since $\operatorname{ord}_p(2) \mid \operatorname{ord}_{p^{k+1}}(2)$, we have $\operatorname{ord}_p(2) \in \{1, 2, q, 2q\}$ and, by Lemma 22, we get $\operatorname{ord}_p(2) = 2q$. Hence, $\operatorname{ord}_{p^{k+1}}(2) = \operatorname{ord}_p(2)$. This means, by Proposition 16, that p is a Wieferich prime of order k.

Next, we prove that (B) implies (C). Assume that p is a Wieferich prime of order k. Then, by Proposition 16, we have $2^{p-1} \equiv 1 \pmod{p^{k+1}}$ and, by part (i) of Proposition 8, we get $\operatorname{ord}_{p^{k+1}}(2) \mid p - 1$. Next, from the basic assumption $p^k \mid L_q$, we obtain $2^q \equiv -1 \pmod{p^k}$, which yields $2^{2q} \equiv 1 \pmod{p^k}$. Hence, $\operatorname{ord}_{p^k}(2) \mid 2q$ and, by Lemma 22, we obtain $\operatorname{ord}_{p^k}(2) = 2q$. Further, by part (v) of Proposition 8, we get $\operatorname{ord}_{p^{k+1}}(2) \in \{2q, 2pq\}$.

Suppose that $\text{ord}_{p^{k+1}}(2) = 2pq$. Since $\text{ord}_{p^{k+1}}(2) \mid p-1$, we get $2pq \mid p-1$, a contradiction. Hence, $\text{ord}_{p^{k+1}}(2) = 2q$.

Finally, we prove that (C) implies (A). Assume, that $\text{ord}_{p^{k+1}}(2) = 2q$. Then $2^{2q} \equiv 1 \pmod{p^{k+1}}$ yielding $p^{k+1} \mid (2^q - 1)(2^q + 1)$. Suppose that $p \mid 2^q - 1$. Then we have $\text{ord}_p(2) \mid q$, which means that $\text{ord}_p(2) \in \{1, q\}$. Hence, by Lemma 22, a contradiction follows. Therefore, $p^{k+1} \mid 2^q + 1 = L_q$. The proof is complete. □

For Landry numbers with a base $a \in \mathbb{N}$, $a \geq 2$, we can prove the following theorem.

Theorem 24. *Let $a, k \in \mathbb{N}$, $a \geq 2$, let p, q be odd primes, and let $p \nmid a$. Then $p^{k+1} \mid L_q(a)$ if and only if at least one of the below conditions* (A), (B), (C) *holds.*

(A) $\text{ord}_p(a) = 2$, $\text{ord}_{p^{k+1}}(a) = 2p$, $p = q$.

(B) $\text{ord}_p(a) = \text{ord}_{p^{k+1}}(a) = 2$.

(C) $\text{ord}_p(a) = \text{ord}_{p^{k+1}}(a) = 2q$.

Proof. (i) Let $p^{k+1} \mid L_q(a)$. Then $a^q \equiv -1 \pmod{p^{k+1}}$, which yields $\text{ord}_{p^{k+1}}(a) \neq q$. On the other hand, the congruence $a^q \equiv -1 \pmod{p^{k+1}}$ implies $a^{2q} \equiv 1 \pmod{p^{k+1}}$. Hence, $\text{ord}_{p^{k+1}}(a) \mid 2q$. Since q is an odd prime, we have $\text{ord}_{p^{k+1}}(a) \in \{1, 2, 2q\}$. Next, by part (vi) of Proposition 8, there exists an $s \in \{0, \ldots, k\}$ such that $\text{ord}_{p^{k+1}}(a) = p^s \,\text{ord}_p(a)$. Hence, $p^s \,\text{ord}_p(a) \mid 2q$.

Let $s \neq 0$. Since p, q are odd primes, the relation $p^s \,\text{ord}_p(a) \mid 2q$ implies $s = 1$, $p = q$ and $\text{ord}_p(a) \mid 2$. Hence, $\text{ord}_p(a) \in \{1, 2\}$. Suppose that $\text{ord}_p(a) = 1$. Then $\text{ord}_{p^{k+1}}(a) = p$, which means that $a^p \equiv 1 \pmod{p^{k+1}}$. Since we have $p = q$, it follows from $p^{k+1} \mid L_q(a)$ that $a^p \equiv -1 \pmod{p^{k+1}}$. Combining $a^p \equiv 1 \pmod{p^{k+1}}$ and $a^p \equiv -1 \pmod{p^{k+1}}$, we obtain $2 \equiv 0 \pmod{p^{k+1}}$, a contradiction. If $\text{ord}_p(a) = 2$, then $\text{ord}_{p^{k+1}}(a) = 2p = 2q$. Hence, (A).

Let $s = 0$. Then we have $\text{ord}_{p^{k+1}}(a) = \text{ord}_p(a)$. Suppose that $\text{ord}_{p^{k+1}}(a) = 1$. Then $p^{k+1} \mid a-1$. Hence, $p^{k+1} \mid (a-1)(a^{q-1} + \cdots + a + 1) = a^q - 1$, which yields $a^q \equiv 1 \pmod{p^{k+1}}$. On the other hand, from $p^{k+1} \mid L_q(a)$, it follows $a^q \equiv -1 \pmod{p^{k+1}}$. Along with $a^q \equiv 1 \pmod{p^{k+1}}$, this yields $2 \equiv 0 \pmod{p^{k+1}}$, a contradiction. Finally, if $\text{ord}_{p^{k+1}}(a) = 2$, we get (B) and, if $\text{ord}_{p^{k+1}}(a) = 2q$, we get (C).

(ii) The proof of the converse implication consists of the three following parts.

Assume (A). From $\text{ord}_{p^{k+1}}(a) = 2p$, it follows that $p^{k+1} \mid a^{2p} - 1 = (a^p - 1)(a^p + 1)$. Suppose that $p \mid a^p - 1$. Then $\text{ord}_p(a) \in \{1, p\}$, which is a contradiction with $\text{ord}_p(a) = 2$. Hence, $p^{k+1} \mid a^p + 1$. Since $p = q$, we have $p^{k+1} \mid a^q + 1 = L_q(a)$.

Assume (B). From $\text{ord}_{p^{k+1}}(a) = 2$, it follows that $p^{k+1} \mid a^2 - 1 = (a-1)(a+1)$. Suppose that $p \mid a - 1$. Then we have $\text{ord}_p(a) = 1$, which is a contradiction with $\text{ord}_p(a) = 2$. Hence, $p^{k+1} \mid a + 1$, which yields $p^{k+1} \mid (a+1)(a^{q-1} - a^{q-2} + \cdots - a + 1) = a^q + 1 = L_q(a)$.

Assume (C). From $\text{ord}_{p^{k+1}}(a) = 2q$, it follows that $p^{k+1} \mid a^{2q} - 1 = (a^q - 1)(a^q + 1)$. Suppose that $p \mid a^q - 1$. Then $\text{ord}_p(a) \in \{1, q\}$, which is a contradiction with $\text{ord}_p(a) = 2q$. Hence, $p^{k+1} \mid a^q + 1 = L_q(a)$. □

Applying Theorem 24 for $a = 2$ and $k = 1$, we obtain Corollary 25.

Corollary 25. *Let p, q be an odd primes. Then $p^2 \mid L_q$ if and only if*

$$[p, q] = [3, 3] \text{ or } \operatorname{ord}_p(2) = \operatorname{ord}_{p^2}(2) = 2q. \tag{13}$$

Consequently, if $p > 3$, then

$$p^2 \mid L_q \text{ if and only if } p \in W \text{ and } \operatorname{ord}_p(2) = 2q. \tag{14}$$

Proof. Let p be an odd prime satisfying $\operatorname{ord}_p(2) = 2$. Then $2^2 \equiv 1 \pmod p$, which yields $p = 3$. Since $\operatorname{ord}_9(2) = 6$, part (A) in Theorem 24 is equivalent to $[p, q] = [3, 3]$ and part (B) will never occur. Next, part (C) of Theorem 24 yields $\operatorname{ord}_p(2) = \operatorname{ord}_{p^2}(2) = 2q$. Hence, (13). Finally, (14) immediately follows from (13) and Proposition 16. □

We now demonstrate part (C) of Theorem 24 by some examples.

Example 26. (i) Let $k = 1$, $a = 79$, $p = 263$. Then

$$\operatorname{ord}_{263}(79) = \operatorname{ord}_{263^2}(79) = 2 \cdot 131 \text{ and, } 263^2 \mid L_{131}(79) = 79^{131} + 1.$$

(ii) Let $k = 2$, $a = 42$, $p = 23$. Then

$$\operatorname{ord}_{23}(42) = \operatorname{ord}_{23^3}(42) = 2 \cdot 11 \text{ and, } 23^3 \mid L_{11}(42) = 42^{11} + 1.$$

(iii) Let $k = 3$, $a = 119551$, $p = 107$. Then

$$\operatorname{ord}_{107}(119551) = \operatorname{ord}_{107^4}(119551) = 2 \cdot 53 \text{ and, } 107^4 \mid L_{53}(119551) = 119551^{53} + 1.$$

(iv) Let $k = 1$, $a = 26$, $p = 6695256707$. Then

$$\operatorname{ord}_p(26) = \operatorname{ord}_{p^2}(26) = 2q, q = 3347628353 \text{ and, } 6695256707^2 \mid L_q(26) = 26^q + 1.$$

Note, that the number $26^q + 1$ has 4736804899 digits. This can be verified using the formula $N = \lfloor \log_{10}(n) + 1 \rfloor$. Here, N stands for the number of digits of n and $\lfloor \cdot \rfloor$ denotes the floor function.

Remark 27. After a brief inspection of the proof of Theorem 24, we see that its conclusion cannot be true for q having a value of 2. Namely, if $q = 2$, then (B) does not imply $p^{k+1} \mid L_q(a)$. To see this, assume (B). Then $\operatorname{ord}_{p^{k+1}}(a) = 2$, which means $a^2 \equiv 1 \pmod{p^{k+1}}$. Suppose that $p^{k+1} \mid L_2(a)$. Then $a^2 \equiv -1 \pmod{p^{k+1}}$. This, together with $a^2 \equiv 1 \pmod{p^{k+1}}$, yields $2 \equiv 0 \pmod{p^{k+1}}$, a contradiction. It is worth noting that all the remaining implications in Theorem 24 are also true for $q = 2$.

Theorem 28. *Let $a, k \in \mathbb{N}$, $a > 2$, $2 \nmid a$ and let q be a prime. Then* (A) *and* (B) *hold.*

(A) *Let $q \neq 2$. Then $2^{k+1} \mid L_q(a)$ if and only if $2^{k+1} \mid L_1(a)$.*

(B) *Let* $q = 2$. *Then* $2^{k+1} \nmid L_2(a)$.

Proof. We prove (A). First, using the assumption $q \neq 2$, we obtain

$$L_q(a) = L_1(a)(a^{q-1} - a^{q-2} + \cdots - a + 1). \tag{15}$$

Next, applying $2 \nmid a$ and $2 \nmid q$, we get $2 \nmid (a^{q-1} - a^{q-2} + \cdots - a + 1)$. This, together with (15), yields (A).

We prove (B). Since $a > 2$ and $2 \nmid a$, there exists an $\alpha \in \mathbb{N}$ such that $a = 2\alpha + 1$. Hence, $a^2 + 1 = 2(2\alpha^2 + 2\alpha + 1)$. This means that $4 \nmid a^2 + 1$ and, $2^{k+1} \nmid L_2(a)$ follows. $\square$

We conclude this section by Hypothesis 29.

Hypothesis 29. *Every Landry number* $L_n = 2^n + 1$ *with a prime exponent* $n > 3$ *is of the form* $L_n = p_1 \cdots p_k$ *where* $p_1, \ldots, p_k$ *are distinct odd primes and* $k \geq 1$.

6 Some problems related to $\mathrm{ord}_p(2)$

We start this section by recalling some known properties of the quadratic character of 2.

Theorem 30. *Let* p *be a prime,* $p \neq 2$. *Then*

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod{p} \tag{16}$$

and,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{if } p \equiv 1, 7 \pmod{8}; \\ -1, & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases} \tag{17}$$

For a proof of (16) see, for example, [6, p. 86] or [8, p. 51]. An elementary proof of (17), based on Gauss's lemma, can be found in books [8, p. 53] and [15, p. 102]. For some alternative proofs of (17), consult articles [10] and [25].

Proposition 31. *Let* p *be a prime,* $p \neq 2$ *and let* $\mathrm{ord}_p(2) = q$, *where* q *is a prime. Then*

$$p = 3 \text{ or } p \equiv 1, 7 \pmod{8}. \tag{18}$$

Proof. If $q = 2$, then $\mathrm{ord}_p(2) = 2$. Hence, $3 \equiv 0 \pmod{p}$ and $p = 3$ follows. Let $q \neq 2$. Since $q \mid p-1$, there exists a $u \in \mathbb{N}$ such that $p - 1 = 2qu$. Hence, $2^{(p-1)/2} = (2^q)^u \equiv 1^u \equiv 1 \pmod{p}$. Applying (16) and (17), we now obtain $p \equiv 1, 7 \pmod{8}$. $\square$

The below example illustrates that, in (18), both cases $p \equiv 1, 7 \pmod{8}$ can occur.

Example 32. (i) Let $p = 89$. Then $p \equiv 1 \pmod 8$ and we have $\mathrm{ord}_{89}(2) = 11$. (ii) Let $p = 7$. Then $p \equiv 7 \pmod 8$ and we have $\mathrm{ord}_7(2) = 3$. The values of the primes p presented are the least values for which the corresponding cases occur.

Proposition 33. *Let p be a prime, $p \neq 2$ and let $\mathrm{ord}_p(2) = 2q$, where q is a prime. Then* (i) *and* (ii) *hold:*

(i) $p \neq 8k + 5$ *for any* $k \in \mathbb{N}$.

(ii) $p \neq 8k + 7$ *for any* $k \in \mathbb{N}$.

Proof. First observe that, if $q = 2$, then $\mathrm{ord}_p(2) = 4$ and, thus, $15 \equiv 0 \pmod p$. Hence, $p = 3$ or $p = 5$, which yields a contradiction in both cases (i) and (ii).

To prove (i), let $q \neq 2$. Suppose that $p = 8k + 5$ for some $k \in \mathbb{N}$. Then, by Theorem 30, $(2/p) \equiv 2^{(p-1)/2} \equiv -1 \pmod p$. Since $2q \mid p - 1$, there exists a $u \in \mathbb{N}$ such that $p - 1 = 2qu$. Hence,

$$2^{qu} = 2^{(p-1)/2} \equiv -1 \pmod p. \tag{19}$$

Next, it is clear from $\mathrm{ord}_p(2) = 2q$ that $2^{2q} \equiv 1 \pmod p$. Hence, $2^q \equiv -1 \pmod p$. Suppose that u is even. Then

$$2^{qu} = (2^q)^u \equiv (-1)^u \equiv 1 \pmod p. \tag{20}$$

Combining (19) and (20) we obtain $2 \equiv 0 \pmod p$. Hence, $p = 2$, a contradiction.

Suppose that u is odd. Then $u = 2v + 1$ for some $v \in \mathbb{N} \cup \{0\}$. From $p - 1 = 2qu$, it follows that $p = 4qv + 2q + 1$, which yields $p \equiv 2q + 1 \pmod 4$. On the other hand, using the assumption $p = 8k + 5$, we get $p \equiv 1 \pmod 4$. This, together with $p \equiv 2q + 1 \pmod 4$, yields $q \equiv 0 \pmod 2$. Hence, $q = 2$, a contradiction. This proves (i).

The proof of (ii) is similar. □

From Proposition 33, we immediately obtain Corollary 34.

Corollary 34. *Let p be a prime, $p \neq 2$ and let $\mathrm{ord}_p(2) = 2q$, where q is a prime. Then*

$$p = 5 \text{ or } p \equiv 1, 3 \pmod 8. \tag{21}$$

The below example illustrates that, in (21), both cases $p \equiv 1, 3 \pmod 8$ can occur.

Example 35. (i) Let $p = 1049$. Then $p \equiv 1 \pmod 8$ and we have $\mathrm{ord}_{1049}(2) = 2 \cdot 131$. (ii) Let $p = 11$. Then $p \equiv 3 \pmod 8$ and we have $\mathrm{ord}_{11}(2) = 2 \cdot 5$. The values of the primes p presented are the least values for which the corresponding cases occur.

In the remaining part of this section, the following notation will be adopted. If A is a finite set, $\#A$ denotes the number of elements of A. Next, P denotes the set of all odd primes. Finally, for an $n \in \mathbb{N}$, we define

$$\begin{aligned}
\pi(n) &= \#\{p \in P \cup \{2\} : p \leq n\}, \\
E(n) &= \#\{p \in P : p \leq n, \mathrm{ord}_p(2) \text{ is even}\}, \\
O(n) &= \#\{p \in P : p \leq n, \mathrm{ord}_p(2) \text{ is odd}\}, \\
Q(n) &= \#\{p \in P : p \leq n, \mathrm{ord}_p(2) = q, q \in P \cup \{2\}\}, \\
T(n) &= \#\{p \in P : p \leq n, \mathrm{ord}_p(2) = 2q, q \in P \cup \{2\}\}.
\end{aligned}$$

Computer investigation of the values $E(n)$, $O(n)$, $Q(n)$, $T(n)$ and $\pi(\pi(n))$ for $n \leq 10^{10}$ yields the data in Table 1:

n	$E(n)$	$O(n)$	$Q(n)$	$T(n)$	$\pi(n)$	$\pi(\pi(n))$
10^2	16	8	6	5	25	9
10^3	117	50	22	17	168	39
10^4	878	350	106	96	1229	201
10^5	6794	2797	586	590	9592	1184
10^6	55550	22947	3846	3745	78498	7702
10^7	470633	193945	26561	26596	664579	53911
10^8	4081095	1680359	196652	196695	5761455	397557
10^9	36016626	14830907	1511508	1509239	50847534	3048955
10^{10}	322328955	132723555	11982381	11981476	455052511	24106415

Table 1: Some values of $E(n)$, $O(n)$, $Q(n)$, $T(n)$ and $\pi(\pi(n))$.

From Table 1, we immediately obtain

$$\frac{E(10^{10})}{\pi(10^{10})} \doteq 0.708333, \ \frac{O(10^{10})}{\pi(10^{10})} \doteq 0.291666 \text{ and } \frac{O(10^{10})}{E(10^{10})} \doteq 0.411764. \tag{22}$$

The relations given in (22) reveal a significant difference between the numbers $E(n)$ and $O(n)$ in the investigated range. In fact, in 1966, Hasse, [7, p. 23] proved that

$$\lim_{n\to\infty} \frac{E(n)}{\pi(n)} = \frac{17}{24}, \ \lim_{n\to\infty} \frac{O(n)}{\pi(n)} = \frac{7}{24} \text{ and } \lim_{n\to\infty} \frac{O(n)}{E(n)} = \frac{7}{17}. \tag{23}$$

See also Lagarias [14, p. 449]. Furthermore, from Table 1, we obtain

$$\frac{Q(10^{10})}{T(10^{10})} \doteq 1.000075 \text{ and } \frac{\pi(\pi(10^{10}))}{Q(10^{10})} \doteq 2.011821. \tag{24}$$

This leads to a natural question, which can be formulated as Problem 36.

Problem 36. Prove or disprove

$$\lim_{n\to\infty}\frac{Q(n)}{T(n)}=1 \text{ and } \lim_{n\to\infty}\frac{\pi(\pi(n))}{Q(n)}=2. \tag{25}$$

Next, for an $n\in\mathbb{N}$, let us define

$$\begin{aligned}
R(n) &= \#\{p\in P : p\le n, \operatorname{ord}_p(2)=q, q\in P\cup\{2\}, p\equiv 1 \pmod 8\},\\
S(n) &= \#\{p\in P : p\le n, \operatorname{ord}_p(2)=q, q\in P\cup\{2\}, p\equiv 7 \pmod 8\},\\
U(n) &= \#\{p\in P : p\le n, \operatorname{ord}_p(2)=2q, q\in P\cup\{2\}, p\equiv 1 \pmod 8\},\\
V(n) &= \#\{p\in P : p\le n, \operatorname{ord}_p(2)=2q, q\in P\cup\{2\}, p\equiv 3 \pmod 8\}.
\end{aligned}$$

Computer investigation of the values $R(n)$, $S(n)$, $U(n)$, and $V(n)$ for $n\le 10^{10}$, yields the data in Table 2.

n	$R(n)$	$S(n)$	$U(n)$	$V(n)$
10^2	1	4	0	4
10^3	2	19	0	16
10^4	13	92	18	77
10^5	92	493	95	494
10^6	629	3216	594	3150
10^7	4182	22378	4320	22275
10^8	30556	166095	30961	165733
10^9	233384	1278123	233357	1275881
10^{10}	1834805	10147575	1835943	10145532

Table 2: Some values of $R(n)$, $S(n)$, $U(n)$, and $V(n)$.

From Tables 1 and 2, we get

$$\frac{R(10^{10})}{Q(10^{10})}\doteq 0.153125,\ \frac{S(10^{10})}{Q(10^{10})}\doteq 0.846874 \text{ and } \frac{R(10^{10})}{S(10^{10})}\doteq 0.180812.$$

$$\frac{U(10^{10})}{T(10^{10})}\doteq 0.153231,\ \frac{V(10^{10})}{T(10^{10})}\doteq 0.846768 \text{ and } \frac{U(10^{10})}{V(10^{10})}\doteq 0.180960.$$

Hence, we can propose the following problem.

Problem 37. Find the limits (26) and (27) and prove that $\alpha_i=\beta_i$ for $i\in\{1,2,3\}$.

$$\alpha_1=\lim_{n\to\infty}\frac{R(n)}{Q(n)},\ \alpha_2=\lim_{n\to\infty}\frac{S(n)}{Q(n)} \text{ and } \alpha_3=\lim_{n\to\infty}\frac{R(n)}{S(n)}. \tag{26}$$

$$\beta_1=\lim_{n\to\infty}\frac{U(n)}{T(n)},\ \beta_2=\lim_{n\to\infty}\frac{V(n)}{T(n)} \text{ and } \beta_3=\lim_{n\to\infty}\frac{U(n)}{V(n)}. \tag{27}$$

7 Concluding remarks

The following questions play an important role in further investigating the problem of the existence of primes p, q satisfying $p^2 \mid 2^q \pm 1$. Is there a third Wieferich prime? Is the set W of all Wieferich primes finite or infinite? Opinions vary as to what are the correct answers to such questions. See, for example, Beeger [3, p. 52] and Guy [5, p. 14]. If Beeger's point of view is right, that is, $W = \{1093, 3511\}$, then both Hypothesis 1 and Hypothesis 29 hold. This follows immediately from (28) and (29).

$$\mathrm{ord}_{1093}(2) = \mathrm{ord}_{1093^2}(2) = 364 = 2^2 \cdot 7 \cdot 13, \tag{28}$$

$$\mathrm{ord}_{3511}(2) = \mathrm{ord}_{3511^2}(2) = 1755 = 3^3 \cdot 5 \cdot 13. \tag{29}$$

On the other hand, by (12) and (14), both hypotheses may hold true even if the set W is infinite. This fact makes both problems even more interesting.

It is worth noting that a similar disunity of opinion can also be seen in the analogous problem concerning the existence of Wall-Sun-Sun primes. A detailed historical study of this problem can be found in the article [11].

In conclusion, let us note that a statement similar to (12) and (14) can also be proved for Fermat numbers as shown below.

Theorem 38. *Let $n \in \mathbb{N} \cup \{0\}$ and let p be a prime. Then*

$$p^2 \mid F_n \text{ if and only if } p \in W \text{ and } \mathrm{ord}_p(2) = 2^{n+1}. \tag{30}$$

Using a computer, it can be verified that, for $p \leq 10^{10}$, there exist only 20 primes satisfying $\mathrm{ord}_p(2) = 2^k$ for some $k \in \mathbb{N}$:

$$3, 5, 17, 257, 641, 65537, 114689, 274177, 319489, 974849, 2424833, 6700417, 13631489,$$

$$26017793, 45592577, 63766529, 167772161, 825753601, 1214251009, 6487031809.$$

8 Acknowledgment

The author thanks the anonymous referee for carefully reading the manuscript.

References

[1] T. Agoh, K. Dilcher, and L. Skula, Fermat quotients for composite moduli, *J. Number Theory* **66** (1997), 29–50.

[2] N. Beeger, On a new case of the congruence $2^{p-1} \equiv 1 \pmod{p^2}$, *Messenger of Mathematics* **51** (1922), 149–150.

[3] N. Beeger, On the congruence $2^{p-1} \equiv 1 \pmod{p^2}$ and Fermat's last theorem, *Nieuw Arch. Wiskunde* **20** (1939), 51–54.

[4] E. Deza, *Mersenne Numbers and Fermat Numbers, Selected Chapters of Number Theory: Special Numbers*, World Scientific, 2021.

[5] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd edition, Springer, 2004.

[6] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th edition, Oxford University Press, 2008.

[7] H. Hasse, Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod.p ist, *Math. Ann.* **166** (1966), 19–23.

[8] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edition, Springer, 1992.

[9] F. Jakóbczyk, Les applications de la fonction $\lambda_g(n)$ à l'étude des fractions périodiques et de la congruence chinoise $2^n - 2 \equiv 0 \pmod{n}$, *Ann. Univ. Mariae Curie-Skłodowska* **5** (1951), 97–138.

[10] R. Jakimczuk, The quadratic character of 2, *Math. Mag.* **84** (2011), 126–127.

[11] J. Klaška, Donald Dines Wall's conjecture, *Fibonacci Quart.* **56** (2018), 43–51.

[12] J. Klaška, A simple proof of Skula's theorem on prime power divisors of Mersenne numbers, *J. Integer Sequences* **25** (2022), Article 22.4.3.

[13] M. Křížek, F. Luca, and L. Somer, 17 *Lectures on Fermat Numbers, From Number Theory to Geometry*, Canadian Mathematical Society, Springer, 2001.

[14] J. C. Lagarias, The set of primes dividing the Lucas numbers has density 2/3, *Pacific J. Math.* **118** (1985), 449–461.

[15] W. J. LeVeque, *Fundamentals of Number Theory*, Addison-Wesley, 1977.

[16] W. J. LeVeque, *Topics in Number Theory*, Volume I, Dover Publications, 2002.

[17] W. Meissner, Über die Teilbarkeit von $2^p - 2$ durch das Quadrat der Primzahl $p = 1093$, *Sitzungsberichte der Akademie der Wissenschaften* **35** (1913), 663–667.

[18] H. Piersa, Śp. Ksiądz dr Franciszek Jakóbczyk (9 X 1905–3 VI 1992), *Roczniki Filozoficzne* **39–40**, (1991–1992), 5–7.

[19] PrimeGrid, `https://www.primegrid.com`.

[20] A. Rotkiewicz, Sur les nombres de Mersenne dépourvus de diviseurs carrés et sur les nombres naturels n, tels que $n^2 \mid 2^n - 2$, *Mat. Vestnik* **17** (1965), 78–80.

[21] W. Sierpiński, *A Selection of Problems in the Theory of Numbers*, Pergamon Press, 1964.

[22] L. Skula, Prime power divisors of Mersenne numbers and Wieferich primes of higher order, *Integers* **19** (2019), #A19.

[23] N. J. A. Sloane et al., *The On-Line Encyclopedia of Integer Sequences*, available at `https://oeis.org`, 2023.

[24] L. R. Warren and H. G. Bray, On the square-freeness of Fermat and Mersenne numbers, *Pacific J. Math.* **22** (1967), 563–564.

[25] K. S. Williams, The quadratic character of 2 mod p, *Math. Mag.* **49** (1976), 89–90.

[26] K. S. Williams, How was F_6 factored?, *Math. Comp.* **61** (1993), 463–474.

[27] A. Wieferich, Zum letzten Fermat'schen Theorem, *J. Reine Angew. Math.* **136** (1909), 293–302.

2020 *Mathematics Subject Classification:* Primary 11A41; Secondary 11A07.
Keywords: Mersenne number, Fermat number, Wieferich prime, Wieferich number.

(Concerned with sequences A000215, A000225, A001220, and A077816.)

Received February 9 2023; revised versions received March 16 2023; March 17 2023. Published in *Journal of Integer Sequences*, March 17 2023.

Return to Journal of Integer Sequences home page.