SEVERAL NOTES ON JAKÓBCZYK'S HYPOTHESIS ON FERMAT NUMBERS

Jiří Klaška
Institute of Mathematics, Brno University of Technology,
Brno, Czech Republic
klaska@fme.vutbr.cz

Received: 4/1/25, Revised: 2/7/26, Accepted: 5/25/26, Published: 6/26/26

Abstract

Over the past centuries, Fermat numbers have been studied by many authors with a number of notable results achieved. After a short historical introduction, the present article will concentrate on a hypothesis proposed by the Polish mathematician Jakóbczyk more than 70 years ago. The hypothesis will be viewed in a broader context of the sequences of generalized Fermat numbers.

–Dedicated to Professor Michal Křížek

1. Introduction

The famous Polish mathematician Franciszek Jakóbczyk (1905–1992) published in 1951 the following hypothesis not-yet resolved concerning the Fermat numbers.

Hypothesis 1. (Jakóbczyk, [3]). All Fermat numbers $F_n = 2^{2^n} + 1$ are square free.

For the original formulation of Hypothesis 1, see paper [3, p. 127]. Details of the life and work of Franciszek Jakóbczyk can be found in [6]. In 1730, the Swiss mathematician Christian Goldbach (1690–1764) proved, the following property of Fermat numbers.

Theorem 1. (Goldbach, 1730). *Let $m, n \in \mathbb{N} \cup \{0\}$ and let $m \neq n$. Then,*

$$\gcd(F_m, F_n) = 1. \tag{1}$$

Consequently, no two different Fermat numbers are divisible by a single prime.

For a proof of Equation (1) see [5, p. 33]. Should Hypothesis 1 be proven, together with Theorem 1, it would present a pair of remarkable and extraordinary beautiful mathematical statements.

DOI: 10.5281/zenodo.20931052

Hypothesis 1 is closely related to another unsolved number theory problem related to Wieferich primes. Recall that an odd prime p is called a *Wieferich prime* if

$$2^{p-1} \equiv 1 \pmod{p^2}. \tag{2}$$

The term of "Wieferich prime" was introduced in honor of the German mathematician Arthur Wieferich (1884–1954), who found a connection of primes p satisfying Equation (2) with the first case of Fermat last theorem. Wieferich [10] 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 $2^{p-1} \equiv 1 \pmod{p^2}$. So far only two Wieferich primes, 1093 and 3511, are known. Thanks to extensive calculations on a computer, it has been verified that, if the third Wieferich prime exists, then it must be greater than $2^{64} \approx 1.8 \cdot 10^{19}$. Whether the set $\mathcal{W}$ of all Wieferich primes is finite or infinite is not yet known. The following implication was proved by Warren and Bray [9, p. 563].

Theorem 2. (Warren and Bray, 1967). *Let $n \in \mathbb{N}$, $n \geq 2$, and let p be an odd prime. If $p \mid F_n$, then $2^{(p-1)/2} \equiv 1 \pmod{F_n}$.*

Theorem 2 can be extended as follows.

Theorem 3. *Let $n \in \mathbb{N} \cup \{0\}$ and let p be a prime. If $p \mid F_n$, then $p^2 \mid F_n$ if and only if $2^{p-1} \equiv 1 \pmod{p^2}$.*

For a proof of Theorem 3, see for example Křížek et al., [5, p. 68], and one may also refer to Ribenboim [7, p. 87]. The result presented in Theorem 3 provides the basic link between Hypothesis 1 and Wieferich primes.

In this paper, we will study Hypothesis 1 in a broader context of the sequences $\{F_n(a,b)\}_{n=0}^{\infty}$, where $F_n(a,b) = a^{b^n} + 1$, $a, b \in \mathbb{N}$, and $a, b \geq 2$. First, we will find out for which sequences $\{F_n(a,b)\}_{n=0}^{\infty}$ Goldbach's theorem can be generalized.

2. Basic Divisibility Properties of the Numbers $F_n(a,b)$

Proposition 1. *Let a, b, m, n be integers such that $2 < a, b$ and $0 \leq n \leq m$. Then the following three statements are true.*

(i) *If $a \equiv 0 \pmod 2$ and $b \equiv 0 \pmod 2$, then $\gcd(F_m(a,b), F_n(a,b)) = 1$.*

(ii) *If $a \equiv 1 \pmod 2$ and $b \equiv 0 \pmod 2$, then $\gcd(F_m(a,b), F_n(a,b)) = 2$.*

(iii) *If $b \equiv 1 \pmod 2$, then $\gcd(F_m(a,b), F_n(a,b)) = F_n(a,b)$.*

Proof. Since $m > n$, there exists a positive integer k such that $m = n + k$ and we have

$$F_m(a,b) - 1 = a^{b^{n+k}} = (a^{b^n})^{b^k} = (F_n(a,b) - 1)^{b^k}. \tag{3}$$

We prove (i). Let us suppose that $\gcd(F_m(a,b), F_n(a,b)) \neq 1$. Since $2 \nmid F_j(a,b)$ for every $j \in \mathbb{N} \cup \{0\}$, there exists at least one odd prime p such that $p \mid F_m(a,b)$ and $p \mid F_n(a,b)$. Reducing modulo p, from (3) we obtain

$$-1 \equiv (-1)^{b^k} \pmod{p}.$$

Since b is even, this implies that p divides 2, which is a contradiction.

We prove (ii). If $j \in \mathbb{N}$, then,

$$F_j(a,b) = (a^{b^j} - 1) + 2 = (a-1)(a^{b^j-1} + \cdots + a + 1) + 2. \tag{4}$$

Now, as a is odd and b is even, we have

$$a - 1 \equiv 0 \pmod{2} \text{ and } a^{b^j-1} + \cdots + a + 1 \equiv 0 \pmod{2}. \tag{5}$$

Next, it follows from Equations (4) and (5) that $F_j(a,b) \equiv 2 \pmod{4}$. If $j = 0$, then $F_0(a,b) = a + 1 \equiv 0 \pmod{2}$. Hence,

$$2 \mid \gcd(F_m(a,b), F_n(a,b)). \tag{6}$$

Let $p \neq 2$ be a prime satisfying $p \mid F_n(a,b)$. Then, $a^{b^n} \equiv -1 \pmod{p}$. Since $2 \mid b$, we have $a^{b^{n+k}} \equiv (-1)^{b^k} \equiv 1 \pmod{p}$. Hence, $F_{n+k}(a,b) \equiv 2 \pmod{p}$. Consequently, if $p \mid F_n(a,b)$, then $p \nmid F_m(a,b)$. This, together with Equation (6), yields $\gcd(F_m(a,b), F_n(a,b)) = 2$.

We prove (iii). Given that b is odd, we can write

$$F_{n+k}(a,b) = a^{b^{n+k}} + 1 = (a^{b^n} + 1)((a^{b^n})^{b^k-1} - (a^{b^n})^{b^k-2} + \cdots - a^{b^n} + 1), \tag{7}$$

which implies $F_n(a,b) \mid F_{n+k}(a,b)$. This proves (iii). □

Let $\varphi_n(a,b)$ denote the number of prime factors of $F_n(a,b)$ including their multiplicities. The following Corollary 1 follows directly from part (iii) of Proposition 1.

Corollary 1. *Let $a, b \in \mathbb{N}$, $a, b \geq 2$ and let $b \equiv 1 \pmod{2}$. Then the sequence $\{\varphi_n(a,b)\}_{n=0}^{\infty}$ is monotone increasing.*

Is the sequence $\{\varphi_n(2,2)\}_{n=0}^{\infty}$ monotone? This interesting question can be found in the book [5, p. 159, Problem 5]. By 2025, only the first twelve terms of the sequence $\{\varphi_n(2,2)\}_{n=0}^{\infty}$ have been found:

$$\{\varphi_n(2,2)\}_{n=0}^{\infty} = \{1, 1, 1, 1, 1, 2, 2, 2, 2, 3, 4, 5, \dots\}.$$

In addition, it has been proven that $\varphi_{12}(2,2) \geq 8$. Example 1 proves that, if $b \equiv 0 \pmod{2}$, then an analogue of Corollary 1 does not hold.

Example 1. (i) Let us consider the sequence $F_n(3,2) = 3^{2^n} + 1$. Then we have

$F_0(3,2) = 2^2$,
$F_1(3,2) = 2 \cdot 5$,
$F_2(3,2) = 2 \cdot 41$,
$F_3(3,2) = 2 \cdot 17 \cdot 193$,
$F_4(3,2) = 2 \cdot 21523361$,
$F_5(3,2) = 2 \cdot 926510094425921$,
$F_6(3,2) = 2 \cdot 1716841910146256242328924544641$,
$F_7(3,2) = 2 \cdot 257 \cdot 275201 \cdot 138424618868737 \cdot 3913786281514524929 \cdot P_{21}$ and
$F_8(3,2) = 2 \cdot 12289 \cdot 8972801 \cdot 891206124520373602817 \cdot P_{90}$,

where

$$\begin{aligned} P_{21} &= 153849834853910661121, \\ P_{90} &= 707275264749309881405141965802671548079179711 \\ &\quad 820351316861777644606207216944972589404100097. \end{aligned}$$

From the above, we obtain $\{\varphi_n(3,2)\}_{n=0}^{\infty} = \{2, 2, 2, 3, 2, 2, 2, 6, 5, \dots\}$. Hence, the sequence $\{\varphi_n(3,2)\}_{n=0}^{\infty}$ is not monotone.

(ii) Further, let us consider the sequence $F_n(46,2) = 46^{2^n} + 1$. Then we have

$F_0(46,2) = 47$ is prime,
$F_1(46,2) = 29 \cdot 73$,
$F_2(46,2) = 4477457$ is prime,
$F_3(46,2) = 17 \cdot 929 \cdot 1269398609$,
$F_4(46,2) = 97 \cdot 8513 \cdot 624737 \cdot 779065031672321$,
$F_5(46,2) = 257 \cdot 1569884896100468417 \cdot 400359077012692185282901663254593$,
$F_6(46,2) = 944257 \cdot 52208711297 \cdot 6806175851393423565671196264598472321 \cdot P_{53}$,
$F_7(46,2) = 8121089 \cdot 104782627167647104439041 \cdot P_{183}$,
$F_8(46,2) = 20305921 \cdot C_{419}$ and
$F_9(46,2) = P_{852}$ is prime,

where

$$\begin{aligned} P_{53} &= 77761544048050719364650799308637798429621836404447873, \\ P_{183} &= 80001642244279639883661499212679187670060444704882094817435480184310308946237007187319721677041863694475922674939467714881 \\ &\quad 34292694689586630873754779417798022643363364917357775814661 13. \end{aligned}$$

From the above, it follows that $\{\varphi_n(46,2)\}_{n=0}^{\infty} = \{1,2,1,3,4,3,4,3,c,1,\cdots\}$, where $c = \varphi_8(46,2) \geq 3$. This means that the sequence $\{\varphi_n(46,2)\}_{n=0}^{\infty}$ is not monotone.

In connection with [5, p. 159, Problem 5], presented in [5], we can formulate the following more general problem.

Problem 1. Prove or disprove the following statement. There are $a, b \in \mathbb{N}$, where $a, b \geq 2$ and $b \equiv 0 \pmod 2$ such that the sequence $\{\varphi_n(a,b)\}_{n=0}^{\infty}$ is monotone.

3. The Divisibility of $F_n(a,b)$ by the Square of a Prime

In 1997, Agoh, Dilcher, and Skula [1, pp. 30–31], introduced the concept of a Wieferich number with base a that substantially generalizes the concept of Wieferich prime as defined by Equation (2). For the purpose of the present article, it is sufficient to recall that a prime p is called a *Wieferich prime with base* $a \in \mathbb{N}$, $a \geq 2$ if $p \nmid a$ and

$$q(a,p) \equiv 0 \pmod p, \text{ or equivalently, } a^{p-1} \equiv 1 \pmod{p^2}. \tag{8}$$

In Equation (8), $q(a,p) = (a^{\varphi(p)} - 1)/p$, where φ is the Euler function. For details see [1]. In the sequel, the set of all Wieferich primes with base a will be denoted by $\mathcal{W}(a)$. It will also be useful to recall the following definition. Let $a, m \in \mathbb{N}$, $m \geq 2$ and let $\gcd(a,m) = 1$. The smallest positive integer k for which $a^k \equiv 1 \pmod m$ is called the *multiplicative order* of a modulo m, written as $k = \operatorname{ord}_m(a)$. A characterization of the set $\mathcal{W}(a)$ using the multiplicative order of a is provided by part (iii) of Lemma 1.

Lemma 1. *Let $a, h, m \in \mathbb{N}$, $a, m \geq 2$, and let $\gcd(a,m) = 1$. Further, let p be a prime such that $p \nmid a$. Then* (i)–(iii) *hold.*

(i) $a^h \equiv 1 \pmod m$ *if and only if* $\operatorname{ord}_m(a) \mid h$.

(ii) $\operatorname{ord}_{p^2}(a) \in \{p \operatorname{ord}_p(a), \operatorname{ord}_p(a)\}$.

(iii) $p \in \mathcal{W}(a)$ *if and only if* $\operatorname{ord}_{p^2}(a) = \operatorname{ord}_p(a)$.

Part (i) of Lemma 1 can be found in the books [2, p. 148] and [8, p. 348]. For part (ii) and (iii), see [4, p. 4] and [4, p. 9], respectively.

Lemma 2. *Let $a, b, m, n \in \mathbb{N}$, and let $a, b, m \geq 2$. If $a^{b^n} \not\equiv 1 \pmod m$, then $a^{b^t} \not\equiv 1 \pmod m$ for all $t \in \{0, \ldots, n-1\}$.*

Proof. Let us suppose that $a^{b^r} \equiv 1 \pmod{m}$ for some $r \in \{0, \ldots, n-1\}$. Since $r < n$, there exists an $s \in \mathbb{N}$ such that $n = r + s$. It is clear that

$$a^{b^{r+s}} - 1 = (a^{b^r} - 1)((a^{b^r})^{b^s - 1} + \cdots + a^{b^r} + 1). \tag{9}$$

Reducing Equation (9) modulo m, we obtain $a^{b^{r+s}} \equiv 1 \pmod{m}$, which is a contradiction. □

The following Theorem 4 provides a basic link between the square prime divisors of the numbers $F_n(a, b)$ and Wieferich primes with a base a.

Theorem 4. *Let $a, b \in \mathbb{N}$, $a, b \geq 2$, $n \in \mathbb{N} \cup \{0\}$, and let $p \neq 2$ be a prime such that* $\gcd(ab, p) = 1$. *Then* (i) *and* (ii) *hold.*

(i) *If $p^2 \mid F_n(a, b)$, then $p \in \mathcal{W}(a)$ and $\operatorname{ord}_p(a) \mid 2b^n$.*

(ii) *If $p \in \mathcal{W}(a)$ and $\operatorname{ord}_p(a) = 2b^n$, then $p^2 \mid F_n(a, b)$.*

Proof. We prove (i). Let $p^2 \mid a^{b^n} + 1$. Then $p^2 \mid (a^{b^n} + 1)(a^{b^n} - 1) = a^{2b^n} - 1$. This means that $a^{2b^n} \equiv 1 \pmod{p^2}$. Hence, by part (i) of Lemma 3.1, we get

$$\operatorname{ord}_{p^2}(a) \mid 2b^n. \tag{10}$$

Next, by part (ii) of Lemma 3.1, we have $\operatorname{ord}_{p^2}(a) \in \{p \operatorname{ord}_p(a), \operatorname{ord}_p(a)\}$. Let us suppose that $\operatorname{ord}_{p^2}(a) = p \operatorname{ord}_p(a)$. Then by Equation (10), $p \operatorname{ord}_p(a) \mid 2b^n$. Since $p \nmid b$, we find that $p = 2$, which is a contradiction. Hence, $\operatorname{ord}_{p^2}(a) = \operatorname{ord}_p(a)$. By part (iii) of Lemma 3.1, we now obtain $p \in \mathcal{W}(a)$ and, from Equation (10), we get $\operatorname{ord}_p(a) \mid 2b^n$.

We prove (ii). Let $p \in \mathcal{W}(a)$ and let $\operatorname{ord}_p(a) = 2b^n$. Since $p \in \mathcal{W}(a)$, applying part (iii) of Lemma 3.1, we get $\operatorname{ord}_{p^2}(a) = 2b^n$. Hence, by part (i) of Lemma 3.1, we have $a^{2b^n} \equiv 1 \pmod{p^2}$ and, thus, $(a^{b^n} + 1)(a^{b^n} - 1) \equiv 0 \pmod{p^2}$. Suppose now that $a^{b^n} + 1 \equiv 0 \pmod{p}$ and $a^{b^n} - 1 \equiv 0 \pmod{p}$. Then we find $2 \equiv 0 \pmod{p}$, which yields $p = 2$, a contradiction. Consequently, we have either $a^{b^n} + 1 \equiv 0 \pmod{p^2}$ or $a^{b^n} - 1 \equiv 0 \pmod{p^2}$. Suppose that $a^{b^n} - 1 \equiv 0 \pmod{p^2}$. Then using part (i) of Lemma 3.1, we obtain $\operatorname{ord}_{p^2}(a) \mid b^n$, which is a contradiction with $\operatorname{ord}_{p^2}(a) = 2b^n$. Hence, $a^{b^n} + 1 \equiv 0 \pmod{p^2}$, and the result follows. □

Example 2 proves that the converse implications to the statements (i) and (ii) presented in Theorem 4 are not true.

Example 2. Let us consider the sequence $F_n(19, 6) = 19^{6^n} + 1$. For $n = 1$, we have $19^6 + 1 = 2 \cdot 13^2 \cdot 181 \cdot 769$. Hence, $13^2 \mid 19^6 + 1$. First, we show that the converse implication to part (i) of Theorem 4 is not true. Let $p = 7$. Then we have $\operatorname{ord}_7(19) = \operatorname{ord}_{7^2}(19) = 6$. Hence, $7 \in \mathcal{W}(19)$ and $6 = \operatorname{ord}_7(19) \mid 2 \cdot 6$. However, from the equality $19^6 + 1 = 2 \cdot 13^2 \cdot 181 \cdot 769$, it follows that $7^2 \nmid 19^6 + 1$.

Further, let us consider the sequence $F_n(18,6) = 18^{6^n} + 1$. For $n = 1$, we have $18^6 + 1 = 5^2 \cdot 13 \cdot 229 \cdot 457$. Hence, $5^2 \mid 18^6 + 1$. After some calculation, we get $\mathrm{ord}_5(18) = \mathrm{ord}_{5^2}(18) = 4$. Hence, $5 \in \mathcal{W}(18)$ and $4 = \mathrm{ord}_5(18) \neq 2 \cdot 6$. This proves that the converse implication to part (ii) of Theorem 4 is not true.

If $b = 2$, Theorem 4 can be refined substantially.

Theorem 5. *Let $a \in \mathbb{N}$, $a \geq 2$, $n \in \mathbb{N} \cup \{0\}$ and let $p \neq 2$ be a prime such that $p \nmid a$. Then $p^2 \mid F_n(a,2)$ if and only if $p \in \mathcal{W}(a)$ and $\mathrm{ord}_p(a) = 2^{n+1}$. Consequently, we have*

$$p^2 \mid F_n \quad \text{if and only if} \quad p \in \mathcal{W} \text{ and } \mathrm{ord}_p(2) = 2^{n+1}. \tag{11}$$

Proof. Let us assume that $p^2 \mid a^{2^n} + 1$. Then by part (i) of Theorem 4, $p \in \mathcal{W}(a)$ and $\mathrm{ord}_p(a) \mid 2^{n+1}$. Because $p \mid a^{2^n} + 1$, we have $a^{2^n} \equiv -1 \pmod{p}$ and, applying Lemma 2, we find that $a^{2^t} \not\equiv 1 \pmod{p}$ for every $t \in \{0, \ldots, n-1\}$. Hence, $\mathrm{ord}_p(a) \neq 2^t$ for every $t \in \{0, \ldots, n\}$. This, together with $\mathrm{ord}_p(a) \mid 2^{n+1}$, yields $\mathrm{ord}_p(a) = 2^{n+1}$.

The converse implication follows immediately from part (ii) of Theorem 4. □

Note that the assumption $p \neq 2$ in Theorem 5 cannot be omitted. See part (i) of Example 1. Here, we have $2^2 \mid F_0(3,2)$ and $2 \notin \mathcal{W}(3)$.

Statement (11) has already been published, without a proof, in our recent paper [4, p. 19]. Let us now apply (11) to the known Wieferich primes 1093 and 3511. By direct calculation, we find that

$$\begin{aligned} \mathrm{ord}_{1093}(2) &= \mathrm{ord}_{1093^2}(2) = 364 = 2^2 \cdot 7 \cdot 13, \\ \mathrm{ord}_{3511}(2) &= \mathrm{ord}_{3511^2}(2) = 1755 = 3^3 \cdot 5 \cdot 13. \end{aligned}$$

Hence, by (11), we obtain $1093^2 \nmid F_{1092}$ and $3511^2 \nmid F_{3510}$. Finally, note that Theorem 5 admits the possibility of $\mathcal{W}$ being an infinite set, but no Wieferich prime p meets the condition $\mathrm{ord}_p(2) = 2^k$ for some $k \in \mathbb{N}$. This fact makes Hypothesis 1 extremely interesting. An extension of Theorem 5 is provided by Theorem 6.

Theorem 6. *Let $a, D \in \mathbb{N}$, $a, D \geq 2$, $n \in \mathbb{N} \cup \{0\}$ and let $\gcd(a, D) = 1$.*

(i) *If $2 \mid a$, then*

$$D \mid F_n(a,2) \text{ if and only if } \mathrm{ord}_D(a) = 2^{n+1}. \tag{12}$$

(ii) *If $2 \nmid a$, then (12) holds for every $D \neq 2$.*

Proof. Let us assume that $D \mid F_n(a,2)$. Then $a^{2^n} \equiv -1 \pmod{D}$, which implies $a^{2^{n+1}} \equiv 1 \pmod{D}$. By part (i) of Lemma 1, we now obtain $\mathrm{ord}_D(a) \mid 2^{n+1}$ and, by Lemma 2, we conclude that $\mathrm{ord}_D(a) = 2^{n+1}$.

Conversely, assume that $\mathrm{ord}_D(a) = 2^{n+1}$. Since $a^{2^{n+1}} \equiv 1 \pmod{D}$, we have

$$(a^{2^n}+1)(a^{2^n}-1) \equiv 0 \pmod{D}. \tag{13}$$

Let $d = \gcd(a^{2^n}+1, a^{2^n}-1)$. Then $a^{2^n} \equiv -1 \pmod{d}$ and $a^{2^n} \equiv 1 \pmod{d}$, which implies $2 \equiv 0 \pmod{d}$. Hence, $d \mid 2$. This means that

$$\gcd(a^{2^n}+1, a^{2^n}-1) = \begin{cases} 1 & \text{for } a \text{ even}, \\ 2 & \text{for } a \text{ odd}. \end{cases} \tag{14}$$

Let a be even. Combining Equations (13) and (14), we see that either

$$a^{2^n}+1 \equiv 0 \pmod{D} \quad \text{or} \quad a^{2^n}-1 \equiv 0 \pmod{D}. \tag{15}$$

Similarly, when a is odd, then it follows from Equations (13) and (14) that Equation (15) holds for every $D \neq 2$. Let us now suppose that $a^{2^n}-1 \equiv 0 \pmod{D}$. Then by part (i) of Lemma 1, $\mathrm{ord}_D(a) \mid 2^n$, which is a contradiction with $\mathrm{ord}_D(a) = 2^{n+1}$. Now, it is clear from Equation (15) that $D \mid a^{2^n}+1$, which completes the proof. □

Theorem 7. *Let $a, b, D \in \mathbb{N}$, $a, b, D \geq 2$, and let $n \in \mathbb{N} \cup \{0\}$. Then* (i) *and* (ii) *hold.*

(i) *If $2 \nmid b$ and $D \mid F_n(a,b)$, then $D \mid F_{n+k}(a,b)$ for all $k \in \mathbb{N}$.*

(ii) *If $2 \mid b$ and $D \mid F_n(a,b)$, then $D \nmid F_{n+k}(a,b)$ for all $k \in \mathbb{N}$.*

Proof. Let us assume that $D \mid a^{b^n}+1$. Then $a^{b^n} \equiv -1 \pmod{D}$, which yields

$$a^{b^{n+k}}+1 = (a^{b^n})^{b^k}+1 \equiv (-1)^{b^k}+1 \pmod{D}. \tag{16}$$

From Equation (16) now it follows that, if $2 \nmid b$, then $a^{b^{n+k}}+1 \equiv 0 \pmod{D}$ for all $k \in \mathbb{N}$ and, if $2 \mid b$, then $a^{b^{n+k}}+1 \equiv 2 \not\equiv 0 \pmod{D}$ for all $k \in \mathbb{N}$. This proves (i) and (ii). □

The following definitions will be needed for the statement of Corollary 2. Let $a, b \in \mathbb{N}$, $a, b \geq 2$ and let p be a prime. First, let us define the set

$$J(a,b,p^2) = \{n \in \mathbb{N} \cup \{0\} : p^2 \mid F_n(a,b)\}.$$

Next, if $J(a,b,p^2) \neq \emptyset$, we define the number $n_0 = n_0(a,b,p^2) \in \mathbb{N} \cup \{0\}$ by

$$n_0 = \min J(a,b,p^2).$$

Corollary 2. *Let $a, b \in \mathbb{N}$, $a, b \geq 2$ and let p be a prime. Next, let $J(a,b,p^2) \neq \emptyset$. Then* (i) *and* (ii) *hold.*

(i) *If* $2 \nmid b$ *and* $p^2 \mid F_{n_0}(a,b)$*, then the number* n_0 *is equal to the index of the first term of the period of the sequence* $\{F_n(a,b) \bmod p^2\}_{n=0}^{\infty}$.

(ii) *If* $2 \mid b$ *and* $p^2 \mid F_{n_0}(a,b)$*, then the number* n_0 *is equal to the index of the last term of the pre-period of the sequence* $\{F_n(a,b) \bmod p^2\}_{n=0}^{\infty}$.

Example 3 illustrates the difference between cases (i) and (ii) presented in Corollary 2.

Example 3. Let us consider the sequence $F_n(10,3) = 10^{3^n} + 1$. Then we have $487^2 \mid 10^{3^5} + 1$. On the other hand, $487 \nmid F_n(10,3)$ for every $n \in \{0,1,2,3,4\}$. Applying part (i) of Theorem 7, we now obtain $487^2 \mid 10^{3^n} + 1$ for every $n \geq 5$. Hence, we have $n_0 = 5$ and, by direct calculation, we get

$$\{F_n(10,3) \bmod 487^2\}_{n=0}^{\infty} = (11, 1001, 95497, 206448, 78154, 0, 0, 0, 0, 0, \ldots).$$

Further, let us consider the sequence $F_n(2968,6) = 2968^{6^n} + 1$. Then we have $2593^2 \mid F_4(2968,6) = 2968^{6^4} + 1$. Applying part (ii) of Theorem 7, we now find that $2593^2 \nmid F_n(2968,6)$ for all $n \neq 4$. Hence, $n_0 = 4$ and direct calculation yields

$$\{F_n(2968,6) \bmod 2593^2\}_{n=0}^{\infty} = (2969, 3331932, 3699454, 2884630, 0, 2, 2, 2, 2, \ldots).$$

4. Paulo Ribenboim Revised

In the paper [7, p. 87], Paulo Ribenboim published the following short note: "Up to now, no number $a^{a^n} + 1$ with a square factor has ever been found." In fact, if a is odd, then such numbers can easily be found. For example, for every $n \in \mathbb{N} \cup \{0\}$, we have:

$$\begin{array}{lll} 3^2 \mid F_n(17,17), & 5^2 \mid F_n(49,49), & 7^2 \mid F_n(97,97), \\ 11^2 \mid F_n(241,241), & 13^2 \mid F_n(337,337), & 17^2 \mid F_n(577,577), \\ 19^2 \mid F_n(69,69), & 23^2 \mid F_n(803,803), & 29^2 \mid F_n(1681,1681). \end{array} \tag{17}$$

The relations $p^2 \mid F_n(a,a)$ listed in (17) immediately follow from part (i) of Theorem 7 after verifying that $p^2 \mid F_0(a,a)$. Other examples may be found in a similar way. If a is even, to find the square divisors of $F_n(a,a)$, part (i) of Theorem 4 can be used. Applying this result, the relations (18) can be found:

$$\begin{array}{lll} 17^2 \mid F_2(110,110), & 41^2 \mid F_2(834,834), & 73^2 \mid F_2(306,306), \\ 97^2 \mid F_2(3234,3234), & 113^2 \mid F_2(1330,1330), & 193^2 \mid F_2(276,276), \\ 257^2 \mid F_2(2964,2964), & 281^2 \mid F_2(1470,1470), & 577^2 \mid F_2(828,828). \end{array} \tag{18}$$

For an even a, we have also found numbers $F_n(a,a)$ each having a cubic factor. For example, if $a \in \{1022, 4514\}$, then $17^3 \mid F_2(a,a)$. Perhaps the most interesting example found is given in Equation (19).

$$17^3 \mid F_3(158,158) = 158^{158^3} + 1. \tag{19}$$

Finally, let us note that, thanks to part (i) of Theorem 4, nontrivial examples can be found of the numbers $F_n(a,a)$ with an odd a each having a square factor. We can give some examples of the numbers $F_n(a,a)$ satisfying the relations $p \nmid F_0(a,a)$, $p \nmid F_1(a,a)$ and, $p^2 \mid F_2(a,a)$:

$$\begin{array}{lll} 19^2 \mid F_2(1743,1743), & 37^2 \mid F_2(4407,4407), & 127^2 \mid F_2(1155,1155), \\ 163^2 \mid F_2(2547,2547), & 251^2 \mid F_2(1295,1295), & 677^2 \mid F_2(2899,2899). \end{array}$$

5. Concluding Remark

The results presented indicate that, if Jakóbczyk's hypothesis is true, then it describes a very special property of the Fermat numbers F_n that cannot be extended to the numbers $F_n(a,2)$ that have a number of similar properties to F_n. Next, it is clear that resolving Jakóbczyk's hypothesis will require fundamental new discoveries concerning the cardinality of the set $\mathcal{W}$.

Finally, if $\mathcal{W} = \{1093, 3511\}$ as conjectured by Nicolas Beeger, the discoverer of the second Wieferich prime, then every Fermat number is square free.

Acknowledgement. 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] D. M. Burton, *Elementary Number Theory*, Seventh Edition, McGraw-Hill Companies, Inc. 2011.

[3] 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 Sect. A* **5** (1951), 97–138.

[4] J. Klaška, Jakóbczyk's hypothesis on Mersenne numbers and generalizations of Skula's theorem, *J. Integer Seq.* **26** (3) (2023), Article 23.3.8.

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

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

[7] P. Ribenboim, On the square factors of the numbers of Fermat and Ferentinou-Nicolacopoulou, *Bull. Greek Math. Soc.* **20** (1979), 81–92.

[8] K. H. Rosen, *Elementary Number Theory and Its Applications*, Sixth Edition, Addison-Wesley, 2011.

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

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