Article

On Diophantine Equations Related to Order of Appearance in Fibonacci Sequence

Pavel Trojovský [ID]

Department of Mathematics, Faculty of Science, University of Hradec Králové,
500 03 Hradec Králové, Czech Republic; pavel.trojovsky@uhk.cz; Tel.: +42-049-333-2860

Abstract: Let F_n be the nth Fibonacci number. Order of appearance $z(n)$ of a natural number n is defined as smallest natural number k, such that n divides F_k. In 1930, Lehmer proved that all solutions of equation $z(n) = n \pm 1$ are prime numbers. In this paper, we solve equation $z(n) = n + \ell$ for $|\ell| \in \{1, \ldots, 9\}$. Our method is based on the p-adic valuation of Fibonacci numbers.

1. Introduction

The study of Diophantine equations was started by Diophantus of Alexandria in around the third century BC. One of the most surprising properties of Diophantine equations is that a slight modification of the original equation could generate much easier or harder equations. See, for example, the proof of the unsolvability of Fermat's equation in 1995 and compare it with a much simpler matter to prove that similar equation $x^n + y^n = z^{n+1}$ has an infinite family of solutions given by

$$x_k = k^n + 1, \ y_k = k(k^n + 1) \text{ and } z_k = k^n + 1, \text{ for all } k \in \mathbb{N} \text{ and } n \geq 2.$$

Since the 20th century, the study of families of Diophantine equations involving recurrence sequences has held a prominent role in theoretical mathematics. A well-known type of linear-recurrence sequence $C(a, b) = (C_n(a, b))_{n \geq 0}$ is defined for all $n \geq 0$ by recurrence $C_{n+2} = C_{n+1} + C_n$, with initial values $C_0 = a$ and $C_1 = b$. Fibonacci sequence $(F_n)_{n \geq 0}$, which corresponds to the choice of $a = 0$ and $b = 1$, is surely the most famous from these sequences (similarly, the well-known Lucas sequence $(L_n)_{n \geq 0}$ is created by choice $a = 2$ and $b = 1$). An excellent result on this subject is related to equation $F_n = x^s$, with $s > 1$, i.e., the problem of finding all perfect powers in the Fibonacci sequence. In fact, this question was a classical problem that attracted much attention during the past 40 years. In 2006, Bugeaud et al. [1] (Theorem 1) confirmed the expectation: the only perfect powers in that sequence are $0, 1, 8$, and 144.

Another popular area of research that has drawn great interest is the study of the divisibility properties of Fibonacci numbers. For example, it is still an open problem if there are infinitely many primes in the Fibonacci sequence (we recommend [2–6]). Let n be a positive integer number, the order (or rank) of appearance of n in the Fibonacci sequence, denoted by $z(n)$, is defined as the smallest positive integer m, such that $n \mid F_m$ (some authors also call it the Fibonacci entry point or order of apparition; see sequence A001177 in [7]). This function can be implemented in software Mathematica ®, see book [8], the following way

```
z[n_]:=Catch[Do[i;If[Mod[Fibonacci[i],n]==0,Throw[i]],{i,2*n}]]
```

Many papers have been devoted to features of this function. Marques [9,10], Luca, and Pomerance [11] studied the local behavior of the rank of appearance in the Fibonacci sequence. Then, considerable effort was made to find the values of function $z(n)$ when there are certain expressions in its argument containing some operations of powers of Fibonacci and Lucas numbers. Values of $z(\prod_{i=0}^{k} L_{n+i})$ were studied by Marques [12], Marques, and Trojovský [13], and Khaochim and Pongsriiam [14]. Similarly, values of $z(\prod_{i=0}^{k} F_{n+i})$ were found by Marques [15], and Khaochim and Pongsriiam [16], and values of $z(F_n^k)$ and $z(L_n^k)$ derived by Marques [17] and Khaochim and Pongsriiam [18]. Recently, Trojovský [19,20] derived for distinct positive integers m, $n < m$ the values of $z(F_m \pm F_n)$ and $z(L_n - L_m)$, when $m \equiv n \pmod 2$ and $m \equiv n \pmod 4$, respectively.

We also remark on the existence of several results related to upper bounds for $z(n)$, for instance, $z(n) < \infty$ for all $n \geq 1$. The proof of this fact is an immediate consequence of the Théorème Fondamental of Section XXVI in [21]. In 1975, Sallé [22] proved that $z(n) \leq 2n$ for all positive integers n. This is the sharpest upper bound for $z(n)$, since, for example, $z(6) = 12$ and $z(30) = 60$. In the case of a prime number p, one has better upper bound $z(p) \leq p + 1$ (Savin [23] proved that, for primes $p \equiv 13, 17 \pmod{20}$ holds $z(p) \mid (p+1)/2$, so $z(p) \leq (p+1)/2$). Equality $z(p) = p + 1$ is achieved for some prime numbers. For instance, this holds for all the following primes:

$$2, 3, 7, 23, 43, 67, 83, 103, 127, 163, 167, 223, 227, 283, 367, \ldots \tag{1}$$

which is OEIS [7] sequence A000057. Amazingly, these primes are the only ones with the property of dividing at least one number in the sequence $C(a, b)$ for all choices of integers a and b (see [24]).

There is no a closed formula for $z(n)$, so Diophantine equations related to $z(n)$ play an important role in the best comprehension of this function. Marques [25], and Somer and Křížek [26] independently proved that all fixed points of function $z(n)$, that is, all solutions of Diophantine equation $z(n) = n$, have form $n = 5^k$ or $12 \cdot 5^k$ for some $k \geq 0$. A question therefore arises: what happens with slightly modified Diophantine equation $z(n) = n + 1$? Is it easier, like our example related to Fermat's equation?

By using *Mathematica*®, we can find out that the first few solutions of equation $z(n) = n + 1$ are equal to primes given in (1). Indeed, all solutions of equations $z(n) = n \pm 1$ are prime numbers. This fact was proven by Lehmer in Theorem 5.1 in [27].

So, a new question arises: what are the solutions of Diophantine equation $z(n) = P(n)$, for a given polynomial $P(x) \in \mathbb{Z}[x]$ with positive coefficients? Before attacking this problem, we must make some considerations. Since $z(n) \leq 2n$, for all $n > 2$, linear monic polynomials are the only ones that can return some solution of $z(n) = P(n)$.

In view of that, in this paper we work on Diophantine equation $z(n) = n + \ell$, for $\ell \in \{\pm 1, \ldots, \pm 9\}$. In fact, our aim was to provide a general method that could be used to solve this equation for any previously fixed integer ℓ.

It is important to emphasize that knowledge of the arithmetic nature of solutions of equations related to $z(n)$ may lead to important pieces in mathematics. For example, to prove that all solutions of equation $z(n) = z(n^2)$ are prime numbers is implied in the first case of Fermat's Last Theorem (see [28]).

To start, since our method is based on usage of the p-adic valuation of Fibonacci numbers, here we present another proof for Lehmer's result (cases $\ell = \pm 1$).

Theorem 1. *Let n be a positive integer such that $z(n) = n \pm 1$; then, n is a prime number.*

Since the solutions of equation $z(n) = n + \ell$ have very different arithmetic behaviors for $\ell = 0$ (numbers with many divisors) and for $\ell = \pm 1$ (prime numbers), which kind of solutions we can expect for $\ell = \pm 2, \ldots, \pm 9$? This is answered in the next results.

Theorem 2. *Let n, ℓ be any positive integers, $\ell \in \{2, 3, 4, 7, 8, 9\}$. The only solutions of Diophantine equation*

$$z(n) = n + \ell \tag{2}$$

are

$$(n, \ell) \in \{(4,2), (9,3), (49,7), (22,8), (27,9)\}.$$

The reader may wonder what happens in cases $\ell = 5$ and 6. While Equation (2) has at most one solution for each $\ell \in \{2,3,4,7,8,9\}$, these remaining cases seem to have infinitely many solutions of a very special form.

Theorem 3. *Solutions of Diophantine equation* (2) *with* $\ell \in \{5,6\}$ *are*

$$\ell = 5 \quad : \quad 5p, \text{ where } p \text{ runs through all primes with } z(p) = p + 1,$$
$$\ell = 6 \quad : \quad 6m, \text{ where } z(m) = (m+1)/2.$$

Note that, contrary to the case of $\ell = 5$, the hypothesis that $n = 6m$ with $z(m) = (m+1)/2$ does not imply that $z(n) = n + 6$. For instance, values of m belonging to $\{17, 53, 137, 173\}$ satisfy $z(m) = (m+1)/2$, but $6m - z(6m) \geq 66$ for all m in the previous set. Indeed, the set of counterexamples is infinite.

Employed methods in the proofs of Theorems 2 and 3 could be used to work with negative values of ℓ (we leave the proof of this theorem to the reader). For instance, it is not a hard matter to similarly prove the two following theorems:

Theorem 4. *Let* n, ℓ *be any positive integer,* $\ell \in \{2,3,4,7,8,9\}$. *The only solutions of Diophantine equation*

$$z(n) = n - \ell \tag{3}$$

are

$$(n, \ell) \in \{(8,2), (16,4), (28,4), (17,8), (32,8)\}.$$

Theorem 5. *The solutions of Diophantine Equation* (3) *with* $\ell \in \{5,6\}$ *are*

$$(n, \ell) \in \{(26,5), (13,6), (18,6)\} \cup \{(\ell p, \ell), \, z(p) = p - 1\}.$$

2. Necessary Properties of Fibonacci Numbers

Lemma 1. *Let* m, n *be any non-negative integer. We have*

(a) $n \mid m$ *if and only if* $F_n \mid F_m$.
(b) *(d'Ocagne's identity)* $(-1)^n F_{m-n} = F_m F_{n+1} - F_n F_{m+1}$.
(c) $F_{p - \left(\frac{5}{p}\right)} \equiv 0 \pmod{p}$, *for all primes* p.

Here, as usual, $\left(\frac{a}{q}\right)$ denotes the Legendre symbol of a with respect to a prime $q > 2$.

Proofs of these statements can be found in [29]. We refer the reader to [30–32] for more details and additional bibliography. The following lemma is a consequence of the previous and the "only if" part of its proof can be found in [10] (see Lemma 2.2c). For the "if" part, it is enough to see that if $z(n) \mid m$, then $n \mid F_{z(n)} \mid F_m$ (by Lemma 1a).

Lemma 2. *Let* m, n *be any positive integer. Then,*

$$n \mid F_m \text{ if and only if } z(n) \mid m.$$

The p-adic order (or valuation) of r, $\nu_p(r)$, is the exponent of the highest power of a prime p that divides r. Throughout the paper, we use the known facts that $\nu_p(ab^\epsilon) = \nu_p(a) + \epsilon\nu_p(b)$, for $\epsilon \in \{-1,1\}$, and that $a \mid b$ if and only if $\nu_p(a) \leq \nu_p(b)$, for all primes p.

The *p*-adic order of Fibonacci numbers was completely characterized (see [33,34]). For instance, from the main result of Lengyel [34] (see a generalization in [35–37]), we can extract the following statement:

Lemma 3. *For $n \geq 1$, we have*

$$
\nu_2(F_n) = \begin{cases}
0, & n \equiv 1,2 \pmod{3}; \\
1, & n \equiv 3 \pmod{6}; \\
3, & n \equiv 6 \pmod{12}; \\
\nu_2(n) + 2, & n \equiv 0 \pmod{12},
\end{cases}
$$

$\nu_5(F_n) = \nu_5(n)$, *and if p is a prime $\neq 2$ or 5, then*

$$
\nu_p(F_n) = \begin{cases}
\nu_p(n) + \nu_p(F_{z(p)}), & \text{if } n \equiv 0 \pmod{z(p)}; \\
0, & \text{if } n \not\equiv 0 \pmod{z(p)}
\end{cases}
$$

A proof of this result can be found in [34].

3. Proof of Our Main Results

To simplify our presentation, from now on we use the usual notation $[a,b] = \{a, a+1, \ldots, b\}$, for some integers a, b, $a < b$.

3.1. Proof of Theorem 1

3.1.1. Case $z(n) = n + 1$

We used the method proof by contradiction. Let us suppose that $n \geq 2$ is a composite number and $z(n) = n + 1$. In particular, $n \mid F_{n+1}$ and we claim that $n + 1$ is also composite. On the contrary, since n is composite, let q be one of its prime factors; thus, $q \mid n \mid F_{n+1}$, and Lemma 2 yields $z(q) \mid n + 1$. One can conclude that $z(q) = n + 1$ (since $n + 1$ is a prime, and $z(q) > 1$), but this conclusion leads to the following absurdity:

$$
n + 1 = z(q) \leq q + 1 < n. \tag{4}
$$

In the last inequality, we used that q is a proper factor of n. Thus, $n + 1$ is composite, as it was claimed. Therefore, we can write $n + 1 = p_1^{a_1} \cdots p_k^{a_k}$ as its factorization in prime numbers, where $a_i \geq 1$, for $i \in [1,k]$. By hypothesis, n is also composite, so we write $n = q_1^{b_1} \cdots q_s^{b_s}$. We can also claim that there is a prime factor p of $n + 1$ such that, if $q \mid n$, then $z(q) \mid (n+1)/p$. Note that this assertion is equivalent to prove the existence of $i \in [1,k]$, such that

$$
z(q_j) \mid \frac{p_1^{a_1} \cdots p_k^{a_k}}{p_i}
$$

holds for all $j \in [1,s]$. To obtain a contradiction, we suppose the contrary. Thus, there is $j \in [1,s]$, such that $z(q_j) \nmid p_i^{-1}(n+1)$, for all $i \in [1,k]$; so,

$$
p_i^{-1}(n+1) = z(q_j)m_i + r_i, \text{ with } 0 < r_i < z(q_j),
$$

for some integers m_i's and r_i's and for all $i \in [1,k]$. Multiplying the above relation by p_i, we get

$$
n + 1 = z(q_j)p_i m_i + p_i r_i \tag{5}
$$

for all $i \in [1, k]$. Since $q_j \mid n \mid F_{n+1}$, the by Lemma 2, one has that $z(q_j) \mid n + 1$. Therefore, Equation (5) implies that $z(q_j) \mid p_i r_i$, for all $i \in [1, k]$. Since $z(q_j) \nmid r_i$ (because $0 < r_i < z(q_j)$), then $z(q_j)$ and p_i cannot be coprime, that is, $\gcd(z(q_j), p_i) = p_i$. In particular, $p_i \mid z(q_j)$, for all $i \in [1, k]$. However, $p_1, \ldots, p_k$ are pairwise coprime; so, $p_1 \cdots p_k \mid z(q_j)$. Let ℓ be a positive integer, such that $z(q_j) = \ell p_1 \cdots p_k$. The proof can be divided into two cases:

Case 1. $\ell = 1$. *In this case,* $z(q_j) = p_1 \cdots p_k$ *and since* $z(q_j) \nmid p_i^{-1}(n+1)$, *we get that* $p_1 \ldots p_k \nmid p_i^{-1}(n+1)$. *Then we can deduce that* $1 > a_i - 1$, *for all* $i \in [1, k]$, *which yields* $a_i = 1$. *In conclusion,*

$$n < n + 1 = p_1 \cdots p_k = z(q_j) \le q_j + 1. \tag{6}$$

This leads to an absurdity since n is a composite number. For that reason, $n \ge \min\{q_j^2, 2q_j\} > q_j + 1$.

Case 2. $\ell > 1$. *In this case, since* $\ell p_1 \cdots p_k \mid n + 1$, *we get* $\ell = p_1^{c_1} \cdots p_k^{c_k}$, *where* $c_i + 1 \le a_i$, *for* $i \in [1, k]$. *Thus* $z(q_j) = p_1^{c_1+1} \cdots p_k^{c_k+1}$, *but keep in mind that* $z(q_j) \nmid p_i^{-1}(n+1)$ *and so* $c_i + 1 > a_i - 1$. *We then conclude that* $a_i - 1 < c_i + 1 \le a_i$ *yielding* $c_i + 1 = a_i$, *for all* $i \in [1, k]$. *Hence,* $z(q_j) = n + 1$ *and, similarly to the previous case, we obtain the following contradiction:*

$$q_j + 1 < n < n + 1 = z(q_j) \le q_j + 1. \tag{7}$$

This completes the proof of our last assertion. Let p be a prime with such property, i.e., such that $z(q) \mid (n+1)/p$ for all prime factors q of n. Suppose that $q \mid n$, then $q \ne 5$ (otherwise, $5 \mid n \mid F_{n+1}$ and 5 would simultaneously divide n and $n + 1$). So, we again need to consider two cases: if $q = 2$, then 2 divides F_{n+1}, and Lemma 3 yields

$$v_2(F_{n+1}) = \begin{cases} 1, & \text{if } n \equiv 2 \pmod{6}; \\ 3, & \text{if } n \equiv 5 \pmod{12}; \\ v_2(n+1) + 2, & \text{if } n \equiv 11 \pmod{12}. \end{cases}$$

Since n is even, then $n \equiv 2 \pmod 6$ implying

$$1 \le v_2(n) \le v_2(F_{n+1}) = 1,$$

so $v_2(n) = 1$. On the other hand, since $3 = z(2) \mid (n+1)/p$, we have

$$v_2\left(F_{\frac{n+1}{p}}\right) \ge 1 = v_2(n).$$

When $q \ne 2$, Lemma 3 gives

$$v_q\left(F_{\frac{n+1}{p}}\right) = v_q\left(\frac{n+1}{p}\right) + v_q(F_{z(q)}) = v_q(F_{z(q)}) \ge v_q(n),$$

where we used that $v_q((n+1)/p) = 0$ (because $q \nmid p(n+1)$) and the fact that $v_q(n) \le v_q(F_{z(q)}) = v_q(F_{n+1})$ (since $n \mid F_{n+1}$).

In conclusion, we obtain $n \mid F_{(n+1)/p}$, which yields (by Lemma 2) the following absurdity:

$$n + 1 = z(n) \mid \frac{n+1}{p} < n + 1.$$

The proof is then complete. $\square$

3.1.2. Case $z(n) = n - 1$

The proof of this case proceeds along the same lines as the proof of Theorem 1, but there is a point that requires extra care. In the previous subsection, we got a contradiction In inequalities (4), (6), and (7) by the fact that they led to absurdity $n + 1 < n$. Using the same approach in the actual case, we do not get a contradiction, as this approach leads to $n - 1 < n$. Thus, to deal with the actual case, we have to replace $z(q_j) = n + 1$ by $z(q_j) = n - 1$ in our proving. Note that $q_j \neq 2$; on the contrary, $3 = z(2) = n - 1$. Thus, $n = 4$, but $z(4) = 6 \neq 4 - 1$. Therefore, $q_j > 2$. So,

$$n = z(q_j) + 1 \leq q_j + 2 < n,$$

where we used that $n \geq \min\{q_j^2, 3q_j\} > q_j + 2$, for $q_j > 2$. Hence, the proof is finished. □

3.2. Proof of Theorem 2

As said before, our goal was to present a method to solve any of these equations. Thus, in order to avoid unnecessary repetition in the proofs, we prove only Theorem 2 for $\ell = 2$, that is, we prove that the only solution of equation $z(n) = n + 2$ is $n = 4$ (we leave to the reader the task of repeating the arguments to obtain a proof for the other cases).

First, we observed that all solutions of $z(n) = n + 2$ are composite numbers (since $z(p) \leq p + 1$ for any prime p).

To derive a contradiction, suppose that $n > 4$ and $z(n) = n + 2$. In particular, $n \mid F_{n+2}$, and we claim that $n + 2$ is also composite. On the contrary, since n is a composite number, let q be one of its prime factors; thus, $q \mid n \mid F_{n+2}$, and Lemma 2 yields $z(q) \mid n + 2$. One concludes that $z(q) = n + 2$ (since $n + 2$ is prime and $z(q) > 1$). However, this leads to the following absurdity:

$$n + 2 = z(q) \leq q + 1 < n + 1. \tag{8}$$

Thus, $n + 2$ is composite as claimed.

Therefore, we can write $n + 2 = p_1^{a_1} \cdots p_k^{a_k}$ as its factorization in prime numbers, where $a_i \geq 1$, for $i \in [1, k]$, and let us write $n = q_1^{b_1} \cdots q_s^{b_s}$. The essential ingredient in our proof is the following fact:

Key fact: *There exists a prime factor p of $n + 2$, such that if $q \mid n$; then, $z(q) \mid (n + 2)/p$.*

Note that this assertion is equivalent to prove the existence of $i \in [1, k]$, such that

$$z(q_j) \mid \frac{p_1^{a_1} \cdots p_k^{a_k}}{p_i}$$

holds for all $j \in [1, s]$.

To obtain a contradiction, we suppose the contrary. Thus, there exists $j \in [1, s]$, such that $z(q_j) \nmid p_i^{-1}(n + 2)$, for all $i \in [1, k]$ and so

$$p_i^{-1}(n + 2) = z(q_j)m_i + r_i, \text{ with } 0 < r_i < z(q_j),$$

for some integers m_i's and r_i's and for all $i \in [1, k]$. Multiplying the above relation by p_i, we get

$$n + 2 = z(q_j)p_i m_i + p_i r_i, \tag{9}$$

for all $i \in [1, k]$. Since $q_j \mid n \mid F_{n+2}$, then by Lemma 2, one has that $z(q_j) \mid n + 2$. Therefore, Equation (9) implies that $z(q_j) \mid p_i r_i$, for all $i \in [1, k]$. Since $z(q_j) \nmid r_i$ (because $0 < r_i < z(q_j)$), then $z(q_j)$ and p_i cannot be coprime, that is, $\gcd(z(q_j), p_i) = p_i$. In particular, $p_i \mid z(q_j)$, for all $i \in [1, k]$. However, $p_1, \ldots, p_k$ are pairwise coprime, so $p_1 \cdots p_k \mid z(q_j)$. Let m be a positive integer, such that $z(q_j) = mp_1 \cdots p_k$. The proof splits into two cases:

Case 3. $m = 1$. *In this case, $z(q_j) = p_1 \cdots p_k$ and since $z(q_j) \nmid p_i^{-1}(n+2)$, we get that $p_1 \ldots p_k \nmid p_i^{-1}(n+2)$. We then deduce that $1 > a_i - 1$, for all $i \in [1, k]$ which yields $a_i = 1$. In conclusion, we obtain the following contradiction:*

$$n + 2 = p_1 \cdots p_k = z(q_j) \leq q_j + 1 < n + 1. \tag{10}$$

Case 4. $m > 1$. *In this case, since $m p_1 \cdots p_k \mid n + 2$, we get $m = p_1^{c_1} \cdots p_k^{c_k}$, where $c_i + 1 \leq a_i$, for $i \in [1, k]$. Thus $z(q_j) = p_1^{c_1+1} \cdots p_k^{c_k+1}$, but keep in mind that $z(q_j) \nmid p_i^{-1}(n+2)$ and so $c_i + 1 > a_i - 1$. We then conclude that $a_i - 1 < c_i + 1 \leq a_i$ yielding $c_i + 1 = a_i$, for all $i \in [1, k]$. Hence $z(q_j) = n + 2$ and similarly to the previous case, we obtain the contradiction that $n + 2 = z(q_j) \leq q_j + 1 < n + 1$. This completes the proof of our key assertion.*

Let p be a prime with such a property, i.e., such that $z(q) \mid (n+2)/p$ for all prime factors q of n. We claim that $n \mid F_{(n+2)/p}$. In fact, suppose that $q \mid n$, then $q \neq 5$ (otherwise, $5 \mid n \mid F_{n+2}$ and 5 would divide both n and $n + 2$). So, we need to consider two cases: if $q \neq 2$, then Lemma 3 gives

$$\nu_q\left(F_{\frac{n+2}{p}}\right) = \nu_q\left(\frac{n+2}{p}\right) + \nu_q(F_{z(q)}) = \nu_q(F_{z(q)}) \geq \nu_q(n),$$

where we used that $\nu_q((n+2)/p) = 0$ (because $q \mid n$ and $\gcd(n, n+2) = 1$ or 2) and the fact that $\nu_q(n) \leq \nu_q(F_{z(q)}) = \nu_q(F_{n+2})$ (since $n \mid F_{n+2}$).

If $q = 2$, then 2 divides both n and $n + 2$. First, let us show that n has odd prime factors (keep in mind that n is composite). In order to prove that, suppose the contrary, i.e., that $n = 2^s$ for some $s > 2$. If $z(n) = n + 2$, then $z(2^s) = 2(2^{s-1} + 1)$. On the other hand, Theorem 1.1i of [17] gives $z(F_m^s) = m F_m^{s-1}/2$ for $m \equiv 3 \pmod 6$ and $s \geq 3$. Taking $m = 3$, we get $z(2^s) = 3 \cdot 2^{s-2}$ leading to equation $2(2^{s-1} + 1) = 3 \cdot 2^{s-2}$, which clearly has no solution for positive integers s (because $s = 3$, but $2^{3-1} + 1 \neq 3$). Summarizing, n has at least one odd prime factor.

In addition, $2 \mid n \mid F_{n+2}$, implying that $3 \mid n + 2$. Therefore, $n + 2 \equiv 0 \pmod 6$. Thus,

$$\nu_2(F_{n+2}) = \begin{cases} 3, & \text{if } n + 2 \equiv 6 \pmod{12}; \\ \nu_2(n+2) + 2, & \text{if } n + 2 \equiv 0 \pmod{12}, \end{cases}$$

When $12 \mid n + 2$, then $\nu_2(n) = 1$. Since $3 \mid (n+2)/p$, then $\nu_2(F_{(n+2)/p}) \geq 1 = \nu_2(n)$. So, the case that requires an extra care is when $n + 2 \equiv 6 \pmod{12}$. In this occasion, we shall claim that the prime p in the key fact can be taken different from 2. Indeed, by repeating the arguments in the proof of that fact, we get $n = 2^{b_1} q_2^{b_2} \cdots q_s^{b_s}$, $n + 2 = 2^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $p_2 \cdots p_k \mid z(q_j)$. Therefore, $z(q_j) = r p_2 \cdots p_k$ for some positive integer r. If $r = 1$, then we obtain $a_i = 1$ for $i \in [2, k]$ and so $n + 2 = 2^{a_1} z(q_j)$. Since $\gcd(n, n+2) = 2$ and $4 \mid n$ (because $n \equiv 4 \pmod{12}$), one has that $a_1 = 1$, leading to the following contradiction:

$$n + 2 = 2 z(q_j) \leq 2(q_j + 1) < n + 2,$$

where, since $q_j > 2$ (otherwise $n = 4$) and $4 \mid n$, then $n \geq 4 q_j > 2 q_j$. Case $r > 1$ can be similarly handled.

Going back to the proof that $n \mid F_{(n+2)/p}$, now supposing $p \neq 2$, we still need to consider two subcases:

First, note that, in any case, $n \mid F_{n+2}$ leads to $\nu_2(n) \leq \nu_2(F_{n+2}) = 3$, for $n + 2 \equiv 6 \pmod{12}$. The last congruence can also be written as $(n+2)/p = 6(2t+1)/p$ for some positive integer t.

Subcase 1. $p > 3$. In this case, p divides $2t + 1$ and so $2t + 1 = hp$, for some odd integer h. Hence, $(n+2)/p \equiv 6h \equiv 6 \pmod{12}$, yielding $\nu_2(F_{(n+2)/p}) = 3 \geq \nu_2(n)$ (by Lemma 3).

Subcase 2. $p = 3$. In this case, we have $(n+2)/3 = 2(2t+1)$. Since $2 \mid n$ implies that $3 \mid (n+2)/3$ (key fact), then 3 divides $2t + 1$ and thus $6 \mid (n+2)/3$. By Lemma 3, $\nu_2(F_{(n+2)/3}) \geq 3 \geq \nu_2(n)$. This finishes the proof that $\nu_2(n) \leq \nu_2(F_{(n+2)/p})$, for some prime p.

In conclusion, we get that $n \mid F_{(n+2)/p}$, which leads (by Lemma 2) to the following absurdity:

$$n + 2 = z(n) \mid \frac{n+2}{p} < n + 2.$$

The proof is then complete. □

3.3. Proof of Theorem 3

Let us only consider the case $\ell = 5$ (case $\ell = 6$ can similarly be handled). The proof splits into two parts:

Part 1. If $n = 5p$, where $z(p) = p + 1$, then $z(n) = n + 5$ (the "if" part). In fact, $5 \mid F_{n+5}$ (because $5 \mid F_m$ if and only if $5 \mid m$); p also divides F_{n+5}, since $z(p) = p + 1 \mid n + 5 = 5(p + 1)$ and so $5p = n \mid F_{n+5}$. To complete the proof, it suffices to prove that $n \mid F_j$ implies $j \geq n + 5$. If $5p = n \mid F_j$, then both 5 and $z(p) = p + 1$ divides j. Therefore, since $\gcd(5, p + 1) = 1$, $5(p + 1) \mid j$ yielding $j \geq 5(p + 1) = n + 5$ as claimed.

Part 2. If $z(n) = n + 5$, then $n = 5p$, where p is a prime number with $z(p) = p + 1$ (the "only if" part). First, we claim that if $z(n) = n + 5$, then $5 \mid n$. On the contrary, i.e., if $5 \nmid n$, we can repeat the same construction as in the proof of the key fact of previous section to find a prime p, such that if $q \mid n$, then $z(q) \mid (n + 5)/p$. Similarly to that section, we would get the absurdity of n dividing $F_{(n+5)/p}$, where the useful here is the fact that if $q \mid n$, then $v_q(p) = 0$, since $\gcd(n, n + 5) = 1$.

Thus, we can write $n = 5^a m$, where $\gcd(5, m) = 1$. Since $n \mid F_{n+5}$, we claim that $a = 1$. In fact, we would otherwise have the following absurdity:

$$1 < a = v_5(n) \leq v_5(F_{n+5}) = v_5(n + 5) = v_5(5(5^{a-1}m + 1)) = 1,$$

where we used Lemma 3. Therefore, $n = 5m$, so it suffices to prove that $z(m) = m + 1$ (since this is implied in the primality of m).

Since $5m \mid F_{5(m+1)}$, then $m \mid F_{5(m+1)}$. Let $q \neq 2$ be a prime factor of n (observe that $q \neq 5$); then, Lemma 3 gives

$$v_q(F_{5(m+1)}) = v_q(5(m + 1)) + v_q(F_{z(q)}) = v_q(m + 1) + v_q(F_{z(q)}) = v_q(F_{m+1}).$$

Thus, $v_q(m) \leq v_q(F_{m+1})$, for all odd primes q. If $q = 2$, we use Lemma 3 together with the fact that

- $3 \mid m + 1$ if and only if $3 \mid 5(m + 1)$
- $m + 1 \equiv 3 \pmod 6$ if and only if $5(m + 1) \equiv 3 \pmod 6$ (since $15 \equiv 3 \pmod 6$)
- $m + 1 \equiv 6 \pmod{12}$ if and only if $5(m + 1) \equiv 6 \pmod{12}$ (since $30 \equiv 6 \pmod{12}$)
- $m + 1 \equiv 0 \pmod{12}$ if and only if $5(m + 1) \equiv 0 \pmod{12}$,

to obtain that $v_2(F_{5(m+1)}) = v_2(F_{m+1})$ and so $v_2(m) \leq v_2(F_{m+1})$.

In conclusion, we proved that $m \mid F_{m+1}$ and, by Lemma 2, $z(m) \mid m + 1$. To derive a contradiction, suppose that $z(m) \neq m + 1$; then, there exists an integer $s > 1$, such that $m \mid F_{(m+1)/s}$. Thus, $5m \mid 5F_{(m+1)/s} \mid F_{5(m+1)/s}$ (where we used Lemma 1d), and we would have the following absurdity, by Lemma 2,

$$n + 5 = z(n) = z(5m) \mid 5\left(\frac{m+1}{s}\right) = \frac{n+5}{s} < n + 5.$$

The proof is then complete. □

4. Conclusions

In this paper, we were interested in function $z(n)$, which is known as the order of appearance of n in the Fibonacci sequence. We used techniques from p-adic valuation to completely describe the arithmetic nature of solutions of equation $z(n) = n + \ell$, for $\ell \in \{\pm 1, \pm 2, \ldots, \pm 9\}$.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Bugeaud, Y.; Mignotte, M.; Siksek, S. Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas powers. *Ann. Math.* **2006**, *163*, 969–1018. [CrossRef]
2. Baker, R.C.; Harman, G.; Pintz, J. The difference between consecutive primes II. *Proc. Lond. Math. Soc.* **2001**, *83*, 532–562. [CrossRef]
3. Goldston, D.A.; Pintz, J.; Yildirim, C.Y. Primes in Tuples I. *Ann. Math.* **2009**, *170*, 819–862. [CrossRef]
4. Granville, A. Different Approaches to the Distribution of Primes. *Milan J. Math.* **2009**, *78*, 1–25. [CrossRef]
5. Kristyan, S. On the statistical distribution of prime numbers: A view from where the distribution of prime numbers are not erratic. *AIP Conf. Proc.* **2017**, *1863*, 560013.
6. Kristyan, S. Note on the cardinality difference between primes and twin primes and its impact on function x/ln(x) in prime number theorem. *AIP Conf. Proc.* **2018**, *1978*, 470064.
7. Sloane, N.J.A. The On-Line Encyclopedia of Integer Sequences. Available online: https://oeis.org/ (accessed on 7 November 2019).
8. Wolfram, S. *The Mathematica Book*, 4th ed.; Wolfram Media/ Cambridge University Press: Cambridge, UK, 1999.
9. Marques, D. On integer numbers with locally smallest order of appearance in the Fibonacci sequence. *Int. J. Math. Math. Sci.* **2011**, *2011*, 407643. [CrossRef]
10. Marques, D. The order of appearance of integers at most one away from Fibonacci numbers. *Fibonacci Quart.* **2012**, *50*, 36–43.
11. Luca, F.; Pomerance, C. On the local behavior of the order of appearance in the Fibonacci sequence. *Int. J. Number Theory* **2014**, *10*, 915–933. [CrossRef]
12. Marques, D. The order of appearance the product of consecutive Lucas numbers. *Fibonacci Quart.* **2013**, *51*, 38–43. [CrossRef]
13. Marques, D.; Trojovský, P. The order of appearance of the product of five consecutive Lucas numbers. *Tatra Mt. Math. Publ.* **2014**, *59*, 65–77. [CrossRef]
14. Khaochim, N.; Pongsriiam, P. The general case on the order of appearance of the product of consecutive Lucas numbers. *Acta Math. Univ. Comenian.* **2018**, *59*, 277–289.
15. Marques, D. The order of appearance of product of consecutive Fibonacci numbers. *Fibonacci Quart.* **2012**, *50*, 132–139.
16. Khaochim, N.; Pongsriiam, P. On the order of appearance of the product of Fibonacci numbers. *Contrib. Discret. Math.* **2018**, *13*, 45–62.
17. Marques, D. The order of appearance of powers of Fibonacci and Lucas numbers. *Fibonacci Quart.* **2012**, *50*, 239–245.
18. Pongsriiam, P. A complete formula for the order of appearance of the powers of Lucas numbers. *Commun. Korean Math. Soc.* **2016**, *31*, 447–450. [CrossRef]
19. Trojovský, P. The order of appearance of the sum and difference between two Fibonacci numbers. *Asian-Eur. J. Math.* **2019**, *12*, 1950046. [CrossRef]
20. Trojovský, P. On the order of appearance of the difference of two Lucas numbers. *Miskolc Math. Notes* **2018**, *19*, 641–648. [CrossRef]

21. Lucas, E. Théorie des fonctions numériques simplement périodiques. *Am. J. Math.* **1878**, *1*, 184–240, 289–321. [CrossRef]

22. Sallé, H.J.A. Maximum value for the rank of apparition of integers in recursive sequences. *Fibonacci Quart.* **1975**, *13*, 159–161.

23. Savin, D. About Special Elements in Quaternion Algebras Over Finite Fields. *Adv. Appl. Clifford Algebr.* **2017**, *27*, 1801–1813 [CrossRef]

24. Alfred, U. Primes which are factors of all Fibonacci sequences. *Fibonacci Quart.* **1964**, *2*, 33–38.

25. Marques, D. Fixed points of the order of appearance in the Fibonacci sequence. *Fibonacci Quart.* **2012**, *50*, 346-352.

26. Somer, L.; Křížek, M. Fixed points and upper bounds for the rank of appearance in Lucas sequences. *Fibonacci Quart.* **2013**, *51*, 291–306.

27. Lehmer, D.H. An extended theory of Lucas' functions. *Ann. Math.* **1930**, *31*, 419–448. [CrossRef]

28. Sun, Z.H.; Sun, Z.W. Fibonacci numbers and Fermat's last theorem. *Acta Arith.* **1992**, *60*, 371–388. [CrossRef]

29. Koshy, T. *Fibonacci and Lucas Numbers with Applications*; Wiley: New York, NY, USA, 2001.

30. Benjamin, A.; Quinn, J. The Fibonacci numbers—Exposed more discretely. *Math. Mag.* **2003**, *76*, 182–192.

31. Kalman, D.; Mena, R. The Fibonacci Numbers–Exposed. *Math. Mag.* **2003**, *76*, 167–181.

32. Ribenboim, P. *My Numbers, My Friends: Popular Lectures on Number Theory*; Springer: New York, NY, USA, 2000.

33. Halton, J.H. On the divisibility properties of Fibonacci numbers. *Fibonacci Quart.* **1966**, *4*, 217–240.

34. Lengyel, T. The order of the Fibonacci and Lucas numbers. *Fibonacci Quart.* **1995**, *33*, 234–239.

35. Kreutz, A.; Lelis, J.; Marques, D.; Silva, E.; Trojovský, P. The p-adic order of the k-Fibonacci and k-Lucas numbers. *p-Adic Numbers Ultrametr. Anal. Appl.* **2017**, *9*, 15–21. [CrossRef]

36. Sanna, C. The p-adic valuation of Lucas sequences. *Fibonacci Quart.* **2016**, *54*, 118–124.

37. Marques, D.; Trojovský, P. The p-adic order of some Fibonomial Coefficients. *J. Integer Seq.* **2015**, *18*, 15.3.1.