RELATING FIBONACCI NUMBERS TO THE INFINITUDES OF CERTAIN PRIMES

John P. Georges
Department of Mathematics, Trinity College, Hartford, Connecticut
john.georges@trincoll.edu

David W. Mauro[1]
Department of Mathematics, Trinity College, Hartford, Connecticut
david.mauro@trincoll.edu

Yan Wang
Department of Mathematics, Millsaps College, Jackson, Mississippi
wangy@millsaps.edu

Received: 8/11/22, Accepted: 2/28/23, Published: 3/24/23

Abstract

Properties of the Fibonacci numbers are used to prove the infinitude of primes of the form $4k + 3$, $8k + 5$ and $12k + 5$. In addition, we give a result on the prime factors of Fibonacci numbers and Lucas numbers.

1. Introduction

Euclid's proof of the infinitude of primes (Elements IX, 20) has played an important role in the development of mathematical thought. It has prompted investigations into the structure of numbers and led to the discovery of deeper results such as the Fundamental Theorem of Arithmetic and the Prime Number Theorem (see [3]). On a less sublime level, minor alterations to Euclid's proof have produced elementary proofs of the infinitude of both $4k + 1$ primes and $4k + 3$ primes. (These results are subsumed under Dirichlet's Theorem (see [2]), the proof of which is decidedly not elementary.)

The infinitude of primes, much like the Pythagorean Theorem, has many different proofs [1]. Generally speaking, these proofs underscore the interconnectedness of mathematical ideas. Wuderlich [8] proved the infinitude of primes by using properties of the Fibonacci numbers; Robbins [6] subsequently used these properties to fashion a proof for the infinitude of $4k + 1$ primes.

DOI:
[1]corresponding author

In this paper, we will explore more deeply the relationship between the Fibonacci numbers and the infinitude of certain primes. In Section 2 we will introduce terminology, notation and useful results about the Fibonacci numbers. In Section 3 we will present proofs of the infinitude of $4k+3$ primes, $8k+5$ primes, and $12k+5$ primes. In addition, we give a result on the prime factors of Fibonacci numbers and Lucas numbers.

2. Terminology, Notation and Preliminary Results

Throughout this paper, unless otherwise specified, sets are collections of positive integers. For an arbitrary set $X = \{x_1, x_2, \dots\}$, $x_i < x_j$ whenever $i < j$. We define $\pi(X)$ to be the collection of all primes appearing as factors of elements in X; thus, $\pi(\mathbb{N})$ is the set of all prime numbers.

Let $\mathbb{F}$ and $\mathbb{L}$ denote the sequence of Fibonacci numbers and Lucas numbers, respectively. For positive integer n, let F_n and L_n denote the nth Fibonacci number and the nth Lucas number, respectively. Recall that $L_n = F_{n-1} + F_{n+1}$ (where $F_0 = 0$); thus, $F_{2n} = F_n(F_{n-1} + F_{n+1}) = F_n L_n$. Furthermore, $\gcd(F_n, L_n) = 1$ if $n \not\equiv 0 \pmod 3$, and $\gcd(F_n, L_n) = 2$ otherwise. We define the mapping $F : X \to \mathbb{F}$ as $F(x_i) = F_{x_i}$, and $F(X)$ as the image of X under F.

We cite below several results intended to facilitate the subsequent presentation.

Theorem 1 ([4]). *For any positive integers m and n, we have* $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

Theorem 2 ([5]). *For any odd positive integer k, if p is an odd prime such that $p \mid F_k$, then $p \equiv 1 \pmod 4$. Moreover, if F_k is even, then $3 \mid k$ and $4 \nmid F_k$.*

Binet's Formula and completing the square can be used to derive the following formula.

Theorem 3. *For positive integers k and n,*

$$F_{(2k+1)n} = F_n \left[\sum_{m=0}^{k-1} (-1)^{mn} 5 F_{(k-m)n}^2 + (-1)^{kn} (2k+1) \right].$$

More than two hundred years ago, Lagrange investigated the behavior of the unit digits of the Fibonacci numbers. He discovered the sequence of these digits was periodic with the length of the period being 60 (equivalently, the sequence of Fibonacci numbers modulo 10 has period of length 60). In 1960, Wall [7] showed that for any positive integer m, the sequence of Fibonacci numbers modulo m is periodic. The above results led to the development and study of such periods, known as Pisano periods. In Table 1 below we provide information about the Pisano

periods associated with $m = 4, 8$, and 12:

m	Period/Length
4	(1, 1, 2, 3, 1, 0)/6
8	(1, 1, 2, 3, 5, 0, 5, 5, 2, 7, 1, 0)/12
12	(1, 1, 2, 3, 5, 8, 1, 9, 10, 7, 5, 0, 5, 5, 10, 3, 1, 4, 5, 9, 2, 11, 1, 0)/24

Table 1. Pisano Periods for $m = 4, 8, 12$.

3. Main Results

In this section we will present proofs of the infinitude of primes of the form $4k+3$, $8k+5$, and $12k+5$. Our general approach will be to use properties of the Fibonacci numbers and modular arithmetic to produce infinite collections of primes of the desired forms.

Theorem 4. *There are infinitely many primes of the form* $4k + 3$.

Proof. Let $X = \{x_i | x_i = 2^{i+1}, i \in \mathbb{N}\}$. We make the following observations:

(1) For each $i \in \mathbb{N}$,

$$F_{x_i} = F_{2^{i+1}} = F_{2(2^i)} = F_{2^i} L_{2^i} = \prod_{j=1}^{i} L_{2^j}.$$

(2) For each $i \in \mathbb{N}$, $3 \nmid 2^i$, implying that $\gcd(F_{2^i}, L_{2^i}) = 1$.

(3) For i odd, $x_i \equiv 4 \pmod 6$ and for i even, $x_i \equiv 2 \pmod 6$. Referring to Table 1, it follows that $F_{x_i} \equiv 3 \pmod 4$ when i is odd and $F_{x_i} \equiv 1 \pmod 4$ when i is even, implying $L_{2^i} \equiv 3 \pmod 4$ for all $i \in \mathbb{N}$.

(4) Since $L_{2^i} \equiv 3 \pmod 4$, each L_{2^i} has at least one prime factor of the form $4k + 3$.

Now let L be the infinite set $\{L_{2^i} | i \in \mathbb{N}\}$. By (4), to show the infinitude of the $4k+3$ primes, it suffices to show that the elements of L are pairwise relatively prime. To that end, suppose to the contrary that there exist positive integers $m < n$ and an integer $d \geq 2$ such that $d \mid L_{2^m}$ and $d \mid L_{2^n}$. Then $d \mid F_{2^n}$ since by (1), F_{2^n} can be expressed as the product $\prod_{j=1}^{n-1} L_{2^j}$ which has the factor L_{2^m}. Hence $d \mid F_{2^n}$ and $d \mid L_{2^n}$, contradicting (2). □

Theorem 5. *There are infinitely many primes of the form* $8k + 5$.

Proof. Let $W_7 = \{w_i | w_i = 7^{i+1}, i \in \mathbb{N}\}$. We make the following observations:

(1) For i odd, $w_i \equiv 1 \pmod{12}$ and for i even, $w_i \equiv 7 \pmod{12}$. Referring to Table 1, it follows that $F(w_i) \equiv 1 \pmod 8$ when i is odd and $F(w_i) \equiv 5 \pmod 8$ when i is even.

(2) By Theorem 3, for each $i \in \mathbb{N}$,

$$F(w_i) = F_{w_i} = F_{7^i}(5F^2_{3(7^i)} - 5F^2_{2(7^i)} + 5F^2_{7^i} - 7) = F_7 \prod_{j=1}^{i} a_j,$$

where $a_j = 5F^2_{3(7^j)} - 5F^2_{2(7^j)} + 5F^2_{7^j} - 7$.

(3) From (1) and (2) above, for each $i \in \mathbb{N}$, $a_i \equiv 5 \pmod 8$. Noting that $F(w_i)$ is odd and a_i is a factor of $F(w_i)$, it follows that all prime divisors of a_i are congruent to 1 modulo 4, implying that a_i has at least one prime divisor of the form $8k + 5$.

(4) From Theorem 1, F_{7^i} is a divisor of both $F_{3(7^i)}$ and $F_{2(7^i)}$. As a result, $\gcd(F_{7^i}, a_i) = \gcd(F_{7^i}, -7)$. Since 7 is a prime of the form $4k+3$, by Theorem 2, $\gcd(F_{7^i}, -7) = 1$. It follows from (2) that the elements of $A = \{a_i, i \in \mathbb{N}\}$ are pairwise relatively prime.

Finally, for each $i \in \mathbb{N}$, by selecting a prime divisor of a_i of the form $8k + 5$, we obtain an infinite collection of $8k + 5$ primes. □

By replacing 7 with any other prime of the form $12k + 7$ (e.g., 19), similar observations will lead to a proof of Theorem 5. Note that $\pi(F(W_7))$ and $\pi(F(W_{19}))$ are disjoint.

Theorem 6. *There are infinitely many primes of the form* $12k + 5$.

Proof. Let $V_{11} = \{v_i | v_i = 11^{i+1}, i \in \mathbb{N}\}$. By Theorem 3, we have

$$F(v_i) = F_{11^i}\left[\sum_{m=0}^{4}(-1)^m 5F^2_{(5-m)11^i} - 11\right] = F_{11^i} b_i = F_{11} \prod_{j=1}^{i} b_j.$$

Similarly to the methods used in the proof of Theorem 5, it may be argued that for i odd, $F(v_i) \equiv 1 \pmod{12}$ and for i even, $F(v_i) \equiv 5 \pmod{12}$; that each b_i possesses a prime divisor of the form $12k + 5$; and that F_{11^i} and b_i are relatively prime. Hence, it follows that $\pi(F(V_{11}))$ contains infinitely many primes of the form $12k + 5$. □

By replacing 11 with any other prime of the form $24k + 11$ (e.g., 59), similar observations will lead to a proof of Theorem 6. Note that $\pi(F(V_{11}))$ and $\pi(F(V_{59}))$ are disjoint.

A consequence of Wall's Theorem [7] is that any prime divides some Fibonacci number; that is, $\pi(\mathbb{N}) = \pi(\mathbb{F})$. The following theorem further relates $\pi(\mathbb{N})$ to $\mathbb{F}$ and $\mathbb{L}$.

Theorem 7. *Let F_{odd} and F_{even} denote the sets of Fibonacci numbers with odd subscripts and even subscripts, respectively. Then*

1. $\pi(F_{even}) = \pi(\mathbb{N})$,
2. $\pi(F_{odd}) \cup \pi(\mathbb{L}) = \pi(\mathbb{N})$,
3. $\pi(F_{odd}) \cap \pi(\mathbb{L}) = \{2\}$.

Proof. Note that for any odd i, $F_i \mid F_{2i}$, implying that $\pi(F_{odd}) \subseteq \pi(F_{even})$. Since $\pi(F_{odd} \cup F_{even}) = \pi(\mathbb{N})$, (1) follows.

To prove (2), we observe that for every prime p, p divides some element of F_{even}. Let $p \mid F_{2^t w}$, where $t \geq 1$ and w is odd. Then $p \mid F_w L_w L_{2w} \cdots L_{2^{t-1}w}$; that is, $p \in \pi(F_{odd})$ or $p \in \pi(\mathbb{L})$.

To prove (3), suppose to the contrary that there exists an odd prime $q \in \pi(F_{odd}) \cap \pi(\mathbb{L})$. Let b be the smallest odd integer such that $q \mid F_b$ and $q \mid L_j$ for some integer j. Since $q \mid L_j$, q divides $F_j L_j (= F_{2j})$. By the choice of b and Theorem 1, $b \mid 2j$, which implies $b \mid j$. Thus $q \mid F_j$ and $q \mid L_j$, a contradiction. To complete the proof, 2 divides both F_3 and L_3. □

We point out that Theorem 7 gives a bipartition of the set of odd primes. We also note that primes of the form $4k + 3$ are elements of $\pi(\mathbb{L})$, but not all primes of the form $4k + 1$ are elements of $\pi(F_{odd})$ (e.g., $29, 41, \ldots$).

References

[1] M. Aigner and G. Ziegler, *Proofs from THE BOOK (4th ed.),* Springer-Verlag, Berlin, New York, 2009.

[2] P. G. L. Dirichlet, Beweis des satzes, dass jede unbegrenzte arithmetische progression, deren erstes glied und differenz ganze zahlen ohne gemeinschaftlichen factor sind, unendlich viele primzahlen enthält [Proof of the theorem that every unbounded arithmetic progression, whose first term and common difference are integers without common factors, contains infinitely many prime numbers], *Abhandlungen der Königlichen Preußischen Akademie der Wissenschaften zu Berlin,* 48 (1837), 45–71.

[3] G. H. Hardy, *A Mathematician's Apology,* Cambridge University Press, 1940.

[4] T. Koshy, *Fibonacci and Lucas Numbers with Applications,* Wiley, New York, 2001.

[5] F. Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein,* Springer Monographs in Mathematics, New York, 2000.

[6] N. Robbins, On Fibonacci numbers and primes of the form 4k+1, *Fibonacci Quart.* **32** (1994), 15–16.

[7] D. D. Wall, Fibonacci series modulo m, *Amer. Math. Monthly* **67** (1960), 525-532. doi.org/10.2307/2309169

[8] M. Wunderlich, Another proof of the infinite primes theorem, *Amer. Math. Monthly* **72** (1965), 305. doi.org/10.2307/2313710