EXACT DIVISIBILITY PROPERTIES OF SOME SUBSEQUENCES OF FIBONACCI NUMBERS

CHATCHAWAN PANRAKSA, ARAM TANGBOONDUANGJIT, AND KENG WIBOONTON

Abstract. For each positive integer n, we consider the following sequence of numbers

$$F(n), \quad F(nF(n)), \quad F(nF(nF(n))), \quad \dots,$$

where $F(n)$ is the nth Fibonacci number defined in the usual way. Let $G_k(n)$ be the kth term of this sequence. We prove that $F(n)^k \parallel G_k(n)$ for all positive integers k and n with $n > 3$. For the first nontrivial case when $n = 3$, we prove that $F(3)^{2k-1} \parallel G_k(3)$ for all positive integers k. We also provide an alternative proof of the divisibility of $G_k(n)$ by $F(n)^k$ first proved by two authors of this work. Finally, we give explicit formulas of the quotients obtained from dividing $G_k(n)$ by $F(n)^k$ for the cases when $k = 2$ and $k = 3$.

1. Introduction

Perhaps one of the most studied sequences of natural numbers is the Fibonacci sequence $(F(n))$ which is defined by

$$F(0) = 0, \quad F(1) = 1, \quad \text{and} \quad F(n) = F(n-1) + F(n-2) \quad \text{for } n \geq 2.$$

In this paper, we form a subsequence $(G_k(n))$ of the Fibonacci sequence as follows: for each nonnegative integer n, let

$$G_1(n) = F(n) \quad \text{and} \quad G_k(n) = F\big(nG_{k-1}(n)\big) \quad \text{for } k \geq 2.$$

For instance, the first few terms of this sequence are $F(n)$, $F(nF(n))$, $F(nF(nF(n)))$. A well-known theorem states that the Fibonacci sequence is a divisibility sequence, i.e., if $m \mid n$, then $F(m) \mid F(n)$. It follows immediately from this theorem that $F(n) \mid G_k(n)$ for all positive integers n and k. However, Tangboonduangjit and Wiboonton [6] asserted that higher powers of $F(n)$ are present in $G_k(n)$. In fact, they proved the following: $F(n)^k \mid G_k(n)$ for all positive integers n and k. At this point, a natural question arises as to whether $F(n)^k$ is the highest power of $F(n)$ that can divide $G_k(n)$. This paper answers the question in the affirmative for the case when $n > 3$. In Section 2, we provide a number of lemmas that are keys to achieve our goal. We prove the main results in Section 3 as well as offer an alternative proof of the main theorem first proved in [6]. Finally, in Section 4, we provide concrete examples of our main results by deriving explicit formulas of the quotients upon dividing $G_k(n)$ by $F(n)^k$ for the cases when $k = 2$ and $k = 3$. From these formulas, we see that the quotients have nonzero remainders modulo $F(n)$ when $n > 3$.

2. Preliminaries

The following lemma (see [7]) allows us to express $F(kn + r)$ as the sum of products of the lower terms of Fibonacci numbers and will prove extremely useful in proving some other lemmas and main results.

Research fully supported by the Faculty of Science, Mahidol University.

Lemma 2.1. *Let n and k be positive integers, and r a nonnegative integer. Then*

$$F(kn+r) = \sum_{j=0}^{k} \binom{k}{j} F(n)^j F(n-1)^{k-j} F(r+j),$$

where we interpret 0^0 in the summand to be 1 for the case when $n = 1$.

We also need the following standard results about Fibonacci numbers (see [1]).

Lemma 2.2. *Let m and n be positive integers. Then*

(a) *(Cassini's identity) $F(n-1)F(n+1) - F(n)^2 = (-1)^n$.*
(b) $\gcd\big(F(m), F(n)\big) = F\big(\gcd(m,n)\big)$.
(c) *If $F(n) \mid F(m)$ and $n \geq 3$, then $n \mid m$.*
(d) *If $n \mid m$, then $F(n) \mid F(m)$.*
(e) *$F(2n) = F(n)L(n)$, where $L(n)$ are Lucas numbers defined by $L(n) = F(n)+2F(n-1)$.*

The following lemma was used by Matijasevich [3, 4, 5] as one of the key steps to resolve Hilbert's 10th problem.

Lemma 2.3. [6] *Let $n \neq 2$ and m be positive integers. Then*

$$F(n)^2 \mid F(m) \quad \textit{if and only if} \quad nF(n) \mid m.$$

Next we have a corollary of the above lemma.

Lemma 2.4. *Let n and m be positive integers. If $3 \mid n$, then*

$$\frac{F(n)^2}{2} \,\Big|\, F(m) \quad \textit{if and only if} \quad \frac{nF(n)}{2} \,\Big|\, m.$$

Proof. Since $3 \mid n$, Lemma 2.2(d) implies that $2 = F(3)$ divides $F(n)$. Thus, $F(n)$ is even. Suppose that

$$\frac{nF(n)}{2} \,\Big|\, m, \quad \text{so that} \quad nF(n) \mid 2m.$$

By Lemma 2.3, the last statement implies

$$F(n)^2 \mid F(2m).$$

Now since $\frac{nF(n)}{2}$ divides m and $F(n)$ is even, it follows that $n \mid m$. Thus, $F(n) \mid F(m)$ by Lemma 2.2(d) and since $F(n)$ is even, this also implies that $F(m)$ is even. Since $L(m) = F(m) + 2F(m-1)$, it follows that $L(m)$ is even. We therefore obtain

$$F(n)^2 \mid F(2m) \Rightarrow F(n)^2 \mid F(m)L(m) \Rightarrow F(n) \,\Big|\, \frac{F(m)}{F(n)} L(m) \Rightarrow \frac{F(n)}{2} \,\Big|\, \frac{F(m)}{F(n)} \frac{L(m)}{2}, \tag{2.1}$$

where the first implication follows from Lemma 2.2(e). Let

$$d = \gcd\Big(\frac{F(m)}{2}, \frac{L(m)}{2}\Big).$$

Then the definition of $L(m)$ implies that $d \mid F(m-1)$, so that $2d \mid 2F(m-1)$. Since d divides $\frac{F(m)}{2}$, we have $2d \mid F(m)$. Thus, $2d \mid \gcd(F(m), 2F(m-1))$. Now, since $\gcd(F(m), F(m-$

$1)) = 1$ and $F(m)$ is even, we have $\gcd(F(m), 2F(m-1)) = 2$ and therefore $d = 1$. Since $\frac{F(n)}{2}$ divides $\frac{F(m)}{2}$, it follows that

$$\gcd\left(\frac{F(n)}{2}, \frac{L(m)}{2}\right) = 1.$$

Hence,

$$\frac{F(n)}{2} \,\Big|\, \frac{F(m)}{F(n)}\frac{L(m)}{2} \Rightarrow \frac{F(n)}{2} \,\Big|\, \frac{F(m)}{F(n)} \Rightarrow \frac{F(n)^2}{2} \,\Big|\, F(m). \tag{2.2}$$

Now we suppose that

$$\frac{F(n)^2}{2} \,\Big|\, F(m).$$

Then since $F(n)$ is even, we have $F(n) \mid F(m)$. Since $3 \mid n$, it follows that $n \geq 3$ and by Lemma 2.2(c) we have $n \mid m$. Consequently, by the same argument above, $F(m)$ and therefore $L(m)$ is even. Hence the chains of implications (2.1) and (2.2) can all be reversed, so that

$$\frac{F(n)^2}{2} \,\Big|\, F(m) \Rightarrow F(n)^2 \mid F(2m).$$

By Lemma 2.3 and the fact that $F(n)$ is even, we have

$$F(n)^2 \mid F(2m) \Rightarrow nF(n) \mid 2m \Rightarrow \frac{nF(n)}{2} \,\Big|\, m.$$

Thus the proof is complete. □

Lemma 2.5. *Let n be a positive integer. Then $F(n-1)^2 \equiv F(n+1)^2 \equiv (-1)^n \pmod{F(n)}$.*

Proof. This follows immediately from Cassini's Identity and the fact that $F(n-1) \equiv F(n+1) \pmod{F(n)}$. □

Lemma 2.6. *Let n be a positive integer such that $n \geq 3$. Then $F(n-3) = 2F(n-1) - F(n)$.*

Proof. Let n be a positive integer such that $n \geq 3$. By definition, $F(n) = F(n-1) + F(n-2)$ and $F(n-1) = F(n-2) + F(n-3)$. Subtracting these two equations, we find $F(n) - F(n-1) = F(n-1) - F(n-3)$, or equivalently,

$$F(n-3) = 2F(n-1) - F(n).$$

□

Lemma 2.7. *Let n be a positive integer such that $3 \nmid n$ and $2 \nmid n$. Then*

(a) $F(n) \equiv 1 \pmod 4$.
(b) $F(n-1)^{F(n)-1} \equiv 1 \pmod{F(n)}$.

Proof. By hypothesis, $n \equiv 1$ or $5 \pmod 6$. For the case in which $n \equiv 1 \pmod 6$, we write $n = 6k + 1$ where k is a nonnegative integer. Then from Lemma 2.1 we have

$$F(n) = F(6k+1) = \sum_{j=0}^{k} \binom{k}{j} 8^j 5^{k-j} F(1+j) = 5^k F(1) + 8\ell = 5^k + 8\ell,$$

where ℓ is a nonnegative integer. Now since $5^k \equiv 1 \pmod 4$, it follows that $F(n) \equiv 1 \pmod 4$. Similarly, for the case in which $n \equiv 5 \pmod 6$, by writing $n = 6k+5$ where k is a nonnegative integer and by appealing to the same lemma as before, we have

$$F(n) = F(6k+5) = \sum_{j=0}^{k} \binom{k}{j} 8^j 5^{k-j} F(5+j) = 5^k F(5) + 8\ell = 5^{k+1} + 8\ell,$$

where ℓ is a nonnegative integer. Therefore, $F(n) \equiv 1 \pmod 4$ in this case as well. This proves (a). To prove (b), we use Lemma 2.5 together with part (a) to conclude that there exists a nonnegative integer k such that

$$F(n-1)^{F(n)-1} = F(n-1)^{4k} = \big(F(n-1)^2\big)^{2k} \equiv \big((-1)^n\big)^{2k} = (-1)^{2k} \equiv 1 \pmod{F(n)}.$$

□

Lemma 2.8. *Let n be a positive integer. If $2 \nmid n$ and $3 \mid n$, then $F(n) \equiv 2 \pmod 4$.*

Proof. Since $3 \mid n$, it follows from Lemma 2.2 that $F(n)$ is even. This implies that $F(n) \equiv 0 \pmod 4$ or $F(n) \equiv 2 \pmod 4$. Assume the former case. Then by Lemma 2.2 we have

$$\gcd\big(F(n), 8\big) = \gcd\big(F(n), F(6)\big) = F\big(\gcd(n,6)\big) = F(3) = 2.$$

Since $4 \mid \gcd\big(F(n), 8\big)$, it follows that $4 \mid 2$, which is a contradiction. Hence, $F(n) \equiv 2 \pmod 4$. □

Lemma 2.9. *Let r and m be positive integers. If m is odd, then $2^{r+2} \mid\mid F(3 \cdot m \cdot 2^r)$.*

Proof. Assume that m is odd. The proof is by induction on r. When $r = 1$ the statement is $2^3 \mid\mid F(3 \cdot m \cdot 2)$ or $8 \mid\mid F(6 \cdot m)$ which is true since

$$\gcd(F(6 \cdot m), 2^4 3^2) = \gcd(F(6 \cdot m), F(12)) = F(\gcd(6 \cdot m, 12)) = F(6) = 2^3.$$

Now we assume that the statement is true for some integer $k \geq 1$. Then by Lemma 2.2(e) and the induction hypothesis we have

$$F(3 \cdot m \cdot 2^{k+1}) = F\big(2(3 \cdot m \cdot 2^k)\big) = F(3 \cdot m \cdot 2^k) L(3 \cdot m \cdot 2^k) = 2^{k+2} c_k L(3 \cdot m \cdot 2^k),$$

where c_k is an odd integer. It follows from Lemma 2.2 that $2 \mid\mid L(3 \cdot m \cdot 2^k)$. Consequently, $2^{k+3} \mid\mid F(3 \cdot m \cdot 2^{k+1})$. This completes our proof by induction. □

Lemma 2.10. *Let k be a positive integer. Then $2^{2k-1} \mid\mid G_k(3)$.*

Proof. We prove by induction on k. For $k = 1$ the statement is $2 \mid\mid G_1(3)$ which is true by inspection. Now assume that the statement is true for some positive integer k, that is, $G_k(3) = m \cdot 2^{2k-1}$ for some positive odd integer m. Then Lemma 2.2(c) implies that

$$G_{k+1}(3) = F\big(3G_k(3)\big) = F(3m \cdot 2^{2k-1}).$$

By Lemma 2.9, $2^{(2k-1)+2} \mid\mid F(3 \cdot m \cdot 2^{2k-1})$. Therefore, $2^{2(k+1)-1} \mid\mid G_{k+1}(3)$. Hence the proof by induction is complete. □

From the above Lemma, we can also conclude that $2^{2k-1} \mid G_k(n)$ for all positive integers k and n in which $3|n$.

Lemma 2.11. *Let m, ℓ, and k be positive integers with $m \geq 2$ and $\ell \geq 3$. Then*

$$m^{k+2} \,\Bigg|\, \binom{m^k}{\ell} m^\ell.$$

Proof. By Hermite's Divisibility Theorem (see [2, pp. 9-10]) which states that

$$\frac{n}{\gcd(n,k)} \,\Big|\, \binom{n}{k},$$

where n and k are positive integers, we have

$$m^k \,\Big|\, \binom{m^k}{\ell} \gcd(m^k, \ell).$$

So it suffices to show that $\gcd(m^k, \ell) \mid m^{\ell-2}$. Let p be a prime number and r a positive integer such that $p^r \,||\, \gcd(m^k, \ell)$. Then

$$m^k = p^{r+i}c_1 \quad \text{and} \quad \ell = p^{r+j}c_2,$$

where $i, j \geq 0$ and $\gcd(p, c_1) = \gcd(p, c_2) = 1$. We must show that $p^r \mid m^{\ell-2}$. This is equivalent to showing that r is no greater than the largest exponent s of p such that $p^s \mid m^{\ell-2}$. We see that

$$s = \frac{r+i}{k}(p^{r+j}c_2 - 2).$$

Now since $\dfrac{r+i}{k} \geq 1$, it suffices to show that $r \leq p^{r+j}c_2 - 2$. Since $\ell \geq 3$, the statement is true when $r = 1$ so we may assume that $r \geq 2$. Then

$$p^{r+j}c_2 - 2 \geq p^r - 2 \geq 2^r - 2 \geq r.$$

Hence, $r \leq s$ as desired and the proof is now complete. □

3. Exact Divisibility

The divisibility of $G_k(n)$ by $F(n)^k$ was already proved in the paper of the similar title by two of the authors. In this section, we provide an alternative proof of that same theorem and prove further that the divisibility of $G_k(n)$ by $F(n)^k$ is in fact exact for all positive integers n and k with $n > 3$. We start by proving a general result on divisibility of a power of a Fibonacci number into another Fibonacci number.

Lemma 3.1. *Let n and k be positive integers. Then*

$$F(n)^{k+1} \mid F(nF(n)^k).$$

Proof. By Lemma 2.1, we have

$$F(nF(n)^k) = \sum_{\ell=1}^{p} \binom{p}{\ell} F(n)^\ell F(n-1)^{p-\ell} F(\ell),$$

where $p = F(n)^k$. It is easy to see that $F(n)^{k+1}$ divides $\binom{p}{\ell}F(n)^\ell$ for $\ell = 1$ and $\ell = 2$ and by Lemma 2.11, $F(n)^{k+1}$ divides $\binom{p}{\ell}F(n)^\ell$ for each $\ell = 3, \ldots, p$. Therefore, $F(n)^{k+1}$ divides $F(nF(n)^k)$ as desired. □

Theorem 3.2. [6] *Let n and k be positive integers. Then*

$$F(n)^k \mid G_k(n).$$

Proof. Let a positive integer n be given. We prove by induction on k. For $k = 1$ the statement is $F(n) \mid G_1(n)$ which is obvious since $G_1(n) = F(n)$. Now we assume that $F(n)^k \mid G_k(n)$ for some positive integer k. Then $G_k(n) = mF(n)^k$ for some positive integer m. Consequently,

$$G_{k+1}(n) = F\big(nG_k(n)\big) = F(nmF(n)^k)$$

is divisible by $F(n)^{k+1}$ by Lemma 3.1 and Lemma 2.2(d). Therefore, $F(n)^{k+1}$ divides $G_{k+1}(n)$. Since the positive integer n was arbitrary, we conclude that $F(n)^k \mid G_k(n)$ for all positive integers n and k. □

Theorem 3.3. *Let n and k be positive integers.*

(a) *If $n = 1$ or 2, then $G_k(n) = 1$.*

(b) *If $n = 3$, then $F(n)^{2k-1} \,||\, G_k(n)$.*

(c) *If $n > 3$, then $F(n)^k \,||\, G_k(n)$.*

Proof. For $n = 1$ or 2, it is trivial. For $n = 3$, the result follows from Lemma 2.10. Let a positive integer $n > 3$ be fixed. We prove by induction on k. For $k = 1$, the statement is trivial since $G_1(n) = F(n)$ and for $k = 2$, the statement follows from Theorem 4.1 in the next section. Assume that the statement holds for some integer $k \geq 2$. Then, by the division algorithm, $G_k(n) = qF(n)^{k+1} + r$, where q and r are positive integers with $1 \leq r < F(n)^{k+1}$. Now since $F(n)^k \mid G_k(n)$ by Theorem 3.2 above, it follows that $r = jF(n)^k$ for some positive integer j with $1 \leq j < F(n)$. Hence we can express $G_{k+1}(n)$ as follows:

$$\begin{aligned} G_{k+1}(n) &= F\big(nG_k(n)\big) \\ &= F\big(qnF(n)^{k+1} + jnF(n)^k)\big) \\ &= F\big(qnF(n)^{k+1} + 1\big)F\big(jnF(n)^k\big) + F\big(qnF(n)^{k+1}\big)F\big(jnF(n)^k - 1\big), \end{aligned}$$

where we apply Lemma 2.1 in the last equality. Lemma 3.1 and Lemma 2.2(d) imply that $F(n)^{k+2}$ divides $F\big(qnF(n)^{k+1}\big)$. Moreover, by Lemma 2.2(b), we have

$$\gcd\big(F(n), F\big(qnF(n)^{k+1} + 1\big)\big) = F\big(\gcd(n, qnF(n)^{k+1} + 1)\big) = F(1) = 1.$$

It therefore suffices to show that $F(n)^{k+2}$ does not divide $F\big(jnF(n)^k\big)$ for each $1 \leq j < F(n)$. By Lemma 2.1 we have

$$F\big(jnF(n)^k\big) = \sum_{\ell=1}^{p} \binom{p}{\ell} F(jn)^\ell F(jn-1)^{p-\ell} F(\ell), \tag{3.1}$$

where $p = F(n)^k$. For $\ell > 2$, it follows from Lemma 2.11 that $F(n)^{k+2}$ divides $\binom{p}{\ell}F(jn)^\ell$. Therefore it suffices to show that $F(n)^{k+2}$ does not divide the sum of the first two terms on the right-hand side of equation (3.1). This sum can be expressed as follows:

$$F(n)^k F(jn) F(jn-1)^{F(n)^k-1} + \frac{1}{2} F(n)^k \big(F(n)^k - 1\big) F(jn)^2 F(jn-1)^{F(n)^k-2} = A + B,$$

where A and B denote the first and second summand, respectively. We consider two cases.

Case 1. Suppose that $F(n)$ is odd. Then $F(n)^{k+2} \mid B$ and since $j < F(n)$, by Lemma 2.3, it follows that $F(n)^2 \nmid F(jn)$. Hence, $F(n)^{k+2} \nmid (A + B)$.

Case 2. Suppose that $F(n)$ is even. Assume that $F(n)^{k+2} \mid (A+B)$. Then $\frac{1}{2}F(n)^{k+2}$ divides $A+B$. Now since $\frac{1}{2}F(n)^{k+2}$ divides B, it follows that $\frac{1}{2}F(n)^{k+2}$ divides A, so that $\frac{1}{2}F(n)^2$ divides $F(jn)$. By Lemma 2.4, we have that $\frac{1}{2}nF(n)$ divides jn. Since $1 \le j < F(n)$, this implies $j = \frac{1}{2}F(n)$. We consider two more subcases.

Case 2.1. Suppose that $j = \frac{1}{2}F(n)$ is even. Then since $\frac{1}{2}F(n)^2$ divides $F(jn)$, we have $F(jn) = 2a_jF(n)$ for some positive integer a_j. Thus, $F(n)^{k+2} \mid B$. This implies that $F(n)^{k+2} \mid A$. Hence, $F(n)^2 \mid F(jn)$. Since $n > 3$, it follows from Lemma 2.3 that $nF(n) \mid nj$ or $F(n) \mid j$, which is a contradiction to the fact that $j < F(n)$.

Case 2.2. Suppose that $j = \frac{1}{2}F(n)$ is odd. Then $F(n) = 2(2m+1)$ for some positive integer m. Since

$$G_k(n) = qF(n)^{k+1} + jF(n)^k = F(n)^k(qF(n)+j),$$

it follows that $2^k \mid\mid G_k(n)$. This contradicts Lemma 2.10.

We have contradictions for both of the cases and therefore $F(n)^{k+2} \nmid (A+B)$. In all cases, we have $F(n)^{k+2} \nmid (A+B)$ and hence, the proof is complete. □

4. The Quotient Formulas

In this section, we provide the explicit formulas of the quotients upon dividing $G_k(n)$ by $F(n)^k$ for the cases when $k=2$ and $k=3$.

4.1. The Case $k = 2$.

Theorem 4.1. *Let $n \ge 3$ be a positive integer. Then*

$$\frac{G_2(n)}{F(n)^2} = \frac{F\big(nF(n)\big)}{F(n)^2} \equiv \begin{cases} \frac{1}{2}F(n-3) & \text{if } 3 \mid n, \\ 1 & \text{if } 3 \nmid n, \end{cases}$$

where the congruence is taken modulo $F(n)$.

Proof. By Theorem 3.2 we know that $G_2(n)/F(n)^2$ is an integer. By Lemma 2.1 we have

$$\frac{G_2(n)}{F(n)^2} = \frac{F\big(nF(n)\big)}{F(n)^2} = \sum_{j=1}^{F(n)} \binom{F(n)}{j} F(j)F(n)^{j-2}F(n-1)^{F(n)-j}.$$

Taken modulo $F(n)$, this sum reduces to

$$F(n-1)^{F(n)-1} + \binom{F(n)}{2} F(n-1)^{F(n)-2}.$$

For convenience, we let

$$A = F(n-1)^{F(n)-1} \quad \text{and} \quad B = \binom{F(n)}{2} F(n-1)^{F(n)-2} = \frac{1}{2}F(n)\big(F(n)-1\big)F(n-1)^{F(n)-2}$$

and consider the following three cases.

Case 1. Suppose that $3 \mid n$ and $2 \mid n$. By Lemma 2.2(d) we have $F(3) \mid F(n)$ or $2 \mid F(n)$. Since $6 \mid n$, we have again by Lemma 2.2(d) that $F(6) \mid F(n)$ or $8 \mid F(n)$. By Lemma 2.5 we have

$$A = F(n-1)^{F(n)-2} \cdot F(n-1) = \big(F(n-1)^2\big)^{\frac{F(n)-2}{2}} \cdot F(n-1) \equiv F(n-1) \pmod{F(n)}$$

and, by the same token,

$$B \equiv \frac{1}{2}F(n)\big(F(n)-1\big) \pmod{F(n)}.$$

Thus,

$$\begin{aligned} A+B &\equiv F(n-1) + \frac{1}{2}F(n)\big(F(n)-1\big) \equiv \frac{1}{2}\big(2F(n-1) + F(n)^2 - F(n)\big) \\ &\equiv \frac{1}{2}F(n-3) + \frac{1}{2}F(n)^2 \equiv \frac{1}{2}F(n-3) \pmod{F(n)}, \end{aligned}$$

where we have used Lemma 2.6 in the penultimate congruence.

Case 2. Suppose that $3 \mid n$ and $2 \nmid n$. By Lemma 2.8 there exists a nonnegative integer k such that $F(n) = 4k+2$. Thus by Lemma 2.5

$$F(n-1)^{F(n)-2} = F(n-1)^{4k} = \big(F(n-1)^2\big)^{2k} \equiv (-1)^{2k} \equiv 1 \pmod{F(n)}.$$

By the same argument as in the previous case, it follows that

$$\begin{aligned} A+B &= F(n-1)^{F(n)-2}\Big(F(n-1) + \frac{1}{2}F(n)\big(F(n)-1\big)\Big) \equiv F(n-1) + \frac{1}{2}F(n)\big(F(n)-1\big) \\ &\equiv \frac{1}{2}F(n-3) \pmod{F(n)}. \end{aligned}$$

From Cases 1 and 2, we therefore conclude that if $3 \mid n$, then

$$\frac{G_2(n)}{F(n)^2} \equiv \frac{1}{2}F(n-3) \pmod{F(n)}.$$

Case 3. Suppose that $3 \nmid n$. By Lemma 2.2(c) $F(n)$ is odd so that 2 divides $F(n)-1$ and therefore $B \equiv 0 \pmod{F(n)}$. For the case in which $2 \mid n$, we have

$$A = F(n-1)^{F(n)-1} = \big(F(n-1)^2\big)^{\frac{F(n)-1}{2}} \equiv 1 \pmod{F(n)}.$$

For the case in which $2 \nmid n$, it follows from Lemma 2.7 that

$$A = F(n-1)^{F(n)-1} \equiv 1 \pmod{F(n)}.$$

In either case, we see that $A \equiv 1 \pmod{F(n)}$. Thus, $A + B \equiv 1 + 0 \equiv 1 \pmod{F(n)}$.

From Case 3, we therefore conclude that if $3 \nmid n$, then

$$\frac{G_2(n)}{F(n)^2} \equiv 1 \pmod{F(n)}.$$

Hence the proof is complete. □

4.2. **The Case $k = 3$.**

Theorem 4.2. *Let $n \geq 3$ be a positive integer. Then*

$$\frac{G_3(n)}{F(n)^3} = \frac{F\Big(nF\big(nF(n)\big)\Big)}{F(n)^3} \equiv \begin{cases} 1 & \text{if } 3 \nmid n \text{ and } 4 \nmid n, \\ F(n-1) & \text{if } 3 \nmid n \text{ and } 4 \mid n, \\ \frac{(-1)^n}{4} F(n-3)^2 & \text{if } 3 \mid n, \end{cases}$$

where the congruence is taken modulo $F(n)$.

Proof. We proceed in a similar manner as the proof for the case in which $k = 2$. By Lemma 2.1 we have

$$\begin{aligned} \frac{G_3(n)}{F(n)^3} &= \sum_{j=1}^{G_2(n)} \binom{G_2(n)}{j} F(j) F(n)^{j-3} F(n-1)^{G_2(n)-j} \\ &\equiv \sum_{j=1}^{3} \binom{G_2(n)}{j} F(j) F(n)^{j-3} F(n-1)^{G_2(n)-j} \pmod{F(n)}. \end{aligned}$$

For convenience, we let

$$A = G_2(n) F(n)^{-2} F(n-1)^{G_2(n)-1}, \quad B = \binom{G_2(n)}{2} F(n)^{-1} F(n-1)^{G_2(n)-2},$$

and

$$C = \binom{G_2(n)}{3} 2F(n-1)^{G_2(n)-3}.$$

Then the last congruence becomes

$$\frac{G_3(n)}{F(n)^3} \equiv A + B + C \pmod{F(n)}.$$

We first show that $C \equiv 0 \pmod{F(n)}$. Since

$$2\binom{G_2(n)}{3} = \frac{1}{3} G_2(n) \big(G_2(n) - 1\big)\big(G_2(n) - 2\big)$$

and 3 is prime, it follows that 3 divides one of the factors. By Theorem 3.2, $G_2(n) = F(n)^2 \ell$ for some positive integer ℓ. If 3 divides $\big(G_2(n) - 1\big)\big(G_2(n) - 2\big)$ then $2\binom{G_2(n)}{3}$ is a multiple of $F(n)^2$ and therefore is divisible by $F(n)$. If 3 divides $G_2(n)$ then $3 \mid F(n)^2$ or $3 \mid \ell$. Since 3 is prime, this implies that $3 \mid F(n)$ or $3 \mid \ell$ and therefore,

$$\frac{G_2(n)}{3} = \frac{F(n)}{3} \cdot \ell F(n) \quad \text{or} \quad \frac{\ell}{3} \cdot F(n)^2$$

where $F(n)/3$ or $\ell/3$ is an integer. Hence, $2\binom{G_2(n)}{3}$ is divisible by $F(n)$ in this case as well. In either case, we conclude that $C \equiv 0 \pmod{F(n)}$. Now we observe that

$$A + B = F(n-1)^{G_2(n)-2} \cdot \frac{G_2(n)}{F(n)^2} \Big(F(n-1) + \frac{G_2(n) - 1}{2} \cdot F(n) \Big).$$

We consider the following three cases.

Case 1. Suppose that $3 \nmid n$ and $4 \nmid n$. Since $4 \nmid n$, Lemma 2.2(c) implies that $3 = F(4)$ does not divide $F(n)$. Now since $3 \nmid n$ and $3 \nmid F(n)$ we have $3 \nmid nF(n)$ (because 3 is prime).

Thus by Lemma 2.2(c) once again, $2 = F(3)$ does not divide $F\big(nF(n)\big) = G_2(n)$, so that $2 \mid (G_2(n) - 1)$. Furthermore, since $3 \nmid n$, by Theorem 4.1, we have

$$\frac{G_2(n)}{F(n)^2} \equiv 1 \pmod{F(n)}.$$

Consequently,

$$\begin{aligned} A + B &\equiv F(n-1)^{G_2(n)-2} \cdot 1 \cdot \Big(F(n-1) + \frac{G_2(n)-1}{2} \cdot F(n)\Big) \\ &\equiv F(n-1)^{G_2(n)-1} \pmod{F(n)}. \end{aligned}$$

Suppose that $2 \mid n$. Then, by Lemma 2.5

$$F(n-1)^{G_2(n)-1} = \big(F(n-1)^2\big)^{\frac{G_2(n)-1}{2}} \equiv 1 \pmod{F(n)}.$$

Suppose that $2 \nmid n$. Since $3 \nmid n$, Lemma 2.2(c) implies that $2 = F(3)$ does not divide $F(n)$. Since 2 is prime, we have $2 \nmid nF(n)$. A previous argument shows $3 \nmid nF(n)$. Consequently, by Lemma 2.7,

$$G_2(n) = F\big(nF(n)\big) \equiv 1 \pmod 4.$$

Writing $G_2(n) = 4k+1$ for some nonnegative integer k and appealing to Lemma 2.5, we obtain

$$F(n-1)^{G_2(n)-1} = F(n-1)^{4k} = \big(F(n-1)^2\big)^{2k} \equiv (-1)^{2k} \equiv 1 \pmod{F(n)}.$$

In either case, we have $A + B \equiv 1 \pmod{F(n)}$. Hence,

$$A + B + C \equiv 1 + 0 \equiv 1 \pmod{F(n)}.$$

Case 2. Suppose that $3 \nmid n$ and $4 \mid n$. In the following argument, we make repeated applications of Lemma 2.2(c) wherever it is appropriate. Since $4 \mid n$, it follows that $3 = F(4)$ divides $F(n)$. This implies that $3 \mid nF(n)$ and thus $2 = F(3)$ divides $F\big(nF(n)\big) = G_2(n)$. Since $3 \nmid n$, we have that $2 = F(3)$ does not divide $F(n)$ so that $F(n)$ and therefore $F(n)^2$ are odd. Thus 2 divides $G_2(n)/F(n)^2$. Since $3 \nmid n$, it follows by Theorem 4.1 that

$$\frac{G_2(n)}{F(n)^2} \equiv 1 \equiv F(n) + 1 \pmod{F(n)}.$$

Since $\gcd(F(n), 2) = 1$, $2 \mid (G_2(n)/F(n)^2)$, and $2 \mid (F(n) + 1)$, it follows that

$$\frac{G_2(n)}{2F(n)^2} \equiv \frac{F(n)+1}{2} \pmod{F(n)}.$$

Consequently,

$$\begin{aligned} A + B &= F(n-1)^{G_2(n)-2} \cdot \frac{G_2(n)}{2F(n)^2}\Big(2F(n-1) + \big(G_2(n)-1\big)F(n)\Big) \\ &\equiv F(n-1)^{G_2(n)-2} \cdot \frac{F(n)+1}{2} \cdot 2F(n-1) \\ &\equiv \big(F(n-1)^2\big)^{(G_2(n)-2)/2}(F(n)+1)F(n-1) \\ &\equiv 1^{(G_2(n)-2)/2} \cdot F(n-1) \\ &\equiv F(n-1) \pmod{F(n)}. \end{aligned}$$

The penultimate congruence follows from Lemma 2.5 since $4 \mid n$, Hence in this case we get

$$A + B + C \equiv F(n-1) \pmod{F(n)}.$$

Case 3. Suppose that $3 \mid n$. Then by Lemma 2.2(c) $2 = F(3)$ divides $F(n)$ and $2 = F(3)$ divides $F(nF(n)) = G_2(n)$. We note also that by Lemma 2.2(d) $G_2(n) - 1 \equiv -1 \mod F(n)$ since $n \mid nF(n)$. Hence,

$$\begin{aligned}
A + B &= F(n-1)^{G_2(n)-2} \cdot \frac{G_2(n)}{F(n)^2}\Big(F(n-1) + \big(G_2(n)-1\big) \cdot \frac{F(n)}{2}\Big) \\
&\equiv F(n-1)^{G_2(n)-2} \cdot \frac{1}{2}F(n-3)\Big(F(n-1) + \big(G_2(n)-1\big) \cdot \frac{F(n)}{2}\Big) \\
&\equiv F(n-1)^{G_2(n)-2} \cdot \frac{1}{2}F(n-3)\Big(F(n-1) - \frac{F(n)}{2}\Big) \\
&\equiv (F(n-1)^2)^{(G_2(n)-2)/2} \cdot \frac{1}{2}F(n-3)\Big(\frac{2F(n-1) - F(n)}{2}\Big) \\
&\equiv ((-1)^n)^{(G_2(n)-2)/2} \cdot \Big(\frac{1}{2}F(n-3)\Big)^2 \\
&\equiv \big((-1)^{(G_2(n)-2)/2}\big)^n \cdot \frac{1}{4}F(n-3)^2 \pmod{F(n)},
\end{aligned}$$

where we apply Theorem 4.1 to the second congruence and Lemmas 2.5 and 2.6 to the penultimate congruence. Now we consider the term $\dfrac{G_2(n)-2}{2}$. Since $2 \mid F(n)$, $3 \mid n$ and $(2,3) = 1$, we have $6 \mid nF(n)$. Thus, Lemma 2.2(d) implies that $8 = F(6)$ divides $F(nF(n)) = G_2(n)$. Let $G_2(n) = 8m$ for some positive integer m. Then

$$\frac{G_2(n)-2}{2} = \frac{8m-2}{2} = 4n - 1,$$

so that $\dfrac{G_2(n)-2}{2}$ is odd. Continuing from the chain of congruences modulo $F(n)$ above, we have

$$A + B + C \equiv (-1)^n \frac{1}{4}F(n-3)^2 \pmod{F(n)}.$$

This completes the proof for this case. □

5. Acknowledgement

The authors are grateful for financial support from the research grant provided by the Faculty of Science, Mahidol University during the period in which this research was conducted.

References

[1] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, Wiley, New York, 2001.
[2] T. Koshy, *Catalan Numbers with Applications*, Oxford University Press, New York, 2009.
[3] Y. Matijasevich, *Enumerable sets are Diophantine*, Soviet Math., **11** (1970), 354–358.
[4] Y. Matijasevich, *My collaboration with Julia Robinson*, Math. Intelligencer, **14.4** (1992), 38–45.
[5] Y. Matijasevich, *Hilbert's Tenth Problem*, MIT Press, 1996.
[6] A. Tangboonduangjit and K. Wiboonton, *Divisibility properties of some subsequences of Fibonacci numbers*, East-West J. Math., Special Volume, (2012), 331–336.
[7] J. Vinson, *The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence*, The Fibonacci Quarterly, **1.1** (1963), 37–45.

MSC2010: 11B39

Department of Mathematics, Faculty of Science, Mahidol University, Bangkok, 10400, Thailand
E-mail address: chatchawan.pan@mahidol.ac.th

Department of Mathematics, Faculty of Science, Mahidol University, Bangkok, 10400, Thailand
E-mail address: aram.tan@mahidol.ac.th

Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok, 10330, Thailand
E-mail address: keng.w@chula.ac.th