On the Inverse of a Fibonacci Number Modulo a Fibonacci Number Being a Fibonacci Number

On the inverse of a Fibonacci number modulo a Fibonacci number being a Fibonacci number

Carlo Sanna*

Department of Mathematical Sciences, Politecnico di Torino
Corso Duca degli Abruzzi 24, 10129 Torino, Italy

carlo.sanna@polito.it
https://orcid.org/0000-0002-2111-7596

Abstract

Let $(F_n)_{n\geq 1}$ be the sequence of Fibonacci numbers. For all integers a and $b \geq 1$ with $\gcd(a, b) = 1$, let $[a^{-1} \bmod b]$ be the multiplicative inverse of a modulo b, which we pick in the usual set of representatives $\{0, 1, \ldots, b-1\}$. Put also $[a^{-1} \bmod b] := \infty$ when $\gcd(a, b) > 1$.

We determine all positive integers m and n such that $[F_m^{-1} \bmod F_n]$ is a Fibonacci number. This extends a previous result of Prempreesuk, Noppakaew, and Pongsriiam, who considered the special case $m \in \{3, n-3, n-2, n-1\}$ and $n \geq 7$.

Let $(L_n)_{n\geq 1}$ be the sequence of Lucas numbers. We also determine all positive integers m and n such that $[L_m^{-1} \bmod L_n]$ is a Lucas number.

Keywords: congruences; Fibonacci numbers; Lucas numbers; modular arithmetic; modular multiplicative inverse.
MSC2020: Primary: 11B39, Secondary: 11A99.

1 Introduction

Let $(F_n)_{n\geq 1}$ be the sequence of Fibonacci numbers, which is defined by $F_1 := 1$, $F_2 := 1$, and $F_n := F_{n-1} + F_{n-2}$ for every integer $n \geq 3$. Several authors studied modular multiplicative inverses related to Fibonacci numbers. For instance, Komatsu, Luca, and Tachiya [3] (see also [2]) studied the multiplicative order of $F_{n+1}F_n^{-1}$ modulo F_m, where m and n are positive integers such that $\gcd(F_m, F_{n+1}F_n) = 1$. Luca, Stănică, and Yalçiner [5] studied the positive integers M such that the invertible residue classes modulo M represented by Fibonacci numbers form a subgroup. For all integers a and $b \geq 1$ with $\gcd(a, b) = 1$, let $[a^{-1} \bmod b]$ be the unique $x \in \{0, 1, \ldots, b-1\}$ such that $ax \equiv 1 \pmod b$. For the sake of convenience, put also $[a^{-1} \bmod b] := \infty$ when $\gcd(a, b) > 1$. Alecci, Murru, and Sanna [1] determined the Zeckendorf representation of $[a^{-1} \bmod F_n]$, for every fixed $a \geq 3$ and for every integer $n \geq 1$. (The case $a = 2$ was previously solved by Prempreesuk, Noppakaew, and Pongsriiam [6]). Motivated by some results in knot theory [4], Song [9] found four families of pairs (F_m, F_n) of Fibonacci numbers such that $[F_m^{-1} \bmod F_n]$ and $[F_n^{-1} \bmod F_m]$ are both Fibonacci numbers. Sanna [8] proved that these families, together with some isolated pairs, are indeed all the pairs of Fibonacci numbers with such a property. For integers $n \geq 7$ and $m \in \{3, n-3, n-2, n-1\}$, Prempreesuk, Noppakaew, and Pongsriiam [6] found necessary and sufficient conditions for $[F_m^{-1} \bmod F_n]$ to be a Fibonacci number.

Our first result is the following.

*C. Sanna is a member of the INdAM group GNSAGA and of CrypTO, the group of Cryptography and Number Theory of the Politecnico di Torino.

Theorem 1.1. *Let ℓ, m, n be integers with $\ell \geq 2$, $m \geq 3$, $n \geq 4$ and $m < 4n$. Then*

$$F_\ell = [F_m^{-1} \bmod F_n] \tag{1}$$

if and only if:

(c1) $\ell = n - \frac{1}{2}\big(3 + (-1)^n\big)$ *and* $m = n - 2$*; or*

(c2) $\ell = n - \frac{1}{2}\big(3 - (-1)^n\big)$ *and* $m \in \{n-1, n+1, n+2\}$*; or*

(c3) $\ell = 2$*,* $m = 2n - 2$*, and* n *is odd; or*

(c4) $\ell = 2$*,* $m \in \{2n-1, 2n+1, 2n+2\}$*, and* n *is even; or*

(c5) $\ell = n - 2$ *and* $m = 3n - 2$*; or*

(c6) $\ell = n - 1$ *and* $m \in \{3n-1, 3n+1, 3n+2\}$*; or*

(c7) $\ell = 2$ *and* $m = 4n - 1$*.*

We remark that, in Theorem 1.1, the conditions on ℓ, m, n are not restrictive. In fact, since $F_1 = F_2 = 1$, there is no loss in generality in assuming that $\ell, m, n \geq 2$. Moreover, the cases in which $m = 2$ or $n \in \{2, 3\}$ are easy to study. Hence, for the sake of brevity, we did not include them. Finally, in light of Lemma 2.3, the condition $m < 4n$ is not a restriction.

Let $(L_n)_{n\geq 1}$ be the sequence of Lucas numbers, which is defined by $L_1 := 2$, $L_2 := 1$, and $L_n = L_{n-1} + L_{n-2}$ for every integer $n \geq 3$.

Our second result is the following.

Theorem 1.2. *Let ℓ, m, n be integers with $\ell \geq 1$, $m \geq 2$, $n \geq 5$, and $m \leq 4n$. Then*

$$L_\ell = [L_m^{-1} \bmod L_n] \tag{2}$$

if and only if:

(d1) $\ell = \frac{1}{2}(n \pm 1)$*,* $m = \frac{1}{2}(n \mp 1)$*, and* $n \equiv 1 \pmod 4$*; or*

(d2) $\ell = \frac{1}{2}(n+1)$*,* $m = \frac{1}{2}(3n+1)$*, and* n *is odd; or*

(d3) $\ell = 1$ *and* $m = 2n - (-1)^n$*; or*

(d4) $\ell = \frac{1}{2}(n-1)$*,* $m = \frac{1}{2}(5n+1)$*, and* $n \equiv 1 \pmod 4$*; or*

(d5) $\ell = \frac{1}{2}(n+1)$*,* $m = \frac{1}{2}(5n-1)$*, and* $n \equiv 1 \pmod 4$*; or*

(d6) $\ell = \frac{1}{2}(n+1)$*,* $m = \frac{1}{2}(7n+1)$*, and* n *is odd.*

We remark that, in Theorem 1.2, the conditions on ℓ, m, n are not restrictive. In fact, the cases in which $m = 1$ or $n \in \{2, 3, 4\}$ are easy to study. Hence, for the sake of brevity, we did not include them. Furthermore, in light of Lemma 2.3, the condition $m \leq 4n$ is not a restriction.

The proof of Theorem 1.1 (resp. 1.2) is based on approximating $F_\ell F_m / F_n$ (resp. $L_\ell L_m / L_n$) with an appropriate linear combination of Fibonacci (resp. Lucas) numbers, which depends on the size of m relatively to ℓ and n. This approximation is sufficiently accurate to imply certain identities for the integers ℓ, m, n that satisfy (1) (resp. (2)). Then, these identities make possible to determine ℓ, m, n.

2 Preliminaries

It is well known that the Binet formulas

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad L_n = \alpha^n + \beta^n \tag{3}$$

hold for every integer $n \geq 1$, where $\alpha := (1+\sqrt{5})/2$ and $\beta := (1-\sqrt{5})/2$ (see, e.g., [7, Ch. 1]).

In fact, it is useful to extend the sequences of Fibonacci and Lucas numbers to all integers by using (3). In particular, from (3) it follows that

$$F_{-n} = (-1)^{n+1} F_n \quad \text{and} \quad L_{-n} = (-1)^n L_n, \tag{4}$$

for every integer n.

We also need the following lemmas.

Lemma 2.1. *We have that*

(i) $L_a L_b = L_{a+b} + (-1)^b L_{a-b}$;

(ii) $5F_a F_b = L_{a+b} - (-1)^b L_{a-b}$;

(iii) $F_a F_b = F_{a+b} - F_{a+b-2} - F_{a-1}F_{b-1}$;

for all integers a, b.

Proof. These identities follow easily from (3). □

Lemma 2.2. *We have that*

(i) $F_a F_b - F_c F_d = (-1)^{a+1} F_{c-a} F_{d-a}$;

(ii) $L_a L_b - L_c L_d = (-1)^a 5 F_{c-a} F_{d-a}$;

(iii) $5F_a F_b - L_c L_d = (-1)^{a+1} L_{c-a} L_{d-a}$;

for all integers a, b, c, d *with* $a + b = c + d$.

Proof. These identities can be proved either directly from (3), or by taking appropriate differences of pairs of the identities of Lemma 2.1 and, eventually, employing (4). □

Lemma 2.3. *We have that*

(i) $F_{a+4n} \equiv F_a \pmod{F_n}$;

(ii) $L_{a+4n} \equiv L_a \pmod{L_n}$;

for all integers a *and* $n \geq 1$.

Proof. Using (3) one can verify that

$$F_{a+4n} - F_a = F_n L_n L_{a+2n} \quad \text{and} \quad L_{a+4n} - L_a = 5F_n F_{a+2n} L_n,$$

from which the claim follows. □

Lemma 2.4. *Let* a, b, n *be integers. We have that:*

(i) $|F_a F_b| < F_n - 1$ *if* $|a| + |b| \leq n$ *and* $n \geq 5$;

(ii) $|5F_a F_b| < L_n - 1$ *if* $|a| + |b| \leq n - 1$ *and* $n \geq 6$;

(iii) $|L_a| < L_n - 1$ *if* $|a| \leq n - 1$ *and* $n \geq 4$;

(iv) $|L_a L_b| < L_n - 1$ *if* $|a| + |b| \leq n - 1$, $\{|a|, |b|\} \notin \{0, n-1\}$, *and* $n \geq 6$.

Proof. By (4), we have that $|F_k| = F_{|k|}$ and $|L_k| = L_{|k|}$, for every integer k. Hence, throughout the proof, we can assume that $a, b \geq 0$. Moreover, by symmetry, we can assume that $a \geq b$.

Let us prove (i) and (ii). If $b = 0$ or $a + b \leq 4$, then (i) and (ii) follow easily. Hence, assume that $b \geq 1$ and $a + b \geq 5$. Then, by Lemma 2.1(iii), we have that

$$F_a F_b = F_{a+b} - F_{a+b-2} - F_{a-1}F_{b-1} \leq F_n - F_3 < F_n - 1,$$

whenever $a + b \leq n$, which proves (i). Furthermore, by Lemma 2.1(ii), we have that

$$5F_a F_b = L_{a+b} - (-1)^b L_{a-b} \leq L_{a+b} + L_{a-b} \leq L_{n-1} + L_{n-3} = L_n - L_{n-4} < L_n - 1,$$

whenever $a + b \leq n - 1$ and $n \geq 6$, which proves (ii).

If $a \leq n - 1$ and $n \geq 4$, then

$$L_a \leq \max\{2, L_{n-1}\} = L_{n-1} = L_n - L_{n-2} < L_n - 1,$$

which proves (iii).

By Lemma 2.1(i), we have that

$$L_{a+b} = L_{a+b} + (-1)^b L_{a-b} \leq L_{a+b} + L_{a-b}.$$

Therefore, if $a + b \leq n - 2$ and $n \geq 5$, then

$$L_{a+b} \leq 2L_{n-2} = L_n - L_{n-3} < L_n - 1.$$

Furthermore, if $a + b = n - 1$, $b \geq 1$, and $n \geq 6$, then

$$L_{a+b} \leq L_{n-1} + L_{n-3} = L_n - L_{n-4} < L_n - 1.$$

Thus (iv) is proved. □

3 Proof of Theorem 1.1

With a bit of patience, one can check that Theorem 1.1 holds for $n = 4$. Hence, hereafter, assume that $n \geq 5$.

Suppose that (1) is satisfied. Hence, we have that $F_\ell < F_n$ and

$$F_\ell F_m - AF_n = 1, \tag{5}$$

for some integer $A \geq 0$. In particular, from $F_\ell < F_n$ it follows that $\ell < n$. Moreover, since $m \geq 3$, we get that $A \geq 1$. Consequently, we have that $F_\ell F_m \geq F_n + 1$. Hence, by Lemma 2.4(i), we get that $m > n - \ell$.

Define the four disjoint intervals

$$I_1 := (n - \ell, n + \ell], \quad I_2 := (n + \ell, 3n - \ell], \quad I_3 := (3n - \ell, 3n + \ell], \quad I_4 := (3n + \ell, 4n).$$

By the previous considerations, we have that m belongs to exactly one of such intervals.

For every integer k, put $F_k^+ := F_k$ if $k \geq 0$, and $F_k^+ := 0$ if $k < 0$. Then, define

$$A_{\ell,m,n} := F_{\ell+m-n} - (-1)^\ell F^+_{-\ell+m-n} + (-1)^n F^+_{\ell+m-3n} - (-1)^{\ell+n} F^+_{-\ell+m-3n}$$

and

$$B_{\ell,m,n} := F_\ell F_m - A_{\ell,m,n} F_n. \tag{6}$$

Let us prove that

$$B_{\ell,m,n} = \begin{cases} (-1)^{\ell+1} F_{m-n} F_{n-\ell} & \text{if } m \in I_1; \\ (-1)^n F_\ell F_{m-2n} & \text{if } m \in I_2; \\ (-1)^{\ell+n+1} F_{m-3n} F_{n-\ell} & \text{if } m \in I_3; \\ F_\ell F_{m-4n} & \text{if } m \in I_4. \end{cases} \tag{7}$$

By Lemma 2.2(i), we have that

$$F_\ell F_m - F_{\ell+m-n}F_n = (-1)^{\ell+1}F_{m-n}F_{n-\ell}. \tag{8}$$

Hence, we get that $B_{\ell,m,n} = (-1)^{\ell+1}F_{m-n}F_{n-\ell}$ for each $m \in I_1$.

By (8), Lemma 2.2(i), and (4), we have that

$$\begin{aligned} F_\ell F_m - \big(F_{\ell+m-n} - (-1)^\ell F_{-\ell+m-n}\big)F_n &= (-1)^{\ell+1}(F_{m-n}F_{n-\ell} - F_{-\ell+m-n}F_n) \\ &= (-1)^{\ell+m+n}F_{-\ell}F_{2n-m} = (-1)^n F_\ell F_{m-2n} \end{aligned} \tag{9}$$

Hence, we get that $B_{\ell,m,n} = (-1)^n F_\ell F_{m-2n}$ for each $m \in I_2$.

By (9) and Lemma 2.2(i), we have that

$$\begin{aligned} F_\ell F_m - \big(F_{\ell+m-n} - (-1)^\ell F_{-\ell+m-n} + (-1)^n F_{\ell+m-3n}\big)F_n \\ = (-1)^n(F_\ell F_{m-2n} - F_{\ell+m-3n}F_n) = (-1)^{\ell+n+1}F_{m-3n}F_{n-\ell}. \end{aligned} \tag{10}$$

Hence, we get that $B_{\ell,m,n} = (-1)^{\ell+n+1}F_{m-3n}F_{n-\ell}$ for each $m \in I_3$.

Finally, by (10), (4), and Lemma 2.2(i), we have that

$$\begin{aligned} F_\ell F_m - \big(F_{\ell+m-n} - (-1)^\ell F_{-\ell+m-n} + (-1)^n F_{\ell+m-3n} - (-1)^{\ell+n}F_{-\ell+m-3n}\big)F_n \\ = (-1)^{\ell+n+1}(F_{m-3n}F_{n-\ell} - F_{-\ell+m-3n}F_n) = (-1)^{\ell+m}F_{-\ell}F_{4n-m} = F_\ell F_{m-4n}. \end{aligned}$$

Hence, we get that $B_{\ell,m,n} = F_\ell F_{m-4n}$ for each $m \in I_4$. The proof of (7) is complete.

At this point, considering the four cases in (7), one can easily check that $B_{\ell,m,n}$ is equal to $\pm F_a F_b$, where a and b are integers (depending on ℓ, m, n) such that $|a| + |b| \le n$.

Therefore, from (6) and Lemma 2.4(i), we get that

$$\left|\frac{F_\ell F_m}{F_n} - A_{\ell,m,n}\right| = \frac{|B_{\ell,m,n}|}{F_n} = \frac{|F_a F_b|}{F_n} < 1 - \frac{1}{F_n}.$$

Consequently, recalling (5), we have that

$$|A - A_{\ell,m,n}| \le \left|A - \frac{F_\ell F_m}{F_n}\right| + \left|\frac{F_\ell F_m}{F_n} - A_{\ell,m,n}\right| < \frac{1}{F_n} + \left(1 - \frac{1}{F_n}\right) = 1,$$

which implies that $A = A_{\ell,m,n}$, since A and $A_{\ell,m,n}$ are both integers. Then, from (5) and (6), we get that $B_{\ell,m,n} = 1$.

Note that, for every integer k, we have that $|F_k| = 1$ if and only if $k \in \{-2, -1, 1, 2\}$. In particular, we have that $F_{-2} = -1$ and $F_{-1} = F_1 = F_2 = 1$. Therefore, from $B_{\ell,m,n} = 1$ we can determine ℓ and m in terms of n in each of the four cases in (7).

If $m \in I_1$, then $(-1)^{\ell+1}F_{m-n}F_{n-\ell} = 1$. Hence, we have that $m \in \{n-2, n-1, n+1, n+2\}$ and $\ell \in \{n-2, n-1\}$ (recall that $\ell < n$). If $m = n-2$, then either $\ell = n-2$ and n is even, or $\ell = n-1$ and n is odd. This is case (c1). If $m \in \{n-1, n+1, n+2\}$, then either $\ell = n-1$ and n is even, or $\ell = n-2$ and n is odd. This is case (c2).

If $m \in I_2$, then $(-1)^n F_\ell F_{m-2n} = 1$. Hence, $\ell = 2$ and $m \in \{2n-2, 2n-1, 2n+1, 2n+2\}$. If $m = 2n-2$, then $F_{m-2n} = -1$ and consequently n is odd, which is case (c3). If $m \in \{2n-1, 2n+1, 2n+2\}$, then $F_{m-2n} = 1$ and consequently n is even, which is case (c4).

If $m \in I_3$, then $(-1)^{\ell+n+1}F_{m-3n}F_{n-\ell} = 1$. Hence, it follows that $\ell \in \{n-2, n-1\}$ and $m \in \{3n-2, 3n-1, 3n+1, 3n+2\}$. If $\ell = n-2$, then $(-1)^{\ell+n+1}F_{n-\ell} = -1$ and consequently $m = 3n-2$, which is case (c5). If $\ell = n-1$, then $(-1)^{\ell+n+1}F_{n-\ell} = 1$ and consequently $m \in \{3n-1, 3n+1, 3n+2\}$, which is case (c6).

If $m \in I_4$, then $F_\ell F_{m-4n} = 1$. Hence, we have that $\ell = 2$ and $m = 4n-1$ (recall that $m < 4n$), which is case (c7).

At this point, we have proved that if (1) is true then the integers ℓ, m, n are of the form given by (c1)–(c7).

Vice versa, using (7), on can easily verify that if ℓ, m, n are of the form given by (c1)–(c7) then $B_{\ell,m,n} = 1$. In turn, by (6), this implies that (1) is true.

The proof of Theorem 1.1 is complete.

4 Proof of Theorem 1.2

With a bit of patience, one can check that Theorem 1.2 holds for $n = 5$. Hence, hereafter, assume that $n \geq 6$.

Suppose that (2) is satisfied. Hence, we have that $L_\ell < L_n$ and

$$L_\ell L_m - C L_n = 1, \tag{11}$$

for some integer $C \geq 0$. In particular, from $L_\ell < L_n$ it follows that $\ell < n$. Moreover, since $m \geq 2$, we get that $C \geq 1$. Consequently, we have that $L_\ell L_m \geq L_n + 1$. Hence, by Lemma 2.4(iv), we get that $m \geq n - \ell$.

Define the four disjoint intervals

$$J_1 := [n-\ell, n+\ell), \quad J_2 := [n+\ell, 3n-\ell), \quad J_3 := [3n-\ell, 3n+\ell), \quad J_4 := [3n+\ell, 4n].$$

By the previous considerations, we have that m belongs to exactly one of such intervals.

For every integer k, put $L_k^+ := L_k$ if $k \geq 0$, and $L_k^+ := 0$ if $k < 0$. Then, define

$$C_{\ell,m,n} := L_{\ell+m-n} + (-1)^\ell L^+_{-\ell+m-n} - (-1)^n L^+_{\ell+m-3n} - (-1)^{\ell+n} L^+_{-\ell+m-3n}$$

and

$$D_{\ell,m,n} := L_\ell L_m - C_{\ell,m,n} L_n. \tag{12}$$

Let us prove that

$$D_{\ell,m,n} = \begin{cases} (-1)^\ell 5 F_{m-n} F_{n-\ell} & \text{if } m \in J_1; \\ (-1)^{n+1} L_\ell L_{m-2n} & \text{if } m \in J_2; \\ (-1)^{\ell+n+1} 5 F_{m-3n} F_{n-\ell} & \text{if } m \in J_3; \\ L_\ell L_{m-4n} & \text{if } m \in J_4. \end{cases} \tag{13}$$

From Lemma 2.2(ii), it follows that

$$L_\ell L_m - L_{\ell+m-n} L_n = (-1)^\ell 5 F_{m-n} F_{n-\ell}. \tag{14}$$

Hence, we have that $D_{\ell,m,n} = (-1)^\ell 5 F_{m-n} F_{n-\ell}$ for every $m \in J_1$.

From (14), Lemma 2.2(iii), and (4), it follows that

$$\begin{aligned} L_\ell L_m - \big(L_{\ell+m-n} + (-1)^\ell L_{-\ell+m-n}\big) L_n &= (-1)^\ell (5 F_{m-n} F_{n-\ell} - L_{-\ell+m-n} L_n) \\ &= (-1)^{\ell+m+n+1} L_{-\ell} L_{2n-m} = (-1)^{n+1} L_\ell L_{m-2n}. \end{aligned} \tag{15}$$

Hence, we have that $D_{\ell,m,n} = (-1)^{n+1} L_\ell L_{m-2n}$ for every $m \in J_2$.

From (15) and Lemma 2.2(ii), it follows that

$$\begin{aligned} L_\ell L_m - \big(L_{\ell+m-n} + (-1)^\ell L_{-\ell+m-n} - (-1)^n L_{\ell+m-3n}\big) L_n \\ = (-1)^{n+1} (L_\ell L_{m-2n} - L_{\ell+m-3n} L_n) = (-1)^{\ell+n+1} 5 F_{m-3n} F_{n-\ell}. \end{aligned} \tag{16}$$

Hence, we have that $D_{\ell,m,n} = (-1)^{\ell+n+1} 5 F_{m-3n} F_{n-\ell}$ for every $m \in J_3$.

Finally, from (16), Lemma 2.2(iii), and (4), it follows that

$$\begin{aligned} L_\ell L_m - \big(L_{\ell+m-n} + (-1)^\ell L_{-\ell+m-n} - (-1)^n L_{\ell+m-3n} - (-1)^{\ell+n} L_{-\ell+m-3n}\big) L_n \\ = (-1)^{\ell+n+1} (5 F_{m-3n} F_{n-\ell} - L_{-\ell+m-3n} L_n) = (-1)^{\ell+m} L_{-\ell} L_{4n-m} = L_\ell L_{m-4n}. \end{aligned}$$

Hence, we have that $D_{\ell,m,n} = L_\ell L_{m-4n}$ for every $m \in J_4$. The proof of (13) is complete.

Suppose that C', D' are integers such that

$$\left| \frac{L_\ell L_m}{L_n} - C' \right| < 1 - \frac{1}{L_n} \quad \text{and} \quad D' = L_\ell L_m - C' L_n.$$

Then, by (11), we have that

$$|C - C'| \leq \left|C - \frac{L_\ell L_m}{L_n}\right| + \left|\frac{L_\ell L_m}{L_n} - C'\right| < \frac{1}{L_n} + \left(1 - \frac{1}{L_n}\right) = 1.$$

Consequently, we have that $C' = C$ and, by (11) again, that $D' = 1$.

Hereafter, we will make use of such a fact several times, by taking $C' = C_{\ell,m,n} + s$ and $D' = D_{\ell,m,n} - sL_n$ for some $s \in \{-1, 0, 1\}$.

We will also use the fact that, for every integer k, we have that $|L_k| = 1$ if and only if $k \in \{-1, 1\}$. Precisely, we have that $L_{-1} = -1$ and $L_1 = 1$.

If $m = n - \ell$, then from (13), (4), and Lemma 2.1(ii) it follows that

$$D_{\ell,m,n} = (-1)^\ell 5F_{-\ell}F_{n-\ell} = -5F_\ell F_{n-\ell} = -L_n + (-1)^{n-\ell}L_{2\ell-n}.$$

Hence, by Lemma 2.4(iii), we have that

$$\left|\frac{L_\ell L_m}{L_n} - (C_{\ell,m,n} - 1)\right| = \frac{|L_{2\ell-n}|}{L_n} < 1 - \frac{1}{L_n},$$

which implies that $(-1)^{n-\ell}L_{2\ell-n} = 1$. Therefore, either $n - \ell$ is even and $2\ell - n = 1$, or $n - \ell$ is odd and $2\ell - n = -1$. Recalling that $m = n - \ell$, it follows that $\ell = \frac{1}{2}(n \pm 1)$, $m = \frac{1}{2}(n \mp 1)$, and $n \equiv 1 \pmod 4$, which is case (d1).

If $m \in J_1 \setminus \{n - \ell\}$, then (13) and Lemma 2.4(ii) yield that

$$\left|\frac{L_\ell L_m}{L_n} - C_{\ell,m,n}\right| = \frac{5|F_{m-n}F_{n-\ell}|}{L_n} < 1 - \frac{1}{L_n},$$

which implies that $(-1)^\ell 5F_{m-n}F_{n-\ell} = 1$. However, this last equality is clearly impossible.

If $m = n + \ell$, then (13) and Lemma 2.1(i) yield that

$$D_{\ell,m,n} = (-1)^{n+1}L_\ell L_{\ell-n} = (-1)^{n+1}L_{2\ell-n} - (-1)^\ell L_n.$$

Hence, by Lemma 2.4(iii), we have that

$$\left|\frac{L_\ell L_m}{L_n} - \left(C_{\ell,m,n} - (-1)^\ell\right)\right| = \frac{|L_{2\ell-n}|}{L_n} < 1 - \frac{1}{L_n},$$

which implies that $(-1)^{n+1}L_{2\ell-n} = 1$. Therefore, either n is odd and $2\ell - n = 1$, or n is even and $2\ell - n = -1$. However, the latter case is impossible. Hence, recalling that $m = n + \ell$, we get that $\ell = \frac{1}{2}(n + 1)$, $m = \frac{1}{2}(3n + 1)$, and n is odd, which is case (d2).

If $m \in J_2 \setminus \{n + \ell\}$ and $(\ell, m) \neq (n - 1, 2n)$, then (13) and Lemma 2.4(iv) yield that

$$\left|\frac{L_\ell L_m}{L_n} - C_{\ell,m,n}\right| = \frac{|L_\ell L_{m-2n}|}{L_n} < 1 - \frac{1}{L_n},$$

which implies that $(-1)^{n+1}L_\ell L_{m-2n} = 1$. Thus $\ell = 1$ and either $m = 2n + 1$ and n is odd, or $m = 2n - 1$ and n is even. This is case (d3).

If $\ell = n - 1$ and $m = 2n$ then, by (13), we get that

$$D_{\ell,m,n} = (-1)^{n+1}2L_{n-1} = (-1)^{n+1}L_n + (-1)^{n+1}L_{n-3}.$$

Hence, by Lemma 2.4(iii), we have that

$$\left|\frac{L_\ell L_m}{L_n} - \left(C_{\ell,m,n} + (-1)^{n+1}\right)\right| = \frac{|L_{n-3}|}{L_n} < 1 - \frac{1}{L_n},$$

which implies that $(-1)^{n+1}L_{n-3} = 1$, but this last equality is impossible.

If $m = 3n - \ell$, then (13), (4), and Lemma 2.1(ii) yield that

$$\begin{aligned} D_{\ell,m,n} &= (-1)^{\ell+n+1} 5F_{-\ell}F_{n-\ell} = (-1)^n 5F_\ell F_{n-\ell} = (-1)^n \big(L_n - (-1)^{n-\ell} L_{2\ell-n}\big) \\ &= (-1)^n L_n - (-1)^\ell L_{2\ell-n}. \end{aligned}$$

Hence, by Lemma 2.4(iii), we have that

$$\left| \frac{L_\ell L_m}{L_n} - \big(C_{\ell,m,n} + (-1)^n\big) \right| = \frac{|L_{2\ell-n}|}{L_n} < 1 - \frac{1}{L_n},$$

which implies that $(-1)^{\ell+1} L_{2\ell-n} = 1$. Therefore, either ℓ is even and $2\ell - n = -1$, or ℓ is odd and $2\ell - n = 1$. That is, we have that $n \equiv 1 \pmod 4$ and either $\ell = \frac{1}{2}(n-1)$ and $m = \frac{1}{2}(5n+1)$, or $\ell = \frac{1}{2}(n+1)$ and $m = \frac{1}{2}(5n-1)$. These are cases (d4) and (d5).

If $m \in J_3 \setminus \{3n - \ell\}$, then (13) and Lemma 2.4(ii) yield that

$$\left| \frac{L_\ell L_m}{L_n} - C_{\ell,m,n} \right| = \frac{|5F_{m-3n}F_{n-\ell}|}{L_n} < 1 - \frac{1}{L_n},$$

which implies that $(-1)^{\ell+n+1} 5F_{m-3n}F_{n-\ell} = 1$, but this last equality is impossible.

If $m = 3n + \ell$, then (13) and Lemma 2.1(i) yield that

$$D_{\ell,m,n} = L_\ell L_{\ell-n} = L_{2\ell-n} + (-1)^{\ell+n} L_n.$$

Hence, by Lemma 2.4(iii), we get that

$$\left| \frac{L_\ell L_m}{L_n} - \big(C_{\ell,m,n} + (-1)^{\ell+n}\big) \right| = \frac{|L_{2\ell-n}|}{L_n} < 1 - \frac{1}{L_n},$$

which implies that $L_{2\ell-n} = 1$. Hence, we get that $2\ell - n = 1$. Recalling that $m = 3n + \ell$, it follows that $\ell = \frac{1}{2}(n+1)$, $m = \frac{1}{2}(7n+1)$, and n is odd, which is case (d6).

If $m \in J_4 \setminus \{3n + \ell, 4n\}$ and $(\ell, m) \neq (n-1, 4n)$, then (13) and Lemma 2.4(iv) yield that

$$\left| \frac{L_\ell L_m}{L_n} - C_{\ell,m,n} \right| = \frac{|L_\ell L_{m-4n}|}{L_n} < 1 - \frac{1}{L_n},$$

which implies that $L_\ell L_{m-4n} = 1$. Hence, we have that $\ell = 1$ and $m = 4n + 1$, which is impossible, since $m \leq 4n$.

If $\ell = n - 1$ and $m = 4n$ then, by (13), we get that

$$D_{\ell,m,n} = 2L_{n-1} = L_n + L_{n-3}.$$

Hence, by Lemma 2.4(iii), we have that

$$\left| \frac{L_\ell L_m}{L_n} - (C_{\ell,m,n} + 1) \right| = \frac{|L_{n-3}|}{L_n} < 1 - \frac{1}{L_n},$$

which implies that $L_{n-3} = 1$, but this last equality is impossible.

At this point, we have proved that if (2) is true then the integers ℓ, m, n are of the form given by (d1)–(d6).

Vice versa, using (13), on can easily verify that if ℓ, m, n are of the form given by (d1)–(d6) then $D_{\ell,m,n} = 1$. In turn, by (12), this implies that (2) is true.

The proof of Theorem 1.2 is complete.

Statements and declarations

Competing interests

The author declare that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References

[1] G. Alecci, N. Murru, and C. Sanna, *Zeckendorf representation of multiplicative inverses modulo a Fibonacci number*, Monatsh. Math. **201** (2023), no. 1, 1–9.

[2] Y. F. Bilu, T. Komatsu, F. Luca, A. Pizarro-Madariaga, and P. Stănică, *On a divisibility relation for Lucas sequences*, J. Number Theory **163** (2016), 1–18.

[3] T. Komatsu, F. Luca, and Y. Tachiya, *On the multiplicative order of F_{n+1}/F_n modulo F_m*, Integers **12B** (2012/13), no. Proceedings of the Integers Conference 2011, Paper No. A8, 13.

[4] S. Lee, *Twisted torus knots that are unknotted*, Int. Math. Res. Not. IMRN (2014), no. 18, 4958–4996.

[5] F. Luca, P. Stănică, and A. Yalçiner, *When do the Fibonacci invertible classes modulo M form a subgroup?*, Ann. Math. Inform. **41** (2013), 265–270.

[6] B. Prempreesuk, P. Noppakaew, and P. Pongsriiam, *Zeckendorf representation and multiplicative inverse of F_m* mod F_n, Int. J. Math. Comput. Sci. **15** (2020), no. 1, 17–25.

[7] P. Ribenboim, *My numbers, my friends*, Springer-Verlag, New York, 2000, Popular lectures on number theory.

[8] C. Sanna, *Pairwise modular multiplicative inverses and Fibonacci numbers*, Integers **23** (2023), Paper No. A3, 7.

[9] H.-J. Song, *Modular multiplicative inverses of Fibonacci numbers*, East Asian Math. J. **35** (2019), no. 3, 285–288.