International Journal of Mathematics and
Computer Science, **15**(2020), no. 1, 17–25

Zeckendorf Representation and Multiplicative Inverse of $F_m \bmod F_n$

Bencharat Prempreesuk, Passawan Noppakaew, Prapanpong Pongsriiam[1]

Department of Mathematics
Faculty of Science
Silpakorn University
Nakhon Pathom, 73000, Thailand

email: meenbencharat@gmail.com, p.noppakaew@gmail.com, prapanpong@gmail.com, pongsriiam_p@silpakorn.edu

(Received August 1, 2019, Accepted September 4, 2019)

Abstract

Let m and n be positive integers and let F_m and F_n be the mth and nth Fibonacci numbers. In this article, we find the Zeckendorf representation of the multiplicative inverse of F_m modulo F_n when m is small or when m is closed to n and $(m,n) \leq 2$.

1 Introduction

Let $(F_n)_{n\geq 0}$ be the Fibonacci sequence defined by the recurrence $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. The divisibility properties of the Fibonacci numbers have been a popular area of research; see for example in [1, 2, 3, 5, 6, 7, 10, 11, 12] for some recent results. We write $\gcd(m,n)$ or simply (m,n) to denote the greatest common divisor of positive integers m and n and write $\lfloor x \rfloor$ for the greatest integer which is less than or equal to the real number x. Three well-known facts which are closely related to our article are the following:

[1]Prapanpong Pongsriiam is the corresponding author.

Key words and phrases: Fibonacci number, Zeckendorf representation, multiplicative inverse, congruence, Diophantine equation.
AMS (MOS) Subject Classifications: 11B39, 11A05, 11A07.
ISSN 1814-0432, 2020, http://ijmcs.future-in-tech.net

(i) $\gcd(F_m, F_n) = F_{\gcd(m,n)}$,

(ii) if a and n are positive integers and $\gcd(a, n) = 1$, then there exists a unique integer x such that $1 \leq x \leq n$ and $ax \equiv 1 \pmod{n}$,

(iii) every positive integer n can be uniquely written as $n = F_{n_1} + F_{n_2} + \cdots + F_{n_k}$, where $k \geq 1$, $n_1 > n_2 > \cdots > n_k \geq 2$ and $n_i - n_{i+1} \geq 2$ for all $i = 1, 2, \ldots, k-1$.

The integer x in (ii) is called the least positive multiplicative inverse of a modulo n and is denoted by $a^{-1} \bmod n$. If the condition $1 \leq x \leq n$ in (ii) is omitted, then there are infinitely many such x but they are all congruent to each other modulo n. So we may say that the multiplicative inverse of a mod n is unique (up to) modulo n. The representation of n in (iii) is called the Zeckendorf representation of n. It is sometimes convenient to sacrifice the uniqueness of the representation and allow $n_k = 1$ or change the order to $n = F_{n_k} + F_{n_{k-1}} + \cdots + F_{n_2} + F_{n_1}$ where $n_k < n_{k-1} < \ldots < n_1$. However, we will restrict ourselves to the original form as stated in (iii). So, for instance, $4 = F_4 + F_2$ is the Zeckendorf representation but $4 = F_2 + F_4 = F_1 + F_4 = F_4 + F_1$ are not counted as the Zeckendorf representation of 4.

In this article, we are interested in finding the least positive multiplicative inverse of F_m mod F_n and write it in the form of Zeckendorf representation. The condition we necessarily impose on m and n is that $(m, n) = 1$ or 2 so that $(F_m, F_n) = F_{(m,n)} = 1$ and $F_m^{-1} \bmod F_n$ exists. The calculation of $F_m^{-1} \bmod F_n$ might be easy but determining its Zeckendorf representation is quite difficult. Our purpose is to obtain a general formula for the Zeckendorf representation of $F_m^{-1} \bmod F_n$ when m is very near or very far from n.

We give some preliminaries and lemmas in the next section. Then we show our main results in Section 3. For other related results, see for example in [8, 9, 13] and references therein.

2 Auxiliary Results

Lemma 2.1. *Let n and k be positive integers. Then the following statements hold.*

(i) (Cassini-Catalan identity) *If $n > k$, then $F_{n-k}F_{n+k} - F_n^2 = (-1)^{n-k+1}F_k^2$.*

(ii) (Binet's formula) $F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ *where* $\alpha = \frac{1+\sqrt{5}}{2}$ *and* $\beta = \frac{1-\sqrt{5}}{2}$.

(iii) $F_{n+k} = F_nF_{k+1} + F_{n-1}F_k$.

Proof. The statements (i) and (ii) are proved in [4, p. 83] and [4, p. 79] respectively. By (ii) and the fact that $\alpha\beta = -1$, $\alpha^2 + 1 = \alpha(\alpha - \beta)$, $\beta^2 = \beta(\beta - \alpha)$, we see that the right-hand side of (iii) is equal to

$$\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)\left(\frac{\alpha^{k+1} - \beta^{k+1}}{\alpha - \beta}\right) + \left(\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}\right)\left(\frac{\alpha^k - \beta^k}{\alpha - \beta}\right)$$

$$= \frac{\alpha^{n+k+1} + \beta^{n+k+1} - \alpha^n\beta^{k+1} - \alpha^{k+1}\beta^n}{(\alpha - \beta)^2} + \frac{\alpha^{n+k-1} + \beta^{n+k-1} - \alpha^{n-1}\beta^k - \alpha^k\beta^{n-1}}{(\alpha - \beta)^2}$$

$$= \frac{\alpha^{n+k+1} + \beta^{n+k+1} + \alpha^{n+k-1} + \beta^{n+k-1} - (\alpha\beta + 1)\alpha^{n-1}\beta^k - (\alpha\beta + 1)\alpha^k\beta^{n-1}}{(\alpha - \beta)^2}$$

$$= \frac{(\alpha^2 + 1)\alpha^{n+k-1} + (\beta^2 + 1)\beta^{n+k-1}}{(\alpha - \beta)^2} = \frac{\alpha^{n+k} - \beta^{n+k}}{(\alpha - \beta)} = F_{n+k}.$$

□

Lemma 2.2. (Period of the Fibonacci sequence) *The sequence $(F_n)_{n\geq 1}$ is simply periodic modulo m for every $m \geq 2$. In particular, we have*

(i) $F_n \equiv 1 \pmod 2$ *if and only if* $n \equiv 1, 2 \pmod 3$,

(ii) $F_n \equiv 0 \pmod 2$ *if and only if* $n \equiv 0 \pmod 3$.

Proof. Wall [14] obtained the first statement as a special case of his general theorem. The statements (i) and (ii) can be obtained by direct calculation of $(F_n \bmod 2)_{n\geq 1}$; see also in [4, p. 208] and [4, Chapter 35]. □

Recall that the Lucas sequence $(L_n)_{n\geq 0}$ is defined by $L_0 = 2$, $L_1 = 1$, and $L_n = L_{n-1} + L_{n-2}$ for $n \geq 2$. The sum of Fibonacci numbers over an arithmetic progression is given in the next lemma.

Lemma 2.3. (Koshy [4, p. 85]) *Let $k \geq 1$ and j any integer. Then*

$$\sum_{i=0}^{n} F_{ki+j} = \begin{cases} \frac{F_{nk+k+j} - (-1)^k F_{nk+j} - F_j - (-1)^j F_{k-j}}{L_k - (-1)^k - 1}, & \text{if } j < k; \\ \frac{F_{nk+k+j} - (-1)^k F_{nk+j} - F_j + (-1)^k F_{j-k}}{L_k - (-1)^k - 1}, & \text{otherwise.} \end{cases}$$

3 Main Results

Theorem 3.1. (Multiplicative inverse of F_m mod F_n when m is closed to n) *For each $n \geq 3$, the following statements hold.*

(i) *If n is even, then $F_{n-1}^{-1} \bmod F_n = F_{n-1}$. If n is odd, then $F_{n-1}^{-1} \bmod F_n = F_{n-2}$.*

(ii) *If n is odd, then $F_{n-2}^{-1} \bmod F_n = F_{n-1}$. If n is even, then $F_{n-2}^{-1} \bmod F_n = F_{n-2}$.*

Proof. Applying Lemma 2.1 with $k = 1$ together with the definition of the Fibonacci number, we see that $F_{n-1}^2 \equiv F_{n-1}(F_{n+1} - F_n) \equiv F_{n-1}F_{n+1} \equiv (-1)^n \pmod{F_n}$. If n is even, then the above implies that $F_{n-1}^{-1} \equiv F_{n-1} \pmod{F_n}$. If n is odd, then the above implies that $F_{n-1}^2 \equiv -1 \pmod{F_n}$, and so $F_{n-1}(-F_{n-1}) \equiv 1 \pmod{F_n}$, which means that $F_{n-1}^{-1} \equiv -F_{n-1} \equiv F_n - F_{n-1} \equiv F_{n-2} \pmod{F_n}$. This proves (i). Since $F_{n-2} = F_n - F_{n-1}$, we see that $F_{n-2}^{-1} \equiv (-F_{n-1})^{-1} \equiv (-1)^{-1}F_{n-1}^{-1} \equiv -F_{n-1}^{-1} \pmod{F_n}$. Therefore (ii) follows from (i). □

Since $F_1 = F_2 = 1$, it is obvious that $F_1^{-1} \bmod F_n = F_2^{-1} \bmod F_n = 1$ for all $n \geq 1$. Consider $F_3 = 2$. Since $2\left(\frac{1+F_n}{2}\right) \equiv 1 + F_n \equiv 1 \pmod{F_n}$, we see that $2^{-1} \bmod F_n = (1 + F_n)/2$ provided that $1 + F_n$ is divisible by 2. By Lemma 2.2, we know that $F_n + 1 \equiv 0 \pmod 2$ if and only if $n \equiv 1, 2 \pmod 3$. In addition, if $n \equiv 0 \pmod 3$, then F_n is even and $(2, F_n) = 2 \neq 1$, and thus $2^{-1} \bmod F_n$ does not exist. In conclusion, $2^{-1} \bmod F_n = (1 + F_n)/2$ if $n \equiv 1, 2 \pmod 3$, and $2^{-1} \bmod F_n$ does not exist if $n \equiv 0 \pmod 3$. However, it is not obvious what the Zeckendorf representation of $2^{-1} \bmod F_n$ looks like. This is given in the next theorem.

Theorem 3.2. (Multiplicative inverse of $F_m \bmod F_n$ when m is small) *Suppose $n \geq 7$ and $n \not\equiv 0 \pmod 3$. Then the Zeckendorf representation of $F_3^{-1} \bmod F_n$ is given by*

$$F_3^{-1} \bmod F_n = \begin{cases} \sum_{k=0}^{\lfloor \frac{n}{3} \rfloor - 2} F_{n-3k-2} + F_3, & \text{if } n \equiv 1 \pmod 3; \\ \sum_{k=0}^{\lfloor \frac{n}{3} \rfloor - 2} F_{n-3k-2} + F_4, & \text{if } n \equiv 2 \pmod 3. \end{cases} \tag{3.1}$$

Proof. We first show that the right-hand side of (3.1) is in the correct form. Recall that $\lfloor x \rfloor$ is the largest integer $\leq x$ and if $n \equiv r \pmod m$ and $0 \leq r < m$, then $\left\lfloor \frac{n}{m} \right\rfloor = \frac{n-r}{m}$. We use this without further reference. For $0 \leq k \leq \lfloor \frac{n}{3} \rfloor - 3$, we have $(n-3k-2)-(n-3(k+1)-2) = 3 \geq 2$ and $n-3(\lfloor \frac{n}{3} \rfloor - 2)-2 = n - 3\lfloor \frac{n}{3} \rfloor + 4$. If $n \equiv 1 \pmod 3$, then $n - 3\lfloor \frac{n}{3} \rfloor + 4 - 3 = n - 3(\frac{n-1}{3}) + 1 = 2$. If $n \equiv 2 \pmod 3$, then $n - 3\lfloor \frac{n}{3} \rfloor + 4 - 4 = n - 3(\frac{n-2}{3}) = 2$. This shows that the right-hand side of (3.1) is the Zeckendorf representation. It remains to show that it is an inverse of F_3 modulo F_n and it is also less than F_n (so that it is the least positive inverse).

Let $m = \lfloor n/3 \rfloor$, $n \equiv r \pmod 3$, and $r \in \{1, 2\}$. Then $m = \frac{n-r}{3}$ and so $n = 3m + r$. Therefore the congruence condition in (3.1) is equivalent to the following :

$$\text{if } n \equiv 1 \pmod 3, \text{ then } 2\left(\sum_{k=0}^{m-2} F_{3m-3k-1} + F_3\right) \equiv 1 \pmod{F_{3m+1}}, \quad (3.2)$$

$$\text{if } n \equiv 2 \pmod 3, \text{ then } 2\left(\sum_{k=0}^{m-2} F_{3m-3k} + F_4\right) \equiv 1 \pmod{F_{3m+2}}. \quad (3.3)$$

We first consider (3.2). Let $y = \sum_{k=0}^{m-2} F_{3m-3k-1} + F_3$. Observe that y can be written as $\sum_{k=0}^{m-1} F_{3k+2} + 1$. By Lemma 2.3,

$$\sum_{k=0}^{m-1} F_{3k+2} = \frac{F_{3m+2} + F_{3m-1} - 2}{4}.$$

Therefore the left hand-side of the congruence in (3.2) is

$$2y = \frac{F_{3m+2} + F_{3m-1} + 2}{2} = \frac{2F_{3m+1} + 2}{2} = F_{3m+1} + 1 \equiv 1 \pmod{F_{3m+1}}.$$

This shows that (3.2) holds, y is an inverse of 2 modulo F_n, and $y = \frac{F_{3m+1}+1}{2} = \frac{F_n+1}{2} < F_n$. Therefore $y = 2^{-1} \bmod F_n$, as required. Similarly, for (3.3), we have

$$\sum_{k=0}^{m-2} F_{3m-3k} = \sum_{k=0}^{m-1} F_{3k+3} - 2 = \frac{F_{3m+3} + F_{3m} - 2}{4} - 2,$$

and therefore the left-hand side of the congruence in (3.3) is

$$\frac{F_{3m+3} + F_{3m} + 2}{2} = F_{3m+2} + 1 \equiv 1 \pmod{F_{3m+2}}.$$

This completes the proof. □

We can write $F_{n-3}^{-1} \bmod F_n$ in terms of 2^{-1} and F_{n-1} modulo F_n, which is shown in Lemma 3.3. Then combining it with Theorem 3.2, we obtain the Zeckendorf representation of $F_{n-3}^{-1} \bmod F_n$ in Theorem 3.4.

Lemma 3.3. *Suppose $n \geq 7$ and $n \not\equiv 0 \pmod 3$. Then*

$$F_{n-3}^{-1} \equiv 2^{-1}(-1)^n F_{n-1} \pmod{F_n}.$$

Proof. Since $(F_n, F_{n-3}) = F_{(n,n-3)} = F_{(n,3)} = F_1 = 1$, $F_{n-3}^{-1} \bmod F_n$ exists. By Lemma 2.1, $F_{n-3}F_{n+3} = F_n^2 + (-1)^{n-2}F_3^2 \equiv 4(-1)^n \pmod{F_n}$ and $F_{n+3} = F_nF_4 + F_{n-1}F_3 \equiv 2F_{n-1} \pmod{F_n}$. Thus $F_{n-3}(2F_{n-1}) \equiv 4(-1)^n \pmod{F_n}$. Since $(2, F_n) = 1$, we have $F_{n-3}F_{n-1} \equiv 2(-1)^n \pmod{F_n}$. So $F_{n-3}(2^{-1})(-1)^nF_{n-1} \equiv 1 \pmod{F_n}$. That is $F_{n-3}^{-1} \equiv 2^{-1}(-1)^nF_{n-1} \pmod{F_n}$, as desired. □

Theorem 3.4. (Another multiplicative inverse of $F_m \bmod F_n$ when m is closed to n) *Assume that $n \geq 7$ and $n \not\equiv 0 \pmod 3$. Then $F_{n-3}^{-1} \bmod F_n$ exists and its Zeckendorf representation is given by*

$$F_{n-3}^{-1} \bmod F_n = \begin{cases} F_{n-1} + \sum_{k=0}^{\frac{n-10}{3}} F_{n-3k-6} + F_2, & \text{if } n \equiv 1 \pmod 6; \\ \sum_{k=0}^{\frac{n-r-3}{3}} F_{n-3k-r+1} + F_2, & \text{if } n \equiv r \pmod 6 \text{ and} \\ & r \in \{2, 4, 5\}. \end{cases} \tag{3.4}$$

Proof. Similar to the proof of Theorem 3.2, it is not difficult to see that the right-hand side of (3.4) is a Zeckendorf representation. So it remains to show that it is indeed $F_{n-3}^{-1} \bmod F_n$.
Case 1 $n \equiv 1 \pmod 6$. Then $n = 6m+1$ for some $m \geq 1$ and the right-hand side of (3.4) is

$$F_{6m} + \sum_{k=0}^{2m-3} F_{6m-3k-5} + F_2 = F_{6m} + \sum_{k=0}^{2m-2} F_{3k+1}. \tag{3.5}$$

By Lemma 2.3,

$$\sum_{k=0}^{2m-2} F_{3k+1} = \frac{F_{6m-2} + F_{6m-5}}{4} = \frac{2F_{6m-3}}{4} = \frac{F_{6m-3}}{2}.$$

Therefore the right-hand side of (3.5) is equal to

$$\begin{aligned} \frac{2F_{6m} + F_{6m-3}}{2} &= \frac{F_{6m} + F_{6m-1} + F_{6m-2} + F_{6m-3}}{2} \\ &= \frac{F_{6m+1} + F_{6m-1}}{2} = \frac{F_n + F_{n-2}}{2}. \end{aligned}$$

By Lemma 2.2, F_n and F_{n-2} are odd and so $(F_n + F_{n-2})/2$ is an integer less than F_n and

$$F_{n-3}\left(\frac{F_n + F_{n-2}}{2}\right) = \frac{F_{n-3}F_n + F_{n-3}F_{n-2}}{2}. \tag{3.6}$$

Observe that

$$F_{n-3}F_{n-2} = (F_n - 2F_{n-2})F_{n-2} \equiv -2F_{n-2}^2 \pmod{F_n}. \tag{3.7}$$

By Theorem 3.1, we obtain that $F_{n-2}^2 \equiv (-1)^n \pmod{F_n}$. Therefore $F_{n-3}F_n + F_{n-3}F_{n-2} \equiv 2(-1)^{n-1} \pmod{F_n}$. Since $(2, F_n) = 1$, this implies that the right-hand side of (3.6) is $\equiv (-1)^{n-1} \equiv 1 \pmod{F_n}$, as desired.
Case 2 $n \equiv r \pmod 6$ for some $r \in \{2, 4, 5\}$. Then $n = 6m + r$ for some $m \geq 1$. Similar to Case 1, we obtain by Lemma 2.3, that the right-hand side of (3.4) is equal to

$$\sum_{k=0}^{2m} F_{3k+1} = \frac{F_{6m+4} + F_{6m+1}}{4} = \frac{2F_{6m+3}}{4} = \frac{F_{6m+3}}{2} = \frac{F_{n-r+3}}{2}.$$

Since $\frac{F_{n-r+3}}{2} \leq \frac{F_{n+1}}{2} < F_n$, it remains to show that

$$\frac{F_{n-3}F_{n-r+3}}{2} \equiv 1 \pmod{F_n}. \tag{3.8}$$

If $r = 2$, then $F_{n-3}F_{n-r+3} = F_{n-3}F_{n+1} \equiv F_{n-3}F_{n-1} \equiv -F_{n-3}F_{n-2} \pmod{F_n}$, and we already proved in (3.7) that this is $\equiv 2F_{n-2}^2 \equiv 2(-1)^n \equiv 2(-1)^{6m+2} \equiv 2 \pmod{F_n}$, which implies (3.8). If $r = 4$, then we similarly obtain that $F_{n-3}F_{n-r+3} = F_{n-3}F_{n-1} \equiv -F_{n-3}F_{n-2} \equiv 2 \pmod{F_n}$, which implies (3.8). If $r = 5$, then $F_{n-3}F_{n-r+3} = F_{n-3}F_{n-2} \equiv 2(-1)^{n-1} \equiv 2 \pmod{F_n}$, which also leads to (3.8). In any case, (3.8) is proved, as desired. This completes the proof. □

Corollary 3.1. *Let $n \geq 7$, $m \in \{3, n-3, n-2, n-1\}$, and $(m, n) \leq 2$. Then F_m^{-1} mod F_n is a Fibonacci number if and only if $m \in \{n-2, n-1\}$.*

Proof. If $m \in \{n-2, n-1\}$, then the result follows from Theorem 3.1. Observe that if x is a Fibonacci number, then $x = F_\ell$ for some ℓ is already a Zeckendorf representation. Since the Zeckendorf representation is unique, we see from Theorems 3.2 and 3.4 that if $m \in \{3, n-3\}$, then F_m^{-1} mod F_n is not a Fibonacci number. This completes the proof. □

Perhaps, Corollary 3.1 also holds for all $m = 3, 4, \ldots, n-1$ with $(m, n) \leq 2$, but we currently do not have a proof. We leave this for future research and we do not mind if the reader will solve it.

References

[1] M. Jaidee, P. Pongsriiam, Arithmetic functions of Fibonacci and Lucas numbers, The Fibonacci Quarterly, **57,** no. 3, (2019), 246–254.

[2] N. Khaochim, P. Pongsriiam, On the order of appearance of products of Fibonacci numbers, Contributions to Discrete Mathematics, **13,** no. 2, (2018), 45–62.

[3] N. Khaochim, P. Pongsriiam, The general case on the order of appearance of product of consecutive Lucas numbers, Acta Mathematica Universitatis Comenianae, **87,** no. 2, (2018), 277–289.

[4] T. Koshy, Fibonacci and Lucas Number with Applications, Wiley, 2001.

[5] K. Onphaeng, P. Pongsriiam, The converse of exact divisibility by powers of the Fibonacci and Lucas numbers, The Fibonacci Quarterly, **56,** no. 4, (2018), 296–302.

[6] P. Phunphayap, P. Pongsriiam, Explicit formulas for the p-adic valuations of Fibonomial coefficients, Journal of Integer Sequences, **21,** no. 3, (2018), Article 18.3.1.

[7] P. Pongsriiam, The order of appearance of factorials in the Fibonacci sequence and certain Diophantine equations, Periodica Mathematica Hungarica, online first version https://link.springer.com/journal/10998/onlineFirst/page/1

[8] P. Pongsriiam, Fibonacci and Lucas numbers associated with Brocard-Ramanujan equation, Communications of the Korean Mathematical Society, **32,** no. 3, (2017), 511–522.

[9] P. Pongsriiam, Fibonacci and Lucas Numbers which are one away from their products, The Fibonacci Quarterly, **55,** no. 1, (2017), 29–40.

[10] P. Pongsriiam, Factorization of Fibonacci numbers into products of Lucas numbers and related results, JP Journal of Algebra, Number Theory and Applications, **38,** no. 4, (2016), 363–372.

[11] P. Pongsriiam, A complete formula for the order of appearance of the powers of Lucas numbers, Communications of the Korean Mathematical Society, **31,** no. 3, (2016), 447–450.

[12] P. Pongsriiam, Exact divisibility by powers of the Fibonacci and Lucas numbers, Journal of Integer Sequences, **17,** no. 11, (2014), Article 14.11.2.

[13] B. Prempreesuk, P. Pongsriiam, N. Kanyamee, Numerical methods for finding multiplicative inverses of a modulo N, Songklanakarin Journal of Science and Technology, **40,** no. 6, (2018), 1361–1367.

[14] D. D. Wall, Fibonacci Series Modulo m, The American Mathematical Monthly, **67,** (1960), 525–532.