

Zeckendorf representation of multiplicative inverses modulo a Fibonacci number

*Original*

Zeckendorf representation of multiplicative inverses modulo a Fibonacci number / Alecci, G., Murru, N., Sanna, C.. - In: MONATSHEFTE FÜR MATHEMATIK. - ISSN 0026-9255. - STAMPA. - 201:(2023). [10.1007/s00605-022-01724-y]

*Availability:*

This version is available at: 11583/2966724 since: 2022-06-11T07:28:50Z

*Publisher:*

Springer

*Published*

DOI:10.1007/s00605-022-01724-y

*Terms of use:*

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

*Publisher copyright*

(Article begins on next page)



# Zeckendorf representation of multiplicative inverses modulo a Fibonacci number

Gessica Alecci<sup>1</sup> · Nadir Murru<sup>2</sup> · Carlo Sanna<sup>1</sup> 

Received: 21 March 2022 / Accepted: 18 May 2022 / Published online: 10 June 2022  
© The Author(s) 2022

## Abstract

Prempreesuk, Noppakaew, and Pongsriiam determined the Zeckendorf representation of the multiplicative inverse of 2 modulo  $F_n$ , for every positive integer  $n$  not divisible by 3, where  $F_n$  denotes the  $n$ th Fibonacci number. We determine the Zeckendorf representation of the multiplicative inverse of  $a$  modulo  $F_n$ , for every fixed integer  $a \geq 3$  and for all positive integers  $n$  with  $\gcd(a, F_n) = 1$ . Our proof makes use of the so-called base- $\varphi$  expansion of real numbers.

**Keywords** Base- $\varphi$  expansion · Fibonacci number · Multiplicative inverse · Zeckendorf representation

**Mathematics Subject Classification** Primary 11B39 · Secondary 11A67, 11A99

## 1 Introduction

Let  $(F_n)_{n \geq 1}$  be the sequence of Fibonacci numbers, which is defined by the initial conditions  $F_1 = F_2 = 1$  and by the linear recurrence  $F_n = F_{n-1} + F_{n-2}$  for  $n \geq 3$ . It is well known [22] that every positive integer  $n$  can be written as a sum of distinct non-

---

Communicated by Adrian Constantin.

---

✉ Nadir Murru  
nadir.murru@unitn.it

Gessica Alecci  
gessica.alecci@polito.it

Carlo Sanna  
carlo.sanna@polito.it

<sup>1</sup> Department of Mathematical Sciences, Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Torino, Italy

<sup>2</sup> Department of Mathematics, Università degli Studi di Trento, Via Sommarive 14, I-38123 Povo (Trento), Italy

consecutive Fibonacci numbers, that is,  $n = \sum_{i=1}^m d_i F_i$ , where  $m \in \mathbb{N}$ ,  $d_i \in \{0, 1\}$ , and  $d_i d_{i+1} = 0$  for all  $i \in \{1, \dots, m-1\}$ . This is called the *Zeckendorf representation* of  $n$  and, apart from the equivalent use of  $F_1$  instead of  $F_2$  or vice versa, is unique.

The Zeckendorf representation of integer sequences has been studied in several works. For instance, Filipponi and Freitag [6, 7] studied the Zeckendorf representation of numbers of the form  $F_{kn}/F_n$ ,  $F_n^2/d$  and  $L_n^2/d$ , where  $L_n$  are the Lucas numbers and  $d$  is a Lucas or Fibonacci number. Filipponi, Hart, and Sanchis [8, 13, 14] analyzed the Zeckendorf representation of numbers of the form  $mF_n$ . Filipponi [8] determined the Zeckendorf representation of  $mF_n F_{n+k}$  and  $mL_n L_{n+k}$  for  $m \in \{1, 2, 3, 4\}$ . Bugeaud [3] studied the Zeckendorf representation of smooth numbers. The study of Zeckendorf representations has been also approached from a combinatorial point of view [1, 9, 12, 21]. Moreover, generalizations of the Zeckendorf representation to linear recurrences other than the sequence of Fibonacci numbers have been considered [4, 5, 10, 11, 16].

For all integers  $a$  and  $m \geq 1$  with  $\gcd(a, m) = 1$ , let  $(a^{-1} \bmod m)$  denote the least positive multiplicative inverse of  $a$  modulo  $m$ , that is, the unique  $b \in \{1, \dots, m\}$  such that  $ab \equiv 1 \pmod{m}$ . Prempreesuk, Noppakaew, and Pongsriiam [17] determined the Zeckendorf representation of  $(2^{-1} \bmod F_n)$ , for every positive integer  $n$  that is not divisible by 3. (The condition  $3 \nmid n$  is necessary and sufficient to have  $\gcd(2, F_n) = 1$ .) In particular, they showed [17, Theorem 3.2] that

$$(2^{-1} \bmod F_n) = \begin{cases} \sum_{k=0}^{(n-7)/2} F_{n-3k-2} + F_3 & \text{if } n \equiv 1 \pmod{3}; \\ \sum_{k=0}^{(n-8)/2} F_{n-3k-2} + F_4 & \text{if } n \equiv 2 \pmod{3}; \end{cases}$$

for every integer  $n \geq 8$ . We extend their result by determining the Zeckendorf representation of the multiplicative inverse of  $a$  modulo  $F_n$ , for every fixed integer  $a \geq 3$  and every positive integer  $n$  with  $\gcd(a, F_n) = 1$ . Precisely, we prove the following result.

**Theorem 1.1** *Let  $a \geq 3$  be an integer. Then there exist integers  $M, n_0, i_0 \geq 1$  and periodic sequences  $\mathbf{z}^{(0)}, \dots, \mathbf{z}^{(M-1)}$  and  $\mathbf{w}^{(1)}, \dots, \mathbf{w}^{(i_0)}$  with values in  $\{0, 1\}$  such that, for all integers  $n \geq n_0$  with  $\gcd(a, F_n) = 1$ , the Zeckendorf representation of  $(a^{-1} \bmod F_n)$  is given by*

$$(a^{-1} \bmod F_n) = \sum_{i=i_0}^{n-1} z_{n-i}^{(n \bmod M)} F_i + \sum_{i=1}^{i_0-1} w_n^{(i)} F_i.$$

From the proof of Theorem 1.1 it follows that  $M, n_0, i_0, \mathbf{z}^{(0)}, \dots, \mathbf{z}^{(M-1)}$ , and  $\mathbf{w}^{(1)}, \dots, \mathbf{w}^{(i_0)}$  can be computed from  $a$  (see also Remark 4.1 at the end of the paper).

## 2 Preliminaries on Fibonacci numbers

Let us recall that for every integer  $n \geq 1$  it holds the *Binet formula*

$$F_n = \frac{\varphi^n - \bar{\varphi}^n}{\sqrt{5}},$$

where  $\varphi := (1 + \sqrt{5})/2$  is the Golden ratio and  $\bar{\varphi} := (1 - \sqrt{5})/2$  is its algebraic conjugate. Furthermore, it is well known that for every integer  $m \geq 1$  the Fibonacci sequence  $(F_n)_{n \geq 1}$  is (purely) periodic modulo  $m$ . Let  $\pi(m)$  denote its period length, or the so-called *Pisano period*.

The next lemma gives a formula for the inverse of  $a$  modulo  $F_n$ .

**Lemma 2.1** *For all integers  $a \geq 1$  and  $n \geq 3$  with  $\gcd(a, F_n) = 1$ , we have that*

$$(a^{-1} \bmod F_n) = \frac{bF_n + 1}{a},$$

where  $b := (-F_r^{-1} \bmod a)$  and  $r := (n \bmod \pi(a))$ .

**Proof** Since  $r \equiv n \pmod{\pi(a)}$ , we have that  $F_r \equiv F_n \pmod{a}$ . In particular, it follows that  $\gcd(a, F_r) = \gcd(a, F_n) = 1$ . Hence,  $F_r$  is invertible modulo  $a$ , and consequently  $b$  is well defined. Moreover, we have that

$$bF_n + 1 \equiv -F_r^{-1}F_r + 1 \equiv 0 \pmod{a},$$

and thus  $c := (bF_n + 1)/a$  is an integer. On the one hand, we have that

$$ac \equiv bF_n + 1 \equiv 1 \pmod{F_n}.$$

On the other hand, since  $b \leq a - 1$  and  $n \geq 3$ , we have that

$$0 \leq c \leq \frac{(a - 1)F_n + 1}{a} = F_n - \frac{F_n - 1}{a} < F_n.$$

Therefore, we get that  $c = (a^{-1} \bmod F_n)$ , as desired.

## 3 Preliminaries on base- $\varphi$ expansion

We need some basic results regarding the so-called *base- $\varphi$  expansion* of real numbers, which was introduced by Bergman [2] in 1957 (see also [19]), and which is a particular case of non-integer base expansion (see, e.g., [15, 18]). Let  $\mathfrak{D}$  be the set of sequences in  $\{0, 1\}$  that have no two consecutive terms equal to 1, and that are not ultimately equal to the periodic sequence  $0, 1, 0, 1, \dots$ . Then for every  $x \in [0, 1)$  there exists a unique sequence  $\delta(x) = (\delta_i(x))_{i \in \mathbb{N}}$  in  $\mathfrak{D}$  such that  $x = \sum_{i=1}^{\infty} \delta_i(x)\varphi^{-i}$ . Precisely,  $\delta_i(x) = \lfloor T^{(i)}(x) \rfloor$  for every  $i \in \mathbb{N}$ , where  $T^{(i)}$  denotes the  $i$ th iterate of the map

$T : [0, 1) \rightarrow [0, 1)$  defined by  $T(\hat{x}) := (\varphi\hat{x} \bmod 1)$  for every  $\hat{x} \in [0, 1)$ . Furthermore, letting  $\mathcal{F} := \mathbb{Q}(\varphi) \cap [0, 1)$ , if  $x \in \mathcal{F}$  then  $\delta(x)$  is ultimately periodic. In particular, if  $x \in \mathcal{F}$  is given as  $x = x_1 + x_2\varphi$ , where  $x_1, x_2 \in \mathbb{Q}$ , then the preperiod and the period of  $\delta(x)$  can be effectively computed by finding the smallest  $i \in \mathbb{N}$  such that  $T^{(i)}(x) = T^{(j)}(x)$  for some  $j \in \mathbb{N}$  with  $j < i$ . Conversely, for every ultimately periodic sequence  $\mathbf{d} = (d_i)_{i \in \mathbb{N}}$  in  $\mathfrak{D}$  we have that the number  $x = \sum_{i=1}^{\infty} d_i \varphi^{-i}$  belongs to  $\mathcal{F}$ , and  $x_1, x_2 \in \mathbb{Q}$  such that  $x = x_1 + x_2\varphi$  can be effectively computed in terms of the preperiod and period of  $\mathbf{d}$  by using the formula for the sum of the geometric series. Moreover, in the case that  $x$  is a rational number in  $[0, 1)$  then  $\delta(x)$  is purely periodic [20].

The next lemma collects two easy inequalities for sums involving sequences in  $\mathfrak{D}$ .

**Lemma 3.1** *For every sequence  $(d_i)_{i \in \mathbb{N}}$  in  $\mathfrak{D}$  and for every  $m \in \mathbb{N} \cup \{\infty\}$ , we have:*

- (1)  $\sum_{i=1}^m d_i \varphi^{-i} \in [0, 1)$  and
- (2)  $\sum_{i=1}^m d_i (-\varphi)^{-i} \in (-1, \varphi^{-1})$ .

**Proof** Since  $(d_i)_{i \in \mathbb{N}}$  belongs to  $\mathfrak{D}$ , there exists  $k \in \mathbb{N}$  such that  $d_k = d_{k+1} = 0$ . Let  $k$  be the minimum integer with such property. Then

$$\begin{aligned} \sum_{i=1}^{\infty} d_i \varphi^{-i} &= \sum_{i=1}^{k-1} d_i \varphi^{-i} + \sum_{i=k+2}^{\infty} d_i \varphi^{-i} < \sum_{j=1}^{\lfloor k/2 \rfloor} \varphi^{-(2j-1)} + \sum_{i=k+2}^{\infty} \varphi^{-i} \\ &= \left(1 - \varphi^{-2\lfloor k/2 \rfloor}\right) + \varphi^{-k} \leq 1, \end{aligned}$$

and (1) is proved. Let us prove (2). On the one hand, we have

$$\sum_{i=1}^m d_i (-\varphi)^{-i} \leq \sum_{j=1}^m d_{2j} \varphi^{-2j} < \sum_{j=1}^{\infty} \varphi^{-2j} = \varphi^{-1},$$

where the second inequality is strict because  $\mathfrak{D}$  does not contain sequences that are ultimately equal to  $(0, 1, 0, 1, \dots)$ . On the other hand, similarly, we have

$$\sum_{i=1}^m d_i (-\varphi)^{-i} \geq -\sum_{j=1}^m d_{2j-1} \varphi^{-(2j-1)} > -\sum_{j=1}^{\infty} \varphi^{-(2j-1)} = -1.$$

Thus (2) is proved.

The following lemma relates base- $\varphi$  expansion and Zeckendorf representation.

**Lemma 3.2** *Let  $N$  be a positive integer and write  $N = x\varphi^m / \sqrt{5}$  for some  $x \in \mathcal{F}$  and some integer  $m \geq 2$ . Then the Zeckendorf representation of  $N$  is given by*

$$N = \sum_{i=1}^{m-1} \delta_{m-i}(x) F_i.$$

Moreover, we have  $\delta_m(x) = 0$ .

**Proof** Let  $R := N - \sum_{i=1}^{m-1} \delta_{m-i}(x)F_i$ . We have to prove that  $R = 0$ . Since  $R$  is an integer, it suffices to show that  $|R| < 1$ . We have

$$\begin{aligned} \sqrt{5}N &= x\varphi^m = \sum_{i=1}^{\infty} \delta_i(x)\varphi^{m-i} = \sum_{i=1}^m \delta_i(x)\varphi^{m-i} + \sum_{i=m+1}^{\infty} \delta_i(x)\varphi^{m-i} \\ &= \sum_{i=0}^{m-1} \delta_{m-i}(x)\varphi^i + \sum_{i=1}^{\infty} \delta_{i+m}(x)\varphi^{-i} \\ &= \sum_{i=0}^{m-1} \delta_{m-i}(x)(\varphi^i - \bar{\varphi}^i) + \sum_{i=0}^{m-1} \delta_{m-i}(x)\bar{\varphi}^i + \sum_{i=1}^{\infty} \delta_{i+m}(x)\varphi^{-i} \\ &= \sqrt{5} \sum_{i=1}^{m-1} \delta_{m-i}(x)F_i + \sum_{i=0}^{m-1} \delta_{m-i}(x)(-\varphi)^{-i} + \sum_{i=1}^{\infty} \delta_{i+m}(x)\varphi^{-i}. \end{aligned}$$

Hence, we get that

$$\sqrt{5}R = \sum_{i=0}^{m-1} \delta_{m-i}(x)(-\varphi)^{-i} + \sum_{i=1}^{\infty} \delta_{i+m}(x)\varphi^{-i}.$$

For the sake of contradiction, suppose that  $\delta_m(x) = 1$ . Then  $\delta_{m+1}(x) = 0$  and, by Lemma 3.1, it follows that

$$\sqrt{5}R = 1 + \sum_{i=1}^{m-1} \delta_{m-i}(x)(-\varphi)^{-i} + \sum_{i=2}^{\infty} \delta_{i+m}(x)\varphi^{-i} \in (1 - 1 + 0, 1 + \varphi^{-1} + \varphi^{-1}) = (0, \sqrt{5}),$$

which is a contradiction, since  $R$  is an integer.

Therefore,  $\delta_m(x) = 0$  and, again by Lemma 3.1, we have

$$\sqrt{5}R = \sum_{i=1}^{m-1} \delta_{m-i}(x)(-\varphi)^{-i} + \sum_{i=1}^{\infty} \delta_{i+m}(x)\varphi^{-i} \in (-1 + 0, \varphi^{-1} + 1) \subseteq (-\sqrt{5}, \sqrt{5}),$$

so that  $|R| < 1$ , as desired.

The next lemma regards the base- $\varphi$  expansions of the sum of two numbers.

**Lemma 3.3** *Let  $x, y \in [0, 1)$ ,  $m \in \mathbb{N}$ , and put  $v := x + y\varphi^{-m}$ . Suppose that there exists  $\lambda \in \mathbb{N}$  such that  $\lambda + 2 \leq m$  and  $\delta_\lambda(x) = \delta_{\lambda+1}(x) = 0$ . Then, putting*

$$w := \sum_{i=\lambda+2}^{\infty} \delta_i(x)\varphi^{-i} + \sum_{i=m+1}^{\infty} \delta_{i-m}(y)\varphi^{-i},$$

we have that  $v, w \in [0, 1)$  and

$$\delta_i(v) = \begin{cases} \delta_i(x) & \text{if } i \leq \lambda, \\ \delta_i(w) & \text{if } i > \lambda, \end{cases} \quad (1)$$

for every  $i \in \mathbb{N}$ .

**Proof** From Lemma 3.1(1), we have that

$$0 \leq w < \varphi^{-(\lambda+1)} + \varphi^{-m} < \varphi^{-(\lambda+1)} + \varphi^{-(\lambda+2)} = \varphi^{-\lambda}.$$

Hence,  $w \in [0, \varphi^{-\lambda}) \subseteq [0, 1)$  and so  $w = \sum_{i=\lambda+1}^{\infty} \delta_i(w)\varphi^{-i}$ . Therefore, recalling that  $\delta_{\lambda+1}(x) = 0$ , we get that

$$\begin{aligned} v &= x + y\varphi^{-m} = \sum_{i=1}^{\infty} \delta_i(x)\varphi^{-i} + \sum_{i=1}^{\infty} \delta_i(y)\varphi^{-i-m} = \sum_{i=1}^{\infty} \delta_i(x)\varphi^{-i} + \sum_{i=m+1}^{\infty} \delta_{i-m}(y)\varphi^{-i} \\ &= \sum_{i=1}^{\lambda} \delta_i(x)\varphi^{-i} + w = \sum_{i=1}^{\lambda} \delta_i(x)\varphi^{-i} + \sum_{i=\lambda+1}^{\infty} \delta_i(w)\varphi^{-i}, \end{aligned}$$

which is the base- $\varphi$  expansion of  $v$ . (Note that  $\delta_{\lambda}(x) = 0$ .) In particular, by Lemma 3.1(1), we have that  $v \in [0, 1)$ . Thus (1) follows.

#### 4 Proof of Theorem 1.1

Fix an integer  $a \geq 3$ . Let us begin by defining  $M, n_0, i_0$ , and  $z^{(0)}, \dots, z^{(M-1)}$ . Put  $M := \pi(a)$ . For each  $r \in \{0, \dots, M-1\}$  with  $\gcd(a, F_r) = 1$ , let  $b_r := (-F_r^{-1} \bmod a)$ ,  $x_r := b_r/a$ , and  $z^{(r)} := \delta(x_r)$ . Note that  $x_r \in (0, 1)$ . Since  $x_r$  is a positive rational number, we have that  $z^{(r)}$  is a (purely) periodic sequence belonging to  $\mathfrak{D}$ . Let  $\ell$  be the least common multiple of the period lengths of  $z^{(0)}, \dots, z^{(M-1)}$ , and put  $i_0 := \ell + 3$ . Finally, let  $n_0 := \max\{i_0 + 1, \lceil \log(2a)/\log \varphi \rceil\}$ .

Pick an integer  $n \geq n_0$  with  $\gcd(a, F_n) = 1$  and, for the sake of brevity, put  $r := (n \bmod M)$ . From Lemma 2.1 and Binet's formula (2), we get that

$$(a^{-1} \bmod F_n) = \frac{b_r F_n + 1}{a} = \frac{b_r(\varphi^n - \bar{\varphi}^n)}{\sqrt{5}a} + \frac{1}{a} = (x_r + y_n \varphi^{-n}) \frac{\varphi^n}{\sqrt{5}}, \quad (2)$$

where

$$y_n := \frac{\sqrt{5}}{a} - x_r(-\varphi)^{-n}.$$

Since  $n \geq n_0$ , it follows that  $y_n \in (0, 1)$  and  $x_r + y_n\varphi^{-n} \in (0, 1)$ . Therefore, from (2) and Lemma 3.2, we get that

$$(a^{-1} \bmod F_n) = \sum_{i=1}^{n-1} \delta_{n-i}(x_r + y_n\varphi^{-n})F_i.$$

Since  $\delta(x_r)$  is (purely) periodic and belongs to  $\mathfrak{D}$ , we have that  $\delta(x_r)$  contains infinitely many pairs of consecutive zeros. Furthermore, since the period length of  $\delta(x_r)$  is at most  $\ell$ , we have that among every  $\ell + 1$  consecutive terms of  $\delta(x_r)$  there are two consecutive zero. In particular, there exists  $\lambda = \lambda(r)$  such that  $n - \ell - 3 \leq \lambda \leq n - 2$  and  $\delta_\lambda(x_r) = \delta_{\lambda+1}(x_r) = 0$ . Consequently, by Lemma 3.3, we get that  $\delta_i(x_r + y_n\varphi^{-n}) = \delta_i(x_r)$  for each positive integer  $i \leq \lambda$  and, a fortiori, for each positive integer  $i \leq n - i_0$ . Therefore, we have that

$$\begin{aligned} (a^{-1} \bmod F_n) &= \sum_{i=i_0}^{n-1} \delta_{n-i}(x_r)F_i + \sum_{i=1}^{i_0-1} \delta_{n-i}(x_r + y_n\varphi^{-n})F_i \tag{3} \\ &= \sum_{i=i_0}^{n-1} z_{n-i}^{(r)}F_i + \sum_{i=1}^{i_0-1} w_n^{(i)}F_i, \end{aligned}$$

where  $w^{(1)}, \dots, w^{(i_0)}$  are the sequences defined by  $w_n^{(i)} := \delta_{n-i}(x_r + y_n\varphi^{-n})$ . Note that, by construction,

$$z_1^{(r)}, z_2^{(r)}, \dots, z_{n-i_0}^{(r)}, w_n^{(i_0-1)}, w_n^{(i_0-2)}, \dots, w_n^{(1)}$$

is a string in  $\{0, 1\}$  with no consecutive zeros. Hence, (3) is the Zeckendorf representation of  $(a^{-1} \bmod F_n)$ .

It remains only to prove that  $w^{(1)}, \dots, w^{(i_0)}$  are periodic. By (3) and the uniqueness of the Zeckendorf representation, it suffices to prove that

$$R(n) := (a^{-1} \bmod F_n) - \sum_{i=i_0}^{n-1} z_{n-i}^{(r)}F_i = \sum_{i=1}^{i_0-1} w_n^{(i)}F_i \tag{4}$$

is a periodic function of  $n$ . From the last equality in (4), we have that  $0 \leq R(n) < \sum_{i=1}^{i_0-1} F_i$ . (Actually, one can prove that  $0 \leq R(n) < F_{i_0}$ , but this is not necessary for our proof.) Fix a prime number  $p > \max\{a, \sum_{i=1}^{i_0-1} F_i\}$ . It suffices to prove that  $R(n)$  is periodic modulo  $p$ . Recalling that  $(a^{-1} \bmod F_n) = (b_r F_n + 1)/a$  and that the sequence of Fibonacci numbers is periodic modulo  $p$ , it follows that  $(a^{-1} \bmod F_n)$  is periodic modulo  $p$ . Hence, it suffices to prove that  $R'(n) := \sum_{i=i_0}^{n-1} z_{n-i}^{(r)}F_i$  is periodic modulo  $p$ . Using that  $z^{(r)}$  has period length dividing  $\ell$ , we get that

$$\begin{aligned}
R'(n + \ell M) - R'(n) &= \sum_{i=i_0}^{n+\ell M-1} z_{n+\ell M-i}^{((n+\ell M) \bmod M)} F_i - \sum_{i=i_0}^{n-1} z_{n-i}^{(r)} F_i \\
&= \sum_{i=i_0}^{n+\ell M-1} z_{n+\ell M-i}^{(r)} F_i - \sum_{i=i_0}^{n-1} z_{n-i}^{(r)} F_i \\
&= \sum_{i=n}^{n+\ell M-1} z_{n+\ell M-i}^{(r)} F_i + \sum_{i=i_0}^{n-1} (z_{n+\ell M-i}^{(r)} - z_{n-i}^{(r)}) F_i \\
&= \sum_{j=1}^{\ell M} z_j^{(r)} F_{n+\ell M-j},
\end{aligned}$$

which is a linear combination of sequences that are periodic modulo  $p$ . Hence  $R'(n)$  is periodic modulo  $p$ . The proof is complete.

**Remark 4.1** The proof of Theorem 1.1 provides a way to compute the positive integers  $M, i_0, n_0$  and the periods of the periodic sequences  $z^{(0)}, \dots, z^{(M-1)}$  and  $w^{(1)}, \dots, w^{(i_0)}$ . Indeed, going through the proof, we have that:  $M = \pi(a)$  is the Pisano period of  $a$ , which can be computed in an obvious way;  $z^{(r)} = \delta((-F_r^{-1} \bmod a)/a)$  and so the period of  $z^{(r)}$  can be computed as explained at the beginning of Section 3;  $i_0$  and  $n_0$  have simple formulas in terms of  $\ell$ , which is the least common multiple of the period lengths of  $z^{(0)}, \dots, z^{(M-1)}$ . Finally, the periods of  $w^{(1)}, \dots, w^{(i_0)}$  can be computed from (4) and the fact that  $R(n)$  is periodic with period length at most  $\pi(p)^2 \ell M$ , which follows from the arguments after (4). However, note that proceeding in this way might be impractical, since  $\ell$  might be exponential in  $M$ , and thus  $p$  might be double exponential in  $M$ ; making the search for the periods of  $w^{(1)}, \dots, w^{(i_0)}$  extremely long.

**Acknowledgements** The authors are members of GNSAGA of INdAM and of CryptTO, the group of Cryptography and Number Theory of Politecnico di Torino.

**Funding** Open access funding provided by Università degli Studi di Trento within the CRUI-CARE Agreement.

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

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

## References

1. Artz, J., Rowell, M.: A tiling approach to Fibonacci product identities. *Involve* **2**(5), 581–587 (2009)
2. Bergman, G.: A number system with an irrational base. *Math. Mag.* **31**, 98–110 (1957/58)
3. Bugeaud, Y.: On the Zeckendorf representation of smooth numbers. *Moscow Math. J.* **21**(1), 31–42 (2021)
4. Daykin, D.E.: Representation of natural numbers as sums of generalized Fibonacci numbers. *J. London Mathematical Society* **35**, 143–160 (1960)
5. Demontigny, P., Do, T., Kulkarni, A., Miller, S.J., Moon, D., Varma, U.: Generalizing Zeckendorf's Theorem to  $f$ -decompositions. *J. Number Theory* **141**, 136–158 (2014)
6. Filippini, P., Freitag, H.T.: On the  $F$ -Representation of Integral Sequences  $\{F_n^2/d\}$  and  $\{L_n^2/d\}$  where  $d$  is Either a Fibonacci or a Lucas Number. *Fibonacci Quart.* **27**(3), 276–282 (1989)
7. Filippini, P., Freitag, H.T.: The Zeckendorf Representation of  $\{F_{kn}/F_n\}$ . *Applications of Fibonacci Numbers* **5**, 217–19 (1993)
8. Filippini, P., Hart, E.L.: The Zeckendorf decomposition of certain Fibonacci-Lucas products. *Fibonacci Quart.* **36**(3), 240–247 (1998)
9. Gerdemann, D.: Combinatorial proofs of Zeckendorf family identities. *Fibonacci Quart.* **46**(47), 249–261 (2009)
10. Grabner, P.J., Tichy, R.F.: Contributions to digit expansions with respect to linear recurrences. *J. Number Theory* **35**, 160–169 (1990)
11. Grabner, P.J., Tichy, R.F.: Generalized Zeckendorf expansions. *Appl. Math. Lett.* **7**(2), 25–28 (1994)
12. McGregor, D., Rowell, M.J.: Combinatorial proofs of Zeckendorf representations of Fibonacci and Lucas products. *Involve* **4**(1), 75–89 (2011)
13. Hart, E.L.: On Using Patterns in Beta-Expansions To Study Fibonacci-Lucas Products. *Fibonacci Quart.* **36**, 396–406 (1998)
14. Hart, E., Sanchis, L.: On the occurrence of  $F_n$  in the Zeckendorf decomposition of  $nF_n$ . *Fibonacci Quart.* **37**, 21–33 (1999)
15. Parry, W.: On the  $\beta$ -expansions of real numbers. *Acta Math. Acad. Sci. Hungar.* **11**, 401–416 (1960)
16. Pethő, A., Tichy, R.F.: On digit expansions with respect to linear recurrences. *J. Number Th.* **33**, 243–256 (1989)
17. Premreesuk, B., Noppakaew, P., Pongsriiam, P.: Zeckendorf representation and multiplicative inverse of  $F_m \bmod F_n$ . *Int. J. Math. Comput. Sci.* **15**(1), 17–25 (2020)
18. Rényi, A.: Representations for real numbers and their ergodic properties. *Acta Math. Acad. Sci. Hungar.* **8**, 477–493 (1957)
19. Rousseau, C.: The phi number system revisited. *Math. Mag.* **68**(4), 283–284 (1995)
20. Schmidt, K.: On periodic expansions of Pisot numbers and Salem numbers. *Bull. London Math. Soc.* **12**, 269–278 (1980)
21. Wood, P.M.: Bijective proofs for Fibonacci identities related to Zeckendorf's theorem. *Fibonacci Quart.* **45**(2), 138–145 (2007)
22. Zeckendorf, E.: Représentation des nombres naturels par une somme de nombres de Fibonacci ou de nombres de Lucas. *Bull. Soc. Roy. Sci. Liege* **41**, 179–82 (1972)

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.