The multiplicative inverses modulo a Fibonacci number in terms of the Zeckendorf representation

Based on a joint work with N. Murru and C. Sanna

Gessica Alecci

6^{th} Number Theory Meeting

Politecnico di Torino

22^{nd} September, 2022

Preliminaries on Fibonacci numbers

Let $(F_n)_{n\geq 1}$ be the sequence of Fibonacci numbers, defined as usual by

$$F_1 = F_2 = 1 \qquad \text{and} \qquad F_n = F_{n-1} + F_{n-2}$$

for $n \geq 3$.
Every positive integer n can be uniquely written as a sum of distinct non-consecutive Fibonacci numbers

$$n = \sum_{i=1}^{m} d_i F_i$$

where $m \in \mathbb{N}$, $d_i \in \{0, 1\}$, and $d_i d_{i+1} = 0$ for all $i \in \{1, \ldots, m-1\}$.
This is called the *Zeckendorf representation* of n.

Algorithm to find the Zeckendorf representation

Find the Zeckendorf representation of the positive integer n.

1. Let F_k be the greatest Fibonacci number not greater than n, subtract F_k to n and set d_k as 1;
2. if the remainder of the subtraction is 0, the Zeckendorf representation has been found, if not repeat step 1 till the remainder is 0.

Examples

$$19 = 8 + 5 + 3 + 2 + 1 \qquad \text{NO}$$
$$19 = 13 + 5 + 1 \qquad \text{YES}$$

$$19 = 1 \cdot F_7 + 0 \cdot F_6 + 1 \cdot F_5 + 0 \cdot F_4 + 0 \cdot F_3 + 1 \cdot F_2 + 0 \cdot F_1$$
$$Z(19) = 1010010$$

$$\begin{aligned} 2022 = {} & 1 \cdot F_{17} + 0 \cdot F_{16} + 0 \cdot F_{15} + 1 \cdot F_{14} + 0 \cdot F_{13} + \\ & 0 \cdot F_{12} + 0 \cdot F_{11} + 0 \cdot F_{10} + 1 \cdot F_9 + 0 \cdot F_8 + 1 \cdot F_7 + \\ & 0 \cdot F_6 + 0 \cdot F_5 + 0 \cdot F_4 + 0 \cdot F_3 + 1 \cdot F_2 + 0 \cdot F_1 \end{aligned}$$
$$Z(2022) = 10010000101000010$$

Multiplicative inverse of 2 mod F_n

Theorem (Prempreesuk, Noppakaew, and Pongsriiam)

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

for every integer $n \geq 7$ and $n \not\equiv 0 \pmod 3$.

Multiplicative inverse of 2 mod F_n

Theorem (Prempreesuk, Noppakaew, and Pongsriiam)

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

for every integer $n \geq 7$ and $n \not\equiv 0 \pmod 3$.

Problem

What about the multiplicative inverse of a modulo F_n, for every fixed integer $a \geq 3$ and every positive integer n with $\gcd(a, F_n) = 1$?

Multiplicative inverse of a mod F_n

Theorem (Murru, Sanna, and A.)

Let $a \geq 3$ be an integer. Then there exist integers $M, n_0, i_0 \geq 1$ and periodic sequences $\boldsymbol{z}^{(0)}, \ldots, \boldsymbol{z}^{(M-1)}$ and $\boldsymbol{w}^{(1)}, \ldots, \boldsymbol{w}^{(i_0)}$ 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

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

Later we'll see a sketch of the proof.

Preliminaries on Fibonacci numbers

For every integer $n \geq 1$ it holds the *Binet formula*

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

where $\varphi := (1+\sqrt{5})/2$ is the Golden mean and $\overline{\varphi} := (1-\sqrt{5})/2$ is its algebraic conjugate.

Furthermore, for every integer $m \geq 1$ the Fibonacci sequence $(F_n)_{n\geq 1}$ is (purely) periodic modulo m and let $\pi(m)$ denote its period length (the so-called *Pisano period*).

Preliminaries on Fibonacci numbers

Lemma 1

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

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

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

Proof of Lemma 1

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.

Preliminaries on Fibonacci numbers

Lemma 1

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

$$(a^{-1} \bmod F_n) = \frac{bF_n + 1}{a}, \tag{2}$$

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

The formula (2) allows us to find $a^{-1} \bmod F_n$ as a sum of rational numbers but the Zeckendorf representation is defined for integer numbers.

Preliminaries on base-φ expansion

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 $0,1,0,1,\ldots$.
Then for every $x \in [0,1)$ there exists a unique sequence $\boldsymbol{\delta}(x) = (\delta_i(x))_{i\in\mathbb{N}}$ in $\mathfrak{D}$ such that $x = \sum_{i=1}^{\infty} \delta_i(x)\varphi^{-i}$.
Furthermore, if $x \in \mathbb{Q}(\varphi) \cap [0,1)$ then $\boldsymbol{\delta}(x)$ is purely periodic.

Lemma 2

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

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

Connecting base-φ expansion and Zeckendorf repr.

Lemma 3

Let N be a positive integer and write $N = x\varphi^m/\sqrt{5}$ for some $x \in \mathbb{Q}(\varphi) \cap [0,1)$ 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 $\delta_m(x) = 0$.

Base-φ expansions of the sum of two numbers

Lemma 4

Let $x, y \in [0,1)$, $m \in \mathbb{N}$, and put $v := x + y\varphi^{-m}$. If $\exists \lambda \in \mathbb{N}$ 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

$$\delta_i(v) = \begin{cases} \delta_i(x) & \text{if } i \leq \lambda, \\ \delta_i(w) & \text{if } i > \lambda, \end{cases} \tag{3}$$

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

Sketch of the proof (1/2)

Main idea: write $(a^{-1} \bmod F_n)$ as a linear combination of sequences.

Sketch of the proof (1/2)

Main idea: write $(a^{-1} \bmod F_n)$ as a linear combination of sequences.

Firstly, we put $M := \pi(a)$. For each $r \in \{0, \ldots, M-1\}$ with $\gcd(a, F_r) = 1$, let $b_r := (-F_r^{-1} \bmod a)$, $x_r := b_r/a$, and $\boldsymbol{z}^{(r)} := \boldsymbol{\delta}(x_r)$.

Sketch of the proof (1/2)

Main idea: write $(a^{-1} \bmod F_n)$ as a linear combination of sequences.

Firstly, we put $M := \pi(a)$. For each $r \in \{0, \ldots, M-1\}$ with $\gcd(a, F_r) = 1$, let $b_r := (-F_r^{-1} \bmod a)$, $x_r := b_r/a$, and $\boldsymbol{z}^{(r)} := \boldsymbol{\delta}(x_r)$.
We rewrite $(a^{-1} \bmod F_n) = (x_r + y_n\varphi^{-n})\frac{\varphi^n}{\sqrt{5}}$ where $y_n := \frac{\sqrt{5}}{a} - x_r(-\varphi)^{-n}$.
From Lemma 3 we get that

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

Sketch of the proof (1/2)

Main idea: write $(a^{-1} \bmod F_n)$ as a linear combination of sequences.

Firstly, we put $M := \pi(a)$. For each $r \in \{0, \ldots, M-1\}$ with $\gcd(a, F_r) = 1$, let $b_r := (-F_r^{-1} \bmod a)$, $x_r := b_r/a$, and $\boldsymbol{z}^{(r)} := \boldsymbol{\delta}(x_r)$.
We rewrite $(a^{-1} \bmod F_n) = (x_r + y_n\varphi^{-n})\frac{\varphi^n}{\sqrt{5}}$ where $y_n := \frac{\sqrt{5}}{a} - x_r(-\varphi)^{-n}$.
From Lemma 3 we get that

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

Secondly, we define the sequences $\boldsymbol{w}^{(1)}, \cdots, \boldsymbol{w}^{(i_0)}$ such that $w_n^{(i)} := \delta_{n-i}(x_r + y_n\varphi^{-n})$.
So from Lemma 4, we have

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

Sketch of the proof (2/2)

By construction,

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

is a string in $\{0,1\}$ with no consecutive 1's so (4) is the Zeckendorf representation of $(a^{-1} \bmod F_n)$.
Note that $\boldsymbol{w}^{(1)}, \cdots, \boldsymbol{w}^{(i_0)}$ are periodic because

$$R(n) := (a^{-1} \bmod F_n) - \sum_{i=i_0}^{n-1} z_{n-i}^{(r)} F_i = \sum_{i=1}^{i_0-1} w_n^{(i)} F_i \tag{5}$$

is a periodic function of n.

Open problems

Filipponi and Freitag 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.

Problem 1

What can we say about the Zeckendorf representation of F_m^k mod F_n with $k \geq 3$?

Open problems

Filipponi and Freitag 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.

Problem 1

What can we say about the Zeckendorf representation of F_m^k mod F_n with $k \geq 3$?

Grabner and others considered the generalizations of the Zeckendorf representation for other linear recurrences.

Problem 2

What about these kinds of representations with other sequences?

References

- E. Zeckendorf. *Répresentation des nombres naturels par une somme de nombres de Fibonacci ou de nombres de Lucas*, Bull. Soc. Roy. Sci. Liege **41** (1972), 179–82.
- 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.
- A. Rényi, *Representations for real numbers and their ergodic properties*, Acta Math. Acad. Sci. Hungar. **8** (1957), 477–493.
- G. Alecci, N. Murru, and C. Sanna, *Zeckendorf representation of multiplicative inverses modulo a Fibonacci number*, Monatshefte für Mathematik (2022).

Thank you!

gessica.alecci@polito.it