

Midy's Theorem in non-integer bases and divisibility of Fibonacci numbers

Zuzana Masáková and Edita Pelantová

Abstract. Fractions $\frac{p}{q} \in [0, 1)$ with prime denominator q written in decimal have a curious property described by Midy's Theorem, namely that two halves of their period (if it is of even length $2n$) sum up to $10^n - 1$. A number of results generalise Midy's theorem to expansions of $\frac{p}{q}$ in different integer bases, considering non-prime denominators, or dividing the period into more than two parts. We show that a similar phenomena can be studied even in the context of numeration systems with non-integer bases, as introduced by Rényi. First we define the Midy property for a general real base $\beta > 1$ and derive a necessary condition for validity of the Midy property. For $\beta = \frac{1}{2}(1 + \sqrt{5})$ we characterize prime denominators q , which satisfy the property.

Contents

1 Introduction	2
2 Preliminaries	3
3 Necessary condition	6
4 Sufficient condition for the base $\tau = \frac{1+\sqrt{5}}{2}$	8
5 The Midy property of prime numbers	12

MSC 2020: 11A63 (primary); 11K16, 11B39 (secondary).

Keywords: Midy theorem, β -expansions, Fibonacci numbers.

Contact information:

Z. Masáková:

Affiliation: FNSPE, Czech Technical University in Prague, Czech Republic.

Email: zuzana.masakova@jfifi.cvut.cz

E. Pelantová:

Affiliation: FNSPE, Czech Technical University in Prague, Czech Republic.

Email: edita.pelantova@jfifi.cvut.cz

1 Introduction

The number $\frac{3}{7}$ in decimal system has a purely periodic expansion, namely $0.(428571)^\omega$. Note that the first half of the period 428 and the second half 571 sum up to 999. Similar behaviour appears with the fraction $\frac{18}{19} = 0.(947368421052631578)^\omega$. The sum of the two halves of the period is $947368421 + 052631578 = 999999999$. Here we always consider the period of minimal length.

According to Dickson [3], this phenomenon for fractions of the form $\frac{1}{q}$ with prime denominator was observed experimentally already by Goodwyn in 1802 [5].

The first proof of this fact was probably given in 1836 by a French college mathematics professor Étienne Midy in his privately published treatise on the properties of numbers and periodic decimal fractions [12]. Nowadays, under the name Midy's theorem, one usually finds the following result, although in Midy's text, one can actually find methods to show stronger properties of decimal fractions.

Theorem 1.1. *Let $q > 5$ be a prime number. If a rational number $\frac{p}{q} \in (0, 1)$ has the minimal period of even length then the sum of the first and the second half of the period is a number whose expansion in the decimal system uses only the digit 9.*

One can hardly cherish expectations of some theoretical consequences of this theorem, yet alone a down to earth application. Nevertheless, this result can serve for the general public as an illustration that mathematics can simply be fun. Proofs and generalisations of this theorem have been for decades a source of amusement of many, both mathematical amateurs and professionals. A historical survey can be found in [18] and later [15].

A nice presentation of Midy's theorem using group-theoretical proofs is given by Leavitt [9], who calls the phenomenon the nines-property and gives a criterion to decide about the parity of the period-length of the fraction $\frac{p}{q}$ in the decimal system in terms of quadratic residues. Leavitt also shows a sufficient condition for a fraction with non-prime denominator to have the nines-property.

A number of authors have focused on generalisations of Midy's theorem to considering fractions with non-prime denominators, cutting the period of the fraction into more than two blocks of equal length, and translating the problem into non-decimal number systems with integer base $b \in \mathbb{N}$, see e.g. [4, 6, 10, 11].

The aim of this contribution is to give a first glimpse to similar phenomena that appear when looking at fractions in numeration systems with non-integer base. In 1957 A. Rényi [16] introduced positional systems where the role of base is played by any real $\beta > 1$. A representation of a given positive number x in the form $x = \sum_{k=-\infty}^N x_k \beta^k$, with $x_k \in \mathbb{N}$, is found by the greedy algorithm and is called the β -expansion of x . The greedy algorithm produces digits in the set $\mathcal{D} = \{0, 1, \dots, \lceil \beta \rceil - 1\}$. In case that the base β is not an integer, some combinations of digits do not appear in the β -expansion of any positive number x . One can characterize the strings of digits admissible for β -expansions

using lexicographic comparison with the so-called quasigreedy β -expansion of the number 1, usually denoted by $d_\beta^*(1) = t_1^* t_2^* t_3^* \cdots$, see [13]. The string $d_\beta^*(1)$ is composed of digits over the set \mathcal{D} , and it is the lexicographically largest string with infinitely many non-zero digits such that $1 = \sum_{k=1}^{+\infty} t_k^* \beta^{-k}$. For example, if $\beta = 10$, then $d_\beta^*(1) = 9^\omega$.

Our special attention is given to the numeration system with the golden ratio base $\tau = \frac{1+\sqrt{5}}{2} \approx 1.618$. The digits in this system are only 0 and 1 and the base satisfies $\tau^2 = \tau + 1$. Consequently, the quasigreedy τ -expansion of 1 is $d_\tau^*(1) = (10)^\omega$.

It is known [17] that every rational number $\frac{p}{q} \in (0, 1)$ has a purely periodic τ -expansion. For example, $\frac{3}{7}$ has the τ -expansion $0.(0100001001010010)^\omega$, whose period-length is equal to 16. The first half of the period 01000010 represents the number $x_1 = \tau^6 + \tau$, whereas the second half 01010010 gives $x_2 = \tau^6 + \tau^4 + \tau$. Using $\tau^{k+2} = \tau^{k+1} + \tau^k$, we easily derive that $x_1 + x_2 = \tau^7 + \tau^5 + \tau^3 + \tau = \tau^8 - 1$ and hence, the τ -expansion of the sum is equal to 10101010. Note that this string is a prefix of the quasigreedy expansion $d_\tau^*(1)$. In case of the classical decimal system, the sum of the two halves of the period is a prefix of the string 9^ω , which is the quasigreedy expansion of unity for the decimal base.

In both the presented examples for the bases $\beta = 10$ and $\beta = \tau$ it holds that if a period of a fraction is of even length, say $2n$, then the sum of the two halves has the value $\beta^n - 1$.

This observation suggests how the ‘nines-property’ given for the decimal system can be extended to systems with arbitrary real base $\beta > 1$, see Definition 2.2. In Section 3 we show necessary condition so that a fraction with denominator q has the Midy property in a base $\beta > 1$. In Section 4 we study sufficient conditions for the golden ratio base τ . With the use of divisibility properties of Fibonacci numbers, we characterize the prime denominators $q \in \mathbb{N}$, for which an analogy of Midy's theorem holds in base τ , see Section 5.

2 Preliminaries

Given a real number $\beta > 1$, one can obtain the β -expansion of a positive real number x by the greedy algorithm: Find k such that $\beta^k \leq x < \beta^{k+1}$, $r_k = x$, and for $i \leq k$ repeat: $x_i := \lfloor r_i / \beta^i \rfloor$, $r_{i-1} := x - x_i \beta^i$. Then

$$x = \sum_{i \leq k} x_i \beta^i, \quad x_j \in \mathcal{D} := \{k \in \mathbb{N} : k < \beta\},$$

and for every $j \leq k$, we have $\sum_{i \leq j} x_i \beta^i < \beta^{j+1}$. For the β -expansion of x , we write

$$(x)_\beta = \begin{cases} x_k x_{k-1} \cdots x_0 . x_{-1} x_{-2} \cdots & \text{if } k \geq 0, \\ 0.0^{-k-1} x_k x_{k-1} \cdots & \text{if } k < 0. \end{cases}$$

In case $x \in (0, 1)$, the β -expansion of x can be defined by the β -transformation given by $T_\beta : [0, 1] \rightarrow [0, 1]$, $T_\beta(x) = \beta x - \lfloor \beta x \rfloor$, setting $(x)_\beta = 0.x_1 x_2 x_3 \cdots$ where $x_i = \lfloor \beta T^{i-1}(x) \rfloor$. Note that for every $n \in \mathbb{N}$, we have

$$T^n(x) = 0.x_{n+1} x_{n+2} x_{n+3} \cdots = \left(x - \sum_{k=1}^n x_k \beta^{-k}\right) \beta^n.$$

In general, not all combinations of digits in \mathcal{D} appear in a β -expansion. The sequences of digits which are admissible as β -expansions are described by the lexicographic condition, using the so-called quasigreedy expansion of 1, denoted $d_\beta^*(1) = t_1^*t_2^*t_3^*\cdots$, defined by $\lim_{x \rightarrow 1^-} (x)_\beta = 0.t_1^*t_2^*t_3^*\cdots$, where the limit is considered in the product topology. The theorem by Parry [13] then says that $0.x_1x_2x_3\cdots$ with $x_i \in \mathbb{N}$, is a β -expansion of some $x \in (0, 1)$ if and only if for every $i \geq 1$, we have $x_ix_{i+1}x_{i+2}\cdots \prec d_\beta^*(1)$, where \preceq stands for standard lexicographic order on strings.

The so-called β -integers are real numbers whose β -expansion has no non-zero digits to the right of the fractional point,

$$\mathbb{Z}_\beta = \{x \in \mathbb{R} : (|x|)_\beta = x_nx_{n-1}\cdots x_1x_0.0^\omega\}.$$

Example 2.1. Let $\tau = \frac{1}{2}(1 + \sqrt{5}) \approx 1.618$ be the golden ratio. By the greedy algorithm, we can calculate the τ -expansion of 2. We have $\tau^1 \leq 2 < \tau^2$, thus $k = 1$,

$$\begin{aligned} r_1 &= 2, & x_1 &= \lfloor 2/\tau^1 \rfloor = 1, \\ r_0 &= 2 - \tau, & x_0 &= \lfloor (2 - \tau)/\tau^0 \rfloor = 0, \\ r_{-1} &= 2 - \tau, & x_{-1} &= \lfloor (2 - \tau)/\tau^{-1} \rfloor = 0, \\ r_{-2} &= 2 - \tau, & x_{-2} &= \lfloor (2 - \tau)/\tau^{-2} \rfloor = 1. \end{aligned}$$

Since $r_{-3} = 2 - \tau - \tau^{-2} = 0$, we have $x_i = 0$ for every $i \leq -3$ and $(2)_\tau = 10.010^\omega$, where by 0^ω we mean infinite repetition of the digit 0. As usual in the decimal system, we can omit the suffix 0^ω .

Let us now compute the τ -expansion of $1/2$ using the τ -transformation. We have

$$\begin{aligned} x_1 &= \lfloor \frac{\tau}{2} \rfloor = 0, & T_\tau(1/2) &= \frac{\tau}{2} - \lfloor \frac{\tau}{2} \rfloor = \frac{\tau}{2}, \\ x_1 &= \lfloor \frac{\tau^2}{2} \rfloor = 1, & T_\tau^2(1/2) &= \frac{\tau^2}{2} - \lfloor \frac{\tau^2}{2} \rfloor = \frac{1}{2\tau}, \\ x_2 &= \lfloor \frac{1}{2} \rfloor = 0, & T_\tau^3(1/2) &= \frac{1}{2}. \end{aligned}$$

Since $T_\tau^3(1/2) = T_\tau^0(1/2)$, we have $T_\tau^{n+3}(1/2) = T_\tau^n(1/2)$, and thus $(1/2)_\tau = 0.(010)^\omega$. Similarly, one can obtain the purely periodic τ -expansion of $\frac{3}{7}$ as it was mentioned in the introduction, $(3/7)_\tau = 0.(0100001001010010)^\omega$.

Note that for all $(2)_\tau$, $(1/2)_\tau$, and $(3/7)_\tau$, the string of digits does not contain two consecutive digits equal to 1. This is not a coincidence. For, the quasigreedy expansion of 1 satisfies $d_\tau^*(1) = (10)^\omega$. The Parry lexicographic condition says that a β -expansion has only digits in the set $\{0, 1\}$, does not contain the string 11 and does not end with the tail $(01)^\omega$.

With this in hand, we can find the first few non-negative τ -integers. Their τ -expansions are

$$0, 1, 10, 100, 101, 1000, 1001, 1010, 10000, \dots$$

They have values

$$0, 1, \tau, \tau^2, \tau^2 + 1, \tau^3, \tau^3 + 1, \tau^3 + \tau, \tau^4, \dots$$

Definition 2.2. Let $\beta > 1$. We say that $q \in \mathbb{N}$ has the *Midy property in base β* , if there exists a positive integer $p < q$ coprime with q such that

- the β -expansion of $\frac{p}{q}$ is purely periodic $(\frac{p}{q})_\beta = 0.(c_1c_2 \cdots c_{2n})^\omega$ where $2n$ is the length of the shortest period; and
- $x + y = \beta^n - 1$, where x, y are β -integers with β -expansions $(x)_\beta = c_1c_2 \cdots c_n$ and $(y)_\beta = c_{n+1}c_{n+2} \cdots c_{2n}$, respectively.

The number p is then said to *testify* to the Midy property of q in base β .

From the above given examples, we see that in base τ the number $q = 7$ has the Midy property whereas the number $q = 2$ has not. For, the only fraction $\frac{p}{q}$ in the interval $(0, 1)$ with denominator $q = 2$ is $\frac{1}{2}$ with the τ -expansion $(\frac{1}{2})_\tau = 0.(010)^\omega$ of odd length.

Remark 2.3. Note that directly from the definition it follows that if an integer q has the Midy property in base β , then the base is an algebraic integer. Indeed, we have

$$\beta^n - 1 = x + y \quad \text{where } x = \sum_{i=1}^n c_i \beta^{n-i} \text{ and } y = \sum_{i=1}^n c_{n+i} \beta^{n-i},$$

which shows that β is a root of a monic polynomial with integer coefficients.

Our aim is to search for bases in which infinitely many fractions $\frac{p}{q}$ satisfy the Midy property. The crucial point is to have infinitely many positive fractions $\frac{p}{q} < 1$, with purely periodic expansion. Pure periodicity in non-integer bases was studied already by Schmidt [17], later by Hama and Imahashi [8], Akiyama [2], Adamczewski et al. [1] and others. Let us summarize the results.

Denote $\gamma(\beta)$ supremum of real numbers γ such that every $x \in [0, \gamma) \cap \mathbb{Q}$ has a purely periodic β -expansion. Based on the results of Schmidt [17], Akiyama [2] has shown that if $\gamma(\beta) > 0$, then β is a Pisot unit. Recall that an algebraic integer $\beta = \beta^{(1)} > 1$ is a Pisot number of degree d , if its minimal polynomial $f \in \mathbb{Z}[X]$ is of degree d , and the other roots $\beta^{(i)}$, $i = 2, \dots, d$ of f , called the algebraic conjugates of β , are in modulus smaller than 1. The number β is an algebraic unit, if its norm, $N(\beta) = \prod_{i=1}^d \beta^{(i)}$ is equal to ± 1 . There are two classes of quadratic Pisot units, namely the roots $\beta > 1$ of the polynomials

$$X^2 - mX - 1, \quad m \geq 1, \tag{1}$$

$$X^2 - mX + 1, \quad m \geq 3. \tag{2}$$

From Schmidt [17], it follows that if β is a root of (1), then $\gamma(\beta) = 1$, i.e. every fraction in the interval $(0, 1)$ has a purely periodic β -expansion. On the other hand, for roots of (2), it is shown in [8] that no fraction has a purely periodic β -expansion, and hence $\gamma(\beta) = 0$.

Let $f(X) = X^d - c_{d-1}X^{d-1} - c_{d-2}X^{d-2} - \cdots - c_1X - c_0 \in \mathbb{Z}[X]$ be the minimal

polynomial of β , the companion matrix of β is defined as

$$C = \begin{pmatrix} 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & \cdots & 0 & c_1 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 0 & c_{d-2} \\ 0 & 0 & \cdots & 1 & c_{d-1} \end{pmatrix}$$

The spectrum of C is formed by the roots of f , in particular, the determinant of C is equal to the norm of β , $\det C = N(\beta)$. Denote $\mathbf{v} = (1, \beta, \beta^2, \dots, \beta^{d-1})^T$. Then \mathbf{v} is a left eigenvector of C corresponding to the eigenvalue β ,

$$\mathbf{v}^T C = \beta \mathbf{v}^T.$$

Example 2.4. The minimal polynomial of the golden ratio $\tau = \frac{1}{2}(1 + \sqrt{5})$ is given by $f(X) = X^2 - X - 1$, the companion matrix of τ is $C = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. The algebraic conjugate of τ is $\tau' = \frac{1}{2}(1 - \sqrt{5}) = -\frac{1}{\tau} \sim -0.618$, and thus τ is a Pisot number.

3 Necessary condition

Lemma 3.1. *Let $q \in \mathbb{N}$, $q > 2$ and $\beta > 1$. Then q satisfies the Midy property for β if and only if there exists $p \in \mathbb{N}$, $0 < p < q$, p coprime with q and $N \in \mathbb{N}$ such that*

$$T^N\left(\frac{p}{q}\right) = \frac{q-p}{q} \quad \text{and} \quad T^N\left(\frac{q-p}{q}\right) = \frac{p}{q}. \quad (3)$$

Proof. Suppose that a number $z \in (0, 1)$ has purely periodic expansion with period of even length $2n$, say $(z)_\beta = 0.(c_1 c_2 \cdots c_{2n})^\omega$, i.e.

$$(T^n(z))_\beta = 0.(c_{n+1} c_{n+2} \cdots c_{2n} c_1 c_2 \cdots c_n)^\omega \quad \text{and} \quad T^{2n}(z) = z,$$

This can be written using the β -integers $x := c_1 \beta^{n-1} + c_2 \beta^{n-2} + \cdots + c_{n-1} \beta + c_n$ and $y := c_{n+1} \beta^{n-1} + c_{n+2} \beta^{n-2} + \cdots + c_{2n-1} \beta + c_{2n}$, as

$$z = \frac{x\beta^n + y}{\beta^{2n} - 1} \quad \text{and} \quad T^n(z) = \frac{y\beta^n + x}{\beta^{2n} - 1}.$$

We derive

$$z + T^n(z) = \frac{(x+y)(\beta^n + 1)}{\beta^{2n} - 1} = \frac{x+y}{\beta^n - 1}. \quad (4)$$

Let q satisfy the Midy property in base β . This means that we have (4) for some $z = \frac{p}{q}$ where p is coprime with q , and, moreover, $x+y = \beta^n - 1$. Equation (4) gives $\frac{p}{q} + T^n\left(\frac{p}{q}\right) = 1$. Hence, $T^n\left(\frac{p}{q}\right) = \frac{q-p}{q}$ and $T^n\left(\frac{q-p}{q}\right) = T^{2n}\left(\frac{p}{q}\right) = \frac{p}{q}$. It suffices to set $N = n$.

For the opposite implication, assume that Equation (3) is satisfied for some $N \in \mathbb{N}$ and $p \in \{1, 2, \dots, q-1\}$ coprime with q . Denote d the shortest period of the β -expansion of

$\frac{p}{q}$. Obviously, d divides $2N$. If d divides N , then $\frac{p}{q} = T^N(\frac{p}{q}) = \frac{q-p}{q}$, which happens only for $\frac{p}{q} = \frac{1}{2}$. Since $q > 2$ and p is coprime with q , this is not possible.

Thus $2N = kd$ for some odd k , i.e. the minimal period-length d is even. We have $N = kd/2 = (k-1)d + d/2$. Substituting into (3), we obtain

$$\frac{q-p}{q} = T^N(\frac{p}{q}) = T^{d/2}\left(T^{(k-1)d}(\frac{p}{q})\right) = T^{d/2}\left(\frac{p}{q}\right),$$

and consequently also

$$T^{d/2}\left(\frac{q-p}{q}\right) = T^{d/2}\left(T^{d/2}\left(\frac{p}{q}\right)\right) = T^d\left(\frac{p}{q}\right) = \frac{p}{q}.$$

Therefore (3) is satisfied also for $N = d/2$.

Therefore the β -expansion of $z = \frac{p}{q}$ is purely periodic of length d . Thus (4) is satisfied with $n = d/2$. Combining with (4), we derive $z + T^n(z) = 1 = \frac{x+y}{\beta^n - 1}$, whence $x + y = \beta^n - 1$. This concludes the proof. \square

Theorem 3.2. *Let $C \in \mathbb{Z}^{d \times d}$ be the companion matrix of an algebraic integer $\beta > 1$ of degree d . If $q \in \mathbb{N}$, $q > 2$, has the Midy property in base β , then there exists a positive integer N such that $C^N \equiv -I \pmod{q}$.*

Proof. Denote $\mathbf{v} = (1, \beta, \beta^2, \dots, \beta^{d-1})^T$. If $x \in \frac{1}{q}\mathbb{Z}[\beta]$, then there exists a unique integer vector $\mathbf{a}(x) = (a_0, a_1, \dots, a_{d-1})^T \in \mathbb{Z}^d$ such that

$$x = \frac{1}{q} \mathbf{v}^T \mathbf{a}(x).$$

Let $d = \lfloor \beta x \rfloor$ be the first digit in the β -expansion of x . Then

$$T(x) = \beta x - d = \frac{1}{q}(\mathbf{v}^T C \mathbf{a}(x) - qd) = \frac{1}{q} \mathbf{v}^T (C \mathbf{a}(x) - qd \mathbf{e}_1) \in \frac{1}{q}\mathbb{Z}[\beta], \quad (5)$$

where by $\mathbf{e}_i \in \mathbb{R}$ we mean the i^{th} column of the identity matrix $I \in \mathbb{R}^{d \times d}$, in other words, \mathbf{e}_i denotes the i^{th} vector of the canonical base of the vector space \mathbb{R}^d .

From (5), we see that the set $\frac{1}{q}\mathbb{Z}[\beta] \cap [0, 1)$ is closed under the transformation T . Equation (5) implies that

$$\mathbf{a}(T(x)) = C \mathbf{a}(x) - qd \mathbf{e}_1 \equiv C \mathbf{a}(x) \pmod{q}. \quad (6)$$

Clearly, $\mathbf{a}(\frac{p}{q}) = p \mathbf{e}_1$ and $\mathbf{a}(\frac{q-p}{q}) = (q-p) \mathbf{e}_1$. Applying (6) to Equation (3) we obtain

$$\mathbf{a}\left(T^N\left(\frac{p}{q}\right)\right) \equiv C^N \mathbf{a}\left(\frac{p}{q}\right) \equiv C^N p \mathbf{e}_1 \equiv -p \mathbf{e}_1 \pmod{q}.$$

Since p and q are coprime, we have derived $C^N \mathbf{e}_1 \equiv -\mathbf{e}_1 \pmod{q}$. In order to finish the proof, we need to verify that $C^N \mathbf{e}_i \equiv -\mathbf{e}_i \pmod{q}$ holds for all vectors \mathbf{e}_i , $i = 2, 3, \dots, d$. For this purpose, we show by induction the following claim:

For any $n \in \mathbb{N}$ and any $i = 2, \dots, d$ one has $C^n \mathbf{e}_i = C^{n+1} \mathbf{e}_{i-1}$.

Indeed, if $n = 0$, then the claim can be checked directly from the definition of the companion matrix C . Assume that the statement is valid for $n \in \mathbb{N}$. Then with the use of the induction hypothesis, we have $C^{m+1}\mathbf{e}_i = CC^m\mathbf{e}_i = CC^{n+1}\mathbf{e}_{i-1} = C^{m+2}\mathbf{e}_{i-1}$, i.e. the statement is valid for $n + 1$, as well.

Combining the claim with the relation $C^N\mathbf{e}_1 \equiv -\mathbf{e}_1 \pmod{q}$ we obtain

$$C^N\mathbf{e}_2 \equiv C^{N+1}\mathbf{e}_1 \equiv CC^N\mathbf{e}_1 \equiv C(-\mathbf{e}_1) \equiv -\mathbf{e}_2 \pmod{q}.$$

We proceed analogously to show $C^N\mathbf{e}_i \equiv -\mathbf{e}_i \pmod{q}$, for all i . This proves that $C^N \equiv -I \pmod{q}$. \square

Remark 3.3. If $\beta > 1$ is an algebraic number of an odd degree d and β has norm $N(\beta) = 1$, then no integer q satisfies the Midy property in base β . For, $N(\beta) = 1 = \det C = \det C^N$ and $\det(-I) = (-1)^d = -1$, the equality $C^N \equiv -I \pmod{q}$ cannot hold true. In particular, no $q > 2$ satisfies the Midy property in the Tribonacci base β - the positive root of the polynomial $X^3 - X^2 - X - 1$.

Remark 3.4. Let us mention that the necessary condition given in Theorem 3.2 is not sufficient. As counterexample consider $\beta > 1$, the quadratic Pisot number with minimal polynomial $X^2 - 3X + 1$. The companion matrix $C = \begin{pmatrix} 0 & -1 \\ 1 & 3 \end{pmatrix}$ satisfies for $q = 5$ that $C^5 \equiv -I \pmod{q}$. Nevertheless, it is known that no rational number in $(0, 1)$ has a purely periodic β -expansion, and thus $q = 5$ does not satisfy the Midy property.

4 Sufficient condition for the base $\tau = \frac{1+\sqrt{5}}{2}$

Our aim is to show that the necessary condition derived in Theorem 3.2 for an integer q to satisfy the Midy property in base $\beta > 1$ is also sufficient in case of β being the golden ratio τ . Powers of the companion matrix C of the golden ratio can be expressed using the well known Fibonacci sequence $(F_n)_{n \in \mathbb{N}}$, defined by

$$F_0 = 0, F_1 = 1, \text{ and } F_{n+2} = F_{n+1} + F_n \text{ for } n \in \mathbb{N}.$$

It can be easily computed that for any positive exponent $N \in \mathbb{N}$, we have

$$C^N = \begin{pmatrix} F_{N-1} & F_N \\ F_N & F_{N+1} \end{pmatrix}.$$

Theorem 4.1. *Let C be the companion matrix of the golden ratio τ , let $q, N \in \mathbb{N}$, $q > 2$ and $N > 1$. If $C^N \equiv -I \pmod{q}$, then q has the Midy property in base τ . Every $p \in \mathbb{N}$, $0 < p < q$, testifies to the Midy property of q .*

Proof. First we show that for any fraction $x \in \mathbb{Q} \cap (0, 1)$ with denominator q it holds that $T^N(x) = 1 - x$. Then also $T^N(1 - x) = 1 - (1 - x) = x$, hence $T^{2N}(x) = x$. By Lemma 3.1, this implies the statement.

Let c_1, c_2, \dots, c_N be the digits of the τ -expansion of $x = \frac{p}{q}$ obtained by first N iterations of the transformation T . Then

$$(0, 1) \ni T^N\left(\frac{p}{q}\right) = \left(\frac{p}{q} - \frac{c_1}{\tau} - \frac{c_2}{\tau^2} - \dots - \frac{c_N}{\tau^N}\right) \tau^N = \frac{1}{q} \left(p\tau^N - q \sum_{k=0}^{N-1} c_{N-k} \tau^k \right). \quad (7)$$

By induction, one can easily verify the following formula connecting Fibonacci numbers and the golden mean,

$$\tau^k = \left(\tau + \frac{1}{\tau}\right) F_k + \left(\frac{-1}{\tau}\right)^k, \text{ for } k \geq 0. \quad (8)$$

Substituting into (7), one has

$$T^N\left(\frac{p}{q}\right) = \frac{1}{q} \left(\left(\tau + \frac{1}{\tau}\right) \underbrace{\left(pF_N - q \sum_{k=0}^{N-1} c_{N-k} F_k \right)}_{=:A} + p \left(\frac{-1}{\tau}\right)^N - q \underbrace{\sum_{k=0}^{N-1} c_{N-k} \left(\frac{-1}{\tau}\right)^k}_{=:B} \right)$$

The assumption $C^N \equiv -I \pmod{q}$ implies that $F_N \equiv 0 \pmod{q}$ and $F_{N-1} \equiv -1 \pmod{q}$. Therefore $A \in \mathbb{Z}$ can be written in the form

$$A = pF_N - q \sum_{k=0}^{N-1} c_{N-k} F_k = \ell q \quad \text{for some } \ell \in \mathbb{Z}.$$

Consequently, we have the following estimate,

$$T^N\left(\frac{p}{q}\right) = |T^N\left(\frac{p}{q}\right)| > \left(\tau + \frac{1}{\tau}\right) |\ell| - \frac{1}{\tau^N} - |B|. \quad (9)$$

Recall that in the sequence of digits c_1, c_2, \dots, c_N , there are never two consecutive digits equal to 1. Therefore we have the estimate on $B = \sum_{k=0}^{N-1} c_{N-k} \left(\frac{-1}{\tau}\right)^k$,

$$|B| \leq \begin{cases} \sum_{k=0}^{\infty} \frac{1}{\tau^{2k}} - \frac{1}{\tau^{N+1}} \sum_{k=0}^{\infty} \frac{1}{\tau^{2k}} = \tau - \frac{1}{\tau^N}, & \text{if } c_N = 1, \\ \sum_{k=0}^{\infty} \frac{1}{\tau^{2k+1}} = 1, & \text{if } c_N = 0. \end{cases}$$

We will now show that $A = \ell q = 0$. Assume that the opposite is true, i.e. $|\ell| \geq 1$.

In case $c_N = 0$, estimate (9) gives $T^N\left(\frac{p}{q}\right) > \left(\tau + \frac{1}{\tau}\right) - \frac{1}{\tau^N} - 1 = \frac{2}{\tau} - \frac{1}{\tau^N} > 1$, which is a contradiction.

If $c_N = 1$, then the digit $c_{N+1} = 0$, and thus $T^{N+1}\left(\frac{p}{q}\right) = \tau T^N\left(\frac{p}{q}\right) < 1$, i.e. $T^N\left(\frac{p}{q}\right) < \frac{1}{\tau}$. If $\ell \neq 0$, we obtain $T^N\left(\frac{p}{q}\right) > \left(\tau + \frac{1}{\tau}\right) - \frac{1}{\tau^N} - \tau + \frac{1}{\tau^N} = \frac{1}{\tau}$, which is again a contradiction. Thus we have derived that $A = 0$.

Now we use another expression for the powers of the golden ratio using Fibonacci numbers, namely

$$\tau^k = F_k \tau + F_{k-1}, \quad (10)$$

which holds for $k \geq 0$ defining $F_{-1} = 1$. We substitute for τ^k into (7), to obtain

$$T^N\left(\frac{p}{q}\right) = \frac{1}{q} \left(\underbrace{\tau \left(pF_N - q \sum_{k=0}^{N-1} c_{N-k} F_k \right)}_{=A} + pF_{N-1} - q \underbrace{\sum_{k=0}^{N-1} c_{N-k} F_{k-1}}_{\in \mathbb{Z}} \right).$$

Since $A = 0$ and $F_{N-1} = -1 \pmod{q}$, there exists $n \in \mathbb{Z}$ such that

$$T^N\left(\frac{p}{q}\right) = \frac{1}{q}(-p + nq) = n - \frac{p}{q}$$

Since both $T^N\left(\frac{p}{q}\right) \in (0, 1)$ and $\frac{p}{q} \in (0, 1)$, necessarily $n = 1$ and thus $T^N\left(\frac{p}{q}\right) = \frac{q-p}{p}$ as we wanted to show. \square

Remark 4.2. Let $p, q \in \mathbb{N}$, $1 \leq p < q$, p coprime with q . If p testifies to the Midy property of q in base τ , then the minimal period d of the τ -expansion of $\frac{p}{q}$ is even and the equation $C^N \equiv -I \pmod{q}$, is satisfied also for $N = \frac{d}{2}$, see the proof of Lemma 3.1. In particular, $\det C^{d/2} = (-1)^{d/2} \equiv \det(-I) \equiv 1 \pmod{q}$. Hence $\frac{d}{2}$ is even, i.e. the minimal period d is divisible by 4. The sum of the two halves of the τ -expansion of $\frac{p}{q}$ is equal to $\tau^{d/2} - 1 = \sum_{k=1}^{d/4} \tau^{2k-1}$ and thus its τ -expansion is $(10)^{d/4}$, which is a prefix of $d_\tau^*(1) = (10)^\omega$.

Example 4.3. The number $q = 3$ satisfies the Midy property in base τ , as

$$C^4 = \begin{pmatrix} F_3 & F_4 \\ F_4 & F_5 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \equiv -I \pmod{3}.$$

Indeed, $\left(\frac{1}{3}\right)_\tau = 0.(00101000)^\omega$. The first half of the period 0010 represents the number τ , the second half 1000 represents the number τ^3 . Their sum is

$$\tau^3 + \tau = (\tau^3 + \tau + 1) - 1 = (\tau^3 + \tau^2) - 1 = \tau^4 - 1.$$

The τ -expansion of the sum is the string 1010 and it is a prefix of $d_\tau^*(1) = (10)^\omega$.

Similarly, $q = 5$ satisfies Midy property in base τ , as

$$C^{10} = \begin{pmatrix} F_9 & F_{10} \\ F_{10} & F_{11} \end{pmatrix} = \begin{pmatrix} 34 & 55 \\ 55 & 89 \end{pmatrix} \equiv -I \pmod{5}.$$

Indeed, $\left(\frac{1}{5}\right)_\tau = 0.(00010010101001001000)^\omega$. The first half of the period 0001001010 represents the number $\tau^6 + \tau^3 + \tau$, the second half 1001001000 represents the number $\tau^9 + \tau^6 + \tau^3$. Their sum is $\tau^9 + 2\tau^6 + 2\tau^3 + \tau = \tau^{10} - 1$. The τ -expansion of the sum is the string 1010101010 and it is a prefix of $d_\tau^*(1) = (10)^\omega$.

Corollary 4.4. *Let q satisfy the Midy property in base τ . If $d \in \mathbb{N}$, $d > 2$, is a divisor of q , then d has the Midy property in τ as well.*

Proof. By Theorem 3.2, there exists a positive integer N such that $C^N \equiv -I \pmod{q}$. As d is divisor of q , necessarily $C^N \equiv -I \pmod{d}$. By Theorem 4.1, d has the Midy property in base τ . \square

Corollary 4.5. *Let $q \in \mathbb{N}, q > 2$.*

1. *If q is a divisor of F_{2n-1} for some $n \in \mathbb{N}, n \geq 3$, then q has the Midy property in base τ .*
2. *If q is a multiple of F_{2n} for some $n \in \mathbb{N}, n \geq 3$, then q does not have the Midy property in base τ .*

Proof. In view of Corollary 4.4 it suffices to show that $q = F_n, n \geq 5$ satisfies the Midy property if and only if n is odd.

Note that $\det C = -1$ and thus $\det C^k = F_{k-1}F_{k+1} - F_k^2 = (-1)^k$. This fact together with the recurrence for the Fibonacci sequence implies that

$$F_{k+1}^2 \equiv (-1)^k \pmod{F_k} \quad \text{and} \quad F_{k+1} \equiv F_{k-1} \pmod{F_k}. \quad (11)$$

Thus

$$C^k = \begin{pmatrix} F_{k-1} & F_k \\ F_k & F_{k+1} \end{pmatrix} \equiv \begin{pmatrix} F_{k+1} & 0 \\ 0 & F_{k+1} \end{pmatrix} \pmod{F_k}. \quad (12)$$

1. Let $q = F_{2n-1}$. Put $N = 2(2n - 1)$. Using (11) and (12) we deduce

$$C^N = C^{2n-1}C^{2n-1} \equiv \begin{pmatrix} F_{2n}^2 & 0 \\ 0 & F_{2n}^2 \end{pmatrix} \equiv -I \pmod{F_{2n-1}}.$$

By Theorem 4.1, the number $q = F_{2n-1}$ satisfies the Midy property.

2. Let $q = F_{2n}$. Assume for contradiction that F_{2n} has the Midy property, i.e. by Theorem 3.2 there exists $N \in \mathbb{N}, N > 0$ such that

$$C^N = \begin{pmatrix} F_{N-1} & F_N \\ F_N & F_{N+1} \end{pmatrix} \equiv -I \pmod{F_{2n}}. \quad (13)$$

In particular, $F_N \equiv 0 \pmod{F_{2n}}$, i.e. F_{2n} is a divisor of F_N . From the well known fact that F_m divides F_r if and only if m divides r we derive that $N = 2n\ell$ for some $\ell \in \mathbb{N}$. Using (11) and (12) we obtain that

$$C^{2n} \equiv \begin{pmatrix} F_{2n-1} & 0 \\ 0 & F_{2n-1} \end{pmatrix} \pmod{q} \quad \text{and} \quad C^{4n} \equiv \begin{pmatrix} F_{2n-1}^2 & 0 \\ 0 & F_{2n-1}^2 \end{pmatrix} \equiv I \pmod{q}$$

Thus $C^N = C^{2n\ell} \equiv I$ for ℓ even and $C^N \equiv C^{2n}$ for ℓ odd. Therefore (13) implies that

$$C^N = C^{2n} \equiv \begin{pmatrix} F_{2n-1} & 0 \\ 0 & F_{2n-1} \end{pmatrix} \equiv -I \pmod{q},$$

in particular, $F_{2n-1} \equiv -1 \pmod{F_{2n}}$.

From the assumption, we have that $n \geq 3$, therefore $2 \leq F_{2n-1} \leq F_{2n} - 2$, and hence $F_{2n-1} \not\equiv \pm 1 \pmod{F_{2n}}$. Consequently, $C^{2n} \not\equiv -I \pmod{q}$. In summary, for every exponent N we have $C^N \not\equiv -I \pmod{q}$. Thus F_{2n} does not satisfy the Midy property. \square

In view of the sufficient condition given in Theorem 4.1, the knowledge of divisibility of Fibonacci numbers will be crucial. For a positive given $m \in \mathbb{N}$ denote $a(m)$ the smallest positive integer such that m divides $F_{a(m)}$. The sequence $(a(m))_{m \geq 0}$ is registered in Sloane's On-Line Encyclopedia of Integer Sequences under the code A001177.

It can be shown (e.g. [7]) that m divides F_n if and only if $a(m)$ divides n . By Item (1) of Corollary 4.5, this directly implies the following.

Corollary 4.6. *Let $q > 2$ be an integer such that $a(q)$ is odd. Then q satisfies the Midy property in base τ .*

According to our knowledge, the description of odd values in the sequence $(a(m))_{m \geq 0}$ is not known. Among the first 70 members of the sequence $(a(m))_{m \geq 0}$ the following are odd,

$$a(5) = 5, a(10) = 15, a(13) = 7, a(17) = 9, a(25) = 25, a(26) = 21, \\ a(34) = 9, a(37) = 19, a(50) = 75, a(53) = 27, a(61) = 15, a(65) = 35.$$

In the following section, we inspect the Midy property in base τ for all prime denominators q . We will see that the necessary condition given in Corollary 4.6 is not sufficient, since for example $a(7) = 8$ and still 7 has the Midy property (cf. Theorem 5.3).

On the other hand, Corollary 4.6 decides about the Midy property of some non-primes, such as 10, 25, 26, 34, 50, 65.

5 The Midy property of prime numbers

In order to give characterisation of primes satisfying the Midy property for the golden ratio base, we will need to work in the finite field \mathbb{Z}_q . Let us recall some facts from finite fields. We say that a is a quadratic residue mod q , if there exist $b \in \mathbb{Z}_q$ such that $a \equiv b^2 \pmod{q}$. The Legendre symbol is a multiplicative function defined as

$$\left(\frac{a}{q}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } q \text{ and } a \not\equiv 0 \pmod{q} \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } q, \\ 0 & \text{if } a \equiv 0 \pmod{q}. \end{cases}$$

We also use the quadratic reciprocity law. For distinct odd primes q_1, q_2 , we have

$$\left(\frac{q_1}{q_2}\right) \cdot \left(\frac{q_2}{q_1}\right) = (-1)^{\frac{q_1-1}{2} \frac{q_2-1}{2}}.$$

In particular, we derive that 5 is a quadratic residue mod q if and only if $q = 5$ or q is a quadratic residue mod 5, which happens exactly for $q \equiv \pm 1 \pmod{5}$.

Halton [7] derived the following result about the value $a(q)$ for prime q : If q is an odd prime, then $a(q)$ divides $q - \left(\frac{5}{q}\right)$. By the above knowledge of quadratic residues, this amounts to saying that

$$\begin{aligned} a(q) \text{ divides } q - 1 & \quad \text{if } q \equiv \pm 1 \pmod{5}, \\ a(q) \text{ divides } q + 1 & \quad \text{if } q \equiv \pm 2 \pmod{5}. \end{aligned} \tag{14}$$

Lemma 5.1. *Let \mathbb{F} be a field and let $A \in \mathbb{F}^{2 \times 2}$ be a matrix such that $A^2 = I$. Then*

- (i) *either $\det A = 1$ and $A = \pm I$*
- (ii) *or $\det A = -1$ and the matrix A is similar to $D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, i.e. $A = R^{-1}DR$ for some non-singular matrix $R \in \mathbb{F}^{2 \times 2}$.*

Proof. Since $A^2 - I = (A - I)(A + I) = \Theta$,

- (i) either one of the matrices $A - I$ and $A + I$ is the zero matrix Θ , i.e. $A = \pm I$, and in this case $\det A = 1$,
- (ii) or none of the matrices is the zero matrix. In that case both $A - I$ and $A + I$ are singular, equivalently, have 0 as an eigenvalue. This implies that the matrix A has two different eigenvalues, 1 and -1 , and thus is diagonalisable. As $\det A$ is the product of eigenvalues, we have $\det A = -1$. \square

Below, we will work both in the real numbers and in the finite field \mathbb{Z}_q . Equality of elements a and b in \mathbb{R} will be denoted $a = b$, whereas equality in \mathbb{Z}_q we write $a \equiv b \pmod{q}$. Obviously $a = b$ implies $a \equiv b \pmod{q}$ and not vice versa.

Lemma 5.2. *Let $q \in \mathbb{N}$ be a prime, $q \neq 5$, and let $C = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ be the companion matrix of the polynomial $X^2 - X - 1$. If $C^{2\ell} \equiv I \pmod{q}$ for some odd $\ell \in \mathbb{N}$, then 5 is a quadratic residue \pmod{q} and consequently $q \equiv \pm 1 \pmod{5}$.*

Proof. We use the fact that for an odd integer ℓ , we have $\det C^\ell \equiv -1$ and we verify easily that $C^\ell = \begin{pmatrix} F_{\ell-1} & F_\ell \\ F_\ell & F_{\ell+1} \end{pmatrix}$ has the inverse $C^{-\ell} = \begin{pmatrix} -F_{\ell-1} & F_\ell \\ F_\ell & -F_{\ell+1} \end{pmatrix}$. From $C^{2\ell} \equiv I \pmod{q}$ we obtain $C^\ell \equiv C^{-\ell} \pmod{q}$. Denoting $a := F_{\ell+1} \equiv -F_{\ell-1} \pmod{q}$, we thus derive that $F_\ell \equiv F_{\ell+1} - F_{\ell-1} \equiv 2a \pmod{q}$. With this, we have

$$C^\ell \equiv \begin{pmatrix} -a & 2a \\ 2a & a \end{pmatrix} \equiv a \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix} \pmod{q} \quad \text{and thus} \quad C^{2\ell} \equiv a^2 \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} \equiv I \pmod{q}.$$

Necessarily $5 \equiv (a^{-1})^2 \pmod{q}$. In other words, 5 is a quadratic residue \pmod{q} . By the quadratic reciprocity law, we have for the Legendre symbol $\left(\frac{5}{q}\right) = \left(\frac{q}{5}\right) = 1$, and thus q is a quadratic residue $\pmod{5}$. Since q is a prime, necessarily $q \equiv \pm 1 \pmod{5}$. \square

Theorem 5.3. *Let $q > 2$ be a prime, $q = 5$ or $q \equiv \pm 2 \pmod{5}$. Then q has the Midy property in the golden ratio base.*

Proof. We have shown in Example 4.3 that 5 satisfies the Midy property.

Suppose that $q \equiv \pm 2 \pmod{5}$. For such primes, we have from (14) that $a(q)$ divides $q + 1$, and thus $F_{q+1} \equiv 0 \pmod{q}$. Therefore $a := F_{q+2} \equiv F_q \pmod{q}$. As $q + 1$ is even, $\det C^{q+1} \equiv F_{q+2}F_q \equiv 1 \equiv a^2 \pmod{q}$. Equality $a^2 \equiv 1 \pmod{q}$ implies $a \equiv \pm 1 \pmod{q}$. Thus $C^{q+1} \equiv \pm I \pmod{q}$ and in both cases $\det C^{q+1} \equiv 1 \pmod{q}$.

If $C^{q+1} \equiv -I \pmod{q}$, the proof is finished. Let us discuss the case $C^{q+1} \equiv I \pmod{q}$. Denote by r the minimal positive integer such that $C^r = I$. Since $C^{2r} = I$ and $q \equiv \pm 2$

mod 5, Lemma 5.2 implies that r is even, say $r = 2r'$. As $C^r = C^{2r'} = I$, the same Lemma 5.2 forces $r' = 2r''$. Consider the matrix $A = C^{r'} = C^{2r''}$ with determinant $\det A = (\det C)^{2r''} = 1$. By Lemma 5.1, we have that $A = C^{r'} = \pm I$. Since $r' < r$, necessarily $C^{r'} = -I$. Using the sufficient condition in Theorem 4.1, we conclude that q has the Midy property for the golden ratio. \square

Theorem 5.4. *Let $q \in \mathbb{N}$ be a prime, $q \equiv \pm 1 \pmod{5}$. Write $q - 1 = 2^k \ell$ for $k \in \mathbb{N}$ and odd $\ell \in \mathbb{N}$. Then q has the Midy property in the golden ratio base if and only if the list of matrices $C^{2^\ell}, C^{4^\ell}, \dots, C^{2^{k-1}\ell}$ contains a matrix which equals $-I \pmod{q}$.*

Proof. Since $q \equiv \pm 1 \pmod{5}$, by quadratic reciprocity, 5 is a quadratic residue mod q , i.e. there exists $b \in \mathbb{Z}_q$ such that $b^2 \equiv 5 \pmod{q}$. Denote $\lambda_1 = 2^{-1}(1 + b)$ and $\lambda_2 = 2^{-1}(1 - b)$. Then $\lambda_1 + \lambda_2 \equiv 1 \pmod{q}$ and $\lambda_1 \lambda_2 = 2^{-2}(1 - b^2) \equiv -1 \pmod{q}$ and thus λ_1, λ_2 are the roots of the characteristic polynomial

$$(X - \lambda_1)(X - \lambda_2) = X^2 - X - 1$$

of the matrix C . Obviously, $b \not\equiv \pm 1, 0 \pmod{q}$. This implies $\lambda_1 \not\equiv \lambda_2$ and both λ_1 and λ_2 belong to the multiplicative group $\mathbb{Z}_q \setminus \{0\}$. The order of the elements of this group divides $q - 1$, and therefore $\lambda_1^{q-1} \equiv \lambda_2^{q-1} \equiv 1 \pmod{q}$. Hence there exists a non-singular matrix $R \in \mathbb{Z}_q^{2 \times 2}$ such that

$$C \equiv R^{-1} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} R \pmod{q} \quad \text{and} \quad C^{q-1} \equiv I \pmod{q}.$$

In order to prove the theorem, we show two implications.

The implication (\Leftarrow) follows by Theorem 4.1. For the opposite direction (\Rightarrow) we proceed by contradiction. Assume that q satisfies the Midy property, i.e. by Theorem 3.2, there exists $N \in \mathbb{N}$ such that $C^N \equiv -I \pmod{q}$. In particular, for both eigenvalues λ_1, λ_2 of C it holds that $\lambda_1^N \equiv \lambda_2^N \equiv -1 \pmod{q}$.

In the same time, suppose that no matrix in the list $C^{2^\ell}, \dots, C^{2^{k-1}\ell}$ is equal to $-I \pmod{q}$. Since all matrices in the list are powers of C^2 , their determinant is equal to 1 mod q . Moreover, $C^{2^{k-1}\ell} = C^{q-1} \equiv I \pmod{q}$. Lemma 5.1 implies that all matrices in the list are equal to $I \pmod{q}$. As $C^{2^\ell} \equiv I \pmod{q}$ with ℓ odd and $\det C^\ell \equiv -1$, Lemma 5.1 forces that C^ℓ is similar to the matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. In particular, for one of the eigenvalues of the matrix C , say λ_1 , it holds that

$$\lambda_1^\ell \equiv 1 \pmod{q} \quad \text{and} \quad \lambda_1^N \equiv -1 \pmod{q}.$$

Let r be the order of λ_1 in the multiplicative group of the field \mathbb{Z}_q . Necessarily r divides ℓ , in particular, r is odd. On the other hand $\lambda_1^{2N} \equiv 1 \pmod{q}$, and thus r divides $2N$, too. The fact $\det C = -1$ and $\det(-I) = 1$ forces N to be even. Thus the odd number r divides $N/2$. We derive that $\lambda_1^{N/2} \equiv 1 \pmod{q}$ and $\lambda_1^N \equiv 1 \pmod{q}$, as well. This is a contradiction. \square

If $\frac{q-1}{2}$ is odd, then the list of matrices in the previous theorem is empty, and it cannot contain $-I$. By Theorem 5.3 we obtain the following Corollary.

Corollary 5.5. *Let $q \in \mathbb{N}$ be a prime such that $q \equiv -1 \pmod{20}$ or $q \equiv 11 \pmod{20}$. Then q does not have the Midy property. Consequently, no Fibonacci number F_{2n-1} with $n \geq 3$ is divisible by such a prime q .*

Remark 5.6. If q is prime, $q \equiv \pm 1 \pmod{5}$, and $\frac{q-1}{2}$ is even, then necessarily $q \equiv 1 \pmod{20}$ or $q \equiv 9 \pmod{20}$. Among such primes some have the Midy property in base τ and some do not have. For example,

- $41 \equiv 101 \equiv 1 \pmod{20}$. The prime 41 has the Midy property, whereas 101 has not.
- $109 \equiv 29 \equiv 9 \pmod{20}$. While 109 has the Midy property in base τ , the prime 29 has not.

Remark 5.7. Mersenne primes are defined as primes of the form $q = 2^s - 1$, which forces the exponent s to be also prime. Of course, not all numbers of the form $2^s - 1$ are prime even if s is prime. Suppose that $q = 2^s - 1$ is a Mersenne prime. We can derive the following conclusions about the Midy property of q in base τ :

- if $s \equiv 3 \pmod{4}$, then $q = 2^{4k+3} - 1 = 8(2^4)^k - 1 \equiv 2 \pmod{5}$, and by Theorem 5.3, the Mersenne prime $q = 2^s - 1$ has the Midy property in base τ .
- if $s \equiv 1 \pmod{4}$, then $q = 2^{4k+1} - 1 = 2(2^4)^k - 1 \equiv 1 \pmod{5}$, and $q \equiv -1 \pmod{4}$. This forces $q \equiv -1 \pmod{20}$, and by Corollary 5.5 the Mersenne prime $q = 2^s - 1$ does not have the Midy property in base τ .

Today (April 2024), 51 Mersenne primes are known. Precisely 19 of them satisfy the Midy property in base τ .

Fermat primes are primes of the form $f_n = 2^{2^n} + 1$, where $n \in \mathbb{N}$.

- $f_0 = 3$ and $f_1 = 5 = F_5$ have the Midy property by Example 4.3.
- If $n \geq 2$, then $f_n = (2^4)^{2^{n-2}} + 1 \equiv 2 \pmod{5}$, and by Theorem 5.3, the Fermat prime f_n has the Midy property.

Thus every Fermat primes satisfies the Midy property in base τ . Unfortunately, as of today, only 5 Fermat primes are known, namely f_n , for $n = 0, 1, 2, 3, 4$.

6 Comments

Let us discuss possible generalizations of our result to other bases.

- Theorem 4.1 is stated for the golden ratio base. It is likely that one can generalize it for all bases β which are quadratic Pisot units with norm equal to -1 , i.e. roots of polynomials $f(X) = X^2 - mX - 1$, $m \geq 1$. However, much less is known about

divisibility properties of sequences defined by the linear recurrence with characteristic polynomial f . Some results of this kind can be found in [14].

On the other hand, no q can satisfy the Midy property in base β which is a quadratic Pisot unit with norm equal to $+1$. For, it is known [8] that no rational number in the interval $(0, 1)$ has purely periodic β -expansion.

- The original Midy's theorem considers integer bases, which are naturally not algebraic units. One can observe $q \in \mathbb{N}$ with the Midy property even in non-integer bases $\beta > 1$ that are non-units. According to Akiyama [2], if the base β is chosen to be the quadratic Pisot number with minimal polynomial $X^2 - mX - n$, $m \geq n$, then every reduced fraction whose denominator is coprime to $N(\beta) = n$ has a purely periodic β -expansion. For example, let $\beta = 1 + \sqrt{3}$, i.e. β is a root of $X^2 - 2X - 2$. Then

$$\left(\frac{4}{5}\right)_\beta = 0.(201100100121011021112000)^\omega.$$

For the two halves of the period, we have

$$201100100121 + 011021112000 = 2121212121$$

which is a prefix of $d_\beta^*(1) = (21)^\omega$.

- As it was already mentioned in Remark 3.3, in the Tribonacci base, i.e., when $\beta > 1$ is a root of $X^3 - X^2 - X - 1$, no denominator q has the Midy property. On the other hand, we have tested fractions in base $\beta > 1$ which is a root of $X^4 - X^3 - X^2 - X - 1$ and we have found fractions $\frac{p}{q}$ such that

$$T^N\left(\frac{p}{q}\right) = \frac{q-p}{q} \quad \text{and} \quad T^N\left(\frac{q-p}{q}\right) = \frac{p}{q},$$

which by Lemma 3.1 implies the Midy property. For instance, for $\frac{p}{q} = \frac{1}{5}$ the previous equalities are satisfied with $N = 156$; for $\frac{p}{q} = \frac{1}{10}$ and $\frac{p}{q} = \frac{1}{25}$ with $N = 780$, for $\frac{p}{q} = \frac{1}{17}$ with $N = 2456$.

References

- [1] B. Adamczewski, C. Frougny, A. Siegel, and W. Steiner. Rational numbers with purely periodic β -expansion. *Bull. Lond. Math. Soc.*, 42:538-552, 2010.
- [2] S. Akiyama. Pisot numbers and greedy algorithm. In *Number theory (Eger, 1996)*, pages 9-21. de Gruyter, Berlin, 1998.
- [3] L. E. Dickson. *History of the theory of numbers. Vol. I: Divisibility and primality*. Chelsea Publishing Co., New York, 1966.
- [4] B. D. Ginsburg. Midy's (nearly) secret theorem - an extension after 165 years. *College Math. J.*, 35(1):26-30, 2004.

- [5] H. Goodwyn. Curious properties of prime numbers taken as the divisors of unity. *J. Natur. Philos. Chem. Arts*, 1:314-316, 1802.
- [6] A. Gupta and B. Sury. Decimal expansion of $1/p$ and subgroup sums. *Integers*, 5(1):A19, 5, 2005.
- [7] J. H. Halton. On the divisibility properties of Fibonacci numbers. *Fibonacci Quart.*, 4:217-240, 1966.
- [8] M. Hama and T. Imahashi. Periodic β -expansions for certain classes of Pisot numbers. *Comment. Math. Univ. St. Pauli*, 46:103-116, 1997.
- [9] W. G. Leavitt. A theorem on repeating decimals. *Amer. Math. Monthly*, 74:669-673, 1967.
- [10] J. Lewittes. Midy's theorem for periodic decimals. *Integers*, 7:A2, 11, 2007.
- [11] H. W. Martin. Generalizations of Midy's theorem on repeating decimals. *Integers*, 7:A3, 7, 2007.
- [12] E. Midy. *De Quelques Propriétés des Nombres et des Fractions Décimales Périodiques*. College of Nantes, France, 1836.
- [13] W. Parry. On the β -expansions of real numbers. *Acta Math. Hung.*, 11(3-4):401-416, 1960.
- [14] M. Renault. The period, rank, and order of the (a, b) -Fibonacci sequence mod m . *Math. Mag.*, 86(5):372-380, 2013.
- [15] K. A. Ross. Repeating decimals: a period piece. *Math. Mag.*, 83(1):33-45, 2010.
- [16] A. Rényi. Representations for real numbers and their ergodic properties. *Acta Math. Hung.*, 8:477-493, 1957.
- [17] K. Schmidt. On periodic expansions of Pisot numbers and Salem numbers. *Bull. Lond. Math. Soc.*, 12(4):269-278, 1980.
- [18] M. Shrader-Frechette. Complementary rational numbers. *Math. Mag.*, 51(2):90-98, 1978.

Received: January 9, 2024

Accepted for publication: April 25, 2024

Communicated by: Emilie Charlier, Julien Leroy and Michel Rigo