ICMASE 2025

A VIETORIS-BASED NUMBER SEQUENCE AND THEIR APPLICATION IN CRIPTOGRAPHY

Regina De ALMEIDA[1,2,*], Paula CATARINO[1,2]

[1]*Department of Mathematics, University of Trás-os-Montes e Alto Douro, Portugal*
[2]*CMAT - Centre of Mathematics, Polo CMAT-UTAD*

ABSTRACT

In this study, one considers an integer sequence associated with the sequence of rational numbers known as the *Vietoris' sequence*. In 1958, L. Vietoris presented a result in [5] concerning the positivity problems of trigonometric sums, wherein this sequence naturally emerged. The first Vietoris' numbers of the sequence are

$$1,\ \frac{1}{2},\ \frac{1}{2},\frac{3}{8},\ \frac{3}{8},\ \frac{5}{16},\ \frac{5}{16},\ \frac{35}{128},\ \frac{35}{128},\ \frac{63}{256},\ \frac{63}{256},\ \frac{231}{1024},\ \frac{231}{1024},\ \cdots,$$

which is related with the sequence A283208 in the On-Line Encyclopedia of Integer Sequences (OEIS) in [4]. This sequence, which will be denoted by $\{v_n\}_{n\geqslant 0}$, is defined as

$$v_n = \frac{1}{2^n}\binom{n}{\lfloor \frac{n}{2} \rfloor}, \qquad n \geqslant 0,$$

where $\lfloor\cdot\rfloor$ is the floor function. It is also well established that the recurrence relation governing this sequence is given by the following expression

$$v_n = \begin{cases} 1, & n = 0 \\ d_n\ v_{n-1}, & n \neq 0 \end{cases} \tag{1}$$

where, for $\sigma(n) = \frac{1+(-1)^n}{2}$,

$$d_n = \frac{n+\sigma(n)}{n+1} = \begin{cases} 1, & n\ even \\ \frac{n}{n+1}, & n\ odd \end{cases}.$$

For further information on Vietoris numbers, see for example [1, 3].
In view of the identity $v_{2n+1} = v_{2n+2}$ for $n \in \mathbb{N}_0$, it is natural to consider the subsequence of Vietoris' sequence with odd index $\{v_{2n+1}\}_{n\geqslant 0}$. In [2] the elements of sequence $\{v_{2n+1}\}_{n\geqslant 0}$ were explicitly represented as follows

$$v_{2n+1} = \frac{a_n}{2^{n+1+m_n}}, \tag{2}$$

where the sequence $\{a_n\}_{n\geqslant 0}$ is the numerators of the subsequence of the Vietoris' number sequence $\{v_{2n+1}\}_{n\geqslant 0}$ and

$$m_n = \left\lfloor \frac{n+1}{2} \right\rfloor + \left\lfloor \frac{n+1}{2^2} \right\rfloor + \cdots + \left\lfloor \frac{n+1}{2^m} \right\rfloor, \quad m \leq \log_2(n+1). \tag{3}$$

The sequence $\{n+m_n\}_{n\geqslant 0}$ is called the minimal exponent integer sequence with respect to 2 and is the sequence A283208 in the OEIS in [4].

[*]*Corresponding Author's E-mail: ralmeida@utad.pt*

Due to inherent challenges and potential vulnerabilities associated with using rational sequences in cryptographic encoding and decoding processes, one will consider, in this study the sequence of integer odd numbers $\{a_n\}_{n\geqslant 0}$. The first numbers of the sequence $\{a_n\}_{n\geqslant 0}$ are

$$1,\ 3,\ 5,\ 35,\ 63,\ 231,\ \cdots,$$

which are identified as the sequence A001790 in the OEIS in [4]. These numbers emerge as the numerators of the coefficients in the Maclaurin series expansion associated with the corresponding real-valued function $f(x) = \frac{1}{\sqrt{1-x}}$ for $x < 1$.

On account of equation (2), the sequence $\{a_n\}_{n\geqslant 0}$ can be expressed in terms of Vietoris' numbers, by

$$a_n = 2^{n+1+m_n} v_{2n+1}. \tag{4}$$

Furthermore, applying (2) in (1), on obtains the following recurrence relation

$$a_n = \alpha_{m_n} a_{n-1}, \qquad n \in \mathbb{N},$$

where $\alpha_{m_n} = \frac{2n+1}{n+1} 2^{m_n - m_{n-1}}$ and m_n is defined in (3).

In this study, matrices whose elements are derived from the sequence $\{a_n\}_{n\geqslant 0}$ are introduced, along with an analysis of some of their fundamental properties. These matrices are subsequently employed to explore potential applications in cryptography, particularly in the construction of encoding and decoding algorithms.

***K*eywords** Cryptography · Recurrence relation · Vietoris' number

References

[1] Cação I., Falcão M.I., Malonek H.R., Miranda F., and Tomaz G., Remarks on the Vietoris Sequence and Corresponding Convolution Formulas. In: Gervasi, O., et al. Computational Science and Its Applications – ICCSA 2023 Workshops. ICCSA 2023. Lecture Notes in Computer Science, vol 14104. Springer, Cham., 677-692, 2023.

[2] Cação I., Falcão M.I., and Malonek H.R., Hypercomplex Polynomials, Vietoris' Rational Numbers and a Related Integer Numbers Sequence, Complex Anal. Oper. Theory 11:1059 - 1076, 2017.

[3] Catarino P.,and De Almeida R., A Note on Vietoris' Number Sequence, Mediterranean Journal of Mathematics, 19(1), 41, 2022.

[4] Sloane, N.J.A., Plouffe, S., The Encyclopedia of Integer Sequences, Academic Press, San Diego, 1995.

[5] Vietoris L., Über das Vorzeichen gewisser trigonometrischer Summen. Sitzungsber. Österr. Akad. Wiss 167: 125–135, 1958.