Malaysian Journal of Mathematical Sciences

Journal homepage: https://einspem.upm.edu.my/journal

Power of Frobenius Endomorphism and its Performance on PseudoTNAF System

Yunos, F. *[1], Yusof, A. M.[2], Hadani, N. H.[3], Ariffin, M. R. K.[1,3], and Sapar, S. H.[1,3]

[1]*Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, Malaysia*
[2]*Faculty of Science and Natural Resource, Universiti Malaysia Sabah, Malaysia*
[3]*Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia*

E-mail: faridahy@upm.edu.my
**Corresponding author*

Received: 15 June 2021
Accepted: 8 October 2021

Abstract

Let E be an elliptical curve defined over F_{2^m} and the mapping τ is a Frobenius endomorphism from the set F_{2^m} to itself. The Koblitz curve is a special curve whose τ has been used to improve the calculation performance of its scalar multiplication, nP where P is a point on the curve E. Moreover, the multiplier, n is τ -adic non adjacent form (TNAF) expansion where its digit is generated by the repeated division of an integer in the ring of $Z(\tau)$ by τ. Previous research has found that the power of Frobenius endomorphism τ^m has some advantages in TNAF, Reduced TNAF and their equivalent i.e. pseudoTNAF expansions. In this paper, new finding of τ^m based on v-simplex and arithmetic sequences is provided. With this approach, the performance of converting modulo $\rho\frac{\tau^m-1}{\tau-1}$ to $r+s\tau$ an element of $Z(\tau)$ in pseudoTNAF's system is enhanced.

Keywords: cryptography; field; Frobenius endomorphism; Koblitz curve; number of elliptic points; sequence of arithmetic; sequence of simplex; τ-adic non adjacent.

1 Introduction

Elliptical Curve Cryptography (ECC) was introduced in 1985 by [9]. ECC's secret messaging system is a public key mechanism for which scalar multiplication (SM) is the dominant operation. This SM involves computing integer n with a point P on an elliptic curve. The ECC system has been standardized as the most effective cryptographic system used since 1987 due to its difficulty in finding the secret key n which is a multiplier of P. Koblitz's curves originally named anomalous binary curves are defined over F_2 as follows:

$$E_a : y^2 + xy = x^3 + ax^2 + 1,$$

with $a \in \{0, 1\}$ as suggested by [12] in 1997. Cost of computational operations on Koblitz curve can be reduced in the existence of Frobenius endomorphism [10]. Let $\tau : E_a(F_{2^m}) \rightarrow E_a(F_{2^m})$ be a Frobenius mapping for a point $P = (x, y)$ on $E_a(F_{2^m})$ be defined as $\tau(x, y) = (x^2, y^2)$ and $\tau(\infty) = \infty$. $E_a(F_{2^m})$ forms an abelian group under addition operation. The identity of the abelian group is the point at infinity ∞, whereas the point addition can be computed by the chord and tangent method [11]. Suppose the trace for the mapping is $t = (-1)^{1-a}$ and its identity is given by $\tau^2 = t\tau - 2$, so $(\tau^2 + 2)P = t\tau(P)$. For fast computation on such curves, Koblitz considered a base-τ expansion of elements in ring $Z(\tau)$ with $\tau = \frac{1+\sqrt{-7}}{2}$. Suppose P and Q are points on Koblitz curve. SM is n multiple repetition of a point on the curve and is denoted as $nP = P + P + \cdots + P$ such that $nP = Q$.

Solinas [12] introduced a multiplier of SM in the form of τ-adic non-adjacent (TNAF) (see Definition 2.1) on the Koblitz curve to reduce elliptical SM costs. To improve its performance, another SM algorithm based on a reduced τ-adic non-adjacent form (RTNAF) (see Definition 2.2) was developed by [13]. He also showed that given a Lucas relation $U(t, 2)$, $U_{m+1} = tU_m - 2U_{m-1}$ where $U_0 = 0$, $U_1 = 1$, then

$$\tau^m = \tau U_m - 2U_{m-1}, \tag{1}$$

for all $m > 0$. This equation can be applied for computing the order of the curve via the norm of $\tau^m - 1$ and to convert the relation τ^m into $r + s\tau$ which is an element in the ring of $Z(\tau)$ where r and s are integers. Once $r + s\tau$ is computed, an equivalent integer n modulo $\frac{\tau^m - 1}{\tau - 1}$ (i.e. based on RTNAF) can be easily obtained before implementing nP.

Brumley & Järvinen [2] presented an efficient procedure to compute $r + s\tau$ from the input all bit c_i among $\sum_{i=0}^{l-1} c_i\tau^i$ expansion using recurrence $U(t, 2)$ sequence and equation (1). They applied it onto a Field Programmable Gate Array (FPGA) to produce an equivalent integer n. It is known that FPGA is an integrated circuit reprogrammed by a customer or a designer to be desired application or functionality requirements after manufacturing.

Yunos *et al.* [16] introduced a better alternative to the TNAF and RTNAF known as pseudoTNAF (see Definition 2.3) if it satisfies a specific criteria. In addition, they rephrased equation (1) to construct another power of τ expression as follows:

$$\tau^m = y_m t^m + x_m t^{m+1}\tau, \tag{2}$$

with $x_0 = 0$, $y_0 = 1$, $x_m = x_{m-1} + y_{m-1}$ and $y_m = -2x_{m-1}$ for $m > 0$. It is obviously useful to accelerate the process of transforming an expansion in the form of TNAF($\sum_{i=0}^{l-1} c_i\tau^i$) (see Definition 2.1) into $r + s\tau$ an element of $Z(\tau)$. Ali & Yunos [1] applied it to obtain the minimum and maximum of TNAF's norms that occur among all elements in $Z(\tau)$ on Koblitz curve. Furthermore, the operation cost of the SM can be calculated after the length of pseudoTNAF expansion is estimated more precisely. Indirectly, by using equation (2), Yunos *et al.* [16] and Hadani *et al.* [8] found that $N(\tau^m - 1)$ can be used as an alternative calculation method to determine the number of points on the curve.

Until now, studies on finding the practical formula for τ^m to strengthen the invulnerability of the pseudoTNAF-based cryptographic system is still active and equation (2) is efficiently used to convert $\frac{\tau^m-1}{\tau-1}$ into $r + s\tau$. The following are some research that benefits from this conversion. Yunos & Suberi [17] determined that selection of coefficients r_0 and r_1 from $\rho = r_0 + r_1\tau$, and the coefficients of r and s from $\frac{\tau^m-1}{\tau-1}$ are either even or odd. However, they do not explain how to identify the appropriate m so that the coefficients r and s becomes even or odd. They were also unable to find the nature of ρ so that the density of non-zero digits (measured by the Hamming weights) in expansion of pseudoTNAF with mod $\rho\frac{\tau^m-1}{\tau-1}$ is lower than for those in the TNAF and RTNAF.

In recognition of the importance of τ^m, Hadani *et al.* [8] produced another formula of τ^m as follows:

$$\tau^m = -2s_{m-1} + s_m\tau, \tag{3}$$

as detailed in Propositions 2.1 and 2.2. The construction was based upon pyramid number's formula [3], Nichomacus Theorem [7] and Faulhaber formula [6] but it is still a bit complex. Our objective of this research is to derive τ^m in a more concise form which is based on v-simplex and arithmetic sequences. Our concern here, can this formula help us to enhance the performance of converting $\rho\frac{\tau^m-1}{\tau-1}$ to $r + s\tau$ before doing a scalar multiplication (nP) where n in the form of pseudoTNAF?

The organization of this paper is as follows. Section 1 describes three types of τ^m (refer (1), (2) and (3)) with some advantages. In Section 2, the preliminaries of this study is presented. Meanwhile, Section 3 discusses on how to construct a general formula for the coefficient $f_i(m)$ in expansion of s_m for $2 \leq i \leq \frac{m+1}{2}$ and $m \geq 2i - 1$ (refer Definition 2.7), and then introduce a new approach for developing $\tau^m = r_m + s_m\tau$ an element in $Z(\tau)$. The main advantage of using this formula is discussed in Section 4. The concluding chapter contains a summary of the paper, and also proposes future studies.

2 Preliminaries

The following are some definitions from [17] considered in this paper.

Definition 2.1. *A τ-adic non-adjacent form (also called τ-NAF or TNAF) of nonzero $\bar{n}$ in $Z(\tau)$ is equal to $\sum_{i=0}^{l-1} c_i\tau^i$ where $c_i \in \{-1, 0, 1\}$ and $c_ic_{i+1} = 0$ for all i. If $c_{l-1} \neq 0$ then l is said to be the length of τ-NAF.*

TNAF($\bar{n}$) in the form $\sum_{i=0}^{l-1} c_i\tau^i$ is an expansion with its digits generated by successively divid-

ing $\bar{n}$ by τ and allowing remainders $-1, 0$, or 1. An example to obtain a TNAF for certain integer is shown in Example 5.1.

Definition 2.2. *A Reduced τ-adic non-adjacent form (also called RTNAF) of nonzero $\bar{n}$ in $Z(\tau)$ is $\sum_{i=0}^{l-1} c_i\tau^i$ that is equal to n mod $\frac{\tau^m-1}{\tau-1}$, where $c_i \in \{-1, 0, 1\}$ and $c_i c_{i+1} = 0$ for all i. If $c_{l-1} \neq 0$ then l is said to be the length of RTNAF.*

Definition 2.3. *A Pseudo τ-adic Non-Adjacent Form (also called pseudoTNAF) of nonzero $\bar{n}$ in $Z(\tau)$ is $\sum_{i=0}^{l-1} c_i\tau^i$ that is equal to n mod $\rho\frac{\tau^m-1}{\tau-1}$, where $\rho \in Z(\tau), c_i \in \{-1, 0, 1\}$ and $c_i c_{i+1} = 0$ for all i. If $c_{l-1} \neq 0$ then l is said to be the length of pseudoTNAF.*

Definition 2.4. *Let $N : Q(\tau) \to Q$ be a rational set as a function of norm. Let $\alpha = x + y\tau$ an element $Q(\tau)$. The norm of α is $N(\alpha) = x^2 + txy + 2y^2$ where $t = (-1)^{1-a}$ and $a \in \{0, 1\}$.*

An expression $\frac{\tau^m-1}{\tau-1}$ and $\rho\frac{\tau^m-1}{\tau-1}$ as in Definitions 2.2 and 2.3 can be converted into $r + s\tau$. We choose any integer n from interval $[1, |\rho'|N(r' + s'\tau) - 1]$ such that $r + s\tau = \rho'(r' + s'\tau)$ where ρ' is an integer. After that, $\bar{n}$ in $Z(\tau)$ can be generated from dividing an integer n by $r + s\tau$. Lastly, RTNAF$(\bar{n})$ and pseudoTNAF$(\bar{n})$ can be written in the form of expansion $\sum_{i=0}^{l-1} c_i\tau^i$ where the digits are generated by successively dividing $\bar{n}$ by τ, allowing remainders $-1, 0$, or 1. Whereas SM, $\bar{n}P$ process is illustrated in Figure 1 and can be found in Yunos & Suberi [17] in 2018.

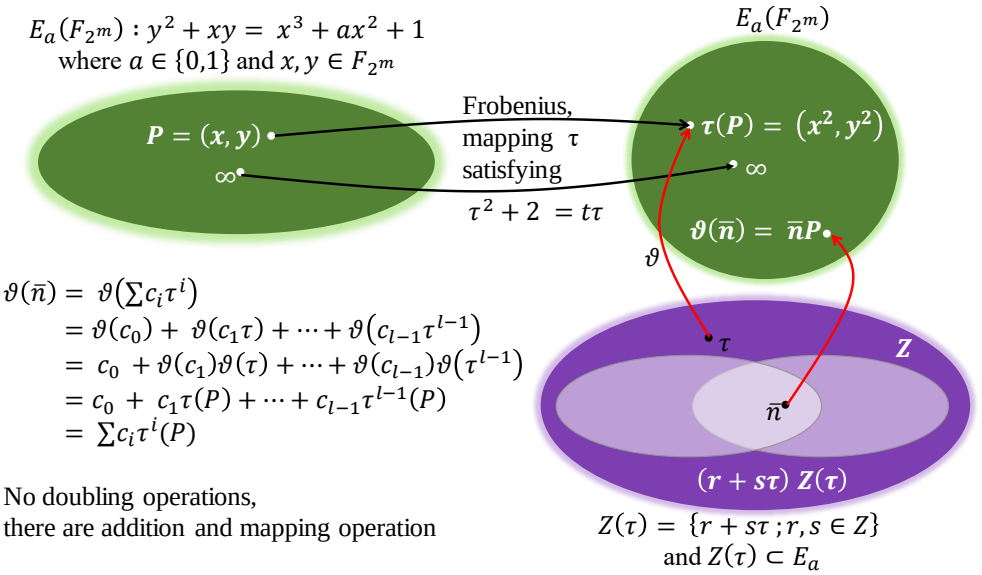

Figure 1: Illustration of SM on Koblitz curve.

Definition 2.5. [5] *A v-simplex for $j, v \in \mathbb{Z}^+$ can be expressed as*

$$\frac{j(j+1)(j+2)\cdots(j+v-1)}{v!} = \binom{j+v-1}{v}.$$

Remark 2.1. *If $v = 1$ then 1-simplex number also known as linear number with formula $\frac{j}{1} = \binom{j}{1}$. If $v = 2$ then 2-simplex number also known as triangular number with formula $\frac{j(j+1)}{2} = \binom{j+1}{2}$. Another formula is $\sum_{k=1}^{j} k = 1 + 2 + 3 + \cdots + j$ [5].*

If $v = 3$ then 3-simplex also known as tetrahedral number with formula $\frac{j(j+1)(j+2)}{6} = \binom{j+2}{3}$ [5].

If $v = 4$ then 4-simplex also known as pentatope number with formula $\frac{j(j+1)(j+2)(j+3)}{24} = \binom{j+3}{4}$ [4].

Definition 2.6. [14] *A sequence $a_1, a_2, a_3, \ldots, a_k, \ldots$ is called an arithmetic progression if there exist a scalar d known as common difference among consecutive terms of the sequence such that $a_k - a_{k-1} = d$ for all $k > 1$.*

Theorem 2.1. [14],[15] *If a_1 and d are the first term and common difference respectively in arithmetic sequence with pattern $a_1, a_1+d, a_1+2d, a_1+3d, \ldots$ then the k^{th} term can be written as $a_k = a_1+(k-1)d$.*

Definition 2.7. [8] *Given $\tau^m = r_m + s_m\tau$ an element of $Z(\tau)$ for any positive integer m. Let $f_1(m) = 1$. We defined $f_i(m)$ be a coefficient in expansion of s_m for $i \in \{1, \ldots, \lfloor \frac{m-1}{2} \rfloor\}$.*

Proposition 2.1. [8] *Given $\tau^m = r_m + s_m\tau$ an element of $Z(\tau)$ for any positive integer m. Let $s_1 = 1$ and $s_2 = t$. If $f_i(m) = \frac{(-2)^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j)$ for $2 \leq i \leq \frac{m+1}{2}$ and $m \geq 2i-1$, then the coefficient s_m can be written as $s_m = \sum_{i=1}^{\lfloor \frac{m+1}{2} \rfloor} f_i(m)t^{m-2i+1}$ with $f_1(m) = 1$ and $m \geq 3$.*

Proposition 2.2. [8] *If s_m from Proposition 2.1, then the coefficient r_m can be written as $r_m = -2s_{m-1}$ with $f_1(m) = 1$ and $m \geq 3$.*

3 Results and Discussion

In this section, we consider $\tau^m = r_m + s_m\tau$ in which s_m expansion has the coefficient $f_i(m)$ (Definition 2.7). The identity equation $\tau^2 = t\tau - 2$ is chose to transform τ^m into $r_m + s_m\tau$ for $m \in \mathbb{Z}^+$. Followed by the following examples for calculation of two values of m.
For $\tau^3 = \tau^2\tau = -2t + (t^2-2)\tau$, then $r_3 = -2t$ and $s_3 = t^2 - 2$ are obtained.
For $\tau^4 = \tau\tau^3 = -2t^2 + 4 + (t^3 - 4t)\tau$, then $r_4 = -2t^2 + 4$ and $s_4 = t^3 - 4t$ are observed.
Next, the data of s_m and r_m for $1 \leq m \leq 15$ are listed as in Table 1. Subsequently, the term s_m in $\tau^m = r_m + s_m\tau$ from this table can be represented in Table 2.

Table 1: All r_m and s_m of τ^m for $1 \leq m \leq 15$.

m	r_m	s_m
1	0	1
2	-2	t
3	$-2t$	t^2-2
4	$-2t^2+4$	t^3-4t
5	$-2t^3+8t$	t^4-6t^2+4
6	$-2t^4+12t^2-8$	t^5-8t^3+12t
7	$-2t^5+16t^3-24t$	$t^6-10t^4+24t^2-8$
8	$-2t^6+20t^4-48t^2+16$	$t^7-12t^5+40t^3-32t$
9	$-2t^7+24t^5-80t^3+64t$	$t^8-14t^6+60t^4-80t^2+16$
10	$-2t^8+28t^6-120t^4+160t^2-32$	$t^9-16t^7+84t^5-160t^3+80t$
11	$-2t^9+32t^7-168t^5+320t^3-160t$	$t^{10}-18t^8+112t^6-280t^4+240t^2-32$
12	$-2t^{10}+36t^8-224t^6+560t^4-480t^2+64$	$t^{11}-20t^9+144t^7-448t^5+560t^3-192t$
13	$-2t^{11}+40t^9-288t^7+896t^5-1120t^3+384t$	$t^{12}-22t^{10}+180t^8-672t^6+1120t^4-672t^2+64$
14	$-2t^{12}+44t^{10}-360t^8+1344t^6-2240t^4+1344t^2-128$	$t^{13}-24t^{11}+220t^9-960t^7+2016t^5-1792t^3+448t$
15	$-2t^{13}+48t^{11}-440t^9+1920t^7-4032t^5+3584t^3-896t$	$t^{14}-26t^{12}+264t^{10}-1320t^8+3360t^6-4032t^4+1792t^2-128$

Table 2: List of all coefficient $f_i(m)$ in s_m expansion for $1 \leq i \leq 8$ and $1 \leq m \leq 15$.

m	$f_1(m)$	$f_2(m)$	$f_3(m)$	$f_4(m)$	$f_5(m)$	$f_6(m)$	$f_7(m)$	$f_8(m)$
1	1							
2	1							
3	1	-2						
4	1	-4						
5	1	-6	4					
6	1	-8	12					
7	1	-10	24	-8				
8	1	-12	40	-32				
9	1	-14	60	-80	16			
10	1	-16	84	-160	80			
11	1	-18	112	-280	240	-32		
12	1	-20	144	-448	560	-192		
13	1	-22	180	-672	1120	-672	64	
14	1	-24	220	-960	2016	-1792	448	
15	1	-26	264	-1320	3360	-4032	1792	-128

Referring to Table 2, the general form of a certain $f_i(m)$ can be identified by its relation to the sequence of v-simplex number (Definition 2.5) for $v = 2, 3, 4, 5$ and the arithmetic sequence as in Definition 2.6 and Theorem 2.1. The sequence $\{f_2(m)\}_{m=3}^{m=12} = \{-2, -4, -6, \ldots, -20\}$ is observed where its general formula for $\{f_2(m)\}_{m=3}^{m=\infty}$ is as follows:

Lemma 3.1. *If* $\{f_2(m)\}_{m=3}^{m=\infty} = \{-2, -4, -6, -8, -10, \ldots\}$, *then the coefficient* $f_2(m)$ *can be written as* $f_2(m) = -2(m-2)$.

Proof. By Theorem 2.1 and Definition 2.6, the sequence $\{f_2(m)\}_{m=3}^{m=\infty} = \{-2, -4, -6, -8, -10, \ldots\}$ is an arithmetic with its common difference $d = -2$. Substitute both values into formula in Theorem 2.1 for the m^{th} term that is $f_2(m) = f_2(3)+(m-3)d$. Therefore, $f_2(m) = -2+(m-3)(-2) = -2(m-2)$. □

Referring to Table 2, it is observed that the sequence $\{f_3(m)\}_{m=5}^{m=12} = \{4, 12, 24, 40, 60, 84, 112, 144\}$ with its general term $f_3(m)$ can be found from the following argument:

Lemma 3.2. *Let* $\{f_3(m)\}_{m=5}^{m=\infty} = \{4, 12, 24, 40, 60, 84, 112, 144, \ldots\}$. *If* $\{1, 3, 6, 10, 15, 21, 28, 36, \ldots\}$ *satisfies a sequence of triangular number, then the coefficient* $f_3(m)$ *can be written as* $f_3(m) = 2(m-4)(m-3)$.

Proof. It is known that $\{1, 3, 6, 10, 15, 21, 28, 36, \ldots\}$ is a sequence of triangular number as in Definition 2.5 with a general formula $\frac{j^2+j}{2}$ for integer $j \geq 1$. Next, sequence $\{f_3(m)\}_{m=5}^{m=\infty} = \{4, 12, 24, 40, 60, 84, 112, 144, \ldots\}$ is rewritten as $4\{1, 3, 6, 10, 15, 21, 28, 36, \ldots\}$. Substituting $j = m - 4$ into $4(\frac{j^2+j}{2})$, coefficient $f_3(m)$ can be written as $f_3(m) = 2(m-4)(m-3)$ with integer $m \geq 5$. □

Further from Table 2, the sequence $\{f_4(m)\}_{m=7}^{m=12} = \{-8, -32, -80, -160, -280, -448\}$ has general term $f_4(m)$ obtained by the following lemma:

Lemma 3.3. *Let* $\{f_4(m)\}_{m=7}^{m=\infty} = \{-8, -32, -80, -160, -280, -448, \dots\}$. *If* $\{1, 4, 10, 20, 36, 56, \dots\}$ *satisfies a sequence of tetrahedral number, then the coefficient* $f_4(m)$ *can be written as* $f_4(m) = -\frac{4}{3}(m-6)(m-5)(m-4)$.

Proof. It is known that $\{1, 4, 10, 20, 36, 56, \dots\}$ is a sequence of tetrahedral (Definition 2.5) with formula $\frac{j(j+1)(j+2)}{6}$ for integer $j \geq 1$. Next, sequence $\{-8, -32, -80, -160, -280, -448, \dots\}$ can be written as $-8\{1, 4, 10, 20, 36, 56, \dots\}$. By substituting $j = m-6$ into $-8\frac{j(j+1)(j+2)}{6}$, we obtained that $f_4(m) = -\frac{4}{3}(m-6)(m-5)(m-4)$ for integer $m \geq 7$. □

Through observation, sequence $\{f_5(m)\}_{m=9}^{m=15} = \{16, 80, 240, 560\}$ from Table 2 can be reconstructed using a pattern of pentatope number. A general term $f_5(m)$ for integers $m \geq 9$ was developed as follows:

Lemma 3.4. *Let* $\{f_5(m)\}_{m=9}^{m=\infty} = \{16, 80, 240, 560, \dots\}$. *If* $\{1, 5, 15, 35, 70, \dots\}$ *satisfies a sequence of pentatope numbers, then the coefficient* $f_5(m)$ *can be written as* $f_5(m) = \frac{2}{3}(m-8)(m-7)(m-6)(m-5)$.

Proof. It is known that the sequence $\{1, 5, 15, 35, 70, \dots\}$ has a pattern of sequence of pentatope number as in Definition 2.5 with formula $\frac{j(j+1)(j+2)(j+3)}{24}$ for integer $j \geq 1$. Now, $\{f_5(m)\}_{m=9}^{m=\infty} = \{16, 80, 240, 560, \dots\}$ can be written as $16\{1, 5, 15, 35, 70, \dots\}$ with formula $16\frac{j(j+1)(j+2)(j+3)}{24}$. We substitute $j = m-8$ into this relation in order to get $f_5(m) = \frac{2}{3}(m-8)(m-7)(m-6)(m-5)$ for integer $m \geq 9$. □

Finally, observing from Table 2, we found that $\{f_6(m)\}_{m=11}^{m=15} = \{-32, -192, -672, -1792, -4032\}$ can be rearranged like a pattern of 5-simplex number and this sequence in general term is illustrated as follows:

Lemma 3.5. *Let* $\{f_6(m)\}_{m=11}^{m=\infty} = \{-32, -192, -672, -1792, -4032, \dots\}$. *If* $\{1, 6, 21, 56, \dots\}$ *satisfies a sequence of 5-simplex number, then the coefficient* $f_6(m)$ *can be written as*

$$f_6(m) = -4\frac{(m-10)(m-9)(m-8)(m-7)(m-6)}{15}.$$

Proof. It is known that sequence $\{1, 6, 21, 56, \dots\}$ with pattern of 5-simplex number has general formula $\frac{j(j+1)(j+2)(j+3)(j+4)}{120}$ with integer $j \geq 1$ as in Definition 2.5. Now,

$$\{f_6(m)\}_{m=11}^{m=\infty} = \{-32, -192, -672, -1792, -4032, \dots\}$$

can be rewritten as $-32\{1, 6, 21, 56, \dots\}$ with general formula $-32\frac{j(j+1)(j+2)(j+3)(j+4)}{120}$. We substitute $j = m-10$ into this relation to obtain $f_6(m) = -4\frac{(m-10)(m-9)(m-8)(m-7)(m-6)}{15}$ for integer $m \geq 11$. □

Next, the patterns of $f_2(m)$ up to $f_6(m)$ of Lemmas 3.1-3.5 can be used to construct the coefficient $f_i(m) = (-2)^{i-1}\binom{m-i}{i-1}$ in s_m expansion. The argument of proof is as follows:

Theorem 3.1. *If* $f_1(m) = 1$, *then*

$$f_i(m) = (-2)^{i-1}\binom{m-i}{i-1},$$

for $2 \leq i \leq \frac{m+1}{2}$ *and* $m \geq 2i-1$.

Proof. The argument of this proof is to use mathematical induction as follows :

If $i = 2$, we have the relation $f_2(m) = -2(m-2)$ in Lemma 3.1 and found that

$$f_2(m) = (-2)^{2-1}\binom{m-2}{2-1} \text{ is true.}$$

If $i = 3$ the relation $f_3(m) = 2(m-3)(m-4)$ in Lemma 3.2, then

$$\begin{aligned} f_3(m) &= \frac{4(m-3)(m-4)}{2!} \\ &= \frac{4(m-3)!}{2!(m-5)!} \\ &= (-2)^{3-1}\binom{m-3}{3-1} \text{ is true.} \end{aligned}$$

Subsequently, if $i = 3, 4, 5$, then $f_i(m) = (-2)^{i-1}\binom{m-i}{i-1}$ is true by using Lemmas 3.3, 3.4 and 3.5. Now, assume that $f_k(m) = (-2)^{k-1}\binom{m-k}{k-1}$ is true for $i = k$. Therefore,

$$\begin{aligned} f_{k+1}(m) &= \frac{f_k(m)}{2\frac{(-2)^{-1}(m-k)}{(m-2k+1)(m-2k)}} \\ &= \frac{(-2)^{k-1}\binom{m-k}{k-1}}{k\frac{(-2)^{-1}(m-k)}{(m-2k+1)(m-2k)}} \\ &= \frac{(-2)^{k-1}\frac{(m-k)!}{(k-1)!(m-2k+1)!}}{k\frac{(-2)^{-1}(m-k)}{(m-2k+1)(m-2k)}} \\ &= (-2)^k\frac{(m-k-1)!}{k(k-1)!(m-2k-1)!} \\ &= (-2)^k\binom{m-k-1}{k} \\ &= (-2)^{k+1-1}\binom{m-(k+1)}{(k+1)-1}. \end{aligned}$$

Thus, $f_{k+1}(m) = (-2)^{k+1-1}\binom{m-(k+1)}{(k+1)-1}$ is also true by using $f_k(m)$. In conclusion, $f_i(m) = (-2)^{i-1}\binom{m-i}{i-1}$ is true for all $2 \leq i \leq \frac{m+1}{2}$ and $m \geq 2i-1$.

□

Furthermore, the following corollary is obtained:

Corollary 3.1. *Let* $\tau^m = r_m + s_m\tau$ *and* $f_i(m) = (-2)^{i-1}\binom{m-i}{i-1}$ *be a coefficient in expansion of* s_m *if and only if* $f_i(m) = \frac{(-2)^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j)$ *for* $2 \leq i \leq \frac{m+1}{2}$ *and* $m \geq 2i-1$.

Proof. ($\Rightarrow$)

$$\begin{aligned} f_i(m) &= (-2)^{i-1}\tbinom{m-i}{i-1} \\ &= (-2)^{i-1}\frac{(m-i)!}{(i-1)!(m-2i+1)!} \\ &= \frac{(-2)^{i-1}}{(i-1)!}\cdot\frac{(m-i)(m-i-1)\cdots(m-2i+2)(m-2i+1)!}{(m-2i+1)!} \\ &= \frac{(-2)^{i-1}}{(i-1)!}\cdot(m-i)(m-i-1)\cdots(m-2i+3)(m-2i+2) \\ &= \frac{(-2)^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j). \end{aligned}$$

($\Leftarrow$)

$$\begin{aligned} f_i(m) &= \frac{(-2)^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j) \\ &= \frac{(-2)^{i-1}}{(i-1)!}\cdot(m-i)(m-i-1)\cdots(m-2i+3)(m-2i+2) \\ &= \frac{(-2)^{i-1}}{(i-1)!}\cdot\frac{(m-i)(m-i-1)\cdots(m-2i+2)(m-2i+1)!}{(m-2i+1)!} \\ &= (-2)^{i-1}\frac{(m-i)!}{(i-1)!(m-2i+1)!} \\ &= (-2)^{i-1}\tbinom{m-i}{i-1}. \end{aligned}$$

□

In this paper, we also improve the result of [8] as in the following theorem:

Theorem 3.2. *Let $\tau^m = r_m + s_m\tau$ and $r_m = -2s_{m-1}$. If $f_i(m) = (-2)^{i-1}\binom{m-i}{i-1}$ then*

$$r_m = \sum_{i=1}^{\lfloor\frac{m}{2}\rfloor}(-2)^i\tbinom{m-1-i}{i-1}t^m \quad \textit{and} \quad s_m = \sum_{i=1}^{\lfloor\frac{m+1}{2}\rfloor}(-2)^{i-1}\tbinom{m-i}{i-1}t^{m+1}$$

for $m \geq 2$.

Proof. By using Proposition 2.2, we obtain

$$\begin{aligned} \tau^m &= -2s_{m-1} + s_m\tau \\ &= -2\sum_{i=1}^{\lfloor\frac{m}{2}\rfloor} f_i(m-1)t^{m-2i} + \sum_{i=1}^{\lfloor\frac{m+1}{2}\rfloor} f_i(m)t^{m-2i+1}\tau. \end{aligned}$$

If $f_i(m) = (-2)^{i-1}\binom{m-i}{i-1}$ and $t^2 = 1$ then

$$\tau^m = \sum_{i=1}^{\lfloor\frac{m}{2}\rfloor}(-2)^i\tbinom{m-1-i}{i-1}t^m + \sum_{i=1}^{\lfloor\frac{m+1}{2}\rfloor}(-2)^{i-1}\tbinom{m-i}{i-1}t^{m+1}\tau.$$

Therefore, $r_m = \sum_{i=1}^{\lfloor \frac{m}{2} \rfloor} (-2)^i \binom{m-1-i}{i-1} t^m$ and $s_m = \sum_{i=1}^{\lfloor \frac{m+1}{2} \rfloor} (-2)^{i-1} \binom{m-i}{i-1} t^{m+1}$. □

The formulas r_m and s_m from Theorem 3.2 are very important to simplify the process of transformations as follow:

Firstly, to recover $(r_m - 1) + s_m\tau$ that is an element in $Z(\tau)$ from $\tau^m - 1$ by substituting $r_m - 1$ and s_m into Definition 2.4, the number of points can be calculated through Koblitz curve E_a with

$$N(\tau^m - 1) = (r_m - 1)^2 + t(r_m - 1)s_m + s_m^2.$$

In order to estimate the operating cost of the $nP's$ scalar multiplication, it is an alternative method to calculate the points of Koblitz curve rather than using equation (2).

Secondly, to obtain TNAF(n) from the expansion of $\sum_{i=0}^{l-1} c_i\tau^i$ and the algorithm given as follows:

Algorithm 3.1

Input: $a \in \{0, 1\}$, l, all coefficients $c_m \in \{-1, 0, 1\}$ for $m = 0, 1, ..., l - 1$.
Output: $r + s\tau \in Z(\tau)$
Computation:
1. $t \leftarrow (-1)^{1-a}$;
2. For m from 0 to 1 do $d_m \leftarrow \tau^m$
3. For m from 2 to $l - 1$ do
4. $\quad h_m \leftarrow \lfloor \frac{m}{2} \rfloor$
5. $\quad g_m \leftarrow \lfloor \frac{m+1}{2} \rfloor$
6. $\quad r_m \leftarrow \sum_{k=1}^{h_m} \frac{(-2)^k (m-1-k)!}{(k-1)!(m-2k)!} t^m$
7. $\quad s_m \leftarrow \sum_{k=1}^{g_m} \frac{(-2)^{k-1} (m-k)!}{(k-1)!(m-2k+1)!} t^{m+1}$
8. $\quad d_m \leftarrow r_m + s_m\tau$
9. $r + s\tau \leftarrow add(c_m \cdot d_m, m = 0..l - 1)$
10. $Return\ (r + s\tau)$

For example, Algorithm 3.1 can be applied to recover $1 - 4\tau$ from $1 - \tau^3 - \tau^6$ (refer the reverse calculation in Example 5.1).

Remark 3.1. *Either curve E_0 or E_1 can be chose to give input $a \in \{0, 1\}$ in this algorithm. The same should be done if one want to choose a as an input of three algorithms in Section 4. Whereas, rewritten r_m and s_m in Theorem 3.2 into factorial symbols, the formulas were obtained in steps 6 and 7 in Algorithm 3.1, and steps 5 and 6 in Algorithm 4.1.*

The main advantage of using formula τ^m in Theorem 3.2 is discussed in the following section.

4 Performance of Converting $\rho\frac{\tau^m-1}{\tau-1}$ to $r + s\tau$

Converting $\frac{\tau^m-1}{\tau-1}$ into $r + s\tau$ illustrated in the following proof. This is an important transformation before finding pseudoTNAF's of integer in modulo $\rho\frac{\tau^m-1}{\tau-1}$.

Theorem 4.1. *If* $\tau^m = r_m + s_m\tau$ *and* $\frac{\tau^m-1}{\tau-1} = r + s\tau$, *then*

$$r = \frac{1 - t - r_m + r_m t + 2s_m}{3 - t},$$

and

$$s = \frac{1 - r_m - s_m}{3 - t},$$

for $m \geq 2$.

Proof. Let $\tau^m = r_m + s_m\tau$ and rewrite $\frac{\tau^m-1}{\tau-1}$ as follows:

$$\begin{aligned}
\frac{\tau^m - 1}{\tau - 1} &= \frac{r_m + s_m\tau - 1}{\tau - 1} \\
&= \frac{r_m + s_m\tau - 1}{\tau - 1}.\frac{\bar{\tau} - 1}{\bar{\tau} - 1} \\
&= \frac{\bar{\tau}(r_m + s_m\tau - 1) - r_m - s_m\tau + 1}{\tau\bar{\tau} - \tau - \bar{\tau} + 1} \\
&= \frac{(t - \tau)(r_m + s_m\tau - 1) - r_m - s_m\tau + 1}{2 - \tau - t + \tau + 1} \\
&= \frac{r_m t + s_m t\tau - t - r_m\tau - s_m t^2 + \tau - r_m - s_m\tau + 1}{3 - t} \\
&= \frac{r_m t + s_m t\tau - t - r_m\tau - s_m(t\tau - 2) + \tau - r_m - s_m\tau + 1}{3 - t} \\
&= \frac{1 - t - r_m + r_m t + 2s_m + (1 - r_m - s_m)\tau}{3 - t}.
\end{aligned}$$

Therefore, it is proven that

$$r = \frac{1 - t - r_m + r_m t + 2s_m}{3 - t},$$

and

$$s = \frac{1 - r_m - s_m}{3 - t},$$

for $m \geq 2$. □

Now, we proceed with the following algorithm in converting $\rho\frac{\tau^m-1}{\tau-1}$ to $r + s\tau$ by using the formula τ^m from Theorem 3.2. After that, Theorem 4.1 is applied for converting $\frac{\tau^m-1}{\tau-1}$ into $\rho_2+\rho_3\tau$. Finally, directly multiply ρ with $\rho_2 + \rho_3\tau$ in order to get $r + s\tau$ an element of $Z(\tau)$.

This Algorithm 4.1 is an important part before finding pseudoTNAF an integer n mod $\rho\frac{\tau^m-1}{\tau-1}$. The performance of running Algorithm 4.1 will be compared to the following algorithms. That is, Algorithms 4.2 and 4.3 using equations (1) and (2) respectively.

Algorithm 4.1

Input: $a \in \{0,1\}$, $m \geq 2$, nonzero integer ρ_0, ρ_1.
Output: $r + s\tau \in Z(\tau)$
Computation:
1. $t \leftarrow (-1)^{1-a}$;
2. $r_0 \leftarrow 1, s_0 \leftarrow 0, r_1 \leftarrow 0, s_1 \leftarrow 1$
3. $h_m \leftarrow \lfloor \frac{m}{2} \rfloor$
4. $g_m \leftarrow \lfloor \frac{m+1}{2} \rfloor$
5. $r_m \leftarrow \sum_{k=1}^{h_m} \frac{(-2)^k (m-1-k)!}{(k-1)!(m-2k)!} t^m$
6. $s_m \leftarrow \sum_{k=1}^{g_m} \frac{(-2)^{k-1} (m-k)!}{(k-1)!(m-2k+1)!} t^{m+1}$
7. $\rho_2 \leftarrow \frac{1-r_m+r_m t+2s_m-t}{3-t}$
8. $\rho_3 \leftarrow \frac{1-r_m-s_m}{3-t}$
9. $r \leftarrow \rho_0\rho_2 - 2\rho_1\rho_3$
10. $s \leftarrow \rho_1\rho_2 + \rho_0\rho_3 + \rho_1\rho_3 t$
11. Return (r, s)

Algorithm 4.2

Input: $a \in \{0,1\}$, $m \geq 2$, nonzero integer ρ_0, ρ_1
Output: $r + s\tau \in Z(\tau)$
Computation:
1. $t \leftarrow (-1)^{1-a}$
2. $U_0 \leftarrow 0, U_1 \leftarrow 1$,
3. For i from 2 to m do $U_i \leftarrow tU_{i-1} - 2U_{i-2}$
4. $\rho_2 \leftarrow -2(sum('U_i', 'i' = 2..m-2)) - 1$
5. $\rho_3 \leftarrow sum('U_i', 'i' = 2..m-1) + 1$
6. $r \leftarrow \rho_0\rho_2 - 2\rho_1\rho_3$
7. $s \leftarrow \rho_1\rho_2 + \rho_0\rho_3 + \rho_1\rho_3 t$
8. Return (r, s)

Algorithm 4.3

Input: $a \in \{0,1\}$, $m \geq 2$, nonzero integer ρ_0, ρ_1
Output: $r + s\tau \in Z(\tau)$
Computation:
1. $t \leftarrow (-1)^{1-a}$
2. $r_0 \leftarrow 1, s_0 \leftarrow 0, r_1 \leftarrow 0, s_1 \leftarrow 1$, $x_0 \leftarrow 0, y_0 \leftarrow 1$
3. For m from 1 to $m-1$ do
4. $\quad x_m \leftarrow x_{m-1} + y_{m-1}$
5. $\quad y_m \leftarrow -2x_{m-1}$
6. $\quad r_m \leftarrow y_m t^m$
7. $\quad s_m \leftarrow x_m t^{m+1}$
8. $\rho_2 \leftarrow add(r_m, m = 0..m-1)$
9. $\rho_3 \leftarrow add(s_m, m = 0..m-1)$;
10. $r \leftarrow \rho_0\rho_2 - 2\rho_1\rho_3$
11. $s \leftarrow \rho_1\rho_2 + \rho_0\rho_3 + \rho_1\rho_3 t$
12. Return (r, s)

Note that the performance of running process for Algorithm 4.1 is faster than the other version as shown in Table 3 and its graphical representation in Figure 4. That is, comparison of time and memory in average on standard Koblitz curves. We used a Maple programming with computer performance with Intel(R) Core(TM) i7 processor, 8 GB RAM and 64-bit operating system.

Table 3: Performance of converting $\rho\frac{\tau^m-1}{\tau-1}$ to $r+s\tau$.

	Algorithm 4.1	**Algorithm 4.2**	**Algorithm 4.3**
Curve	Time (s), Memory (bits)	Time (s), Memory (bits)	Time (s), Memory (bits)
K-163	0.0154, 3044914	0.0344, 3374718	0.0688, 4465634
K-233	0.0154, 4475665	0.0316, 3567508	0.0816, 4480097
K-283	0.0186, 4481532	0.022, 3561963	0.0874, 4020754
K-409	0.0192, 2471115	0.044, 2662914	0.1812, 2443794
K-571	0.0188, 4485270	0.0406, 2691790	0.2094, 4463296

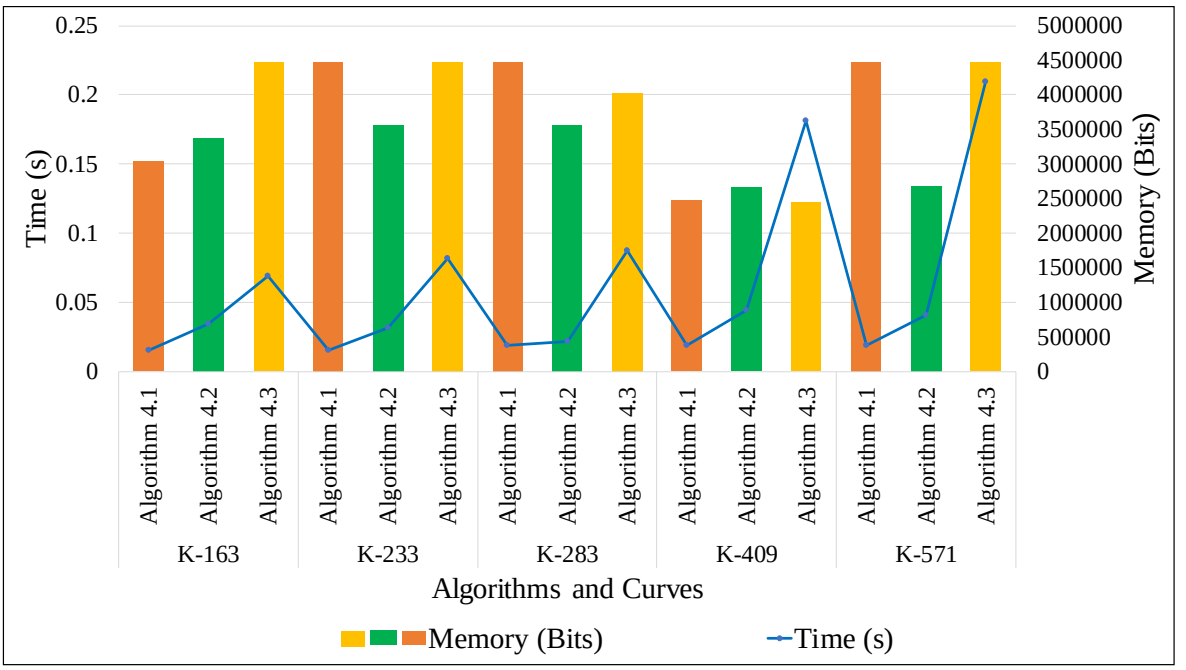

Figure 2: Graphical representation of Table 3.

Another advantage of using Algorithm 4.1 is the coefficients r and s either even or odd can be identified. This result is also an extension of study conducted by [17] in 2018 to solve the SM problem on the Koblitz curve. The following is an example of the impact of being able to identify the parity of r and s whether it will be an even or odd number by choosing some value of m, t, $\rho_0 = 1$ and $\rho_1 = 0$.

Example 4.1. *Suppose* $m = 163$, $t = -1$, $\rho_0 = 1$ *and* $\rho_1 = 0$. *We have*

$$r_{163} = -\sum_{i=1}^{81}(-2)^i\binom{162-i}{i-1} = 3334746503586958025881130$$

and

$$s_{163} = \sum_{i=1}^{82} (-2)^{i-1} \binom{163-i}{i-1} = 18240263746345052749579 43,$$

then by using Theorem 4.1, we obtain

$$r = \frac{1 - r_{163} + s_{163}}{2} = -75536006447622637546 1593,$$

and

$$s = \frac{1 - r_{163} - s_{163}}{4} = -12896932195555365825209768.$$

From the above value, we found that r and s are odd and even numbers, respectively. In fact, generally its already proven in [17], if ρ_0, m are odd and ρ_1 is even, then r and s are an odd and even numbers, respectively.

5 Conclusions and Future Work

In this study, a new finding of power of Frobenius endomorphism expression by using v-simplex and arithmetic sequence was introduced. With this approach, we enhance the performance of transformation process as required in pseudoTNAF's system before doing SM process.

This research can be extended by looking at the nature of ρ such that pseudoTNAF has low-density as suggested by previous researcher. Besides, the improvements of result from previous studies need to be done in deriving the TNAF formulas that has the least Hamming weight in its expansion. We also believe that the design of FPGA based Lucas sequence block can be improved.

Acknowledgement This work was supported by Universiti Putra Malaysia with Putra Grants GP / 2018/9595400 so that the study has a significant impact on the environment of ECC cryptography systems based on τ-adic non-adjacent.

Conflicts of Interest The authors declare no conflict of interest.

References

[1] N. A. Ali & F. Yunos (2016). Maximum and minimum norms for τ-NAF expansion on Koblitz curve. *Indian Journal of Science and Technology*, *9*(28), 1–8.

[2] B. B. Brumley & K. Järvinen (2007). Koblitz curves and integer equivalents of frobenius expansions. In C. Adams, A. Miri & M. Wiener (Eds.), *Selected Areas in Cryptography-SAC 2007*,. Springer, Berlin, Heidelberg.

[3] Cupillari & Antonella (1989). *The Nuts and Bolts of Proofs*. Wadsworth Publishing Company, Belmont, California.

[4] E. Deza & M. Deza (2012). Pentatope numbers and their multidimensional analogues. In *Figurate Numbers*, pp. 162. World Scientific Publishing, 5 Toh Tuck Link, Singapore.

[5] M. L. D'Ooge, F. E. Robbins & L. C. Karpinski (1926). Introduction to arithmetic. In U. of Michigan Studies: Humanistic Series 16 (Ed.), *Nicomachus of Gerasa*, pp. 247. Macmillan and Company, London, New York.

[6] J. Faulhaber (1631). *Academia Algebrae: Darinnen die miraculosische Inventiones zu den hochsten Cossen weiters continuirt und profitiert werden*. Johann Remelins, German.

[7] N. Gerasa (1938). *Introduction to Arithmetic*. Edward Brothers, London.

[8] N. H. Hadani, F. Yunos, M. R. K. Ariffin, S. H. Sapar & N. N. A. Rahman (2019). Alternative method to find the number of points on Koblitz curve. *Malaysian Journal of Mathematical Science*, *13*(S), 13–30.

[9] N. Koblitz (1987). Elliptic curve cryptosystem. *Mathematics Computation*, *48*(177), 203–209.

[10] N. Koblitz (1992). Cm curves with good cryptographic properties. In *Advances in cryptology CRYPTO 91: Proceedings 576*, pp. 279–287. Springer, Berlin, Heidelberg.

[11] S. A. Musa & G. Xu (2017). Fast scalar multiplication for elliptic curves over binary fields by efficiently computable formulas. pp. 206–226. Cham.

[12] J. A. Solinas (1997). An improved algorithm for arithmetic on a family of elliptic curves. In *Advance in Cryptology-CRYPTO'97*, pp. 357–371. Springer, Berlin, Heidelberg.

[13] J. A. Solinas (2000). Efficient arithmetic on Koblitz curves. *Design, Codes and Cryptography*, *19*, 195–249.

[14] M. Sullivan (2019). *Algebra and trigonometry*. Pearson, United States.

[15] S. Yasser, A. Hesham, M. Hassan & W. Alexan (2020). AES–secured bit–cycling steganography in sliced 3D images. *In International Conference on Innovative Trends in Communication and Computer Engineering (ITCE)*, pp. 227–231.

[16] F. Yunos, K. A. M. Atan, M. R. Md Said & M. R. K. Ariffin (2014). A reduced τ -NAF (RTNAF) representation for scalar multiplication on anomalous binary curves (ABC). *Pertanika Journal of Science and Technology*, *22*(2), 489–506.

[17] F. Yunos & S. Suberi (2018). Even and odd nature for pseudo τ-adic non-adjacent form. *Malaysian Journal of Science*, *37*, 94–102.

Appendix A

Example 5.1. *Find TNAF of* $1-4\tau$ *as follows.*
Consider $\overline{n}=1-4\tau$ *and* $\overline{\tau}=t-\tau$ *as conjugates of* τ*. Firstly, let* $t=1$ *then* $\tau\cdot\overline{\tau}=2$ *is shown :*

$$\tau\cdot\tau=-\tau^2+\tau=-\tau+2+\tau=2.$$

Followed by the next steps in obtaining TNAF$(1-4\tau)$ until we get the last remainder to be 0 when repeatedly dividing $1-4\tau$ by τ:
Step 1 : The result when $1-4\tau$ divide by τ is not in element of $Z(\tau)$:

$$\frac{1-4\tau}{\tau} = -4 + \frac{1}{\tau}\cdot\frac{\overline{\tau}}{\overline{\tau}} = -\frac{7}{2} - \frac{\tau}{2} \notin Z(\tau).$$

Therefore, we need to choose the first remainder to be either $c_0 = -1$ or $c_0 = +1$ so that $1-4\tau-c_0$ can be divided by τ :
If $c_0 = -1$ then

$$\frac{1-4\tau+1}{\tau} = -4 + \frac{2}{\tau}\cdot\frac{\overline{\tau}}{\overline{\tau}} = -3 - \tau \in Z(\tau),$$

or if $c_0 = 1$ then

$$\frac{1-4\tau+1}{\tau} = -4 \in Z(\tau). \tag{4}$$

Choose one of c_0 above so that the next division will be as follows.

$$\frac{-3-\tau}{\tau} = \frac{-3}{\tau}\cdot\frac{\overline{\tau}}{\overline{\tau}} - 1 = \frac{-5}{2} + \frac{3}{2}\tau \notin Z(\tau),$$

$$\text{or } \frac{-4}{\tau} = \frac{-4}{\tau}\cdot\frac{\overline{\tau}}{\overline{\tau}} = -2 + 2\tau \in Z(\tau), \tag{5}$$

produced an element of $Z(\tau)$. Thus, we prefer $c_0 = 1$ because of equation (4) and write

$$TNAF(1-4\tau) = [1, c_1, c_2, \ldots, c_{l-2}, c_{l-1}].$$

Next, we consider the second remainder $c_1 = 0$ because equation (5) and write

$$TNAF(1-4\tau) = [1, 0, c_2, \ldots, c_{l-2}, c_{l-1}].$$

Step 2 : The division $-2+2\tau$ by τ produced an element of $Z(\tau)$:

$$\frac{-2+2\tau}{\tau} = \frac{-2}{\tau}\cdot\frac{\overline{\tau}}{\overline{\tau}} + 2 = 1 + \tau \in Z(\tau).$$

Therefore, choose the third remainder $c_2 = 0$ and write

$$TNAF(1-4\tau) = [1, 0, 0, c_3, c_4, \ldots, c_{l-2}, c_{l-1}].$$

Step 3 : Since $1+\tau$ cannot be divided by τ then choose the fourth remainder $c_3 = \pm 1$ so that $1+\tau-c_3$ can be divided by τ :
If $c_3 = -1$ then

$$\frac{1+\tau+1}{\tau} = \frac{2}{\tau}\cdot\frac{\overline{\tau}}{\overline{\tau}} + 1 = 2 - \tau \in Z(\tau), \tag{6}$$

or if $c_3 = 1$ then

$$\frac{1+\tau-1}{\tau} = 1 \in Z(\tau).$$

Consider one of c_3 above so that the next division is

$$\frac{2-\tau}{\tau} = \frac{2}{\tau} - 1 = -\tau \in Z(\tau), \tag{7}$$

or

$$\frac{1}{\tau} = \frac{1}{\tau}\cdot\frac{\overline{\tau}}{\overline{\tau}} = \frac{1}{2} - \frac{\tau}{2} \notin Z(\tau),$$

produced an element of $Z(\tau)$. Therefore, we choose $c_3 = -1$ because of equation (6) and write

$$TNAF(1-4\tau) = [1, 0, 0, -1, c_4, \ldots, c_{l-2}, c_{l-1}].$$

After that, the fifth remainder, $c_4 = 0$ because of equation (7) and write

$$TNAF(1-4\tau) = [1, 0, 0, -1, 0, c_5, \ldots, c_{l-2}, c_{l-1}].$$

Step 4 : Since $-\tau$ can be divided by τ :

$$\frac{-\tau}{\tau} = \frac{-\tau}{\tau} \cdot \frac{\overline{\tau}}{\overline{\tau}} = -1,$$

Then the sixth remainder is $c_5 = 0$ and write

$$TNAF(1-4\tau) = [1, 0, 0, -1, 0, 0, c_6, \ldots, c_{l-2}, c_{l-1}].$$

Step 5 : Since -1 cannot be divided by τ then $c_6 = -1$:

$$\frac{-1+1}{\tau} = 0.$$

Therefore, we have to choose either $c_6 = -1$ or $c_6 = 1$ so that $-1 - c_0$ can be divided by τ :
If $c_6 = -1$ then $\frac{-1+1}{\tau} = 0$ or if $c_6 = 1$ then

$$\frac{-1-1}{\tau} = \frac{2}{\tau} \cdot \frac{\overline{\tau}}{\overline{\tau}} = -1 + \tau.$$

We choose $c_6 = -1$ since the divisions $-1 - c_0$ by τ results in 0 and is written as $TNAF(1-4\tau) = [1, 0, 0, -1, 0, 0, -1] = 1 - \tau^3 - \tau^6$. It has seven digits and it Hamming's weight is three.