Malaysian Journal of Mathematical Sciences 13(S) August: 13–30 (2019)
Special Issue: The 6th International Cryptology and Information Security Conference (CRYPTOLOGY2018)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

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

Alternative Method to Find the Number of Points on Koblitz Curve

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

[1] *Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia*
[2] *Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, Malaysia*
[3] *Pusat Teknologi Pintar UKM-MTDC, Kolej PERMATApintar Negara, Malaysia*

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

ABSTRACT

A Koblitz curve E_a is defined over field F_{2^m}. Let $\tau = \frac{(-1)^{1-a}+\sqrt{-7}}{2}$ where $a \in \{0,1\}$ denotes the Frobenius endomorphism from the set $E(F_{2^m})$ to itself. It can be used to improve the performance of computing scalar multiplication on Koblitz Curves. In this paper, another version of formula for $\tau^m = r_m + s_m\tau$ where r_m and s_m are integers is introduced. Through this approach, we discover an alternative method to find the number of points through the curve E_a.

Keywords: Koblitz curve, scalar multiplication, Frobenius endomorphism, elliptic curve cryptosystem, number of points.

1. Introduction

Elliptic Curve Cryptography (ECC) was discovered by (Koblitz, 1987). Elliptic curve based schemes have scalar multiplication (SM) as the dominant operation on it. Let P and Q be the point on Koblitz Curve. SM is the repeated addition of a point along the curve up to n times and denoted as $nP = P + P + \cdots + P$ for some scalar n such that $nP = Q$. Frobenius endomorphism can be used to improve the performance of computing SM on Koblitz curves. Koblitz curves are defined over F_2 as follows:

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

where $a \in \{0, 1\}$ as suggested by (Koblitz, 1992). The Frobenius map $\tau : E_a(F_{2^m}) \to E_a(F_{2^m})$ for a point $P = (x, y)$ on $E_a(F_{2^m})$ is defined by $\tau(x, y) = (x^2, y^2), \tau(\infty) = \infty$ where ∞ is the point at infinity. It stands that $(\tau^2 + 2)P = t\tau(P)$ for all $P \in E_a(F_{2^m})$ and the trace of Frobenius map is $t = (-1)^{1-a}$. The τ-NAF proposed by (Solinas, 2000) is one of the most efficient algorithm to compute SM on Koblitz curves.

To proceed the discussion of this paper, the following definitions that can be found in (Ali et al., 2017), (Hankerson et al., 2006), (Hazewinkel, 1994), (Koblitz, 1987), (Solinas, 1997), (Suberi et al., 2016), (Yunos et al., 2015a), (Yunos et al., 2014b), (Yunos et al., 2015b) and Hadani and Yunos (2018) will be applied.

Definition 1.1. *An element of the ring $Z(\tau)$ is defined as $r+s\tau$ where $r, s \in Z$.*

Definition 1.2. *A τ-adic Non-Adjacent Form (TNAF) of nonzero $\bar{n}$ of an element of $Z(\tau)$ is defined as $\tau NAF(\bar{n}) = \sum_{i=0}^{l-1} c_i\tau^i$ where l is the length of the expansion $\tau NAF(\bar{n}), c_i \in \{-1, 0, 1\}, c_{l-1} \neq 0$ and $c_ic_{i+1} = 0$.*

Definition 1.3. *A Reduced τ-adic Non-Adjacent Form (RTNAF) of nonzero $\bar{n}$ of an element of $Z(\tau)$ is defined as $RTNAF(\bar{n}) = \sum_{i-0}^{l-1} c_i\tau^i$ in modulo $\frac{\tau^m-1}{\tau-1}$ where l is the length of the expansion $RTNAF(\bar{n}), c_i \in \{-1, 0, 1\}, c_{l-1} \neq 0$ and $c_ic_{i+1} = 0$.*

The detail example on finding the TNAF and RTNAF can be refer to (Yunos and Suberi, 2018) and (Suberi et al., 2018).

Definition 1.4. *Let $N : Q(\tau) \to Q$ the rational set as a function of norm. Let $\alpha = r + st$ an element $Q(\tau)$. The norm of α is defined as $N(\alpha) = r^2 + trs + 2s^2$ where $t = (-1)^{(1-a)}$ for $a \in \{0, 1\}$.*

Definition 1.5. *Lucas sequence is a sequence of integers that can be used in calculation of irrational quadratic numbers. Lucas sequence, U_i and V_i are defined as follows;*

$$\begin{aligned} U_0 &= 0, U_1 = 1 \text{ and } U_\kappa = tU_{\kappa-1} - 2U_{\kappa-2} \\ &\quad \text{for } \kappa \geq 2; \\ V_0 &= 2, V_1 = t \text{ and } V_\kappa = tV_{\kappa-1} - 2V_{\kappa-2} \\ &\quad \text{for } \kappa \geq 2; \end{aligned}$$

Theorem 1.1 from (Yunos et al., 2014a) shown below will be applied in the discussion of this paper.

Theorem 1.1. *If $a_0 = 0, b_0 = 1, a_m = a_{m-1} + b_{m-1}$ and $b_m = -2a_{m-1}$, then $\tau^m = b_m t^m + a_m t^{m+1}\tau$ for $m > 0$.*

(Solinas, 2000) generated the formula for $\tau^m = U_m\tau - 2U_{m-1}$ that to be is used to find TNAF($\bar{n}$)mod $(\tau^m - 1)$. (Yunos et al., 2014a) produced Theorem 1.1 as an alternative version for the formula τ^m. That is, if $x_0 = 0, y_0 = 1, x_m = x_{m-1} + y_{m-1}$ and $y_m = -2x_{m-1}$, then $\tau^m = y_m t^m + x_m t^{m+1}\tau$ for $m > 0$. As a result, the process to convert the expansion of TNAF$\left(\sum_{m=0}^{l-1} c_m\tau^m\right)$ into an element of $Z(\tau)$ became easier. Both τ^m formulas that were produced by (Solinas, 2000) and (Yunos et al., 2014a) can be used to calculate the number of points on the curve E_a. The formulas are as follows ;

$$\begin{aligned} \#E_a(F_{2^m}) &= p \cdot \#E_a(F_2) \\ &\quad \text{where } p > 2 \text{ is a prime }, \\ \#E_a(F_{2^m}) &= 2^m + 1 - V_m, \\ \#E_a(F_{2^m}) &= N(\tau^m - 1), \\ \#E_a(F_{2^m}) &= \#E_a(F_{2^m}) \cdot N\left(\frac{\tau^m - 1}{\tau - 1}\right) \\ &\quad \text{where } |P| = N\left(\frac{\tau^m - 1}{\tau - 1}\right), \\ \#E_a(F_{2^m}) &= b_m^2 + 2a_m^2 + a_m b_m + 1 \\ &\quad -(2b_m + a_m)t^m. \end{aligned} \tag{1}$$

Formula $N(\sum_{m=0}^{l-1} c_m\tau^m) = r^2 + trs + 2s^2$ where $r = \sum_{m=0}^{l-1} c_m b_m t^m$ and $s = \sum_{m=0}^{l-1} c_m a_m t^{m+1}$ was applied by (Ali and Yunos, 2016) to find maximum and minimum norms.

In this paper, our approach is to introduce a_{i_m} for $2 \leq i \leq \frac{m+1}{2}$. Subsequently, alternative formula for τ^m is proposed. As a result, by using the new τ^m, we find the number of points that passes through the curve E_a.

In the next section, we introduced alternative form of τ^m by proving the Propositions 2.1 and 2.2 hence provide alternative version differ from τ^m that was introduced by (Solinas, 2000) and (Yunos et al., 2014a).

2. Alternative formula for τ^m

We begin with the identity of $\tau^2 = t\tau - 2$. We expand τ for $m \in Z^+$ in form of $r_m + s_m\tau$. For example, for $m = 1$ and $m = 2$, we obtain $\tau^1 = 0 + 1\tau$ and $\tau^2 = -2 + t\tau$ respectively. We input the data onto Table 1 for value of r_m and s_m for $m \in \{1, 2, 3, \ldots, 12\}$ using the method of expansion of τ identity.

Table 1: All r_m and s_m of τ^m for $1 \leq m \leq 12$

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	$-2t^{10} + 36t^8 - 224t^6 + 560t^4 - 480t^2$ $+64$	$t^{11} - 20t^9 + 144t^7 - 448t^5 + 560t^3$ $-192t$

Definition 2.1 was introduced through this table.

Definition 2.1.
Given $\tau^m = r_m + s_m\tau$ is an element of $\mathbb{Z}(\tau)$ for any positive integer m. Let $a_{1_m} = 1$. We define a_{i_m} is the coefficient in s_m expansion for $i \in \{1, ..., \lfloor\frac{m-1}{2}\rfloor\}$.

Next, we start with the generation of Table 2. By using Definition 2.1 and

Table 1, we disintegrate the s_m of τ^m for $1 \leq m \leq 12$ as given in the following table.

Table 2: s_m of τ^m for $1 \leq m \leq 12$

m	$s_m = \sum_{i=1}^{m} a_{i_m} t^{m-2i+1}$					
	$a_{1_m} t^{m-1}$	$a_{2_m} t^{m-3}$	$a_{3_m} t^{m-5}$	$a_{4_m} t^{m-7}$	$a_{5_m} t^{m-9}$	$a_{6_m} t^{m-11}$
1	1					
2	1					
3	1	-2				
4	1	$-4t$				
5	1	$-6t^2$	4			
6	1	$-8t^3$	$12t$			
7	1	$-10t^4$	$24t^2$	-8		
8	1	$-12t^5$	$40t^3$	$-32t$		
9	1	$-14t^6$	$60t^4$	$-80t^2$	16	
10	1	$-16t^7$	$84t^5$	$-160t^3$	$80t$	
11	1	$-18t^8$	$112t^6$	$-280t^4$	$240t^2$	-32
12	1	$-20t^9$	$144t^7$	$-448t^5$	$560t^3$	$-192t$

From Table 2, we can observed the pattern of a_{2_m} for $1 \leq m \leq 12$ to obtain the general form of s_m. We found that the sequence of $\{a_{2_m}\}_{m=3}^{m=12} = \{-2, -4, -6, -8, -10, -12, -14, -16, -18, -20\}$ can be written in the form of $\{(-1)^{2-1} \frac{2}{(2-1)!} (3-2), (-1)^{2-1} \frac{2}{(2-1)!} (4-2), (-1)^{2-1} \frac{2}{(2-1)!} (5-2), \ldots, (-1)^{2-1} \frac{2}{(2-1)!} (12-2)\}$ that is $a_{2_m} = (-1)^{2-1} \frac{2}{(2-1)!} \prod_{j=2}^{2(2)-2} (m-j)$. We obtained the following conjecture from this pattern.

Conjecture 2.1. *Sequence* $\{a_{2_m}\}_{m=3}^{m=\infty} = \{-2, -4, -6, -8, -10, \ldots\}$ *has a general formula of* $a_{2_m} = a_{2_{m-1}} - 2$.

Followed by the following result for the purpose to proof argument in Lemma 2.2.

Lemma 2.1. *If* $a_{2_m} = a_{2_{m-1}} - 2$*, then the coefficient*

$$a_{2_m} = -2(m-2)$$

for any integer $m \geq 3$.

Proof. The proof of this lemma can be found in Hadani and Yunos (2018). □

Now, we observe the sequence of $\{a_{3_m}\}_{m=3}^{m=12} = \{4, 12, 24, 40, 60, 84, 112, 144\}$. We identified that this sequence can be written in the form of $\{(-1)^{3-1}\frac{2^{3-1}}{(3-1)!}(5-3)\ (5-4)\ ,\ (-1)^{3-1}\ \frac{2^{3-1}}{(3-1)!}\ (6-3)\ (6-4)\ ,\ (-1)^{3-1}\frac{2^{3-1}}{(3-1)!}(7-3)(7-4), \ldots, (-1)^{3-1}\frac{2^{3-1}}{(3-1)!}(12-3)(12-4)\}$ that is $a_{3_m} = (-1)^{3-1}\frac{2^{3-1}}{(3-1)!}\prod_{j=3}^{2(3)-2}(m-j)$. From the pattern of the sequence that we obtained, we can conclude the general form of a_{i_m} as in the following Lemma.

Lemma 2.2. If $a_{1_m} = 1$ then coefficient in s_m expansion is

$$a_{i_m} = (-1)^{i-1}\frac{2^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j)$$

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

Proof.

We prove by using mathematical induction as follows.
For $i = 2$, then

$$\begin{aligned} a_{2_m} &= -2(m-2) \text{ from Lemma 2.1} \\ &= (-1)^{2-1}\frac{2^{2-1}}{(2-1)!}\prod_{j=2}^{2(2)-2}(m-j) \text{ is true.} \end{aligned}$$

Assume that $i = k$, then $a_{k_m} = (-1)^{k-1}\frac{2^{k-1}}{(k-1)!}\prod_{j=k}^{2k-2}(m-j)$ is true for $2 \leq k \leq \frac{m+1}{2}$.

Now, let $i = k + 1$,

$$
\begin{aligned}
a_{k+1_m} &= a_{k_m}\Big((-1)\frac{2}{k}\frac{(m-2k+1)(m-2k)}{m-k}\Big) \\
&= \Big((-1)^{k-1}\frac{2^{k-1}}{(k-1)!}\prod_{j=k}^{2k-2}(m-j)\Big) \\
&\quad \Big((-1)\frac{2}{k}\frac{(m-2k+1)(m-2k)}{m-k}\Big) \\
&= \Big((-1)^{k-1}\frac{2^{k-1}}{(k-1)!}(m-k)(m-(k+1)) \\
&\quad (m-(k+2))\cdots(m-(2k-2))\Big) \\
&\quad \Big((-1)\frac{2}{k}\frac{(m-2k+1)(m-2k)}{m-k}\Big) \\
&= \big((-1)^{k+1-1}\big)\frac{2^{k+1-1}}{(k+1-1)!}\big((m-(k+1)) \\
&\quad (m-(k+2))\cdots(m-(2k-2))\cdot \\
&\quad (m-(2k-1))(m-(2(k+1)-2))\big)
\end{aligned}
$$

$$
= (-1)^{k+1-1}\frac{2^{k+1-1}}{(k+1-1)!}\prod_{j=k+1}^{2(k+1)-2}(m-j)
$$

Subsequently it is true for all integers $i \in N$.■

Below is the propositions of s_m and r_m from $\tau^m = r_m + s_m\tau$ which used Lemma 2.2 to assist the proving of the proposition. These propositions will bring out another version for the expansion of τ^m.

Proposition 2.1.
Given $\tau^m = r_m + s_m\tau$ is an element of $\mathbb{Z}(\tau)$ for any positive integer m. Let $s_1 = 1$ and $s_2 = t$. If a_{i_m} from Lemma 2.2, then the coefficient s_m can be written as

$$
s_m = \sum_{i=1}^{\lfloor \frac{m+1}{2} \rfloor} a_{i_m} t^{m-2i+1} \tag{2}
$$

where $a_{1_m} = 1$ and $m \geq 3$.

Proof. By mathematical induction we have the following
If $m = 3$, then from Table 2, we obtain

$$\begin{aligned}
s_3 &= t^2 - st \\
&= 1t^2 + (-1)^{2-1}\frac{2^{2-1}}{(2-1)!}(3-2)t^2 \\
&= 1t^2 + (-1)^{2-1}\frac{2^{2-1}}{(2-1)!}\prod_{j=2}^{2(2)-2}(3-j)t^2 \\
&= a_{1_3}t^2 + a_{2_3}t \\
&= a_{1_3}t^{3-2(1)+1} + a_{2_3}t^{3-2(2)+1} \\
&= \sum_{i=1}^{\lfloor\frac{3+1}{2}\rfloor} a_{i_3}t^{3-2i+1}.
\end{aligned}$$

The hypothesis (2) is true for $m = 3$.
Assume that if $m = k$, then

$$s_k = \sum_{i=1}^{\lfloor\frac{k+1}{2}\rfloor} a_{i_k}t^{k-2i+1} \text{ where } a_{1_k} = 1 \text{ and } k \geq 3 \text{ is true.}$$

Now, if $m = k + 1$, we can separate the proof into two different cases. That is for k is an odd number (O) and k is an even number (E) as follows.

For $k \in O$,

$$
\begin{aligned}
s_{k+1} &= t \sum_{i=1}^{\lfloor \frac{k+1}{2} \rfloor} a_{i_k} \frac{k+1-i}{k-2i+2} t^{k-2i+1} \\
&= t\Bigg(a_{1_k} t^{k-1} + a_{2_k} \frac{k-1}{k-2} t^{k-3} + a_{3_k} \frac{k-2}{k-4} t^{k-5} + \cdots + \\
&\quad a_{\lfloor \frac{k+1}{2} \rfloor_k} \frac{k+1-\lfloor \frac{k+1}{2} \rfloor}{k-2\lfloor \frac{k+1}{2} \rfloor + 2} t^{k-2\lfloor \frac{k+1}{2} \rfloor + 1} \Bigg) \\
&= a_{1_k} t^{k} + a_{2_k} \frac{k-1}{k-2} t^{k-2} + a_{3_k} \frac{k-2}{k-4} t^{k-4} + \cdots + \\
&\quad a_{\lfloor \frac{k+1}{2} \rfloor_k} \frac{k+1-\lfloor \frac{k+1}{2} \rfloor}{k-2\lfloor \frac{k+1}{2} \rfloor + 2} t^{k-2\lfloor \frac{k+1}{2} \rfloor + 2}
\end{aligned}
$$

By using a_{i_k} from Lemma 2.2 and since $\lfloor \dfrac{k+1}{2} \rfloor = \lfloor \dfrac{k+2}{2} \rfloor$ when $k \in O$, we have the following.

$$
\begin{aligned}
s_{k+1} &= 1t^{k} + (-1)^{2-1} \frac{2^{2-1}}{(2-1)!} \cancel{(k-2)} \left(\frac{k-1}{\cancel{k-2}} \right) t^{k-2} + \\
&\quad (-1)^{3-1} \frac{2^{3-1}}{(3-1)!} (k-3) \cancel{(k-4)} \left(\frac{k-2}{\cancel{k-4}} \right) t^{k-5} + \cdots + \\
&\quad (-1)^{\lfloor \frac{k+1}{2} \rfloor - 1} \frac{2^{\lfloor \frac{k+1}{2} \rfloor - 1}}{(\lfloor \frac{k+1}{2} \rfloor - 1)!} (k - \lfloor \frac{k+1}{2} \rfloor)(k - \lfloor \frac{k+1}{2} \rfloor - 1) \cdots (k - 2\lfloor \frac{k+2}{2} \rfloor + 3) \\
&\quad \cancel{(k - 2\lfloor \frac{k+2}{2} \rfloor + 2)} \left(\frac{k+1-\lfloor \frac{k+1}{2} \rfloor}{\cancel{k - 2(\lfloor \frac{k+2}{2} \rfloor + 2}} \right) t^{k+2-2\lfloor \frac{k+1}{2} \rfloor}, \\
&= 1t^{k-2(1)+2} + (-1)^{2-1} \frac{2^{2-1}}{(2-1)!} (k+1-2) t^{k-2(2)+2} + \\
&\quad (-1)^{3-1} \frac{2^{3-1}}{(3-1)!} (k+1-3)(k+1-4) t^{k-2(3)+2} + \cdots + \\
&\quad (-1)^{\lfloor \frac{k+1+1}{2} \rfloor - 1} \frac{2^{\lfloor \frac{k+1+1}{2} \rfloor - 1}}{(\lfloor \frac{k+1+1}{2} \rfloor - 1)!} (k+1 - \lfloor \frac{k+1+1}{2} \rfloor)(k - \lfloor \frac{k+1+1}{2} \rfloor) \\
&\quad (k - \lfloor \frac{k+1+1}{2} \rfloor - 1) \cdots (k+1 - 2(\lfloor \frac{k+1+1}{2})\rfloor + 2) t^{k-2\lfloor \frac{k+1+1}{2} \rfloor + 2}
\end{aligned}
$$

$$\begin{aligned}
&= a_{1_{k+1}} t^{k+1-1} + a_{2_{k+1}} t^{k+1-3} + a_{3_{k+1}} t^{k+1-5} + \cdots + \\
&\quad a_{\lfloor \frac{k+1+1}{2} \rfloor_{k+1}} t^{k+1-2(\lfloor \frac{k+1+1}{2} \rfloor)+1} \\
&= \sum_{i=1}^{\lfloor \frac{k+1+1}{2} \rfloor} a_{i_{k+1}} t^{k+1-2i+1}
\end{aligned}$$

Therefore, the hypothesis (2) is also true for $m = k+1$ where k is an odd number.
Now, we consider if k is even. That is, for $k \in E$,

$$\begin{aligned}
s_{k+1} &= t \sum_{i=1}^{\lfloor \frac{k+1}{2} \rfloor} a_{i_k} \frac{k+1-i}{k-2i+2} t^{k-2i+1} + a_{\lfloor \frac{k+2}{2} \rfloor_{k+1}} t^{k-2\lfloor \frac{k+2}{2} \rfloor + 2} \\
&= \Bigg(a_{1_k} t^k + a_{2_k} \frac{k-1}{k-2} t^{k-2} + a_{3_k} \frac{k-2}{k-4} t^{k-4} + \cdots + \\
&\quad a_{\lfloor \frac{k+1}{2} \rfloor_k} \frac{k+1-\lfloor \frac{k+1}{2} \rfloor}{k-2\lfloor \frac{k+1}{2} \rfloor + 2} t^{k-2\lfloor \frac{k+1}{2} \rfloor + 2} \Bigg) + a_{\lfloor \frac{k+2}{2} \rfloor_{k+1}} t^{k-2\lfloor \frac{k+2}{2} \rfloor + 2}
\end{aligned}$$

By using a_{i_k} from Lemma 2.2, we have the following

$$\begin{aligned}
&= \Bigg(1t^k + (-1)^{2-1} \frac{2^{2-1}}{(2-1)!} \cancel{(k-2)} \Big(\frac{k-1}{\cancel{k-2}} \Big) t^{k-2} + \\
&\quad (-1)^{3-1} \frac{2^{3-1}}{(3-1)!} (k-3) \cancel{(k-4)} \Big(\frac{k-2}{\cancel{k-4}} \Big) t^{k-5} + \cdots + \\
&\quad (-1)^{\lfloor \frac{k+1}{2} \rfloor - 1} \frac{2^{\lfloor \frac{k+1}{2} \rfloor - 1}}{(\lfloor \frac{k+1}{2} \rfloor - 1)!} (k - \lfloor \frac{k+1}{2} \rfloor)(k - \lfloor \frac{k+1}{2} \rfloor - 1) \cdots \\
&\quad \cancel{(k - 2\lfloor \frac{k+2}{2} \rfloor} + 2) \Big(\frac{k+1-\lfloor \frac{k+1}{2} \rfloor}{\cancel{k-2(\lfloor \frac{k+2}{2} \rfloor}+2} \Big) t^{k+2-2\lfloor \frac{k+1}{2} \rfloor} \Bigg) \\
&\quad + (-1)^{\lfloor \frac{k+2}{2} \rfloor - 1} \frac{2^{\lfloor \frac{k+2}{2} \rfloor - 1}}{(\lfloor \frac{k+2}{2} \rfloor - 1)!} (k+1-\lfloor \frac{k+2}{2} \rfloor)(k - \lfloor \frac{k+1}{2} \rfloor) \cdots \\
&\quad (k - 2\lfloor \frac{k+2}{2} \rfloor + 2)
\end{aligned}$$

$$\begin{aligned}
&= 1t^k + (-1)^{2-1}\frac{2^{2-1}}{(2-1)!}(k-1)t^{k-2} + (-1)^{3-1}\frac{2^{3-1}}{(3-1)!}(k-2)(k-3)t^{k-5} \\
&\quad + \cdots + (-1)^{\lfloor \frac{k+1}{2} \rfloor -1}\frac{2^{\lfloor \frac{k+1}{2} \rfloor -1}}{(\lfloor \frac{k+1}{2} \rfloor -1)!}(k+1-\lfloor \frac{k+1}{2} \rfloor)(k-\lfloor \frac{k+1}{2} \rfloor) \\
&\quad (k-\lfloor \frac{k+1}{2} \rfloor -1)\cdots(k+1-2(\lfloor \frac{k+1}{2})\rfloor)t^{k+2-2\lfloor \frac{k+1}{2} \rfloor} \\
&\quad +(-1)^{\lfloor \frac{k+2}{2} \rfloor -1}\frac{2^{\lfloor \frac{k+2}{2} \rfloor -1}}{(\lfloor \frac{k+2}{2} \rfloor -1)!}(k+1-\lfloor \frac{k+2}{2} \rfloor)(k-\lfloor \frac{k+1}{2} \rfloor)\cdots \\
&\quad (k-2\lfloor \frac{k+2}{2} \rfloor +2)
\end{aligned}$$

$$\begin{aligned}
&= 1t^{k-2(1)+2} + (-1)^{2-1}\frac{2^{2-1}}{(2-1)!}(k+1-2)t^{k-2(2)+2} + \\
&\quad (-1)^{3-1}\frac{2^{3-1}}{(3-1)!}(k+1-3)(k+1-4)t^{k-2(3)+2} + \cdots + \\
&\quad (-1)^{\lfloor \frac{k+1+1}{2} \rfloor -1}\frac{2^{\lfloor \frac{k+1+1}{2} \rfloor -1}}{(\lfloor \frac{k+1+1}{2} \rfloor -1)!}(k+1-\lfloor \frac{k+1+1}{2} \rfloor)(k-\lfloor \frac{k+1+1}{2} \rfloor) \\
&\quad (k-\lfloor \frac{k+1+1}{2} \rfloor -1)\cdots(k+1-2(\lfloor \frac{k+1+1}{2})\rfloor +2)t^{k-2\lfloor \frac{k+1+1}{2} \rfloor +2} \\
&= a_{1_{k+1}}t^{k+1-1} + a_{2_{k+1}}t^{k+1-3} + a_{3_{k+1}}t^{k+1-5} + \cdots + \\
&\quad a_{\lfloor \frac{k+1+1}{2} \rfloor_{k+1}}t^{k+1-2\lfloor \frac{k+1+1}{2} \rfloor +1} \\
&= \sum_{i=1}^{\lfloor \frac{k+1+1}{2} \rfloor} a_{i_{k+1}}t^{k+1-2i+1}.
\end{aligned}$$

□

Proposition 2.1 is important as it will aid the proving of next proposition for r_m in $\tau^m = r_m + s_m t$.

Next, we will show the proving of proposition for r_m given $\tau^m = r_m + s_m\tau$.

Proposition 2.2.
If s_m from Proposition 2.1, then the coefficient r_m can be written as

$$r_m = -2s_{m-1} \tag{3}$$

where $a_{1_m} = 1$ *and* $m \geq 3$.

Proof. By mathematical induction we have the following.
If $m = 3$, then from Table 2, we obtain

$$\begin{aligned} r_3 &= -2t \\ &= -2a_{1_2}t \\ &= -2s_2. \end{aligned}$$

The hypothesis (3) is true for $m = 3$.
Assume that if $m = k$, then

$$\begin{aligned} r_k &= -2s_{k-1} \text{ is true for } k-2i+1 \leq 0 \\ &= -2\sum_{i=1}^{\lfloor \frac{k}{2} \rfloor} a_{i_{k-1}} t^{k-2i} \end{aligned}$$

is true for $k \geq 3$.
Now, if $m = k+1$, we can separate the proof into two different cases. That is for k is an even number (E) and k is an odd number (O) as follows.
For $k \in E$,

$$\begin{aligned} r_{k+1} &= -2t\sum_{i=1}^{\lfloor \frac{k}{2} \rfloor} a_{i_{k-1}} \frac{k-i}{k-2i+1} t^{k-2i} \\ &= -2t\Bigg(a_{1_{k-1}} t^{k-2(1)} + a_{2_{k-1}} \frac{k-2}{k-2(2)+1} t^{k-2(2)} + \\ & \quad a_{3_{k-1}} \frac{k-3}{k-2(3)+1} t^{k-2(3)} + \cdots + a_{\lfloor \frac{k}{2} \rfloor_{k-1}} \frac{k-\lfloor \frac{k}{2} \rfloor}{k-2\lfloor \frac{k}{2} \rfloor + 1} t^{k-2\lfloor \frac{k}{2} \rfloor} \Bigg) \\ & \quad \text{By using } a_{i_k} \text{ from Lemma 2.2 and since } \lfloor \frac{k}{2} \rfloor = \lfloor \frac{k+1}{2} \rfloor \\ & \quad \text{when } k \in E, \text{ we have the following.} \\ r_{k+1} &= -2\Bigg(1t^{k-1} + (-1)^{2-1} \frac{2^{2-1}}{(2-1)!}(k-2)t^{k-3} + \\ & \quad (-1)^{3-1} \frac{2^{3-1}}{(3-1)!}(k-3)(k-1-3)t^{k-5} + \cdots + \\ & \quad (-1)^{\lfloor \frac{k+1}{2} \rfloor - 1} \frac{2^{\lfloor \frac{k+1}{2} \rfloor - 1}}{(\lfloor \frac{k+1}{2} \rfloor - 1)!}(k - \lfloor \frac{k+1}{2} \rfloor)(k-1-\lfloor \frac{k+1}{2} \rfloor)(k-2-\lfloor \frac{k+1}{2} \rfloor)\cdots \\ & \quad (k-2\lfloor \frac{k+1}{2} \rfloor)t^{k-2\lfloor \frac{k+1}{2} \rfloor + 1} \Bigg) \end{aligned}$$

$$
\begin{aligned}
&= -2\left(a_{1_k}t^{k-1} + a_{2_k}t^{k-3} + a_{3_k}t^{k-5} + \cdots + a_{\lfloor \frac{k+1}{2} \rfloor_k} t^{k+1-2\lfloor \frac{k+1}{2} \rfloor}\right) \\
&= -2\sum_{i=1}^{\lfloor \frac{k+1}{2} \rfloor} a_{i_{k+1-1}} t^{k+1-2i} \\
&= -2s_{k+1-1}.
\end{aligned}
$$

Therefore, the hypothesis (3) is also true for $m = k+1$ where k is an even number.

Now, we consider if k is odd. That is, for $k \in O$,

$$
\begin{aligned}
r_{k+1} &= -2\left(t\sum_{i=1}^{\lfloor \frac{k}{2} \rfloor} a_{i_{k-1}} \frac{k-i}{k-2i+1} t^{k-2i} + a_{\lfloor \frac{k+1}{2} \rfloor_k} t^{k+1-2\lfloor \frac{k+1}{2} \rfloor}\right) \\
&= -2\Bigg(1t^{k-1} + (-1)^{2-1}\frac{2^{2-1}}{(2-1)!}(k-2)t^{k-3} + \\
&\quad (-1)^{3-1}\frac{2^{3-1}}{(3-1)!}(k-3)(k-1-3)t^{k-5} + \cdots + \\
&\quad (-1)^{\lfloor \frac{k}{2} \rfloor - 1}\frac{2^{\lfloor \frac{k}{2} \rfloor - 1}}{(\lfloor \frac{k}{2} \rfloor - 1)!}(k - \lfloor \frac{k}{2} \rfloor)(k-1-\lfloor \frac{k}{2} \rfloor)(k-2-\lfloor \frac{k}{2} \rfloor)\cdots \\
&\quad (k - 2\lfloor \frac{k}{2} \rfloor)t^{k-2\lfloor \frac{k}{2} \rfloor + 1} + (-1)^{\lfloor \frac{k+1}{2} \rfloor - 1}\frac{2^{\lfloor \frac{k+1}{2} \rfloor - 1}}{(\lfloor \frac{k+1}{2} \rfloor - 1)!}\cdot \\
&\quad (k - \lfloor \frac{k+1}{2} \rfloor)(k-1-\lfloor \frac{k+1}{2} \rfloor)\cdots \\
&\quad (k - 2\lfloor \frac{k+1}{2} \rfloor)t^{k-2\lfloor \frac{k+1}{2} \rfloor + 1}\Bigg) \\
&= -2\Bigg(a_{1_k}t^{k-1} + a_{2_k}t^{k-3} + a_{3_k}t^{k-5} + \cdots + \\
&\quad a_{\lfloor \frac{k}{2} \rfloor_k} t^{k-2\lfloor \frac{k}{2} \rfloor + 1} + a_{\lfloor \frac{k+1}{2} \rfloor_k} t^{k-2\lfloor \frac{k+1}{2} \rfloor + 1}\Bigg) \\
&= -2\sum_{i=1}^{\lfloor \frac{k+1}{2} \rfloor} a_{i_{k+1-1}} t^{k+1-2i} \\
&= -2s_{k+1-1}
\end{aligned}
$$

□

Proved Propositions 2.1 and 2.2 therefore resulted in the introduction of Theorem 2.1 as a new version for the expansion of τ^m.

Theorem 2.1. Let $a_{1_m} = 1$, then

$$\begin{aligned}\tau^m &= -2\left(t^{m-2} + \sum_{i=1}^{\lfloor \frac{m}{2} \rfloor}(-1)^{i-1}\frac{2^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-1-j)t^{m-2i}\right) \\ &\quad + \left(t^{m-1} + \sum_{i=1}^{\lfloor \frac{m+1}{2} \rfloor}(-1)^{i-1}\frac{2^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j)t^{m-2i+1}\right)\tau\end{aligned}$$

Proof. We have

$$\begin{aligned}\tau^m &= r_m + s_m\tau \\ &= -2s_{m-1} + s_m\tau \quad \text{from Proposition 2.2} \\ &= -2\sum_{i=1}^{\lfloor \frac{m}{2} \rfloor} a_{i_{m-1}}t^{m-2i} + \sum_{i=1}^{\lfloor \frac{m+1}{2} \rfloor} a_{i_m}t^{m-2i+1} \text{ from Proposition 2.1} \\ &= -2\left(t^{m-2} + \sum_{i=1}^{\lfloor \frac{m}{2} \rfloor}(-1)^{i-1}\frac{2^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-1-j)t^{m-2i}\right) \\ &\quad + \left(t^{m-1} + \sum_{i=1}^{\lfloor \frac{m+1}{2} \rfloor}(-1)^{i-1}\frac{2^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j)t^{m-2i+1}\right)\tau \text{ from Lemma 2.2}\end{aligned}$$

□

Below is the example to illustrate this version.

Example 2.1. Consider $m = 3$ and let $a_{1_m} = 1$, then

$$\begin{aligned}
\tau^3 &= -2\Bigg(t^1 + \sum_{i=1}^{\lfloor \frac{2}{2} \rfloor}(-1)^{i-1}\frac{2^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(2-j)t^{3-2i}\Bigg) \\
&\quad +\Bigg(t^2 + \sum_{i=1}^{\lfloor \frac{3+1}{2} \rfloor}(-1)^{i-1}\frac{2^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(3-j)t^{4-2i}\Bigg)\tau \\
&= -2t + \Big(t^2 - 2\prod_{j=2}^{2}(3-j)\Big)\tau \\
&= -2t + (t^2-2)\tau.
\end{aligned}$$

By introducing Theorem 2.1 as a new properties for τ^m, hence we can calculate the number of points using alternative method as follows ;

From 1 we have

$$\begin{aligned}
\#E_a(F_{2^m}) &= N(\tau^m - 1) \\
&= N(r_m + s_m\tau - 1) \quad \text{by letting } \tau^m = r_m + s_m\tau \\
&\quad \text{By Proposition 2.2, we obtain,} \\
\#E_a(F_{2^m}) &= N((-2s_{m-1}) + s_m\tau - 1) \\
&= (2s_{m-1}+1)^2 - t(2s_{m-1}+1)s_m + 2{s_m}^2 \\
&\quad \text{from Definition 1.4} \\
&= \Big(2\sum_{i=1}^{m-1} a_{i_{m-1}} t^{m-2i} + 1\Big)^2 - t\Big(2\sum_{i=1}^{m-1} a_{i_{m-1}} t^{m-2i} + 1\Big) \\
&\quad \Big(\sum_{i=1}^{m} a_{i_m} t^{m-2i+1}\Big) + 2\Big(\sum_{i=1}^{m} a_{i_m} t^{m-2i+1}\Big)^2 \\
&\quad \text{by Proposition 2.1} \\
&= \Bigg(2\Big(\sum_{i=1}^{m-1}(-1)^{i-1}\frac{2^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-1-j)t^{m-2i}\Big) + 1\Bigg)^2 \\
&\quad -t\Bigg(2\Big(\sum_{i=1}^{m-1}(-1)^{i-1}\frac{2^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-1-j)t^{m-2i}\Big) + 1\Bigg)
\end{aligned}$$

$$\left(\sum_{i=1}^{m}(-1)^{i-1}\frac{2^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j)t^{m-2i+1}\right)+$$
$$2\left(\sum_{i=1}^{m}(-1)^{i-1}\frac{2^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j)t^{m-2i+1}\right)^2$$
$$\text{from Lemma 2.2} \tag{4}$$

Example shown below is the illustration for $\#E_a(F_{2^m})$.

Example 2.2. *Consider a field F_{2^3} with an elliptic curve*

$$E_1 : y^2 + xy = x^3 + x^2 + 1,$$

since the coefficient $a = 1$ is selected.
Now we can calculate the number of points that passes through this curve using formula 4 .

$$\begin{aligned}\#E_a(F_{2^3}) &= \left(2\Big(\sum_{i=1}^{2}(-1)^{i-1}\frac{2^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(2-j)\Big)+1\right)^2 - \\ &\quad \left(2\Big(\sum_{i=1}^{2}(-1)^{i-1}\frac{2^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(2-j)\Big)+1\right) \\ &\quad \left(\sum_{i=1}^{3}(-1)^{i-1}\frac{2^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(3-j)\right)+ \\ &\quad 2\left(\sum_{i=1}^{3}(-1)^{i-1}\frac{2^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(3-j)\right)^2 \\ &= 14\end{aligned}$$

The points are ($(100, 011)$, $(101, 000)$, $(110, 011)$, $(011, 000)$, $(001, 101)$, $(111, 111)$, $(000, 001)$, $(111, 000)$, $(010, 111)$, $(011, 011), (110, 101), (101, 101)$, $(100, 111)$) and ∞. Refer to (Yunos and Atan, 2016) on how to find these points.

3. Conclusion

As a conclusion, we propose new method to discover the number of points through the curve E_a i.e using $\tau^m = r_m + s_m\tau$ for $s_m = \sum_{i=1}^{m}(-1)^{i-1}\frac{2^{i-1}}{(i-1)!}\prod_{j=i}^{2i-2}(m-j)t^{m-2i+1}$.

Acknowledgement

The authors are grateful to Universiti Putra Malaysia for a support via Geran Putra GP/2018/9595400.

References

Ali, N. A. and Yunos, F. (2016). Maximum and Minimum Norms for τ-NAF Expansion on Koblitz Curve. *Indian Journal of Science and Technology*, 28(9):1–7.

Ali, N. A., Yunos, F., and Jamal, N. H. (2017). A Total Norm of τ-Adic Non-Adjacent Form Occurring Among All Element of $Z(\tau)$: An Alternative Formula. In *AIP Conference Proceedings*, volume 1795, pages 1–8. AIP Publishing.

Hadani, N. H. and Yunos, F. (2018). Alternative Formula of τ^m in Scalar Multiplication on Koblitz Curve. In *AIP Conference Proceedings*, volume 1974, pages 1–9. AIP Publishing.

Hankerson, D., Menezes, A., and Vanstone, S. (2006). *Guide to Elliptic Curve Cryptography.* Springer-Verlag, Berlin, Germany.

Hazewinkel, M. (1994). *Arithmetic Series.* Kluwer Academic.

Koblitz, N. (1987). Elliptic Curve Cryptosystems,. *Mathematics Computation*, 48:203–209.

Koblitz, N. (1992). CM-Curves with Good Cryptographic Properties. In *Proceedings of the* 11^{th} *Annual International Cryptology Conference on Advances in Cryptology*, pages 279–287. Springer Verlag, London.

Solinas, J. A. (1997). An Improved Algorithm for Arithmetic on a Family of Elliptic Curves. In *Proceedings of the International Annual Conference on Cryptology*, pages 357–371. Springer, Berlin, Germany.

Solinas, J. A. (2000). *Efficient Arithmetic on Koblitz Curves. In Designs, Codes and Cryptography.* Springer, Boston, Massaachusetts.

Suberi, S., Yunos, F., and Said, M. R. M. (2016). An Even and Odd Situation for the Multiplier of Scalar Multiplication with Pseudo τ-Adic Non-Adjacent form. In *AIP Conference Proceedings*, volume 1750, pages 1–9. AIP Publishing.

Suberi, S., Yunos, F., Said, M. R. M., Sapar, S. H., and Said Husain, S. K. (2018). Formula of τ-adic Non Adjacent form with the Least Number of Non Zero Coefficients. *Jurnal Karya Asli Lorekan Ahli Matematik*, 11(1):23–30.

Yunos, F. and Atan, K. A. M. (2016). Improvement to Scalar Multiplication on Koblitz Curves by Using Pseudo τ-adic Non-Adjacent Form. In *AIP Conference Proceedings*, volume 1750, pages 1–8. AIP Publishing.

Yunos, F., Atan, K. A. M., Ariffin, M. R. K., and Said, M. R. M. (2014a). A Reduced τ-adic Naf (RTNAF) Representation for an Efficient Scalar Multiplication on Anomalous Binary Curves (ABC). *Pertanika Journal of Science and Technology*, 22:489–506.

Yunos, F., Atan, K. A. M., Ariffin, M. R. K., and Said, M. R. M. (2015a). Pseudo τ-Adic Non Adjacent Form for Scalar Multiplication on Koblitz Curves. *Malaysian Journal of Mathematical Sciences*, 9:71–88.

Yunos, F., Mohd Atan, K. A., Md Said, M. R., and Kamel Ariffin, M. R. (2014b). Pseudo τ-adic NAF for Scalar Multiplication on Koblitz Curves. In *Conference Proceeding of the* 4^{th} *International Cryptology and Information Security Conference 2014*, pages 120–130. AIP Publishing.

Yunos, F., Mohd Atan, K. A., Md Said, M. R., and Kamel Ariffin, M. R. (2015b). *Kembangan Pseudo TNAF bagi Pendaraban Skalar ke atas Lengkuk Koblitz*. PhD thesis, Universiti Putra Malaysia, Serdang, Selangor, Malaysia.

Yunos, F. and Suberi, S. (2018). Even and Odd Nature for Pseudo τ-Adic Non-Adjacent form. *Malaysian Journal of Science*, 37(2):94–102.