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

¹Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia
²Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, Malaysia
³Pusat 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 $\tau = \frac{(-1)^{a}+\sqrt{7}}{2}$ 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 \( \mathbb{F}_2 \) 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 \( \tau : E_a(\mathbb{F}_{2^m}) \to E_a(\mathbb{F}_{2^m}) \) for a point \( P = (x, y) \) on \( E_a(\mathbb{F}_{2^m}) \) is defined by \( \tau(x, y) = (x^2, y^2), \tau(\infty) = \infty \) where \( \infty \) is the point at infinity. It stands that \( (\tau^2 + 2)P = t\tau(P) \) for all \( P \in E_a(\mathbb{F}_{2^m}) \) and the trace of Frobenius map is \( t = (-1)^{1-a} \).

The \( \tau \)-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 \( \mathbb{Z}(\tau) \) is defined as \( r + st \) where \( r, s \in \mathbb{Z} \).

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

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

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 \( \alpha \) 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:

$$
U_0 = 0, U_1 = 1 \text{ and } U_\kappa = tU_{\kappa-1} - 2U_{\kappa-2} \\
V_0 = 2, V_1 = t \text{ and } V_\kappa = tV_{\kappa-1} - 2V_{\kappa-2}
$$

for $\kappa \geq 2$;

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 is is used to find $\mathrm{TNAF}((\bar{a}) \mod (\tau^m - 1))$. (Yunos et al., 2014a) produced Theorem 1.1 as an alternative version for the formula $\tau^m$. 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 $\mathrm{TNAF}\left(\sum_{m=0}^{l-1} c_m \tau^m\right)$ into an element of $Z(\tau)$ became easier. Both $\tau^m$ 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;

$$
\#E_a(F_{2^m}) = p \cdot \#E_a(F_2)
$$

where $p > 2$ is a prime ,

$$
\#E_a(F_{2^m}) = 2^m + 1 - V_m
$$

$$
\#E_a(F_{2^m}) = N(\tau^m - 1),
$$

$$
\#E_a(F_{2^m}) = \#E_a(F_{2^m}) \cdot N\left(\frac{\tau^m - 1}{\tau - 1}\right)
$$

where $|P| = N\left(\frac{\tau^m - 1}{\tau - 1}\right)$,

$$
\#E_a(F_{2^m}) = b_m^2 + 2a_m^2 + a_mb_m + 1
$$

$$
-2b_m + a_m t^m.
$$

Formula $N(\sum_{m=0}^{l-1} c_m \tau^m) = r^2 + trs + 2s^2$ where $r = \sum_{m=0}^{l-1} c_mb_m t^m$ and $s = \sum_{m=0}^{l-1} c_ma_m t^{m+1}$ was applied by (Ali and Yunos, 2016) to find maximum and minimum norms.
In this paper, our approach is to introduce \( a_{im} \) for \( 2 \leq i \leq \frac{m+1}{2} \). Subsequently, alternative formula for \( \tau^m \) is proposed. As a result, by using the new \( \tau^m \), we find the number of points that passes through the curve \( E_a \).

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

2. Alternative formula for \( \tau^m \)

We begin with the identity of \( \tau^2 = t\tau - 2 \). We expand \( \tau \) 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 on to Table 1 for value of \( r_m \) and \( s_m \) for \( m \in \{1, 2, 3, \ldots, 12\} \) using the method of expansion of \( \tau \) identity.

<table>
<thead>
<tr>
<th>( m )</th>
<th>( r_m )</th>
<th>( s_m )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>-2</td>
<td>( t )</td>
</tr>
<tr>
<td>3</td>
<td>-2t</td>
<td>( t^2 - 2 )</td>
</tr>
<tr>
<td>4</td>
<td>-2t^2 + 4</td>
<td>( t^4 - 4t )</td>
</tr>
<tr>
<td>5</td>
<td>-2t^3 + 8t</td>
<td>( t^6 - 6t^2 + 4 )</td>
</tr>
<tr>
<td>6</td>
<td>-2t^4 + 12t^2 - 8</td>
<td>( t^8 - 8t^3 + 12t )</td>
</tr>
<tr>
<td>7</td>
<td>-2t^5 + 16t^4 - 24t</td>
<td>( t^9 - 10t^4 + 24t^2 - 8 )</td>
</tr>
<tr>
<td>8</td>
<td>-2t^6 + 20t^5 - 48t^4 + 16t</td>
<td>( t^9 - 12t^5 + 40t^3 - 32t )</td>
</tr>
<tr>
<td>9</td>
<td>-2t^7 + 24t^6 - 80t^5 + 64t</td>
<td>( t^9 - 14t^6 + 60t^4 - 80t^2 + 16 )</td>
</tr>
<tr>
<td>10</td>
<td>-2t^8 + 28t^7 - 120t^6 + 160t^5 - 32</td>
<td>( t^9 - 16t^7 + 84t^5 - 160t^3 + 80t )</td>
</tr>
<tr>
<td>11</td>
<td>-2t^9 + 32t^8 - 168t^7 + 320t^6 - 160t^4</td>
<td>( t^{10} - 18t^8 + 112t^6 - 280t^4 + 240t^2 - 32 )</td>
</tr>
<tr>
<td>12</td>
<td>-2t^{10} + 36t^9 - 224t^8 + 560t^7 - 480t^5 + 164</td>
<td>( t^{11} - 20t^9 + 144t^7 - 448t^5 + 560t^3 - 192t )</td>
</tr>
</tbody>
</table>

Definition 2.1 was introduced through this table.

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

Next, we start with the generation of Table 2. By using Definition 2.1 and
we disintegrate the \( s_m \) of \( \tau^m \) for \( 1 \leq m \leq 12 \) as given in the following table.

Table 2: \( s_m \) of \( \tau^m \) for \( 1 \leq m \leq 12 \)

<table>
<thead>
<tr>
<th>( m )</th>
<th>( a_{1m}t^{m-1} )</th>
<th>( a_{2m}t^{m-3} )</th>
<th>( a_{3m}t^{m-5} )</th>
<th>( a_{4m}t^{m-7} )</th>
<th>( a_{5m}t^{m-9} )</th>
<th>( a_{6m}t^{m-11} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>-2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>-4t</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>-6t^2</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>-8t^4</td>
<td>12t</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>-10t^4</td>
<td>24t^2</td>
<td>-8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>-12t^6</td>
<td>40t^4</td>
<td>-32t</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>-14t^6</td>
<td>60t^4</td>
<td>-80t^2</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>-16t^6</td>
<td>84t^6</td>
<td>-160t^4</td>
<td>80t</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>-18t^8</td>
<td>112t^6</td>
<td>-280t^4</td>
<td>240t^2</td>
<td>-32</td>
</tr>
<tr>
<td>12</td>
<td>1</td>
<td>-20t^9</td>
<td>144t^8</td>
<td>-448t^5</td>
<td>560t^3</td>
<td>-192t</td>
</tr>
</tbody>
</table>

From Table 2, we can observed the pattern of \( a_{2m} \) for \( 1 \leq m \leq 12 \) as given in the following conjecture.

**Conjecture 2.1.** Sequence \( \{a_{2m}\}_{m=3}^{12} \) has a general formula of \( a_{2m} = a_{2m-1} - 2 \) for any integer \( m \geq 3 \).

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

**Lemma 2.1.** If \( a_{2m} = a_{2m-1} - 2 \), then the coefficient \( a_{2m} = -2(m - 2) \) 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 \( \{a_{3m}\}_{m=3}^{m=12} = \{4, 12, 24, 40, 60, 84, 112, 144\} \). We identified that this sequence can be written in the form of \( \{(−1)^{3−1} \frac{2^{3−1}}{(3−1)!}(5−3)(6−4), (−1)^{3−1} \frac{2^{3−1}}{(3−1)!}(7−3)(7−4), \ldots, (−1)^{3−1} \frac{2^{3−1}}{(3−1)!}(12−3)(12−4)\} \) that is \( a_{3m} = (−1)^{3−1} \frac{2^{3−1}}{(3−1)!} \prod_{j=3}^{2(m−2)} (m−j) \). From the pattern of the sequence that we obtained, we can conclude the general form of \( a_{im} \) as in the following Lemma.

**Lemma 2.2.** If \( a_{1m} = 1 \) then coefficient in \( s_m \) expansion is

\[
a_{im} = (−1)^{i−1} \frac{2^{i−1}}{(i−1)!} \prod_{j=i}^{2i−2} (m−j)
\]

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

\[
a_{2m} = -2(m−2) \text{ from Lemma 2.1}
\]

\[
= (−1)^{2−1} \frac{2^{2−1}}{(2−1)!} \prod_{j=2}^{2(2)−2} (m−j) \text{ is true.}
\]

Assume that \( i = k \), then \( a_{km} = (−1)^{k−1} \frac{2^{k−1}}{(k−1)!} \prod_{j=k}^{2k−2} (m−j) \) is true for \( 2 \leq k \leq \frac{m+1}{2} \).
Now, let \( i = k + 1 \),

\[
a_{k+1,m} = a_{k,m} \left( \frac{(-1)^{k} 2^{k-1} (m-2k+1)(m-2k)}{m-k} \right)
\]

\[
= \left( \frac{(-1)^{k-1}}{(k-1)!} \prod_{j=k}^{2k-2} (m-j) + \frac{2}{k} \frac{(m-2k+1)(m-2k)}{m-k} \right)
\]

\[
= \left( \frac{(-1)^{k-1}}{(k-1)!} (m-k)(m-(k+1)) \right)
\]

\[
= \left( \frac{2}{k} \frac{(m-2k+1)(m-2k)}{m-k} \right)
\]

\[
= \left( \frac{(-1)^{k} 2^{k} (m-k)(m-(k+1))}{(k-1)!} \prod_{j=k+1}^{2k} (m-j) \right)
\]

\[
= \left( \frac{(-1)^{k+1-1}}{(k+1-1)!} \prod_{j=k+1}^{2k} (m-j) \right)
\]

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 \( \tau^m \).

**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

\[
s_m = \sum_{i=1}^{\lfloor \frac{m+1}{2} \rfloor} a_{i,m} t^{m-2i+1}
\]  \hspace{1cm} (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
\[
\begin{align*}
    s_3 &= t^2 - st \\
    &= t^2 + (-1)^{2-1} \frac{2^{2-1}}{(2-1)!} (3 - 2)t^2 \\
    &= t^2 + (-1)^{2-1} \frac{2^{2-1}}{(2-1)!} \prod_{j=2}^{2(2)-2} (3 - j)t^2 \\
    &= a_{13} t^2 + a_{23} t \\
    &= a_{13} t^{3-2(1)+1} + a_{23} t^{3-2(2)+1} \\
    &= \sum_{i=1}^{\left\lfloor \frac{3+1}{2} \right\rfloor} a_{i3} t^{3-2i+1}.
\end{align*}
\]

The hypothesis (2) is true for \( m = 3 \).
Assume that if \( m = k \), then
\[
    s_k = \sum_{i=1}^{\left\lfloor \frac{k+1}{2} \right\rfloor} a_{ik} t^{k-2i+1} \text{ where } a_{1k} = 1 \text{ and } k \geq 3 \text{ is true.}
\]

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 $k \in O$,

$$s_{k+1} = t \sum_{i=1}^{\lfloor \frac{k+1}{2} \rfloor} a_i k - 2i + 2$$

$$= t \left( a_1 k^{k-1} + a_2 k - 1 \cdot k - 2 + a_3 k - 2 \cdot k - 2 + \cdots + a_{\lfloor \frac{k+1}{2} \rfloor} k^{k-2 \lfloor \frac{k+1}{2} \rfloor + 2} \right)$$

$$= a_1 k^k + a_2 k - 1 \cdot k - 2 + a_3 k - 2 \cdot k - 2 + \cdots + a_{\lfloor \frac{k+1}{2} \rfloor} k^{k-2 \lfloor \frac{k+1}{2} \rfloor + 2}$$

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

$$s_{k+1} = 1t^k + (-1)^2 - 1 \cdot 2^{2 - 1} \cdot (2 - 1)! \cdot (k - 2) \cdot (k - 1) \cdot k - 2 + \cdots +$$

$$(-1)^3 - 1 \cdot 2^{3 - 1} \cdot (3 - 1)! \cdot (k - 3) \cdot (k - 4) \cdot k - 2 + \cdots +$$

$$(-1)^{\lfloor \frac{k+1}{2} \rfloor - 1} \cdot 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \cdot (k - \lfloor \frac{k+1}{2} \rfloor)(k - \lfloor \frac{k+1}{2} \rfloor - 1) \cdots (k - 2 \lfloor \frac{k+2}{2} \rfloor + 3)$$

$$= 1t^k - 2(1) + 2 + (-1)^2 - 1 \cdot 2^{2 - 1} \cdot (2 - 1)! \cdot (k + 1 - 2) \cdot k - 2 + \cdots +$$

$$(-1)^3 - 1 \cdot 2^{3 - 1} \cdot (3 - 1)! \cdot (k + 1 - 3) \cdot (k + 1 - 4) \cdot k - 2 + \cdots +$$

$$(-1)^{\lfloor \frac{k+1}{2} \rfloor - 1} \cdot 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \cdot (k + 1 - \lfloor \frac{k+1}{2} \rfloor)(k + 1 - \lfloor \frac{k+1}{2} \rfloor - 1) \cdots (k + 1 - 2(\lfloor \frac{k+2}{2} \rfloor) + 2)$$
\[ a_{k+1} t^{k+1-1} + a_{2k+1} t^{k+1-2} + a_{3k+1} t^{k+1-5} + \ldots + a_{\left\lfloor \frac{k+1}{2} \right\rfloor} t^{k+1-\left(\left\lfloor \frac{k+1}{2} \right\rfloor \right) + 1} \]
\[ = \sum_{i=1}^{\left\lfloor \frac{k+1}{2} \right\rfloor} a_{i_k+1} t^{k+1-2i+1} \]

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 \(k \in E\),

\[ s_{k+1} = t \sum_{i=1}^{\left\lfloor \frac{k+1}{2} \right\rfloor} a_{i_k} \frac{k+1-i}{k-2i+2} t^{k-2i+1} + a_{\left\lfloor \frac{k+2}{2} \right\rfloor} k+1 \left( k-2 \left(\frac{k+1}{2} \right) + 2 \right) \]
\[ = \left( a_{1_k} t^k + a_{2k} \frac{k-1}{k-2} t^{k-2} + a_{3k} \frac{k-2}{k-4} t^{k-4} + \ldots + a_{\left\lfloor \frac{k+1}{2} \right\rfloor} k+1 \left( k-2 \left(\frac{k+1}{2} \right) + 2 \right) \right) + a_{\left\lfloor \frac{k+2}{2} \right\rfloor} k+1 \left( k-2 \left(\frac{k+1}{2} \right) + 2 \right) \]

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

\[ = \left( t^k + (-1)^{2-1} \frac{2^{2-1}}{2-1)!} k-2 \left(\frac{k+1}{2} \right) + 2 \right) t^{k-2} + \]
\[ (1)^{3-1} \frac{2^{3-1}}{(3-1)!} (k-3)(k-4) \left(\frac{k-1}{k-2} \right) t^{k-5} + \ldots + \]
\[ (1)^{\left\lfloor \frac{k+1}{2} \right\rfloor-1} \frac{2^{\left\lfloor \frac{k+1}{2} \right\rfloor-1}}{(\left\lfloor \frac{k+1}{2} \right\rfloor-1)!} (k-\left\lfloor \frac{k+1}{2} \right\rfloor) (k-\left\lfloor \frac{k+1}{2} \right\rfloor - 1) \ldots \]
\[ (k-2)\left(\frac{k+2}{2} \right) + 2 \right) \left(\frac{k+1-\left\lfloor \frac{k+1}{2} \right\rfloor}{k-2\left(\frac{k+2}{2} \right) + 2} \right) \left( k+1 \left( k+2 \left(\frac{k+1}{2} \right) + 2 \right) \right) \]
\[ + \ldots \]
\[ (k-2)\left(\frac{k+2}{2} \right) + 2 \right) \]
Alternative Method to Find the Number of Points on Koblitz Curve

\[ t^k + (-1)^{2-1} \frac{2^{2-1}}{(2-1)!} (k-1) t^{k-2} + (-1)^{3-1} \frac{2^{3-1}}{(3-1)!} (k-2)(k-3) t^{k-5} \]
\[ + \cdots + (-1)^{\left\lceil \frac{k+1}{2} \right\rceil -1} 2^{\left\lceil \frac{k+1}{2} \right\rceil -1} \frac{1}{\left( \left\lceil \frac{k+1}{2} \right\rceil -1 \right)!} (k+1 - \left\lfloor \frac{k+1}{2} \right\rfloor)(k - \left\lfloor \frac{k+1}{2} \right\rfloor) \]
\[ (k - \left\lfloor \frac{k+1}{2} \right\rfloor) \cdots (k + 1 - 2(\left\lfloor \frac{k+1}{2} \right\rfloor)) t^{k-2-2\left\lceil \frac{k+1}{2} \right\rceil} \]
\[ + (-1)^{\left\lceil \frac{k+2}{2} \right\rceil -1} \frac{2^{\left\lceil \frac{k+2}{2} \right\rceil -1}}{\left( \left\lceil \frac{k+2}{2} \right\rceil -1 \right)!} (k+1 - \left\lfloor \frac{k+2}{2} \right\rfloor)(k - \left\lfloor \frac{k+2}{2} \right\rfloor) \cdots \]
\[ (k - 2\left\lfloor \frac{k+2}{2} \right\rfloor) + 2 \]

\[ = t^{k-2(1)+2} + (-1)^{2-1} \frac{2^{2-1}}{(2-1)!} (k+1 - 2) t^{k-2(2)+2} + \]
\[ (-1)^{3-1} \frac{2^{3-1}}{(3-1)!} (k+1 - 3)(k+1 - 4) t^{k-2(3)+2} + \cdots + \]
\[ (-1)^{\left\lceil \frac{k+1}{2} \right\rceil -1} 2^{\left\lceil \frac{k+1}{2} \right\rceil -1} \frac{1}{\left( \left\lceil \frac{k+1}{2} \right\rceil -1 \right)!} (k+1 - \left\lfloor \frac{k+1}{2} \right\rfloor)(k - \left\lfloor \frac{k+1}{2} \right\rfloor) \]
\[ (k - \left\lfloor \frac{k+1}{2} \right\rfloor) \cdots (k + 1 - 2(\left\lfloor \frac{k+1}{2} \right\rfloor)) + 2) t^{k-2\left\lceil \frac{k+1}{2} \right\rceil+2} \]
\[ = a_{1k+1} t^{k+1-1} + a_{2k+1} t^{k+1-3} + a_{3k+1} t^{k+1-5} + \cdots + \]
\[ a_{\left\lceil \frac{k+1}{2} \right\rceil} t^{k+1-2\left\lceil \frac{k+1}{2} \right\rceil+1} \]
\[ = \sum_{i=1}^{\left\lceil \frac{k+1}{2} \right\rceil} a_{ik+1} t^{k+1-2i+1}. \]

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 \( \tau^m = r_m + s_m t \).

**Proposition 2.2.**

If \( s_m \) from Proposition 2.1 then the coefficient \( r_m \) can be written as

\[ r_m = -2s_{m-1} \quad (3) \]

where \( a_{1m} = 1 \) and \( m \geq 3 \).
Proof. By mathematical induction we have the following.
If \( m = 3 \), then from Table 2 we obtain
\[
\begin{align*}
 r_3 & = -2t \\
 & = -2a_{13}t \\
 & = -2s_2.
\end{align*}
\]
The hypothesis (3) is true for \( m = 3 \).
Assume that if \( m = k \), then
\[
\begin{align*}
 r_k & = -2s_{k-1} \text{ is true for } k - 2i + 1 \leq 0 \\
 & = -2 \sum_{i=1}^{\lfloor \frac{k}{2} \rfloor} a_{ik}t^{k-2i}
\end{align*}
\]
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 \( k \in E \),
\[
\begin{align*}
r_{k+1} & = -2t \sum_{i=1}^{\lfloor \frac{k}{2} \rfloor} a_{ik} \frac{k-i}{k-2i+1}t^{k-2i} \\
 & = -2t \left( a_{1k-1}t^{k-2(1)} + a_{2k-1} \frac{k-2}{k-2(2) + 1}t^{k-2(2)} + \\
 & \quad a_{3k-1} \frac{k-3}{k-2(3) + 1}t^{k-2(3)} + \cdots + a_{\lfloor \frac{k}{2} \rfloor k-1} \frac{k-\lfloor \frac{k}{2} \rfloor}{k-2(\lfloor \frac{k}{2} \rfloor + 1)}t^{k-2(\lfloor \frac{k}{2} \rfloor)} \right)
\end{align*}
\]
By using \( a_{ik} \) from Lemma 2.2 and since \( \lfloor \frac{k}{2} \rfloor = \lfloor \frac{k+1}{2} \rfloor \) when \( k \in E \), we have the following.
\[
\begin{align*}
r_{k+1} & = -2 \left( 1t^{k-1} + (-1)^{2-1} \frac{2^{2-1}}{(2-1)!}(k-2)t^{k-3} + \\
 & \quad (-1)^{3-1} \frac{2^{3-1}}{(3-1)!}(k-3)(k-1-3)t^{k-5} + \cdots + \\
 & \quad (-1)^{\lfloor \frac{k+1}{2} \rfloor-1} \frac{2^{\lfloor \frac{k+1}{2} \rfloor-1}}{\lfloor \frac{k+1}{2} \rfloor-1!}(k-\lfloor \frac{k+1}{2} \rfloor)(k-1-\lfloor \frac{k+1}{2} \rfloor)(k-2-\lfloor \frac{k+1}{2} \rfloor) \cdots \\
 & \quad (k-2\lfloor \frac{k+1}{2} \rfloor)t^{k-2(\lfloor \frac{k+1}{2} \rfloor + 1)} \right)
\end{align*}
\]
Alternative Method to Find the Number of Points on Koblitz Curve

\[
= -2 \left( a_{1k} t^{k-1} + a_{2k} t^{k-3} + a_{3k} t^{k-5} + \cdots + a_{\left\lfloor \frac{k+1}{2} \right\rfloor} t^{k-1-2\left\lfloor \frac{k+1}{2} \right\rfloor} \right)
\]

\[
= -2 \sum_{i=1}^{\left\lfloor \frac{k+1}{2} \right\rfloor} a_{i+1} t^{k+1-2i}
\]

\[
= -2s_{k+1-1}.
\]

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 \( k \in O \),

\[
r_{k+1} = -2 \left( t \sum_{i=1}^{\left\lfloor \frac{k}{2} \right\rfloor} a_{i+1} - i \left( k - 2i + 1 \right) t^{k-2i} + a_{\left\lfloor \frac{k+1}{2} \right\rfloor} t^{k-1-2\left\lfloor \frac{k+1}{2} \right\rfloor} \right)
\]

\[
= -2 \left( 1t^{k-1} + (-1)^2 - 1 \frac{2^2-1}{(2-1)!} (k-2)t^{k-3} + \right)
\]

\[
(1-1)^{3-1} \frac{2^3-1}{(3-1)!} (k-3)(k-2)(k-1) + \cdots +
\]

\[
(1-1)^{\left\lfloor \frac{k}{2} \right\rfloor - 1} \frac{2^{\left\lfloor \frac{k}{2} \right\rfloor - 1}}{\left( \left\lfloor \frac{k}{2} \right\rfloor - 1 \right)!} (k-2)(k-1) \cdots
\]

\[
(k-2) \left( k \right)_{\left\lfloor \frac{k}{2} \right\rfloor + 1} + (-1)^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \frac{2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1}}{\left( \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \right)!} \cdots
\]

\[
(k-2) \left( k \right)_{\left\lfloor \frac{k+1}{2} \right\rfloor + 1}
\]

\[
= -2 \left( a_{1k} t^{k-1} + a_{2k} t^{k-3} + a_{3k} t^{k-5} + \cdots +
\right)
\]

\[
a_{\left\lfloor \frac{k}{2} \right\rfloor} t^{k-2\left\lfloor \frac{k}{2} \right\rfloor + 1} + a_{\left\lfloor \frac{k+1}{2} \right\rfloor} t^{k-2\left\lfloor \frac{k+1}{2} \right\rfloor + 1}
\]

\[
= -2 \sum_{i=1}^{\left\lfloor \frac{k+1}{2} \right\rfloor} a_{i+1} t^{k+1-2i}
\]

\[
= -2s_{k+1-1}.
\]

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

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

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

**Proof.** We have

$$\tau^m = \tau_m + s_m \tau$$

$$= -2s_{m-1} + s_m \tau \quad \text{from Proposition 2.2}$$

$$= -2 \sum_{i=1}^{\left\lfloor \frac{m}{2} \right\rfloor} a_{i_{m-1}} t^{m-2i} + \sum_{i=1}^{\left\lfloor \frac{m+1}{2} \right\rfloor} a_{i_m} t^{m-2i+1} \quad \text{from Proposition 2.1}$$

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

Below is the example to illustrate this version.
Example 2.1. Consider \( m = 3 \) and let \( a_{1,m} = 1 \), then

\[
\tau^3 = -2\left(t^1 + \sum_{i=1}^{\lfloor \frac{3}{2} \rfloor} (-1)^{i-1} \frac{2^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2} (2-j)t^{3-2i}\right)
\]

\[
+ \left(t^2 + \sum_{i=1}^{\lfloor \frac{3}{2} \rfloor} (-1)^{i-1} \frac{2^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2} (3-j)t^{4-2i}\right)\tau
\]

\[
= -2t + \left(t^2 - 2\sum_{j=2}^{\frac{2}{3}} (3-j)\right)\tau
\]

\[
= -2t + (t^2 - 2)\tau.
\]

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

From [1] we have

\[
\#E_a(F_{2^m}) = N(\tau^m - 1)
\]

\[
= N(r_m + s_m\tau - 1) \quad \text{by letting } \tau^m = r_m + s_m\tau
\]

By Proposition 2.2 we obtain,

\[
\#E_a(F_{2^m}) = N((-2s_{m-1}) + s_m\tau - 1)
\]

\[
= (2s_{m-1} + 1)^2 - t(2s_{m-1} + 1)s_m + 2s_m^2
\]

from Definition 1.4

\[
= \left(2\sum_{i=1}^{m-1} a_{i,m-1}t^{m-2i+1} + 1\right)^2 - t\left(2\sum_{i=1}^{m-1} a_{i,m-1}t^{m-2i} + 1\right)
\]

\[
\left(\sum_{i=1}^{m} a_{i,m}t^{m-2i+1}\right) + 2\left(\sum_{i=1}^{m} a_{i,m}t^{m-2i+1}\right)^2
\]

by Proposition 2.1

\[
= \left(2\sum_{i=1}^{m-1} (-1)^{i-1} \frac{2^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2} (m-1-j)t^{m-2i} + 1\right)^2
\]

\[
- t\left(2\sum_{i=1}^{m-1} (-1)^{i-1} \frac{2^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2} (m-1-j)t^{m-2i} + 1\right)
\]

Malaysian Journal of Mathematical Sciences 27

\[
\left( \sum_{i=1}^{m} (-1)^{i-1} \frac{2^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2} (m-j)t^{m-2i+1} \right) + \\
2 \left( \sum_{i=1}^{m} (-1)^{i-1} \frac{2^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2} (m-j)t^{m-2i+1} \right)^2
\]

from Lemma 2.2 (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.

\[
\#E_a(F_{2^3}) = \left( 2 \left( \sum_{i=1}^{2} (-1)^{i-1} \frac{2^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2} (2-j) + 1 \right) \right)^2 - \\
2 \left( \sum_{i=1}^{2} (-1)^{i-1} \frac{2^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2} (2-j) + 1 \right) \\
\left( \sum_{i=1}^{3} (-1)^{i-1} \frac{2^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2} (3-j) \right) + \\
2 \left( \sum_{i=1}^{3} (-1)^{i-1} \frac{2^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2} (3-j) \right)^2
\]

\( = 14 \)

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 \(\infty\). 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 \( \tau^m = \tau_m + s_m \tau \) 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


