Menemui Matematik (Discovering Mathematics)
Vol. 4, No. 1: 60-77 (2022)

Ungkapan Terkini τ^m dalam Pendaraban Skalar yang Berpengganda Kembangan τ-Adic Bukan Bersebelahan

Faridah Yunos[1,2] dan Nurul Hafizah Hadani[2]

[1] *Jabatan Matematik dan Statistik, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia*

[2]*Institut Penyelidikan Matematik, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor Malaysia.*

[1] faridahy@upm.edu.my, [2]hafizahhadani@gmail.com

ABSTRAK

Katakan E suatu lengkuk eliptik yang ditakrifkan ke atas F_{2^m} dan pemetaan τ merupakan endomorfisma Frobenius daripada set $E(F_{2^m})$ kepada dirinya sendiri. Lengkuk Koblitz adalah sejenis lengkuk yang istimewa dengan τ telahpun digunakan untuk meningkatkan prestasi pengiraan suatu pendaraban skalar nP. P ini merupakan suatu titik yang melalui lengkuk E. Manakala, pengganda n-nya merupakan kembangan τ-adic bukan bersebelahan (TNAF) yang digit-digitnya terjana oleh pembahagian berterusan suatu integer dalam $Z(\tau)$ oleh τ . Penyelidikan sebelum ini mendapati bahawa persamaan $\tau^m = r_m + s_m\tau$ dengan integer r_m dan s_m memainkan peranan penting dalam mengenalpasti pola kembangan TNAF. Dalam kertaskerja ini, kami memberikan formula pekali a_{i_m} yang berada dalam kembangan s_m untuk $i \leq 6$. Kami mengaplikasikan nombor segitiga, nombor piramid, Teorem *Nicomachus* dan formula *Faulhaber* disamping aruhan matematik untuk membuktikan formula pekali a_{i_m} tadi. Dengan pendekatan ini, ungkapan terkini τ^m untuk *m* tertentu dapat dihasilkan bagi memgenalpasti situasi ganjil dan genap dalam sistem pseudoTNAF.

Katakunci: Endomorfisma Frobenius, Lengkuk Koblitz, τ -adic bukan bersebelahan (TNAF), pseudo τ-adic bukan bersebelahan (pseudoTNAF)

ABSTRACT

Suppose E an elliptical curve defined over F_{2^m} and τ is Frobenius endomorphism from set with $E(F_{2^m})$ to itself. Koblitz curve is a special type of curves with τ already being used to improve the performance of scalar multiplication nP's computation. P is a point that goes through the curve. Whereas its multiplier is a non-adjacent τ -adic (TNAF) form whose digits are generated by repeating division of an integer in $Z(\tau)$ by τ. Previous research has found that $\tau^m = r_m + s_m\tau$ with integers r_m and s_m play an important role in identifying the patterns of TNAF's expansion. In this paper, we give a formula for coefficients a_{i_m} in s_m for $i \leq 6$. We apply triangle's number, pyramid's number, Theorem *Nicomachus* and *Faulhaber's* formula in addition to mathematical induction to prove this formula. With this approach, the new expression for τ^m for some m can be produced to identify odd and even situations in the pseudoTNAF's system.

Keywords: Frobenius Endomorphism, Koblitz curve, τ-adic non adjacent form (TNAF), pseudo τ-adic non adjacent form (pseudoTNAF)

PENGENALAN

Kriprografi Lengkuk Eliptik (ECC) telah diperkenalkan oleh Neal Koblitz dalam tahun 1985 (Koblitz, 1987). Sistem ECC ini merupakan mekanisma kunci awam dengan pendaraban skalar (PS) merupakan operasinya yang utama. PS ini melibatkan pengiraan gandaan suatu integer *n* dengan suatu titik *P* di atas lengkuk eliptik. Prestasi pengiraannya di atas lengkuk Koblitz telah ditambahbaik dengan kehadiran suatu endomorfisma Frobenius (Koblitz, 1992). Lengkuk Koblitz ditakrifkan di atas F_2 seperti berikut:

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

dengan $a \in \{0,1\}$ sebagaimana yang dicadangkan oleh (Solinas, 1997). Pemetaan Frobenius $\tau :$ $E_a(F_{2^m}) \rightarrow E_a(F_{2^m})$ untuk suatu titik $P = (x, y)$ di atas $E_a(F_{2^m})$ ditakrifkan sebagai $\tau(x, y) = (x^2, y^2)$ dan $\tau(O) = O$ dengan O merupakan suatu titik ketakterhinggaan. Katakan surihan bagi pemetaan tadi adalah $t = (-1)^{1-a}$ dan identitinya menggunakan $\tau^2 = t\tau - 2$ maka $(\tau^2 + 2)P = t\tau(P)$.

Berikut merupakan beberapa takrifan, lema dan teorem yang telah diterjemahkan ke Bahasa Melayu daripada beberapa rujukan yang kita gunakan di dalam kajian ini.

Takrifan 1.1. (Yunos dan Suberi, 2018) $Z(\tau)$ adalah suatu set polinomial dalam sebutan τ. Ditakrifkan $Z(\tau)$ suatu gelanggang hasilbahagi

$$Z(x)/(x^2 - tx + 2^m) .$$

Lema 1.1. (Yunos dan Suberi, 2018) Jika τ merupakan suatu bentuk kuadratik maka $\mathrm{Z}(\tau) = \{ r + s\tau : r, s \in Z\}$.

Takrifan 1.2. (Yunos dan Suberi, 2018) Bentuk τ-adic bukan bersebelahan juga (dikenali sebagai τ-NAF atau TNAF) bagi $\bar{n}$ yang bukan sifar di dalam $Z(\tau)$ adalah bersamaan dengan $\sum_{i=0}^{l-1} c_i \tau^i$ di mana $c_i \in \{-1,0,1\}$ dan $c_i c_{i+1} = 0$ untuk semua i. Jika $c_{l-1} \neq 0$ maka l menjadi panjang bagi kembangan TNAF.

TNAF $(\bar{n})$ yang dalam bentuk $\sum_{i=0}^{l-1} c_i \tau^i$ merupakan suatu kembangan dengan digit-digitnya dijanakan oleh pembahagian berturutan $\bar{n}$ oleh τ serta membenarkan baki $-1, 0$ atau 1. Contoh bagi mendapatkan kembangan TNAF suatu integer adalah seperti di dalam Lampiran A.

Takrifan 1.3. (Yunos dan Suberi, 2018) Bentuk $\tau - \mathrm{adic}$ bukan bersebelahan terturunkan (juga dikenali sebagai RTNAF) bagi $\bar{n}$ yang bukan sifar di dalam $Z(\tau)$ adalah $\sum_{i=0}^{l-1} c_i \tau^i$. Ianya bersamaan dengan $n \bmod \frac{\tau^m - 1}{\tau - 1}$ di mana $c_i \in \{-1,0,1\}$ dan $c_i c_{i+1} = 0$ untuk semua i. Jika $c_{l-1} \neq 0$ maka l mejadi panjang bagi kembangan RTNAF.

Takrifan 1.4. (Yunos dan Suberi, 2018) Bentuk pseudo $\tau-$ adic bukan bersebelahan (juga dikenali sebagai pseudoTNAF) bagi $\bar{n}$ yang bukan sifar di dalam $Z(\tau)$ adalah $\sum_{i=0}^{l-1} c_i \tau^i$. Ianya bersamaan dengan n mod $\rho(\frac{\tau^m-1}{\tau-1})$ di mana $\rho \in Z(\tau)$, $c_i \in \{-1, 0, 1\}$ dan $c_i c_{i+1} = 0$ untuk semua i. Jika $c_{l-1} \neq 0$ maka l menjadi panjang bagi kembangan pseudoTNAF.

Takrifan 1.5. (Yunos dan Atan, 2016) Katakan $N : Z(\tau) \rightarrow Z$ suatu fungsi norma dan $\alpha = x + y\tau$ suatu unsur di dalam $Z(\tau)$. Norma bagi α adalah $N(a) = x^2 + txy + 2y^2$ dengan $t = (-1)^{(1-a)}$ untuk $a \in \{0,1\}$.

$\frac{\tau^m-1}{\tau-1}$ dan $\rho\left(\frac{\tau^m-1}{\tau-1}\right)$ masing-masing di dalam Takrifan 1.3 dan 1.4 boleh ditukarkan ke bentuk $r + s\tau$. Kita memilih sebarang integer n dalam selang $[1, |p'|N(r' + s'\tau) - 1]$ sedemikian hingga $r + s\tau = p'(r' + s'\tau)$ dengan p' suatu integer. Seterusnya, $\bar{n}$ dalam $Z(\tau)$ boleh dijanakan daripada pembahagian n oleh $r + s\tau$. Akhir sekali, digit-digit $-1, 0$ atau 1 dalam kedua-dua kembangan RTNAF$(\bar{n})$ dan pseudoTNAF$(\bar{n})$ dapat dijanakan oleh pembahagian berturutan $\bar{n}$ oleh τ.

Takrifan 1.6. (Yunos dan Atan, 2016) Katakan P dan Q merupakan titik-titik di atas lengkuk Koblitz. Pendaraban skalar adalah penambahan berulangan sebanyak n kali bagi suatu titik di atas lengkuk tersebut dan ditandakan sebagai $nP = P + P + \cdots + P$ untuk beberapa skalar n sedemikian hingga $nP = Q$.

Takrifan 1.7. (D'Ooge (1926) dan Gerasa (1938)) Nombor segitiga mengira objek yang boleh membentuk segitiga sama sisi. Nombor ini diungkapkan sebagai

$$\sum_{k=1}^{j} k = 1 + 2 + 3 + \cdots + j = \frac{j(j+1)}{2},$$

manakala nombor piramid mewakili nombor merajah bagi piramid dengan suatu asas poligon dan jumlah nombor bagi sisi-sisi segitiga diberikan sebagai

$$\sum_{k=1}^{j} k^2 = 1^2 + 2^2 + 3^2 + \cdots + j^2 = \frac{j^3}{3} + \frac{j^2}{2} + \frac{j}{6}.$$

Theorem 1.8. (D'Ooge (1926) dan Gerasa (1938)) **(Teorem Nicomachus)**
Jika $\sum_{k=1}^{j} k = \frac{j(j+1)}{2}$ maka $\sum_{k=1}^{j} k^3 = \frac{j^4}{4} + \frac{j^3}{2} + \frac{j^2}{4}$.

Takrifan 1.9. (D'Ooge (1926) dan Gerasa (1938)) Katakan p merupakan suatu polinomial dan B_j adalah nombor Bernouli. Formula Faulhaber's ditakrifkan sebagai hasitambah bagi integer positif yang setiap satunya berkuasa p dan ditulis sebagai

$$\sum_{k=1}^{n} k^p = \frac{1}{p+1} \sum_{j=0}^{p} (-1)^j \binom{p+1}{j} B_j n^{p+1-j} \text{ dengan } B_1 = -\frac{1}{2}.$$

Catatan: Jika $p = 4$ maka $\sum_{k=1}^{n} k^4 = \frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}$.

Takrifan 1.10. Diberi $\tau^m = r_m + s_m\tau$ suatu unsur bagi $Z(\tau)$ untuk sebarang integer poisitif m. Katakan $a_{1_m} = 1$. Kita takrifkan a_{i_m} merupakan pekali dalam kembangan s_m untuk $i \in \{1, \dots, \left\lfloor \frac{m-1}{2} \right\rfloor\}$.

Dalam kertaskerja ini, kami memperkenalkan formula baharu bagi $\tau^m = r_m + s_m\tau$ suatu unsur di dalam $Z(\tau)$. Dalam Seksyen 2, kami mengulas kajian yang telah dibangunkan oleh para penyelidik terdahulu. Seterusnya dalam Seksyen 3, kita memberikan formula umum bagi a_{i_m} dalam $s_m = \sum_{i=1}^{m} a_{i_m} t^{m-2i+1}$ untuk sebarang integer positif i yang kurang daripada 7.

SOROTAN LITERATUR

Sistem Kriptografi Lengkuk Eliptik (ECC) yang telah dicadangkan oleh (Koblitz, 1987) telah dipiawaikan sebagai sistem kriptografi yang paling berkesan digunakan sekitar tahun 1987. Dalam sistem ini, PS merupakan operasi yang utama dalam pengiraan gandaan integer n dengan suatu titik pada lengkuk eliptik. (Solinas, 1997) memperkenalkan suatu kembangan yang berbentuk τ-adic bukan bersebelahan (TNAF) di atas lengkuk Koblitz untuk mengurangkan kos PS eliptik. Algoritma lain berasaskan τ-adic bukan bersebelahan terturunkan (RTNAF) telah dibangunkan oleh Solinas (2000). Yunos et al. (2014, 2015a, 2015b) memperkenalkan kembangan lain yang setara dengan TNAF yang dikenali sebagai pseudoTNAF bagi $\bar{n}$ mod $\rho\left(\frac{\tau^m-1}{\tau-1}\right)$ dengan $\rho \in Z(\tau)$ (lihat Takrifan 1.4). Di samping itu, mereka memperkenalkan teorem berikut. Mereka menggunakan jujukan Lucas bagi memperolehi τ^m.

Teorem 2.1 *Jika* $x_0 = 0, y_0 = 1, x_i = x_{i-1} + y_{i-1}$ *dan* $y_i = -2x_{i-1}$ *maka* $\tau^i = y_i t^i + x_i t^{i+1}\tau$ *for* $i > 0$.

Sebagai hasilnya, proses untuk menukarkan kembangan bagi TNAF ($\sum_{i=0}^{l-1} c_i\tau^i$) kepada suatu unsur bagi $Z(\tau)$ menjadi lebih mudah. Dengan teorem ini juga, (Ali et al., 2016) dan (Ali dan Yunos, 2016) mengadaptasikannya ke dalam formula *N* ($\sum_{i=0}^{l-1} c_i\tau^i$) untuk mendapatkan norma maksimum, norma minimum dan jumlah norma bagi TNAF$(\bar{n})$ yang terjadi dalam kalangan semua unsur dalam $Z(\tau)$ di atas lengkuk Koblitz. Seterusnya, panjang kembangan TNAF dapat dianggarkan dengan lebih tepat bagi tujuan pengiraan kos operasi pendaraban scalar *nP* dengan *n* berbentuk pseudoTNAF. Secara tak langsung juga, kajian mendapati τ^i dalam Teorem 2.1 boleh digunakan untuk mempermudahkan pengiraan bilangan titik yang melalui lengkuk E_a.

Yunos dan Atan (2016) menyarankan pemilihan $\rho = r_0 + r_1\tau$ yang bersesuaian agar ianya dapat menyebabkan ketumpatan digit yang bukan sifar dalam kembangan pseudoTNAF bermodulo $\rho\left(\frac{\tau^m-1}{\tau-1}\right)$ menjadi lebih rendah daripada yang berada dalam TNAF dan RTNAF. Perlu dimaklumi bahawa pseudoTNAF akan setara dengan TNAF dan RTNAF masing-masing sekiranya $\rho = 1, 1-\tau, \tau-1$. Bagi menguatkan kekebalan sistem kriptografi tersebut, Suberi et al. (2016) dan Yunos dan Suberi (2018) menyarankan beberapa jenis ρ yang sepatutnya tidak dipilih dalam sistem kriptografi yang melibatkan pseudoTNAF. Mereka menerangkan pemilihan pekali-pekali r_0 , r_1 daripada ρ, dan pekali-pekali *r, s* daripada $r + s\tau = \frac{\tau^m-1}{\tau-1}$ sama ada nombor genap atau ganjil yang sesuai digunakan untuk sistem pseudoTNAF. Namun demikian, tidak dijelaskan bagaimana untuk memilih τ^m nya agar dapat menjangkakan yang akhirnya pekali-pekali *r, s* akan menjadi genap atau ganjil daripada transformasi $\frac{\tau^m-1}{\tau-1}$. Namun demikian, mereka masih tidak

dapat mencari sifat sebenar ρ yang menyebabkan kembangan pseudoTNAF berketumpatan rendah seperti yang disarankan oleh Yunos dan Atan (2016) sebelum ini. Sehingga kini, kajian berkaitannya masih lagi dijalankan. Sementara itu, Suberi et al., (2018) pula dapat merungkaikan sifat-sifat pemberat Hamming yang paling sedikit dalam kembangan TNAF yang berpola $[c_0, 0, \dots, 0, c_{l-1}]$ dan $[c_0, 0, \dots, c_{\frac{l-1}{2}}, \dots, 0, c_{l-1}]$ untuk $c_0, c_{\frac{l-1}{2}}, c_{l-1} \in \{-1,1\}$. Selanjutnya, Yunos et al., 2019 telah memperoleh formula TNAF dalam bentuk $a + b\tau$ bagi kembangan $[0, c_1, \dots, c_{l-1}]$, $[-1, c_1, \dots, c_{l-1}]$, $[1, c_1, \dots, c_{l-1}]$ dan $[0,0,0, c_3, c_4, \dots, c_{l-1}]$ untuk $c_i \in \{-1,0,1\}$.

Bertitik tolak daripada beberapa masalah tadi, kami menghuraikan semula sebutan $\tau^i = y_i t^i + x_i t^{i+1}\,\tau$ (Teorem 2.1) dengan harapan pada masa hadapan akan dapat menyelesaikan masalah penyelidik sebelum ini. Terlebih dahulu, kita tukarkan τ^i ke notasi $\tau^m = r_m + s_m\tau$. Untuk kali ini, kami hanya mengutarakan sifat pekali tertentu daripada a_{2_m} sehingga a_{6_m} yang berada dalam kembangan s_m. Dalam kertaskerja ini, kami memperkenalkan formula untuk pola jujukan a_{2_m} sehingga a_{6_m}. Bagi mengukuhkan hujah pembuktiannya, kami mengaitkannya dengan nombor segitiga dan pyramid, Teorem Nicomachus serta Formula Faulhaber disamping aruhan matematik.

HASIL KAJIAN DAN PERBINCANGAN

Dalam kajian ini, kita tidak menggunakan perwakilan $r_m = y_m t^m$ dan $s_m = x_m t^{m+1}$ seperti Teorem 2.1. Tetapi kita memilih identiti $\tau^2 = t\tau - 2$ bagi menukarkan τ^m untuk $m \in \mathbb{Z}^+$ ke bentuk $r_m + s_m\tau$. Berikut merupakan contoh pengiraannya untuk dua nilai m .

$\tau^3 = \tau^2\tau = -2t - (t^2 - 2)\tau$ dengan $r_3 = -2t$ dan $s_m = t^2 - 2$
$\tau^4 = \tau\tau^3 = -2t + 4 + (t^3 - 4t)\tau$ dengan $r_4 = -2t + 4$ dan $s_4 = t^3 - 4t$

Kami mengemukakan data bagi s_m dan r_m seperti berikut.

Jadual 1: Semua r_m dan s_m bagi τ^m untuk $1 \le m \le 12$

m	r_m	s_m
1	0	1
2	-2	t
3	$-2t$	$t^2 - 2$
4	$-2t + 4$	$t^3 - 4t$
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	$-2t^{10} + 36t^8 - 224t^6 + 560t^4 - 480t^2 + 64$	$t^{11} - 20t^9 + 144t^7 - 448t^5 + 560t^3 - 192t$

Sebutan s_m dalam $\tau^m = r_m + s_m\tau$ daripada Jadual 1 di atas diperincikan lagi melalui jadual di bawah.

Jadual 2 : Senarai Semua sebutan $a_{i_m}t^{m-i}$ dalam kembangan s_m untuk $1 \leq i \leq 6$ dan $1 \leq m \leq 12$

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

Merujuk Jadual 2 di atas, kita dapat mengenalpasti bentuk umum bagi s_m yang tertentu. Kita mulainya dengan memerhatikan jujukan $\{a_{2_m}\}_{m=3}^{m=12} = \{-2, -4, -6, -8, -10, \dots, -20\}$ yang mana formula umumnya untuk $\{a_{2_m}\}_{m=3}^{m=\infty}$ diandaikan dengan konjektur berikut:

Konjektur 2.1. Jujukan $\{a_{2_m}\}_{m=3}^{m=\infty} = \{-2, -4, -6, -8, -10, \dots\}$ mempunyai formula umum $a_{2_m} = a_{2_{m-1}} - 2$.

Jujukan $\{a_{2_m}\}_{m=3}^{m=12}$ tadi boleh ditulis semula mengikut susunan $\{-2(3-2), -2(4-2), -2(5-2), -2(6-2), -2(7-2), -2(8-2), -2(9-2), -2(10-2), -2(11-2), -2(12-2)\}$.

Teorem 2.2 berikut menunjukkan formula umum bagi sebutan a_{2_m} untuk $m \geq 3$ dengan menggunakan konjektur di atas.

Teorem 2.2. Jika $a_{2_m} = a_{2_{m-1}} - 2$ maka $a_{2_m} = -2(m-2)$untuk sebarang integer $m \geq 3$.

Bukti. Kita buktikan teorem ini menggunakan induksi matematik sepertimana berikut:

Jika $m = 3$, maka $a_{2_3} = -2(3-2) = -2$ adalah benar.

Andaikan $m = k$, maka $a_{2_k} = -2(k-2)$ juga benar untuk $k \geq 3$.

Sekarang, katakan $m = k + 1$, kita dapati

$a_{2_{k+1}} = a_{2_k} - 2,$

$= -2(k-2) - 2$

$= -2(k-1)$

$= -2\big((k+1) - 2\big)$ adalah benar untuk $m = k + 1$.

Kesimpulannya, $a_{2_m} = -2(m-2)$ benar untuk semua integer $m \geq 3$.■

Merujuk Jadual 2, kita perhatikan bahawa jujukan $\{a_{3_m}\}_{m=5}^{m=12} = \{4, 12, 24, 40, 60, 84, 112, 144\}$ yang mana formula umumnya untuk $\{a_{3_m}\}_{m=3}^{m=\infty}$ diandaikan dengan konjektur berikut:

Konjektur 2.3. Jujukan $\{a_{3_m}\}_{m=3}^{m=\infty} = \{4, 12, 24, 40, 60, 84, 112, 144, \dots\}$ mempunyai formula umum $a_{3_\mathrm{m}} = a_{3_{m-1}} + 4(\mathrm{m}-1) - 12$.

Jujukan $\{a_{3_m}\}_{m=5}^{m=12} = \{4, 12, 24, 40, 60, 84, 112, 144\}$ boleh disusun semula seperti berikut: $\{a_{3_m}\}_{m=5}^{m=12} = \{2(5-3)(5-4), 2(6-3)(6-4), 2(7-3)(7-4), 2(8-3)(8-4), 2(9-3)(9-4), 2(10-3)(10-4), 2(11-3)(11-4), 2(12-3)(12-4)\}$. Teorem 2.4 berikut menggambarkan bentuk umum bagi a_{3_m} untuk $m \geq 5$ dengan menggunakan Konjektur 2.3.

Teorem 2.4. Jika $a_{3_\mathrm{m}} = a_{3_{m-1}} + 4(\mathrm{m}-1) - 12$ maka $a_{3_m} = 2(m-3)(m-4)$ for any integer $m \geq 5$.

Bukti. Kita buktikan teorem ini menggunakan induksi matematiksepertimana berikut:

Jika $m = 5$ maka $a_{3_5} = 2(5-3)(5-4) = 4$ adalah benar.

Andaikan $m = k$, $a_{3_k} = 2(k-3)(k-4)$ adalah benar untuk sebarang nilai $k \geq 5$.

Sekarang, untuk $m = k+1$, kita dapati

$$a_{3_{k+1}} = a_{3_k} + 4k - 12$$
$$= 2(k-3)(k-4) + 4k - 12$$
$$= 2(k-3)(k-4) + 2k + 2k + 2 - 14$$
$$= 2(k-3)(k-4) + 2(k-3) + 2(k-4) + 2$$
$$= 2(k+1-3)(k+1-4) \text{ is true for } m = k+1.$$

Kesimpulannya, $a_{3_m} = 2(m-3)(m-4)$ benar untuk semua integer $m \geq 5$.■

Seterusnya daripada Jadual 2, kita mendapati bahawa jujukan $\{a_{4_m}\}_{m=7}^{m=12} = \{-8, -32, -80, -160, -280, -448\}$ mempunyai formula umum untuk $\{a_{4_m}\}_{m=7}^{m=\infty}$ yang diandaikan dengan konjektur berikut:

Konjektur 2.5. Jujukan $\{a_{4_m}\}_{m=7}^{m=\infty} = \{-8, -32, -80, -160, -280, -448, \ldots\}$ mempunyai formula umum $a_{4_m} = -4(\mathrm{m}-6)(\mathrm{m}-5)$.

$\{a_{4_m}\}_{m=7}^{m=12}$ boleh disusun semula seperti berikut:$\{a_{4_m}\}_{m=7}^{m=12} = \left\{-\left(8 + \frac{4}{3}(7-7)(7^2 - 8(7) + 18)\right), -\left(8 + \frac{4}{3}(8-7)(8^2 - 8(8) + 18)\right), -\left(8 + \frac{4}{3}(9-7)(9^2 - 8(9) + 18)\right), -\left(8 + \frac{4}{3}(10-7)(10^2 - 8(10) + 18)\right), -\left(8 + \frac{4}{3}(11-7)(11^2 - 8(11) + 18)\right), -\left(8 + \frac{4}{3}(12-7)(12^2 - 8(12) + 18)\right)\right\}$. Teorem 2.6 di bawah menunjukkan sebutan umum bagi a_{4_m} untuk sebarang integer $m \geq 7$ dengan menggunakan Konjektur 2.5.

Teorem 2.6. Jika $a_{4_m} = -4(\mathrm{m}-6)(\mathrm{m}-5)$ maka $a_{4_m} = -8 - \frac{4}{3}(m-7)(m^2 - 8m + 18)$ untuk sebarang integer $m \geq 7$.

Bukti:

Menggunakan aruhan matematik, pembuktiannya adalah seperti berikut:

Jika $m = 7$, maka $a_{4_7} = -8 - \frac{4}{3}(7-7)(7^2 - 8(7) + 18) = -8$ adalah benar.

Andaikan $m = k$, $a_{4_k} = -8 + \frac{4}{3}(k-7)(k^2 - 8k + 18)$ adalah benar untuk sebarang nilai $k \geq 7$.

Sekarang, untuk $m = k + 1$ kita dapati

$a_{4_{k+1}}$

$= a_{4_k} + 3(k-5)(k-4)$

$= -8 - \frac{4}{3}(k-7)(k^2 - 8k + 18) - 4(k-5)(k-4)$

$= -8 - \frac{4}{3}(k-7)(k^2 - 8k + 18) - 4(k^2 - 9k + 20)$

$= -8 - \frac{4}{3}(k-7)(k^2 - 8k + 18) - \frac{4}{3}(2(k-7)(k) - 7(k-7) + k^2 - 8k + 18 + 2k - 7)$

$= -8 - \frac{4}{3}\big((k-7)(k^2 - 8k + 18) + 2(k-7)k - 7(k-7) + (k^2 - 8k + 18) + 2k - 7\big)$

$= -8 - \frac{4}{3}\big((k-7) + 1\big)\big((k^2 - 8k + 18) + 2m - 7\big)$

$= -8 - \left(\frac{4}{3}(k-7) + \frac{4}{3}\right)(k^2 - 8k + 18 + 2k + 1 - 8)$

$= -8 - \frac{4}{3}(k - 7 + 1)((k+1)^2 - 8(k+1) - 18)$ juga benar untuk $m = k + 1$.

Kesimpulannya, ianya benar untuk semua $m \geq 7$.■

Korolari 2.7. Katakan $a_{4_7} = -8$. Jika $a_{4_m} = -8 - 4\sum_{i=5}^{m-3}(m-i)(m-i+1)$ maka pekali $a_{4_m} = -8 - 4\frac{(m-7)\left(m^2-8m+18\right)}{3}$. untuk sebarang integer $m > 7$.

Bukti: Katakan $a_{4_7} = -8$

Untuk $m > 7$,

$a_{4_m} = -8 - 4\sum_{i=5}^{m-3}(m-i)(m-i+1)$

$= -8 - 4\sum_{i=5}^{m-3}(m-i)\big((m-i) - 1\big)$

$= -8 - 4(\sum_{i=5}^{m-3}(m-i)^2 - \sum_{i=5}^{m-3}(m-i))$ (1)

Kita bentangkan semula dua siri di atas menggunakan Takrifan 1.7: .

$$\sum_{i=5}^{m-3}(m-i)^2 = \frac{1}{6}(m-5)(m-4)(2(m-5)+1) - 5 \quad (2)$$

$$\sum_{i=5}^{m-3}(m-i) = \frac{(m-5)(m-4)}{2} - 3 \quad (3)$$

Gantikan (2) dan (3) ke dalam (1), kita memperolehi

$$a_{4_m} = -8 - 4\left[\frac{1}{6}(m-5)(m-4)(2(m-5)+1) - 5 - \frac{(m-5)(m-4)}{2} + 3\right]$$

$$= -8 - 4\left[\frac{2m^3-9m^2-18m^2+81m+40m-180}{6} - 5 - \frac{m^2-9m+20}{2} + 3\right]$$

$$= -8 - 4\frac{2m^3-30m^2+148m-252}{6}$$

$$= -8 - 4\frac{(m-7)(m^2-8m+18)}{3}. \blacksquare$$

Melalui pemerhatian, jujukan $\{a_{5_m}\}_{m=9}^{m=12}$=$\{16, 80, 240, 560\}$ daripada Jadual 2 boleh disusun semula menjadi $\left\{16+\frac{2}{3}\left((9-7)^2(9-6)^2-2(9^2-13(9)+54)\right), 16+\frac{2}{3}\left((10-7)^2(10-6)^2-2(10^2-13(10)+54)\right), 16+\frac{2}{3}\left((11-7)^2(11-6)^2-2(11^2-13(11)+54)\right), 16+\frac{2}{3}\left((12-7)^2(12-6)^2-2(12^2-13(12)+54)\right)\right\}$. Teorem 2.8 memberikan formula umum bagi a_{5_m} untuk integer $m \geq 9$ dengan menggunakan konjektur berikut:

Konjektur 2.8. Jujukan $\{a_{5_m}\}_{m=9}^{m=12}$=$\{16, 80, 240, 560, \ldots\}$ mempunyai formula umum $a_{5_m} = a_{5_{m-1}} + \frac{8}{3}(\mathrm{m}-8)(\mathrm{m}-7)(\mathrm{m}-6)$.

Teorem 2.9. Jika $a_{5_m} = a_{5_{m-1}} + \frac{8}{3}(\mathrm{m}-8)(\mathrm{m}-7)(\mathrm{m}-6)$ maka $a_{5_m} = 16 + \frac{2}{3}\left((\mathrm{m}-7)^2(m-6)^2 - 2(m^2-13m+54)\right)$ untuk $m \geq 9$.

Bukti. Menggunakan aruhan matematik, pembuktiannya adalah seperti berikut:

Untuk $m = 9$, maka $a_{5_9} = 16 + \frac{2}{3}\left((9-7)^2(9-6)^2 - 2(9^2-139+54)\right) = 16$ adalah benar.

Andaikan $m = k$, $a_{5_k} = 16 + \frac{2}{3}\left((\mathrm{k}-7)^2(k-6)^2 - 2(k^2-13k+54)\right)$ juga benar untuk sebarang nilai $k \geq 9$.

Sekarang, untuk $m = k+1$ kita dapati

$$a_{5_{k+1}}$$

$$= a_{5_k} + \frac{8}{3}(k-7)(k-6)(k-5)$$

$$= 16 + \frac{2}{3}\left((\mathrm{k}-7)^2(k-6)^2 - 2(k^2-13k+54)\right) + \frac{8}{3}(k-7)(k-6)(k-5)$$

$= 16 + \frac{2}{3}((\mathrm{k}-7)^2(k-6)^2 - 2(k^2-13k+54) + 4k^3 - 72k^2 + 428k - 840)$

$= 16 + \frac{2}{3}[(k-7)^2(k-6)^2 + 2(k-7)^2(k-6) + (k-7)^2 + 2(k-7)(k-6)^2 + (k-6) + 2(k-7) + (k-6)^2 + 2(k-6) + 1 - 2(k^2-13k+54+2k-12)]$

$= 16 + \frac{2}{3}\left[((k-7)^2 + 2(k-7) + 1)((k-6)^2 + 2(k-6) + 1) - 2\left((k^2+2k+1) - 13k + 41\right)\right]$

$= 16 + \frac{2}{3}\left((\mathrm{k}-7+1)^2(k-6+1)^2 - 2((k+1)^2 - 13(k+1) + 54)\right)$ adalah benar untuk m=k+1.

Kesimpulannya, ianya benar untuk semua $m \geq 9$. ■

Akhir sekali, melalui pemerhatian daripada Jadual 2 mendapati bahawa $\{a_{6_m}\}_{m=11}^{m=12} = \{-32, -192\}$ boleh disusun semula seperti $\Big\{112(11) - \frac{4}{3}\Big[\frac{(11-9)^5}{5} + (11-9)^4 + \frac{5}{3}(11-9)^3 + (11-9)^2 + \frac{2}{15}(11-9)\Big] + \frac{8}{3}\Big[\frac{(11-2)^3}{3} + \frac{(11-2)^2}{2} + \frac{11-2}{6} - \frac{13}{2}(11-2)(11-1)\Big] - \frac{1232}{3}$, $112(12) - \frac{4}{3}\Big[\frac{(12-9)^5}{5} + (12-9)^4 + \frac{5}{3}(12-9)^3 + (12-9)^2 + \frac{2}{15}(12-9)\Big] + \frac{8}{3}\Big[\frac{(12-2)^3}{3} + \frac{(12-2)^2}{2} + \frac{12-2}{6} - \frac{13}{2}(12-2)(m-1)\Big] - \frac{1232}{3}\Big\}$. Pola jujukan ini secara umum diilustrasikan dalam Teorem 2.10 dan hujah pembuktiannya dibantu oleh konjektur berikut.

Konjektur 2.10. Jujukan $\{a_{6_m}\}_{m=11}^{m=\infty} = \{-32, -192, \dots\}$ mempunyai formula umum $a_{6_m} = a_{6_{m-1}} - \frac{4}{3}\left((m-10)^4 + 6(m-10)^3 + 13(m-10)^2 + 12(m-10)\right) + \frac{8}{3}\Big((m-3)^2 - \frac{9}{2}(m-3) - \frac{13}{2}(m-2)\Big)$.

Teorem 2.11. Jika $a_{6_m} = a_{6_{m-1}} - \frac{4}{3}\left((m-10)^4 + 6(m-10)^3 + 13(m-10)^2 + 12(m-10)\right) + \frac{8}{3}\Big((m-3)^2 - \frac{9}{2}(m-3) - \frac{13}{2}(m-2)\Big)$ maka $a_{6_m} = 112m - \frac{4}{3}\Big[\frac{(m-9)^5}{5} + (m-9)^4 + \frac{5}{3}(m-9)^3 + (m-9)^2 + \frac{2}{15}(m-9)\Big] + \frac{8}{3}\Big[\frac{(m-2)^3}{3} + \frac{(m-2)^2}{2} + \frac{m-2}{6} - \frac{13}{2}(m-2)(m-1)\Big] - \frac{1232}{3}$ untuk sebarang integer $m \geq 11$.

Bukti.

Menggunakan aruhan matematik, pembuktiannya adalah seperti berikut:

Untuk $m = 11$, maka $a_{6_{11}} = 112m - \frac{4}{3}\Big[\frac{(m-9)^5}{5} + (m-9)^4 + \frac{5}{3}(m-9)^3 + (m-9)^2 + \frac{2}{15}(m-9)\Big] + \frac{8}{3}\Big[\frac{(m-2)^3}{3} + \frac{(m-2)^2}{2} + \frac{m-2}{6} - \frac{13}{2}(m-2)(m-1)\Big] - \frac{1232}{3} = -32$ adalah benar.

Andaikan $m = k$, $a_{6_k} = 112k - \frac{4}{3}\left[\frac{(k-9)^5}{5} + (k-9)^4 + \frac{5}{3}(k-9)^3 + (k-9)^2 + \frac{2}{15}(k-9)\right] + \frac{8}{3}\left[\frac{(k-2)^3}{3} + \frac{(k-2)^2}{2} + \frac{k-2}{6} - \frac{13}{2}(k-2)(k-1)\right] - \frac{1232}{3}$ juga benar untuk sebarang nilai $k \geq 11$.

Sekarang, untuk $m = k + 1$ kita mendapati bahawa

$$a_{6_{k+1}} = a_{6_k} - \frac{4}{3}[(k-9)^4 + 6(k-9)^3 + 13(k-9)^2 + 12(k-9)] + \frac{8}{3}\left[(k-2)^2 - \frac{9}{2}(k-2) - \frac{13}{2}(k-1)\right]$$

$$= 112k - \frac{4}{3}\left[\frac{(k-9)^5}{5} + (k-9)^4 + \frac{5}{3}(k-9)^3 + (k-9)^2 + \frac{2}{15}(k-9)\right] + \frac{8}{3}\left[\frac{(k-2)^3}{3} + \frac{(k-2)^2}{2} + \frac{k-2}{6} - \frac{13}{2}(k-2)(k-1)\right] - \frac{1232}{3} - \frac{4}{3}[(k-9)^4 + 6(k-9)^3 + 13(k-9)^2 + 12(k-9)] + \frac{8}{3}\left[(k-2)^2 - \frac{9}{2}(k-2) - \frac{13}{2}(k-1)\right]$$

$$= 112k - \frac{4}{3}\left[\frac{(k-9)^5}{5} + (k-9)^4 + \frac{5}{3}(k-9)^3 + (k-9)^2 + \frac{2}{15}(k-9)\right] + \frac{8}{3}\left[\frac{(k-2)^3}{3} + \frac{(k-2)^2}{2} + \frac{k-2}{6} - \frac{13}{2}(k-2)(k-1)\right] - \frac{1232}{3} + 112 - \frac{4}{3}\left[\frac{5(k-9)^4+10(k-9)^3+10+5(k-9)+1}{5} + 4(k-9)^3 + 6(k-9)^2 + 4(m-9) + 1 + \frac{5}{3}(3(k-9)^2 + 3(k-9) + 1) + 2(k-9) + 1 + \frac{2}{15}\right] + \frac{8}{3}\left[\frac{3(k-2)^2+3(k-2)+1}{3} + \frac{2(k-2)+1}{2} + \frac{1}{6} - \frac{13}{2}(k-2) - \frac{13}{2}(k-1) - \frac{13}{2}\right]$$

$$= 112(k+1) - \frac{4}{3}\left[\big((k+1)-9\big)^5 + \big((k+1)-9\big)^4 + 5\left(\frac{\big((k+1)-9\big)^3}{3}\right) + \big((k+1)-9\big)^2 + \frac{2}{15}\big((k+1)-9\big)\right] + \frac{8}{3}\left[\frac{\big((k+1)-2\big)^3}{3} + \frac{\big((k+1)-2\big)^2}{2} + \frac{(k+1)-2}{6} - \frac{13}{2}\big((k+1)-2\big)\big((k+1)-1\big)\right] - \frac{1232}{3}.$$

adalah benar untuk $m = k + 1$.

Kesimpulannya ianya benar untuk semua integer $m \geq 11$. ■

Korolari 2.12. Jika $a_{6_m} = -\left[32(m-10) + \frac{4}{3}\sum_{i=9}^{m-3}\left((m-i)^2\big((m-i)+1\big)^2\right) - \frac{8}{3}\sum_{1=2}^{m-10}(m-i)^2 + \frac{104}{3}\sum_{i=2}^{m-10}(m-i) - 144m + 1584\right]$ maka $a_{6_m} = -\left[32(m-10) + \frac{4}{3}[\sum_{i=9}^{m-3}(m-i)^4 + 2\sum_{i=9}^{m-3}(m-i)^3 + \sum_{i=9}^{m-3}(m-i)^2] - \frac{8}{3}\sum_{1=2}^{m-10}(m-i)^2 + \frac{104}{3}\sum_{i=2}^{m-10}(m-i) - 144m + 1584\right]$

Bukti.

Katakan $a_{6_{11}} = -32$.

Untuk $m > 11$,

$$a_{6_m} = -\left[32(m-10) + \frac{4}{3}\sum_{i=9}^{m-3}(m-i)^2((m-i)^2 + 2(m-i) + 1) - \frac{8}{3}\sum_{1=2}^{m-10}(m-i)^2 + \frac{104}{3}\sum_{i=2}^{m-10}(m-i) - 144m + 1584\right]$$

$$= -\left[32(m-10) + \frac{4}{3}[\sum_{i=9}^{m-3}(m-i)^4 + 2\sum_{i=9}^{m-3}(m-i)^3 + \sum_{i=9}^{m-3}(m-i)^2] - \frac{8}{3}\sum_{1=2}^{m-10}(m-i)^2 + \frac{104}{3}\sum_{i=2}^{m-10}(m-i) - 144m + 1584\right] \quad (4)$$

Daripada persamaan ini, siri berikut dikembangkan dengan menggunakan formula Faulhaber (iaitu Takrifan 1.9):

$$\sum_{i=9}^{m-3}(m-i)^4 = \frac{(m-9)^5}{5} + \frac{(m-9)^4}{2} + \frac{(m-9)^3}{3} + \frac{(m-9)}{30} - 17 \quad (5)$$

siri berikut dikembangkan menggunakan Teorem Nicomachus (iaitu Teorem 1.8):

$$\sum_{i=9}^{m-3}(m-i)^3 = \frac{(m-9)^4}{4} + \frac{(m-9)^3}{2} + \frac{(m-9)^2}{4} - 9 \quad (6)$$

siri berikut mewakili nombor piramid (rujuk Takrifan 1.7):

$$\sum_{i=9}^{m-3}(m-i)^2 = \frac{(m-9)^3}{3} + \frac{(m-9)^2}{2} + \frac{(m-9)}{6} - 5 \quad (7)$$

$$\sum_{i=2}^{m-10}(m-i)^2 = \frac{(m-2)^3}{3} + \frac{(m-2)^2}{2} + \frac{(m-2)}{6} - 285 \quad (8)$$

siri berikut mewakili nombor segitiga (rujuk Takrifan 1.7):

$$\sum_{i=2}^{m-10}(m-i) = \frac{(m-2)(m-1)}{2} - 45 \quad (9)$$

Gantikan (5) hingga (9) ke dalam (4), kita perolehi

$$a_{6_m} = -\left[32(m-10) + \frac{4}{3}\left(\frac{(m-9)^5}{5} + \frac{(m-9)^4}{2} + \frac{(m-9)^3}{3} + \frac{(m-9)}{30} - 17\right) + \frac{8}{3}\left(\frac{(m-9)^4}{4} + \frac{(m-9)^3}{2} + \frac{(m-9)^2}{4} - 9\right) + \frac{4}{3}\left(\frac{(m-9)^3}{3} + \frac{(m-9)^2}{2} + \frac{(m-9)}{6} - 5\right) - \frac{8}{3}\left(\frac{(m-2)^3}{3} + \frac{(m-2)^2}{2} + \frac{(m-2)}{6} - 285\right) + \frac{104}{3}\left(\frac{(m-2)(m-1)}{2} - 45\right) - 144m + 1584\right]$$

$$= -\left[32m - 320 + \frac{4}{3}\left(\frac{(m-9)^5}{5} + \frac{(m-9)^4}{2} + \frac{(m-9)^3}{3} + \frac{(m-9)}{30}\right) - \frac{4}{3}(17) + \frac{8}{3}\left(\frac{(m-9)^4}{4} + \frac{(m-9)^3}{2} + \frac{(m-9)^2}{4}\right) - \frac{8}{3}(9) + \frac{4}{3}\left(\frac{(m-9)^3}{3} + \frac{(m-9)^2}{2} + \frac{(m-9)}{6}\right) - \frac{4}{3}(5) - \frac{8}{3}\left(\frac{(m-2)^3}{3} + \frac{(m-2)^2}{2} + \frac{(m-2)}{6}\right) - \frac{8}{3}(285) + \frac{104}{3}\left(\frac{(m-2)(m-1)}{2}\right) - \frac{104}{3}(45) - 144m + 1584\right]$$

$$= -\left[-112m + \frac{4}{3}\left[(m-9)^5 + (m-9)^4 + 5\left(\frac{(m-9)^3}{3}\right) + (m-9)^2 + \frac{2}{15}(m-9)\right] - \frac{8}{3}\left[\frac{(m-2)^3}{3} + \frac{(m-2)^2}{2} + \frac{m-2}{6} - \frac{13}{2}(m-2)(m-1)\right] + \frac{1232}{3}\right]$$

$$= 112m - \frac{4}{3}\left[(m-9)^5 + (m-9)^4 + 5\left(\frac{(m-9)^3}{3}\right) + (m-9)^2 + \frac{2}{15}(m-9)\right] + \frac{8}{3}\left[\frac{(m-2)^3}{3} + \frac{(m-2)^2}{2} + \frac{m-2}{6} - \frac{13}{2}(m-2)(m-1)\right] - \frac{1232}{3}.\blacksquare$$

Dapatan daripada kertaskerja ini hanya mengemukakan formula $\tau^m = -2s_{m-1} + s_m\tau$ yang mempunyai nilai m tidak melebihi 12. Ini kerana untuk kes m yang lain belum dibuktikan lagi formulanya akan berbentuk sedemikian rupa. Katakan $S_1 = 1$, $S_2 = t$ dan

$s_m = t^{m-1} + a_{2_m}t^{m-3} + a_{3_m}t^{m-5} + a_{4_m}t^{m-7} + a_{5_m}t^{m-9} + a_{6_m}t^{m-11}$ untuk $3 \le m \le 12$ (rujuk Jadual 2 semula), maka

$$\tau^m = -2(t^{m-2} + a_{2_{m-1}}t^{m-4} + a_{3_{m-1}}t^{m-6} + a_{4_{m-1}}t^{m-8} + a_{5_{m-1}}t^{m-10} + a_{6_{m-1}}t^{m-12}$$
$$+\left(t^{m-1} + a_{2_m}t^{m-3} + a_{3_m}t^{m-5} + a_{4_m}t^{m-7} + a_{5_m}t^{m-9} + a_{6_m}t^{m-11}\right)\tau.$$

Kita boleh menggunakan formula daripada sama ada Teorem 2.2, 2.4, 2.6, 2.9, 2.11 dan Korolari 2.7, 2.12 untuk mendapatkan sebutan τ^m. Selanjutnya, kita dapat menjangka yang akhirnya pekali-pekali *r, s* akan menjadi genap atau ganjil daripada penjelmaan $\frac{\tau^m-1}{\tau-1}$ kepada $r + s\tau$. Ini adalah untuk mengatasi masalah yang ditinggalkan oleh kajian yang dijalankan oleh Suberi et al. (2016) dan Yunos dan Suberi (2018) sebagaimana yang diterangkan dalam sorotan literature, tetapi untuk nilai m tertentu. Jadual berikut menunjukkan nilai r dan s. Contoh berikut digunakan sebelum melengkapkannya:

Oleh kerana $\bar{\tau} = 1 - \tau$ dan $\tau \cdot \bar{\tau} = 2$, maka kita memperoleh

$$\frac{\tau^3 - 1}{\tau - 1} = -\frac{(-2t-1) + (t^2-2)\tau}{\tau - 1}.\frac{\bar{\tau} - 1}{\bar{\tau} - 1} = -1 + \frac{3t+1}{2}\tau.$$

Oleh itu, jika $t = 1$ maka $\frac{\tau^3-1}{\tau-1} = -1 + 2\tau$ dan jika $t = -1$ maka $\frac{\tau^3-1}{\tau-1} = -1 - \tau$.

Jadual 3: Nilai Genap atau Ganjil bagi r dan s dalam $\frac{\tau^m-1}{\tau-1}$ untuk $1 \le m \le 12$

m	r	s

1	1	0
2	t	1
3	-1	$\frac{3t+1}{2}$
4	$-3t$	t
5	-1	$\frac{-5t+1}{2}$
6	$5t$	-3
7	7	$\frac{-17t+1}{2}$
8	$-3t$	9
9	-17	$\frac{-11t+1}{2}$
10	$-11t$	-11
11	23	$\frac{-45t+1}{2}$
12	$45t$	1

Daripada jadual di atas, kita dapat mengenalpasti bahawa untuk semua m daripada 1 hingga 12, nilai r adalah ganjil, untuk m yang ganjil menghasilkan s yang genap dan untuk m yang genap menghasilkan s yang ganjil. Kesannya terhadap pendaraban skalar di atas lengkuk Koblitz boleh dirujuk dalam kertaskerja Suberi et al. (2016) dan Yunos dan Suberi (2018). Tidak semua kriteria pemilihan m yang perlu dipertimbangkan oleh sistem pseudoTNAF yang telah dibincangkan sebelum ini. Mereka hanya perlu memilih m yang perdana mengikut piawaian yang telah dikemukakan oleh FIPS PUB 186-4 dan boleh didapati di laman web NIST (2013). Ianya merupakan siri rasmi penerbitan yang ke-4 yang berkaitan dengan piawaian dan garis panduan yang diguna pakai dan termaktub di bawah peruntukan dalam Akta Maklumat Persekutuan Pengurusan Keselamatan iaitu The Federal Information Security Management Act (FISMA) tahun 2002. Sudah tentu, pola r dan s yang genap dan ganjil untuk semua m terutamanya nombor perdana yang besar perlu dikaji semula melalui penelitian terhadap pekali a_{i_m}.

KESIMPULAN

Sebagai kesimpulannya, kita telah memperkenalkan formula umum untuk jujukan bagi pekali a_{i_m} yang berada dalam kembangan s_m untuk $i \leq 6$ melalui Teorem 2.2, 2.4, 2.6, 2.9, 2.11 dan Korolari 2.7, 2.12. Kesannya, kita dapat mengagak nilai r yang ganjil dan s yang genap dan ganjil dalam kembangan pseudoTNAF bermodulo $\rho(r + s\tau)$ untuk m yang tidak melebihi 12 sebelum transformasi $\frac{\tau^m-1}{\tau-1}$ kepada $r + s\tau$ dilaksanakan. Pada masa akan datang, kajian akan dilanjutkan

untuk mendapatkan formula umum untuk a_{i_m} ini untuk semua integer positif i. Dengan pendekatan ini, diharapkan formula umum $\tau^m = r_m + s_m\tau$ dapat diungkapkan.

PENGHARGAAN

Para penulis mengucapkan setinggi-tinggi penghargaan kepada Universiti Putra Malaysia kerana memberikan sokongan kewangan melalui Geran Putra GP/2018/9595400.

RUJUKAN

Ali, N.A., Yunos, F. and Jamal, N.H. (2016). A Total Norm of τ-Adic Non-Adjacent Form Occurring Among All Element of Z(τ): An Alternative Formula. Published by the American Institute of Physics.

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

D'Ooge, M. L., Robbins F. E. and Karpinski L. C. (1926). Nicomachus of Gerasa : Introduction to Arithmetic .University of Michigan Press. Reprint. Encyclopedia Britannica, Inc.

Gerasa, N. (1938). Introduction to Arithmetic. Translated by f. r. levin edn. London: Phanes Press. Published by Phanes Press, PO Box 61 14, Grand Rapids, Michigan 49516, USA.

Heuberger, C. and Krenn, D.: Retrieved 03/08/2012. Website, http://arxiv.org/abs/1009.0488.

Koblitz, N. (1987). Elliptic Curve Cryptosystem. Mathematics Computation, 48 (177), 203-209.

Koblitz, N. (1992). CM Curves with Good Cryptographic Properties. In Advances in cryptology CRYPTO 91 Proceedings, 576, 279-287.

Solinas, J. A. (1997). An Improved Algorithm for Arithmetic on a Family of Elliptic Curves. Advance in Cryptology-CRYPTO'97, 1294, 357-371.

Solinas, J.A. (2000). Efficient Arithmetic on Koblitz Curves. In Design, Codes and Cryptography, Solinas, J.A. (Ed). Springer, Boston, Massachusetts, 19, 195-249.

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. Advances In Industrial and Applied Mathematics, Proceedings of 23rd Malaysian National Symposium of Mathematical Sciences (SKSM23), 1750, 1-9.

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

Yunos, F., Mohd Atan, K.A., Md Said, M.R. and Kamel Ariffin, M.R. (2014). A Reduced τ -NAF (RTNAF) Representation for Scalar Multiplication on Anomalous Binary Curves (ABC). Pertanika Journal of Science and Technology, 22(2) Jul.2014, 489-506.

Yunos, F., Mohd Atan, K.A., Md Said, M.R. and Kamel Ariffin, M.R. (2015a). Pseudo τ-adic Non Adjacent Form for Scalar Multiplication on Koblitz Curves. Proceedings of the 4th International Conference on Cryptology and Information Security, Institute for Mathematical Research, Serdang, Malaysia, June 24-26, 2014, 120-130.

Yunos, F., Mohd Atan, K.A., Md Said, M.R. and Kamel Ariffin, M.R. (2015b). Pseudo τ-Adic Non-Adjacent Form for Scalar Multiplication on Koblitz Curves. Malaysian Journal of Mathematical Sciences 9(S) (Special Issue: The 4th International Cryptology and Information Security Conference 2014), 71-88.

Yunos, F. and Mohd Atan, K.A. (2016). Improvement to Scalar Multiplication on Koblitz Curves by Using Pseudo T-Adic Non-Adjacent Form. Advances in Industrial and Applied Mathematics. Proceedings of 23rd Malaysian National Symposium of Mathematical Sciences (SKSM23), AIP Publishing, 1750, 1-8.

Yunos, F. and Suberi, S. (2018). Even and Odd Nature for Pseudo τ-adic Non-adjacent Form. Malaysian Journal of Science, 37, 94-102.

Yunos, F., Suberi, S.M., Said Husain, Sh.K., Ariffin, M.R.K. and Asbullah, M.A. (2019). On Some Specific Patterns of τ-Adic Non-Adjacent Form Expansion over Ring Z (τ). Journal of Engineering and Applied Sciences, Medwell Journals, 1-6.

NIST. Retrieved July 2013, Website, http://nvlpubs.nist.gov/nistpubs/FIPS/-NIST.FIPS.186-4.pdf

Lampiran A

Contoh A1. Dapatkan TNAF bagi $1-4\tau$ sepertimana berikut.

Pertimbangkan $\bar{n} = 1-4\tau$ dan $\bar{\tau} = 1-\tau$ adalah konjugat bagi τ. Pertama sekali, $\tau \cdot \bar{\tau} = 2$ ditunjukkan:

$\tau \cdot \bar{\tau} = -\tau^2 + \tau = -\tau + 2 + \tau = 2.$

Diikuti pula dengan langkah seterusnya bagi memperolehi TNAF $(1-4\tau)$ sehinggalah hasil pembahagiannya 0:

Langkah 1: Hasil pembahagian $1-4\tau$ oleh τ tidak berada dalam $Z(\tau)$*:*

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

Oleh itu, kita diberi pilihan untuk memilih baki pertama $c_0 = \pm 1$ supaya $1-4\tau-c_0$ boleh dibahagikan dengan τ:

Jika $c_0 = -1$ maka $\frac{1-4\tau+1}{\tau} = -4 + \frac{2}{\tau}\cdot\frac{\bar{\tau}}{\bar{\tau}} = -4 + (1-\tau) = -3-\tau \in Z(\tau)$ (A1.1)

atau jika $c_0 = 1$ maka $\frac{1-4\tau-1}{\tau} = -4 \in \mathrm{Z}(\tau).$ (A1.2)

Pilih salah satu daripada c_0 di atas supaya pembahagian seterusnya iaitu

$\frac{-3-\tau}{\tau} = \frac{-3}{\tau} - 1 = \frac{-3}{\tau}\frac{\bar{\tau}}{\bar{\tau}} - 1 = \frac{-5}{2} + \frac{3}{2}\tau \notin Z(\tau)$ (A1.3)

atau $\frac{-4}{\tau} = \frac{-4}{\tau}\cdot\frac{\bar{\tau}}{\bar{\tau}} = \frac{-4\cdot(1-\tau)}{2} = -2 + 2\tau \in Z(\tau)$ (A1.4)

menghasilkan unsur yang berada dalam $Z(\tau)$. Oleh itu, kita memilih $c_0 = 1$ disebabkan oleh (A1.1) dan tuliskan $\mathrm{TNAF}(1-4\tau) = [1, c_1, c_2, \dots, c_{l-2}, c_{l-1}]$. Seterusnya kita memilih baki kedua $c_1 = 0$ disebabkan (A1.4) dan tuliskan $\mathrm{TNAF}(1-4\tau) = [1, 0, c_2, \dots, c_{l-2}, c_{l-1}]$.

Langkah 2: Pembahagian $-2+2\tau$ oleh τ menghasilkan unsur yang berada dalam $Z(\tau)$:

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

Oleh itu, pilih baki ketiga $c_2 = 0$ dan tuliskan $\mathrm{TNAF}(1-4\tau) = [1,0,0, c_3, c_4, \dots, c_{l-2}, c_{l-1}]$.

Langkah 3: Oleh kerana $1+\tau$ tidak boleh dibahagikan oleh τ maka pilih baki keempat $c_3 = \pm 1$ supaya $1+\tau-c_3$ boleh dibahagikan dengan τ:

Jika $c_3 = -1$ maka

$\frac{1+\tau+1}{\tau} = \frac{2+\tau}{\tau} = \frac{2}{\tau}\cdot\frac{\bar{\tau}}{\bar{\tau}} + 1 = 2 - \tau \in Z(\tau)$ (A1.5)

atau jika $c_3 = 1$ maka

$\frac{1+\tau-1}{\tau} = 1 \in Z(\tau).$ (A1.6)

Pilih salah satu daripada c_0 di atas supaya pembahagian seterusnya iaitu

$\frac{2-\tau}{\tau} = \frac{2}{\tau} - 1 = -\tau \in Z(\tau)$ (A1.7)

atau

$$\frac{1}{\tau} = \frac{1}{\tau} \cdot \frac{\bar{\tau}}{\bar{\tau}} = \frac{1}{2} - \frac{\tau}{2} \notin Z(\tau) \qquad \text{(A1.8)}$$

menghasilkan unsur yang berada dalam $Z(\tau)$. Oleh itu, kita memilih $c_3 = -1$ Disebabkan oleh (A1.5) dan tuliskan TNAF$(1 - 4\tau) = [1,0,0,-1, c_4, \dots, c_{l-2}, c_{l-1}]$. Kemudian, pilih baki kelima, $c_4 = 0$ disebabkan oleh (A1.7) dan tuliskan TNAF $(1 - 4\tau) = [1,0,0,-1,0, c_5, \dots, c_{l-2}, c_{l-1}]$.

Langkah 4: Oleh kerana $-\tau$ boleh dibahagikan oleh :

$$\frac{-\tau}{\tau} = \frac{-\tau}{\tau} \cdot \frac{\bar{\tau}}{\bar{\tau}} = -1.$$

maka baki keenam $c_5 = 0$ dan tuliskan TNAF$(1 - 4\tau) = [1,0,0,-1,0,0, c_6, \dots, c_{l-2}, c_{l-1}]$.

Langkah 5: Oleh kerana -1 tidak boleh dibahagikan oleh τ maka $c_6 = -1$:

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

Oleh itu, kita diberi pilihan untuk memilih baki ketujuh, $c_6 = \pm 1$ supaya $-1 - c_0$ boleh dibahagikan dengan τ:

Jika $c_6 = -1$ maka $\frac{-1+1}{\tau} = 0$ atau jika $c_6 = 1$ maka $\frac{-1-1}{\tau} = -\frac{2}{\tau} \cdot \frac{\bar{\tau}}{\bar{\tau}} = -1 + \tau$.

Kita memilih $c_6 = -1$ disebabkan hasil pembahagian $-1 - c_0$ oleh τ adalah 0 dan ditulis TNAF$(1 - 4\tau) = [1,0,0,-1,0,0,-1] = 1 - \tau^3 - \tau^6$. Ianya bersaiz tujuh digit dan berpemberat Hamming empat.