**Ratio Mathematica** Volume 42, 2022

# A study on the number of edges of some families of graphs and generalized Mersenne numbers

Sreekumar K G*
Ramesh kumar P†
Manilal K ‡

**Abstract**

The relationship between the Nandu sequence of the SM family of graphs and the generalized Mersenne numbers is demonstrated in this study. The sequences obtained from the peculiar number of edges of SM family of graphs are known as Nandu sequences. Nandu sequences are related to the two families of SM sum graphs and SM balancing graphs. The SM sum graphs are established from the inherent relationship between powers of 2 and natural numbers, whereas the SM balancing graphs are linked to the balanced ternary number system. In addition, some unusual prime numbers are discovered in this paper. These prime numbers best suit as an alternate for the Mersenne primes in the case of the public key cryptosystem.

**Keywords**: $n^{th}SM$ balancing graphs, $n^{th}SM$ sum graphs, Nandu Sequence, generalized Mersenne numbers, bipartite Kneser type-1 graphs.
**2020 AMS subject classifications**: $05C99$, $40A30$.[1]

*Department of Mathematics, University of Kerala, Thiruvananthapuram, India; sreekumar3121@gmail.com.

†Department of Mathematics, University of Kerala, Thiruvananthapuram, India; ramesh.ker64@gmail.com.

‡Department of Mathematics, University College, University of Kerala, Thiruvananthapuram, India.; manilalvarkala@gmail.com.

[1]Received on January 12th, 2022. Accepted on May 12th, 2022. Published on June 30th, 2022. doi: 10.23755/rm.v39i0.704. ISSN: 1592-7415. eISSN: 2282-8214. ©The Authors. This paper is published under the CC-BY licence agreement.

# 1 Introduction

In computer science, number systems and related ideas are used, particularly in cryptography. The binary number system, which is used in binary computers, and the balanced ternary number system, which is used in ternary computers, are two number systems used in computers. The balanced ternary number system was used in the Russian SETUN computer. Graph theory is used to investigate the combinatorial structure of these two number systems. SM sum graphs and SM balancing graphs are the two categories of graphs based on these number systems that we will focus on here. These graphs are groups of graphs that have been structured in a specific order. SM family of graphs consists of SM sum graph, SM balancing graphs and its complement graphs. For large values of n, these graphs are all non-asymmetric graphs [10] with bigger automorphism groups. The properties of these graphs lead to the discovery of some classical sequences. These sequences are called Nandu sequences or Ne-sequences. These Nandu sequences have a relation with Mersenne primes as well as generalized Mersenne numbers [8]. Furthermore, this is related to the low weight polynomial form of integers [4] which was used in elliptical curve cryptography. The Residue Number System (RNS) [2, 3] has an important role in modular multiplications in computer science. This RNS modular multiplication is used in the prime field based in elliptic curve cryptosystems too. Generalized Mersenne numbers are used in RNS modular multiplication for more efficiency. The newly defined sequence $\{\aleph_n\}$ in this paper are the particular cases of the generalized Mersenne numbers. At present, the modular multiplication requires a maximum of modulus 521. Eventually, the relationship between the Nandu sequence and the generalized Mersenne numbers are established in this work. The use of this relationship in elliptic curve cryptography is yet to be worked out. Also, a study on Mersenne primes in real quadratic fields was done by Sushma Palimar and B.R. Shankar [6]. The primality testing of large numbers in Maple was given in the work of S.Y.Yan [12]. A study on low weight polynomial form of integers for efficient modular multiplication was done by Jaewook Chung and M.Anwar Hasan [4]. A study on generalized double Fibonomial numbers was done by Mansi shah and Devbhadra Shah [7].
In this paper, we established some properties of Nandu sequences. The Nandu sequence $\{Nt_{\sum_n}\}$ for $SM(\sum_n)$ satisfies the recurrence relation $Nt_{\sum_{n+1}} = 2Nt_{\sum_n} + 2^n + n - 1$, $Nt_{\sum_2} = 2$. Let $\aleph_n = \dfrac{Nt_{B_n} - Nt_{\sum_n}}{n}$, where $Nt_{B_n}$ is the Nandu sequence of $SM(B_n)$. We derived a closed form of the generating function of the sequence $\aleph_n$ and is given by $G(x) = \sum_{r=0}^{n-2} 2^{n-2}\left(\frac{3}{2}\right)^r x^r$. The convergence of $\sum \dfrac{1}{\aleph_n}$ is then obtained.
Some preliminaries are given below.

# 2 Preliminary

In this section, we provide the basic definitions and some results from the related work mainly from [9, 10]. We begin with the definition of SM families of graphs. Let's look at how SM balancing graphs are defined [9]. Consider the set $T_n = \{3^m : \text{m is an integer, } 0 \leq m \leq n-1\}$ for a fixed positive integer $n \geq 2$. Let $I = \{-1, 0, 1\}$. Let $x \leq \frac{1}{2}(3^n - 1)$ be any positive integer which is not a power of 3. Then $x$ can be expressed as

$$x = \sum_{j=1}^{n} \alpha_j y_j, \tag{1}$$

where $\alpha_j \in I$, $y_j \in T_n$ and $y_j's$ are distinct. Each $y_j$ such that $\alpha_j \neq 0$ is called a balancing component of $x$. Consider the simple digraph $G = (V, E)$, where $V = \{v_1, v_2, \ldots, v_{\frac{1}{2}(3^n-1)}\}$ and adjacency of vertices is defined by: for any two distinct vertices $v_x$ and $v_{y_j}$, $(v_x, v_{y_j}) \in E$ if (1) holds and $\alpha_j = -1$, and $(v_{y_j}, v_x) \in E$ if (1) holds and $\alpha_j = 1$. This digraph $G$ is called the $n^{th} SMD$ balancing graph, denoted by $SMD(B_n)$. Its underlying undirected graph is called the $n^{th}$ SM balancing graph, denoted by $SM(B_n)$. Let us now look at the definition of SM sum graphs. If $p < 2^n$, is a positive integer which is not a power of 2, then $p = \sum_1^n x_i$, with $x_i = 0$ or $2^m$, for some integer *m*, $0 \leq m \leq n-1$ and $x_i$'s are distinct. Here each $x_i \neq 0$ is called an additive component of $p$. For a fixed integer $n \geq 2$, the simple graph $SM(\sum_n)$, called $n^{th}$ SM sum graph [9], is a graph with vertex set $\{v_1, v_2, \ldots, v_{2^n-1}\}$ and adjacency of vertices defined by, $v_i$ and $v_j$ are adjacent if either $i$ is an additive component of $j$ or $j$ is an additive component of $i$.

In $SM(\sum_n)$, degree of the vertex $v_{2^n-1}$ is $n$ and $\sum\limits_{v \in V} deg\ v = 2n(2^{n-1} - 1)$. In $SM(B_n)$, the number of vertices is $\frac{1}{2}(3^n - 1)$ and $\sum\limits_{v \in V} deg\ v = 2n(3^{n-1} - 1)$.
Note: For a fixed integer $n \geq 2$, let $T_n = \{3^m : \textit{m} \text{ is an integer, } 0 \leq m \leq n-1\}$, $N = \{1, 2, 3, \ldots, t\}$, where $t = \frac{1}{2}(3^n - 1)$. Also, let $P_n = \{2^m : \textit{m} \text{ is an integer, } 0 \leq m \leq n-1\}$, $M = \{1, 2, 3, \ldots, 2^n - 1\}$. Then consider $P_n^c = M - P_n$ , $T_n^c = N - T_n$ throughout this paper unless otherwise specified.

The Hamming weight of a string was defined as the number of 1's in the strings of 0 and 1. Here the number of additive components gives the Hamming weight of string (binary) representation of all numbers in $P_n^c$. The Hamming weight of string (binary) representation of numbers in $P_n$ is always 1.

### Bipartite Kneser type-1 graphs

Let $\mathscr{S}_n = \{1, 2, \cdots, n\}$, for an integer $n > 1$. For any two integers $k \geq 1$ and $n \geq 2k + 1$, the bipartite Kneser graph [10] $H(n, k)$ has all the $k$-element subsets and all the $(n - k)$-element subsets of $\mathscr{S}_n$ as vertices, and two vertices are adjacent if and only if one of them is a subset of the other. Here we define the bipartite Kneser type-1 graph as follows.

**Definition 2.1.** *[10] Let $\mathscr{S}_n = \{1, 2, 3, \ldots, n\}$ for a fixed integer $n > 1$. Let $\phi(\mathscr{S}_n)$ be the set of all non-empty subsets of $\mathscr{S}_n$. Let $V_1$ be the set of 1- element subsets of $\mathscr{S}_n$ and $V_2 = \phi(\mathscr{S}_n) - V_1$. Define a bipartite graph with adjacency of vertices as: a vertex $A \in V_1$ is adjacent to a vertex $B \in V_2$ if and only if $A \subset B$. This graph is called a bipartite Kneser type-1 graph.*

This bipartite Kneser type-1 graph is isomorphic to the graph $SM(\sum_n)$ for each $n$. To study the structure of the bipartite Kneser type-1 graph, we can make use of $SM(\sum_n)$ graph. The automorphism groups of the bipartite Kneser type-1 graphs are isomorphic to the symmetric group $S_n$ for each $n > 2$.

## 3 Nandu sequences of $SM(\sum_n)$ and $SM(B_n)$

The Nandu sequence or Ne-sequence $\{Nt_m\}_{m=1}^{n-1}$ of SM graphs are the sequence of numbers whose terms are the half of the sum of degrees of the vertices of $SM(\sum_n)$ or $SM(B_n)$ for all $n \geq 2$. Here we assume $n \geq 2$ for both the SM sum graph and SM balancing graphs unless otherwise specified. Kinkar Das and I Gutman [5] estimated the Wiener index by means of number of vertices, number of edges, and diameter.

### 3.1 Nandu sequence for the graph $SM(\sum_n)$

**Definition 3.1.** *For the SM sum graph $SM(\sum_n)$, with vertex set $V = \{v_i : 1 \leq i \leq 2^n - 1\}$, the Nandu sequence $\{Nt_{\sum_n}\}$ is defined as a sequence with $n^{th}$ term as $Nt_{\sum_n} = \frac{1}{2} \sum_{v \in V} deg\ v$ and the sequence $\{DNt_{\sum_n}\}$ defined by $DNt_{\sum_n} = \sum_{v \in V} deg\ v$ as double Nandu sequence.*
*i.e.,* $\{Nt_{\sum_n}\} = 2, 9, 28, 75, 186, \ldots$ .

**Theorem 3.1.** *Let $\{Nt_{\sum_n}\}$ be the Nandu sequence for the SM sum graph $SM(\sum_n)$, $n \geq 2$. Then $Nt_{\sum_{n+1}} = 2Nt_{\sum_n} + 2^n + n - 1$, $Nt_{\sum_2} = 2$.*

*Proof.* Consider the graph $SM(\sum_n)$ with vertex set $V = \{v_i : 1 \leq i \leq 2^n - 1\}$. The Nandu sequence is $\{Nt_{\sum_n}\}$ with $Nt_{\sum_n} = \frac{1}{2}\sum_{v \in V} deg\ v$.

Then we have $Nt_{\sum_n} = n(2^{n-1} - 1)$.

$$\begin{aligned} Nt_{\sum_{n+1}} &= (n+1)(2^n - 1) \\ &= n(2^n - 1) + 2^n - 1 \\ &= 2n(2^{n-1} - 1) + 2^n - 1 + n \\ &= 2Nt_{\sum_n} + 2^n + n - 1. \end{aligned}$$

Hence proved. □

**Theorem 3.2.** *Let $Nt_{\sum_n}$ be a Nandu sequence of SM Sum graph. Then the following holds.*

1. *$Nt_{\sum_n}$ is a composite number for all $n > 2$ and is always divisible by n.*
2. *If $\frac{Nt_{\sum_n}}{n}$ is a prime, then $n - 1$ is a prime.*
3. *$\frac{1}{2n}\sum_{v \in V} deg\ v = \frac{Nt_{\sum_n}}{n}$ is a Mersenne number.*
4. *$\frac{Nt_{\sum_n}}{n}$ gives the number of times each element of $P_n$ is used to make numbers in $P_n^c$, the complement of $P_n$ for a fixed n.*

*Proof.* The proof is obvious from the definition of the sequence $Nt_{\sum_n}$. □

**Definition 3.2.** *Let $V$ be the vertex set of $G = SM(\sum_n)$. Let $\Delta$ be the maximum degree of $G$ and $\delta$ be the minimum degree of $G$. The vertex degree polynomial of G is given by $Deg(G, x) = \sum_{m=\delta}^{\Delta} deg(G, m) \cdot x^m = \sum_{k=2}^{n} \binom{n}{k} x^k + n \cdot x^{2^{n-1}-1}$, where $deg(G, m)$ is the number of vertices of degree $m$.*

Let $G = SM(\sum_n)$ be an SM sum graph with vertex set $V$. The derivative of $Deg(G, x)$ at $x = 1$ is $DNt_{\sum_n}$, the $(n-1)^{th}$ term of the double Ne-sequence of $G$.

Now let us see the summation of terms of Nandu Sequence of SM sum graph. Let $\{Nt_{\sum_n}\}$, where $Nt_{\sum_n} = \frac{1}{2}\sum_{v \in V} deg\ v$, be the Nandu sequence for the SM sum graphs. Then its summation is given by $\sum_{r=1}^{n} Nt_{\sum_r} = n2^{n+1} - \frac{n(n+1)}{2} - n$.

**Lemma 3.1.** *[9] If $G = SM(\sum_n)$, $P_n = \{2^m : m \text{ is an integer}, 0 \leq m \leq n-1\}$, then*

$$d(v_i, v_j) = \begin{cases} 1 & \text{if } i \text{ is an additive component of } j \text{ or } j \text{ is an additive component of } i, \\ 2 & \text{if } i, j \in P_n \text{ or } i, j \notin P_n, \ i \text{ and } j \text{ have at least one common additive component}, \\ 3 & \text{if neither } i \text{ nor } j \text{ is an additive component but exactly one of them belongs to } P_n, \\ 4 & \text{if } i, j \notin P_n, \ i \text{ and } j \text{ have no common additive components}. \end{cases}$$

**Proposition 3.1.** *[9] Let $G = SM(\sum_n)$ be an $n^{th}$ $SM$ sum graph. Let $d_r(v_i, v_j)$ denote the number of unordered pairs of vertices for which $d(v_i, v_j) = r$. Then*

$$d_r(v_i, v_j) = \begin{cases} n.(2^{n-1} - 1) & \text{if } r = 1, \\ \dfrac{n(n-1)}{2} + \left[ \dfrac{(2^n - n - 2)(2^n - n - 1)}{2} - \delta_n \right] & \text{if } r = 2, \\ (n+1) \cdot 2^n - (n+2)2^{n-1} - n^2 & \text{if } r = 3, \\ \delta_n & \text{if } r = 4, \end{cases}$$

*where* $\delta_n = \dfrac{1}{2} \sum_{r=2}^{n-2} \left[ \binom{n}{r} \sum_{k=2}^{n-2} \binom{n-r}{k} \right]$.

**Remark 3.1.** *For $n = 2$ or 3, we get that $\delta_n = 0$. In these cases, the diameter of the graph $SM(\sum_n)$ is 2 or 3.*

**Theorem 3.3.** *Suppose $G = SM(\sum_n)$ $n \geq 2$ be an $n^{th}$ $SM$ sum graph. The $(n-1)^{th}$ term of the Nandu sequence is equal to $d_1(v_i, v_j)$, where $v_i v_j$ is an edge of G.*

*Proof.* The proof follows from Proposition 3.1 . □

## 3.2 Nandu sequence for the graph $SM(B_n)$

We introduced two new sequences, called Nandu sequence and Double Nandu sequence for the SM balancing graphs also. Here we discuss some of their properties.

**Proposition 3.2** ([9])**.** *For the $n^{th}$ $SM$ Balancing graph $SM(B_n)$, let $d_r(v_i, v_j)$ be the number of unordered pairs of vertices for which $d(v_i, v_j) = r$. Let $t = \frac{1}{2}(3^n - 1)$. Then*

$$d_r(v_i, v_j) = \begin{cases} n \cdot (3^{n-1} - 1) & \text{if } r = 1, \\ \dfrac{n(n-1)}{2} + \left[ \dfrac{(t-n)(t-n-1)}{2} - \sigma_n \right] & \text{if } r = 2, \\ \frac{1}{2}(n \cdot 3^{n-1} + n - 2n^2) & \text{if } r = 3, \\ \sigma_n & \text{if } r = 4, \end{cases}$$

*where* $\sigma_n = \frac{1}{2}\sum_{r=2}^{n-2}\left[\binom{n}{r}\sum_{k=2}^{n-2}\binom{n-r}{k}2^{r+k-2}\right]$.

**Definition 3.3.** *Consider the SM balancing graph* $SM(B_n)$, $n \geq 2$ , *with vertex set* $V = \{v_i : 1 \leq i \leq \frac{1}{2}(3^n - 1)\}$. *The sequence* $\{Nt_{B_n}\}$ *with* $Nt_{B_n} = \frac{1}{2}\sum_{v\in V} deg\ v$ *is called the Nandu sequence and the sequence* $\{DNt_{B_n}\}$ *defined by* $DNt_{B_n} = \sum_{v\in V} deg\ v$ *is called the double Nandu sequence.*
$i.e.,\{Nt_{B_n}\} = 4, 24, 104, 400, 1452, \ldots$ .

**Definition 3.4.** *Let* $G = SM(B_n)$ *with vertex set* $V$. *Let* $\Delta$ *be the maximum degree of* $G$ *and* $\delta$ *be the minimum degree of* $G$. *The vertex degree polynomial of G is given as*

$$\begin{aligned} Deg(G,x) &= \sum_{m=\delta}^{\Delta} deg(G,m)\cdot x^m \\ &= \sum_{k=2}^{n} 2^{k-1}\binom{n}{k}x^k + n\cdot x^{3^{n-1}-1}. \end{aligned}$$

**Example 3.1.** *For* $n = 5$, $Deg(G,x) = 16x^5 + 40x^4 + 40x^3 + 20x^2 + 5x^{80}$.

**Theorem 3.4.** *Let* $G = SM(B_n)$ *be a SM balancing graph with vertex set* $V$. *The derivative of* $Deg(G,x)$ *at* $x = 1$ *is* $DNt_{B_n}$, *the* $(n-1)^{th}$ *term of the double Ne-sequence of* $G$.

*Proof.* Let $Deg(G,x)'$ be the derivative of $Deg(G,x)$ $w.r.to\ x$.

$$\begin{aligned} Deg(G,x)' &= n(2x+1)^{n-1} - n + n\cdot(3^{n-1}-1)\cdot x^{3^{n-1}-2} \\ \text{Hence, } Deg(G,1)' &= n\cdot 3^{n-1} - n + n\cdot(3^{n-1}-1) \\ &= 2n(3^{n-1}-1) \\ &= DNt_{B_n}. \end{aligned}$$

□

Here we provide the summation for the Nandu sequence of SM balancing graphs.

Let $\{Nt_{B_n}\}$, where $Nt_{B_n} = \frac{1}{2}\sum_{v\in V} deg\ v$, be the Nandu sequence for the SM balancing graphs. Then $\sum_{r=1}^{n} Nt_{B_r} = \frac{3}{4}\left[2n\cdot 3^n + 3^n - 1\right] - n - \frac{n(n+1)}{2}$.

**Theorem 3.5.** *Let* $SM(B_n)$ *be the* $n^{th}$ *SM balancing graph and* $Nt_{B_n}$ *be the Nandu sequence. Then* $Nt_{Bn+1} = 3Nt_{Bn} + 3^n + 2n - 1$, $Nt_{B_2} = 4$, *for all* $n \geq 2$.

*Proof.* Consider the graph $SM(B_n)$.
Then we have $Nt_{B_n} = n(3^{n-1} - 1)$, $Nt_{B_2} = 4$.
For all $n \geq 2$,

$$\begin{aligned} Nt_{B_{n+1}} &= (n+1)(3^n - 1) \\ &= n(3^n - 1) + 3^n - 1 \\ &= 3n(3^{n-1} - 1) + 3^n - 1 + n \\ &= 3Nt_{B_n} + 3^n + 2n - 1. \end{aligned}$$

Hence proved. □

# 4 Relationship between Nandu sequence and generalized Mersenne numbers

Mersenne numbers are numbers of the form $M_n = 2^n - 1$. If a Mersenne number is prime, then $n$ is a prime. But the converse is not true. Mersenne numbers are a particular case of a larger class of numbers, the generalized Mersenne numbers [11], $G_{a,n} = a^n - (a-1)^n$ characterised by their base $a$ and exponent $n$. The idea of generalized Mersenne numbers was introduced by Solinas [8] in 1999 for the use in elliptic curve cryptography. The use of generalised Mersenne numbers in modular arithmetic to perform fast modular multiplications is well known.

**Theorem 4.1.** *Let $Nt_{B_n}$ and $Nt_{\sum_n}$ be the terms of the Nandu sequence of SM balancing graph and SM sum graph respectively. Then $Nt_{B_n} - Nt_{\sum_n} = n(3^{n-1} - 2^{n-1})$.*

*Proof.* The proof follows from the definition of Nandu sequences of SM sum graph and SM balancing graphs. □

**Definition 4.1.** *Let $SM(\sum_n)$ and $SM(B_n)$ be the SM sum graphs and SM balancing graphs respectively, $n \geq 3$. Then the sequence $\{\aleph_n\}$ is defined as $\aleph_n = \dfrac{Nt_{B_n} - Nt_{\sum_n}}{n}$.*

**Theorem 4.2.** *For $n \geq 3$ and when n is odd, $\aleph_n \equiv 0(\mod 5)$*

*Proof.* We have $\aleph_n = \dfrac{Nt_{B_n} - Nt_{\sum_n}}{n} = 3^{n-1} - 2^{n-1}$

Since $n$ is odd, then $n - 1$ is even, say $n - 1 = 2m$, for some integer $m$.
Also, $3^{n-1} - 2^{n-1} = 3^{2m} - 2^{2m}$, which is a multiple of 5. Hence proved. □

**Theorem 4.3.** $\sum \dfrac{1}{\aleph_n}$ *converges.*

*Proof.* Suppose $SM(\sum_n)$ and $SM(B_n)$ be the SM sum graphs and SM balancing graphs respectively. Then we have the sequence $\{\aleph_n\}$ as $\aleph_n = \dfrac{Nt_{B_n} - Nt_{\sum_n}}{n}$.

$$\begin{aligned} Therefore \quad \aleph_n &= 3^{n-1} - 2^{n-1} \\ &= (3-2)(3^{n-2} + 3^{n-3} \cdot 2 + \cdots + 2^{n-2}) \\ &\geq 2^{n-2} + 2^{n-2} + \cdots + 2^{n-2} \\ &= (n-1) \cdot 2^{n-2} \end{aligned}$$

$$\text{But} \quad \frac{1}{3^{n-1} - 2^{n-1}} \leq \frac{1}{(n-1).2^{n-2}} = \frac{4}{(n-1) \cdot 2^n}.$$

Now consider the series $\sum \dfrac{1}{(n-1) \cdot 2^n}$. We have $2^n > n-1$ , for $n \geq 3$.

To check the convergence of $\sum \dfrac{1}{(n-1) \cdot 2^n}$ , it is enough to check the convergence of $\sum \dfrac{1}{(n-1)^2}$. But $\sum \dfrac{1}{(n-1)^2}$ is convergent. Therefore, by comparison test, $\sum \dfrac{1}{\aleph_n}$ converges. □

**Theorem 4.4.** *Let $SM(\sum_n)$ and $SM(B_n)$ be the SM sum graphs and SM balancing graphs. Then $\aleph_{n+1} = 2\aleph_n + 3^{n-1}$, for all $n \geq 2$, given $\aleph_2 = 1$.*

*Proof.* Consider the graph $SM(\sum_n)$ and $SM(B_n)$.
Then we have $\aleph_n = \dfrac{Nt_{B_n} - Nt_{\sum_n}}{n}$.

$$\begin{aligned} \aleph_{n+1} &= 3^n - 2^n \\ &= 3.3^{n-1} - 2.2^{n-1} \\ &= 2(3^{n-1} - 2^{n-1}) + 3^{n-1} \\ &= 2\aleph_n + 3^{n-1}. \end{aligned}$$

Hence proved. □

**Lemma 4.1.** *A closed form of the generating function of the sequence $\aleph_n$ is given by $G(x) = \sum_{r=0}^{n-2} 2^{n-2} \left(\frac{3}{2}\right)^r x^r$.*

*Proof.* We have $\aleph_{n+1} = 2\aleph_n + 3^{n-1}$, for all $n \geq 2$, given $\aleph_2 = 1$.
When $n = 2$,

$$\aleph_3 = 2\aleph_2 + 3$$
$$\aleph_4 = 2\aleph_3 + 3^2 = 2(2\aleph_2 + 3) + 3^2 = 2^2\aleph_2 + 2 \cdot 3 + 3^2$$
$$\text{Similarly, } \aleph_5 = 2\aleph_4 + 3^2 = 2^3\aleph_2 + 2^2 \cdot 3 + 2 \cdot 3^2 + 3^3$$
$$\aleph_6 = 2^4\aleph_2 + 2^3 \cdot 3 + 2^2 \cdot 3^2 + 2 \cdot 3^3 + 3^4.$$

Continuing in this way we get,
$\aleph_n = \sum_{r=0}^{n-2} 2^{n-2}\left(\frac{3}{2}\right)^r$

Therefore, the required generating function is $G(x) = \sum_{r=0}^{n-2} 2^{n-2}\left(\frac{3}{2}\right)^r x^r$. □

**Theorem 4.5.** *Let $SM(\sum_n)$ and $SM(B_n)$ be the SM sum graphs and SM balancing graphs. Then $\aleph_{n+1} = G_{3,n}$.*

**Theorem 4.6.** *If $\aleph_n$ is prime, then n is even. But the converse is not true.*

*Proof.* The proof follows from Theorem 4.2. □

**Definition 4.2.** *Let $SM(\sum_n)$ and $SM(B_n)$ be the SM sum graphs and SM balancing graphs. Then $\aleph_{n+1} = G_{3,n}$. For some values of n, $G_{3,n}$ is a prime. These prime numbers are called SM prime numbers.*

These prime numbers can be used to replace the Mersenne primes in the new public key cryptosystem introduced by D. Aggarwal, et al [1]. In their work, they propose a new public-key cryptosystem whose security is based on the computational intractability of the problem: Given a Mersenne number $p = 2^n - 1$, where $n$ is a prime, a positive integer $h$ and an $n$-bit integer H, decide whether there exist n-bit integers F, G each of Hamming weight less than $h$ such that $H = \frac{F}{G} modulo\ p$.

**Theorem 4.7.** *The series $\sum \frac{1}{Nt_{\sum_n}}$ and $\sum \frac{1}{Nt_{B_n}}$ converges.*

*Proof.* We have for $n \geq 3$, $2^n - 1 > n$. So $\sum \frac{1}{n(2^n-1)} \leq \frac{1}{n^2}$. As $\sum \frac{1}{n^2}$ is convergent, $\sum \frac{1}{n(2^n-1)}$ =$\sum \frac{1}{Nt_{\sum_n}}$ is convergent.
The same way $\sum \frac{1}{Nt_{B_n}}$ also converges. Hence proved. □

We observed that $\aleph_n$ is always an odd number and is a prime when $n = 3, 4, 6, 18, 30$ and $32$ so on. There exists $G_{3,n}$ primes. Currently, the largest modulus required for modular multiplication is 521. For $n = 6$, $\aleph_n = 665$.
Consider the function $A_{G_{3,n}}(x)$ as a function which gives the number of SM primes among the $G_{3,n}$ generalized Mersenne numbers which are less than or equal to the corresponding $\aleph_n$. We get that for $n = 2$, $A_{G_{3,n}}(x) = 1$, for $n = 3$, $A_{G_{3,n}}(x) = 2$, for $n = 4$, $A_{G_{3,n}}(x) = 3$ and for $n = 5$, $A_{G_{3,n}}(x) = 3$ etc.
In fact the sum of degrees of vertices $v_x$, $x \in T_n^c$ minus the sum of degrees of vertices $v_x$, $x \in P_n^c$ is the same as the sum of degrees of vertices $v_x$, $x \in T_n$ minus the sum of degrees of vertices $v_x$, $x \in P_n$. If these difference on either side is divided by $n$, then the quotient is equal to the $\aleph_n$.

**Theorem 4.8.** *If $p_1, p_2, p_3, ..., p_n$ are some odd prime numbers, then $P = \prod_{i=1}^{n} p_i$ is having 1 as an additive component.*

*Proof.* Since $p_1, p_2, p_3, ..., p_n$ are odd prime numbers, each is having 1 as an additive component. Then clearly $P = \prod_{i=1}^{n} p_i$ also has 1 as an additive component. This proves the theorem. □

**Corolary 4.1.** *Let the number of odd prime numbers less than $2^n$ be denoted by $N(\beta)$. Then $N(\beta) \leq 2^{n-1} - 1$ for all $n \geq 3$.*

# 5 Conclusion

The Nandu sequences of the two SM families of graphs were examined, and a relation between these sequences and the generalized Mersenne numbers was established. As a consequence, we have a new sequence of integers called $G_{3,n}$, which is a type of generalized Mersenne number that may be employed in elliptical curve cryptography. These sequences are important in using a graph theory method to investigate the nature and structure of the two number systems - binary and balanced ternary. It has been noted that the $(n-1)^{th}$ term of the Nandu sequence of $SM(\sum_n)$ is identical to unordered pairs of vertices which are at distance one. The $\aleph n$ functions can be studied further in relation to elliptic curve cryptography.

## Conflict of Interest

The authors hereby declare that we have no potential conflict of interest.

# 6 Acknowledgements

The authors would like to thank the anonymous referee for their helpful comments which greatly improved the paper. This research has been promoted/supported by the University of Kerala, India.

# References

[1] Divesh Aggarwal, Antoine Joux, Anupam Prakash, and Miklos Santha, *A new public-key cryptosystem via mersenne numbers*, Annual International Cryptology Conference, Springer, 2018, pp. 459–482.

[2] J-C Bajard and Laurent Imbert, *A full rns implementation of rsa*, IEEE Transactions on computers **53** (2004), no. 6, 769–774.

[3] Jean-Claude Bajard, Marcelo Kaihara, and Thomas Plantard, *Selected rns bases for modular multiplication*, 2009 19th IEEE Symposium on Computer Arithmetic, IEEE, 2009, pp. 25–32.

[4] Jaewook Chung and M Anwar Hasan, *Low-weight polynomial form integers for efficient modular multiplication*, IEEE Transactions on Computers **56** (2006), no. 1, 44–57.

[5] Kinkar Ch Das and Ivan Gutman, *Estimating the wiener index by means of number of vertices, number of edges, and diameter*, MATCH Commun. Math. Comput. Chem **64** (2010), no. 3, 647–660.

[6] Sushma Palimar et al., *Mersenne primes in real quadratic fields*, arXiv preprint arXiv:1205.0371 (2012).

[7] Mansi Shah and Shah Devbhadra, *Generalized double fibonomial numbers*, Ratio Mathematica **40** (2021), 163.

[8] Jerome A Solinas et al., *Generalized mersenne numbers*, Citeseer, 1999.

[9] KG Sreekumar and K Manilal, *Hosoya polynomial and harary index of sm family of graphs*, Journal of information and optimization Sciences **39** (2018), no. 2, 581–590.

[10] ———, *Automorphism groups of some families of bipartite graphs*, Electronic Journal of Graph Theory and Applications **9** (2021), no. 1, 65–75.

[11] Tao Wu and Li-Tian Liu, *Elliptic curve point multiplication by generalized mersenne numbers*, Journal of electronic science and technology **10** (2012), no. 3, 199–208.

[12] SY Yan, *Primality testing of large numbers in maple*, Computers & Mathematics with Applications **29** (1995), no. 12, 1–8.