EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
2025, Vol. 18, Issue 4, Article Number 6605
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

On Generalized Mersenne Numbers and Extended Fermat Numbers

Shefa A. Bani Melhem[1,*], Ala'a Al-Kateeb[1,*], Afnan Dagher[1]

[1] *Department of Mathematics, Faculty of Science, Yarmouk University, Irbid, Jordan*

Abstract. In this paper, we study a generalization of Mersenne numbers and we introduce an extension of Fermat numbers, we find their generating functions binet formulas, related matrix representation and many other properties. Also, we provide some applications in cryptography.

2020 Mathematics Subject Classifications: 11B39, 11B83
Key Words and Phrases: Mersenne and Fermat numbers, generating function, Binet formula, key exchange and authentication protocols

1. Introduction

Fibonacci and Lucas integer sequences and their generalization/ extensions have many interesting properties and have been heavily studied [1–5]. The Fibonacci/ Lucas sequences are given by the following recurrence relations:

$$F_n = F_{n-1} + F_{n-2},\ L_n = L_{n-1} + L_{n-2}$$

where $n \geq 2, F_0 = 0, F_1 = 1$ and $L_0 = 2, L_1 = 1$. There are other Fibonacci and Lucas type sequences such as:

- Pell and Pell-Lucas numbers:

  $$P_n = 2P_{n-1} + P_{n-2}; Q_n = 2Q_{n-1} + Q_{n-2},$$

  where $n \geq 2, P_0 = 0, P_1 = 1, Q_0 = Q_1 = 1$.

- Jacobsthal and Jacobsthal-Lucas numbers:

  $$J_n = J_{n-1} + 2J_{n-2}; j_n = j_{n-1} + 2j_{n-2},$$

  where $n \geq 2, J_0 = 0, J_1 = 1, j_0 = j_1 = 2$.

*Corresponding author.
*Corresponding author.
DOI: https://doi.org/10.29020/nybg.ejpam.v18i4.6605

Email addresses: shefa.bm@yu.edu.jo (Sh. A. Bani Melhem),
alaa.kateeb@yu.edu.jo (Al-Kateeb), afnand@yu.edu.jo (A. Dagher)

All listed above sequences satisfy a set of common properties and identities, for example Binet formulas, Catalan and Cassini's identities. Recently, these sequences were generalized or extended by many authors. Mersenne numbers are given by the formula $M_n = 2^n - 1$ or using the recurrence relation $M_{n+2} = 3M_{n+1} - 2M_n$, where $n \geq 2, M_0 = 0$ and $M_1 = 1$. Also, Fermat numbers are given by $F_n = 2^{2^n} + 1$. Next we define the generalized Mersenne and extended Fermat numbers, which are the main interests of this paper.

Definition 1. *Let $k \geq 3, n \geq 2$ be two integers. We define the generalized Mersenne and extended Fermat numbers respectively by*

$$M_{k,n} = kM_{k,n-1} + (1-k)M_{k,n-2}, F_{k,n} = kF_{k,n-1} + (1-k)F_{k,n-2}$$

where $M_{k,0} = 0, M_{k,1} = 1$ and $F_{k,0} = 2, F_{k,1} = 3$.

Remark 1. *The sequence $M_{k,n}$ was introduced and studied before in [6].*

The search for Mersenne primes is an active field in number theory, since each even perfect number equals $2^{k-1}M_k$, where M_k is a prime Mersenne number. Fermat primes are useful in generating pseudo-random sequences of numbers an important application in computer science and cryptography, also they are important for some integer factorization algorithms like in [7, 8], the new defined sequences maybe used to improve such algorithms. In this paper we introduce and study a generalization to the Mersenne and extended Fermat numbers. This paper is structured as follows in section 2 we introduce the generalized Mersenne and extended Fermat numbers and derive their generating functions and Binet formulas, in section 3 we find more other properties, in section 4 we find the generating matrices of the generalized Mersenne and extended Fermat numbers, also we present some results involving Mersenne numbers and some tridiagonal and Hessenberg matrices, finally, in the last section we gave two applications of the generalized Mersenne numbers matrices in cryptography, namely we present a key-exchange protocol and an authentication scheme using matrices.

2. Basic Properties

Theorem 1 (Generating functions)**.** *The generating functions of the sequences $M_{k,n}$ and F_k, n respectively are*

(i) $M(x) = \frac{x}{1-kx+(k-1)x^2}$

(ii) $F(x) = \frac{2+(3-2k)x}{1-kx+(k-1)x^2}$

Proof. Let $M(x)$ represents the generating functions of $M_{k,n}$. Note,

$$M(x) = \sum_{n=0}^{\infty} M_{k,n}x^n$$

$$\begin{aligned}
&= M_{k,0} + M_{k,1}x + \sum_{n=2}^{\infty} M_{k,n}x^n \\
&= x + \sum_{n=2}^{\infty}(kM_{k,n-1} + (1-k)M_{k,n-2})x^n \\
&= x + kx\sum_{n=0}^{\infty} M_{k,n}x^n + (1-k)x^2\sum_{n=0}^{\infty} M_{k,n}x^n
\end{aligned}$$

Thus, $x = (1 - kx - (1-k)x^2)M(x) \Rightarrow M(x) = \frac{x}{1-kx+(k-1)x^2}$. Similarly we can prove the theorem for $F(x)$.

$$\begin{aligned}
F(x) &= \sum_{n=0}^{\infty} F_{k,n}x^n \\
&= F_{k,0} + F_{k,1}x + \sum_{n=2}^{\infty} F_{k,n}x^n \\
&= 2 + 3x + \sum_{n=2}^{\infty}(kF_{k,n-1} + (1-k)F_{k,n-2})x^n \\
&= 2 + 3x - 2kx + kx\sum_{n=0}^{\infty} F_{k,n}x^n + (1-k)x^2\sum_{n=0}^{\infty} F_{k,n}x^n
\end{aligned}$$

Thus, $2 + (3-2k)x = (1 - kx - (1-k)x^2)F(x) \Rightarrow F(x) = \frac{2+(3-2k)x}{1-kx+(k-1)x^2}$.

Theorem 2 (Binet formula)**.** *The n-th terms of the generalized Mersenne and extended Fermat sequences are given by*

$$M_{k,n} = \frac{(k-1)^n - 1}{k-2}$$

and

$$F_{k,n} = \frac{(k-1)^n + 2k - 5}{k-2}$$

Proof. A proof for $M_{k,n}$ can be found in [6], the formula for $F_{k,n}$ can be proved easily by induction.

Proposition 1. *For $n > 1$ we have $F_{k,n} = M_{k,n} + 2$*

Proof. Immediate from the Binet formulas.

Theorem 3 (Catalan's identity)**.** *We have*

- $M_{k,n-r}M_{k,n+r} - M_{k,n}^2 = -(k-1)^{n-r}M_{k,r}^2$
- $F_{k,n-r}F_{k,n+r} - F_{k,n}^2 = (2k-5)(k-1)^{n-r}M_{k,r}^2$

Proof.

- $$\begin{aligned} M_{k,n-r}M_{k,n+r} - M_{k,n}^2 &= \frac{(k-1)^{n-r}-1}{(k-2)}\frac{(k-1)^{n+r}-1}{(k-2)} - (\frac{(k-1)^n-1}{(k-2)})^2 \\ &= \frac{(k-1)^{2n} - (k-1)^{n-r} - (k-1)^{n+r} + 1}{(k-2)^2} - \frac{(k-1)^{2n} - 2(k-1)^n + 1}{(k-2)^2} \\ &= \frac{-(k-1)^{n-r} - (k-1)^{n+r} + 2(k-1)^n}{(k-2)^2} \\ &= -(k-1)^{n-r}\frac{1 + (k-1)^{2r} - 2(k-1)^r}{(k-2)^2} \\ &= -(k-1)^{n-r}M_{k,r}^2 \end{aligned}$$

- $$\begin{aligned} F_{k,n-r}F_{k,n+r} - F_{k,n}^2 &= \frac{(k-1)^{n-r}+2k-5}{k-2}\frac{(k-1)^{n+r}+2k-5}{k-2} - (\frac{(k-1)^n+2k-5}{k-2})^2 \\ &= \frac{(k-1)^{2n} + (2k-5)(k-1)^{n-r} + (2k+5)(k-1)^{n+r} + (2k+5)^2}{(k-2)^2} \\ &\quad - \frac{(k-1)^{2n} + 2(2k-5)(k-1)^n + (2k-5)^2}{(k-2)^2} \\ &= \frac{(2k-5)(k-1)^{n-r} + (2k+5)(k-1)^{n+r} - 2(2k-5)(k-1)^n}{(k-2)^2} \\ &= (2k-5)(k-1)^{n-r}\frac{1 + (k-1)^{2r} - 2(k-1)^r}{(k-2)^2} \\ &= (2k-5)(k-1)^{n-r}M_{k,r}^2. \end{aligned}$$

Theorem 4 (d'Ocagne's identity)**.** *If $\ell \geq n$, then*

- $M_{k,\ell}M_{k,n+1} - M_{k,\ell+1}M_{k,n} = (k-1)^n M_{k,\ell-n}$.
- $F_{k,\ell}F_{k,n+1} - F_{k,\ell+1}F_{k,n} = -(5-2k)(k-1)^n M_{k,\ell-n}$.

Proof.

- $$M_{k,\ell}M_{k,n+1} - M_{k,\ell+1}M_{k,n} = \frac{(k-1)^\ell - 1}{(k-2)}\frac{(k-1)^{n+1}-1}{(k-2)} - \frac{(k-1)^{\ell+1}-1}{(k-2)}\frac{(k-1)^n-1}{(k-2)}$$

$$= \frac{(k-1)^{\ell+1} - (k-1)^{\ell} - (k-1)^{n+1} + (k-1)^{n}}{(k-2)^2}$$
$$= \frac{(k-1)^{\ell}(k-2) - (k-1)^{n}(k-2)}{(k-2)^2}$$
$$= (k-1)^{n}\frac{(k-1)^{\ell-n} - 1}{k-2}$$
$$= (k-1)^{n} M_{k,\ell-n}$$

- $$F_{k,\ell}F_{k,n+1} - F_{k,\ell+1}F_{k,n} = \frac{(k-1)^{\ell} + 2k - 5}{(k-2)}\frac{(k-1)^{n+1} + 2k - 5}{(k-2)}$$
$$- \frac{(k-1)^{\ell+1} + 2k - 5}{(k-2)}\frac{(k-1)^{n} + 2k - 5}{(k-2)}$$
$$= (2k-5)\frac{-(k-1)^{\ell+1} + (k-1)^{\ell} + (k-1)^{n+1} - (k-1)^{n}}{(k-2)^2}$$
$$= (2k-5)\frac{(k-1)^{\ell}(2-k) + (k-1)^{n}(k-2)}{(k-2)^2}$$
$$= (2k-5)\frac{(k-1)^{n} - (k-1)^{\ell}}{(k-2)} = (2k-5)(k-1)^{n}\frac{1 - (k-1)^{\ell-n}}{(k-2)}$$
$$= -(5-2k)(k-1)^{n} M_{k,\ell-n}.$$

Theorem 5 (Vajda's identity)**.**

(i) (Formulation 1) $M_{k,n+i}M_{k,n+j} - M_{k,n}M_{k,n+i+j} = (k-1)^{n} M_{k,i}M_{k,j}$

(ii) (Formulation 2) $M_{k,n+j}M_{k,m-j} - M_{k,n}M_{k,m} = (k-1)^{n} M_{k,m-n-j}M_{k,j}$

Proof.

(i) (Formulation 1)

$$M_{k,n+i}M_{k,n+j} - M_{k,n}M_{k,n+i+j} = \frac{(k-1)^{n+i} - 1}{(k-2)}\frac{(k-1)^{n+j} - 1}{(k-2)} - \frac{(k-1)^{n} - 1}{(k-2)}\frac{(k-1)^{n+i+j} - 1}{(k-2)}$$
$$= \frac{(k-1)^{n} - (k-1)^{n+i} - (k-1)^{n+j} + (k-1)^{n+i+j}}{(k-2)^2}$$
$$= (k-1)^{n}\frac{1 - (k-1)^{i} - (k-1)^{j} + (k-1)^{i+j}}{(k-2)^2}$$
$$= (k-1)^{n}\frac{1 - (k-1)^{i} - (k-1)^{j}(1 - (k-1)^{i})}{(k-2)^2}$$

$$= (k-1)^n \frac{(1-(k-1)^i)(1-(k-1)^j)}{(k-2)^2}$$
$$= (k-1)^n M_{k,i} M_{k,j}$$

(ii) (Formulation 2)

$$M_{k,n+i}M_{k,m-j} - M_{k,n}M_{k,m} = \frac{(k-1)^{n+j}-1}{(k-2)}\frac{(k-1)^{m-j}-1}{(k-2)} - \frac{(k-1)^n-1}{(k-2)}\frac{(k-1)^m-1}{(k-2)}$$
$$= \frac{(k-1)^m - (k-1)^{m-j} - (k-1)^{n+j} + (k-1)^n}{(k-2)^2}$$
$$= (k-1)^n \frac{1-(k-1)^{m-n-j} + (k-1)^j((k-1)^{m-n-j}-1)}{(k-2)^2}$$
$$= (k-1)^n M_{k,m-n-j} M_{k,j}$$

Theorem 6 (Sum of terms)**.** *If $n \geq 2$, then*

(i) $\sum_{i=0}^{n} M_{k,i} = \frac{1}{k-2}(M_{k,n+1} - n - 1)$

(ii) $\sum_{i=0}^{n} F_{k,i} = \frac{1}{k-2}(F_{k,n+1} - 2 + (n+1)(2k-5)) = \frac{1}{k-2}(M_{k,n+1} + (n+1)(2k-5))$

(iii) $\sum_{i=0}^{n} M_{k,2i} = \frac{1}{k-2}(\frac{1}{k}M_{k,2(n+1)} - n - 1)$

(iv) $\sum_{i=0}^{n} F_{k,2i} = \frac{1}{k-2}(\frac{1}{k}M_{k,2(n+1)} + (n+1)(2k-5)) = \frac{1}{k-2}(\frac{1}{k}(F_{k,2(n+1)} - 2) + (n+1)(2k-5))$

Proof.

(i)

$$\sum_{i=0}^{n} M_{k,i} = \sum_{i=0}^{n} \frac{(k-1)^i - 1}{k-2}$$
$$= \frac{1}{(k-2)}\left(\frac{1-(k-1)^{n+1}}{2-k} - (n+1)\right), \text{ geometric series}$$
$$= \frac{1}{k-2}(M_{k,n+1} - n - 1)$$

(ii)

$$\sum_{i=0}^{n} F_{k,i} = \sum_{i=0}^{n} \frac{(k-1)^i + (2k-5)}{k-2}$$
$$= \frac{1}{(k-2)}\left(\frac{1-(k-1)^{n+1}}{2-k} + (n+1)(2k-5)\right), \text{ geometric series}$$
$$= \frac{1}{k-2}(F_{k,n+1} - 2 + (n+1)(2k-5)) = \frac{1}{k-2}(M_{k,n+1} + (n+1)(2k-5))$$

(iii)

$$\begin{aligned}\sum_{i=0}^{n} M_{k,2i} &= \sum_{i=0}^{n} \frac{((k-1)^2)^i - 1}{k-2} \\ &= \frac{1}{(k-2)} \left(\frac{1-((k-1)^2)^{n+1}}{1-(k-1)^2} - (n+1) \right), \text{ geometric series} \\ &= \frac{1}{(k-2)} \left(\frac{1-((k-1)^{2n+2}}{k(2-k)} - (n+1) \right) \\ &= \frac{1}{k-2} (\frac{1}{k} M_{k,n+1} - n - 1)\end{aligned}$$

(iv)

$$\begin{aligned}\sum_{i=0}^{n} F_{k,2i} &= \sum_{i=0}^{n} \frac{((k-1)^2)^i + (2k-5)}{k-2} \\ &= \frac{1}{(k-2)} \left(\frac{1-((k-1)^2)^{n+1}}{1-(k-1)^2} + (n+1)(2k-5) \right), \text{ geometric series} \\ &= \frac{1}{(k-2)} \left(\frac{1-((k-1)^{2n+2}}{k(2-k)} + (n+1)(2k-5) \right) \\ &= \frac{1}{k-2} (\frac{1}{k} M_{k,2(n+1)} + (n+1)(2k-5)) \\ &= \frac{1}{k-2} (\frac{1}{k} (F_{k,2(n+1)} - 2) + (n+1)(2k-5))\end{aligned}$$

Lemma 1. *We have* $\lim_{n\to\infty} \frac{M_{k,n+1}}{M_{k,n}} = k-1$.

Proof. $\lim_{n\to\infty} \frac{M_{k,n+1}}{M_{k,n}} = \lim_{n\to\infty} \frac{(k-1)^{n+1}-1}{k-2} \cdot \frac{k-2}{(k-1)^n-1} = \lim_{n\to\infty} \frac{(k-1)^{n+1}(1-\frac{1}{(k-1)^{n+1}})}{(k-1)^n(1-\frac{1}{(k-1)^n})} = k-1$

Lemma 2. *The series* $\sum_{n=0}^{\infty} \frac{1}{M_{k,n}}$ *is a convergent series.*

Proof. By ratio test $\lim_{n\to\infty} \frac{M_{k,n}}{M_{k,n+1}} = \frac{1}{k-1} < 1$, so the series is convergent,

Lemma 3. *The series* $\sum_{n=1}^{\infty} \frac{M_{k,n}}{k^n} = \frac{k}{k-1}$.

Proof. Let $S = \sum_{n=1}^{\infty} \frac{M_{k,n}}{k^n}$. Then

$$\sum_{n=1}^{\infty} \frac{M_{k,n}}{k^n} = \frac{1}{k} + \sum_{n=2}^{\infty} \frac{M_{k,n}}{k^n}$$

$$
\begin{aligned}
&= \frac{1}{k} + \sum_{n=1}^{\infty} \frac{M_{k,n+1}}{k^{n+1}} \\
&= \frac{1}{k} + \sum_{n=1}^{\infty} \frac{kM_{k,n} + (1-k)M_{k,n-1}}{k^{n+1}} \\
&= \frac{1}{k} + \sum_{n=1}^{\infty} \frac{M_{k,n}}{k^n} + \frac{(1-k)}{k^2} \sum_{n=1}^{\infty} \frac{M_{k,n-1}}{k^{n-1}} \\
&= \frac{1}{k} + S + \frac{(1-k)}{k^2} \sum_{n=0}^{\infty} \frac{M_{k,n}}{k^n} \\
&= \frac{1}{k} + S + \frac{(1-k)}{k^2} S
\end{aligned}
$$

Thus, $S = \frac{k}{k-1}$.

We need the next remark in the proof of the next theorem. In fact it is exercise 16 in section 3.3 in [9].

Remark 2. *For any three integers a, b and c such that $\gcd(a,b) = \gcd(a,c) = 1$, we have $\gcd(a, bc) = 1$*

Theorem 7. *For $n \geq 1$, we have*

(i) $\gcd(M_{k,n}, k-1) = 1$

(ii) $\gcd(M_{k,n}, k) = \begin{cases} 1, & \text{if } n \text{ is odd} \\ k, & \text{if } n \text{ is even} \end{cases}$

(iii) $\gcd(M_{k,n}, M_{k,n+1}) = 1$

(iv) $\gcd(F_{k,n}, k-1) = 1$

(v) $\gcd(F_{k,n}, k) = \begin{cases} \gcd(3,k), & \text{if } n \text{ is odd} \\ \gcd(2,k), & \text{if } n \text{ is even} \end{cases}$

(vi) $\gcd(F_{k,n}, F_{k,n+1}) = 1$

Proof.

(i) We prove this property using mathematical induction. At first $\gcd(M_{k,1}, k-1) = \gcd(1, k-1) = 1$. Assume that $\gcd(M_{k,n}, k-1) = 1$, consider $\gcd(M_{k,n+1}, k-1) = \gcd(kM_{k,n} + (1-k)M_{k,n-1}, k-1) = \gcd(kM_{k,n}, k-1) = \gcd(M_{k,n}, k-1) = 1$, using the well-known property $\gcd(a+bc, b) = \gcd(a, b)$

(ii) We prove this property using mathematical induction. At first $\gcd(M_{k,1}, k) = 1$ and $\gcd(M_{k,2}, k) = 2$. Assume that $\gcd(M_{k,n}, k) = \begin{cases} 1, & \text{if } n \text{ is odd} \\ k, & \text{if } n \text{ is even} \end{cases}$, now consider

$$\begin{aligned} \gcd(M_{k,n+1}, k) &= \gcd(kM_{k,n} + (1-k)M_{k,n-1}, k) \\ &= \gcd((1-k)M_{k,n-1}, k) \\ &= \gcd(M_{k,n-1}, k) \\ &= \begin{cases} 1, & \text{if } n-1 \text{ is odd} \\ k, & \text{if } n-1 \text{ is even} \end{cases} \\ &= \begin{cases} 1, & \text{if } n+1 \text{ is odd} \\ k, & \text{if } n+1 \text{ is even} \end{cases} \end{aligned}$$

as desired.

(iii) The result is clear for $n = 1$, so we proceed by mathematical induction. Let $d = \gcd(M_{k,n+1}, M_{k,n+2})$. We have $d|M_{k,n+1}$ and $d|M_{k,n+2}$ so it divides any linear combination of them that is

$$d|(M_{k,n+2} - kM_{k,n+1}) = (1-k)M_{k,n}$$

Thus, $d|(\gcd(M_{k,n+1}, (1-k)M_{k,n}))$. Now, from Remark 2 and part 1 we have

$$\gcd(M_{k,n+1}, (1-k)M_{k,n}) = 1$$

which leads to the fact that $d = 1$.

(iv) Similar to number 1 above.

(v) Similar to number 2 above.

(vi) Similar to number 3 above.

Lemma 4. *If k is even, then* $\gcd(M_{k,n}, F_{k,n}) = \begin{cases} 1, & \textit{if } n \textit{ is odd} \\ 2, & \textit{if } n \textit{ is even} \end{cases}$

Proof. Recall that $F_{k,n} = M_{k,n} + 2$ (Proposition 1), also if k is even we have $M_{k,n} \equiv n \mod 2$, thus $\gcd(M_{k,n}, F_{k,n}) = \begin{cases} 1, & \text{if n is odd} \\ 2, & \text{if n is even} \end{cases}$, as desired.

3. Matrix representations

Theorem 8 (Matrix of generalized Mersenne numbers)**.** *Let* $Q_k = \begin{bmatrix} 0 & 1 \\ 1-k & k \end{bmatrix}$. *Then for* $n \geq 2$ *we have*

$$Q_k^n = \begin{bmatrix} (1-k)M_{k,n-1} & M_{k,n} \\ (1-k)M_{k,n} & M_{k,n+1} \end{bmatrix}$$

Proof. We prove the result by mathematical induction:

- If $n = 2$, we have

$$Q_k^2 = \begin{bmatrix} 1-k & k \\ k(1-k) & k^2+(1-k)^2 \end{bmatrix} = \begin{bmatrix} (1-k)M_{k,1} & M_{k,2} \\ (1-k)M_{k,2} & M_{k,3} \end{bmatrix}$$

- Assuming that the result is true for all $2 \leq m \leq n$.
- Consider $Q_k^{n+1} = Q_k Q_k^n = \begin{bmatrix} 0 & 1 \\ 1-k & k \end{bmatrix} \begin{bmatrix} (1-k)M_{k,n-1} & M_{k,n} \\ (1-k)M_{k,n} & M_{k,n+1} \end{bmatrix} = \begin{bmatrix} (1-k)M_{k,n} & M_{k,n+1} \\ (1-k)M_{k,n+1} & M_{k,n+2} \end{bmatrix}$

as desired.

Lemma 5. *For any integers* m *and* n *and* $k \geq 2$ *we have*

(i) $M_{k,n+m} = (1-k)M_{k,n-1}M_{k,m} + M_{k,n}M_{k,m+1}$.

(ii) $M_{k,n+m+1} = (1-k)M_{k,n}M_{k,m} + M_{k,n+1}M_{k,m+1}$.

(iii) $M_{k,2n} = (1-k)M_{k,n-1}M_{k,n} + M_{k,n}M_{k,n+1}$.

(iv) $M_{k,2n+1} = (1-k)M_{k,n}^2 + M_{k,n+1}^2$.

Proof. Consider

$$\begin{aligned} Q_k^{n+m} &= Q_k^n Q_k^m \\ &= \begin{bmatrix} (1-k)M_{k,n+m+1} & M_{k,n+m} \\ (1-k)M_{k,n+m} & M_{k,n+m+1} \end{bmatrix} \\ &= \begin{bmatrix} (1-k)M_{k,n-1} & M_{k,n} \\ (1-k)M_{k,n} & M_{k,n+1} \end{bmatrix} \begin{bmatrix} (1-k)M_{k,m-1} & M_{k,m} \\ (1-k)M_{k,m} & M_{k,m+1} \end{bmatrix} \end{aligned}$$

we get 1 *and* 2 *from equating the corresponding entries of the equal matrices. Also, we get* 3 *and* 4 *by letting* $m = n$ *in* 1 *and* 2.

Lemma 6 (Matrix of Extended Fermat Numbers)**.** *Let* $R_k = \begin{bmatrix} 2 & 3 \\ 3 & 2+k \end{bmatrix}$. *Then*

$$Q_k^n R_k = \begin{bmatrix} F_{k,n} & F_{k,n+1} \\ F_{k,n+1} & F_{k,n+2} \end{bmatrix}$$

Proof. Can be proved easily by mathematical induction.

4. Special Kind of Tridiagonal and Hessenberg matrices

A tridiagonal matrix is a matrix that has nonzero elements only on the main diagonal and on the first diagonal below and above the main diagonal. In this subsection we represent some tridiagonal matrices whose determinant or permanent is a generalized Mersenne number.

Lemma 7. *Suppose that $n \geq 1$ is an integer.*

(i) Let $N_n(k) = \begin{bmatrix} k & k-1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ -1 & k & 1-k & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & -1 & k & 1-k & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & -1 & k & 1-k & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & & & & & ... & -1 & k \end{bmatrix}$

Then $det(N_n) = M_{k,n+1}$.

(ii) Let $H_n(k) = \begin{bmatrix} 0 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ -1 & 0 & 1-k & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & -1 & k & 1-k & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & -1 & k & 1-k & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & -1 & k \end{bmatrix}$.

Then $det(H_n) = M_{k,n}$.

Proof. Clear from Section 2.1 and 2.2 in [3]

Lemma 8. *Suppose that $n \geq 1$ is an integer. Let* $T_n(k) = \begin{bmatrix} k & 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ k-1 & k & 1 & 0 & & \cdots & & 0 \\ 0 & k-1 & k & 1 & 0 & ... & & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & & \\ 0 & & & & & ... & k-1 & k \end{bmatrix}$.

Then $det(T_n) = M_{k,n+1}$.

Proof. Let $\alpha = k-1, \beta = 1$. Then $M_{k,n} = \frac{\alpha^n - \beta^n}{\alpha - \beta}$, following the work of Kilic and Tasci in [10, 11] we have $det(T_n) = M_{k,n+1}$.

Finally, we use Theorems 1-3 from [10] to get the following result.

Lemma 9. *We have*

(i) Let $A_n(k) = \begin{bmatrix} k & 1-k & 0 & ... & ... & ... & 0 \\ 1 & k & 1-k & 0 & & ... & 0 \\ 0 & 1 & k & 1-k & 0 & ... & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \\ 0 & & & & & ... & 1 & k \end{bmatrix}$.

Then $per(A_n) = M_{k,n+1}$.

(ii) *Let* $H_n(k) = \begin{bmatrix} k & 1-k & 0 & ... & ... & 0 \\ 1 & 0 & 0 & 0 & & 0 \\ 0 & 0 & A_n(k) & 0 & \cdots 0 & 0 \\ 0 & & \cdots & & & 0 \end{bmatrix}$.

Then $per(H_n) = \sum_n^{i=0} M_{k,i}$ *where* $n \geq 2$ *and* $A_n(k)$ *defined as the last part.*

(iii) *Let* $G_n(k) = \begin{bmatrix} 1 & 1 & 1 & ... & ... & ... & & 1 \\ -1 & k & 1-k & 0 & & ... & & 0 \\ 0 & -1 & k & 1-k & 0 & ... & & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & & \\ 0 & & & & & ... & -1 & k \end{bmatrix}$.

Then $det(G_n) = \sum_n^{i=0} M_{k,i}$ *where* $n \geq 2$.

Proof. Using $\alpha = k-1, \beta = 1$ and $M_{k,n} = \frac{\alpha^n - \beta^n}{\alpha - \beta}$

(i) Statement 1 is true by Theorem 1 from [10].

(ii) Statement 2 is true by Theorem 2 from [10].

(iii) Statement 3 is true by Theorem 3 from [10].

5. Some Applications

In this section we give two applications in cryptography for the matrix representation of $M_{k,m}$, which was found in Section 3.

5.1. An authentication protocol

In this section we will introduce an authentication protocol based on matrices. At first, Alice chooses a large integer $n = pq$ a product of two primes and an integer $k > 2$. Then Alice chooses two matrices $A = Q_k^{n_1}$ and $B = Q_k^{n_2}$ and computes their squares modulo n. Namely, $C = A^2 = Q_k^{2n_1} \mod n$ and $D = B^2 = Q_k^{2n_2} \mod n$. Alice publishes C and D. The method works as follows:

Algorithm 1. *(i) Alice chooses two random integers* m_1, m_2 *and finds the matrices* $X_1 = Q_k^{m_1}, X_2 = Q_k^{m_2}$. *Then she computes* $Y_1 = X_1^2 \mod n$ *and* $Y_2 = X_2^2 \mod n$ *and sends* Y_1, Y_2 *to Bob.*

(ii) Bob chooses two random numbers $v_1, v_2 \in \{0, 1\}$ *and sends them to Alice.*

(iii) Alice computes $Z = X_1 X_2 A^{v_1} B^{v_2} \mod n$ *and send it to Bob.*

(iv) Bob verifies the identity of Alice by checking that $Z^2 = Y_1 Y_2 C^{v_1} D^{v_2}$

(v) Bob asks Alice to send him one of X_1 *or* X_2 *and he checks that* $Y_1 = X_1^2$ *or* $Y_2 = X_2^2$.

Example 1. *Let* $n = 11 \cdot 13 = 143$, *and* $k = 5$. *If Alice takes on* $n_1 = 2$ *and* $n_2 = 3$. *Then* $A = \begin{bmatrix} 139 & 5 \\ 123 & 21 \end{bmatrix}$ *and* $B = \begin{bmatrix} 123 & 21 \\ 59 & 85 \end{bmatrix}$. *Also, we have*

$$C = A^2 = \begin{bmatrix} 59 & 85 \\ 89 & 55 \end{bmatrix}$$

and

$$D = B^2 = \begin{bmatrix} 66 & 78 \\ 117 & 27 \end{bmatrix}$$

(i) Alice chooses two random integers $m_1 = 3, m_2 = 4$ *and finds the matrices*

$$X_1 = Q_5^{m_1} = \begin{bmatrix} 123 & 21 \\ 59 & 85 \end{bmatrix}$$

$$X_2 = Q_5^{m_2} = \begin{bmatrix} 59 & 85 \\ 89 & 55 \end{bmatrix}$$

Then she computes $Y_1 = X_1^2 = \begin{bmatrix} 66 & 78 \\ 117 & 27 \end{bmatrix}$ *and* $Y_2 = X_2^2 = \begin{bmatrix} 35 & 109 \\ 136 & 8 \end{bmatrix}$ *and sends* Y_1, Y_2 *to Bob.*

(ii) Bob chooses two random numbers $v_1 = 0, v_2 = 1$ *and sends them to Alice.*

(iii) Alice computes $Z = X_1 X_2 A^{v_1} B^{v_2} \mod n = \begin{bmatrix} 111 & 33 \\ 11 & 133 \end{bmatrix}$ *and send it to Bob.*

(iv) Bob verifies the identity of Alice by checking that $Z^2 = Y_1 Y_2 C^{v_1} D^{v_2} = \begin{bmatrix} 100 & 44 \\ 110 & 34 \end{bmatrix}$

(v) Bob asks Alice to send him one of X_1 *or* X_2 *and he checks that* $Y_1 = X_1^2$ *or* $Y_2 = X_2^2$.

We should mention that it is very hard to know the matrices A and B from C and D. Also, be choosing a very large number the problem will be more and more harder.

5.2. A Key Exchange Protocol

In this section we propose a key exchange protocol based on matrices At first Alice and Bob choose and integer $n = pq$ and $k > 2$. Then they choose a 2×2 matrix A The protocol works as follows:

Algorithm 2. *(i) Alice selects an integer* $t > 0$ *and a secret matrix* $B = Q_k^{n_1} \mod n$ *that doesn't commute with A. She computes* $X_1 = A^t B \mod n$ *and send it to Bob.*

(ii) Bob chooses an integer $s > 0$ *and a secret matrix* $C = Q_k^{n_2} \mod n$ *that doesn't commute with A and computes* $X_2 = A^s C \mod n$ *and send it to Alice.*

(iii) Alice computes $K_A = A^t X_2 B \mod n$.

(iv) Bob computes $K_B = A^s X_1 C \mod n$

we have $K_A = K_B = K$.

Example 2. *Let* $k = 4$ *and* $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$.

(i) Alice selects an integer $t = 3$ *and computes* $B = Q_k^3 = \begin{bmatrix} 131 & 13 \\ 104 & 40 \end{bmatrix}$ *which doesn't commute with A. She computes* $X_1 = A^t B = \begin{bmatrix} 24 & 67 \\ 3 & 53 \end{bmatrix}$ *and send it to Bob.*

(ii) Bob chooses $s = 7$ *and find* $C = Q_k^5 \mod n = \begin{bmatrix} 23 & 121 \\ 66 & 78 \end{bmatrix}$ *which doesn't commute with A and computes* $X_2 = A^s C = \begin{bmatrix} 130 & 42 \\ 85 & 72 \end{bmatrix}$ *and send it to Alice.*

(iii) Alice computes $K_A = A^t X_2 B = \begin{bmatrix} 1 & 112 \\ 111 & 29 \end{bmatrix}$.

(iv) Bob computes $K_B = A^s X_1 C = \begin{bmatrix} 1 & 112 \\ 111 & 29 \end{bmatrix}$

6. Conclusion

In this paper we consider a generalization of Merssen and Fermat numbers into complex numbers, we derive some properties of the new sequence. For future work we may consider more generalizations and extensions of such sequence and try to relate them with real life applications.

Acknowledgements

The publication of this paper was supported by the Yarmouk University Research Council.

References

[1] ID Bruggles and VE Hoggatt Jr. A primer on the fibonacci numbers-part iv. *The Fibonacci Quarterly*, 1(4):65–71, 1963.

[2] Marcia Edson and Omer Yayenie. A new generalization of fibonacci sequence & extended binet's formula. 2009.

[3] Sergio Falcón and Ángel Plaza. On the fibonacci k-numbers. *Chaos, Solitons & Fractals*, 32(5):1615–1624, 2007.

[4] Henry W Gould. A history of the fibonacci q-matrix and a higher-dimensional problem. *The Fibonacci Quarterly*, 19(3):250–257, 1981.

[5] VE Hoggat. Fibonacci and lucas numbers, houghton-mifflin. *Palo Alto, California*, 1969.

[6] Paweł Ochalik and Andrzej Włoch. On generalized mersenne numbers, their interpretations and matrix generators. *Annales Universitatis Mariae Curie-Skłodowska, sectio A–Mathematica*, 72(1), 2018.

[7] Tian-Xiao He, Peter JS Shiue, and Yaotsu Chang. Computation of fermat's pseudoprimes (dedicated to the memory of professor leetsch c. hsu). *Journal of Discrete Mathematical Sciences and Cryptography*, 25(2):335–352, 2022.

[8] Kritsanapong Somsuk. The improvement of initial value closer to the target for fermat's factorization algorithm. *Journal of Discrete Mathematical Sciences and Cryptography*, 21(7-8):1573–1580, 2018.

[9] Kenneth H Rosen. *Elementary number theory*. Pearson Education London, 2011.

[10] E Kilic and D Taşci. On sums of second order linear recurrences by hessenberg matrices. *The Rocky Mountain Journal of Mathematics*, pages 531–544, 2008.

[11] Emrah Kilic and Dursun Tasci. On the second order linear recurrences by tridiagonal matrices. *Ars Combin*, 91:11–18, 2009.