Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2025, Volume 31, Number 4, 792-818
DOI: 10.7546/nntdm.2025.31.4.792-818

Cryptography using Fibonacci–Mersenne and Fibonacci-balancing p-sequences with a self-invertible matrix and the Affine–Hill cipher

Elahe Mehraban [1,2], **T. Aaron Gulliver** [3], **Ömür Deveci** [4,*] **and Evren Hincal** [1,2,5]

[1] Mathematics Research Center, Near East University TRNC
Mersin 10, 99138 Nicosia, Turkey

[2] Department of Mathematics, Near East University TRNC
Mersin 10, 99138 Nicosia, Turkey
e-mail: e.mehraban.math@gmail.com

[3] Department of Electrical and Computer Engineering, University of Victoria
Victoria, BC V8W 2Y2, Canada
e-mail: agullive@ece.uvic.ca

[4] Department of Mathematics, Faculty of Science and Letters, Kafkas University
36100, Turkey
e-mail: odeveci36@hotmail.com

[5] Research Center of Applied Mathematics, Khazar University
Baku, Azerbaijan
e-mail: evren.hincal@neu.edu.tr

[*] *Corresponding author*

Received: 18 July 2025 **Revised:** 3 November 2025
Accepted: 5 November 2025 **Online First:** 8 November 2025

Abstract: In this paper, we define two new sequences using the Fibonacci p-numbers, the generalized Mersenne numbers, and m-balancing numbers. These sequences are obtained from

the corresponding characteristic polynomials. The determinants and combinatorial and exponential representations of these new sequences are given. As an application, we provide two algorithms using these new sequences with self-invertible matrices and the Affine–Hill cipher.

Keywords: Mersenne numbers, m-balancing numbers, Fibonacci p-numbers, Cryptography, Self-invertible matrix, Affine–Hill cipher.

2020 Mathematics Subject Classification: 11K31, 11C20, 68P25, 68R01, 68P30, 15A15.

1 Introduction

Integer sequences have numerous applications in various fields [5–7, 9–11, 13–16]. In particular, the Fibonacci p-numbers represent an important class, defined as follows.

Definition 1.1. *For integer $p \geq 0$, the Fibonacci p-numbers, denoted by $\{F_p(n)\}_{-p}^{\infty}$, are defined as*

$$F_p(n) = F_p(n-1) + F_p(n-p-1),\ n \geq 0,$$

with initial conditions $F_p(-p) = \cdots = F_p(0) = 0$ and $F_p(1) = F_p(2) = \cdots = F_p(p) = 1$ (see [21]*).*
For example, if $p = 1$, then we have the Fibonacci sequence [4] and if $p = 3$ we have

$$F_3(n) = F_3(n-1) + F_2(n-4),\ n \geq 0,$$

so $\{F_3(n)\}_0^{\infty} = \{0, 1, 1, 1, 1, 2, 3, \ldots\}$.

One of the generalizations of the Mersenne sequence is as follows:

Definition 1.2. *For integer $k \geq 3$, the generalized Mersenne numbers, denoted by $\{M(k,n)\}_0^{\infty}$, are defined as*

$$M(k,n) = kM(k,n-1) - (k+1)M(k,n-2),\ n \geq 0,$$

with initial conditions $M(k,0) = 0$ and $M(k,1) = 1$.

If $k = 3$, then

$$M(3,n) = 3M(3,n-1) - 4M(3,n-2),\ n \geq 0,$$

so $\{M(3,n)\}_0^{\infty} = \{0, 1, 3, 5, \ldots\}$. Balancing numbers were introduced by Behera and Panda in 1999 [2]. The m-balancing numbers can be defined as follows.

Definition 1.3. *For $m \geq 1$, the m-balancing numbers, denoted by $\{B_{m,n}\}_0^{\infty}$, are*

$$B_{m,n+1} = 6kB_{m,n} - B_{m,n-1},\ n \geq 1,$$

with initial conditions $B_{m,0} = 0$ and $B_{m,1} = 1$ (see [17, 18]*).*

For example, if $m = 1$ we have

$$B_{1,n+1} = 6B_{1,n} - B_{1,n-1}, n \geq 1,$$

so $\{B_{m,n}\}_0^\infty = \{0, 1, 6, 35, \ldots\}$.

The characteristic polynomials of the Fibonacci p-numbers, generalized Mersenne numbers, and m-balancing numbers are $x^{p+1} - x^p - 1$, $x^2 - kx + k + 1$ and $x^2 - 6mx + 1$, respectively.

Definition 1.4. *A matrix M is called self-invertible matrix if $M = M^{-1}$ (see* [1]*).*

The Hill cipher is a polygraphic block cipher [12]. The Affine cipher [22] is based on linear algebra and can be described as follows.

Encryption:

$$C_i \equiv P_i K + B \pmod{m},$$

where K is an $n \times n$ key matrix, and P_i, C_i and B are $1 \times n$ matrices over $\mathbb{Z}_m$. It should satisfy

$$\gcd(\det K \pmod{m}, m) = 1.$$

Decryption:

$$P_i \equiv (C_i - B)K^{-1} \pmod{m}.$$

In 2016, a key matrix of order 3 that reflects an arbitrary line $y = ax + b$ was used to overcome the noninvertible matrix problem in the Affine–Hill cipher when it is modulo a prime number [20]. In [19], a public key cipher was obtained using the generalized Fibonacci matrices with the Affine–Hill cipher. Here, the Fibonacci p-numbers, generalized Mersenne numbers, and m-balancing numbers are used to obtain new sequences and create a public key for the Affine–Hill cipher.

The remainder of this paper is organized as follows. In Sections 2 and 3, we present the Fibonacci–Mersenne p-sequences and Fibonacci-balancing p-sequences, respectively. Then, the Fibonacci–Mersenne p-matrix and Fibonacci-balancing p-matrix are used in Section 4 as a key in the Affine–Hill cipher.

2 The Fibonacci–Mersenne p-sequences

In this section, we define new sequences and obtain some interesting results. The Fibonacci–Mersenne p-sequences, p an integer, are defined as follows.

Definition 2.1. *For integers $k \geq 3$ and $p \geq 3$, the Fibonacci–Mersenne p-sequences, $\{FM_n^k(p)\}_0^\infty$, are defined by*

$$\begin{aligned} FM_{n+p+3}^k(p) = (k+1)FM_{n+p+2}^k(p) - (2k+1)FM_{n+p+1}^k(p) + (k+1)FM_{n+p}^k(p) + FM_{n+2}^k(p) \\ - kFM_{n+1}^k(p) + (k+1)FM_n^k(p),\ n \geq 0, \end{aligned} \tag{1}$$

where $FM_0^k(p) = FM_1^k(p) = \cdots = FM_{p+1}^k(p) = 0$ and $FM_{p+2}^k(p) = 1$.

Example 2.1. *(i) For $k = 3$ and $p = 4$ we have*

$$FM^3_{n+7}(4) = (4)FM^3_{n+6}(4) - (7)FM^3_{n+5}(4) + (4)FM^3_{n+4}(4) + FM^3_{n+2}(4) \\ - 3FM^3_{n+1}(4) + (4)FM^3_n(4),\ n \geq 0,$$

so $\{FM^3_n(4)\}_0^\infty = \{0, 0, 0, 0, 0, 0, 1, 4, 9, 12, 1, -43, \ldots\}$.

(ii) For $k = 4$ and $p = 5$ we have

$$FM^4_{n+8}(5) = (5)FM^4_{n+7}(5) - (9)FM^4_{n+6}(5) + (5)FM^4_{n+5}(5) + FM^4_{n+2}(5) \\ - 4FM^4_{n+1}(5) + (5)FB^4_n(5),\ n \geq 0,$$

so $\{FM^4_n(5)\}_0^\infty = \{0, 0, 0, 0, 0, 0, 0, 1, 5, 16, 40, 81, 155, \ldots\}$.

The recurrence relation (1) gives

$$\begin{bmatrix} FM^k_{n+p+3}(p) \\ FM^k_{n+p+2}(p) \\ \vdots \\ FM^k_{n+2}(p) \\ FM^k_{n+1}(p) \end{bmatrix} = \begin{bmatrix} k+1 & -(2k+1) & k+1 & 0 & \cdots & 0 & 1 & -k & k+1 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} FM^k_{n+p+2}(p) \\ FM^k_{n+p+1}(p) \\ \vdots \\ FM^k_{n+1}(p) \\ FM^k_n(p) \end{bmatrix}.$$

Lemma 2.1. *For $p = 3$, $k = 3$ and $n \geq 6$, we have*

$$(M_3(3))^n = \begin{bmatrix} FM^3_{n+5}(3) & & -3FM^3_{n+4}(3) + 4FM^3_{n+3}(3) & 4FM^3_{n+4}(3) \\ FM^3_{n+4}(3) & & -3FM^3_{n+3}(3) + 4FM^3_{n+2}(3) & 4FM^3_{n+3}(3) \\ \vdots & M^*_3(3) & \vdots & \vdots \\ FM^3_{n+1}(3) & & -3FM^3_n(3) + 4FM^3_{n-1}(3) & 4FM^3_n(3) \\ FM^3_n(3) & & -3FM^3_{n-1}(3) + 4FM^3_{n-2}(3) & 4FM^3_{n-1}(3) \end{bmatrix} := T^n(3, 3),$$

$$M^*_3(3) = \begin{bmatrix} -7FM^3_{n+4}(3) + 4FM^3_{n+3}(3) + F_3(n-2) & 4FM^3_{n+4}(3) + F_3(n-1) & F_3(n) \\ -7FM^3_{n+3}(3) + 4FM^3_{n+2}(3) + F_3(n-3) & 4FM^3_{n+3}(3) + F_3(n-2) & F_3(n-1) \\ \vdots & \vdots & \vdots \\ -7FM^3_n(3) + 4FM^3_{n-1}(3) + F_3(n-6) & 4FM^3_n(3) + F_3(n-5) & F_3(n-4) \\ -7FM^3_{n-1}(3) + 4FM^3_{n-2}(3) + F_3(n-7) & 4FM^3_{n-1}(3) + F_3(n-6) & F_3(n-5) \end{bmatrix},$$

where

$$M_3(3) = \begin{bmatrix} 4 & -7 & 4 & 1 & -3 & 4 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Proof. By induction on n. For $k=3$, $p=3$, and $n=6$ we have

$$(M_3(3))^6 = \begin{bmatrix} -121 & 282 & -154 & 3 & 125 & -156 \\ -39 & 35 & 9 & 2 & 42 & 8 \\ 2 & -47 & 49 & 1 & 0 & 48 \\ 12 & -46 & 37 & 1 & -11 & 36 \\ 9 & -24 & 17 & 1 & -8 & 16 \\ 4 & -7 & 4 & 1 & -3 & 4 \end{bmatrix} = \begin{bmatrix} FM_{11}^3(3) & & 4FM_{10}^3(3) \\ FM_{10}^3(3) & & 4FM_9^3(3) \\ FM_9^3(3) & M_3^*(3) & 4FM_8^3(3) \\ FM_8^3(3) & & 4FM_7^3(3) \\ FM_7^3(3) & & 4FM_6^3(3) \\ FM_6^3(3) & & 4FM_5^3(3) \end{bmatrix},$$

where

$$M_3^*(3) = \begin{bmatrix} -7FM_{10}^3(3)+4FM_9^3(3)+F_3(4) & 4FM_{10}^3(3)+F_3(5) & F_3(6) & -3FM_{10}^3(3)+4FM_9^3(3) \\ -7FM_9^3(3)+4FM_8^3(3)+F_3(3) & 4FM_9^3(3)+F_3(4) & F_3(5) & -3FM_9^3(3)+4FM_8^3(3) \\ \vdots & \vdots & \vdots & \\ -7FM_6^3(3)+4FM_5^3(3)+F_3(0) & 4FM_6^3(3)+F_3(1) & F_3(2) & -3FM_6^3(3)+4FM_5^3(3) \\ -7FM_5^3(3)+4FM_4^3(3)+F_3(-1) & 4FM_5^3(3)+F_3(0) & F_3(1) & -3FM_5^3(3)+4FM_4^3(3) \end{bmatrix},$$

Now, assume that the statement holds for n. Then, for $n+1$ we have

$$(M_3(3))^{n+1} = \begin{bmatrix} 4 & -7 & 4 & 1 & -3 & 4 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} FM_{n+5}^3(3) & & -3FM_{n+4}^3(3)+4FM_{n+3}^3(3) & 4FM_{n+4}^3(3) \\ FM_{n+4}^3(3) & & -3FM_{n+3}^3(3)+4FM_{n+2}^3(3) & 4FM_{n+3}^3(3) \\ \vdots & M_3^*(3) & \vdots & \vdots \\ FM_{n+1}^3(3) & & -3FM_n^3(3)+4FM_{n-1}^3(3) & 4FM_n^3(3) \\ FM_n^3(3) & & -3FM_{n-1}^3(3)+4FM_{n-2}^3(3) & 4FM_{n-1}^3(3) \end{bmatrix}$$

$$= T^{n+1}(3,3),$$

where

$$M_3^*(3) = \begin{bmatrix} -7FM_{n+4}^3(3)+4FM_{n+3}^3(3)+F_3(n-2) & 4FM_{n+4}^3(3)+F_3(n-1) & F_3(n) \\ -7FM_{n+3}^3(3)+4FM_{n+2}^3(3)+F_3(n-3) & 4FM_{n+3}^3(3)+F_3(n-2) & F_3(n-1) \\ \vdots & \vdots & \vdots \\ -7FM_n^3(3)+4FM_{n-1}^3(3)+F_3(n-6) & 4FM_n^3(3)+F_3(n-5) & F_3(n-4) \\ -7FM_{n-1}^3(3)+4FM_{n-2}^3(3)+F_3(n-7) & 4FM_{n-1}^3(3)+F_3(n-6) & F_3(n-5) \end{bmatrix},$$

and the proof is complete. □

Corollary 2.1. *For $p=3$, $k \geq 3$ and $n \geq 6$, we have*

$$(M_3(k))^n = \begin{bmatrix} FM_{n+5}^k(3) & & -kFM_{n+4}^k(3)+(k+1)FM_{n+3}^k(3) & (k+1)FM_{n+4}^k(3) \\ FM_{n+4}^k(3) & & -kFM_{n+3}^k(3)+(k+1)FM_{n+2}^k(3) & (k+1)FM_{n+3}^k(3) \\ \vdots & M_3^*(k) & \vdots & \vdots \\ FM_{n+1}^k(3) & & -kFM_n^k(3)+(k+1)FM_{n-1}^k(3) & 4FM_n^k(3) \\ FM_n^k(3) & & -kFM_{n-1}^k(3)+(k+1)FM_{n-2}^k(3) & (k+1)FM_{n-1}^k(3) \end{bmatrix},$$

$M_3^*(k) =$

$$\begin{bmatrix} -(2k+1)FM_{n+4}^k(3)+(k+1)FM_{n+3}^k(3)+F_3(n-2) & (k+1)FM_{n+4}^k(3)+F_3(n-1) & F_3(n) \\ -(2k+1)FM_{n+3}^k(3)+(k+1)FM_{n+2}^k(3)+F_3(n-3) & (k+1)FM_{n+3}^k(3)+F_3(n-2) & F_3(n-1) \\ \vdots & \vdots & \vdots \\ -(2k+1)FM_n^k(3)+(k+1)FM_{n-1}^k(3)+F_3(n-6) & (k+1)FM_n^k(3)+F_3(n-5) & F_3(n-4) \\ -(2k+1)FM_{n-1}^k(3)+(k+1)FM_{n-2}^k(3)+F_3(n-7) & (k+1)FM_{n-1}^k(3)+F_3(n-6) & F_3(n-5) \end{bmatrix},$$

where

$$M_3(k) = \begin{bmatrix} k+1 & -(2k+1) & k+1 & 1 & -k & k+1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Let $M_p(k) = [m_{i,j}]_{(p+3)\times(p+3)}$ be the companion matrix for the Fibonacci–Mersenne p-sequences. It can easily be established by induction on n that for $p \geq 4$ and $n \geq p+3$

$$(M_p(k))^n = \begin{bmatrix} FM_{n+p+2}^k(p) & -(2k+1)FM_{n+p+1}^k(p)+(k+1)FM_{n+p}^k(p)+F_p(n-p+1) \\ FM_{n+p+1}^k(p) & -(2k+1)FM_{n+p}^k(p)+(k+1)FM_{n+p-1}^k(p)+F_p(n-p) \\ \vdots & \vdots \\ FM_{n+1}^k(p) & -(2k+1)FM_n^k(p)+(k+1)FM_{n-1}^k(p)+F_p(n-2p) \\ FM_n^k(p) & -(2k+1)FM_{n-1}^k(p)+(k+1)FM_{n-2}^k(p)+F_p(n-2p-1) \end{bmatrix}$$

$$\begin{bmatrix} (k+1)FM_{n+p+1}^k(p) \\ (k+1)FM_{n+p}^k(p) \\ M_p^*(k) \quad \vdots \\ (k+1)FM_n^k(p) \\ (k+1)FM_{n-1}^k(p) \end{bmatrix},$$

where $M_p^*(k)$ is a $(p+3)\times p$ matrix given by

$$M_p(k)^* = \begin{bmatrix} (k+1)FM_{n+p+1}^k(p)+F_p(n-p+2) & F_p(n-p+3) & F_p(n-p+4) & \cdots \\ (k+1)FM_{n+p}^k(p)+F_p(n-p+1) & F_p(n-p+2) & F_p(n-p+3) & \cdots \\ \vdots & \vdots & \vdots & \ddots \\ (k+1)FM_n^k(p)+F_p(n-2p+1) & F_p(n-2p+2) & F_p(n-2p+3) & \cdots \\ (k+1)FM_{n-1}^k(p)+F_p(n-2p) & F_p(n-2p+1) & F_p(n-2p+2) & \cdots \end{bmatrix}$$

$$\begin{bmatrix} F_p(n) & -kFM_{n+p+1}^k(p)+(k+1)FM_{n+p}^k(p) \\ F_p(n-1) & -kFM_{n+p}^k(p)+(k+1)FM_{n+p-1}^k(p) \\ \vdots & \vdots \\ F_p(n-p-1) & -kFM_n^k(p)+(k+1)FM_{n-1}^k(p) \\ F_p(n-p-2) & -kFM_{n-1}^k(p)+(k+1)FM_{n-2}^k(p) \end{bmatrix}.$$

It can easily be determined that

$$\det M_p(k) = \begin{cases} k+1, & \text{if } p \text{ is even,} \\ -(k+1), & \text{if } p \text{ is odd,} \end{cases}$$

so then

$$\det(M_p(k))^n = \begin{cases} (k+1)^n, & \text{if } p \text{ is even,} \\ (-k-1)^n, & \text{if } p \text{ is odd.} \end{cases}$$

Lemma 2.2. *The characteristic equation of the Fibonacci–Mersenne p-sequences given by*

$$x^{p+3} - (k+1)x^{p+2} + (2k+1)x^{p+1} - (k+1)x^p - x^2 + kx - (k+1) = 0,$$

does not have multiple roots for $p \geq 3$.

Proof. It is clear that $x^{p+3} - (k+1)x^{p+2} + (2k+1)x^{p+1} - (k+1)x^p - x^2 + kx - (k+1) = (x^{p+1} - x^p - 1)(x^2 - kx + k + 1)$. We show that for $p \geq 3$, $x^{p+1} - x^p - 1 = 0$ has distinct roots. Let β be a root of $h(x) = 0$ where $h(x) = x^{p+1} - x^p - 1 = 0$ so that $\beta \notin \{0, 1\}$. If β is a multiple root, then $h(\beta) = h'(\beta) = 0$. In this case, $h'(\beta) = 0$ and $\beta \neq 0$ give $\beta = \frac{p}{p+1}$, while $h(\beta) = 0$ means $\beta^p(\beta - 1) - 1 = 0$, but then $(\frac{p}{p+1})^p.(-\frac{1}{p+1}) = 1$, which is impossible since the left-hand side is less than 1 for $p \geq 3$. This is a contradiction.

On the other hand, the equations for $k = 3$ and $k = 4$ do not have real roots. For $k \geq 5$, the roots of $x^2 - kx + k + 1 = 0$ are

$$\frac{+k + \sqrt{k^2 - 4(k+1)}}{2} \quad \text{and} \quad \frac{+k - \sqrt{k^2 - 4(k+1)}}{2}.$$

Since

$$\left(\frac{+k + \sqrt{k^2 - 4(k+1)}}{2}\right)^{p+1} - \left(\frac{+k + \sqrt{k^2 - 4(k+1)}}{2}\right)^{p} + 1 \neq 0,$$

and

$$\left(\frac{+k - \sqrt{k^2 - 4(k+1)}}{2}\right)^{p+1} - \left(\frac{+k - \sqrt{k^2 - 4(k+1)}}{2}\right)^{p} + 1 \neq 0,$$

the result follows. □

For the Fibonacci–Mersenne p-sequences, $\{FM_n^k(p)\}$, we have

$$M_p(k) = \begin{bmatrix} k+1 & -(2k+1) & k+1 & 0 & \cdots & 0 & 1 & -k & k+1 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Let $\beta_1, \beta_2, \ldots, \beta_{p+3}$ be the roots of $x^{p+3} - (k+1)x^{p+2} + (2k+1)x^{p+1} - (k+1)x^p - x^2 + kx - (k+1) = (x^{p+1} - x^p - 1)(x^2 - kx + k + 1) = 0$ and U_p be the following $(p+3) \times (p+3)$ Vandermonde matrix

$$U_p = \begin{bmatrix} (\beta_1)^{p+2} & (\beta_2)^{p+2} & \cdots & (\beta_{p+3})^{p+2} \\ (\beta_1)^{p+1} & (\beta_2)^{p+1} & \cdots & (\beta_{p+3})^{p+1} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1 & \beta_2 & \cdots & \beta_{p+3} \\ 1 & 1 & \cdots & 1 \end{bmatrix}.$$

Now let $U_p(i,j)$ be the $(p+3) \times (p+3)$ matrix obtained from U_p by replacing the j-th column of U_p by $V_P(i)$ where $V_P(i)$ is the following $(p+3) \times 1$ matrix

$$V_p(i) = \begin{bmatrix} (\beta_1)^{n+p+3-i} \\ (\beta_2)^{n+p+3-i} \\ \vdots \\ (\beta_{p+3})^{n+p+3-i} \end{bmatrix}.$$

Theorem 2.1. *For $p \geq 3,\ k \geq 3$, and $(M_p(k))^n = f_{i,j}^{(p,n)}$, we have*

$$f_{i,j}^{(p,n)} = \frac{\det U_p(i,j)}{\det U_p}.$$

Proof. For $p \geq 3$ and $k \geq 3$, the matrix $M_p(k)$ is diagonalized, since the eigenvalues of it are distinct. Let $B_p = \mathrm{diag}(\beta_1, \beta_2, \ldots, \beta_{p+3})$ so that $M_p U_p = U_p B_p$. Since U_p is invertible, we have

$$\begin{cases} f_{i,1}^{(p,n)}(\beta_1)^{p+2} + f_{i,2}^{(p,n)}(\beta_1)^{p+1} + \cdots + f_{i,p+3}^{(p,n)} = (\beta_1)^{n+p+3-i}, \\ f_{i,1}^{(p,n)}(\beta_2)^{p+2} + f_{i,2}^{(p,n)}(\beta_2)^{p+1} + \cdots + f_{i,p+3}^{(p,n)} = (\beta_2)^{n+p+3-i}, \\ \vdots \\ f_{i,1}^{(p,n)}(\beta_{p+3})^{p+2} + f_{i,2}^{(p,n)}(\beta_{p+3})^{p+1} + \cdots + f_{i,p+3}^{(p,n)} = (\beta_{p+3})^{n+p+3-i}. \end{cases}$$

so it can be concluded that

$$f_{i,j}^{(p,n)} = \frac{\det U_p(i,j)}{\det U_p},$$

for $1 \leq i, j \leq p+3$. □

Lemma 2.3. *Let $t(x)$ be the generating function of the Fibonacci–Mersenne p-sequences. Then*

$$t(x) = \frac{x^{p+2}}{1 - (k+1)x + (2k+1)x^2 - (k+1)x^3 - x^{p+1} + kx^{p+2} - (k+1)x^{p+3}}. \tag{2}$$

Proof. We have

$$\begin{aligned} t(x) &= \sum_{n=1}^{\infty} FM_n^k(p)x^n \\ &= FM_1^k(p)x + FM_2^k(p)x^2 + \cdots + FM_{p+1}^k(p)x^{p+1} + FM_{p+2}^k(p)x^{p+2} + \sum_{n=p+3}^{\infty} FM_n^k(p)x^n \end{aligned}$$

$$
\begin{aligned}
&= x^{p+2} + \sum_{n=p+3}^{\infty} [(k+1)FM^k_{n+p+2}(p) - (2k+1)FM^k_{n+p+1}(p) + (k+1)FM^k_{n+p}(p) + FM^k_{n+2}(p) \\
&\quad - kFM^k_{n+1}(p) + (k+1)FB^k_n(p)]x^n \\
&= x^{p+2} + \sum_{n=p+3}^{\infty} (k+1)FM^k_{n+p+2}(p)x^n - \sum_{n=p+3}^{\infty} (2k+1)FM^k_{n+p+1}(p)x^n \\
&\quad + \sum_{n=p+3}^{\infty} (k+1)FM^k_{n+p}(p)x^n + \sum_{n=p+3}^{\infty} FM^k_{n+2}(p)x^n - \sum_{n=p+3}^{\infty} kFM^k_{n+1}(p)x^n \\
&\quad + \sum_{n=p+3}^{\infty} (k+1)FM^k_n(p)x^n \\
&= x^{p+2} + (k+1)x\sum_{n=1}^{\infty} FM^k_n(p)x^n - (2k+1)x^2\sum_{n=1}^{\infty} FM^k_n(p)x^n + (k+1)x^3\sum_{n=1}^{\infty} FM^k_n(p)x^n \\
&\quad + x^{p+1}\sum_{n=1}^{\infty} FM^k_n(p)x^n - kx^{p+2}\sum_{n=1}^{\infty} FM^k_n(p)x^n + (k+1)x^{p+3}\sum_{n=1}^{\infty} FM^k_n(p)x^n \\
&= x^{p+2} + (k+1)xt(x) - (2k+1)x^2t(x) + (k+1)x^3t(x) + x^{p+1}t(x) - kx^{p+2}t(x) \\
&\quad + (k+1)x^{p+3}t(x).
\end{aligned}
$$

□

Theorem 2.2. *The Fibonacci–Mersenne p-sequences $\{FM_n(k,p)\}$ have the following exponential representation*

$$t(x) = x^{p+2}\exp\sum_{i=1}^{\infty}\frac{(x)^i}{i}((k+1) - (2k+1)x + (k+1)x^2 + x^p - kx^{p+1} + (k+1)x^{p+2})^i,$$

where $p \geq 3$.

Proof. Using (2), we have

$$\ln t(x) = \ln x^{p+2} - \ln(1 - (k+1)x + (2k+1)x^2 - (k+1)x^3 - x^{p+1} + kx^{p+2} - (k+1)x^{p+3}).$$

Since

$$
\begin{aligned}
&- \ln(1 - (k+1)x + (2k+1)x^2 - (k+1)x^3 - x^{p+1} + kx^{p+2} - (k+1)x^{p+3}) \\
&= -[-x((k+1) - (2k+1)x + (k+1)x^2 + x^p - kx^{p+1} + (k+1)x^{p+2}) \\
&\quad - \frac{1}{2}x^2((k+1) - (2k+1)x + (k+1)x^2 + x^p - kx^{p+1} + (k+1)x^{p+2})^2 \\
&\quad - \cdots - \frac{1}{i}x^i((k+1) - (2k+1)x + (k+1)x^2 + x^p - kx^{p+1} + (k+1)x^{p+2})^i - \cdots],
\end{aligned}
$$

the result follows. □

Let $K(k_1, k_2, \ldots, k_v)$ be the following $v \times v$ companion matrix

$$K(k_1, k_2, \ldots, k_v) = \begin{bmatrix} k_1 & k_2 & \cdots & k_{v-1} & k_v \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}.$$

Theorem 2.3 ([3]). *The (i,j)-th entry, $k_{i,j}^n(k_1,k_2,\ldots,k_v)$, of the matrix $k^n(k_1,k_2,\ldots,k_v)$ is given by*

$$k_{i,j}^n(k_1,k_2,\ldots,k_v)=\sum_{(k_1,k_2,\ldots,k_v)}\frac{t_j+t_{j+1}+\cdots+t_v}{t_1+t_2+\cdots+t_v}\times\binom{t_1+t_2+\cdots+t_v}{t_1,t_2,\ldots,t_v}k_1^{t_1}\cdots k_v^{t_v},\quad(3)$$

where the sum is over the nonnegative integers satisfying $t_1+2t_2+\cdots+vt_v=n-i+j$,

$$\binom{t_1+t_2+\cdots+t_v}{t_1,t_2,\ldots,t_v}=\frac{(t_1+t_2+\cdots+t_v)!}{t_1!t_2!\cdots t_v!}$$

is a multinomial coefficient, and the coefficients in (3) *are defined as* 1 *if* $n=i-j$.

Lemma 2.4. *For the Fibonacci–Mersenne p-sequences, $\{FM_n^k(p)\}$, we have*

(i) $$FM_n^k(p)=\sum_{(t_1,t_2,\ldots,t_{p+3})}\binom{t_1+t_2+\cdots+t_{p+3}}{t_1,t_2,\ldots,t_{p+3}}(k+1)^{t_1}(-2k-1)^{t_2}(k+1)^{t_3}(-k)^{t_{p+2}}(k+1)^{t_{p+3}},$$

where the sum is over the nonnegative integers satisfying $t_1+2t_2+\cdots+(p+3)t_{p+3}=n-p-2$,

(ii) $$FM_n^k(p)=-\sum_{(t_1,t_2,\ldots,t_{p+3})}\frac{t_{p+3}}{t_1+t_2+\cdots+t_{p+3}}\binom{t_1+t_2+\cdots+t_{p+3}}{t_1,t_2,\ldots,t_{p+3}}(k+1)^{t_1}(-2k-1)^{t_2}$$
$$(k+1)^{t_3}(-k)^{t_{p+2}}(k+1)^{t_{p+3}},$$

where the sum is over the nonnegative integers satisfying $t_1+2t_2+\cdots+(p+3)t_{p+3}=n+1$.

Proof. (i) Let $i=p+3$ and $j=1$, and the result follows.

(ii) Let $i=p+2$ and $j=p+1$. The result then follows from Theorem 2.3 and $(M_p(k))^n$. □

3 The Fibonacci-balancing p-sequences

Here, we introduce the Fibonacci-balancing p-sequences, p an integer, and provide some results. The Fibonacci-balancing p-sequences are defined as follows.

Definition 3.1. *For integers $m\geq 1$ and $p\geq 3$, the Fibonacci-balancing p-sequences, $\{FB_n^m(p)\}_0^\infty$, are defined as*

$$FB_{n+p+3}^m(p)=(6m+1)FB_{n+p+2}^m(p)-(6m+1)FB_{n+p+1}^m(p)+FB_{n+p}^m(p)-FB_{n+2}^m(p)$$
$$-6mFB_{n+1}^m(p)+FB_n^m(p),\ n\geq 0,\quad(4)$$

where $FB_0^m(p)=FB_1^m(p)=\cdots=FB_{p+1}^m(p)=0$ and $FB_{p+2}^m(p)=1$.

Example 3.1. *(i) For $m=1$ and $p=3$, we have*

$$FB_{n+6}^1(3)=7FB_{n+5}^1(3)-7FB_{n+4}^1(3)+FB_{n+3}^1(3)-FB_{n+2}^1(3)$$
$$-6FB_{n+1}^1(3)+FB_n^1(3),\ n\geq 0,$$

so the sequence is $\{FB_n^1(3)\}_0^\infty=\{0,0,0,0,0,1,7,42,246,1434,8345,48540,\ldots\}$.

(ii) For $m = 1$ and $p = 4$, we have

$$FB^1_{n+7}(4) = 7FB^1_{n+6}(4) - 7FB^1_{n+5}(4) + FB^1_{n+4}(4) - FB^1_{n+2}(4) \\ - 6FB^1_{n+1}(4) + FB^1_n(4),\ n \geq 0,$$

so the sequence is $\{FB^1_n(4)\}_0^\infty = \{0, 0, 0, 0, 0, 0, , 1, 7, 42, 246, 1435, 8364, 48736, \ldots\}$.

From the recurrence relation (4) we have

$$\begin{bmatrix} FB^m_{n+p+3}(p) \\ FB^m_{n+p+2}(p) \\ \vdots \\ FB^m_{n+2}(p) \\ FB^m_{n+1}(p) \end{bmatrix} = \begin{bmatrix} (6m+1) & -(6m+1) & 1 & 0 & \cdots & 0 & -1 & -6m & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} FB^m_{n+p+2}(p) \\ FB^m_{n+p+1}(p) \\ \vdots \\ FB^m_{n+1}(p) \\ FB^m_n(p) \end{bmatrix}.$$

Lemma 3.1. *For $p = 3$, $m = 1$, and $n \geq 6$, we have*

$(B_1(3))^n =$

$$\begin{bmatrix} FB_{n+5}(3) & -(7FB_{n+4}(3) - FB_{n+3}(3) + FB_{n+2}(3) + 6FB_{n+1}(3) - FB_n(3)) & FB_{n+4}(3) \\ FB_{n+4}(3) & -(7FB_{n+3}(3) - FB_{n+2}(3) + +FB_{n+1}(3) + 6FB_n(3) - FB_{n-1}(3)) & FB_{n+3}(3) \\ \vdots & \vdots & B^*_1(3) \quad \vdots \\ FB_{n+1}(3) & -(7FB_n(3) - FB_{n-1}(3) + FB_{n-2}(3) + 6FB_{n-3}(3) - FB_{n-4}(3)) & FB_n(3) \\ FB_n(3) & -(7FB_{n-1}(3) - FB_{n-2}(3) + FB_{n-3}(3) + 6FB_{n-4}(3) - FB_{n-5}(3)) & FB_{n-1}(3) \end{bmatrix}$$

$:= W_1(3)^n,$

$B^*_1(3) =$

$$\begin{bmatrix} FB_{n+4}(3) - (FB_{n+3}(3) + 6FB_{n+2}(3) - FB_{n+1}(3)) & -(FB_{n+4}(3) + 6FB_{n+3}(3) - FB_{n+2}(3)) \\ FB_{n+3}(3) - (FB_{n+2}(3) + 6FB_{n+1}(3) - FB_n(3)) & -(FB_{n+3}(3) + 6FB_{n+2}(3) - FB_{n+1}(3)) \\ \vdots & \vdots \\ FB_n(3) - (FB_{n-1}(3) + 6FB_{n-2}(3) - FB_{n-3}(3)) & -(FB_n(3) + 6FB_{n-1}(3) - FB_{n-2}(3)) \\ FB_{n-1}(3) - (FB_{n-2}(3) + 6FB_{n-3}(3) - FB_{n-4}(3)) & -(FB_{n-1}(3) + 6FB_{n-2}(3) - FB_{n-3}(3)) \end{bmatrix}$$

$$\begin{bmatrix} -6FB_{n+4}(3) + FB_{n+3}(3) \\ -6FB_{n+3}(3) + FB_{n+2}(3) \\ \vdots \\ -6FB_n(3) + FB_{n-1}(3) \\ -6FB_{n-1}(3) + FB_{n-2}(3) \end{bmatrix}$$

where

$$B_1(3) = \begin{bmatrix} 7 & -7 & 1 & -1 & -6 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Proof. By induction on n. Suppose that $m = 1$, $p = 3$ and $n = 6$. We then have

$$(B_1(3))^6 = \begin{bmatrix} 48540 & -57472 & 5477 & -16703 & -48636 & 8345 \\ 8345 & -9875 & 947 & -2868 & -8358 & 1434 \\ 1434 & -1693 & 163 & -491 & -1434 & 246 \\ 246 & -288 & 29 & -83 & -245 & 42 \\ 42 & -48 & 6 & -13 & -41 & 7 \\ 7 & -7 & 1 & -1 & -6 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} FB_{11}(3) & -(7FB_{10}(3) - FB_9(3) + FB_8(3) + 6FB_7 - FB_6) & & FB_{10}(3) \\ FB_{10}(3) & -(7FB_9(3) - FB_8(3) + FB_7(3) + 6FB_6 - FB_5) & & FB_9(3) \\ FB_9(3) & -(7FB_8(3) - FB_7(3) + FB_6(3) + 6FB_5 - FB_4) & B_1^*(3) & FB_8(3) \\ FB_8(3) & -(7FB_7(3) - FB_6(3) + FB_5(3) + 6FB_4 - FB_3) & & FB_7(3) \\ FB_7(3) & -(7FB_6(3) - FB_5(3) + FB_4(3) + 6FB_3 - FB_2) & & FB_6(3) \\ FB_6(3) & -(7FB_5(3) - FB_4(3) + FB_3(3) + 6FB_2 - FB_1) & & FB_5(3) \end{bmatrix}$$

$$B_1^*(3) =$$

$$\begin{bmatrix} FB_{10}(3) - (FB_9(3) + 6FB_8(3) - FB_7(3)) & -(FB_{10}(3) + 6FB_9(3) - FB_8(3)) & -6FB_9(3) + FB_8(3) \\ FB_9(3) - (FB_8(3) + 6FB_7(3) - FB_6(3)) & -(FB_9(3) + 6FB_8(3) - FB_7(3)) & -6FB_9(3) + FB_8(3) \\ FB_8(3) - (FB_7(3) + 6FB_6(3) - FB_5(3)) & -(FB_8(3) + 6FB_7(3) - FB_6(3)) & -6FB_8(3) + FB_7(3) \\ FB_7(3) - (FB_6(3) + 6FB_5(3) - FB_4(3)) & -(FB_7(3) + 6FB_6(3) - FB_5(3)) & -6FB_7(3) + FB_6(3) \\ FB_6(3) - (FB_5(3) + 6FB_4(3) - FB_3(3)) & -(FB_6(3) + 6FB_5(3) - FB_4(3)) & -6FB_6(3) + FB_5(3) \\ FB_5(3) - (FB_4(3) + 6FB_3(3) - FB_2(3)) & -(FB_5(3) + 6FB_4(3) - FB_3(3)) & -6FB_5(3) + FB_4(3) \end{bmatrix}$$

Now, assume that the statement holds for n. Then for $n + 1$ we have

$$(B_1(3))^{n+1} = \begin{bmatrix} 7 & -7 & 1 & -1 & -6 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\times \begin{bmatrix} FB_{n+5}(3) & -(7FB_{n+4}(3) - FB_{n+3}(3) + FB_{n+2}(3) + 6FB_{n+1}(3) - FB_n(3)) & FB_{n+4}(3) \\ FB_{n+4}(3) & -(7FB_{n+3}(3) - FB_{n+2}(3) + +FB_{n+1}(3) + 6FB_n(3) - FB_{n-1}(3)) & FB_{n+3}(3) \\ \vdots & \vdots & B_1^*(3) \quad \vdots \\ FB_{n+1}(3) & -(7FB_n(3) - FB_{n-1}(3) + FB_{n-2}(3) + 6FB_{n-3}(3) - FB_{n-4}(3)) & FB_n(3) \\ FB_n(3) & -(7FB_{n-1}(3) - FB_{n-2}(3) + FB_{n-3}(3) + 6FB_{n-4}(3) - FB_{n-5}(3)) & FB_{n-1}(3) \end{bmatrix}$$

$$:= W_1(3)^{n+1},$$

where

$B_1^*(3) =$

$$\begin{bmatrix} FB_{n+4}(3) - (FB_{n+3}(3) + 6FB_{n+2}(3) - FB_{n+1}(3)) & -(FB_{n+4}(3) + 6FB_{n+3}(3) - FB_{n+2}(3)) \\ FB_{n+3}(3) - (FB_{n+2}(3) + 6FB_{n+1}(3) - FB_n(3)) & -(FB_{n+3}(3) + 6FB_{n+2}(3) - FB_{n+1}(3)) \\ \vdots & \vdots \\ FB_n(3) - (FB_{n-1}(3) + 6FB_{n-2}(3) - FB_{n-3}(3)) & -(FB_n(3) + 6FB_{n-1}(3) - FB_{n-2}(3)) \\ FB_{n-1}(3) - (FB_{n-2}(3) + 6FB_{n-3}(3) - FB_{n-4}(3)) & -(FB_{n-1}(3) + 6FB_{n-2}(3) - FB_{n-3}(3)) \end{bmatrix}$$

$$\begin{bmatrix} -6FB_{n+4}(3) + FB_{n+3}(3) \\ -6FB_{n+3}(3) + FB_{n+2}(3) \\ \vdots \\ -6FB_n(3) + FB_{n-1}(3) \\ -6FB_{n-1}(3) + FB_{n-2}(3) \end{bmatrix},$$

and we have the result. □

Corollary 3.1. *For $p = 3$, $m \geq 1$, and $n \geq 6$ we have*

$(B_m(3))^n =$

$$\begin{bmatrix} FB_{n+5}(3) & -((6m+1)FB_{n+4}(3) - FB_{n+p}(3) + FB_{n+2}(3) + 6mFB_{n+1}(3) - FB_n(3)) \\ FB_{n+4}(3) & -((6m+1)FB_{n+p}(3) - FB_{n2}(3) + FB_{n+1}(3) + 6mFB_n(3) - FB_{n-1}(3)) \\ \vdots & \vdots \\ FB_{n+1}(3) & -((6m+1)FB_n(3) - FB_{n-1}(3) + FB_{n-2}(3) + 6mFB_{n-3}(3) - FB_{n-4}(3)) \\ FB_n(3) & -((6m+1)FB_{n-1}(3) - FB_{n-2}(3) + FB_{n-3}(3) + 6mFB_{n-4}(3) - FB_{n-5}(3)) \end{bmatrix}$$

$$B_m^*(3) \begin{bmatrix} FB_{n+4}(3) \\ FB_{n+3}(3) \\ \vdots \\ FB_n(3) \\ FB_{n-1}(3) \end{bmatrix} := W_m(3)^n,$$

where $B_m^*(3) =$

$$\begin{bmatrix} FB_{n+4}(3) - (FB_{n+3}(3) + 6mFB_{n+2}(3) - FB_{n+1}(3)) & -(FB_{n+4}(3) + 6mFB_{n+3}(3) - FB_{n+2}(3)) \\ FB_{n+3}(3) - (FB_{n+2}(3) + 6mFB_{n+1}(3) - FB_n(3)) & -(FB_{n+3}(3) + 6mFB_{n+2}(3) - FB_{n+1}(3)) \\ \vdots & \vdots \\ FB_n(3) - (FB_{n-1}(3) + 6mFB_{n-2}(3) - FB_{n-3}(3)) & -(FB_n(3) + 6mFB_{n-1}(3) - FB_{n-2}(3)) \\ FB_{n-1}(3) - (FB_{n-2}(3) + 6FB_{n-3}(3) - FB_{n-4}(3)) & -(FB_{n-1}(3) + 6FB_{n-2}(3) - FB_{n-3}(3)) \end{bmatrix}$$

$$\begin{bmatrix} -6FB_{n+4}(3) + FB_{n+3}(3) \\ -6mFB_{n+3}(3) + FB_{n+2}(3) \\ \vdots \\ -6mFB_n(3) + FB_{n-1}(3) \\ -6FB_{n-1}(3) + FB_{n-2}(3) \end{bmatrix},$$

where

$$B_m(3) = \begin{bmatrix} 6m+1 & -(6m+1) & 1 & -1 & -6m & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Suppose that $B_m(p) = [m_{i,j}]_{(p+3)\times(p+3)}$ is the companion matrix for the Fibonacci-balancing p-sequences. It can be readily established by mathematical induction on n that for $p \geq 3$ and $n \geq p+3$.

$(B_m(p))^n =$

$$\begin{bmatrix} FB_{n+p+2}(p) & -((6m+1)FB_{n+p+1}(p) - FB_{n+p}(p) + FB_{n+2}(p) + 6mFB_{n+1}(p) - FB_n(p)) \\ FB_{n+p+1}(p) & -((6m+1)FB_{n+p}(p) - FB_{n+p-1}(p) + FB_{n+1}(p) + 6mFB_n(p) - FB_{n-1}(p)) \\ \vdots & \vdots \\ FB_{n+1}(p) & -((6m+1)FB_n(p) - FB_{n-1}(p) + FB_{n-p+1}(p) + 6mFB_{n-p}(p) - FB_{n-p-3}(p)) \\ FB_n(p) & -((6m+1)FB_{n-1}(p) - FB_{n-2}(p) + FB_{n-p}(p) + 6mFB_{n-p-1}(p) - FB_{n-p-2}(p)) \end{bmatrix}$$

$$B_m^*(p) \begin{bmatrix} FB_{n+p+1}(p) \\ FB_{n+p}(p) \\ \vdots \\ FB_n(p) \\ FB_{n-1}(p) \end{bmatrix} := W_m(p)^n,$$

$B_m^*(p) =$

$$\begin{bmatrix} FB_{n+p+1}(p) - (FB_{n+p}(p) + 6mFB_{n+2}(p) - FB_{n+1}(p)) & -(FB_{n+4}(p) + 6mFB_{n+3}(p) - FB_{n+2}(p)) \\ FB_{n+p}(p) - (FB_{n+p-1}(p) + 6mFB_{n+1}(p) - FB_n(p)) & -(FB_{n+3}(p) + 6mFB_{n+2}(p) - FB_{n+1}(p)) \\ \vdots & \vdots \\ FB_n(p) - (FB_{n-1}(p) + 6mFB_{n-2}(p) - FB_{n-3}(p)) & -(FB_{n-p+3}(p) + 6mFB_{n-p+2}(p) - FB_{n-p+1}(p)) \\ FB_{n-1}(p) - (FB_{n-2}(p) + 6FB_{n-3}(p) - FB_{n-4}(p)) & -(FB_{n-p+2}(p) + 6mFB_{n-p+1}(p) - FB_{n-p}(p)) \end{bmatrix}$$

$$\begin{bmatrix} \cdots & -(FB_{n+p+1}(p) + 6mFB_{n+p}(p) - FB_{n+p-1}(p)) & -6mFB_{n+p+1}(p) + FB_{n+p}(p) \\ \cdots & -(FB_{n+p}(p) + 6mFB_{n+p-1}(p) - FB_{n+p-2}(p)) - 6m & FB_{n+p}(p) + FB_{n+p-1}(p) \\ \ddots & \vdots & \vdots \\ \cdots & -(FB_n(p) + 6mFB_{n-1}(p) - FB_{n-2}(p)) & -6mFB_n(p) + FB_{n-1}(p) \\ \cdots & -(FB_{n-1}(p) + 6mFB_{n-2}(p) - FB_{n-3}(p)) & -6mFB_{n-1}(p) + FB_{n-2}(p) \end{bmatrix}$$

where

$$B_m(p) = \begin{bmatrix} 6m+1 & -(6m+1) & 1 & 0 & \cdots & 0 & -1 & -6m & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 \end{bmatrix}.$$

It can easily be determined that $\det B_m(p) = (-1)^p$, so

$$\det(B_m(p))^n = \begin{cases} 1, & \text{if } np \text{ is even,} \\ -1, & \text{if } np \text{ is odd.} \end{cases}$$

Lemma 3.2. *The characteristic equation of the Fibonacci-balancing p-sequences*

$$x^{p+3} - (6m+1)x^{p+2} + (6m+1)x^{p+1} - x^p + x^2 + 6mx - 1 = 0,$$

does not have multiple roots for $p \geq 3$.

Proof. It is clear that

$$x^{p+3} - (6m+1)x^{p+2} + (6m+1)x^{p+1} - x^p + x^2 + 6mx - 1 = (x^{p+1} - x^p - 1)(x^2 - 6mx + 1).$$

Based on Lemma 2.3, $x^{p+1} - x^p - 1 = 0$ has distinct roots for $p \geq 3$. On the other hand, the roots of $x^2 - 6mx + 1 = 0$ are $3m + \sqrt{9m^2 - 1}$ and $3m - \sqrt{9m^2 - 1}$.

Since $(3m + \sqrt{9m^2 - 1})^{p+1} - (3m + \sqrt{9m^2 - 1})^p + 1 \neq 0$ and $(3m - \sqrt{9m^2 - 1})^{p+1} - (3m - \sqrt{9m^2 - 1})^p + 1 \neq 0$, the result follows. □

For the Fibonacci-balancing p-sequences, $\{FB_n^m(p)\}$, we have

$$B_m(p) = \begin{bmatrix} 6m+1 & -(6m+1) & 1 & 0 & \cdots & 0 & -1 & -6m & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Let $\alpha_1, \alpha_2, \ldots, \alpha_{p+3}$ be the roots of $x^{p+3} - (6m+1)x^{p+2} + (6m+1)x^{p+1} - x^p + x^2 + 6mx - 1 = 0$ and N_p be the following $(p+3) \times (p+3)$ Vandermonde matrix

$$N_p = \begin{bmatrix} (\alpha_1)^{p+2} & (\alpha_2)^{p+2} & \cdots & (\alpha_{p+3})^{p+2} \\ (\alpha_1)^{p+1} & (\alpha_2)^{p+1} & \cdots & (\alpha_{p+3})^{p+1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{p+3} \\ 1 & 1 & \cdots & 1 \end{bmatrix}.$$

Now let $N_p(i,j)$ be the $(p+3)\times(p+3)$ matrix obtained from N_p by replacing the j-th column of N_p by $W_P(i)$ where $W_P(i)$ is the following $(p+3)\times 1$ matrix

$$W_p(i) = \begin{bmatrix} (\alpha_1)^{n+p+3-i} \\ (\alpha_2)^{n+p+3-i} \\ \vdots \\ (\alpha_{p+2})^{n+p+3-i} \\ (\alpha_{p+3})^{n+p+3-i} \end{bmatrix}.$$

Theorem 3.1. *For $p \geq 3, m \geq 1$, and $(B_m(p))^n = f_{i,j}^{(p,n)}$ we have*

$$b_{i,j}^{(p,n)} = \frac{\det N_p(i,j)}{\det N_p}.$$

Proof. The proof is similar to that for Lemma 2.1 and so is omitted. □

Lemma 3.3. *Let $g(x)$ be the generating function of the Fibonacci-balancing p-sequences. Then*

$$g(x) = \frac{x^{p+2}}{1-(6m+1)x+(6m+1)x^2-x^3+x^{(p+1)}+6mx^{p+2}-x^{p+3}}. \tag{5}$$

Proof. We have

$$\begin{aligned}
g(x) &= \sum_{n=1}^{\infty} FB_n^m(p)x^n \\
&= FB_1^m(p)x + FB_2^m(p)x^2 + \cdots + FB_{p+1}^m(p)x^{p+1} + FB_{p+2}^m(p)x^{p+2} + \sum_{n=p+3}^{\infty} FB_n^m(p)x^n \\
&= x^{p+2} + \sum_{n=p+3}^{\infty} [(6m+1)FB_{n+p+2}^m(p) - (6m+1)FB_{n+p+1}^m(p) \\
&\qquad + FB_{n+p}^m(p) - FB_{n+2}^m(p) - 6mFB_{n+1}^m(p) + FB_n^m(p)]x^n \\
&= x^{p+2} + \sum_{n=p+3}^{\infty} (6m+1)FB_{n+p+2}^m(p)x^n - \sum_{n=p+3}^{\infty} (6m+1)FB_{n+p+1}^m(p)x^n \\
&\quad + \sum_{n=p+3}^{\infty} FB_{n+p}^m(p)x^n - \sum_{n=p+3}^{\infty} FB_{n+2}^m(p)x^n - \sum_{n=p+3}^{\infty} 6kFB_{n+1}^m(p)x^n + \sum_{n=p+3}^{\infty} FB_n^m(p)x^n \\
&= x^{p+2} + (6m+1)x\sum_{n=1}^{\infty} FB_{n+p+2}^m(p)x^n - (6m+1)x^2\sum_{n=1}^{\infty} FB_{n+p+1}^m(p)x^n \\
&\quad + x^3\sum_{n=1}^{\infty} FB_{n+p}^m(p)x^n - x^{p+1}\sum_{n=1}^{\infty} FB_{n+2}^m(p)x^n - 6mx^{p+2}\sum_{n=1}^{\infty} FB_{n+1}^m(p)x^n \\
&\quad + x^{p+3}\sum_{n=1}^{\infty} FB_n^m(p)x^n \\
&= x^{p+2} + (6m+1)xt(x) - (6m+1)x^2t(x) + x^3t(x) - x^{(p+1)}t(x) \\
&\quad - 6mx^{p+2}t(x) + x^{p+3}t(x).
\end{aligned}$$

□

Theorem 3.2. *The Fibonacci-balancing p-sequences $\{FB_n^m(p)\}$ have the following exponential representation*

$$g(x) = x^{p+2} \exp \sum_{i=1}^{\infty} \frac{(x)^i}{i}((6m+1) - (6m+1)x + x^2 - x^p - 6mx^{p+1} + x^{p+2})^i,$$

where $p \geq 3$.

Proof. Using (5), we have

$$\ln g(x) = \ln x^{p+2} - \ln(1 - (6m+1)x + (6m+1)x^2 - x^3 + x^{p+1} + 6mx^{p+2} - x^{p+3}).$$

Since

$$\begin{aligned}
&- \ln (1 - (6m+1)x + (6m+1)x^2 - x^3 + x^{p+1} + 6mx^{p+2} - x^{p+3}) \\
&= -[-x((6m+1) - (6m+1)x^1 + x^2 - x^p - 6mx^{p+1} + x^{p+2}) \\
&\quad - \frac{1}{2}x^2((6m+1) - (6m+1)x^1 + x^2 - x^p - 6mx^{p+1} + x^{p+2})^2 \\
&\quad - \cdots - \frac{1}{i}x^i((6m+1) - (6m+1)x^1 + x^2 - x^p - 6mx^{p+1} + x^{p+2})^i - \cdots],
\end{aligned}$$

the result follows. □

Lemma 3.4. *For the Fibonacci-balancing p-sequences, $\{FB_n(k,p)\}$, we have*

(i) $FB_n^m(p) = \sum_{(t_1,t_2,\ldots,t_{p+3})} \binom{t_1+t_2+\cdots+t_{p+3}}{t_1,t_2,\ldots,t_{p+3}} (6m+1)^{t_1}(-6m-1)^{t_2}(6m)^{t_{p+2}}(-1)^{t_{p+1}}$, *where the sum is over the nonnegative integers satisfying $t_1 + 2t_2 + \cdots + (p+3)t_{p+3} = n - p - 2$,*

(ii) $FB_n^m(p) = -\sum_{(t_1,t_2,\ldots,t_{p+3})} \frac{t_{p+3}}{t_1+t_2+\cdots+t_{p+3}} \binom{t_1+t_2+\cdots+t_{p+3}}{t_1,t_2,\ldots,t_{p+3}}$
$(6m+1)^{t_1}(-6m-1)^{t_2}(6m)^{t_{p+2}}(-1)^{t_{p+1}}$,
where the sum is over the nonnegative integers satisfying $t_1+2t_2+\cdots+(p+3)t_{p+3} = n+1$.

Proof. (i) Let $i = p+3$ and $j = 1$, and the result follows.

(ii) Let $i = p+2$ and $j = p+1$. The result then follows from Theorem 2.3 and $(B_m(p))^n$. □

4 A public key cipher using the Fibonacci– Mersenne p-sequences and the Fibonacci-balancing p-sequences

In this section, a public key for the Affine–Hill cipher is obtained by considering the Fibonacci–Mersenne p-sequences and Fibonacci-balancing p-sequences. The key matrix has a large space so it can provide sufficient security. The algorithm is given below. For illustration purposes, an alphabet of 37 symbols is considered which contains the letters $A - Z$ with numerical equivalents $0 - 25$, the digits $0 - 9$ with numerical equivalents $26 - 35$, and space with numerical equivalent 36 as shown in Table 1.

Table 1. A 37-symbol alphabet

A	B	C	D	E	F	G	H	I	J	K
0	1	2	3	4	5	6	7	8	9	10
L	M	N	O	P	Q	R	S	T	U	V
11	12	13	14	15	16	17	18	19	20	21
W	X	Y	Z	0	1	2	3	4	5	6
22	23	24	25	26	27	28	29	30	31	32
7	8	9	␣							
33	34	35	36							

Algorithm 1

First, Bob sends $n \geq p+3, k \geq 3$, and $p \geq 3$ to Alice. Then, Alice employs the encryption algorithm to get the ciphertext.

Encryption:

Step 1. Divide the plaintext into blocks of size 1×4.

Step 2. Construct a self-invertible matrix M using $FM^k_{n+p}, FM^k_{n+p+1}, FM^k_{n+p+2}, FM^k_{n+p+3}$ and the key matrix is $K := M$ **[?]**. Construct $B := [FM^k_{n+p}, FM^k_{n+p+1}, FM^k_{n+p+2}, FM^k_{n+p+3}]$. We have that $K \equiv K \pmod{37}$ and $B \equiv B \pmod{37}$.

Step 3. Construct $C_i \equiv (P_iK + B) \pmod{37}$.

Step 4. Obtain the ciphertext.

Decryption:

Step 1. Using K (K is self-invertible so $K = K^{-1}$) and B, construct $P \equiv (C - B)K^{-1} \pmod{37}$.

Step 2. Using Table 1, obtain the plaintext.

The algorithm is illustrated in the following example.

Example 4.1. *Bob sends* $p = 3,\ k = 4$*, and* $n = 3$ *to Alice. Alice then creates the ciphertext for the plaintext*

SPRING IS BEAUTIFUL

$$B = [FM^4_6(3), FM^k_7(3), FM^4_8(3), FM^4_9(3)] = [5, 16, 40, 82] \equiv [5, 16, 3, 8] \pmod{37},$$

and

$$M = \begin{bmatrix} FM_6^4(3) & FM_7^4(3) & 1 - FM_6^4(3) & -FM_7^4(3) \\ FM_8^4(3) & FM_9^4(3) & 1 - FM_8^4(3) & -FM_9^4(3) \\ 1 + FM_6^4(3) & FM_7^4(3) & -FM_6^4(3) & -FM_7^4(3) \\ FM_8^4(3) & 1 + FM_9^4(3) & -FM_8^4(3) & -FM_9^4(3) \end{bmatrix} = \begin{bmatrix} 5 & 16 & -4 & -16 \\ 40 & 82 & -40 & -81 \\ 6 & 16 & -5 & -16 \\ 40 & 83 & -40 & -82 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 5 & 16 & 33 & 21 \\ 3 & 8 & 34 & 30 \\ 6 & 16 & 32 & 21 \\ 3 & 9 & 34 & 29 \end{bmatrix} \pmod{37}.$$

Now, calculate $C_i \equiv (P_i K + B) \pmod{37}$:

$$C_1 = [\mathtt{S}, \mathtt{P}, \mathtt{R}, \mathtt{I}],$$
$$C_1 = [\mathtt{N}, \mathtt{G}, \mathtt{\sqcup}, \mathtt{I}],$$
$$C_3 = [\mathtt{S}, \mathtt{\sqcup}, \mathtt{B}, \mathtt{E}],$$
$$C_4 = [\mathtt{A}, \mathtt{U}, \mathtt{T}, \mathtt{I}],$$
$$C_5 = [\mathtt{F}, \mathtt{U}, \mathtt{L}, \mathtt{\sqcup}].$$

Thus

$$C_1 = \begin{bmatrix} 18 & 15 & 17 & 8 \end{bmatrix} \begin{bmatrix} 5 & 16 & 33 & 21 \\ 3 & 8 & 34 & 30 \\ 6 & 16 & 32 & 21 \\ 3 & 9 & 34 & 29 \end{bmatrix} + \begin{bmatrix} 5 & 16 & 3 & 8 \end{bmatrix} \equiv \begin{bmatrix} 7 & 28 & 36 & 19 \end{bmatrix} \pmod{37},$$

$$C_2 = \begin{bmatrix} 13 & 6 & 36 & 8 \end{bmatrix} \begin{bmatrix} 5 & 16 & 33 & 21 \\ 3 & 8 & 34 & 30 \\ 6 & 16 & 32 & 21 \\ 3 & 9 & 34 & 29 \end{bmatrix} + \begin{bmatrix} 5 & 16 & 3 & 8 \end{bmatrix} \equiv \begin{bmatrix} 32 & 32 & 25 & 6 \end{bmatrix} \pmod{37},$$

$$C_3 = \begin{bmatrix} 18 & 36 & 1 & 4 \end{bmatrix} \begin{bmatrix} 5 & 16 & 33 & 21 \\ 3 & 8 & 34 & 30 \\ 6 & 16 & 32 & 21 \\ 3 & 9 & 34 & 29 \end{bmatrix} + \begin{bmatrix} 5 & 16 & 3 & 8 \end{bmatrix} \equiv \begin{bmatrix} 36 & 15 & 28 & 12 \end{bmatrix} \pmod{37},$$

$$C_4 = \begin{bmatrix} 0 & 20 & 19 & 8 \end{bmatrix} \begin{bmatrix} 5 & 16 & 33 & 21 \\ 3 & 8 & 34 & 30 \\ 6 & 16 & 32 & 21 \\ 3 & 9 & 34 & 29 \end{bmatrix} + \begin{bmatrix} 5 & 16 & 3 & 8 \end{bmatrix} \equiv \begin{bmatrix} 18 & 34 & 9 & 18 \end{bmatrix} \pmod{37},$$

$$C_5 = \begin{bmatrix} 5 & 20 & 11 & 36 \end{bmatrix} \begin{bmatrix} 5 & 16 & 33 & 21 \\ 3 & 8 & 34 & 30 \\ 6 & 16 & 32 & 21 \\ 3 & 9 & 34 & 29 \end{bmatrix} + \begin{bmatrix} 5 & 16 & 3 & 8 \end{bmatrix} \equiv \begin{bmatrix} 5 & 16 & 19 & 27 \end{bmatrix} \pmod{37}.$$

The resulting ciphertext is

```
H2␣T66ZG␣P2MS8JSFQT1
```

Bob receives the ciphertext and using k, n, and p calculates $K^{-1} := K$. Therefore

$$P_1 = (C_1 - B)K^{-1} = (\begin{bmatrix}7 & 28 & 36 & 19\end{bmatrix} - \begin{bmatrix}5 & 16 & 3 & 8\end{bmatrix}) \times \begin{bmatrix}5 & 16 & 33 & 21\\ 3 & 8 & 34 & 30\\ 6 & 16 & 32 & 21\\ 3 & 9 & 34 & 29\end{bmatrix} \equiv \begin{bmatrix}18 & 15 & 17 & 8\end{bmatrix} \pmod{37},$$

$$P_2 = (C_2 - B)K^{-1} = (\begin{bmatrix}32 & 32 & 25 & 6\end{bmatrix} - \begin{bmatrix}5 & 16 & 3 & 8\end{bmatrix}) \times \begin{bmatrix}5 & 16 & 33 & 21\\ 3 & 8 & 34 & 30\\ 6 & 16 & 32 & 21\\ 3 & 9 & 34 & 29\end{bmatrix} \equiv \begin{bmatrix}13 & 6 & 36 & 8\end{bmatrix} \pmod{37},$$

$$P_3 = (C_3 - B)K^{-1} = (\begin{bmatrix}36 & 15 & 28 & 12\end{bmatrix} - \begin{bmatrix}5 & 16 & 3 & 8\end{bmatrix}) \times \begin{bmatrix}5 & 16 & 33 & 21\\ 3 & 8 & 34 & 30\\ 6 & 16 & 32 & 21\\ 3 & 9 & 34 & 29\end{bmatrix} \equiv \begin{bmatrix}18 & 36 & 1 & 4\end{bmatrix} \pmod{37},$$

$$P_4 = (C_4 - B)K^{-1} = (\begin{bmatrix}18 & 34 & 9 & 18\end{bmatrix} - \begin{bmatrix}5 & 16 & 3 & 8\end{bmatrix}) \times \begin{bmatrix}5 & 16 & 33 & 21\\ 3 & 8 & 34 & 30\\ 6 & 16 & 32 & 21\\ 3 & 9 & 34 & 29\end{bmatrix} \equiv \begin{bmatrix}0 & 20 & 19 & 8\end{bmatrix} \pmod{37},$$

$$P_5 = (C_5 - B)K^{-1} = (\begin{bmatrix}5 & 16 & 19 & 27\end{bmatrix} - \begin{bmatrix}5 & 16 & 3 & 8\end{bmatrix}) \times \begin{bmatrix}5 & 16 & 33 & 21\\ 3 & 8 & 34 & 30\\ 6 & 16 & 32 & 21\\ 3 & 9 & 34 & 29\end{bmatrix} \equiv \begin{bmatrix}5 & 20 & 11 & 36\end{bmatrix} \pmod{37},$$

and the plaintext is obtained.

We now consider encryption using the Fibonacci-balancing p-sequence. The approach is similar to that for the Fibonacci–Mersenne p-sequence, but Bob sends $m \geq 1$ instead of $k \geq 3$ and $B = [FB^m_{n+p}, FB^m_{n+p+1}, FB^m_{n+p+2}, FB^m_{n+p+3}]$.

Example 4.2. *Bob sends $m = 1, p = 3$ and $n = 3$ to Alice. Using the plaintext in Example 4.1 gives*

$$B = [FB_6(3), FB_7(3), FB_8(3), FB_9(3)] = [7, 42, 246, 1434] \equiv [7, 5, 24, 28] \pmod{37},$$

and

$$M = \begin{bmatrix} FB_6(3) & FB_7(3) & 1 - FB_6(3) & -FB_7(3) \\ FB_8(3) & FB_9(3) & 1 - FB_8(3) & -FB_9(3) \\ 1 + FB_6(3) & FB_7(3) & -FB_6(3) & -FB_7(3) \\ FB_8(3) & 1 + FB_9(3) & -FB_8(3) & -FB_9(3) \end{bmatrix} = \begin{bmatrix} 7 & 42 & -6 & -42 \\ 246 & 1434 & -246 & -1433 \\ 8 & 42 & -7 & -42 \\ 246 & 1435 & -246 & -1434 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 7 & 5 & 31 & 32 \\ 24 & 28 & 13 & 8 \\ 8 & 5 & 30 & 32 \\ 24 & 29 & 13 & 9 \end{bmatrix} \pmod{37}.$$

Now, calculate $C_i \equiv (P_i K + B) \pmod{37}$:

$$P_1 = [\mathtt{S}, \mathtt{P}, \mathtt{R}, \mathtt{I}],$$
$$P_1 = [\mathtt{N}, \mathtt{G}, \mathtt{\sqcup}, \mathtt{I}],$$
$$P_3 = [\mathtt{S}, \mathtt{\sqcup}, \mathtt{B}, \mathtt{E}],$$
$$P_4 = [\mathtt{A}, \mathtt{U}, \mathtt{T}, \mathtt{I}],$$
$$P_5 = [\mathtt{F}, \mathtt{U}, \mathtt{L}, \mathtt{\sqcup}].$$

Thus

$$C_1 = \begin{bmatrix} 18 & 15 & 17 & 8 \end{bmatrix} \begin{bmatrix} 7 & 5 & 31 & 32 \\ 24 & 28 & 13 & 8 \\ 8 & 5 & 30 & 32 \\ 24 & 29 & 13 & 9 \end{bmatrix} + \begin{bmatrix} 7 & 5 & 24 & 28 \end{bmatrix} \equiv \begin{bmatrix} 6 & 18 & 22 & 8 \end{bmatrix} \pmod{37},$$

$$C_2 = \begin{bmatrix} 13 & 6 & 36 & 8 \end{bmatrix} \begin{bmatrix} 7 & 5 & 31 & 32 \\ 24 & 28 & 13 & 8 \\ 8 & 5 & 30 & 32 \\ 24 & 29 & 13 & 9 \end{bmatrix} + \begin{bmatrix} 7 & 5 & 24 & 28 \end{bmatrix} \equiv \begin{bmatrix} 20 & 21 & 24 & 14 \end{bmatrix} \pmod{37},$$

$$C_3 = \begin{bmatrix} 18 & 36 & 1 & 4 \end{bmatrix} \begin{bmatrix} 7 & 5 & 31 & 32 \\ 24 & 28 & 13 & 8 \\ 8 & 5 & 30 & 32 \\ 24 & 29 & 13 & 9 \end{bmatrix} + \begin{bmatrix} 7 & 5 & 24 & 28 \end{bmatrix} \equiv \begin{bmatrix} 28 & 3 & 22 & 35 \end{bmatrix} \pmod{37},$$

$$C_4 = \begin{bmatrix} 0 & 20 & 19 & 8 \end{bmatrix} \begin{bmatrix} 7 & 5 & 31 & 32 \\ 24 & 28 & 13 & 8 \\ 8 & 5 & 30 & 32 \\ 24 & 29 & 13 & 9 \end{bmatrix} + \begin{bmatrix} 7 & 5 & 24 & 28 \end{bmatrix} \equiv \begin{bmatrix} 17 & 4 & 33 & 17 \end{bmatrix} \pmod{37},$$

$$C_5 = \begin{bmatrix} 5 & 20 & 11 & 36 \end{bmatrix} \begin{bmatrix} 7 & 5 & 31 & 32 \\ 24 & 28 & 13 & 8 \\ 8 & 5 & 30 & 32 \\ 24 & 29 & 13 & 9 \end{bmatrix} + \begin{bmatrix} 7 & 5 & 24 & 28 \end{bmatrix} \equiv \begin{bmatrix} 31 & 24 & 16 & 25 \end{bmatrix} \pmod{37}.$$

The resulting ciphertext is

`GSWIUVYO2DW9RE7R5YQZ`

Bob receives the ciphertext and using m, n, and p calculates $K^{-1} := K$. Therefore

$$P_1 = (C_1 - B)K^{-1} = (\begin{bmatrix} 6 & 18 & 22 & 8 \end{bmatrix} - \begin{bmatrix} 7 & 5 & 24 & 28 \end{bmatrix}) \times \begin{bmatrix} 7 & 5 & 31 & 32 \\ 24 & 28 & 13 & 8 \\ 8 & 5 & 30 & 32 \\ 24 & 29 & 13 & 9 \end{bmatrix} \equiv \begin{bmatrix} 18 & 15 & 17 & 8 \end{bmatrix} \pmod{37},$$

$$P_2 = (C_2 - B)K^{-1} = (\begin{bmatrix} 20 & 21 & 24 & 14 \end{bmatrix} - \begin{bmatrix} 7 & 5 & 24 & 28 \end{bmatrix}) \times \begin{bmatrix} 7 & 5 & 31 & 32 \\ 24 & 28 & 13 & 8 \\ 8 & 5 & 30 & 32 \\ 24 & 29 & 13 & 9 \end{bmatrix} \equiv \begin{bmatrix} 13 & 6 & 36 & 8 \end{bmatrix} \pmod{37},$$

$$P_3 = (C_3 - B)K^{-1} = (\begin{bmatrix} 28 & 3 & 22 & 35 \end{bmatrix} - \begin{bmatrix} 7 & 5 & 24 & 28 \end{bmatrix}) \times \begin{bmatrix} 7 & 5 & 31 & 32 \\ 24 & 28 & 13 & 8 \\ 8 & 5 & 30 & 32 \\ 24 & 29 & 13 & 9 \end{bmatrix} \equiv \begin{bmatrix} 18 & 36 & 1 & 4 \end{bmatrix} \pmod{37},$$

$$P_4 = (C_4 - B)K^{-1} = (\begin{bmatrix} 17 & 4 & 33 & 17 \end{bmatrix} - \begin{bmatrix} 7 & 5 & 24 & 28 \end{bmatrix}) \times \begin{bmatrix} 7 & 5 & 31 & 32 \\ 24 & 28 & 13 & 8 \\ 8 & 5 & 30 & 32 \\ 24 & 29 & 13 & 9 \end{bmatrix} \equiv \begin{bmatrix} 0 & 20 & 19 & 8 \end{bmatrix} \pmod{37},$$

$$P_5 = (C_5 - B)K^{-1} = (\begin{bmatrix} 31 & 24 & 16 & 25 \end{bmatrix} - \begin{bmatrix} 7 & 5 & 24 & 28 \end{bmatrix}) \times \begin{bmatrix} 7 & 5 & 31 & 32 \\ 24 & 28 & 13 & 8 \\ 8 & 5 & 30 & 32 \\ 24 & 29 & 13 & 9 \end{bmatrix} \equiv \begin{bmatrix} 5 & 20 & 11 & 36 \end{bmatrix} \pmod{37},$$

and the plaintext is obtained.

We now introduce a new algorithm by using Fibonacci–Mersenne p-matrix.

Algorithm 2

First, Bob sends $n \geq 6,\ k \geq 3,\ k \neq 36q (q \in \mathbb{Z})$, and $p \geq 3$ to Alice. Then, Alice employs the encryption algorithm to get the ciphertext.

Encryption:

Step 1. Divide the plaintext into blocks of size $1 \times (p+3)$.

Step 2. Construct the key matrix $K := (M_p(k))^n$ and $B := [FM^k_{n+p}(p), FM^k_{n+p+4}(p), \ldots, FM^k_{n+2p+2}(p)]$. We have that $K \equiv K \pmod{37}$ and $B \equiv B \pmod{37}$.

Step 3. Calculate $C_i \equiv (P_i K + B) \pmod{37}$.

Step 4. Obtain the ciphertext.

Decryption:

Step 1. Using K and B, calculate $P \equiv (C - B)K^{-1} \pmod{37}$.

Step 2. Using Table 1, obtain the plaintext.

The algorithm is illustrated in the following example.

Example 4.3. *Bob sends $p = 4, k = 3$, and $n = 7$ to Alice. Using the plaintext in Example 4.1 gives*

$$(M_4(3))^7 = \begin{bmatrix} -214 & 739 & -519 & 2 & 3 & 218 & -520 \\ -130 & 306 & -171 & 1 & 2 & 133 & -172 \\ -43 & 42 & 5 & 1 & 1 & 45 & 4 \\ 1 & -47 & 49 & 1 & 1 & 0 & 48 \\ 12 & -47 & 37 & 1 & 1 & -11 & 36 \\ 9 & -24 & 16 & 1 & 1 & -8 & 16 \\ 4 & -7 & 4 & 1 & 1 & -3 & 4 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 8 & 36 & 36 & 2 & 3 & 33 & 35 \\ 18 & 10 & 14 & 1 & 2 & 22 & 13 \\ 31 & 5 & 5 & 1 & 1 & 8 & 4 \\ 1 & 27 & 12 & 1 & 1 & 0 & 11 \\ 12 & 27 & 0 & 1 & 1 & 26 & 36 \\ 9 & 13 & 16 & 1 & 1 & 29 & 16 \\ 4 & 30 & 4 & 1 & 1 & 34 & 4 \end{bmatrix} \pmod{37},$$

$$\begin{aligned} B &= [FM^3_{11}(4),\ FM^3_{12}(4),\ FM^3_{13}(4),\ FM^3_{14}(4),\ FM^3_{15}(4),\ FM^3_{16}(4),\ FM^3_{17}(4)] \\ &= [-43, -130, -214, -177, 511, 2009, 3994] \equiv [31, 18, 8, 2, 30, 11, 35] \pmod{37}. \end{aligned}$$

Now, calculate $C_i \equiv (P_iK + B) \pmod{37}$*:*

$$P_1 = [\mathtt{S}, \mathtt{P}, \mathtt{R}, \mathtt{I}, \mathtt{N}, \mathtt{G}, \mathtt{\sqcup}],$$
$$P_2 = [\mathtt{I}, \mathtt{S}, \mathtt{\sqcup}, \mathtt{B}, \mathtt{E}, \mathtt{A}, \mathtt{U}],$$
$$P_3 = [\mathtt{T}, \mathtt{I}, \mathtt{F}, \mathtt{U}, \mathtt{L}, \mathtt{\sqcup}, \mathtt{\sqcup}],$$

so

$$C_1 = \begin{bmatrix}18 & 15 & 17 & 8 & 13 & 6 & 36\end{bmatrix} \begin{bmatrix}8 & 36 & 36 & 2 & 3 & 33 & 35\\ 18 & 10 & 14 & 1 & 2 & 22 & 13\\ 31 & 5 & 5 & 1 & 1 & 8 & 4\\ 1 & 27 & 12 & 1 & 1 & 0 & 11\\ 12 & 27 & 0 & 1 & 1 & 26 & 36\\ 9 & 13 & 16 & 1 & 1 & 29 & 16\\ 4 & 30 & 4 & 1 & 1 & 34 & 4\end{bmatrix} + \begin{bmatrix}31 & 18 & 8 & 2 & 30 & 11 & 35\end{bmatrix}$$
$$\equiv \begin{bmatrix}1 & 36 & 29 & 29 & 9 & 32 & 22\end{bmatrix} \pmod{37},$$

$$C_2 = \begin{bmatrix}8 & 18 & 36 & 1 & 4 & 0 & 20\end{bmatrix} \begin{bmatrix}8 & 36 & 36 & 2 & 3 & 33 & 35\\ 18 & 10 & 14 & 1 & 2 & 22 & 13\\ 31 & 5 & 5 & 1 & 1 & 8 & 4\\ 1 & 27 & 12 & 1 & 1 & 0 & 11\\ 12 & 27 & 0 & 1 & 1 & 26 & 36\\ 9 & 13 & 16 & 1 & 1 & 29 & 16\\ 4 & 30 & 4 & 1 & 1 & 34 & 4\end{bmatrix} + \begin{bmatrix}31 & 18 & 8 & 2 & 30 & 11 & 35\end{bmatrix}$$
$$\equiv \begin{bmatrix}36 & 32 & 6 & 29 & 3 & 4 & 3\end{bmatrix} \pmod{37},$$

$$C_3 = \begin{bmatrix}19 & 8 & 5 & 20 & 11 & 36 & 36\end{bmatrix} \begin{bmatrix}8 & 36 & 36 & 2 & 3 & 33 & 35\\ 18 & 10 & 14 & 1 & 2 & 22 & 13\\ 31 & 5 & 5 & 1 & 1 & 8 & 4\\ 1 & 27 & 12 & 1 & 1 & 0 & 11\\ 12 & 27 & 0 & 1 & 1 & 26 & 36\\ 9 & 13 & 16 & 1 & 1 & 29 & 16\\ 4 & 30 & 4 & 1 & 1 & 34 & 4\end{bmatrix} + \begin{bmatrix}31 & 18 & 8 & 2 & 30 & 11 & 35\end{bmatrix}$$
$$\equiv \begin{bmatrix}29 & 10 & 13 & 14 & 26 & 4 & 14\end{bmatrix} \pmod{37},$$

Therefore, the ciphertext is

B␣33J6W␣6G3DED3KNO0EO

For the decryption, using $K^{-1} := (M_4(3))^{(-7)}$ *and* B*, calculate* $P \equiv (C - B)K^{-1} \pmod{37}$*.*

$$P_1 = (C_1 - B)K^{-1} = (\begin{bmatrix} 1 & 36 & 29 & 29 & 9 & 32 & 22 \end{bmatrix} - \begin{bmatrix} 31 & 18 & 8 & 2 & 30 & 11 & 35 \end{bmatrix})$$
$$\times \begin{bmatrix} 8 & 36 & 36 & 2 & 3 & 33 & 35 \\ 18 & 10 & 14 & 1 & 2 & 22 & 13 \\ 31 & 5 & 5 & 1 & 1 & 8 & 4 \\ 1 & 27 & 12 & 1 & 1 & 0 & 11 \\ 12 & 27 & 0 & 1 & 1 & 26 & 36 \\ 9 & 13 & 16 & 1 & 1 & 29 & 16 \\ 4 & 30 & 4 & 1 & 1 & 34 & 4 \end{bmatrix}^{-7} \equiv \begin{bmatrix} 18 & 15 & 17 & 8 & 13 & 6 & 36 \end{bmatrix} \pmod{37},$$

$$P_2 = (C_2 - B)K^{-1} = (\begin{bmatrix} 36 & 32 & 6 & 29 & 3 & 4 & 3 \end{bmatrix} - \begin{bmatrix} 31 & 18 & 8 & 2 & 30 & 11 & 35 \end{bmatrix})$$
$$\times \begin{bmatrix} 8 & 36 & 36 & 2 & 3 & 33 & 35 \\ 18 & 10 & 14 & 1 & 2 & 22 & 13 \\ 31 & 5 & 5 & 1 & 1 & 8 & 4 \\ 1 & 27 & 12 & 1 & 1 & 0 & 11 \\ 12 & 27 & 0 & 1 & 1 & 26 & 36 \\ 9 & 13 & 16 & 1 & 1 & 29 & 16 \\ 4 & 30 & 4 & 1 & 1 & 34 & 4 \end{bmatrix}^{-7} \equiv \begin{bmatrix} 8 & 18 & 36 & 1 & 4 & 0 & 20 \end{bmatrix} \pmod{37},$$

$$P_3 = (C_3 - B)K^{-1} = (\begin{bmatrix} 29 & 10 & 13 & 14 & 26 & 4 & 14 \end{bmatrix} - \begin{bmatrix} 31 & 18 & 8 & 2 & 30 & 11 & 35 \end{bmatrix})$$
$$\times \begin{bmatrix} 8 & 36 & 36 & 2 & 3 & 33 & 35 \\ 18 & 10 & 14 & 1 & 2 & 22 & 13 \\ 31 & 5 & 5 & 1 & 1 & 8 & 4 \\ 1 & 27 & 12 & 1 & 1 & 0 & 11 \\ 12 & 27 & 0 & 1 & 1 & 26 & 36 \\ 9 & 13 & 16 & 1 & 1 & 29 & 16 \\ 4 & 30 & 4 & 1 & 1 & 34 & 4 \end{bmatrix}^{-7} \equiv \begin{bmatrix} 19 & 8 & 5 & 20 & 11 & 36 & 36 \end{bmatrix} \pmod{37},$$

and the plaintext obtained is

SPRING IS BEAUTIFUL

Now, we consider encryption using the Fibonacci-balancing p-sequences. The approach is similar to that for the Fibonacci–Mersenne p-sequences, but Bob sends $m \geq 1$ instead of k and Step 1 put $K = B_m(p)^n$, and $B = [HB^m_{n+p}(p), HB^m_{n+p+1}(p), \ldots, HB^m_{n+2p+2}(p)]$.

Here, we study security strength and analysis for these algorithms.

The order of the general linear group, denoted by $GL_\lambda(F_p)$, is

$$| GL_\lambda(F_p) | = (p^\lambda - p^{\lambda-1})(p^\lambda - p^{\lambda-2}) \cdots (p^\lambda - 1).$$

This group consists of all invertible matrices of order $\lambda \times \lambda$ over F_{37} [8]. In this method, matrices M^n_p and B^n_p are used to construct the Affine–Hill cipher encryption key. Note that these matrices

are over F_p. Therefore, the matrices M_p^n and B_p^n are needed to obtain the cipher key. We have

$$\mid GL_{p+3}(F_{37}) \mid = (37^{p+3} - 37^{p+2})(37^{p+3} - 37^{p+1}) \cdots (37^{p+3} - 1),$$

so to obtain the key an attacker needs to check a large number of matrices which confirms that the key is strong. For example, if $p = 47$ we have

$$\mid GL_{50}(F_{37}) \mid = (37^{50} - 37^{49})(37^{50} - 37^{48}) \cdots (37^{50} - 1) = 3.105165707300569 \times 10^{3920}.$$

Therefore, an attacker needs to check 10^{3920} matrices which is intractable.

5 Conclusion

In this paper, two new sequences were defined using the Fibonacci p-numbers, the generalized Mersenne numbers, and m-balancing numbers. A public key cipher was developed which use three parameters k, n, n and p which are known only to Alice and Bob. It was shown that breaking this system is intractable which ensures the security of the data.

References

[1] Acharya, B., Rath, G. S., Patra, S. K., & Panigrahy, S.K. (2007). Novel methods of generating self-invertible matrix for Hill cipher algorithm. *International Journal of Security*, 1(1), 14–21.

[2] Behera, A., & Panda, G. K. (1999). On the square roots of triangular numbers. *The Fibonacci Quarterly*, 37(2), 98–105.

[3] Chen, W.Y.C., & Louck, J. D. (1996). The combinatorial power of the companion matrix. *Linear Algebra and Its Applications*, 232, 261–278.

[4] Deveci, Ö. (2013). The k-nacci sequences and the generalized order k-Pell sequences in the semi-direct product of finite cyclic groups. *Chiang Mai Journal of Science*, 40(1), 89–98.

[5] Deveci, Ö., Hulku, S., & Shannon, A. G. (2021). On the co-complex-type k-Fibonacci numbers. *Chaos, Solitons & Fractals*, 153(2), Article ID 111522.

[6] Deveci, Ö., & Shannon. A. G. (2021). The complex-type k-Fibonacci sequences and their applications. *Communications in Algebra*, 49(3), 1352–1367.

[7] Gautam, R. (2018). Balancing numbers and application. *Journal of Advanced College of Engineering and Management*, 4, 137–143.

[8] Grillet, P. A. (2007). *Abstract Algebra* (2nd ed.). Graduate Texts in Mathematics Series, Vol. 242, Springer, Berlin.

[9] Hashemi, M., & Mehraban, E. (2021). The generalized order $k-$Pell sequences in some special groups of nilpotency class 2. *Communication in Algebra*, 50(4), 1768–1784.

[10] Hashemi, M., & Mehraban, E. (2022). An application of the t-extension of the p-Fibonacci Pascal matrix in coding theory. *Advances in Mathematical Physics*, (2022), Article ID 4619136.

[11] Hashemi, M., & Mehraban, E. (2023). Fibonacci length and the generalized order k-Pell sequences of the 2-generator p-groups of nilpotency class 2. *Journal of Algebra and Its Applications*, 22(3), Article ID 2350061.

[12] Hill, L. S. (1929). Cryptography in an algebraic alphabet. *The American Mathematical Monthly*, 36(6), 306–31.

[13] Hiller, J., Aküzüm, Y., & Deveci, Ö. (2018). The adjacency-Pell–Hurwitz numbers. *Integers*, 18, Article ID A83.

[14] Mehraban, E., Deveci, Ö., & Hincal, E. (2024). The generalized order (k, t)-Mersenne sequences in groups. *Notes on Number Theory and Discrete Mathematics*, 30(2), 271–282.

[15] Mehraban, E., & Hashemi, M. (2023). Coding theory on the generalized balancing sequence. *Notes on Number Theory and Discrete Mathematics*, 29(3), 503–524.

[16] Ochalik, P., & Włoch, A. (2018). On generalized Mersenne numbers, their interpretations and matrix generators. *Annales Universitatis Mariae Curie-Sklodowska, Sectio A Mathematica*, 72(1), 69–76.

[17] Özkoç, A. (2015). Tridiagonal matrices via k-balancing number. *Journal of Advances in Mathematics and Computer Science*, 10(4), 1–11.

[18] Özkoç, A., & Tekcan, A. (2017). On k-balancing numbers. *Notes on Number Theory and Discrete Mathematics*, 23(3), 38–52.

[19] Prasad, K., & Mahato, H. (2022). Cryptography using generalized Fibonacci matrices with Affine–Hill cipher. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(8), 2341–2352.

[20] Prasad, M. G. V., Chari, P. P. P., & Satyam, K. P. (2016). Affine Hill cipher key generation matrix of order 3 by using reflects in an arbitrary line $y = ax + b$. *International Journal of Science Technology and Management*, 5(8), 268–272.

[21] Stakhov, A. P. (2006). Fibonacci matrices, a generalization of the "Cassini formula", and a new coding theory. *Chaos, Solitons & Fractals*, 30(1), 56–66.

[22] Stinson, D. R. (2006). *Cryptography: Theory and Practice* (3rd ed.). Chapman and Hall/CRC, Boca Raton, FL.