J. Appl. & Pure Math. Vol. 6(2024), No. 1 - 2, pp. 37 - 45
https://doi.org/10.23091/japm.2024.037

ITERATION OF 2×2 MATRICES IN $\mathbb{Z}_4$ AND THEIR FOUR COLOR EXPRESSIONS (I)[†]

DAEYEOUL KIM

Abstract. The aim of this article is to consider the sequences generated by repeatedly performing matrix multiplication operations, define the stable, amicable pair, sociable matrix sequences, and analyze the results obtained through iteration. Lastly, numbers are changed to colors to make them easier to understand.

AMS Mathematics Subject Classification : 11A25
Key words and phrases : Iterated matrix, amicable pairs.

1. Introduction

We first clarify that the results of this article may not be new results, but we hope that they will be understood as the results of reinterpreting the meaning of the newly iteration matrix. The Cayley-Hamilton theorem [5, p.70-71] states that square matrix over a commutative ring satisfies its own characteristic equation. In particular, for 2×2 matrix, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, the characteristic polynomial [3, p.200] is given by $p(X) := X^2 - (a+d)X + (ad-bc)$, so the Cayley-Hamilton theorem states that

$$p(A) := A^2 - (a+d)A + (ad-bc)I = O. \tag{1}$$

Here, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $A^n := \underbrace{A \cdots A}_{n \text{ times}}$.

Received November 13, 2023. Revised January 6, 2024. Accepted January 11, 2024.
*Corresponding author.
[†]This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2021R1F1A1051093).
© 2024 KSCAM.

Let $\mathbb{Z}_4$ be the ring of residue classes modulo 4,

$$M_2(\mathbb{Z}_4) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, b, c, d \in \mathbb{Z}_4 \right\}$$

and

$$M_2^d(\mathbb{Z}_4) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_4) | a, b, c, d \text{ are all distinct} \right\}.$$

We easily know that $|M_2(\mathbb{Z}_4)| = 4^4$ and $|M_2^d(\mathbb{Z}_4)| = 24$.

To understand $M_2^d(\mathbb{Z}_4)$ accurately, let the elements of $M_2^d(\mathbb{Z}_4)$ be

$$A_1 := \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix}, \quad A_2 := \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}, \quad A_3 := \begin{pmatrix} 0 & 2 \\ 1 & 3 \end{pmatrix}, \quad A_4 := \begin{pmatrix} 0 & 1 \\ 3 & 2 \end{pmatrix},$$
$$A_5 := \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}, \quad A_6 := \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}, \quad A_7 := \begin{pmatrix} 0 & 2 \\ 3 & 1 \end{pmatrix}, \quad A_8 := \begin{pmatrix} 1 & 3 \\ 2 & 0 \end{pmatrix},$$
$$A_9 := \begin{pmatrix} 1 & 0 \\ 3 & 2 \end{pmatrix}, \quad A_{10} := \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}, \quad A_{11} := \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix}, \quad A_{12} := \begin{pmatrix} 0 & 3 \\ 1 & 2 \end{pmatrix},$$
$$A_{13} := \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix}, \quad A_{14} := \begin{pmatrix} 2 & 3 \\ 1 & 0 \end{pmatrix}, \quad A_{15} := \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}, \quad A_{16} := \begin{pmatrix} 2 & 1 \\ 3 & 0 \end{pmatrix},$$
$$A_{17} := \begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix}, \quad A_{18} := \begin{pmatrix} 2 & 0 \\ 3 & 1 \end{pmatrix}, \quad A_{19} := \begin{pmatrix} 3 & 0 \\ 1 & 2 \end{pmatrix}, \quad A_{20} := \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix},$$
$$A_{21} := \begin{pmatrix} 3 & 1 \\ 0 & 2 \end{pmatrix}, \quad A_{22} := \begin{pmatrix} 3 & 1 \\ 2 & 0 \end{pmatrix}, \quad A_{23} := \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix}, \quad A_{24} := \begin{pmatrix} 3 & 2 \\ 1 & 0 \end{pmatrix}.$$

Let $\mathfrak{A}_i : A_i \to A_i^2 \to A_i^3 \to ...$ be the matrix sequence of A_i.

A sociable(periodic) matrix sequence $\mathfrak{A}_i$ is a sequence for which the same terms are repeated over and over:

$$\cdots \to A_i^m \to \cdots \to A_i^{m+l} \to A_i^m \to \cdots \to A_i^{m+l} \to \cdots .$$

if $l = 0$, that is,

$$\cdots \to A_i^{m-1} \to A_i^m \to A_i^m \to A_i^m \to \cdots ,$$

then $\mathfrak{A}_i$ is a stable matrix sequence, and if $l = 1$, that is,

$$\cdots \to A_i^{m-1} \to A_i^m \to A_i^{m+1} \to A_i^m \to A_i^{m+1} \to A_i^m \to A_i^{m+1} \to \cdots ,$$

$\mathfrak{A}_i$ is an amicable pair matrix sequence for some $m \in \mathbb{N}$. Referring to Figure 1, it is easy to understand the notations of sociable, amicable pair and stable matrix sequence.

Let $\sum_{j=0}^{l} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{m+j} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ and $a' + b' + c' + d' \equiv k \pmod 4$.

For the three cases above, let's define $Per(\mathfrak{A}_i) = l+1$, $Ord(\mathfrak{A}_i) = m$, $Tl(\mathfrak{A}_i) = m + l$ and $Ty(\mathfrak{A}_i) = k$. We call $Per(\mathfrak{A}_i)$ the period length of $\mathfrak{A}_i$, $Ord(\mathfrak{A}_i)$ the order of $\mathfrak{A}_i$ and $Ty(\mathfrak{A}_i)$ the k-type $\mathfrak{A}_i$. If m cannot be found, that is, for sequence $\mathfrak{A}_i$ other than the three cases above, we set $Ord(\mathfrak{A}_i) = \infty$.

The concepts of stable matrix sequence, amicable pair matrix sequence, sociable matrix sequence, and order of matrix sequence were introduced exactly as defined in the iterated divisor functions defined in [1], [2].

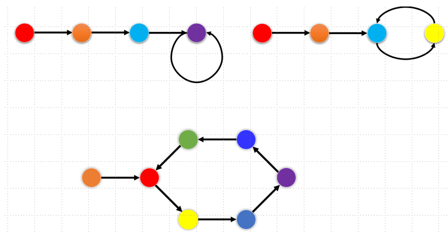

FIGURE 1. Stable, Amicable pair and Sociable matrix sequences

In this paper, the following results were obtained regarding stable, amicable, and sociable for the matrices of $M_2^d(\mathbb{Z}_4)$.

Theorem 1.1. *Let $A_i \in M_2^d(\mathbb{Z}_4)$ and $\mathfrak{A}_i$ be the matrix sequences of A_i.*

(a) $\mathfrak{A}_i$ are stable matrix sequences with $Ord(\mathfrak{A}_i) = 2$ if and only if $i \in \{3, 6, 9, 10, 13, 18, 22, 24\}$.

(b) $\mathfrak{A}_i$ are amicable matrix sequences with $Ord(\mathfrak{A}_i) = 1$ if and only if $i \in \{2, 5, 20, 23\}$.

(c) $\mathfrak{A}_i$ are amicable matrix sequences with $Ord(\mathfrak{A}_i) = 2$ if and only if $i \in \{1, 7, 8, 11, 15, 17, 19, 21\}$.

(d) $\mathfrak{A}_i$ are sociable matrix sequences with $Ord(\mathfrak{A}_i) = 1$ and $Per(\mathfrak{A}_i) = 4$ if and only if $i \in \{4, 12, 14, 16\}$.

Actually, when $k = 0$, we think the sequence is a little easier to understand. So we define a period that extends beyond the existing period. In other words, when $k = 0$, the period is called a perfect period. And the perfect period length of sequence $\mathfrak{A}_i$ is written as $P(\mathfrak{A}_i)$. For example, let's look at $\mathfrak{A}_3$ below.

$$\mathfrak{A}_3 : \ A_3 = \begin{pmatrix} 0 & 2 \\ 1 & 3 \end{pmatrix} \to A_3^2 = \begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix} \circlearrowleft .$$

Then $Per(\mathfrak{A}_3) = 1$ but $P(\mathfrak{A}_3) = 2$. If the sequence $\mathfrak{A}_3$ is expressed as a sequence in terms of a perfect period, it is

$$\mathfrak{A}_3 : \ A_1 = \begin{pmatrix} 0 & 2 \\ 1 & 3 \end{pmatrix} \to A_1^2 = \begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix} \rightleftarrows A_1^3 = \begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix}.$$

Theorem 1.2. *Let $A_i \in M_2^d(\mathbb{Z}_4)$ and $\mathfrak{A}_i$ be the matrix sequences of A_i.*

(a) There is no stable matrix with respect to the perfect period.

(b) $\mathfrak{A}_i$ are amicable matrix sequences with respect to the perfect period and $Ord(\mathfrak{A}_i) = 1$ if and only if $i \in \{2, 5, 20, 23\}$.

(c) $\mathfrak{A}_i$ are amicable matrix sequences with respect to the perfect period and $Ord(\mathfrak{A}_i) = 2$ if and only if $i \in \{1, 7, 8, 11, 15, 17, 19, 21\} \cup \{3, 6, 9, 10, 13, 18, 22, 24\}$.

(d) $\mathfrak{A}_i$ are sociable matrix sequences with respect to the perfect period and $Ord(\mathfrak{A}_i) = 1$ and $Per(\mathfrak{A}_i) = 4$ if and only if $i \in \{4, 12, 14, 16\}$.

2. Proofs of Theorem 1.1 and 1.2

Unless otherwise specified, it is assumed in this section that $A_i \in M_2^d(\mathbb{Z}_4)$ and $p(A_i) = A_i^2 + \alpha A_i + \beta E$.

Lemma 2.1. *Let* $A_{i_1} := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $A_{i_2} := \begin{pmatrix} d & b \\ c & a \end{pmatrix}$, $A_{i_3} := \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ *and* $A_{i_4} := \begin{pmatrix} d & c \\ b & a \end{pmatrix}$. *If* $k, l \in \{1, 2, 3, 4\}$ *then* $Ord(\mathfrak{A}_{i_k}) = Ord(\mathfrak{A}_{i_l})$ *and* $Per(\mathfrak{A}_{i_k}) = Per(\mathfrak{A}_{i_l})$.

Proof. It is well-known that

$$A_{i_k}^2 = (a + d)A_{i_k} - (ad - bc)I \tag{2}$$

with $k \in \{1, 2, 3, 4\}$. Using (2), there exist b and c in $\mathbb{Z}_4$ that satisfy $A_{i_k}^n = bA_{i_k} + cI$ and $A_{i_1}^n = A_{i_2}^n = A_{i_3}^n = A_{i_4}^n$ with $n \in \mathbb{N}$. Therefore, we derive the proof of Lemma 2.1. □

Lemma 2.2. *If* $\beta \equiv 1 \pmod 2$ *then* $Ord(\mathfrak{A}_i) = 1$.

Proof. Let $A_i = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. If $\beta \equiv 1 \pmod 2$ then

$$p(A_i) = A_i^2 - (a + d)A_i + (ad - bc)I \equiv A_i^2 - 2A_i + I \pmod 4 \tag{3}$$

or

$$p(A_i) \equiv A_i^2 - I \pmod{4}. \tag{4}$$

It is easily checked that $A_i^4 = I$ by (3) and (4). This completes the proof of Lemma 2.2. □

Lemma 2.3. *If* $\beta \equiv 2 \pmod 4$ *then* $Ord(\mathfrak{A}_i) = 2$.

Proof. Using $ad - bc \equiv 2 \pmod 4$ and a, b, c, d are distinct in $\mathbb{Z}_4$, we obtain $a + d \equiv 1 \pmod 2$. If $\alpha \equiv 1 \pmod 2$ then $p(A_i) \equiv A_i^2 \pm A_i + 2I \pmod 4$. So, we get

$$A_i^4 = A_i^2 \pm 4A_i + 4I = A_i^2$$

and $A_i^2 = A_i^{2k}$ with $k \in \mathbb{N}$. Since $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq \begin{pmatrix} a+2 & b \\ c & d+2 \end{pmatrix}$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq \begin{pmatrix} -a+2 & -b \\ -c & -d+2 \end{pmatrix}$, we obtain $A_i^2 \neq A_i$.

If $A_i^2 + A_i + 2I = O$ then $A_i^3 = 3A_i + 2I = -A_i + 2I = A_i^2$.

Hence, $A_i \neq A_i^2 = A_i^{2+k}$ with $k \in \mathbb{N}$.

If $A_i^2 - A_i + 2I = O$ then $A_i^3 = 3A_i + 2I \neq A_i + 2I = A_i^2$. Since $A_i \neq -I$, we derive that $A_i \neq 3A_i + 2I = A_i^3$. So, we get

$$A_i \to A_i^2 \to A_i^3 \to A_i^2 \to A_i^3 \to \cdots.$$

Lemma 2.3 is obtained. □

Proof of Theorem 1.1

The matrices that satisfy (4) are $A_2 = \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}$, $A_5 = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$, $A_{20} = \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix}$ and $A_{23} = \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix}$ by Lemma 2.1. Thus we obtain (b), that is, $A_i \to I \to A_i \to I \to \cdots$ with $i \in \{2, 5, 20, 23\}$.

By (3), (d) is obtained. In other words, it is the same as the problem of finding matrices in $M_2^d(\mathbb{Z}_4)$ that satisfy the conditions $a + d \equiv 2 \pmod 4$ and $ad - bc \equiv 1 \pmod 4$. Therefore, if ad is an even number (resp., odd number), bc is an odd number (resp., even number). The matrices that satisfy (3) are $A_4 = \begin{pmatrix} 0 & 1 \\ 3 & 2 \end{pmatrix}$, $A_{12} = \begin{pmatrix} 0 & 3 \\ 1 & 2 \end{pmatrix}$, $A_{14} = \begin{pmatrix} 2 & 3 \\ 1 & 0 \end{pmatrix}$ and $A_{16} = \begin{pmatrix} 2 & 1 \\ 3 & 0 \end{pmatrix}$ by Lemma 2.1.

Consider $A_1 = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix}$ and $A_{15} = \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}$. The characteristic polynomial of these two matrices is $p(X) \equiv X^2 - X + 2 \pmod 4$. By Lemma 2.3, $A_i \neq A_i^3 \neq A_i^2 \neq A_i$ and $A_i^2 \neq A_i^4$ with $i \in \{1, 15\}$.

By Lemma 2.1, we have that $\mathfrak{A}_i (i \in \{1, 7, 8, 11, 15, 17, 19, 21\})$ are amicable matrix sequences with $Ord(\mathfrak{A}_i) = 2$. Thus (c) is obtained.

Finally, we consider $A_3 = \begin{pmatrix} 0 & 2 \\ 1 & 3 \end{pmatrix}$ and $A_{13} = \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix}$. The characteristic polynomial of these two matrices is $p(X) \equiv X^2 + X + 2 \pmod 4$. By Lemma 2.3, $A_i \neq A_i^2 = A_i^3$ with $i \in \{3, 13\}$. By Lemma 2.1, we obtain that $\mathfrak{A}_i (i \in \{3, 6, 9, 10, 13, 18, 22, 24\})$ are stable matrix sequences with $Ord(\mathfrak{A}_i) = 2$. Thus (a) is obtained. □

Lemma 2.4. *Let* $A := \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \in M_2^d(\mathbb{Z}_4)$ *and* $A^n := \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}$ *with* $n \in \mathbb{N}$. *Then* $TS(A^n) := a_n + b_n + c_n + d_n \equiv 2 \pmod 4$.

Proof. It is easily checked that

$$a_1 + b_1 + c_1 + d_1 = 0 + 1 + 2 + 3 \equiv 2 \pmod 4.$$

If $a_1 \equiv d_1 \pmod 2$ then $a_1 + d_1 \equiv 0 \pmod 2$ and $a_1 d_1 - b_1 c_1 \equiv 1 \pmod 2$. On the other hand, if $a_1 \not\equiv d_1 \pmod 2$ then $a_1 + d_1 \equiv 1 \pmod 2$ and $a_1 d_1 - b_1 c_1 \equiv 0 \pmod 2$. Thus we obtain

$$a_1 + d_1 \not\equiv a_1 d_1 - b_1 c_1 \pmod 2. \tag{5}$$

Recall that

$$A^2 = (a + d)A - (ad - bc)E \tag{6}$$

by (1). It follows from (5) and (6) that

$$a_2 + b_2 + c_2 + d_2 \equiv 2(a_1 + d_1) + 2(a_1 d_1 - a_c c_1) \equiv 2 \pmod 4.$$

Assume that $a_i + b_i + c_i + d_i \equiv 2 \pmod 4$ with $1 \leq i \leq n - 1$. By (5), we obtain $A^n = (a + d)A^{n-1} - (ad - bc)A^{n-2}$ and

$$a_n + b_n + c_n + d_n \equiv 2(a_1 + d_1) + 2(a_1 d_1 - a_c c_1) \equiv 2 \pmod 4.$$

By induction method, we derive the proof of Lemma 2.4. □

Proof of Theorem 1.2

If $Per(\mathfrak{A}_i)$ is an even number, it can be seen from Lemma 2.4 that $Per(\mathfrak{A}_i) = P(\mathfrak{A}_i)$. Therefore, in all cases (b),(c) and (d) of Theorem 1, we obtain that $Per(\mathfrak{A}_i) = P(\mathfrak{A}_i)$. In the case of stable sequences in Theorem 1.1 (a), the value of $Per(\mathfrak{A}_i)$ becomes an odd number, so in order for $P(\mathfrak{A}_i) = 0$, it is necessary to regard them as an amicable pair even though they have the same value. In other words, it is considered an amicable pair sequence as shown below.

$$\mathfrak{A}_i:\ A_i = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \to A_i^2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \rightleftarrows A_i^3 = \begin{pmatrix} a_2 & b_2 \\ Cc_2 & d_2 \end{pmatrix}.$$

There is no stable matrix with respect to the perfect period. This completes the proof of Thoerem 1.2. □

For easy understanding, below are the calculations of whether the 24 matrix sequences($\mathfrak{A}_1 \sim \mathfrak{A}_{24}$) are stable, amicable, and sociable matrix sequence.

$\mathfrak{A}_1:\ A_1 = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \to A_1^2 = \begin{pmatrix} 3 & 2 \\ 3 & 2 \end{pmatrix} \rightleftarrows A_1^3 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix},$

$Per(\mathfrak{A}_1) = 2,\ Ord(\mathfrak{A}_1) = 2,\ Tl(\mathfrak{A}_1) = 3.$

$\mathfrak{A}_2:\ A_2 = \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix} \rightleftarrows A_2^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$

$Per(\mathfrak{A}_2) = 2,\ Ord(\mathfrak{A}_2) = 1,\ Tl(\mathfrak{A}_2) = 2.$

$\mathfrak{A}_3:\ A_3 = \begin{pmatrix} 0 & 2 \\ 1 & 3 \end{pmatrix} \to A_3^2 = \begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix} \circlearrowleft,$

$Per(\mathfrak{A}_3) = 1,\ Ord(\mathfrak{A}_1) = 2,\ Tl(\mathfrak{A}_1) = 2.$

$\mathfrak{A}_4:\ A_4 = \begin{pmatrix} 0 & 1 \\ 3 & 2 \end{pmatrix} \to A_4^2 = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix} \to A_4^3 = \begin{pmatrix} 2 & 3 \\ 1 & 0 \end{pmatrix} \to A_4^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$

$Per(\mathfrak{A}_4) = 4,\ Ord(\mathfrak{A}_4) = 1,\ Tl(\mathfrak{A}_4) = 4.$

$\mathfrak{A}_5:\ A_5 = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \rightleftarrows A_5^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$

$Per(\mathfrak{A}_5) = 2,\ Ord(\mathfrak{A}_5) = 1,\ Tl(\mathfrak{A}_5) = 2.$

$\mathfrak{A}_6:\ A_6 = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} \to A_6^2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \circlearrowleft,$

$Per(\mathfrak{A}_6) = 1,\ Ord(\mathfrak{A}_6) = 2,\ Tl(\mathfrak{A}_6) = 2.$

$\mathfrak{A}_7:\ A_7 = \begin{pmatrix} 0 & 2 \\ 3 & 1 \end{pmatrix} \to A_7^2 = \begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix} \rightleftarrows A_7^3 = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix},$

$Per(\mathfrak{A}_7) = 2,\ Ord(\mathfrak{A}_7) = 2,\ Tl(\mathfrak{A}_7) = 3.$

$\mathfrak{A}_8:\ A_8 = \begin{pmatrix} 1 & 3 \\ 2 & 0 \end{pmatrix} \to A_8^2 = \begin{pmatrix} 3 & 3 \\ 2 & 2 \end{pmatrix} \rightleftarrows A_8^3 = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix},$

$Per(\mathfrak{A}_8) = 2,\ Ord(\mathfrak{A}_8) = 2,\ Tl(\mathfrak{A}_8) = 3.$

$\mathfrak{A}_9:\ A_9 = \begin{pmatrix} 1 & 0 \\ 3 & 2 \end{pmatrix} \to A_9^2 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \circlearrowleft,$

$Per(\mathfrak{A}_9) = 1,\ Ord(\mathfrak{A}_9) = 2,\ Tl(\mathfrak{A}_9) = 2.$

$\mathfrak{A}_{10}:\ A_{10} = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \to A_{10}^2 = \begin{pmatrix} 2 & 3 \\ 2 & 3 \end{pmatrix} \circlearrowleft,$

$Per(\mathfrak{A}_{10}) = 1,\ Ord(\mathfrak{A}_{10}) = 2,\ Tl(\mathfrak{A}_{10}) = 2.$

$$\mathfrak{A}_{11}: \ A_{11} = \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} \to A_{11}^2 = \begin{pmatrix} 2 & 3 \\ 2 & 3 \end{pmatrix} \rightleftarrows A_{11}^3 = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix},$$

$Per(\mathfrak{A}_{11}) = 2$, $Ord(\mathfrak{A}_{11}) = 2$, $Tl(\mathfrak{A}_{11}) = 3$.

$$\mathfrak{A}_{12}: \ A_{12} = \underleftarrow{\begin{pmatrix} 0 & 3 \\ 1 & 2 \end{pmatrix} \to A_{12}^2 = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix} \to A_{12}^3 = \begin{pmatrix} 2 & 1 \\ 3 & 0 \end{pmatrix} \to A_{12}^4 =} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$Per(\mathfrak{A}_{12}) = 4$, $Ord(\mathfrak{A}_{12}) = 1$, $Tl(\mathfrak{A}_{12}) = 4$.

$$\mathfrak{A}_{13}: \ A_{13} = \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix} \to A_{13}^2 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \circlearrowleft,$$

$Per(\mathfrak{A}_{13}) = 1$, $Ord(\mathfrak{A}_{13}) = 2$, $Tl(\mathfrak{A}_{13}) = 2$.

$$\mathfrak{A}_{14}: \ A_{14} = \underleftarrow{\begin{pmatrix} 2 & 3 \\ 1 & 0 \end{pmatrix} \to A_{14}^2 = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix} \to A_{14}^3 = \begin{pmatrix} 0 & 1 \\ 3 & 2 \end{pmatrix} \to A_{14}^4 =} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$Per(\mathfrak{A}_{14}) = 4$, $Ord(\mathfrak{A}_{14}) = 1$, $Tl(\mathfrak{A}_{14}) = 4$.

$$\mathfrak{A}_{15}: \ A_{15} = \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix} \to A_{15}^2 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \rightleftarrows A_{15}^3 = \begin{pmatrix} 0 & 3 \\ 0 & 3 \end{pmatrix},$$

$Per(\mathfrak{A}_{15}) = 2$, $Ord(\mathfrak{A}_{15}) = 2$, $Tl(\mathfrak{A}_{15}) = 3$.

$$\mathfrak{A}_{16}: \ A_{16} = \underleftarrow{\begin{pmatrix} 2 & 1 \\ 3 & 0 \end{pmatrix} \to A_{16}^2 = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix} \to A_{16}^3 = \begin{pmatrix} 0 & 3 \\ 1 & 2 \end{pmatrix} \to A_{16}^4 =} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$Per(\mathfrak{A}_{16}) = 4$, $Ord(\mathfrak{A}_{16}) = 1$, $Tl(\mathfrak{A}_{16}) = 4$.

$$\mathfrak{A}_{17}: \ A_{17} = \begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix} \to A_{17}^2 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \rightleftarrows A_{17}^3 = \begin{pmatrix} 0 & 0 \\ 3 & 3 \end{pmatrix},$$

$Per(\mathfrak{A}_{17}) = 2$, $Ord(\mathfrak{A}_{17}) = 2$, $Tl(\mathfrak{A}_{17}) = 3$.

$$\mathfrak{A}_{18}: \ A_{18} = \begin{pmatrix} 2 & 0 \\ 3 & 1 \end{pmatrix} \to A_{18}^2 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \circlearrowleft,$$

$Per(\mathfrak{A}_{18}) = 1$, $Ord(\mathfrak{A}_{18}) = 2$, $Tl(\mathfrak{A}_{18}) = 2$.

$$\mathfrak{A}_{19}: \ A_{19} = \begin{pmatrix} 3 & 0 \\ 1 & 2 \end{pmatrix} \to A_{19}^2 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \rightleftarrows A_{19}^3 = \begin{pmatrix} 3 & 0 \\ 3 & 0 \end{pmatrix},$$

$Per(\mathfrak{A}_{19}) = 2$, $Ord(\mathfrak{A}_{19}) = 2$, $Tl(\mathfrak{A}_{19}) = 3$.

$$\mathfrak{A}_{20}: \ A_{20} = \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix} \rightleftarrows A_{20}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$Per(\mathfrak{A}_{20}) = 2$, $Ord(\mathfrak{A}_{20}) = 1$, $Tl(\mathfrak{A}_{20}) = 2$.

$$\mathfrak{A}_{21}: \ A_{21} = \begin{pmatrix} 3 & 1 \\ 0 & 2 \end{pmatrix} \to A_{21}^2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \rightleftarrows A_{21}^3 = \begin{pmatrix} 3 & 3 \\ 0 & 0 \end{pmatrix},$$

$Per(\mathfrak{A}_{21}) = 2$, $Ord(\mathfrak{A}_{21}) = 2$, $Tl(\mathfrak{A}_{21}) = 3$.

$$\mathfrak{A}_{22}: \ A_{22} = \begin{pmatrix} 3 & 1 \\ 2 & 0 \end{pmatrix} \to A_{22}^2 = \begin{pmatrix} 3 & 3 \\ 2 & 2 \end{pmatrix} \circlearrowleft,$$

$Per(\mathfrak{A}_{22}) = 1$, $Ord(\mathfrak{A}_{22}) = 2$, $Tl(\mathfrak{A}_{22}) = 2$.

$$\mathfrak{A}_{23}: \ A_{23} = \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \rightleftarrows A_{23}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$Per(\mathfrak{A}_{23}) = 1$, $Ord(\mathfrak{A}_{23}) = 2$, $Tl(\mathfrak{A}_{23}) = 2$.

$$\mathfrak{A}_{24}: \ A_{24} = \begin{pmatrix} 3 & 2 \\ 1 & 0 \end{pmatrix} \to A_{24}^2 = \begin{pmatrix} 3 & 2 \\ 3 & 2 \end{pmatrix} \circlearrowleft,$$

$Per(\mathfrak{A}_{24}) = 1$, $Ord(\mathfrak{A}_{24}) = 2$, $Tl(\mathfrak{A}_{24}) = 2$.

3. Maxtrix sequences expressed in 4 colors

First, let's change $0, 1, 2$, and 3 to to four colors as shown in Figure 2.

FIGURE 2. Four colors: $0, 1, 2, 3$

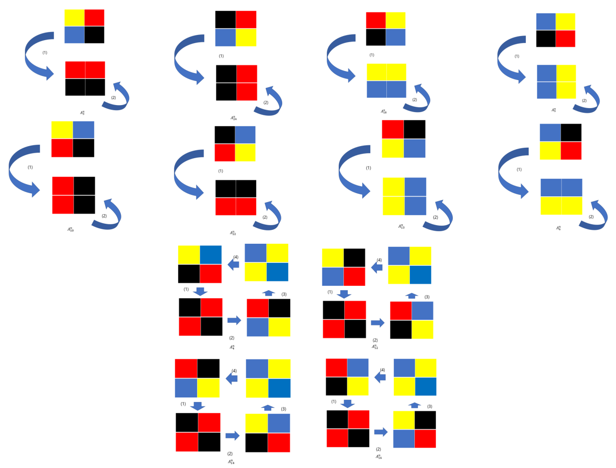

FIGURE 3. Stable and Sociable matrix sequences

The cases of the stable matrix sequences (Figure 3), the amicable pair matrix sequences (Figure 4), and the sociable matrix sequences (Figure 3) are represented in Figure 3, 4. It is easy to understand that the four matrices that satisfy Lemma 2.1 have the same form as long as the positions are changed.

That is, in fact, we only need to check whether the six matrix sequences($\mathfrak{A}_1$, $\mathfrak{A}_2$, $\mathfrak{A}_3$, $\mathfrak{A}_4$, $\mathfrak{A}_6$, $\mathfrak{A}_{15}$) are amicable, sociable, and stable.

Looking at the Figures 3 and 4, it is very easy to understand how the matrix sequence changes.

Remark 3.1. Looking at Figure 3 and 4, $A_i^4 = I$ but $A_i^2 = -I$ cannot be found in $M_2^d(\mathbb{Z}_4)$. In other words, we can see that the matrix A_i that satisfies $A_i^2 = -I$ does not exist in $M_2^d(\mathbb{Z}_4)$. This may not seem difficult even using the Cayley-Hamilton theorem.

Remark 3.2. It is well known [4, p.89] that the 4-torsion group in elliptic curves has the structure of $\mathbb{Z}_4 \oplus \mathbb{Z}_4$. The 24 matrix sequences of this article can also be interpreted as the endormorphism of $E[4]$. Here, $E[4] = \{P \in E | 4P = \infty\}$ and ∞ is the point at infiinity in E.

4. Discussion

Matrices are a very fundamental research topic in economics, physics, biology, and engineering. Matrix theory is also fundamentally used in the fields of AI,

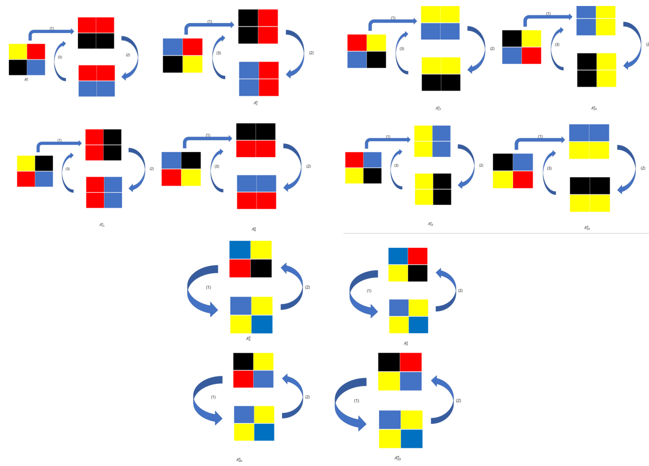

FIGURE 4. Amicable pair matrix sequences

robotics, and medical mathematics, which have been actively studied recently. The iterated matrix defined on $\mathbb{Z}_4$ studied in this paper can be usefully used to find the automorphism group of an elliptic curve. Future research will be conducted on the results for the overall case, rather than for different cases, and the study is planned to utilize this to construct a polyhedron. Lastly, in the future, the structures obtained from subgroups obtained through repeated execution of matrices have interesting structures, and we plan to conduct joint research with researchers majoring in art.

Conflicts of interest : The author declares no conflict of interest.

Data availability : Not applicable

References

1. D. Kim and A. Bayad, *Polygon numbers associated with the sum of odd divisors function*, Exp. Math. **26** (2017), 287-297.
2. D. Kim, A. Bayad and S. Park, *Iterated stable numbers and iterated amicable pairs*, Mathematical Methods in the Applied Sciences **44** (2021), 12479-12499.
3. S. Lang, *Linear Algebra*, Springer-Velag, 1987.
4. J.H. Silvermann, *The arithmetic of Elliptic curves*, Springer-Velag, 1992.
5. F. Zhang, *Matrix Theory*, Springer, 1999.

Daeyeoul Kim received Ph.D. degree from Jeonbuk National University. His research interests focus on number theory.

Department of Mathematics and Institute of Pure and Applied Mathematics, Jeonbuk National University, 567 aekje-daero, Deokjin-gu, Jeonju-si, Jeollabuk-do, 54896, Republic of Korea.
e-mail: kdaeyeoul@jbnu.ac.kr