Songklanakarin J. Sci. Technol.
45 (2), 308–313, Mar. – Apr. 2023

http://www.sjst.psu.ac.th

Original Article

$*$-Regularity in the ring of matrices over the ring of integers modulo n

Wannisa Apairat and Sompong Chuysurichay*

Division of Computational Science, Faculty of Science,
Prince of Songkla University, Hat Yai, Songkhla, 90110 Thailand

Received: 1 November 2022; Revised: 2 February 2023; Accepted: 9 March 2023

Abstract

For any positive integer $n \geq 2$, we give necessary and sufficient conditions of the existence of the Moore-Penrose inverse of any square matrix over the ring of integers modulo n. In particular, the formula for the Moore-Penrose inverse of any 2×2 matrix is also explained if it exists. We also characterize all values of k and n for which the ring of all $k \times k$ matrices over the ring of integers modulo n is $*$-regular with respect to the matrix transposition as an involution. It turns out that the ring of $k \times k$ matrices over the ring of integers modulo n is $*$-regular if and only if n is square-free and either $k = 1$ or $k = 2$ and each prime divisor of n must have the form $4m + 3$ for some nonnegative integer m.

Keywords: Moore-Penrose inverse, $*$-regular ring, regular number

1. Introduction

The Moore-Penrose inverse is a type of a generalized inverse defined and developed on the set of matrices over some particular rings by E. H. Moore and R. Penrose (Moore, 1920; Penrose, 1955). It has been explored extensively over various fields such as polynomial rings, integral domains (Bapat, Rao, & Prasad, 1990; Rao, 1983) and also been used in other perspectives such as the least squares method in statistics (Ben-Israel & Greville, 2003). Many authors have developed several necessary and sufficient conditions for the existence of the Moore-Penrose inverses since the discovery. Bapat, Rao and Prasad have studied the generalized inverses over the integral domains and one of their results has shown that a matrix A over an integral domain with rank r has the Moore-Penrose inverse if and only if the sum of squares of all $r \times r$ minors of A is an invertible element (Bapat *et al.*, 1990). Zhu, Chen, Zhang and Patrício have studied representations of the Moore-Penrose inverse of 2×2 matrices over a $*$-regular ring with two terms $*$-cancellation and presented some formulae of the Moore Penrose inverses (Zhu, Chen, Zhang, & Patrício, 2014). The ring of integers modulo n, denoted by $\mathbb{Z}_n$ is a simple ring in the literature yet various types of ring structures sit inside this small but it is the classical one. To study the ring of matrices over this type of ring, we need to combine some known facts from elementary number theory and linear algebra. All of these matters inspire us to study the Moore-Penrose inverse of $k \times k$ matrices over $\mathbb{Z}_n$, to extend and simplify the formulae seen in the work of Zhu *et al.* (2014) and also to classify the $*$-regularity in the ring of $k \times k$ matrices over $\mathbb{Z}_n$ by using the existence property of the Moore-Penrose inverse.

The focus of this paper is two-fold. Firstly, we give necessary and sufficient conditions for the existence of the Moore-Penrose inverse in any square matrix over $\mathbb{Z}_n$. The Chinese Remainder Theorem will give reduction of calculation to the (reduced) matrix over the ring of integers modulo prime powers in the prime factorization of n. In the case of 2×2 matrix, an explicit formula for any Moore-Penrose invertible matrix is presented. Let p be a prime number and suppose that M is a 2×2 matrix over $\mathbb{Z}_p m$ with $u = \det(M)$ and v = sum of squares of all entries of M. We prove that the Moore-Penrose inverse of M exists if and only if u is a unit in $\mathbb{Z}_p m$ and the Moore-Penrose inverse of M is given by u^{-1} adj(M) where adj(M) is the adjoint matrix of M, or else u must be zero in $\mathbb{Z}_p m$ and v is a unit in $Z_p m$ and the Moore-Penrose inverse of M is given by $v^{-1}M^T$, where M^T is the transpose of M. By Applying the Chinese Remainder Theorem, we can extend the results to the general 2×2 matrices over $\mathbb{Z}_n$. We still do not know whether similar formulae exist for $k \times k$ matrices where $k \geq 3$. Nevertheless, the Chinese Remainder Theorem allows us to

*Corresponding author
Email address: sompong.c@psu.ac.th

work on the ring of $k \times k$ matrices over $\mathbb{Z}_{p^m}$, where p is a prime number and m is a positive integer, as we factorize the modulus n into a product of distinct prime powers.

Secondly, we characterize all possible values of k and n for which the ring of $k \times k$ matrices over $\mathbb{Z}_n$ is $*$-regular, i.e. every matrix has its Moore-Penrose inverse, with respect to the involution $*$ defined by the matrix transposition. We prove that the ring of $k \times k$ matrices over $\mathbb{Z}_n$ is $*$-regular if and only if n is square-free and either $k = 1$ (with no additional conditions) or $k = 2$, and all divisors of n can be written as the form $4m + 3$ for some nonnegative integer m. The result exploits the sum of squares lemma from elementary number theory (Koshy, 2007).

2. Preliminaries

Let R be an associative ring with the identity $1 \neq 0$. An element $a \in R$ is regular (in the sense of von Neumann) if there exists an $x \in R$ such that $axa = a$. A ring R is called regular if every element in R is regular. An involution $*$ in R is an anti-isomorphism of degree 2 in R i.e., $(x^*)^* = x$, $(x + y)^* = x^* + y^*$ and $(xy)^* = y^*x^*$ for all $x, y \in R$. A ring with involution $*$ is called a $*$-ring. An element $a \in R$ is $*$- cancellable if $a^*ax = 0$ implies $ax = 0$ and $yaa^* = 0$ implies ya = 0 for any $x, y \in R$. A $*$-ring is $*$-cancellable if every element in R is $*$-cancellable. If a ring R is regular and $*$-cancellable then it is called a $*$-regular ring. A $*$-ring is said to satisfy the k-term $*$-cancellation law (SC_k) if $a_1^*a_1 + a_2^*a_2 + \cdots + a_k^*a_k = 0$ implies $a_1 = a_2 = \cdots = a_k = 0$ for any $a_1, a_2, a_3, \ldots, a_k \in R$. An element $a \in R$ is Moore-Penrose invertible if there is an element $x \in R$ satisfying

$$axa = a \tag{1}$$

$$xax = x \tag{2}$$

$$(ax)^* = ax \tag{3}$$

$$(xa)^* = xa \tag{4}$$

These equations are called the Moore-Penrose equations. If x exists, then it is unique (Penrose, 1955) and it is called the Moore-Penrose inverse of a, denoted by a †.

We recall standard definitions and notations from number theory and matrix theory. For any positive integer $n \geq 2$, let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ denote the ring of integers modulo n with the usual addition and multiplication. Let $M_k(\mathbb{Z}_n)$ represent the set of all $k \times k$ matrices over $\mathbb{Z}_n$. The actual involution defined on the ring of matrices over any ring R should be defined by $M^* = [a^*_{ij}]$ t if $M = [a_{ij}]$. However, we use the matrix transpose as an involution in the ring $M_k(\mathbb{Z}_n)$ because of the following result.

Theorem 2.1 The only involution on $\mathbb{Z}_n$ is the identity function.

Proof. Let $*$: $\mathbb{Z}_n \rightarrow \mathbb{Z}_n$ be an involution and $a = 1^*$. For any $x \in \mathbb{Z}_n \backslash \{0\}$, we have $x^* = (\underbrace{1 + 1 + \cdots + 1}_{x \text{ terms}})^* = \underbrace{1^* + 1^* + \cdots + 1^*}_{x \text{ terms}} = ax$. Since $0^* = 0$, $x^* = ax$ for all $x \in \mathbb{Z}_n$. This implies $a^2 = a^* = (1^*)^* = 1$ and hence $a = 1^* = 1^* \cdot 1^* = a^2 = 1$. Thus $x^* = x$ for all $x \in \mathbb{Z}_n$.

3. Moore-Penrose Inverses of Matrices over $\mathbb{Z}_n$

In this section, we give necessary and sufficient conditions for the existence of Moore-Penrose inverses and provide the algorithm to find the Moore-Penrose inverse in $M_k(\mathbb{Z}_n)$. For $k = 1$ and $k = 2$, we illustrate an explicit formula for the Moore-Penrose inverse of M for any $n \geq 2$. We note that the Moore-Penrose inverses of 1×1 matrices over $\mathbb{Z}_n$ are studied extensively in the field of number theory (Apostol & Tóth, 2015; Ehrlich, 1968). We recall some definition and theorems for completeness. An integer a is called regular modulo n if there is an integer x satisfying $a^2x \equiv a \pmod{n}$. The following result comes from (Apostol & Tóth, 2015) with a slight modification for our use.

Theorem 3.1 Let a be any integer. Then the following statements are equivalent:

(i) a is regular modulo n,

(ii) $\gcd(a, n) = \gcd(a^2, n)$,

(iii) $\gcd(a, n) = \gcd(a^k, n)$ for all $k \geq 2$.

Proof. Let a be any integer.

(i) $\Rightarrow$ (ii) Suppose a is regular modulo n. Then there is an $x \in \mathbb{Z}_n$ such that $a^2 x \equiv a(\text{mod } n)$. That is, $a^2x = a + ny$ for some $y \in \mathbb{Z}$. Assume that $\gcd(a, n) = d$ and $\gcd(a^2, n) = e$. Since $\gcd(a, n) = d$, $d|a$ and $d|n$. Thus $d|a^2$ so $d|e$. Since $\gcd(a^2, n) = e$, $e|a^2$ and $e|n$. Thus $e|(a^2x - ny)$, i.e., $e|a$. Hence $e|d$. Since d and e are non-negative integers, $d = e$. Therefore, $\gcd(a, n) = \gcd(a^2, n)$.

(ii) $\Rightarrow$ (iii) Suppose that $\gcd(a, n) = \gcd(a^2, n) = d$. Then $\gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1 = \gcd\left(\frac{a^2}{d}, \frac{n}{d}\right)$. Since $\gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, we have $\gcd\left(\frac{a}{d} \cdot a, \frac{n}{d}\right) = \gcd\left(a, \frac{n}{d}\right)$. Hence $\gcd\left(a, \frac{n}{d}\right) = 1$. We will proceed by induction on k. For $k = 2$, this is obvious by the assumption. Let $k \geq 2$ and suppose that $\gcd(a, n) = \gcd(a^k, n) = d$. Then $\gcd\left(\frac{a}{d}, \frac{n}{d}\right) = \gcd\left(\frac{a^k}{d}, \frac{n}{d}\right) = 1$. Since $\gcd\left(a, \frac{n}{d}\right) = 1$ and $\gcd\left(\frac{a^k}{d}, \frac{n}{d}\right) = 1$, $\gcd\left(\frac{a^k}{d} \cdot a, \frac{n}{d}\right) = \gcd\left(a, \frac{n}{d}\right) = 1$. Thus $\gcd(a^{k+1}, n) = d = \gcd(a, n)$. This proves that $\gcd(a^k, n) = \gcd(a, n)$ for all $k \geq 2$.

(iii) $\Rightarrow$ (i) Suppose that $\gcd(a, n) = \gcd(a^k, n)$ for all $k \geq 2$. Then $\gcd(a, n) = \gcd(a^3, n)$. Thus $\gcd(a, n) = a^3x + ny$ for some $x, y \in \mathbb{Z}$. Choose $b = \frac{a^2x}{\gcd(a,n)}$, then $a^2b = \frac{a^4x}{\gcd(a,n)} = a^3x \cdot \frac{a}{\gcd(a,n)} = (\gcd(a, n) - ny) \cdot \frac{a}{\gcd(a,n)} \equiv a \pmod{n}$. Thus a is regular modulo n. ■

In our context, a is regular in $\mathbb{Z}_n$ if and only if a is a regular number modulo n where $a \in \{0, 1, \ldots, n-1\}$. In this case, the Moore-Penrose equations can be reduced to equations (1) and (2).

Theorem 3.2 Let a be any integer. Then a † exists in $\mathbb{Z}_n$ if and only if a is regular modulo n. If a † exists, then $a^\dagger = \frac{a^2x}{\gcd(a,n)}$ (mod n), where x is an integer satisfying the equation $\gcd(a, n) = a^3x + ny$ for some integer y.

Proof. Let a be any integer.

($\Rightarrow$) Suppose that a † exists in $\mathbb{Z}_n$. Then there is an element $b \in \mathbb{Z}_n$ such that (1) holds. Thus a is regular modulo n.

($\Leftarrow$) Suppose that a is regular modulo n. Then there is an integer x such that $a^2x \equiv a \pmod{n}$. From the proof of Theorem 3.1, choose an integer $b \in \mathbb{Z}_n$ such that $b \equiv \frac{a^2x}{\gcd(a,n)} \pmod{n}$ where x satisfies $\gcd(a, n) = a^3x + ny$ for some $y \in \mathbb{Z}$. Then $a^2b \equiv a \pmod{n}$ as seen in Theorem 3.1. We also have that $b^2a \equiv \frac{a^2x}{\gcd(a,n)} \cdot a^3x \equiv \frac{a^2x}{[\gcd(a,n)]^2} \cdot (\gcd(a,n) - ny) \equiv \frac{a^2x}{\gcd(a,n)} \equiv b \pmod{n}$. By the uniqueness of a† , we conclude that a† $= b$.■

Next, suppose that $k \geq 2$. We will start with some auxiliary results.

Lemma 3.3 Let $M \in M_k(\mathbb{Z}_p n)$, where $n \geq 2$. If $\det(M)$ is a zero divisor of $\mathbb{Z}_p n$, then M† does not exist.

Proof. Suppose M† exists and $\det(M)$ is a zero divisor of $\mathbb{Z}_p n$. Then $\det(M) = pq$ in $\mathbb{Z}_p n$ for some $q \in \{1,2, \ldots, p^{n-1} - 1\}$. From (2), we have, $\det(M†) = pq(\det(M†))^2 = pq_1$ where $q_1 \equiv q(\det(M†))^2 \pmod{p^n}$. By induction on m, we have $\det(M^\dagger) = p^{2^m-1}q_m$ for some $q_m \in \mathbb{Z}$ and for all $m \in \mathbb{N}$. This implies $\det(M^\dagger) = 0$ in $\mathbb{Z}_{p^n}$. From (2.1), we have $\det(M) = 0$ in $\mathbb{Z}_p n$, a contradiction. ■

Lemma 3.4 For any $n \geq 2$, suppose that $M = pN$ for some nonzero $N \in M_k(\mathbb{Z}_p n)$. Then M† does not exist.

Proof. Suppose M† exists. From (3), $M^\dagger = p\left(M^\dagger M M^\dagger\right) = pN_1$ where $N_1 \in M_k(\mathbb{Z}_{p^n})$. By induction, we have $M^\dagger = p^{2^m-1}N_m$ where $N_m \in M_k(\mathbb{Z}_{p^n})$ for all $m \in \mathbb{N}$. Hence $M^\dagger = 0$ in $M_k(\mathbb{Z}_{p^n})$. This implies $M = (M^\dagger)^\dagger = 0$ in $\mathbb{Z}_{p^n}$, a contradiction. Therefore, M† does not exist. ■

Lemma 3.5 Let $M \in M_k(\mathbb{Z}_{p^n})$. Suppose $M^\dagger$ exists and $\det(M) = 0$ in $\mathbb{Z}_{p^n}$. Then $\det(M^\dagger) = 0$ in $\mathbb{Z}_{p^n}$.

Proof. Let $M \in M_k\left(\mathbb{Z}_{p^n}\right)$. Suppose $M^\dagger$ exists and $\det(M) = 0$ in $\mathbb{Z}_{p^n}$. From (2), we have $\det(M^\dagger) = \det(M^\dagger M M^\dagger) = \det(M^\dagger)\det(M)\det(M^\dagger) = 0$ in $\mathbb{Z}_{p^n}$.■

Theorem 3.6 Suppose $M = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in M_2(\mathbb{Z}_p)$ is nonzero. Then $M^\dagger$ exists if and only if either $\det(M) \not\equiv 0 \pmod{p}$ or $\det(M) \equiv 0 \pmod{p}$ and $a^2 + b^2 + c^2 + d^2$ is a unit in $\mathbb{Z}_p$. If $M^\dagger$ exists, then $M^\dagger = \begin{cases} (a^2 + b^2 + c^2 + d^2)^{-1}M^T & \text{if } \det(M) \equiv 0 \pmod{p} \\ (ad - bc)^{-1}\operatorname{adj}(M) & \text{if } \det(M) \not\equiv 0 \pmod{p} \end{cases}$

Proof. Let $M = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in M_2(\mathbb{Z}_p)$ be a nonzero matrix in $\mathbb{Z}_p$. If $\det(M) \not\equiv 0 \pmod{p}$, then M^{-1} exists. Thus $M^\dagger = M^{-1} = (ad - bc)^{-1}\operatorname{adj}(M)$. Suppose $\det(M) \equiv 0 \pmod{p}$. By Theorem 13 appearing in (Bapat *et al.*, 1990) $M^\dagger$ exists if and only if $a^2 + b^2 + c^2 + d^2$ is a unit in $\mathbb{Z}_p$. In case $M^\dagger$ exists, let $u = a^2 + b^2 + c^2 + d^2$ and $N = u^{-1}M^T$. Then M and N satisfy the Moore-Penrose equations by a direct computation. Therefore, $M^\dagger = u^{-1}M^T = (a^2 + b^2 + c^2 + d^2)^{-1}M^T$.

Lemma 3.7 Let a a be any integer. For any positive integer n, $\gcd(a, p) = 1$ if and only if $\gcd(a, p^n) = 1$.

Proof. Let a be an integer.

($\Rightarrow$) Suppose $\gcd(a, p) = 1$. We will prove that $\gcd(a, p^n) = 1$ by induction on n. For $n = 1$, it is obvious. Next, suppose that $\gcd(a, p^n) = 1$ for any $n \in \mathbb{N}$. Then there are integers w, x, y, z such that $ax + py = 1$ and $aw + p^nz = 1$. Thus $1 = (ax + py)(aw + p^nz) = (a^2wx + ap^nxz + apwy + p^{n+1}yz)$. This implies that $\gcd(a, p^{n+1}) = 1$. Therefore, $\gcd(a, p^n) = 1$ for all positive integers n.

($\Leftarrow$) Suppose $\gcd(a, p^n) = 1$. Then there are integers x and y such that $ax + p^ny = 1$. Thus $ax + p(p^{n-1})y = 1$. Therefore, $\gcd(a, p) = 1$.■

Theorem 3.8 Suppose $M = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in M_2(\mathbb{Z}_{p^n})$ is nonzero and $\det(M) = 0$ in $\mathbb{Z}_{p^n}$. Then $M^\dagger$ exists if and only $a^2 + b^2 + c^2 + d^2$ is a unit in $\mathbb{Z}_{p^n}$.

Proof. ($\Rightarrow$) Suppose $M^\dagger$ exists in $\mathbb{Z}_{p^n}$. Then $M^\dagger$ also exists in $\mathbb{Z}_p$. By Theorem 3.6, $a^2 + b^2 + c^2 + d^2$ is a unit in $\mathbb{Z}_p$ and is also a unit in $\mathbb{Z}_{p^n}$ by Lemma 3.7.

($\Leftarrow$) Suppose $a^2 + b^2 + c^2 + d^2$ is a unit in $\mathbb{Z}_{p^n}$ and let $u = a^2 + b^2 + c^2 + d^2$. Then $M^\dagger = u^{-1}M^T$ by direct computation.

Theorem 3.9. Let $M = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in M_2\left(\mathbb{Z}_{p^n}\right)$. Then $M^\dagger$ exists in $M_2\left(\mathbb{Z}_{p^n}\right)$ if and only if either one of the following holds:

(i) $M = 0$ in $M_2\left(\mathbb{Z}_{p^n}\right)$, or

(ii) $\det(M)$ is a unit in $\mathbb{Z}_{p^n}$, or

(iii) $\det(M) = 0$ in $\mathbb{Z}_{p^n}$ and $a^2 + b^2 + c^2 + d^2$ is a unit in $\mathbb{Z}_{p^n}$.

$$\text{Moreover, } M^\dagger = \begin{cases} 0 & \text{if } M = 0, \\ (ad-bc)^{-1}\text{adj}(M) & \text{if } \det(M) \text{ is a unit in } \mathbb{Z}_{p^n} \\ (a^2+b^2+c^2+d^2)^{-1}M^T & \text{if } a^2+b^2+c^2+d^2 \text{ is a unit in } \mathbb{Z}_{p^n}. \end{cases}$$

Proof. Let $M = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in M_2(\mathbb{Z}_{p^n})$.

($\Rightarrow$) Suppose $M^\dagger$ exists in $M_2(\mathbb{Z}_{p^n})$. We consider 2 cases.

Case 1: $M = 0$ in $M_2(\mathbb{Z}_{p^n})$. Then $M^\dagger = 0$ in $M_2(\mathbb{Z}_{p^n})$.

Case 2: $M \neq 0$ in $M_2(\mathbb{Z}_{p^n})$. Since $\det(M)$ can be either a unit, a zero divisor, or a zero element, we consider 3 subcases.

Case 2.1: $\det(M)$ is a unit in $\mathbb{Z}_{p^n}$. Then $M^\dagger = (ad-bc)^{-1}\text{adj}(M)$.

Case 2.2: $\det(M)$ is a zero divisor in $\mathbb{Z}_{p^n}$. Then $M^\dagger$ does not exist by Theorem 3.3.

Case 2.3: $\det(M) = 0$ in $\mathbb{Z}_{p^n}$. Then $a^2+b^2+c^2+d^2$ is a unit in $\mathbb{Z}_{p^n}$ by Theorem 3.8. and $M^\dagger = (a^2+b^2+c^2+d^2)^{-1}M^T$.

($\Leftarrow$) The converse is clear.

Theorem 3.9 cannot be extended further to 3×3 matrices over $\mathbb{Z}_{p^n}$ for $n \geq 2$, using the concept of rank and sum of squares of minors explained in (Bapat *et al.*, 1990). The following matrix over $\mathbb{Z}_9$ gives a counterexample.

Example 3.10 Let $A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 3 & 0 \\ 1 & 1 & 3 \end{bmatrix} \in M_3(\mathbb{Z}_9)$. Since the largest size of nonvanishing minor of A is 2, $\text{rank}(A) = 2$. A part of Theorem 13 in Bapat *et al.* (1990) states that "a matrix A of rank r has a Moore-Penrose inverse if and only if the sum of squares of all $r \times r$ minors of A is invertible over an integral domain R". We follow this theorem by computing the sum of squares of all 2×2 minors of A which gives $\sum_{ij} M_{ij}^2(A) \equiv 5$ (mod 9), where $M_{ij}(A)$ denotes the minor of A obtained by deleting the i^{th} row and the j^{th} column of A. We know that 5 is a unit in $\mathbb{Z}_9$. However, A is not Moore-Penrose invertible.

Example 3.10 shows that the Moore-Penrose inverse of a matrix over $\mathbb{Z}_n$ does not only rely on the sum of squares of its minors. More investigation is needed for matrices of size larger than 2. However, the following result holds true for square matrices of any size.

Let $n = p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m}$, where $p_1, p_2, \ldots, p_m$ are distinct primes and $a_1, a_2, \ldots, a_m$ are positive integers.

Theorem 3.11 Let $M \in M_k(\mathbb{Z}_n)$. Then $M^\dagger$ exists in $M_k(\mathbb{Z}_n)$ if and only if $M^\dagger$exists in $M_k(\mathbb{Z}_{{p_i}^{a_i}})$ for all $i = 1,2,\ldots,m$.

Proof. Let $M \in M_k(\mathbb{Z}_n)$.

($\Rightarrow$) Suppose $M^\dagger$exists in $M_k(\mathbb{Z}_n)$. The Moore-Penrose equations (1) - (4) in modulo n can be reduced to equations in modulo $p_i^{a_i}$ for every $i = 1,2,\ldots,m$. Hence $M^\dagger$exists in $M_k(\mathbb{Z}_{{p_i}^{a_i}})$ for every $i = 1,2,\ldots,m$.

($\Leftarrow$) Let $M = [a_{ij}] \in M_k(\mathbb{Z}_n)$. Suppose $M^\dagger$ exists in $M_k(\mathbb{Z}_{{p_i}^{a_i}})$, say ${M_i}^\dagger$, for every $i = 1,2,\ldots,m$. Let $M_i^\dagger = [x_{\alpha\beta}(i)] \in M_k(\mathbb{Z}_{p_i^{a_i}})$ for each $i = 1,2,\ldots,m$. By the Chinese Remainder Theorem, there are $y_{\alpha\beta}(i) \in \mathbb{Z}_n$ congruent to $x_{\alpha\beta}(i)$ modulo $p_i^{a_i}$ for every $i = 1,2,\ldots,m$. Let $N = [y_{\alpha\beta}(i)]$. Then M and N satisfy the Moore-Penrose equations (1)-(4) in $M_k(\mathbb{Z}_n)$. Therefore $M^\dagger = N$.

Algorithm

Notation: $M_{p_i^{a_i}}$ stands for a matrix M in $M_k(\mathbb{Z}_n)$ all of whose entries are considered in $\mathbb{Z}_{{p_i}^{a_i}}$.

Input:

Step 1. Write $n = p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m}$, where all p_i are distinct primes and all a_i are positive integers.

Step 2. $M \in M_k(\mathbb{Z}_n)$.

Output: $M^\dagger \in M_k(\mathbb{Z}_n)$ if it exists.

Step 1. Construct $M \equiv M_{p_i^{a_i}}$ for every $i = 1,2,\ldots,m$.

Step 2. Compute $M^\dagger_{p_i^{a_i}} \in M_k(\mathbb{Z}_{{p_i}^{a_i}})$.

- If $M^\dagger_{p_i^{a_i}}$ does not exist for some i then $M^\dagger$ does not exist in $M_k(\mathbb{Z}_n)$.
- If $M^\dagger_{p_i^{a_i}}$ exists for every $i = 1,2,\ldots,m$ then $M^\dagger_{p_i^{a_i}} = [x_{\alpha\beta}(i)]$ for each $M_{p_i^{a_i}}$.

Step 3. Compute $M^\dagger = [y_{\alpha\beta}]$, where $y_{\alpha\beta} \equiv x_{\alpha\beta}(i)$ (mod $p_i^{a_i}$) for all $i = 1,2,\ldots,m$ by using the Chinese Remainder Theorem.

Example 3.12 Let $M = \begin{bmatrix} 16 & 6 \\ 14 & 19 \end{bmatrix} \in M_2(\mathbb{Z}_{20})$.

Step 1. Write $n = 2^2 \cdot 5$. Compute $M_4 = \begin{bmatrix} 0 & 2 \\ 2 & 3 \end{bmatrix}$ and $M_5 = \begin{bmatrix} 1 & 1 \\ 4 & 4 \end{bmatrix}$

Step 2. We have $M_4^\dagger = \begin{bmatrix} 0 & 2 \\ 2 & 3 \end{bmatrix}$ and $M_5^\dagger = \begin{bmatrix} 4 & 1 \\ 4 & 1 \end{bmatrix}$.

Step 3. Compute $M^\dagger = \begin{bmatrix} x & z \\ y & w \end{bmatrix}$, where

$$\begin{aligned} x &\equiv 0 (\text{mod } 4) \quad & z &\equiv 2 (\text{mod } 4) \\ x &\equiv 4 (\text{mod } 5) \quad & z &\equiv 1 (\text{mod } 5) \end{aligned}$$

$$\begin{aligned} y &\equiv 2 (\text{mod } 4) \quad & w &\equiv 3 (\text{mod } 4) \\ y &\equiv 4 (\text{mod } 5) \quad & w &\equiv 1 (\text{mod } 5) \end{aligned}$$

By the Chinese Remainder Theorem, we have $x = 4, y = 14, z = 6, w = 11$ in $\mathbb{Z}_{20}$. Thus $M^\dagger = \begin{bmatrix} 4 & 6 \\ 14 & 11 \end{bmatrix}$ in $M_2(\mathbb{Z}_{20})$.

4. $*$-Regularity of Matrices over the Ring of Integers Modulo n .

In this section, we characterize all values of k and n for which the ring of all $k \times k$ matrices over $\mathbb{Z}_n$ is $*$-regular. Firstly, we focus on $k = 1$. We note that $M_1(\mathbb{Z}_n)$ is $*$-regular if and only if $\mathbb{Z}_n$ is regular. It is well-known that $\mathbb{Z}_n$ is regular if and only if n is square-free (Apostol & Tóth, 2015; Ehrlich, 1968). Thus, we have the following result.

Theorem 4.1. $M_1(\mathbb{Z}_n)$ is $*$ -regular if and only if n is square-free. Moreover, if $M = [a] \in M_1(\mathbb{Z}_n)$ then $M^\dagger = [a^\dagger]$ where $a^\dagger \equiv \frac{a^2 x}{\gcd(a,n)}$ (mod n) and x is chosen from the equation $\gcd(a, n) = a^3 x + ny$ for some $y \in \mathbb{Z}$.

Proof. This is a consequence of Theorem 3.2. ∎

Next, suppose that $k \geq 2$. The following theorems (Theorem 4.2 - 4.5) are cited from Hartwig and Patrício (2012), Kaplansky (1972), Koliha and Patrício (2002) and Lemma 4.6 is cited from Koshy (2007).

Theorem 4.2 R satisfies SC_1 if and only if R is $*$ -cancellable.

Theorem 4.3 $M_k(R)$ satisfies SC_1 if and only if R satisfies SC_k.

Theorem 4.4 $M_k(R)$ is regular if and only if R is regular.

Theorem 4.5 $M_k(R)$ is $*$ -regular if and only if R is regular and satisfies SC_k.

Lemma 4.6 If p is an odd prime, then there are integers x and y such that $1 + x^2 + y^2 \equiv 0$ (mod p), where $0 \leq x, y < \frac{p}{2}$.

Next, we focus on the ring $M_k(\mathbb{Z}_n)$.

Theorem 4.7 For any $n \geq 2$, $\mathbb{Z}_n$ does not satisfy SC_k for all $k \geq 3$.

Proof. Suppose $n \geq 2$ and $k \geq 3$. Then $p|n$ for some prime p, so $n = pl$ for some $l \in \mathbb{N}$. Note that $0 < l < n$. If $p = 2$, then $\underbrace{0^2 + 0^2 + \cdots + 0^2}_{k-2 \text{ terms}} + 1^2 + 1^2 = 2$, and hence $\underbrace{0^2 + 0^2 + \cdots + 0^2}_{k-2 \text{ terms}} + l^2 + l^2 = 2l^2 = ln$. Thus, $\mathbb{Z}_2$ does not satisfy SC_k for all $k \geq 3$. Suppose $p \geq 3$. By Lemma 4.6, there are integers x and y such that $0 \leq x, y < \frac{p}{2}$ and $\underbrace{0^2 + 0^2 + \cdots + 0^2}_{k-3 \text{ terms}} + 1^2 + x^2 + y^2 = pm$ for some m, so $\underbrace{0^2 + 0^2 + \cdots + 0^2}_{k-3 \text{ terms}} + l^2 + (lx)^2 + (ly)^2 = lmn \equiv 0$ (mod n). Thus, $\mathbb{Z}_n$ does not satisfy SC_k for all $k \geq 3$. ∎

Lemma 4.8 Let p be a prime number. Then $\mathbb{Z}_p$ satisfies SC_2 if and only if $p \equiv 3$ (mod 4).

Proof. (⇒) Suppose $\mathbb{Z}_p$ satisfies SC_2. If $p = 2$, then $1^2 + 1^2 = 0$ in $\mathbb{Z}_2$. This implies $1 = 0$ in $\mathbb{Z}_2$, a contradiction. Thus, p must be an odd prime. Suppose $p \equiv 1$ (mod 4). Then -1 is a quadratic residue modulo p. Thus, there is some $x \in \mathbb{N}$ such that $x^2 \equiv -1$ (mod p). Note that $x \not\equiv 0$ (mod p). Therefore, we have $x^2 + 1^2 \equiv 0$ (mod p). This implies $\mathbb{Z}_p$ does not satisfy SC_2. Hence $p \equiv 3$ (mod 4).

(⇐) Let p be a prime such that $p \equiv 3$ (mod 4). Suppose $aa^* + bb^* = 0$ in $\mathbb{Z}_p$. Then $a^2 + b^2 \equiv 0$ (mod p). Assume that $a \not\equiv 0$ (mod p). Then there is an $x \in \mathbb{Z}$ such that $ax \equiv 1$ (mod p). Thus $(bx)^2 = b^2x^2 \equiv -(ax)^2 \equiv -1$ (mod p). But -1 is a quadratic nonresidue modulo p , a contradiction. Thus, $a \equiv 0$ (mod p) and hence $b \equiv 0$ (mod p) . This shows that $\mathbb{Z}_p$ satisfies SC_2. ∎

Theorem 4.9 $\mathbb{Z}_n$ satisfies SC_2 if and only if $n = p_1p_2 \cdots p_k$ where p_i are distinct primes of the form $4m+3$ for some integer m.

Proof. (⇒) Suppose $\mathbb{Z}_n$ satisfies SC_2. Let $n = a^2b$ where $a, b \in \mathbb{N}$ and b is square-free. Suppose $a > 1$ .Then $(ab)^2 + 0^2 = (a^2b)b = nb \equiv 0 \pmod{n}$. This implies $\mathbb{Z}_n$ does not satisfy SC_2. Thus, $a = 1$ and n is square-free. Let $n = p_1p_2 \cdots p_k$ where p_i are distinct primes. Suppose $p_i \equiv 2$ or $p_i \equiv 1 \pmod 4$ for some i. Then $p_i = x^2 + y^2$ for some x, y such that $1 \le x, y < p_i$. Thus $\left(\frac{nx}{p_i}\right)^2 + \left(\frac{ny}{p_i}\right)^2 = \frac{n^2}{p_i^2}(x^2+y^2) = \frac{n^2}{p_i} \equiv 0 \pmod{n}$. Note that $1 \le \frac{nx}{p_i}, \frac{ny}{p_i} < n$. This implies $\mathbb{Z}_n$ does not satisfy SC_2. Therefore, $n = p_1p_2 \cdots p_k$ where p_i are distinct primes of the form $4m+3$.

(⇐) Suppose $n = p_1p_2 \cdots p_k$ where p_i are distinct primes of the form $4m+3$. Let a, b be such that $a^2 + b^2 = 0$ in $\mathbb{Z}_n$. Then $a^2 + b^2 = 0$ in $\mathbb{Z}_{p_i}$ for all i. This implies $a = b = 0$ in $\mathbb{Z}_{p_i}$ for all i. It follows that $p_i | a$ and $p_i | b$ for all i. Thus, $[p_1, p_2, \ldots, p_k] | a$ and $[p_1, p_2, \ldots, p_k] | b$ for all i. But $[p_1, p_2, \ldots, p_k] = p_1p_2 \cdots p_k = n$. Hence $a = b = 0$ in $\mathbb{Z}_n$. Therefore, $\mathbb{Z}_n$ satisfies SC_2.■

Theorem 4.10 $M_2(\mathbb{Z}_n)$ is $*$-regular if and only if $n = p_1p_2 \cdots p_k$ where p_i are distinct primes of the form $4m+3$ for all $i = 1,2,\ldots,k$.

Proof. $M_2(\mathbb{Z}_n)$is $*$-regular if and only if $\mathbb{Z}_n$ is regular and satisfies SC_2 if and only if $n = p_1p_2 \cdots p_k$ where p_i are distinct primes of the form $4m+3$ for all $i = 1,2,\ldots,k$.■

Finally, we get a characterization for $*$-regularity in $M_k(\mathbb{Z}_n)$.

Theorem 4.11 $M_k(\mathbb{Z}_n)$ is $*$ -regular if and only if n is square-free and either one of the following statements holds:

(i) $k = 1$, or

(ii) $k = 2$ and each prime divisor of n can be written as the form $4m+3$ for some nonnegative integer m.

5. Conclusions

In this paper, we have characterized all possible values of k and n for which the ring of $k \times k$ matrices over $\mathbb{Z}_n$ is $*$-regular. It turns out that a ring of $k \times k$ matrices over $\mathbb{Z}_n$ is $*$-regular if and only if n is square-free and either $k = 1$ (with no additional conditions) or $k = 2$, and all divisors of n can be written as the form $4m + 3$ for some nonnegative integer m. In the case of 2 × 2 matrices, the Moore-Penrose inverse formula is presented in Theorem 3.9 and 3.10. However, more investigation is needed for the case $k \geq 3$.

Acknowledgements

The first author is grateful to the Science Achievement Scholarship of Thailand (SAST) for financial support. The authors would like to thank the referees for their valuable comments and suggestions.

References

Apostol, B. & Tóth, L. (2015). Some remarks on regular integers modulo n. *Filomat, 29*(4),687-701.

Bapat, R. B., Bhaskara Rao, K. P. S., & Manjunatha Prasad, K. (1990). Generalized inverses over integral domains. *Linear Algebra and its Applications, 140*, 181-196.

Ben-Israel, A. & Greville, T. N. E. (2003). *Generalized inverses: Theory and applications bibliography for the 2nd edition*. Berlin, Germany: Springer.

Ehrlich, G. (1968). Unit-regular rings. *Portugaliae Mathematica, 27,* 209-212.

Harte, R. E. & Mbekhta, M. (1992). On generalized inverses in C*-algebra. *Studia Mathematica, 103*, 71-77.

Hartwig, R. E. & Patrício, P. (2012). When does the Moore-Penrose inverse flip? *Operators and Matrices, 6*,181-192.

Kaplansky, I. (1972). *Fields and rings*. Chicago, IL: University of Chicago Press.

Koliha, J. J., Djordjevíc, D., & Cvetkovíc, D. (2007). Moore-Penrose inverse in rings with involution. *Linear Algebra and its Applications, 426*, 371-381.

Koliha, J. J. & Patrício, P. (2002). Elements of rings with equal spectral idempotents. *Journal of the Australian Mathematical Society 72*, 137-152.

Koshy, T. (2007). *Elementary number theory with applications (2nd ed.)*. Amsterdam, The Netherlands: Elsevier.

Moore, E. H. (1920). On the reciprocal of the general algebraic matrix. *Bulletin of the American Mathematical Society, 26*, 394-395.

Penrose, R. (1955). A generalized inverse for matrices. *Mathematical Proceedings of the Cambridge Philosophical Society, 51(3),* 406-413.

Tóth, L. (2008) Regular integers modulo n. *Annales Universitatis Scientiarum Budapestinensis de Rolando Eotvos Nominatae Sectio Computatorica, 29*, 264–275.

Zhu, H., Chen, J., Zhang, X., & Patrício, P. (2014). The Moore-Penrose inverse of 2×2 matrices over a certain $*$-regular ring. *Applied Mathematics and Computation*, *246*, 263-267.