DETERMINANTS OF ARROWHEAD MATRICES OVER RINGS OF INTEGERS MODULO THE SQUARE OF A PRIME

By
MISS Pornrudee MODJAM

A Thesis Submitted in Partial Fulfillment of the Requirements
for Master of Science (MATHEMATICS)
Department of MATHEMATICS
Graduate School, Silpakorn University
Academic Year 2021

ดีเทอร์มิแนนต์ของเมทริกซ์หัวลูกศรบนริงของจำนวนเต็มมอดุโลจำนวนเฉพาะยกกำลังสอง

โดย
นางสาวพรฤดี โหมดแจ่ม

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์ แผน ก แบบ ก 2 ระดับปริญญามหาบัณฑิต
ภาควิชาคณิตศาสตร์
บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร
ปีการศึกษา 2564

DETERMINANTS OF ARROWHEAD MATRICES OVER RINGS OF INTEGERS MODULO THE SQUARE OF A PRIME

By
MISS Pornrudee MODJAM

A Thesis Submitted in Partial Fulfillment of the Requirements
for Master of Science (MATHEMATICS)
Department of MATHEMATICS
Graduate School, Silpakorn University
Academic Year 2021

Title	Determinants of Arrowhead Matrices over Rings of Integers Modulo the Square of a Prime
By	MISS Pornrudee MODJAM
Field of Study	(MATHEMATICS)
Advisor	Associate Professor SOMPHONG JITMAN, Ph.D.

Graduate School Silpakorn University in Partial Fulfillment of the Requirements for the Master of Science

....Dean of graduate school
(Associate Professor Jurairat Nunthanid, Ph.D.)

Approved by

....Chair person
(Assistant Professor Wannarut Rungrottheera, Ph.D.)

....Advisor
(Associate Professor Somphong Jitman, Ph.D.)

....External Examiner
(Associate Professor Sajee Pianskool, Ph.D.)

620720002 : MAJOR: MATHEMATICS

KEY WORDS : MATRICES, ARROWHEAD MATRICES, DETERMINANTS, INTEGER MODULO p^2

PORNRUDEE MODJAM : DETERMINANTS OF ARROWHEAD MATRICES OVER RINGS OF INTEGER MODULO THE SQUARE OF A PRIME. THESIS ADVISOR : ASSOC. PROF. SOMPHONG JITMAN, Ph.D.

Arrowhead matrices are a special type of matrices that have been of interest and extensively studied due to their nice algebraic structures and wide applications. In this thesis, the enumeration of arrowhead matrices with prescribed determinant over the rings $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$ are studied, where p is a prime number. The number of $n \times n$ arrowhead matrices over $\mathbb{Z}_p$ of a fixed determinant a is determined for all positive integers n and for all elements $a \in \mathbb{Z}_p$. This result is applied in the enumeration of $n \times n$ singular and non-singular arrowhead matrices over $\mathbb{Z}_{p^2}$. Moreover, the number of $n \times n$ non-singular arrowhead matrices over $\mathbb{Z}_{p^2}$ of a fixed determinant b is established for all positive integers n and for all units $b \in \mathbb{Z}_{p^2}$. For singular arrowhead matrices over $\mathbb{Z}_{p^2}$, an upper bound for the number of $n \times n$ arrowhead matrices over $\mathbb{Z}_{p^2}$ with zero determinant and a lower bound for the number of $n \times n$ arrowhead matrices over $\mathbb{Z}_{p^2}$ with a non-zero determinant are presented. Some illustrative enumerations are presented as well.

Acknowledgements

This thesis was accomplished with the help of my thesis advisor, Associate Professor Dr.Somphong Jitman. He dedicates his time to give advice and check the various mistakes in my study and research with attention as well. I appreciate every help from him.

I would like to thank my thesis committees, Assistant Professor Dr.Wannarut Rungrottheera and Associate Professor Dr.Sajee Pianskool, for their comments and suggestions.

I am very grateful to the Development and Promotion of Science and Technology Talents Project (DPST) for the financial support through out my study time.

Finally, I would like to thank family and friends for the support and encouragement over the period of this research.

Pornrudee MODJAM

CONTENTS

Chapter 1

Introduction

Determinants of matrices have been known for their nice properties and wide applications. Classically, determinants appear in the Heron's formula for the area of a triangle in [6] and in the calculation of the cross-product of vectors in $\mathbb{R}^3$ in [2]. Moreover, in [2], various applications of determinants are presented such as the determination of the singularity of matrices, the existence of the solution of linear systems, and the solution of linear systems using Cramer's rule. Therefore, properties of matrices and their determinants have been extensively studied. Especially, matrices over fields and their determinants are interesting due to their rich algebraic structures and wide applications. Singularity of matrices is useful in applications (see, for example, [2] and [10]).

The number of $n \times n$ singular (resp., nonsingular) matrices over a finite field $\mathbb{F}_q$ has been determined in [13]. As a generalization of the prime field $\mathbb{Z}_p$, the number of $n \times n$ matrices over $\mathbb{Z}_m$ of a fixed determinant has been first studied in [1]. In [8], a different and simpler technique was applied to determine the number of such matrices over $\mathbb{Z}_m$. Later, the number of $n \times n$ matrices over commutative finite chain rings of a fixed determinant has been completely determined in [3]. Diagonal matrices are interesting subfamilies of the ones in [3]. As a special case of [3], the determinants of diagonal matrices over commutative finite chain rings of a fixed determinant are presented in [4] and applied in the study of the determinants of some circulant matrices over commutative finite chain rings.

An element a in a commutative ring R with identity 1 is called a *unit* if there exists $b \in R$ such that $ab = 1$. A nonzero element a in a commutative ring R is call a zero-divisor if there exists a nonzero element $b \in R$ such that $ab = 0$. We note that a commutative finite chain ring is a disjoint union of the zero, zero-divisors, and units. The results on diagonal matrices over commutative finite chain rings in [4] and on matrices over commutative finite chain rings in [3] are established based on the three types of the determinants, i.e., zero, zero-divisors, and units.

Let R be a commutative ring with identity 1. For a positive integer n, an $n \times n$ *arrowhead matrix* over R is defined to be a square matrix containing zeros in all entries except for the first row, first column, and main diagonal. Precisely, the arrowhead matrix is in the form of

$$A = \begin{pmatrix} * & * & * & * & \cdots & * \\ * & * & 0 & 0 & \cdots & 0 \\ * & 0 & * & 0 & \cdots & 0 \\ * & 0 & 0 & * & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ * & 0 & 0 & 0 & \cdots & * \end{pmatrix},$$

where $*$s are arbitrary elements in R and they are not necessarily the same. From the definition, it is easily seen that an arrowhead matrix is a generalization of a diagonal matrix and it is a special case of a square matrix over R.

Arrowhead matrices are important for the computation of the eigenvalues via divide and conquer approaches in [9] as well as their application. In [11], applications of the arrowhead matrices of large order, the infinite invertible arrowhead matrices are given. In [14], a new algorithm for solving an eigenvalue problem for a real symmetric arrowhead matrix is given. The algorithm computed all eigenvalues and all components of the corresponding eigenvectors with high relative accuracy. Their results extended to Hermitian arrowhead matrices and other forms of arrowhead matrices.

In this thesis, we generalize results on the enumeration of diagonal matrices with prescribed determinant in [4] to arrowhead matrices. Alternatively, this can be viewed as an interesting subfamily of matrices studied in [3]. The number of $n \times n$ singular arrowhead matrices and the number of $n \times n$ non-singular arrowhead matrices over R are completely determined for all positive integers n. The complete enumeration is presented for $n \times n$ arrowhead matrices over $\mathbb{Z}_p$. For $n \times n$ arrowhead matrices over $\mathbb{Z}_{p^2}$, the enumeration is given for $n \times n$ non-singular arrowhead matrices whose determinant is a fixed unit in $\mathbb{Z}_{p^2}$. For singular arrowhead matrices over $\mathbb{Z}_{p^2}$, an upper bound for the number of $n \times n$ arrowhead matrices over $\mathbb{Z}_{p^2}$ with zero determinant and a lower bound for the number of $n \times n$ arrowhead matrices over $\mathbb{Z}_{p^2}$ with a non-zero determinant are presented.

The thesis is organized as follows. In Chapter 2, definitions, basic concepts, and preliminary results used in this thesis are recalled. The enumeration of $n \times n$ arrowhead matrices of fixed determinant over $\mathbb{Z}_p$ is presented in Chapter

3. In Chapter 4, the enumeration of $n \times n$ singular and non-singular arrowhead matrices over $\mathbb{Z}_{p^2}$ is given together with the number of $n \times n$ non-singular arrowhead matrices over $\mathbb{Z}_{p^2}$ whose determinant is a fixed unit in $\mathbb{Z}_{p^2}$. Subsequently, bounds for the number of $n \times n$ arrowhead matrices over $\mathbb{Z}_{p^2}$ with a fixed non-unit determinant are presented. Summary and discussion are given in Chapter 5.

Chapter 2

Preliminaries

In this chapter, basic concepts and elementary results in algebra used in the thesis are recalled together with some illustrative examples. The reader may refer to [12] for more details.

2.1 Rings

In this section, some properties of rings are reviewed. Especially, algebraic structures of the rings $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$ are recalled, where p is a prime number.

Definition 2.1. A *ring* is an algebraic structure composed of a non-empty set R and two binary operations on R, *addition* $(+)$ and *multiplication* $(\cdot)$, satisfying the following axioms:

1. Closure under addition $[\forall a, b \in R,\ a + b \in R]$.

2. Associativity of addition $[\forall a, b, c \in R,\ (a + b) + c = a + (b + c)]$.

3. Identity element for addition $[\exists z \in R\ \forall a \in R,\ z + a = a = a + z]$.

   The element z is often denoted by $0 \in R$.

4. Inverse elements for addition $[\forall a \in R\, \exists w \in R,\ a + w = 0 = w + a]$.

   The inverse of a is often denoted by $-a \in R$.

5. Commutative of addition $[\forall a, b \in R,\ a + b = b + a]$.

6. Closure under multiplication $[\forall a, b \in R,\ a \cdot b \in R]$.

7. Associativity of multiplication $[\forall a, b, c \in R,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)]$.

8. Product is distributive over addition

   $[\forall a, b, c \in R,\ a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + b \cdot a\ ]$.

For multiplication, we usually write ab instead of $a \cdot b$.

A ring R is called a *commutative ring* if R satisfies the additional axiom $ab = ba$ for all $a, b \in R$, and it is called a *ring with identity* if R contains a multiplicative identity element 1_R such that $1_R a = a = a 1_R$ for all $a \in R$. A ring R is called a *commutative ring with identity* if it is a commutative ring and it is a ring with identity.

Example 2.2. Some examples of rings are given as follows.

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are commutative rings with identity under the usual addition and multiplication of numbers.

2. For a prime number p, $(\mathbb{Z}_p, +, \cdot)$ and $(\mathbb{Z}_{p^2}, +, \cdot)$ are commutative rings with identity under the addition and multiplication modulo p and p^2, respectively.

An element a in a commutative ring R with identity 1 is called a *unit* if there exists $b \in R$ such that $ab = 1$. Denote by $\mathcal{U}(R) = \{a \in R \mid a \text{ is a unit in } R\}$ the set of units in R.

We mainly focus on the determinant of arrowhead matrices over $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$, where p is a prime number. The set $\mathcal{U}(\mathbb{Z}_p)$ and $\mathcal{U}(\mathbb{Z}_{p^2})$ are presented in the following lemma.

Lemma 2.3 ([12, Example 1.2.1 (5)])**.** *Let p be a prime number. Then*

$$\mathcal{U}(\mathbb{Z}_p) = \mathbb{Z}_p \setminus \{0\} \quad \textit{and} \quad |\mathcal{U}(\mathbb{Z}_p)| = p - 1.$$

Lemma 2.4 ([5, Lemma 2.1])**.** *Let p be a prime number. Then*

$$\mathcal{U}(\mathbb{Z}_{p^2}) = \{a \in \mathbb{Z}_{p^2} \mid p \nmid a\} \quad \textit{and} \quad |\mathcal{U}(\mathbb{Z}_{p^2})| = p(p-1).$$

A nonzero element a in a commutative ring R is call a *zero-divisor* if there exists a nonzero element $b \in R$ such that $ab = 0$. Denote by $\mathcal{ZD}(R) = \{a \in R \mid a \text{ is a zero-divisor in } R\}$ the set of zero-divisors in R.

Clearly, $\mathbb{Z}_p$ contains no zero-divisor. The zero-divisors in $\mathbb{Z}_{p^2}$ are presented in the following lemma.

Lemma 2.5 ([5, Lemma 2.2])**.** *Let p be a prime number. Then*

$$\mathcal{ZD}(\mathbb{Z}_{p^2}) = \{a \in \mathbb{Z}_{p^2} \mid p|a \textit{ and } a \neq 0\} \quad \textit{and} \quad |\mathcal{ZD}(\mathbb{Z}_{p^2})| = p - 1.$$

2.2 Matrices, Determinants, and Arrowhead Matrices

In this section, basic concepts and properties of matrices, determinants, and arrowhead matrices are recalled.

2.2.1 Matrices and Determinants

Let R be a commutative ring and let n be a positive integer. An $n \times n$ *matrix* over R is an array of elements in R arranged in n rows and n columns. A *diagonal matrix* is a square matrix where all the elements are 0 except for those in the diagonal from the top left corner to the bottom right corner, denoted by $\mathrm{diag}(a_1, a_2, a_3, \dots, a_n)$.

A *permutation* π of n elements is a one-to-one and onto function on the set $\{1, 2, \dots, n\}$.

Let π be a permutation on $\{1, 2, \dots, n\}$. An *inversion pair* (i, j) of π is a pair of positive integers $i, j \in \{1, \dots, n\}$ for which $i < j$ but $\pi(i) > \pi(j)$. Denote by $\mathrm{inv}(\pi)$ the number of inversion pairs in π. The *sign* of π, denoted by $sign(\pi)$, is defined by

$$\begin{aligned} sign(\pi) &= (-1)^{\mathrm{inv}(\pi)} \\ &= \begin{cases} +1, & \text{if the number of inversions in } \pi \text{ is even} \\ -1, & \text{if the number of inversions in } \pi \text{ is odd,} \end{cases} \end{aligned}$$

We call π an *even permutation* if $sign(\pi) = +1$, whereas π is called an *odd permutation* if $sign(\pi) = -1$.

Definition 2.6. Given a square matrix $A = [a_{ij}]$ over R, the *determinant*of A is defined to be

$$\det(A) = \sum_{\pi \in S_n} sign(\pi) a_{1,\pi(1)} a_{2,\pi(2)} a_{3,\pi(3)} \dots a_{n,\pi(n)},$$

where the sum is over all permutations of n elements.

Let A be an $n \times n$ matrix over R. The *i-j minor* of A, denoted it by M_{ij}, is the determinant of the $(n-1) \times (n-1)$ matrix which results from deleting the the i^{th} row and the j^{th} column of A. The *i-j cofactor* of A, denoted by C_{ij} is defined to be

$$C_{ij} = (-1)^{i+j} M_{ij}.$$

It is well known (see, for example, [12]) that the determinant of A can be given in terms of cofactors of A of the form

$$\det(A) = \sum_{i=1}^{n} a_{ij} C_{ij} = \sum_{j=1}^{n} a_{ij} C_{ij}$$

The first formula consists of expanding the determinant along the i^{th} row and the second expands the determinant along j^{th} column of A.

For an $n \times n$ matrix A over R, an *elementary row* (resp., *column*) *operation* on A is defined to be any of the following three operations on the rows (resp., columns) of A.

1. Switching the ith and jth rows (resp., columns) of A;

   denoted by $R_i \leftrightarrow R_j$ (resp., $C_i \leftrightarrow C_j$).

2. Multiplying the ith row (resp., column) of A by a nonzero scalar k;

   denoted by $kR_i \to R_i$ (resp., $kC_i \to C_i$).

3. Adding a scalar k multiple of the jth (resp., column) of A to the ith row (resp., column);

   denoted by $R_i + kR_j \to R_i$ (resp., $C_i + kC_j \to C_i$).

Useful relations between the determinant and elementary row (resp., column) operations of matrices are given in the following theorems.

Theorem 2.7 ([7, Theorem 3.16]). *Let A be an $n \times n$ matrix over a ring R and let B be a matrix which results from swiching two rows of A. Then* $\det(B) = -\det(A)$.

Theorem 2.8 ([7, Theorem 3.18]). *Let A be an $n \times n$ matrix over a ring R and let B be a matrix which results from multiplying a row of A by a scalar $k \in R$. Then* $\det(B) = k \det(A)$.

Suppose we were to multiply all n rows of A by k to obtain B, i.e., $B = kA$. We have the following property.

Theorem 2.9 ([7, Theorem 3.19]). *Let A and B be $n \times n$ matrices over a ring R and k a scalar, such that $B = kA$. Then* $\det(B) = k^n \det(A)$.

Theorem 2.10 ([7, Theorem 3.21]). *Let A be an $n \times n$ matrix over a ring R and let B be a matrix which results from adding a multiple of a row to another row. Then* $\det(A) = \det(B)$.

The determinant of a diagonal matrix can be easily computed as in the following theorem.

Theorem 2.11 ([7, Theorem 3.13]). *Let A be a diagonal matrix over a ring R. Then* $\det(A)$ *is obtained by taking the product of the entries on the main diagonal.*

2.2.2 Arrowhead Matrices

Let R be a commutative ring with identity 1. For a positive integer n, an $n \times n$ *arrowhead matrix* over R is defined to be a square matrix containing zeros in all entries except for the first row, first column, and main diagonal. Precisely, the arrowhead matrix is of the form

$$A = \begin{pmatrix} * & * & * & * & \cdots & * \\ * & * & 0 & 0 & \cdots & 0 \\ * & 0 & * & 0 & \cdots & 0 \\ * & 0 & 0 & * & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ * & 0 & 0 & 0 & \cdots & * \end{pmatrix},$$

where $*$s are arbitrary elements in R and they are not necessarily the same. From the definition, it is easily seen that an arrowhead matrix is a generalization of a diagonal matrix and it is a special case of a square matrix over R.

We note that for $n \in \{1, 2\}$, every $n \times n$ matrix over R is an arrowhead matrix. For $n \geq 3$, some examples of $n \times n$ arrowhead matrices are given in the following example.

Example 2.12. Some examples of arrowhead matrices are given as follows.

1. $A_1 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ is an arrowhead matrix over $\mathbb{Z}_2$ with $\det(A_1) = 0$.

2. $A_2 = \begin{pmatrix} 1 & 2 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 2 & 0 & 2 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$ is an arrowhead matrix over $\mathbb{Z}_3$ with $\det(A_2) = 2$.

For a positive integer n, let $\mathcal{A}_n(R)$ denote the set of $n \times n$ arrowhead matrices over R. For each element $a \in R$, let

$$\mathcal{A}_n(R, a) = \{A \in \mathcal{A}_n(R) \mid \det(A) = a\}.$$

be the set of all $n \times n$ arrowhead matrices over R whose determinant is a.

Let

$$\mathcal{IA}_n(R) = \{A \in \mathcal{A}_n(R) \mid \det(A) \in \mathcal{U}(R)\}$$

be the set of all $n \times n$ non-singular arrowhead matrices over R. It follows that

$$\mathcal{IA}_n(R) = \bigcup_{a \in \mathcal{U}(R)} \mathcal{A}_n(R, a).$$

We note that $\mathcal{U}(\mathbb{Z}_p) = \mathbb{Z}_p \smallsetminus \{0\}$ by Lemma 2.3 and $\mathcal{U}(\mathbb{Z}_{p^2}) = \{b \in \mathbb{Z}_{p^2} \mid p \nmid b\}$ is given in Lemma 2.4. It follows that

$$\mathcal{IA}_n(\mathbb{Z}_p) = \bigcup_{a \in \mathbb{Z}_p \smallsetminus \{0\}} \mathcal{A}_n(\mathbb{Z}_p, a) \quad \text{and} \quad \mathcal{IA}_n(\mathbb{Z}_{p^2}) = \bigcup_{a \in \{b \in \mathbb{Z}_{p^2} \mid p \nmid b\}} \mathcal{A}_n(\mathbb{Z}_{p^2}, a).$$

From the definitions above, it is not difficult to see that $\mathcal{A}_n(R)$ is a group under addition and $\mathcal{IA}_n(R)$ is a group under multiplication.

For groups G and H, let $\varphi : G \to H$ be a group homomorphism. The *image* of φ is defined to be the set

$$\mathrm{im}(\varphi) = \{\varphi(g) : g \in G\}.$$

The *kernel* of φ is defined to be

$$\ker(\varphi) = \{g \in G : \varphi(g) = e_H\},$$

where e_H is the identity of H.

The following isomorphism theorem for groups is useful in the enumeration of $n \times n$ non-singular arrowhead matrices over $\mathbb{Z}_{p^2}$ in Section 4.1.

Theorem 2.13 ([12, Theorem 1.4.2]). *Let G and H be groups and let $\varphi : G \to H$ be a group homomorphism. Then $G/(ker\varphi) \cong im(\varphi)$.*

Chapter 3

Enumeration of Arrowhead Matrices with Prescribed Determinant over $\mathbb{Z}_p$

In this chapter, the determinants of arrowhead matrices over $\mathbb{Z}_p$ are studied together with the determination of the number of arrowhead matrices over $\mathbb{Z}_p$ with a fixed determinant.

First, the number of $n \times n$ non-singular arrowhead matrices over $\mathbb{Z}_p$ is explicitly determined. A recursive formula for the number $|\mathcal{IA}_n(\mathbb{Z}_p)|$ is derived in the following proposition.

Proposition 3.1. *Let p be a prime number. Then*

$$|\mathcal{IA}_1(\mathbb{Z}_p)| = p - 1$$

and

$$|\mathcal{IA}_n(\mathbb{Z}_p)| = p^{2n-3}(p-1)^n + p^2(p-1)|\mathcal{IA}_{n-1}(\mathbb{Z}_p)|$$

for all $n \geq 2$.

Proof. Clearly, $|\mathcal{IA}_1(\mathbb{Z}_p)| = p - 1$. Let $n \geq 2$ be an integer and let

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1,n-1} & a_{1n} \\ a_{21} & a_{22} & 0 & \cdots & 0 & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1,1} & 0 & 0 & \cdots & a_{n-1,n-1} & 0 \\ a_{n1} & 0 & 0 & \cdots & 0 & a_{nn} \end{pmatrix} \in \mathcal{IA}_n(\mathbb{Z}_p).$$

We consider the following two cases.

Case 1: $a_{nn} \neq 0$. For convenience, for each $i \in \{1, 2, \ldots, n\}$, denote by R_i (resp., C_i) the ith row (resp, ith column) of A. Applying the following elementary row and column operations, it can be concluded that

$$R_1 - a_{1n}{a_{nn}}^{-1}R_n \to R_1 \quad A \sim \begin{pmatrix} a_{11} - a_{1n}a_{n1}{a_{nn}}^{-1} & a_{12} & a_{13} & \cdots & a_{1,n-1} & 0 \\ a_{21} & a_{22} & 0 & \cdots & 0 & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1,1} & 0 & 0 & \cdots & a_{n-1,n-1} & 0 \\ a_{n1} & 0 & 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$

$$C_1 - a_{n1}{a_{nn}}^{-1}C_n \to C_1 \quad \sim \begin{pmatrix} a_{11} - a_{1n}a_{n1}{a_{nn}}^{-1} & a_{12} & a_{13} & \cdots & a_{1,n-1} & 0 \\ a_{21} & a_{22} & 0 & \cdots & 0 & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1,1} & 0 & 0 & \cdots & a_{n-1,n-1} & 0 \\ 0 & 0 & 0 & \cdots & 0 & a_{nn} \end{pmatrix}.$$

Let

$$C = \begin{pmatrix} a_{11} - a_{1n}a_{n1}{a_{nn}}^{-1} & a_{12} & a_{13} & \cdots & a_{1,n-1} \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1,1} & 0 & 0 & \cdots & a_{n-1,n-1} \end{pmatrix}.$$

Then

$$\det(A) = \det\left(\begin{pmatrix} & & & 0 \\ & C & & \vdots \\ & & & 0 \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix}\right) = (-1)^{n+n} a_{nn}\det(C) = a_{nn}\det(C).$$

Let

$$S = \left\{ \begin{pmatrix} s_{11} & s_{12} & s_{13} & \cdots & s_{1,n-1} \\ s_{21} & s_{22} & 0 & \cdots & 0 \\ s_{31} & 0 & s_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{n-1,1} & 0 & 0 & \cdots & s_{n-1,n-1} \end{pmatrix} \in \mathcal{A}_{n-1}(\mathbb{Z}_p) \;\middle|\; \det\left(\begin{pmatrix} s_{11} - a_{1n}a_{n1}{a_{nn}}^{-1} & s_{12} & s_{13} & \cdots & s_{1,n-1} \\ s_{21} & s_{22} & 0 & \cdots & 0 \\ s_{31} & 0 & s_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{n-1,1} & 0 & 0 & \cdots & s_{n-1,n-1} \end{pmatrix}\right) \neq 0 \right\}.$$

It follows that

$$\begin{pmatrix} s_{11} & s_{12} & s_{13} & \cdots & s_{1,n-1} \\ s_{21} & s_{22} & 0 & \cdots & 0 \\ s_{31} & 0 & s_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{n-1,1} & 0 & 0 & \cdots & s_{n-1,n-1} \end{pmatrix} \in S$$

if and only if

$$\begin{pmatrix} s_{11} - a_{1n}a_{n1}{a_{nn}}^{-1} & s_{12} & s_{13} & \cdots & s_{1,n-1} \\ s_{21} & s_{22} & 0 & \cdots & 0 \\ s_{31} & 0 & s_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{n-1,1} & 0 & 0 & \cdots & s_{n-1,n-1} \end{pmatrix} \in \mathcal{IA}_{n-1}(\mathbb{Z}_p).$$

Hence, the map $\psi : S \to \mathcal{IA}_{n-1}(\mathbb{Z}_p)$ defined by

$$\begin{pmatrix} s_{11} & s_{12} & s_{13} & \cdots & s_{1,n-1} \\ s_{21} & s_{22} & 0 & \cdots & 0 \\ s_{31} & 0 & s_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{n-1,1} & 0 & 0 & \cdots & s_{n-1,n-1} \end{pmatrix} \mapsto \begin{pmatrix} s_{11} - a_{1n}a_{n1}{a_{nn}}^{-1} & s_{12} & s_{13} & \cdots & s_{1,n-1} \\ s_{21} & s_{22} & 0 & \cdots & 0 \\ s_{31} & 0 & s_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{n-1,1} & 0 & 0 & \cdots & s_{n-1,n-1} \end{pmatrix}$$

is a bijection and it can be concluded that $|S| = |\mathcal{IA}_{n-1}(\mathbb{Z}_p)|$.

Since $0 \neq \det(A) = a_{nn}\det(C)$ if and only if $\det(C) \neq 0$, we have

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1,n-1} \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1,1} & 0 & 0 & \cdots & a_{n-1,n-1} \end{pmatrix} \in S$$

which has $|S| = |\mathcal{IA}_{n-1}(\mathbb{Z}_p)|$ possibilities. Since a_{1n} and a_{n1} can be arbitrary elements in $\mathbb{Z}_p$, the number of choices of a_{1n} and a_{n1} are p^2. The number of choices for a_{nn} is $p-1$. In this case, the number of choices of A in $\mathcal{IA}_n(\mathbb{Z}_p)$ is $p^2(p-1)|\mathcal{IA}_{n-1}(\mathbb{Z}_p)|$.

Case 2: $a_{nn} = 0$. Since $\det(A) \neq 0$, it follows that $a_{1n} \neq 0$ and $a_{n1} \neq 0$. Applying the following elementary row and column operations, we have

$$R_i - a_{i1}{a_{n1}}^{-1}R_n \to R_i \quad A \sim \begin{pmatrix} 0 & a_{12} & a_{13} & \cdots & a_{1,n-1} & a_{1n} \\ 0 & a_{22} & 0 & \cdots & 0 & 0 \\ 0 & 0 & a_{33} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_{n-1,n-1} & 0 \\ a_{n1} & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

$$C_1 \leftrightarrow C_n \quad \sim \begin{pmatrix} a_{1n} & a_{12} & a_{13} & \cdots & a_{1,n-1} & 0 \\ 0 & a_{22} & 0 & \cdots & 0 & 0 \\ 0 & 0 & a_{33} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_{n-1,n-1} & 0 \\ 0 & 0 & 0 & \cdots & 0 & a_{n1} \end{pmatrix} =: A'.$$

Since $\det(A') = -\det(A) \neq 0$ if and only if $a_{1n}, a_{22}, \ldots, a_{n-1,n-1}, a_{n1} \neq 0$, the number of matrices $\operatorname{diag}(a_{1n}, a_{22}, a_{33}, \ldots, a_{n-1,n-1}, a_{n1})$ is $(p-1)^n$, a_{1j} for each $j = 1, \ldots, n-1$ has p^{n-1} possibilities, and a_{i1} for each $i = 2, \ldots, n-1$ has p^{n-2} possibilities. In this case, the number of A in $\mathcal{IA}_n(\mathbb{Z}_p)$ is $p^{2n-3}(p-1)^n$.

From both cases, we have

$$|\mathcal{IA}_n(\mathbb{Z}_p)| = p^{2n-3}(p-1)^n + p^2(p-1)|\mathcal{IA}_{n-1}(\mathbb{Z}_p)|$$

as desired. $\square$

From the recursive formula of $|\mathcal{IA}_n(\mathbb{Z}_p)|$ given in Proposition 3.1, an explicit expression for the number $|\mathcal{IA}_n(\mathbb{Z}_p)|$ can be derived using the mathematical induction in the following theorem.

Theorem 3.2. *Let p be a prime number. Then*

$$|\mathcal{IA}_n(\mathbb{Z}_p)| = p^{2n-3}(p-1)^n(p + (n-1))$$

for all positive integers n.

Proof. The proof is given based on the mathematical induction. For $n = 1$, we have

$$
\begin{aligned}
|\mathcal{IA}_1(\mathbb{Z}_p)| &= p - 1 \\
&= p^{2(1)-3}(p-1)^1(p + (1-1)).
\end{aligned}
$$

Let $k \geq 2$ be an integer. Assume that

$$|\mathcal{IA}_{k-1}(\mathbb{Z}_p)| = p^{2(k-1)-3}(p-1)^{k-1}(p + ((k-1)-1)).$$

From Proposition 3.1, we have that

$$
\begin{aligned}
|\mathcal{IA}_k(\mathbb{Z}_p)| &= p^{2k-3}(p-1)^k + p^2(p-1)|\mathcal{IA}_{k-1}(\mathbb{Z}_p)| \\
&= p^{2k-3}(p-1)^k + p^2(p-1)(p^{2(k-1)-3}(p-1)^{k-1}(p + ((k-1)-1))) \\
&= p^{2k-3}(p-1)^k + p^2(p-1)(p^{2k-5}(p-1)^{k-1}(p + (k-2))) \\
&= p^{2k-3}(p-1)^k + p^{2k-3}(p-1)^k(p + (k-2)) \\
&= p^{2k-3}(p-1)^k(p + (k-1)).
\end{aligned}
$$

By the mathematical induction, it can be concluded that

$$|\mathcal{IA}_n(\mathbb{Z}_p)| = p^{2n-3}(p-1)^n(p + (n-1))$$

for all positive integers n. □

The relation between $|\mathcal{A}_n(\mathbb{Z}_p, 1)|$ and $|\mathcal{A}_n(\mathbb{Z}_p, a)|$ for all $a \in \mathbb{Z}_p \smallsetminus \{0\}$ in the following proposition is key to determine the number $|\mathcal{A}_n(\mathbb{Z}_p, a)|$ later in Corollary 3.4.

Proposition 3.3. *Let p be a prime number and let n be a positive integer. Then*

$$|\mathcal{A}_n(\mathbb{Z}_p, a)| = |\mathcal{A}_n(\mathbb{Z}_p, 1)|$$

for all $a \in \mathbb{Z}_p \smallsetminus \{0\}$.

Proof. Let $a \in \mathbb{Z}_p \smallsetminus \{0\}$ and let $f : \mathcal{A}_n(\mathbb{Z}_p, 1) \to \mathcal{A}_n(\mathbb{Z}_p, a)$ be the function defined by

$$f(A) = \operatorname{diag}(a, 1, 1, \ldots, 1)A.$$

Let

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & 0 & 0 & \cdots & a_{nn} \end{pmatrix} \in \mathcal{A}_n(\mathbb{Z}_p, 1).$$

Then $\det(A) = 1$ and

$$\begin{aligned} f(A) &= \operatorname{diag}(a, 1, 1, \ldots, 1)A \\ &= \begin{pmatrix} aa_{11} & aa_{12} & aa_{13} & \cdots & aa_{1n} \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & 0 & 0 & \cdots & a_{nn} \end{pmatrix}. \end{aligned} \tag{3.1}$$

It follows that $f(A) \in \mathcal{A}_n(\mathbb{Z}_p)$ and

$$\begin{aligned}\det(f(A)) &= \det(\mathrm{diag}(a, 1, 1, \dots, 1)A) \\ &= \det(\mathrm{diag}(a, 1, 1, \dots, 1)) \cdot \det(A) \\ &= a \cdot 1 \\ &= a.\end{aligned}$$

Hence, $f(A) \in \mathcal{A}_n(\mathbb{Z}_p, a)$.

Let $A, B \in \mathcal{A}_n(\mathbb{Z}_p, 1)$ be such that $f(A) = f(B)$. Then $\mathrm{diag}(a, 1, 1, \dots, 1)A = \mathrm{diag}(a, 1, 1, \dots, 1)B$. Since $\mathrm{diag}(a, 1, 1, \dots, 1)$ is invertible, we have that $A = B$. Hence, f is injective.

Let $X \in \mathcal{A}_n(\mathbb{Z}_p, a)$. Since a is invertible, let $A = \mathrm{diag}(a^{-1}, 1, 1, \dots, 1)X$. Using the argument similar to that of (3.1), it can be deduced that $A \in \mathcal{A}_n(\mathbb{Z}_p)$ and $\det(A) = \det(\mathrm{diag}(a^{-1}, 1, 1, \dots, 1)X) = a^{-1} \cdot a = 1$. Hence, $A \in \mathcal{A}_n(\mathbb{Z}_p, 1)$ and

$$f(A) = f(\mathrm{diag}(a^{-1}, 1, 1, \dots, 1)X) = \mathrm{diag}(a, 1, 1, \dots, 1)\mathrm{diag}(a^{-1}, 1, 1, \dots, 1)X = X.$$

It follows that f is surjective.

All together f is a bijection. Therefore, $|\mathcal{A}_n(\mathbb{Z}_p, 1)| = |\mathcal{A}_n(\mathbb{Z}_p, a)|$ as desired. $\square$

From Proposition 3.3, it can be deduced that

$$|\mathcal{A}_n(\mathbb{Z}_p, a)| = |\mathcal{A}_n(\mathbb{Z}_p, 1)| = |\mathcal{A}_n(\mathbb{Z}_p, b)|$$

for all $a, b \in \mathbb{Z}_p \setminus \{0\}$.

Using Theorem 3.2 and Proposition 3.3, we have the following corollary.

Corollary 3.4. *Let p be a prime number and let n be positive integer. Then*

$$|\mathcal{A}_n(\mathbb{Z}_p, a)| = p^{2n-3}(p-1)^{n-1}(p+(n-1))$$

for all $a \in \mathbb{Z}_p \setminus \{0\}$.

Proof. From Proposition 3.3, we have $|\mathcal{A}_n(\mathbb{Z}_p, a)| = |\mathcal{A}_n(\mathbb{Z}_p, 1)|$ for all $a \in \mathbb{Z}_p \setminus \{0\}$. Since $\mathcal{IA}_n(\mathbb{Z}_p) = \bigcup_{a \in \mathbb{Z}_p \setminus \{0\}} \mathcal{A}_n(\mathbb{Z}_p, a)$ is a disjoint union and $|\mathbb{Z}_p \setminus \{0\}| = p-1$ by Lemma 2.3, it follows that $|\mathcal{IA}_n(\mathbb{Z}_p)| = |\mathbb{Z}_p \setminus \{0\}||\mathcal{A}_n(\mathbb{Z}_p, 1)| = (p-1)|\mathcal{A}_n(\mathbb{Z}_p, 1)|$. By Theorem 3.2 and and Proposition 3.3, we have

$$\begin{aligned}
|\mathcal{A}_n(\mathbb{Z}_p, a)| &= |\mathcal{A}_n(\mathbb{Z}_p, 1)| \\
&= \frac{|\mathcal{IA}_n(\mathbb{Z}_p)|}{p-1} \\
&= \frac{p^{2n-3}(p-1)^n(p+(n-1))}{p-1} \\
&= p^{2n-3}(p-1)^{n-1}(p+(n-1))
\end{aligned}$$

as desired. □

The number of $n \times n$ arrowhead matrices over $\mathbb{Z}_p$ is $|\mathcal{A}_n(\mathbb{Z}_p)| = p^{3n-2}$ and the number of $n \times n$ non-singular arrowhead matrices over $\mathbb{Z}_p$ is

$$|\mathcal{IA}_n(\mathbb{Z}_p)| = p^{2n-3}(p-1)^n(p+(n-1))$$

given in Theorem 3.2. The number $|\mathcal{A}_n(\mathbb{Z}_p, 0)|$ of $n \times n$ singular arrowhead matrices over $\mathbb{Z}_p$ can be deduced in the following corollary.

Corollary 3.5. *Let p be a prime number. Then*

$$|\mathcal{A}_n(\mathbb{Z}_p, 0)| = |\mathcal{A}_n(\mathbb{Z}_p)| - |\mathcal{IA}_n(\mathbb{Z}_p)| = p^{3n-2} - p^{2n-3}(p-1)^n(p+(n-1))$$

for all positive integers n.

We note that $|\mathcal{A}_n(\mathbb{Z}_p)| = p^{3n-2}$ and the numbers $|\mathcal{IA}_n(\mathbb{Z}_p)|$, $|\mathcal{A}_n(\mathbb{Z}_p, a)|$ for all elements $a \in \mathbb{Z}_p \setminus \{0\}$, and $|\mathcal{A}_n(\mathbb{Z}_p, 0)|$ are given in Theorem 3.2, Corollary 3.4, and Corollary 3.5, respectively. Some illustrative calculations are presented in Table 3.1.

Table 3.1: Number of Arrowhead Matrices over $\mathbb{Z}_p$

p	n	$\lvert\mathcal{A}_n(\mathbb{Z}_p)\rvert$	$\lvert\mathcal{IA}_n(\mathbb{Z}_p)\rvert$	$\lvert\mathcal{A}_n(\mathbb{Z}_p, a)\rvert$, $a \in \mathbb{Z}_p \setminus \{0\}$	$\lvert\mathcal{A}_n(\mathbb{Z}_p, 0)\rvert$
2	3	128	32	32	96
2	4	1,024	160	160	864
2	5	8,192	768	768	7,424
2	6	65,536	3,584	3,584	61,952
3	3	2,187	1,080	540	1107
3	4	59,049	23,328	11,664	35,721
3	5	1,594,323	489,888	244,944	1,104,435
3	6	43,046,721	10,077,696	5,038,848	32,969,025
5	3	78,125	56,000	14,000	22,125
5	4	9,765,625	6,400,000	1,600,000	3,365,625
5	5	1,220,703,125	720,000,000	180,000,000	500,703,125
7	3	823,543	666,792	111,132	156,751
7	4	282,475,249	217,818,720	36,303,120	64,656,529

Chapter 4

Enumeration of Arrowhead Matrices with Prescribed Determinant over $\mathbb{Z}_{p^2}$

In this chapter, the enumeration of $n \times n$ arrowhead matrices with prescribed determinant over $\mathbb{Z}_{p^2}$ is focused on. The number of $n \times n$ non-singular (resp., singular) arrowhead matrices over $\mathbb{Z}_{p^2}$ is presented. For non-singular arrowhead matrices, the number of $n \times n$ arrowhead matrices over $\mathbb{Z}_{p^2}$ with a given unit determinant is given. For singular arrowhead matrices, bounds on the number of $n \times n$ arrowhead matrices with a fixed determinant over $\mathbb{Z}_{p^2}$ are presented.

4.1 Non-Singular Arrowhead Matrices over $\mathbb{Z}_{p^2}$

In this section, the number of $n \times n$ non-singular arrowhead matrices over $\mathbb{Z}_{p^2}$ is presented together with the number of $n \times n$ arrowhead matrices over $\mathbb{Z}_{p^2}$ whose determinant is a fixed unit in $\mathbb{Z}_{p^2}$.

An explicit formula for the number $|\mathcal{IA}_n(\mathbb{Z}_{p^2})|$ of $n \times n$ non-singular matrices is given in the following theorem.

Theorem 4.1. *Let p be a prime number. Then*

$$|\mathcal{IA}_n(\mathbb{Z}_{p^2})| = p^{5n-5}(p-1)^n(p+(n-1))$$

for all positive integers n.

Proof. By considering the two sets $\mathcal{A}_n(\mathbb{Z}_{p^2})$ and $\mathcal{A}_n(\mathbb{Z}_p)$ as additive groups, let $\phi : \mathcal{A}_n(\mathbb{Z}_{p^2}) \to \mathcal{A}_n(\mathbb{Z}_p)$ be the group homomorphism defined by

$$A = [a_{ij}] \mapsto [a_{ij} \pmod p].$$

For each $X \in \mathcal{A}_n(\mathbb{Z}_p)$, by abuse of notation, we have $X + pI_n \in \mathcal{A}_n(\mathbb{Z}_{p^2})$ and $\phi(X + pI_n) = X$. It follows that ϕ is a surjective homomorphism. By the First Isomorphism Theorem for groups (see Theorem 2.13), it follows that $\mathcal{A}_n(\mathbb{Z}_p) \cong \mathcal{A}_n(\mathbb{Z}_{p^2})/\ker(\phi)$. Hence,

$$|\ker(\phi)| = \frac{|\mathcal{A}_n(\mathbb{Z}_{p^2})|}{|\mathcal{A}_n(\mathbb{Z}_p)|} = \frac{p^{2(3n-2)}}{p^{3n-2}} = p^{3n-2}.$$

For $A \in \mathcal{A}_n(\mathbb{Z}_{p^2})$, we have $\det(\phi(A)) = \det(A) \pmod p$ since the congruence modulo p is a ring homomorphism from $\mathbb{Z}_{p^2}$ onto $\mathbb{Z}_p$. By Lemma 2.4, it follows that $\det(A)$ is a unit in $\mathbb{Z}_{p^2}$ if and only if $\det(\phi(A)) \neq 0$ in $\mathbb{Z}_p$. Hence, A is invertible over $\mathbb{Z}_{p^2}$ if and only if $\phi(A)$ is invertible. It follows that the restriction map $\phi|_{\mathcal{IA}_n(\mathbb{Z}_{p^2})} : \mathcal{IA}_n(\mathbb{Z}_{p^2}) \to \mathcal{IA}_n(\mathbb{Z}_p)$ is surjective. From Theorem 3.2, we have

$$|\mathcal{IA}_n(\mathbb{Z}_p)| = p^{2n-3}(p-1)^n(p + (n-1)).$$

Hence,

$$\begin{aligned}
|\mathcal{IA}_n(\mathbb{Z}_{p^2})| &= |\ker(\phi)||\mathcal{IA}_n(\mathbb{Z}_p)| \\
&= p^{3n-2}|\mathcal{IA}_n(\mathbb{Z}_p)| \\
&= p^{3n-2}p^{2n-3}(p-1)^n(p + (n-1)) \\
&= p^{5n-5}(p-1)^n(p + (n-1))
\end{aligned}$$

as desired. $\square$

Since the number of $n \times n$ arrowhead matrices over $\mathbb{Z}_{p^2}$ is $p^{2(3n-2)}$, the next corollary follows immediately from Theorem 4.1.

Corollary 4.2. *Let p be a prime number. Then the number of $n \times n$ singular arrowhead matrices over $\mathbb{Z}_{p^2}$ is*

$$p^{5n-5}\left(p^{n+1} - (p-1)^n(p + (n-1))\right)$$

for all positive integers n.

For each $a \in \mathcal{U}(\mathbb{Z}_{p^2})$, the relation between $|\mathcal{A}_n(\mathbb{Z}_{p^2}, 1)|$ and $|\mathcal{A}_n(\mathbb{Z}_{p^2}, a)|$ in the following proposition is key to determined the number $|\mathcal{A}_n(\mathbb{Z}_{p^2}, a)|$ in Corollary 4.4.

Proposition 4.3. *Let p be a prime number and let n be a positive integer. Then*

$$|\mathcal{A}_n(\mathbb{Z}_{p^2}, a)| = |\mathcal{A}_n(\mathbb{Z}_{p^2}, 1)|$$

for all $a \in \mathcal{U}(\mathbb{Z}_{p^2})$.

Proof. Let $a \in \mathcal{U}(\mathbb{Z}_{p^2})$ and let $\varphi : \mathcal{A}_n(\mathbb{Z}_{p^2}, 1) \to \mathcal{A}_n(\mathbb{Z}_{p^2}, a)$ be the map defined by

$$\varphi(A) = \operatorname{diag}(a, 1, 1, \ldots, 1)A.$$

Using arguments similar to those in the proof of Proposition 3.3, it can be concluded that φ is a bijection from $\mathcal{A}_n(\mathbb{Z}_{p^2}, 1)$ onto $\mathcal{A}_n(\mathbb{Z}_{p^2}, a)$. Therefore, $|\mathcal{A}_n(\mathbb{Z}_{p^2}, 1)| = |\mathcal{A}_n(\mathbb{Z}_{p^2}, a)|$ as desired. $\square$

From Proposition 4.3, it can be deduced that $|\mathcal{A}_n(\mathbb{Z}_{p^2}, a)| = |\mathcal{A}_n(\mathbb{Z}_{p^2}, 1)| = |\mathcal{A}_n(\mathbb{Z}_{p^2}, b)|$ for all units $a, b \in \mathcal{U}(\mathbb{Z}_{p^2})$.

For a fixed unit $a \in \mathbb{Z}_{p^2}$, the number of $n \times n$ arrowhead matrices over $\mathbb{Z}_{p^2}$ whose determinant is a will be given in Corollary 4.4.

Corollary 4.4. *Let p be a prime number and let n be a positive integer. Then*

$$|\mathcal{A}_n(\mathbb{Z}_{p^2}, a)| = p^{5n-6}(p-1)^{n-1}(p + (n-1))$$

for all $a \in \mathcal{U}(\mathbb{Z}_{p^2})$.

Proof. First, we note that $\mathcal{I}\mathcal{A}_n(\mathbb{Z}_{p^2})$ is disjoint union of $\mathcal{A}_n(\mathbb{Z}_{p^2}, a)$ for all $a \in \mathcal{U}(\mathbb{Z}_{p^2})$. Precisely,

$$\mathcal{I}\mathcal{A}_n(\mathbb{Z}_{p^2}) = \bigcup_{a \in \mathcal{U}(\mathbb{Z}_{p^2})} \mathcal{A}_n(\mathbb{Z}_{p^2}, a)$$

is a disjoint union. By Proposition 4.3, $\mathcal{A}_n(\mathbb{Z}_{p^2}, a)$ has the same number of elements as $\mathcal{A}_n(\mathbb{Z}_{p^2}, 1)$, and hence,

$$\begin{aligned}
|\mathcal{I}\mathcal{A}_n(\mathbb{Z}_{p^2})| &= \left| \bigcup_{a \in \mathcal{U}(\mathbb{Z}_{p^2})} \mathcal{A}_n(\mathbb{Z}_{p^2}, a) \right| \\
&= \sum_{a \in \mathcal{U}(\mathbb{Z}_{p^2})} |\mathcal{A}_n(\mathbb{Z}_{p^2}, a)| \\
&= \sum_{a \in \mathcal{U}(\mathbb{Z}_{p^2})} |\mathcal{A}_n(\mathbb{Z}_{p^2}, 1)| \\
&= |\mathcal{U}(\mathbb{Z}_{p^2})||\mathcal{A}_n(\mathbb{Z}_{p^2}, 1)|.
\end{aligned}$$

From Lemma 2.4, we have $|\mathcal{U}(\mathbb{Z}_{p^2})| = p(p-1)$. By Proposition 4.3, it can be deduced that

$$\begin{aligned}|\mathcal{A}_n(\mathbb{Z}_{p^2},a)| &= |\mathcal{A}_n(\mathbb{Z}_{p^2},1)| \\ &= \frac{|\mathcal{I}\mathcal{A}_n(\mathbb{Z}_{p^2})|}{|\mathcal{U}(\mathbb{Z}_{p^2})|} \\ &= \frac{p^{5n-5}(p-1)^n(p+(n-1))}{p(p-1)} \\ &= p^{5n-6}(p-1)^{n-1}(p+(n-1)).\end{aligned}$$

The proof is completed. □

The numbers $|\mathcal{I}\mathcal{A}_n(\mathbb{Z}_{p^2})|$ and $|\mathcal{A}_n(\mathbb{Z}_{p^2},a)|$ for all $a \in \mathbb{Z}_p \setminus \{0\}$ are given in Theorem 4.1 and Corollary 4.4, respectively. Some illustrative calculations are presented in Table 4.1.

Table 4.1: Number of Arrowhead Matrices over $\mathbb{Z}_{p^2}$

p	n	$\lvert\mathcal{I}\mathcal{A}_n(\mathbb{Z}_{p^2})\rvert$	$\lvert\mathcal{U}(\mathbb{Z}_{p^2})\rvert$	$\lvert\mathcal{A}_n(\mathbb{Z}_{p^2},a)\rvert$, $a \in \mathcal{U}(\mathbb{Z}_{p^2})$
2	3	$4,096$	2	$2,048$
2	4	$163,840$	2	$81,920$
2	5	$6,291,456$	2	$3,145,728$
2	6	$234,881,024$	2	$117,440,512$
3	3	$2,361,960$	6	$393,660$
3	4	$1,377,495,072$	6	$229,582,512$

4.2 Singular Arrowhead Matrices over $\mathbb{Z}_{p^2}$

In this section, the number of $n \times n$ singular arrowhead matrices with prescribed determinant over $\mathbb{Z}_{p^2}$ are studied. Unlike the previous section, only bounds on the number of $n \times n$ arrowhead matrices over $\mathbb{Z}_{p^2}$ with prescribed non-unit determinant are given. Precisely, a lower bound on the number of $n \times n$ arrowhead matrices with zero determinant over $\mathbb{Z}_{p^2}$ and an upper bound on the number of $n \times n$ arrowhead matrices over $\mathbb{Z}_{p^2}$ with a fixed non-zero determinant are presented.

From Corollary 4.2, the number of $n \times n$ singular arrowhead matrices over $\mathbb{Z}_{p^2}$ is

$$p^{5n-5}\left(p^{n+1} - (p-1)^n(p + (n-1))\right)$$

for all positive integers n. Lower and upper bounds on the number of $n \times n$ singular arrowhead matrices over $\mathbb{Z}_{p^2}$ with prescribed determinant are given in the following subsections.

4.2.1 Singular Arrowhead Matrices over $\mathbb{Z}_{p^2}$ with Zero Determinant

In this subsection, a lower bound on the number of $n \times n$ singular arrowhead matrices over $\mathbb{Z}_{p^2}$ with zero determinant is derived.

Proposition 4.5. *Let p be a prime number. Then $|\mathcal{A}_1(\mathbb{Z}_{p^2}, 0)| = 1$ and*

$$\begin{aligned} |\mathcal{A}_n(\mathbb{Z}_{p^2}, 0)| \geq{}& p^5(p-1)|\mathcal{A}_{n-1}(\mathbb{Z}_{p^2}, 0)| + p^{6n-8}(p^2 + p - 1) \\ &- p^{5n-8}(p-1)^n(p^2 + (p+1)n - 2) \end{aligned}$$

for all $n \geq 2$.

Proof. Clearly, $|\mathcal{A}_1(\mathbb{Z}_{p^2},0)| = 1$. Let $n \geq 2$ be an integer and let

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1,n-1} & a_{1n} \\ a_{21} & a_{22} & 0 & \cdots & 0 & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1,1} & 0 & 0 & \cdots & a_{n-1,n-1} & 0 \\ a_{n1} & 0 & 0 & \cdots & 0 & a_{nn} \end{pmatrix} \in \mathcal{A}_n(\mathbb{Z}_{p^2},0).$$

Consider the following two cases.

Case 1: $a_{1n} \in \mathcal{U}(\mathbb{Z}_{p^2})$ or $a_{nn} \in \mathcal{U}(\mathbb{Z}_{p^2})$.

Case 1.1: $a_{nn} \in \mathcal{U}(\mathbb{Z}_{p^2})$. Using elementary row operations, we have that

$$a_{nn}{}^{-1}R_n \to R_n \quad A \sim \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1,n-1} & a_{1n} \\ a_{21} & a_{22} & 0 & \cdots & 0 & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1,1} & 0 & 0 & \cdots & a_{n-1,n-1} & 0 \\ a_{n1}a_{nn}{}^{-1} & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

$$R_1 - a_{1n}R_n \to R_1 \quad \sim \begin{pmatrix} a_{11} - a_{1n}a_{n1}a_{nn}{}^{-1} & a_{12} & a_{13} & \cdots & a_{1,n-1} & 0 \\ a_{21} & a_{22} & 0 & \cdots & 0 & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1,1} & 0 & 0 & \cdots & a_{n-1,n-1} & 0 \\ a_{n1}a_{nn}{}^{-1} & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Let

$$C = \begin{pmatrix} a_{11} - a_{1n}a_{n1}{a_{nn}}^{-1} & a_{12} & a_{13} & \cdots & a_{1,n-1} \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1,1} & 0 & 0 & \cdots & a_{n-1,n-1} \end{pmatrix}.$$

Then

$$\det(A) = \det\left(\begin{pmatrix} & & & 0 \\ & C & & \vdots \\ & & & 0 \\ a_{n1}{a_{nn}}^{-1} & \cdots & 0 & 1 \end{pmatrix}\right) = (-1)^{n+n}(1)\det(C) = \det(C). \quad (4.1)$$

Let

$$T = \left\{ \begin{pmatrix} t_{11} & t_{12} & t_{13} & \cdots & t_{1,n-1} \\ t_{21} & t_{22} & 0 & \cdots & 0 \\ t_{31} & 0 & t_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ t_{n-1,1} & 0 & 0 & \cdots & t_{n-1,n-1} \end{pmatrix} \in \mathcal{A}_{n-1}(\mathbb{Z}_{p^2}) \;\middle|\; \det\left(\begin{pmatrix} t_{11} - a_{1n}a_{n1}a_{nn}^{-1} & t_{12} & t_{13} & \cdots & t_{1,n-1} \\ t_{21} & t_{22} & 0 & \cdots & 0 \\ t_{31} & 0 & t_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ t_{n-1,1} & 0 & 0 & \cdots & t_{n-1,n-1} \end{pmatrix}\right) = 0 \right\}.$$

Since

$$\begin{pmatrix} t_{11} & t_{12} & t_{13} & \cdots & t_{1,n-1} \\ t_{21} & t_{22} & 0 & \cdots & 0 \\ t_{31} & 0 & t_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ t_{n-1,1} & 0 & 0 & \cdots & t_{n-1,n-1} \end{pmatrix} \in T$$

if and only if

$$\begin{pmatrix} t_{11} - a_{1n}a_{n1}a_{nn}^{-1} & t_{12} & t_{13} & \cdots & t_{1,n-1} \\ t_{21} & t_{22} & 0 & \cdots & 0 \\ t_{31} & 0 & t_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ t_{n-1,1} & 0 & 0 & \cdots & t_{n-1,n-1} \end{pmatrix} \in \mathcal{A}_{n-1}(\mathbb{Z}_{p^2}, 0).$$

The map $\varphi : T \to \mathcal{A}_{n-1}(\mathbb{Z}_{p^2}, 0)$ be defined by

$$\begin{pmatrix} t_{11} & t_{12} & t_{13} & \cdots & t_{1,n-1} \\ t_{21} & t_{22} & 0 & \cdots & 0 \\ t_{31} & 0 & t_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ t_{n-1,1} & 0 & 0 & \cdots & t_{n-1,n-1} \end{pmatrix} \mapsto \begin{pmatrix} t_{11} - a_{1n}a_{n1}a_{nn}^{-1} & t_{12} & t_{13} & \cdots & t_{1,n-1} \\ t_{21} & t_{22} & 0 & \cdots & 0 \\ t_{31} & 0 & t_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ t_{n-1,1} & 0 & 0 & \cdots & t_{n-1,n-1} \end{pmatrix}$$

is a bijection. It follows that $|T| = |\mathcal{A}_{n-1}(\mathbb{Z}_{p^2}, 0)|$. From (4.1), $\det(A) \equiv 0 \pmod{p^2}$ if and only if $\det(C) \equiv 0 \pmod{p^2}$. The number of matrices C with determinant 0 is $|T| = |\mathcal{A}_{n-1}(\mathbb{Z}_{p^2}, 0)|$. The number of choices for a_{1n}, a_{n1} is p^4. The number of choices for a_{nn} is $p(p-1)$ by Lemma 2.4. In this case, there are $p^5(p-1)|\mathcal{A}_{n-1}(\mathbb{Z}_{p^2}, 0)|$ possibilities for A.

Case 1.2: $a_{nn} \notin \mathcal{U}(\mathbb{Z}_{p^2})$ and $a_{1n} \in \mathcal{U}(\mathbb{Z}_{p^2})$. We note that

$$
\begin{aligned}
\det(A) =& (-1)^{1+n} a_{1n} \det\left(\begin{pmatrix} a_{21} & a_{22} & 0 & \cdots & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1,1} & 0 & 0 & \cdots & a_{n-1,n-1} \\ a_{n1} & 0 & 0 & \cdots & 0 \end{pmatrix}\right) \\
&+ (-1)^{n+n} a_{nn} \det\left(\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1,n-1} \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1,1} & 0 & 0 & \cdots & a_{n-1,n-1} \end{pmatrix}\right) \\
=& (-1)^{1+n} a_{1n} (-1)^{n+1} a_{n1} \det\left(\begin{pmatrix} a_{22} & 0 & \cdots & 0 \\ 0 & a_{33} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{n-1,n-1} \end{pmatrix}\right) \\
&+ a_{nn} \det\left(\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1,n-1} \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1,1} & 0 & 0 & \cdots & a_{n-1,n-1} \end{pmatrix}\right)
\end{aligned}
$$

$$=a_{1n}a_{n1}\det\left(\begin{pmatrix} a_{22} & 0 & \cdots & 0 \\ 0 & a_{33} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{n-1,n-1} \end{pmatrix}\right)$$

$$+\,a_{nn}\det\left(\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1,n-1} \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1,1} & 0 & 0 & \cdots & a_{n-1,n-1} \end{pmatrix}\right).$$

If $a_{n1} = 0$ and

$$\det\left(\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1,n-1} \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1,1} & 0 & 0 & \cdots & a_{n-1,n-1} \end{pmatrix}\right) \notin \mathcal{U}(\mathbb{Z}_{p^2})$$

which has $p^{2(3n-5)} - |\mathcal{IA}_{n-1}(\mathbb{Z}_{p^2})|$ choices, then $\det(A) = 0$. The number of choices for a_{1n} is $p(p-1)$ by Lemma 2.4. The number of choices for a_{n1} is 1. The number of choices for a_{nn} is $p^2 - p(p-1)$ by Lemma 2.5. In this case, there are at least

$$p^2(p-1)(p^{2(3n-5)} - |\mathcal{IA}_{n-1}(\mathbb{Z}_{p^2})|)$$

possibilities for A.

Case 2: $a_{nn} \notin \mathcal{U}(\mathbb{Z}_{p^2})$ and $a_{1n} \notin \mathcal{U}(\mathbb{Z}_{p^2})$. Then the elements in the last column are divisible by p. Let $B = [b_{ij}]$ be the matrix in $\mathcal{A}_n(\mathbb{Z}_{p^2})$ be defined by $b_{1n} = \frac{a_{1n}}{p}$,

$b_{nn} = \frac{a_{nn}}{p}$, and $b_{ij} = a_{ij}$ for all $i = 1, \ldots, n$ and $j = 1, \ldots, n-1$. Let $C = [c_{ij}]$ be the matrix in $\mathcal{A}_n(\mathbb{Z}_p)$ defined by $c_{ij} \equiv b_{ij} \pmod{p}$. We note that $\det(A) = p\det(B) \in \mathbb{Z}_{p^2}$. Then $\det(A) = 0 \in \mathbb{Z}_{p^2}$ if and only if $\det(B) \equiv 0 (\mathrm{mod}\ p)$ which is equivalent to $\det(C) = 0 \in \mathbb{Z}_p$. For each matrix $C \in \mathcal{A}_n(\mathbb{Z}_p, 0)$, there are p^{3n-4} corresponding matrices $B \in \mathcal{A}_n(\mathbb{Z}_{p^2}, 0)$. Since the number of possible matrices C is $|\mathcal{A}_n(\mathbb{Z}_p, 0)|$ and the matrix A is uniquely determined by B by multiplying the last column by p, A has $p^{3n-4}|\mathcal{A}_n(\mathbb{Z}_p, 0)|$ possibilities.

Summarizing the two cases above, it can be concluded that

$$\begin{aligned}|\mathcal{A}_n(\mathbb{Z}_{p^2}, 0)| \geq\ & p^5(p-1)|\mathcal{A}_{n-1}(\mathbb{Z}_{p^2}, 0)| + p^2(p-1)(p^{2(3n-5)} - |\mathcal{IA}_{n-1}(\mathbb{Z}_{p^2})|) \\ & + p^{3n-4}|\mathcal{A}_n(\mathbb{Z}_p, 0)|.\end{aligned}$$

From Theorem 4.1 and Corollary 3.5, we have

$$|\mathcal{IA}_{n-1}(\mathbb{Z}_{p^2})| = p^{5n-10}(p-1)^{n-1}(p + (n-2))$$

and

$$|\mathcal{A}_n(\mathbb{Z}_p, 0)| = p^{3n-2} - p^{2n-3}(p-1)^n(p + (n-1)).$$

A lower bound for $|\mathcal{A}_n(\mathbb{Z}_{p^2}, 0)|$ can be summarized in the following recursive form

$$\begin{aligned}|\mathcal{A}_n(\mathbb{Z}_{p^2}, 0)| \geq\ & p^5(p-1)|\mathcal{A}_{n-1}(\mathbb{Z}_{p^2}, 0)| + p^{6n-8}(p^2 + p - 1) \\ & - p^{5n-8}(p-1)^n(p^2 + (p+1)n - 2).\end{aligned}$$

This completes the proof. $\square$

The above recursive lower bound for $|\mathcal{A}_n(\mathbb{Z}_{p^2}, 0)|$ is key to determine an explicit lower bound in the next corollary.

Corollary 4.6. *Let p be a prime number. Then $|\mathcal{A}_n(\mathbb{Z}_{p^2},0)| = 1$ and*

$$|\mathcal{A}_n(\mathbb{Z}_{p^2},0)| \geq (p^5(p-1))^{n-1} + p^{5n-6}(p^2+p-1)\left(\sum_{i=0}^{n-2} p^i(p-1)^{n-i-2}\right) - p^{5n-8}(p-1)^n((n-1)p^2 + \frac{1}{2}(n^2+n-2)p + \frac{1}{2}(n^2-3n+2))$$

for all $n \geq 2$.

Proof. The statement will be proved by the mathematical induction. For $n = 2$, we have

$$\begin{aligned}|\mathcal{A}_2(\mathbb{Z}_{p^2},0)| \geq& p^5(p-1)|\mathcal{A}_1(\mathbb{Z}_{p^2},0)| + p^{6(2)-8}(p^2+p-1) \\ &- p^{5(2)-8}(p-1)^2(p^2+(p+1)(2)-2) \\ =& p^5(p-1) + p^4(p^2+p-1) - p^2(p-1)^2(p^2+2p) \\ =& (p^5(p-1))^{2-1} + p^{5(2)-6}(p^2+p-1)\left(\sum_{i=0}^{2-2} p^i(p-1)^{2-i-2}\right) \\ &- p^{5(2)-8}(p-1)^2((2-1)p^2 + \frac{1}{2}(2^2+2-2)p + \frac{1}{2}(2^2-3(2)+2))\end{aligned}$$

by Proposition 4.5.

Let $k \geq 3$ be an integer. Assume that

$$|\mathcal{A}_k(\mathbb{Z}_{p^2},0)| \geq (p^5(p-1))^{k-1} + p^{5k-6}(p^2+p-1)\left(\sum_{i=0}^{k-2} p^i(p-1)^{k-i-2}\right) - p^{5k-8}(p-1)^k((k-1)p^2 + \frac{1}{2}(k^2+k-2)p + \frac{1}{2}(k^2-3k+2)).$$

By Proposition 4.5 and the induction hypothesis, it can be deduced that

$$
\begin{aligned}
|\mathcal{A}_{k+1}(\mathbb{Z}_{p^2},0)| \geq\, & p^5(p-1)|\mathcal{A}_k(\mathbb{Z}_{p^2},0)| + p^{6(k+1)-8}(p^2+p-1) \\
& - p^{5(k+1)-8}(p-1)^{k+1}(p^2+(p+1)(k+1)-2) \\
\geq\, & p^5(p-1)((p^5(p-1))^{k-1} + p^{5k-6}(p^2+p-1)\left(\sum_{i=0}^{k-2} p^i(p-1)^{k-i-2}\right) \\
& - p^{5k-8}(p-1)^k((k-1)p^2 + \frac{1}{2}(k^2+k-2)p + \frac{1}{2}(k^2-3k+2))) \\
& + p^{6(k+1)-8}(p^2+p-1) \\
& - p^{5(k+1)-8}(p-1)^{k+1}(p^2+(k+1)p+(k+1-2)) \\
=\, & (p^5(p-1))^k + p^{5k-1}(p^2+p-1)(p-1)\left(\sum_{i=0}^{k-2} p^i(p-1)^{k-i-2}\right) \\
& - p^{5k-3}(p-1)^{k+1}((k-1)p^2 + \frac{1}{2}(k^2+k-2)p + \frac{1}{2}(k^2-3k+2)) \\
& + p^{6k-2}(p^2+p-1) - p^{5k-3}(p-1)^{k+1}(p^2+(k+1)p+(k+1-2)) \\
=\, & (p^5(p-1))^k + p^{5k-1}(p^2+p-1)((p-1)\left(\sum_{i=0}^{k-2} p^i(p-1)^{k-i-2}\right) + p^{k-1}) \\
& - p^{5k-3}(p-1)^{k+1}(((k-1)p^2 + \frac{1}{2}(k^2+k-2)p + \frac{1}{2}(k^2-3k+2)) \\
& + (p^2+(k+1)p+(k+1-2))) \\
=\, & (p^5(p-1))^k + p^{5k-1}(p^2+p-1)\left(\sum_{i=0}^{k-1} p^i(p-1)^{k-i-1}\right) \\
& - p^{5k-3}(p-1)^{k+1}((k)p^2 + \frac{1}{2}(k^2+3k)p + \frac{1}{2}(k^2-k)) \\
=\, & (p^5(p-1))^{(k+1)-1} + p^{5(k+1)-6}(p^2+p-1)\left(\sum_{i=0}^{(k+1)-2} p^i(p-1)^{(k+1)-i-2}\right) \\
& - p^{5(k+1)-8}(p-1)^{k+1}(((k+1)-1)p^2 + \frac{1}{2}((k+1)^2+(k+1)-2)p \\
& + \frac{1}{2}((k+1)^2-3(k+1)+2)).
\end{aligned}
$$

By the mathematical induction, it follows that

$$|\mathcal{A}_k(\mathbb{Z}_{p^2},0)| \geq (p^5(p-1))^{k-1} + p^{5k-6}(p^2+p-1)\left(\sum_{i=0}^{k-2} p^i(p-1)^{k-i-2}\right)$$
$$- p^{5k-8}(p-1)^k((k-1)p^2 + \frac{1}{2}(k^2+k-2)p + \frac{1}{2}(k^2-3k+2))$$

for all $n \geq 2$. □

Illustrative computation of lower bounds for $|\mathcal{A}_n(\mathbb{Z}_{p^2},0)|$ is presented in Table 4.2.

Table 4.2: Lower Bounds for $|\mathcal{A}_n(\mathbb{Z}_{p^2},0)|$

p	n	Lower Bounds for $\|\mathcal{A}_n(\mathbb{Z}_{p^2},0)\|$
2	3	$6,272$
2	4	$471,040$
2	5	$33,816,576$
3	3	$723,897$
3	4	$629,757,585$

4.2.2 Singular Arrowhead Matrices over $\mathbb{Z}_{p^2}$ with Non-Zero Determinant

In this subsection, an upper bound on the number of $n \times n$ singular arrowhead matrices over $\mathbb{Z}_{p^2}$ with a fixed non-zero determinant are presented.

The following proposition, a relation between $|\mathcal{A}_n(\mathbb{Z}_{p^2},p)|$ and $|\mathcal{A}_n(\mathbb{Z}_{p^2},b)|$ is given for all $b \in \mathcal{ZD}(\mathbb{Z}_{p^2})$. This relation is key to determine the upper bound for $|\mathcal{A}_n(\mathbb{Z}_{p^2},b)|$ in Corollary 4.8.

Proposition 4.7. *Let p be a prime number and let n be a positive integer. Then*

$$|\mathcal{A}_n(\mathbb{Z}_{p^2}, b)| = |\mathcal{A}_n(\mathbb{Z}_{p^2}, p)|$$

for all $b \in \mathcal{ZD}(\mathbb{Z}_{p^2})$.

Proof. Let $b \in \mathcal{ZD}(\mathbb{Z}_{p^2})$. Then $b = ap$ for some $1 \leq a < p$. Let $\psi : \mathcal{A}_n(\mathbb{Z}_{p^2}, p) \to \mathcal{A}_n(\mathbb{Z}_{p^2}, ap)$ be the function defined by

$$\psi(A) = \operatorname{diag}(a, 1, 1, \ldots, 1)A.$$

Let

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & 0 & 0 & \cdots & a_{nn} \end{pmatrix} \in \mathcal{A}_n(\mathbb{Z}_{p^2}, p).$$

Then $\det(A) = p$ and

$$\begin{aligned} \psi(A) &= \operatorname{diag}(a, 1, 1, \ldots, 1)A \\ &= \begin{pmatrix} aa_{11} & aa_{12} & aa_{13} & \cdots & aa_{1n} \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ a_{31} & 0 & a_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & 0 & 0 & \cdots & a_{nn} \end{pmatrix}. \end{aligned} \tag{4.2}$$

It follows that $\psi(A)$ is an $n \times n$ arrowhead matrix over $\mathbb{Z}_{p^2}$ and

$$\begin{aligned}\det(\psi(A)) &= \det(\mathrm{diag}(a,1,1,\ldots,1)A)\\ &= \det(\mathrm{diag}(a,1,1,\ldots,1)) \cdot \det(A)\\ &= a \cdot p\\ &= ap.\end{aligned}$$

Hence, $\psi(A) \in \mathcal{A}_n(\mathbb{Z}_{p^2}, ap)$.

Let $A, B \in \mathcal{A}_n(\mathbb{Z}_{p^2}, p)$ be such that $\psi(A) = \psi(B)$. Then

$$\mathrm{diag}(a,1,1,\ldots,1)A = \mathrm{diag}(a,1,1,\ldots,1)B.$$

Since $\mathrm{diag}(a,1,1,\ldots,1)$ is invertible, we have $A = B$. Hence, ψ is injective.

Let $X \in \mathcal{A}_n(\mathbb{Z}_{p^2}, ap)$. Then $\det(X) = ap$. Since a is a unit, $\mathrm{diag}(a^{-1},1,1,\ldots,1)$ is the inverse of $\mathrm{diag}(a,1,1,\ldots,1)$. Let $A = \mathrm{diag}(a^{-1},1,1,\ldots,1)X$. Using the argument similar to that of (4.2), $A \in \mathcal{A}_n(\mathbb{Z}_{p^2})$ and

$$\det(A) = \det(\mathrm{diag}(a^{-1},1,1,\ldots,1)X) = a^{-1} \cdot ap = p.$$

It follows that $A \in \mathcal{A}_n(\mathbb{Z}_{p^2}, p)$ and

$$\psi(A) = \psi(\mathrm{diag}(a^{-1},1,1,\ldots,1)X) = \mathrm{diag}(a,1,1,\ldots,1)\mathrm{diag}(a^{-1},1,1,\ldots,1)X = X.$$

Hence, ψ is surjective.

All together, it can be concluded that ψ is a bijection from $\mathcal{A}_n(\mathbb{Z}_{p^2}, p)$ onto $\mathcal{A}_n(\mathbb{Z}_{p^2}, ap)$. Therefore, $|\mathcal{A}_n(\mathbb{Z}_{p^2}, p)| = |\mathcal{A}_n(\mathbb{Z}_{p^2}, b)|$ as desired. $\square$

An upper bound for $n \times n$ singular arrowhead matrices over $\mathbb{Z}_{p^2}$ with non-zero determinant is shown in the next corollary.

Corollary 4.8. *Let p be a prime number and let n be a positive integer. Then*

$$
\begin{aligned}
|\mathcal{A}_n(\mathbb{Z}_{p^2}, b)| \leq & \frac{p^{6n-4}}{p-1} - p^{5n-5}(p-1)^{n-1}(p+(n-1)) \\
& - \frac{(p^5(p-1))^{n-1}}{p-1} + \frac{p^{5n-6}(p^2+p-1)}{p-1}\left(\sum_{i=0}^{n-2} p^i(p-1)^{n-i-2}\right) \\
& - p^{5n-8}(p-1)^{n-1}((n-1)p^2 + \frac{1}{2}(n^2+n-2)p + \frac{1}{2}(n^2-3n+2))
\end{aligned}
$$

for all $b \in \mathcal{ZD}(\mathbb{Z}_{p^2})$.

Proof. Let $\mathcal{ZDA}_n(\mathbb{Z}_{p^2})$ denote the set of $n \times n$ singular arrowhead matrices over $\mathbb{Z}_{p^2}$ with non-zero determinant. We note that $\mathcal{ZDA}_n(\mathbb{Z}_{p^2})$ is disjoint union of $\mathcal{A}_n(\mathbb{Z}_{p^2}, b)$ for all $b \in \mathcal{ZD}(\mathbb{Z}_{p^2})$. Precisely,

$$\mathcal{ZDA}_n(\mathbb{Z}_{p^2}) = \bigcup_{b \in \mathcal{ZD}(\mathbb{Z}_{p^2})} \mathcal{A}_n(\mathbb{Z}_{p^2}, b)$$

which is a disjoint union. By Proposition 4.7, $\mathcal{A}_n(\mathbb{Z}_{p^2}, b)$ and $\mathcal{A}_n(\mathbb{Z}_{p^2}, p)$ have the same cardinality, and hence,

$$
\begin{aligned}
|\mathcal{ZDA}_n(\mathbb{Z}_{p^2})| &= \left| \bigcup_{b \in \mathcal{U}(\mathbb{Z}_{p^2})} \mathcal{A}_n(\mathbb{Z}_{p^2}, b) \right| \\
&= \sum_{b \in \mathcal{U}(\mathbb{Z}_{p^2})} |\mathcal{A}_n(\mathbb{Z}_{p^2}, b)| \\
&= \sum_{b \in \mathcal{U}(\mathbb{Z}_{p^2})} |\mathcal{A}_n(\mathbb{Z}_{p^2}, p)| \\
&= |\mathcal{ZD}(\mathbb{Z}_{p^2})||\mathcal{A}_n(\mathbb{Z}_{p^2}, p)|.
\end{aligned}
$$

From Lemma 2.5, we have $|\mathcal{ZD}(\mathbb{Z}_{p^2})| = p - 1$. By Corollary 4.2, Proposition 4.5, and Proposition 4.7, it can be concluded that

$$
\begin{aligned}
|\mathcal{A}_n(\mathbb{Z}_{p^2}, b)| &= |\mathcal{A}_n(\mathbb{Z}_{p^2}, p)| \\
&= \frac{|\mathcal{ZDA}_n(\mathbb{Z}_{p^2})|}{|\mathcal{ZD}(\mathbb{Z}_{p^2})|} \\
&= \frac{|\mathcal{A}_n(\mathbb{Z}_{p^2})| - |\mathcal{IA}_n(\mathbb{Z}_{p^2})| - |\mathcal{A}_n(\mathbb{Z}_{p^2}, 0)|}{p-1} \\
&\leq \frac{p^{6n-4}}{p-1} - p^{5n-5}(p-1)^{n-1}(p+(n-1)) \\
&\quad - \frac{(p^5(p-1))^{n-1}}{p-1} + \frac{p^{5n-6}(p^2+p-1)}{p-1}\left(\sum_{i=0}^{n-2} p^i(p-1)^{n-i-2}\right) \\
&\quad - p^{5n-8}(p-1)^{n-1}((n-1)p^2 + \frac{1}{2}(n^2+n-2)p + \frac{1}{2}(n^2-3n+2)).
\end{aligned}
$$

The proof is completed. $\square$

Illustrative computation of upper bounds for $|\mathcal{A}_n(\mathbb{Z}_{p^2}, b)|$ is presented, where $b \in \mathcal{ZD}(\mathbb{Z}_{p^2})$, in Table 4.3.

Table 4.3: Upper Bounds for $|\mathcal{A}_n(\mathbb{Z}_{p^2}, b)|$, where $b \in \mathcal{ZD}(\mathbb{Z}_{p^2})$

p	n	Upper Bounds for $\lvert\mathcal{A}_n(\mathbb{Z}_{p^2}, b)\rvert$
2	3	6,016
2	4	413,696
2	5	27,000,832
2	6	1,719,664,640
3	3	848,556
3	4	739,765,872

Chapter 5

Conclusion and Remarks

In this thesis, the enumeration of arrowhead matrices with prescribed determinant over $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$ has been studied. The number of $n \times n$ non-singular (resp., singular) arrowhead matrices over $\mathbb{Z}_p$ has been determined together with the number of $n \times n$ arrowhead matrices over $\mathbb{Z}_p$ whose determinant is a for all positive integers n and $a \in \mathbb{Z}_p$. Subsequently, the enumeration of $n \times n$ non-singular (resp., singular) arrowhead matrices over $\mathbb{Z}_{p^2}$ has been given. The number of $n \times n$ non-singular arrowhead matrices over $\mathbb{Z}_{p^2}$ whose determinant is a has been determined for all positive integers n and for all $a \in \mathcal{U}(\mathbb{Z}_{p^2})$. For $n \times n$ singular arrowhead matrices over $\mathbb{Z}_{p^2}$, bounds on the number of $n \times n$ singular arrowhead matrices have been presented. An upper bound for the number of $n \times n$ singular arrowhead matrices over $\mathbb{Z}_{p^2}$ with zero determinant has been derived as well as a lower bound for the number of $n \times n$ singular arrowhead matrices over $\mathbb{Z}_{p^2}$ with a zero-divisor determinant.

It is interesting to studied the $n \times n$ arrowhead matrices over $\mathbb{Z}_{p^2}$ whose determinant is a zero-divisor in $\mathbb{Z}_{p^2}$. In general, the study of $n \times n$ arrowhead matrices with prescribed determinant over other rings is another interesting problem.

References

[1] Brent, R. P., McKay, B. D.: Determinants and ranks of random matrices over $\mathbb{Z}_m$, *Discrete Mathematics* **66**, 35–49 (1987).

[2] Cheney, W., Kincaid, D. R.: *Linear Algebra Theory and Applications 2nd edition*, Jones and Bartlett Publishers, (2010).

[3] Choosuwan, P., Jitman, S., Udomkavanich, P.: Determinants of matrices over commutative finite principal ideal rings, *Finite Fields and Their Applications* **48**, 126–140 (2017).

[4] Jitman, S.: Determinants of some special matrices over commutative finite chain rings, *Special Matrices* **8**, 242–256 (2020).

[5] Jitman, S., Dukdokjan, K., Wongwilai, C.: On the solutions of some equations over rings of integers modulo the square of a prime. *Bruce Landman*, (2021).

[6] Klain, D. A.: An intuitive derivation of Heron's formula, *The American Mathematical Monthly* **111**, 709–712 (2004).

[7] Kuttler, K.: *A First Course in Linear Algebra*, Lyryx Learning, (2017).

[8] Lockhart, J.M., Wardlaw, W.P.: Determinants of matrices over the integers modulo m, *Mathematics Magazine* **80**, 207–214 (2007).

[9] Lota, D.S., Szweda, M., Trawinski, T.: Determinants of the block arrowhead matrices, *Selected Problems on Experimental Mathematics*, 73–88 (2017).

[10] Lovsz, L.: Singular spaces of matrices and their application in combinatorics, *Bulletin Brazilian Mathematical Society* **20**, 87–99 (1989).

[11] Marrero, J. A., Tomeo, V.: Infinite invertible arrowhead matrices and applications, In: The Proceedings of the 15th International Conference on Computational and Mathematical Methods in Science and Engineering (CMMSE 2015), 2–11 (2015).

[12] Meemark, Y.: *Abstract Algebra*, Danex Intercorporation Company Limited, (2015).

[13] Mukhopadhyay, A.: On the probability that the determinant of an $n \times n$ matrix over a finite field vanishes, *Discrete Mathematics* **51**, 311–315 (1984).

[14] Stor, N. J., Slapničar, I., Barlow, J. L.: Accurate eigenvalue decomposition of arrowhead matrices and applications. *Linear Algebra and its Applications* **464**, 62–89 (2015).

Biography

Name	Miss Pornrudee Modjam
Address	6 Village No. 10, Kungpayom Sub-district, Banpong District, Ratchaburi, 70110
Date of Birth	December 19, 1996
Education	
2018	Bachelor of Science in Mathematics, (First Class Honors), Slipakorn University
2021	Master of Science in Mathematics, Slipakorn University