View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Montclair State University Digital Commons

Montclair State University
Montclair State University Digital Commons

Theses, Dissertations and Culminating Projects

5-2018

Magic Squares of Squares of Order Three Over Finite Fields

Giancarlo Labruna
Montclair State University

Follow this and additional works at: https://digitalcommons.montclair.edu/etd

 Part of the Mathematics Commons

Recommended Citation

Labruna, Giancarlo, "Magic Squares of Squares of Order Three Over Finite Fields" (2018). *Theses, Dissertations and Culminating Projects*. 138.
https://digitalcommons.montclair.edu/etd/138

This Thesis is brought to you for free and open access by Montclair State University Digital Commons. It has been accepted for inclusion in Theses, Dissertations and Culminating Projects by an authorized administrator of Montclair State University Digital Commons. For more information, please contact digitalcommons@montclair.edu.

Abstract

A magic square M over an integral domain $\mathbf{D}$ is a 3×3 matrix with entries from $\mathbf{D}$ such that the elements from each row, column, and diagonal add to the same sum. If all the entries in M are perfect squares in $\mathbf{D}$, we call M a magic square of squares over $\mathbf{D}$. Martin LaBar raised an open question in 1984, which states, "Is there a magic square of squares over the ring $\mathbb{Z}$ of the integers which has all the nine entries distinct?" We approach to answering a similar question in case $\mathbf{D}$ is a finite field. Our main result confirms that a magic square of squares over a finite field $\mathbf{F}$ of characteristic greater than 3 can only hold 3, 5, 7, or 9 distinct entries. Corresponding to LaBar's question, we claim that there are infinitely many prime numbers p such that, over a finite field of characteristic p, magic squares of squares with nine distinct elements exist. Constructively, we build magic squares of squares using consecutive quadratic residue triples derived from twin primes. We classify all the magic squares of squares over any finite fields of characteristic 2. Description of magic squares over a finite field of characteristic 3 is provided.

MONTCLAIR STATE UNIVERSITY

Magic Squares of Squares of Order Three over Finite Fields

by

Giancarlo Labruna

A Master's Thesis Submitted to the Faculty of

Montclair State University

In Partial Fulfillment of the Requirements

For the Degree of

Master's in Mathematics

May 2018

College of Science and Mathematics

Department of Mathematical Sciences

Thesis Committee:

[redacted]

Dr. Aihua Li

Thesis Sponsor

[redacted]

Dr. Deepak Bal

Committee Member

[redacted]

Dr. Jonathan Cutler

Committee Member

MAGIC SQUARES OF SQUARES OF ORDER THREE OVER FINITE FIELDS

A THESIS

Submitted in partial fulfillment of the requirements

for the degree of Master's in Mathematics

by

Giancarlo Labruna

Montclair State University

Montclair, NJ

May 2018

Copyright © 2018 by *Giancarlo Labruna*. All rights reserved.

Acknowledgments

First, I would like to thank Dr. Aihua Li for her role as advisor for three years. Without her guidance, patience, support, and dedication, this thesis could not have been made possible. Also, I would like to thank Drs. Deepak Bal and Jonathan Cutler for their time and roles as committee members for my thesis. I would like to thank my family for supporting me in getting a graduate degree. Last (but certainly not least), I would like to thank all of my Montclair State University friends, who usually sit in the "fishbowl", for their support as we all have gone through a lot of time preparing our theses.

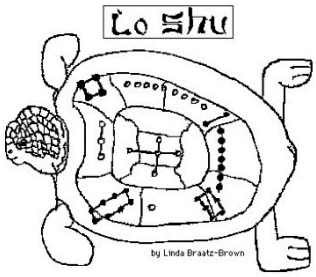
Contents

Chapter 1

Introduction

1.1 History and Background

A magic square is an $n \times n$ array such that each of its rows, columns, and the two diagonals have the same sum. As early as 2800 B.C., Chinese literature demonstrated how the first magic square, the Chinese Lo Shu, made its first appearance (*Lo-Shu Magic Square*). In ancient China, there was a huge flood. People tried to make sacrifices for the river god to stop the flooding. However, nothing had worked until a turtle emerged from the river. A child noticed that a grid with dots on the turtle's shell followed a pattern: each of the rows, columns, and the diagonals of the grid added to 15. People believed that 15 is the number of sacrifices they had to make for the river god to stop the flooding. The representation is shown in the figure below. Since it was first discovered, magic squares and their properties have been studied for centuries.



4	9	2
3	5	7
8	1	6

Figure 1.1: Graphical Representation of Lo Shu.

Magic squares eventually reached other places in the world such as India, Arabia, and in medieval Europe. In places like Egypt and India, magic squares can be engraved on materials such as stone or metal and were worn as talismans (*Lo Shu Magic Square*). Magic squares of order at least 3 were devoted to the planets, moon, and the sun in talismans (*Lo Shu Magic Square*). These magic squares were placed in polygons and then the polygons were placed within a circle that would be inscribed with signs of the zodiac. People also believed that magic squares provided longevity and prevented diseases. In the 9^{th} century, they were used to decipher horoscopes by Arabian astrologers (*Lo Shu Magic Square*). For a long period of time, magic squares have evolved to become a special interest for many cultures.

We focus on a special type of 3×3 magic squares. These magic squares are called *magic squares of squares*. They are magic squares but each of their entries is a perfect square of an integer. Martin LaBar in 1984 proposed a question, which is still open today. He asked, "Does there exist a 3×3 magic square such that the nine integers are distinct perfect squares of integers?" (LaBar 69). In 1996, Martin Gardner offered $100 for anyone who can determine whether such a magic square exists (Bremner 289). LaBar's question is the motivation for this thesis. We investigate whether a magic square of squares over a finite field with nine distinct elements exists. If not, we find the maximal number of distinct square entries that a magic square of squares can possess.

1.2 Basic Number Theory Results

In this section, we give some existing results from number theory that are important for this thesis. They can be found in any regular number theory book. We first define a quadratic residue.

Definition 1. (Rosen 402) Let p be a prime number. An integer a is a *quadratic residue modulo* p if $a \equiv b^2 \pmod{p}$ for some integer b. If a is not a quadratic residue (mod p), it is called a *quadratic nonresidue* (mod p).

We now provide the definition for the Legendre symbol which is useful in determining whether an integer is a quadratic residue modulo a prime number p.

Definition 2. (Legendre symbol) (Lehmer 172) For any prime p, the *Legendre symbol* of an integer $x \pmod{p}$ is given by

$$\left(\frac{x}{p}\right) = \begin{cases} 0, & \text{if } p \text{ divides } x \\ 1, & \text{if } x \text{ is a quadratic residue modulo } p \text{ and } p \nmid x \\ -1, & \text{if } x \text{ is a quadratic nonresidue modulo } p \text{ and } p \nmid x \end{cases}. \tag{1.1}$$

Note that the Legendre symbol can be used to test whether an integer is a quadratic residue (for this thesis, we use the Legendre symbol to determine whether an integer is a quadratic residue in a field $\mathbf{F}$). This test is needed during the construction of magic squares of squares over a finite field.

Theorem 3. *(Quadratic Reciprocity) (Hoffstein et al. 168) Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ -\left(\frac{q}{p}\right), & \text{if } p \equiv 3 \pmod{4} \text{ and } q \equiv 3 \pmod{4} \end{cases}. \tag{1.2}$$

Some useful properties of the Legendre symbol are given in the next theorem.

Theorem 4. *Let p be an odd prime and $a, b \in \mathbb{Z}$. Then*

1. *If* $a \equiv b \pmod{p}$, *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

In the later construction of magic squares of squares over a finite field, we frequently need two numbers, -1 and 2, to be quadratic residue modulo a prime number p. The following lemma gives a test for -1 or 2 to be quadratic residue modulo a prime number.

Lemma 5. Let p be an odd prime number. Then -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod{4}$ and 2 is a quadratic residue if and only if $p \equiv 1$ or $7 \pmod{8}$.

The well-known Dirichlet's Theorem guarantees the existence of infinitely many of primes of special types. It made it possible for us to construct many magic squares of squares over infinitely many finite fields.

Theorem 6. *(Dirichlet's Theorem) If* a *and* b *are relatively prime positive integers, then there are infinitely many primes* p *of the form* $aq + b$ *where* q *is an integer.*

Results involving Legendre symbol are very useful for our investigation. We can also apply the Legendre symbol to test if an element of $\mathbf{F}$ is indeed a quadratic residue. Another useful result is Fermat's Little Theorem.

Theorem 7. *(Fermat's Little Theorem) Let* p *be a prime number and* a *be an integer. If* $a \not\equiv 0 \pmod{p}$, *then* $a^{p-1} \equiv 1 \pmod{p}$.

The following proposition gives a method to determine if an element in a finite field is a quadratic residue or not.

Proposition 8. *(Gazali et al. 202) Let* p *be an odd prime and* $q = p^n$, *where* n *is a positive integer. Assume* $\mathbf{F}$ *is the finite field with* q *elements and* $0 \neq a \in \mathbf{F}_q$. *Then,* a *is a quadratic residue in* $\mathbf{F}$ *if and only if* $a^{\frac{q-1}{2}} = 1$.

In the next section, we provide some existing results on magic squares.

1.3 Definitions and Existing Results

To start off this section, we give some formal definitions about magic squares.

Definition 9. A *magic square (MS) of order 3* is a 3×3 matrix M with integer entries such that all of its rows, columns, and the two diagonals add to the same sum. This common sum is called the *magic sum of* M and it satisfies the following:

$$S(M) = \sum_{i=1}^{3} a_{ij} = \sum_{j=1}^{3} a_{ij} = a_{11} + a_{22} + a_{33} = a_{13} + a_{22} + a_{31}, \ \forall \ i, j \in \{1, 2, 3\}.$$

The *degree of* M, denoted $\deg(M)$, is the number of distinct entries M possesses and M is said to be *trivial* if $\deg(M) = 1$. Also, a magic square M is a *magic square of squares (MSS)* if all of its entries are perfect squares.

We now give an example of a magic square.

Example 1. In Figure 1.1, the pattern of the dots on the back of the turtle form a small magic square and the degree of this magic square is 9 because the numbers of the dots in each box are distinct. Also, the magic sum is 15. The matrix representation of the magic square is

$$\begin{bmatrix} 4 & 9 & 2 \\ 3 & 5 & 7 \\ 8 & 1 & 6 \end{bmatrix}.$$

Definition 10. A magic square M is *isomorphic* to another MS N ($M \cong N$) if one can be obtained by rotations or reflections of the square along the center vertical or horizontal axis or the diagonals.

The following example shows two magic squares which are isomorphic to each other.

Example 2. The two magic squares M and N are isomorphic to each other:

$$M = \begin{bmatrix} 4 & 9 & 2 \\ 3 & 5 & 7 \\ 8 & 1 & 6 \end{bmatrix} \quad \cong \quad \begin{bmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{bmatrix} = N.$$

We generalize the concept of magic squares of integers into that over any finite field.

Definition 11. Let $\mathbf{F}$ be a finite field. A magic square (MS) $M = [a_{ij}]_{3\times 3}$ with $a_{ij} \in \mathbf{F}$ is called an *MS over* $\mathbf{F}$ provided that each of its rows, columns, and main diagonals have the same sum. Furthermore, M is an *MSS over* $\mathbf{F}$ if all of its entries are perfect squares in $\mathbf{F}$. The degree of M, $\deg(M)$ is defined in the same way as in the integer case.

We investigate MSS over finite fields of some characteristic. We define this in the next definition.

Definition 12. The *characteristic* of a finite field $\mathbf{F}$ is the smallest positive integer p such that $p \cdot 1_F = 0_F$.

For example, $\mathbb{Z}_5$ is a finite field of characteristic 5. A magic squares of squares over $\mathbb{Z}_5$ is given below.

Example 3. The following matrix is an MSS of degree 3 over the field $\mathbb{Z}_5$ with magic sum 0:

$$M = \begin{bmatrix} 1 & 4 & 0 \\ 4 & 0 & 1 \\ 0 & 1 & 4 \end{bmatrix}.$$

Note that all three entries of M are squares in $\mathbb{Z}_5$. These are all of the squares in $\mathbb{Z}_5$. Consequently, the degree of every MSS over $\mathbb{Z}_5$ is at most three and all the three squares have to be used.

In order for an MS to be an MSS over a field $\mathbf{F}$, we need to determine if each of the entries of it is a quadratic residue in $\mathbf{F}$, defined in Definition 1. If so, we can

say that this MS is indeed an MSS. The following lemma provides a configuration for all 3×3 magic squares over a field.

Lemma 13. (Sallows, 1997) Let $M = [a_{ij}]_{3\times 3}$ be a matrix with integer entries. Then M is a magic square if and only if M is a function of three integers a, b, c with the following form:

$$M = M(a,b,c) = \begin{bmatrix} a & 3c-a-b & b \\ c-a+b & c & c+a-b \\ 2c-b & a+b-c & 2c-a \end{bmatrix}. \tag{1.3}$$

Furthermore, the magic sum must be $S(M) = 3c$.

It is straightforward to check that the above result is true for any magic square over a finite field $\mathbf{F}$. Magic squares are interesting to many people for various reasons. It is the open question by Martin LaBar that motivated the start of this project. The unsolved question is given below.

Open Question. (LaBar 69) Does there exists a 3×3 magic square such that all of its entries are perfect squares of integers?

Throughout, our magic squares are all of order 3. In this thesis, we attempt to answer a similar question over finite fields. Below we give a theorem pertaining what degrees can be achieved by a magic square over $\mathbb{Z}_p$.

Theorem 14. *(Hengeveld and Li, 2012) Let p be a prime at least 5. Then the degree of every MS over $\mathbb{Z}_p$ is odd.*

In this thesis, we attempt to show that the above Theorem 14 is true over for any finite field of characteristic greater than or equal to five. That is, over any finite field $\mathbf{F}$ of characteristic $p \geq 5$, the degree of every MSS over $\mathbf{F}$ is odd. In this thesis, we study magic squares of squares of order three whose entries are selected from a finite field. In the next section, we raise research questions for this thesis.

1.4 Research Questions

The main focus of this thesis is to attempt to answer a similar question as the one raised by Martin LaBar regarding the existence of a degree 9 MSS over the integers. Corresponding to LaBar's question for magic squares of squares over the integers, we raise similar questions for magic squares of squares over any finite field. Specifically, "does there exists a magic square of squares of degree 9 over a given finite field?". Let $\mathbf{F}$ be a finite field:

Research Questions.

1. Does there exist a MSS over $\mathbf{F}$ of degree 9?
2. Given an integer r with $2 \leq r \leq 9$, for what finite field $\mathbf{F}$ does there exist an MSS of degree r over $\mathbf{F}$?
3. For a given prime number p, what is the maximal degree that an MSS over a finite field $\mathbf{F}$ of characteristic p can achieve?
4. Can we get an MSS of even degree?

The answer to question 4 parallels the result in Theorem 14. The above questions are what we attempt to answer in this thesis.

1.5 Overview of Main Results

Instead of attempting LaBar's open question for MSS over the integers, we focus on a similar question for finite fields. We first characterize all MSSs over any field of characteristic 2. We show that a magic square of squares of degree 4 exists which does not happen for MSS over the integers. Work is done over finite fields of characteristic 3. In the characteristic 3 case, we show that the degree of any non-trivial MS must be 3 or 9 and both types are achievable over any finite field of characteristic 3.

Chapter 4 focuses on MSS over finite fields of characteristic greater than three.

In this chapter, we generalize the result given by Hengeveld and Li in Theorem 14 over finite fields.

The main results show that there are infinitely many finite fields of characteristic greater than 3 over which MSS of full degree exists. The same is true for MSS of degree 3, 5, or 7. Precisely, we construct magic squares of squares of degree 3, 5, 7, or 9 over infinitely many finite fields. The main technique used is based on Dirichlet's Theorem. A study on consecutive quadratic residue triples is performed which helps the construction of MSS over certain finite fields in a different way.

Chapter 2

MSS over Finite Fields of Characteristic 2 or 3

2.1 Case of Characteristic 2

In this part of the thesis, we first give results about the existence of magic squares of squares and their degrees over a finite field $\mathbf{F}$ with characteristic 2. We start the section with a lemma.

Lemma 15. Let $\mathbf{F}$ be any finite field of characteristic 2. Then every element in $\mathbf{F}$ is a quadratic residue in $\mathbf{F}$.

Proof. Assume the order of $\mathbf{F}$ is 2^n, where n is a positive integer. The group $\mathbf{F} \setminus \{0\}$ is of order $2^n - 1$. So for every $x \in \mathbf{F}$,

$$x^{2^n-1} = 1 \Longrightarrow x = x^{2^n} = \left(x^{2^{n-1}}\right)^2.$$

Thus x is a quadratic residue in $\mathbf{F}$. ■

From the above lemma, we know that all MS over a finite field of characteristic 2 are also MSS.

Example 4. Consider $\mathbf{F} = \mathbb{Z}_2[x]/(x^3 + x + 1) \cong GF(2^3)$, the Galois field of 8 elements. Note that in $\mathbf{F}$, $x^3 = x + 1$ and $x^4 = x^2 + x$. The eight elements in $\mathbf{F}$

are $0, 1, x, x+1, x^2, x^2+1, x^2+x$, and x^2+x+1. The following table shows all of these eight elements are squares of some elements in $\mathbf{F}$.

a	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
a^2	0	1	x^2	x^2+1	x^2+x	x^2+x+1	x	$x+1$

This example confirms Lemma 15.

We can classify all MSS over a finite field of characteristic 2.

Theorem 16. *Let $\mathbf{F}$ be a finite field of characteristic 2 with 2^n elements ($n \geq 1$) and $a, b, c \in \mathbf{F}$. Then*

1. *If $n = 1$ ($\mathbf{F} = \mathbb{Z}_2$), all the non-trivial MSS are of degree 2 which are listed below:*

$$M(0,1,0) = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \quad M(0,0,1) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix},$$

$$M(1,0,1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \text{ and } \quad M(1,1,0) = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

2. *For $n > 1$ ($|\mathbf{F}| \geq 4$), every non-trivial MSS over $\mathbf{F}$ has degree 2 or 4 and is in one of the following forms:*

$$M(a,b,a) = \begin{bmatrix} a & b & b \\ b & a & b \\ b & b & a \end{bmatrix}, \quad M(a,a,c) = \begin{bmatrix} a & c & a \\ c & c & c \\ a & c & a \end{bmatrix}, \text{ or}$$

$$M(a,b,c) = \begin{bmatrix} a & a+b+c & b \\ a+b+c & c & a+b+c \\ b & a+b+c & a \end{bmatrix},$$

where $a, b, c \in \mathbf{F}$. Furthermore, $M(a, b, c)$ is of degree 4 if and only if a, b, and c are all distinct.

Proof. Let $\mathbf{F}$ be a finite field of characteristic 2. The general form of an MS over $\mathbf{F}$ is

$$M(a,b,c) = \begin{bmatrix} a & a+b+c & b \\ a+b+c & c & a+b+c \\ b & a+b+c & a \end{bmatrix}, \tag{2.1}$$

where $a, b, c \in \mathbf{F}$. Note that $\deg(M(a, b, c)) \leq 4$. To show what possible degrees we can obtain for $M(a, b, c)$, we consider all the possible cases:

Case 1. If $a = c \neq b$, then

$$M(a,b,a) = \begin{bmatrix} a & 2a+b & b \\ b & a & 2a+b \\ 2a+b & b & a \end{bmatrix} = \begin{bmatrix} a & b & b \\ b & a & b \\ b & b & a \end{bmatrix}.$$

Since $a \neq b$, $\deg(M(a, b, a)) = 2$.

Case 2. In the case of $a = b \neq c$,

$$M(a,a,c) = \begin{bmatrix} a & 2a+c & a \\ c & c & c \\ a & 2a+c & a \end{bmatrix} = \begin{bmatrix} a & c & a \\ c & c & c \\ a & c & a \end{bmatrix}.$$

Since $a \neq c$, $\deg(M(a, a, c)) = 2$.

Case 3. If a, b, and c are all distinct, then $\deg(M(a, b, c)) = 4$. This is because $a+b+c \neq a, b$, or c. Without loss of generality, let $a+b+c = a$. Then $b+c = 0$ which implies that $b = -c = c$. By the form in (2.1), $\deg(M(a, b, c)) \leq 4$. Thus, $\deg(M(a, b, c)) = 4$.

The above analysis covers all possible cases for $M(a, b, c)$ over $\mathbf{F}$ of characteristic 2. Thus, every non-trivial MSS over $\mathbf{F}$ has degree 2 or 4. ■

The above theorem shows us what kinds of MSSs we can get over a finite field of characteristic 2. It is obvious that the different forms of the MSSs given in the above theorem are non-isomorphic. It is also interesting to see that we obtained an MSS of degree 4 over a finite field of characteristic 2. Among the magic squares over the integers or any finite field of characteristic greater than 2, no one is of degree 4. Thus it is a unique situation here.

Now, we claim a corollary to Theorem 16.

Corollary 17. Let $\mathbf{F}$ be a field of characteristic 2 with at least 4 elements. Then for every $x \in \mathbf{F}$, there exists an MSS of degree 4 over $\mathbf{F}$ with the magic sum x.

Proof. We consider the following cases:

Case 1. When $x = 0$, take $a \in \mathbf{F}$ with $a \neq 0, 1$. We construct the MS $M(1, a+1, x) = M(1, a+1, 0)$ as follows:

$$M(1, a+1, 0) = \begin{bmatrix} 1 & a & a+1 \\ a & 0 & a \\ a+1 & a & 1 \end{bmatrix}.$$

From the above, $M(1, a+1, 0)$ is an MSS of degree 4 with magic sum 0.

Case 2. When $x = 1$, take $a \in \mathbf{F}$ with $a \neq 0, 1$. An MSS $M(0, a+1, 1)$ is given by the following:

$$M(0, a+1, 1) = \begin{bmatrix} 0 & a & a+1 \\ a & 1 & a \\ a+1 & a & 0 \end{bmatrix}.$$

We see from the above that $M(0, a+1, 1)$ is an MSS of degree 4 with magic sum 1.

Case 3. If $x \neq 0, 1$, then

$$M(1,0,x) = \begin{bmatrix} 1 & x+1 & 0 \\ x+1 & x & x+1 \\ 0 & x+1 & 1 \end{bmatrix}$$

is an MSS of degree 4 with magic sum x.

We have considered all the elements $x \in \mathbf{F}$ and have constructed a magic square of squares of degree 4 over $\mathbf{F}$ having the magic sum x. ■

2.2 Case of Characteristic 3

Throughout this section, all the considered finite fields are of characteristic 3. We give a closer look at what types of MSS we can achieve over a finite field of characteristic 3, denoted by $\mathbf{F}$.

Lemma 18. Let $a, b, c \in \mathbf{F}$. If $a + b + c = 0$, then $a + b = 2c$, $b + c = 2a$, and $a + c = 2b$. On the other hand, if $a + b = 2c$ or $b + c = 2a$ or $a + c = 2b$, then $a + b + c = 0$.

Proof. Recall that we are doing modulo 3 arithmetic. Assume $a+b+c = 0$. Then $a + b = -c = 2c$. Similarly, $a + c = 2b$ and $b + c = 2a$. The proof of the rest is similar. ■

We present the following existing result. It states that 2 can be a quadratic residue in some finite field of characteristic 3.

Lemma 19. (Lahtonen, 2016) Over the finite field $\mathbf{F}$ of order 3^n where n is a positive integer, 2 is a quadratic residue in $\mathbf{F}$ if and only if n is even.

In the following theorem, we show that every non-trivial MS over $\mathbf{F}$ is of odd degree.

Theorem 20. *Let* $\mathbf{F}$ *be a finite field of characteristic 3. Then the magic sum of any MS over* $\mathbf{F}$ *must be* 0. *Every non-trivial MS over* $\mathbf{F}$ *is of degree* 3 *or* 9 *and there exists an MSS of degree 3 if 2 is a quadratic residue of* $\mathbf{F}$.

Proof. Since the characteristic of $\mathbf{F}$ is 3 and the magic sum of any MS is three times the middle entry, the magic sum of M over $\mathbf{F}$ must be 0. It reduces the general form $M = M(a, b, c)$ for MS over $\mathbf{F}$ defined in Lemma 13 into the following form:

$$M(a,b,c) = \begin{bmatrix} a & 2(a+b) & b \\ c+2a+b & c & c+a+2b \\ 2(b+c) & a+b+2c & 2(a+c) \end{bmatrix}.$$

Note that the full degree of an MS is 9 but it is possible over $\mathbf{F}$ there is no MS of degree 9. This occurs especially when $\mathbf{F}$ has less than 9 quadratic residues. We consider the following cases: For every $a, b, c \in \mathbf{F}$,

1. If $a = b \neq c$, then

$$M(a,a,c) = \begin{bmatrix} a & a & a \\ c & c & c \\ 2(a+c) & 2(a+c) & 2(a+c) \end{bmatrix}.$$

   Without loss of generality, if $2(a+c) = a$ then $2a+2c = a$ which is the same as $a = c$, a contradiction. Similarly, if $2(a+c) = c$ we would eventually get $a = c$. Thus, $\deg(M(a,a,c)) = 3$.

2. If $a = c \neq b$, then

$$M(a,b,a) = \begin{bmatrix} a & 2(a+b) & b \\ b & a & 2(a+b) \\ 2(a+b) & b & a \end{bmatrix}.$$

If a, b, and $2(a+b)$ are distinct, then $\deg(M(a,b,b)) = 3$. Assume $2(a+b) = a$. Then $2(a+b) = 2a+2b = a$ which is the same as $a = b$, a contradiction. Also, if $2(a+b) = b$ then $2(a+b) = 2a+2b = b$ which gives us $a = b$. Hence, $\deg(M(a,b,b)) = 3$.

3. If a, b, and c are all distinct, then $\deg(M(a,b,c)) \geq 3$ and one of the following cases will occur:

   Case 1. If $a+b+c = 0$, then by Lemma 18, $2c = a+b$, $2a = b+c$, and $2b = a+c$. It implies

$$M(a,b,c) = \begin{bmatrix} a & 2a+2b & b \\ c+2a+b & c & c+a+2b \\ 2b+2c & a+b+2c & 2a+2c \end{bmatrix} = \begin{bmatrix} a & c & b \\ a & c & b \\ a & c & b \end{bmatrix}.$$

   It clearly shows that $\deg(M(a,b,c)) = 3$.

   Case 2. $a+b+c \neq 0$. By Lemma 18, $2c \neq a+b$, $2a \neq b+c$, and $2b \neq a+c$. Rewrite M into:

$$M(a,b,c) = \begin{bmatrix} a & 2(a+b) & b \\ (a+b+c)+a & c & (a+b+c)+b \\ 2(b+c) & (a+b+c)+c & 2(a+c) \end{bmatrix}.$$

   Then all the nine elements are distinct which shows that $\deg(M(a,b,c)) = 9$. Without loss of generality, if $(a+b+c)+a = a$, we have $a+b+c = 0$, a contradiction. If $(a+b+c)+a = b$, then $2a+c = 0$, a contradiction again. Similarly, it is straightforward to check all these 9 entries are distinct. Hence, $\deg(M(a,b,c)) = 9$.

All of the cases given above cover all possibilities of what types of MSS we can achieve over a finite field of characteristic 3.

Finally, assume 2 is a quadratic residue in $\mathbf{F}$. Then,

$$M(1,1,0) = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 2 & 2 & 2 \end{bmatrix}, \quad M(1,0,1) = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{bmatrix},$$

and

$$M(0,1,2) = \begin{bmatrix} 0 & 2 & 1 \\ 0 & 2 & 1 \\ 0 & 2 & 1 \end{bmatrix}$$

created from the previous proof are certainly MSS over $\mathbf{F}$. Thus, the proof is complete. ■

We give examples of magic squares constructed based on the above theorem. One example shows over $\mathbb{Z}_3$ there is no non-trivial MSS. Another example shows MSS of degree 3 over another finite field exists.

Example 5. Consider the finite field $\mathbb{Z}_3 = \{0, 1, 2\}$. There is no MSS of degree 3 over $\mathbb{Z}_3$ because 2 is not a quadratic residue mod 3 but 2 has to be an entry of every magic square of degree 3 over $\mathbb{Z}_3$. The following are MS of degree 3 over $\mathbb{Z}_3$:

$$M(1,1,0) = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 2 & 2 & 2 \end{bmatrix}, \quad M(1,0,1) = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{bmatrix},$$

and

$$M(0,1,2) = \begin{bmatrix} 0 & 2 & 1 \\ 0 & 2 & 1 \\ 0 & 2 & 1 \end{bmatrix}.$$

Note that the magic sum of every MS over $\mathbb{Z}_3$ must be 0.

Example 6. Over the finite field $\mathbf{F} = \mathbb{Z}_3[x]/(x^2 + 1) \cong GF(9)$, there exists a magic square of squares of degree 3 and a magic square of degree 9. However,

there is no magic square of squares of degree 9.

Note that in $\mathbf{F}$, $x^2 = -1$. The nine elements of $\mathbf{F}$ are $0, 1, 2, x, 2x, x+1, x+2, 2x+1, 2x+2$. By Lemma 19, 2 is a quadratic residue in $\mathbf{F}$ because $|\mathbf{F}| = 3^2$. The matrices $M(1,1,0), M(1,0,1)$, and $M(0,1,2)$ are all magic squares of squares of degree 3 over $\mathbf{F}$ because 0, 1, 2 are all quadratic residues in $\mathbf{F}$.

The following matrix represents a magic square over $\mathbf{F}$ which is of degree 9:

$$M(0,1,x) = \begin{bmatrix} 0 & 2 & 1 \\ x+1 & x & x+2 \\ 2x+2 & 2x+1 & 2x \end{bmatrix}.$$

However, it is not a magic square of squares over $\mathbf{F}$ because $x+1$ is not a perfect square in $\mathbf{F}$. Actually, magic squares of squares over $\mathbf{F}$ do not exist because $\mathbf{F}$ has only 5 perfect squares: $0, 1, 2 = x^2, x = (2x+1)^2$, and $2x = (2x+2)^2$. This example shows that over a finite field of characteristic 3, magic squares of squares of degree 9 may not exist.

Chapter 3

Possible Degrees for an MS over a Finite Field

In Chapter 2, we show that over a finite field of characteristic 2, the degree of an MS can only be 1, 2, or 4. Over a finite field of characteristic 3, the only possible degree of an MS is 3 or 9. In Hengeveld's thesis [3], it is shown that over $\mathbb{Z}_p$, where p is a prime greater than 3, the degree of an MS is odd. In this chapter, we consider finite fields with characteristic greater than 3. We show similar results as the case over $\mathbb{Z}_p$.

The following lemma shows that the equality of two entries in a magic square M over $\mathbf{F}$ may cause the equality of another pair of entries in M. This behavior tells something about the degree of M.

Lemma 21. Consider an MS of the form $M = M(a, b, c)$. Then

1. $c - a + b = 2c - b \iff c + a - b = b$;
2. $c - a + b = a \iff c + a - b = 2c - a$;
3. $3c - a - b = b \iff b + a - c = 2c - b$;
4. $3c - a - b = a \iff a + b - c = 2c - a$.

Proof. We skip the proof because it is straightforward. ■

Each equivalence in the above lemma represents two pairs of equal entries of $M(a, b, c)$. That is, if two entries of $M(a, b, c)$ are equal, there is another pair of identical entries. So, $\deg(M(a, b, c)) \leq 7$.

The following theorem generalizes Theorem 14 to any finite field whose characteristic is greater than 3.

Theorem 22. *Let* $\mathbf{F}$ *be a finite field of characteristic greater than* 3. *Then the degree of every non-trivial MS over* $\mathbf{F}$ *is odd.*

Proof. Let the characteristic of $\mathbf{F}$ be greater than 3 and $M(a, b, c)$ be a non-trivial MS over $\mathbf{F}$. We have the following:

1. If $a = c \neq b$, then

$$M(a, b, a) = \begin{bmatrix} a & 2a - b & b \\ b & a & 2a - b \\ 2a - b & b & a \end{bmatrix}.$$

   From the above, $\deg(M(a, b, c)) \leq 3$. Without loss of generality, if $2a - b = a$, then $a = b$, a contradiction. This is the same outcome if $2a - b = b$. So $\deg(M(a, b, a)) = 3$.

2. If $a = b \neq c$, then

$$M(a, a, c) = \begin{bmatrix} a & 3c - 2a & a \\ c & c & c \\ 2c - a & 2a - c & 2c - a \end{bmatrix}.$$

   Note that $3c - 2a$ cannot equal to a or c as we would ultimately end up having $a = c$, which is a contradiction. If $3c - 2a = 2c - a$ or $2a - c$, then $a = c$ which is also a contradiction. Similarly, setting $2c - a$ or $2a - c$ equal to any of the other elements of $M(a, a, c)$ causes contradiction as well. Hence, $\deg(M(a, a, c)) = 5$.

3. If a, b, and c are all distinct, we show that $M(a, b, c)$ can only achieve degrees 5, 7, or 9. We examine all of the possible cases:

Case 1. $2c = a + b$. For this case, $M(a, b, c)$ has the following form:

$$M(a,b,c) = \begin{bmatrix} a & c & 2c-a \\ 3c-2a & c & 2a-c \\ a & c & 2c-a \end{bmatrix}.$$

From the above, $\deg(M(a, b, c)) \leq 5$. Without loss of generality, if $3c - 2a = a$ then $3c = 3a$ which implies that $a = c$, a contradiction. It is similar for the case of $3c-2a = c$. If $3c-2a = 2a-c$ or $2c-a$, we would also get $a = c$. Similarly, one can show the remaining elements cannot be equal to each other as the resulting outcome causes the impossible equality: $a = c$. Thus, $\deg(M(a, b, c)) = 5$.

Case 2. $2b = a + c$. In this case, $M(a, b, c)$ has the following form:

$$M(a,b,c) = \begin{bmatrix} 2b-c & 4c-3b & b \\ 2c-b & c & b \\ 2c-b & 3b-2c & 3b-2c \end{bmatrix}.$$

Note that $\deg(M(a, b, c)) \leq 7$. We need to check if all the seven in elements in $M(a, b, c)$ are distinct. Without loss of generality, set $2b - c = b$. If $2b - c = b$, then $b - c = 0$ which implies $b = c$, a contradiction. Similarly, one can check all the seven elements are distinct. Hence, $\deg(M(a, a, c)) = 7$.

Case 3. $2a = b + c$. The degree of $M(a, b, c)$ is 7. This proof is similar as in the case of $2b = a + c$.

Case 4. $2c \neq a + b, 2b \neq a + c$, and $b + c \neq 2a$, but $2a + b = 3c$ or $2b + a = 3c$.

$M(a, b, c)$ has the following form:

$$M(a,b,c) = \begin{bmatrix} a & a & 3c-2a \\ 4c-3a & c & 3a-2c \\ 2a-c & 2c-a & 2c-a \end{bmatrix},$$

which implies that the degree of $M(a, b, c)$ is at most 7. We next show that all the seven elements are distinct. Without loss of generality, let $4c - 3a = a$. Then $4c = 4a$ which gives $a = c$, a contradiction. The other cases are done similarly. Then $\deg(M(a, b, c)) = 7$.

Case 5. $2c \neq a + b, 2b \neq a + c$, $b + c \neq 2a$, $2a + b \neq 3c$, and $2b + a \neq 3c$. With these conditions, one can show that all of the elements of $M(a, b, c)$ are distinct. Hence, $\deg(M(a, b, c)) = 9$.

The above analysis covers all of the possible cases and the only outcome for the degree of $M(a, b, c)$ is 5, 7, or 9. It confirms the theorem. ■

Chapter 4

Construction of MSS with a Desired Degree

4.1 Searching for Special Prime Numbers

In this section, we explore on how to obtain an MSS of a desired degree in a finite field that has an appropriate prime number as its characteristic. We apply Dirichlet's Theorem for such a search. Let $\mathbf{F}$ be a finite field of characteristic $p > 3$. By Theorem 22, the possible degrees for an MS over $\mathbf{F}$ is 3, 5, 7, or 9. In the following theorem, we show that for each possible degree there are infinitely many finite fields over which an MSS of that degree exists. The theorem is proved constructively.

Theorem 23. *Let* $\mathbf{F}$ *be a finite field with characteristic* p*, where* p *is in the form of* $p = 120m + 1$ *for some integer* m*. Then for each* $r \in \{3, 5, 7, 9\}$*, there exists*

an MSS over $\mathbf{F}$ *of degrees* r*. Some of such MSSs are given below:*

$$M(0,1,0) = \begin{bmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \end{bmatrix}, \qquad M(1,1,0) = \begin{bmatrix} 1 & -2 & 1 \\ 0 & 0 & 0 \\ -1 & 2 & -1 \end{bmatrix},$$

$$M(1,2,0) = \begin{bmatrix} 1 & -3 & 2 \\ 1 & 0 & -1 \\ -2 & 3 & -1 \end{bmatrix}, \qquad M(1,4,0) = \begin{bmatrix} 1 & -5 & 4 \\ 3 & 0 & -3 \\ -4 & 5 & -1 \end{bmatrix}.$$

Note that the above MSS have degrees $3, 5, 7,$ *or* 9*, respectively.*

Proof. By Dirichlet's Theorem, there exist infinitely many primes p in the form of $p = 120m + 1$ for some integer m. Since $p \equiv 1 \pmod 8$, -1 and 2 are quadratic residues modulo p by Lemma 5. Also, 3 and 5 are quadratic residues modulo p since $p \equiv 1 \pmod 4$ and $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$ and $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1$. Thus, the above MS are MSS over $\mathbf{F}$. ■

From the proof of the above theorem, we see that for $M(0,1,0), M(1,1,0)$, $M(1,2,0)$, and $M(1,4,0)$ to be MSS over $\mathbf{F}$, $-1, 2, 3$, and 5 must be quadratic residues modulo p. This is the reason why we select p in the form of $p = 120m+1$. By Dirichlet's Theorem, there are infinitely many such primes p. For example, 241, 601, 1201, or 1321 are among them. The MS are MSS over any finite field of characteristic $p = 241$, 601, 1201, or 1321.

We now present a corollary on the existence of an MSS of degree 9 over infinitely many finite fields.

Corollary 24. For each $r \in \{3, 5, 7, 9\}$, there are infinitely many finite fields over which an MSS of degree r exists.

Proof. Immediately from Theorem 23, we can create a finite field $\mathbf{F}$ with characteristic $p = 120m + 1$. Over $\mathbf{F}$, there is an MSS of degree r. By Dirichlet's Theorem, there are infinitely many such primes. ■

We reflect on the open question raised by Martin LaBar. The above corollary answers his question in terms of finite fields.

4.2 Constructing MSS Using Consecutive Quadratic Residue Triples

We first define a special type of triples which will be used to construct MSSs later.

Definition 25. Let p be a prime number and a be any integer. A triple of consecutive integers $(a, a+1, a+2)$ is called a *consecutive quadratic residue triple* (CQR-triple) modulo p if $a, a+1$ and $a+2$ are all quadratic residues modulo p.

Example 7. If $p = 61$, $(3, 4, 5)$ is a CQR-triple. It is because $3 = 8^2, 4 = 2^2$, and $5 = 26^2$ modulo 61.

We now show the existence of infinitely many primes that can produce a CQR-triple.

Lemma 26. Let a a positive integer greater than 1. Then there exist infinitely many primes p such that a is a quadratic residue modulo p.

Proof. Let $a = 2^{e_0} q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}$ be the primary decomposition of a where each q_i is an odd prime, $e_0 \geq 0$, and $e_1, \ldots, e_r$ are positive integers. By Dirichlet's Theorem, there exist infinitely many primes p in the form of $p = (4q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r})m + 1$ (m is an integer). Then for any such a prime p,

$$\left(\frac{a}{p}\right) = \left(\frac{2^{e_0}}{p}\frac{q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}}{p}\right) = \left(\frac{2}{p}\right)^{e_0} \left(\frac{q_1}{p}\right)^{e_1} \left(\frac{q_2}{p}\right)^{e_2} \cdots \left(\frac{q_r}{p}\right)^{e_r}.$$

Note that if $e_0 > 0$, $p \equiv 1 \pmod 8$, so 2 is a quadratic residue mod p. If $e_0 = 0$, a is odd and $p = 4am + 1$. In either case, by the form of p,

$$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)^{e_0} \left(\frac{1}{p}\right)^{e_1} \left(\frac{1}{p}\right)^{e_2} \cdots \left(\frac{1}{p}\right)^{e_r} = 1.$$

Thus, there exist infinitely many primes p such that a is a quadratic residue modulo p. ■

Corollary 27. Let p_1 and $p_1 + 2$ be odd twin primes. Then there exist infinitely many primes p such that $(p_1, p_1 + 1, p_1 + 2)$ is a CQR-triple modulo p.

Proof. Let $p_1 + 1 = 2^{e_0} q_1^{e_1} q_2^{e_2} \cdots q_s^{e_s}$ be the primary decomposition, where $e_i > 0$ for each $i = 0, 1, \ldots, s$ and $q_1, \ldots, q_s$ are distinct odd primes. It is obvious that p_1 and $p_1 + 2$ are not in the set $\{q_1, q_2, \cdots, q_s\}$. By Dirichlet's Theorem, there are infinitely many primes in the form of $p = [4p_1(p_1 + 2)q_1 q_2 \cdots q_s]m + 1$ for some integers m. Now we test if $p_1 + 1$ is a quadratic residue modulo p. By the Legendre symbol,

$$\left(\frac{p_1 + 1}{p}\right) = \left(\frac{q_1}{p}\right)^{e_1} \left(\frac{q_2}{p}\right)^{e_2} \cdots \left(\frac{q_s}{p}\right)^{e_s}.$$

Since $p \equiv 1 \pmod 4$, for each i, $\left(\frac{q_i}{p}\right) = \left(\frac{p}{q_i}\right)$. By the form of p, $\left(\frac{p}{q_i}\right) = 1$. So

$$\left(\frac{p_1 + 1}{p}\right) = 1.$$

As we can see, p_1 is a quadratic residue. Also, $\left(\frac{p_1}{p}\right) = 1$ and $\left(\frac{p_1+2}{p}\right) = 1$. Thus, for any twin primes p_1 and $p_1 + 2$, there exist infinitely many primes p such that $(p_1, p_1 + 1, p_1 + 2)$ is a CQR-triple modulo p. ■

4.3 Using CQR-Triples to Construct MSS of Full Degree

We defined CQR-triple in the previous section and showed that there exist infinitely many prime numbers admitting CQR-triples. In this chapter, we demonstrate a method of constructing MSSs of full degree using CQR-triples. Let $\mathbf{F}$ be a finite field of characteristic $p > 3$ and $k \in \mathbf{F}$ with $k \neq 0, 1, -1$. It is obvious that

the matrix $M(1,k,0)$ is a magic square over $\mathbf{F}$ of degree at least 5:

$$M = M(1,k,0) = \begin{bmatrix} 1 & -1-k & k \\ k-1 & 0 & 1-k \\ -k & k+1 & -1 \end{bmatrix}. \tag{4.1}$$

For this magic square to be a magic square of squares over $\mathbf{F}$ of degree 9, the following conditions are needed: (1) -1 is a quadratic residue in $\mathbf{F}$, (2) $k \neq (p-1)/2$, (3) $k \neq (p+1)/2$, and most importantly, $(k-1, k, k+1)$ must be a CQR-triple mod p. Satisfying conditions (2) and (3) guarantees that all the nine entries of M are distinct. To satisfy condition (1), it needs $p \equiv 1 \pmod 4$. We show below that there are infinitely many finite fields in which all of these conditions are satisfied. Thus we can build magic squares of squares of degree 9 over them.

Theorem 28. *There are infinitely many finite fields over which an MSS of degree 9 exist.*

Proof. Let p_1 and p_1+1 be odd twin primes. Then $k = p_1 + 1$ is even. We create a prime number in the same way as that in the proof of Corollary 27. Select a prime number in the form of $p = 4p_1(p_1+1)(p_1+2)m + 1$, where $m \in \mathbb{Z}$. One can see that $p > 240$ since $(3,4,5)$ is the smallest CQR-triple starting with an odd prime. Note that there are infinitely many such primes by Dirichlet's Theorem. Let $\mathbf{F}$ be any finite field of characteristic p. It is obvious that k equals none of these: $0, 1, -1, (p-1)/2, (p+2)/2$. Thus $k \neq -k-1$ and $k \neq -k+1$ in $\mathbf{F}$. Thus we obtain a magic square of degree 9 from the configuration (4.1):

$$M(1,k,0) = M(1,p_1+1,0) = \begin{bmatrix} 1 & -(p_1+2) & p_1+1 \\ p_1 & 0 & -p_1 \\ -(p_1+1) & p_1+2 & -1 \end{bmatrix}. \tag{4.2}$$

Since $p \equiv 1 \pmod 4$, -1 is a quadratic residue (mod p). Similarly as in the

proof of Corollary 27, (p_1, p_1+1, p_1+2) is a CQR-triple (mod p). This makes $M(1, p_1+1, 0)$ an MSS of degree 9 over $\mathbf{F}$. ■

The following example is constructed by using the twin primes 3 and 5. Any prime number p in the form of $p = 4(3 \cdot 4 \cdot 5)m + 1$, where $m \in \mathbb{Z}$, makes $(3, 4, 5)$ a CQR-triple (mod p). That is, $(3, 4, 5)$ is a CQR-triple in any finite field of characteristic p. The prime $p = 61$ is such a prime.

Example 8. Consider twin primes 3 and 5. Then $(3, 4, 5)$ is a CQR-triple modulo $p = 61$. Let $\mathbf{F}$ be any finite field of characteristic 61. The magic square

$$M(1,4,0) = \begin{bmatrix} 1^2 & -26^2 & 2^2 \\ 8^2 & 0^2 & -8^2 \\ -2^2 & 26^2 & -1^2 \end{bmatrix} = \begin{bmatrix} 1 & -5 & 4 \\ 3 & 0 & -3 \\ -4 & 5 & -1 \end{bmatrix} \pmod{61}.$$

Consider another pair of odd primes 11 and 13 (twin primes).

Example 9. Select a prime number p in the form of $p = 4(11 \cdot 3 \cdot 13)m + 1 = 1716m + 1$. The triple $(11, 12, 13)$ is a CQR-triple and there are infinitely many such primes p. In any finite field $\mathbf{F}$ of characteristic p, the following magic square is a magic square of squares of degree 9 in $\mathbf{F}$. By an easy check, $3433 = 1716 \times 2 + 1$ is a prime number. Let $\mathbf{F} = \mathbb{Z}_{3433}$. Then we obtain a magic square of squares in $\mathbf{F}$:

$$M(1,12,0) = \begin{bmatrix} 1^2 & -203^2 & 1687^2 \\ 1236^2 & 0^2 & -1236^2 \\ -1687^2 & 203^2 & -1 \end{bmatrix} = \begin{bmatrix} 1 & -13 & 12 \\ 11 & 0 & -11 \\ -12 & 13 & -1 \end{bmatrix} \pmod{3433}.$$

The above examples demonstrate a method of constructing MSS from a pair of twin primes. One can obtain infinitely many prime numbers p such that the twin primes can produce a CQR-triple (mod p). Using the resulted CQR-triple, an MSS of degree 9 can be constructed over any finite field of characteristic p.

Chapter 5

Constructing MSS with Nonzero Sum

In the previous chapter, we discussed how to construct an MSS using CQR-triples. In either example given at the end of Chapter 4, the MSS has 0 as the middle entry, that is, the magic sum is 0. In this chapter, we provide a set of MSSs, each with nonzero magic sum, by other methods. In the example given below, we show how to construct another MSS with nonzero magic sum using the CQR-triple $(3, 4, 5)$.

Example 10. Consider the CQR-triple $(3, 4, 5)$ modulo the prime number $p = 9241$. A magic square over $\mathbb{Z}_p$ is shown below:

$$M(1,0,4) = \begin{bmatrix} 1^2 & 2930^2 & 9241^2 \\ 8392^2 & 9239^2 & 4513^2 \\ 3515^2 & 8908^2 & 623^2 \end{bmatrix} = \begin{bmatrix} 1 & 11 & 0 \\ 3 & 4 & 5 \\ 8 & -3 & 7 \end{bmatrix} \pmod{p}.$$

Since $p - 1 = 9240 = 8 \cdot 11 \cdot 3 \cdot 7 \cdot 5$, -1, 2, 3, 5, 7, 11, are all quadratic residues mod 9241. Thus $M(1, 0, 4)$ is an MSS over $\mathbb{Z}_{9241}$.

In a similar way, we can construct many MSSs. We provide a chart showing the MSSs along with the forms of primes (characteristic of the ground field), and one representative.

MSS	Degree of MSS	Form of Prime p and One Representative
$\begin{bmatrix} 1 & 12 & 2 \\ 6 & 5 & 4 \\ 8 & -2 & 9 \end{bmatrix}$	9	$5760m+1, \quad 23041$
$\begin{bmatrix} 1 & 8 & 3 \\ 6 & 4 & 2 \\ 5 & 0 & 7 \end{bmatrix}$	9	$10080m+1, \quad 20161$
$\begin{bmatrix} 1 & 11 & 3 \\ 7 & 5 & 3 \\ 7 & -1 & 9 \end{bmatrix}$	7	$1155m+1, \quad 2311$
$\begin{bmatrix} 1 & 3 & 5 \\ 7 & 3 & -1 \\ 1 & 3 & 5 \end{bmatrix}$	5	$105m+1, \quad 211$
$\begin{bmatrix} 0 & 11 & 1 \\ 5 & 4 & 3 \\ 7 & -3 & 8 \end{bmatrix}$	9	$9240m+1, \quad 9241$
$\begin{bmatrix} 0 & 14 & 1 \\ 6 & 5 & 4 \\ 9 & -4 & 10 \end{bmatrix}$	9	$4200m+1, \quad 4201$
$\begin{bmatrix} 2 & 12 & 1 \\ 4 & 5 & 6 \\ 9 & -2 & 8 \end{bmatrix}$	9	$5760m+1, \quad 23041$
$\begin{bmatrix} 3 & 8 & 1 \\ 2 & 4 & 6 \\ 7 & 0 & 5 \end{bmatrix}$	9	$10080m+1, \quad 20161$

$\begin{bmatrix} 3 & 11 & 1 \\ 3 & 5 & 7 \\ 9 & -1 & 7 \end{bmatrix}$	7	$1155m + 1, \quad 2311$
$\begin{bmatrix} 4 & 10 & 1 \\ 2 & 5 & 8 \\ 9 & 0 & 6 \end{bmatrix}$	9	$4800m + 1, \quad 4801$
$\begin{bmatrix} 5 & 3 & 1 \\ -1 & 3 & 7 \\ 5 & 3 & 1 \end{bmatrix}$	5	$105m + 1, \quad 211$
$\begin{bmatrix} 3 & -5 & 5 \\ 3 & 1 & -1 \\ -3 & 7 & -1 \end{bmatrix}$	9	$105m + 1, \quad 211$
$\begin{bmatrix} 5 & -5 & 3 \\ -1 & 1 & 3 \\ -1 & 7 & -3 \end{bmatrix}$	7	$105m + 1, \quad 211$

Chapter 6

Conclusions and Future Direction

LaBar's open question concerned about the existence of MSS over the integers. In our case, we focused on whether such an MSS exists over finite fields. In Chapter 2, we provided results on the existence of MSS over a finite field of characteristic 2. We claimed that every MS over a finite field of characteristic 2 is an MSS and can achieve degree 2 or 4. Next, we showed that every non-trivial MSS over a finite field of characteristic 3 must have degree 3 or 9. In Chapter 3, we investigate MS or MSS over finite fields of characteristic greater than 3. We generalized Hengeveld and Li's result (Theorem 14) regarding the degree of an MS. We claimed a similar result that the degree of a non-trivial MS over any finite field of characteristic greater than 3 must be 3, 5, 7, or 9.

In Chapter 4, for each of the possible degrees 3, 5, 7, or 9, we construct MSS of the indicated degree over infinitely many finite fields. The construction involves finding consecutive quadratic residue triples using twin primes. The resulting MSS have magic sum 0.

In Chapter 5, we apply Dirichlet's Theorem to construct MSS with magic sum not equal to 0. For each configuration, there are infinitely many primes admitting the configuration as the MSS.

Many questions remain to be answered. For example,

- Can we use the CQR-triple method to construct MSS of degree less than 9?

- Can we find a degree 9 MSS over a finite field of characteristic 3?
- Over what finite fields an MSS of degree 9 does not exist?
- What number in a finite field cannot be the magic sum of an MSS over it?

Chapter 7

References

[1] Bremner, Andrew. *"On squares of squares"*. Acta Arithmetica 88.3 (1999): 289-297.

[2] Gazali, Wikaria, et. al. *"An Algorithm to Find Square Root of Quadratic Residues over Finite Fields using Primitive Elements"*. Procedia Computer Science 116 (2017): 198-205.

[3] Hengeveld, Stewart. *"Construction and Analysis of Magic Squares of Squares over Certain Finite Fields"*. Dissertation, Montclair State University, 2012.

[4] Hoffstein, Jeffrey, et. al. *"An Introduction to Mathematical Cryptography"*. Springer Science+Business Media, New York, 2014.

[5] Hungerford, Thomas W. *"Abstract Algebra: An Introduction"*. 3rd ed. Brooks/Cole, 2012.

[6] Jones, Gareth, A. and J.M. Jones. *"Elementary Number Theory"*. Springer-Verlag London Limited, 1998.

[7] LaBar, Martin. *"Problem 270"*, College Math. Journal (1984): 69.

[8] Lahtonen, J. (2016, February 25). When is 2 a quadratic residue in a finite field? [Msg 2]. Message posted to https://math.stackexchange.com/questions/1670849/when-is-2-a-quadratic-residue-in-a-finite-field

[9] Lehmer, D.H., et. al. *"Pairs of Consecutive Power Residues."* Canadian Journal of Mathematics 15 (1963): 172-177.

[10] "Lo-Shu Magic Square." http://www.numeroworld.com/lo-shu-magic-square.asp. Accessed 22 October 2017.

[11] "Lo Shu Magic Square." http://www.taliscope.com/LoShu_en.html. Accessed 6 November 2017.

[12] "Magic Squares- History." http://plaza.ufl.edu/ufkelley/magic/history.htm. Accessed 25 February 2017.

[13] Rosen, Kenneth H. *"Elementary Number Theory and its Applications"*, 6^{th} ed., Pearson, 2011.

[14] Sallows, Lee. *"The Lost Theorem"*. The Mathematical Intelligencer 19.4 (1997): 51-54.