5-2017

Constructing Magic Squares of Squares Modulo Certain Prime Numbers

Nicholas Ryan Bilynsky
Montclair State University

Abstract

A magic square is a square table of numbers such that each row, column, or diagonal adds up to the same sum. This research is inspired by an open question posed by Martin Labar in 1984. The open question states: "Can a 3×3 magic square be constructed using nine distinct perfect squares?" Though unsolved, this question sheds light on the existence of a Magic Square of Squares modulo a prime number p. For over two thousand years, many mathematicians have looked at these magical properties. In this thesis, the focus is on certain prime numbers p in the form of $am + 1$. We show that there exist Magic Squares of Squares with nine distinct elements mod p, for certain primes p. Constructions of such magic squares of squares are given. It is known that a magic square of squares can only admit 1, 2, 3, 5, 7, or 9 distinct numbers. We show that for infinitely many carefully selected prime numbers, non-trivial magic squares of squares with 2, 3, 5, 7, or 9 distinct perfect squares can be constructed. The results provide a positive answer to the open question regarding integers modulo certain prime numbers.

The configurations used in the construction all have the appearance of 0, 1, 2, or 4. A further study investigates how many times each of these values can occur in a magic square of squares using the considered configurations. In addition, the constructions require the existence of quadruplet of consecutive quadratic residues. For each prime number considered, a set of such quadruplets is provided and used to construct desired magic squares of squares.

MONTCLAIR STATE UNIVERSITY

/ Constructing Magic Squares of Squares Modulo Certain Prime Numbers /

by

Nicholas Ryan Bilynsky

A Master's Thesis Submitted to the Faculty of

Montclair State University

In Partial Fulfillment of the Requirements

For the Degree of

Master of Science

May 2017

College of Science and Mathematics

Department of Mathematical Science

Thesis Committee:

[redacted]

Thesis Sponsor: Dr. Aihua Li

[redacted]

Committee Member: Dr. Mark S. Korlie

[redacted]

Committee Member: Dr. Bogdan G. Nita

Constructing Magic Squares of Squares Modulo Certain Prime Numbers

A Thesis

Submitted in partial fulfillment of the requirements for the degree of Master of Science in Pure and Applied Mathematics

Nicholas Ryan Bilynsky

Montclair State University

Montclair, NJ

May 2017

Acknowledgments

I would like to start off by thanking Dr. Aihua Li for her time and devotion in guiding me in writing this thesis. I also wish to thank Dr. Bogdan G. Nita and Dr. Mark S. Korlie for being part of my thesis committee. Additionally, from the undergraduate side of my career as a student of mathematics, I would like to thank Dr. Patricia J. Garruto from Caldwell University for inspiring me to become a graduate student at Montclair State University. Finally, from the bottom of my heart, I would like to thank my family for helping me become the person I am now and will be in the years ahead. Without them, I would not have been able to overcome all of the difficult challenges life presented to me.

Contents

1 Introduction

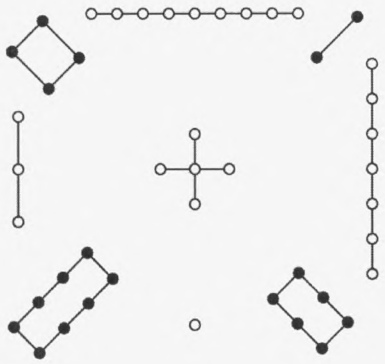
1.1 History

A magic square is a square table of numbers such that each row, column, and diagonal adds up to the same sum. The topic of magic squares is more than two-thousand centuries old. The magic square got its name from the belief that these squares were lucky from civilization to civilization and had magical, mystical, or religious properties. Many mathematicians traced these influences in China, India, Persia, Arabia, Europe, and America.

The first recorded history of magic squares dated between 2800 and 2200, B. C. E. In ancient times, a turtle swam into the Lo River with a design on its shell. The patterns consisted of dots, lines, and squares which gave light to what modern mathematicians know as the Lo Shu Magic Square. This 3 by 3 magic square consists of every natural number from 1 to 9 and has a magic sum (the sum of each row, column, or diagonal) of 15. The number 15 has a special significance to the Chinese people because it is the number of days in the 24 cycles of the Chinese Year.

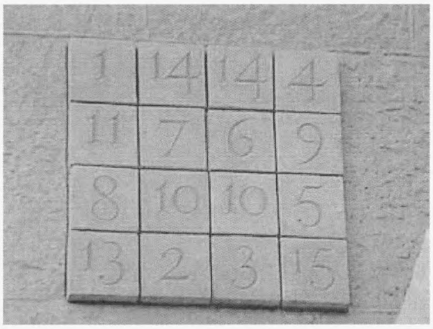
In Europe, a magic square, with the magic sum of 33 can be found on the wall on the exterior of the Sagrada Familia Church in Barcelona. This magic square holds religious properties because Jesus Christ was crucified at the age of 33. In the Renaissance Era, Albrecht Dürher, a German amateur mathematician and artist, engraved Melancholia I: "It shows many mathematical objects including a sphere, a truncated rhombohedron, and in the upper right hand corner, a magic square of order 4" (Moler [9]).

Many other mathematicians and scientists have examined the mystical powers of these squares, such as Benjamin Franklin, Leonhard Euler, Sir Arthur Cayley, Edouard Lucas, John Conway, and Martin Labar.



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

Figure 1: The Lo Shu Square with magic sum 15 and the matrix format



1	14	14	4
11	7	6	9
8	10	10	5
13	2	3	15

Figure 2: Sagradia Familia Church Magic Square with magic sum 33

Definition 1.1 *A magic square (denoted M.S. herein) over $\mathbb{Z}$ is a 3×3 matrix denoted $M = [a_{ij}]_{3\times 3}$ where $a_{ij} \in \mathbb{Z}$, such that for every $i, j \in \{1,2,3\}$, $\sum\limits_{i=1}^{3} a_{ij} = \sum\limits_{j=1}^{3} a_{ij} = \sum\limits_{i=1}^{3} a_{ii} = \sum\limits_{i=1}^{3} a_{i(4-i)} = S$. We call the constant S the magic sum. If for all $i, j \in \{1,2,3\}$ $a_{ij} = b_{ij}^2$, for some $b_{ij} \in \mathbb{Z}$, then call M a magic square of squares over $\mathbb{Z}$.*

Referring to the magic sum defined above, it is known that $S = 3a_{22}$.

Lemma 1.2 *1. Every M.S. $[a_{ij}]$ has the magic sum $S = 3a_{22}$.*

2. Consider two magic squares A and B. We say A is isomorphic to B if B can be obtained by rotations and/or reflections about the rows, columns, main diagonal, or the minor diagonal from A.

1.2 The Open Question and Related Questions

My research is inspired by an open question posed by Martin Labar in 1984 [2] which remains unanswered about the existance of a 3×3 magic square with nine distinct elements being perfect squares, known as a magic square of squares, or, for the purposes of this paper, M.S.S.

Question 1.3 *[1] Can a 3×3 magic square be constructed using nine distinct perfect squares?*

For over thirty years, this question remains unsolved. In lieu of answering the open question via the integers, we answer a similar question by working on $\mathbb{Z}_p$, where p is a prime number. In an earlier work done by Stewart Hengeveld [1], a similar question was raised:

Question 1.4 *Can a 3×3 magic square be constructed using nine distinct perfect squares from a finite field?*

The answer to this question, according to Hengeveld, depends on the chosen prime number. A 3×3 magic square can be constructed using nine distinct perfect squares from $\mathbb{Z}_p$ when $p = 29$ or $p = 59$, but not for many other primes such as $p = 17$ and $p = 19$ [1]. In my case, I establish the existence of an M.S.S. with nine distinct elements over $\mathbb{Z}_p$ for many prime numbers p, examine how many of what entry appears, determine how many distinct elements this M.S.S. can achieve, and examine what other quadratic residues can make an M.S.S.

The next lemma shows that every 3 by 3 magic square of integers can be determined by three integers a, b, c.

Lemma 1.5 *A $3\times$ 3 magic square M is determined by three elements, say a, b, c as represented below:*

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

If $a = b = c, M(a,b,c) = diag(a)$ is called a trivial M.S. I am interested only in nontrivial M.S. I investigate several different types of prime numbers. For each type, quadruplets of consecutive perfect squares are developed and they are used in constructing M.S.S. over the corresponding field. In addition, I construct M.S.S. of all possibles degrees; specifically degrees $3, 5, 7$ and 9. For certain fixed prime numbers p, I examine how many entries of an M.S.S. can admit a special value. Different relationships among a, b, c may give different types of magic squares of squares. For example, when $c = b - a$, $M(a, b, c)$ has the form:

$$M(a,b,b-a) = \begin{bmatrix} b-a & 4a-2b & b \\ 2a & a & 0 \\ 2a-b & 2b-2a & 3a-b \end{bmatrix}$$

which contains 0 as an entry.

1.3 Basic Definitions and Existing Theorems over $\mathbb{Z}_p$

For a ring R, $M = [a_{ij}]_{3\times 3}$ denotes a three-by-three square matrix with a_{ij} being the entry in the (i, j)-position of M and $a_{ij} \in R$. The ring of interest for this thesis is $\mathbb{Z}_p$, the p-element integral domain with characteristic p.

Definition 1.6 *Let p be a prime number and M be a 3×3 matrix with entries from $\mathbb{Z}_p$. We say M is a magic square over $\mathbb{Z}_p$ if the sum of each row, column, and both diagonals are congruent to a constant S* mod *p. Furthermore, if all entries of M are quadratic residues* mod *p, we say M is a magic square of squares (denoted as M.S.S. herein) over $\mathbb{Z}_p$. Define S_p ={all M.S. over $\mathbb{Z}_p$} and SS_p ={all M.S.S. over $\mathbb{Z}_p$}.*

Definition 1.7 *Let p be any prime and $M = [a_{ij}] \in M_{3\times 3}(\mathbb{Z}_p)$ be a magic square over $\mathbb{Z}_p$. We define the degree of M, denoted* $\deg(M)$*, to be the number of distinct entries in M. The degree of S_p, denoted $\alpha(S_p)$, is the maximum degree of all magic squares in S_p. That is, $\alpha(S_p) = max\{\deg(M) | M \in S_p\}$. Similarly, $\alpha(SS_p)$ is defined as $\alpha(SS_p) = max\{\deg(M) | M \in SS_p\}$.*

Stewart Hengeveld, in a prior thesis, indicated that nontrivial magic squares only odd degrees for any prime $p \geq 5$.

Theorem 1.8 *[1] Let $M \in S_p$, where $p \geq 5$, M is nontrivial, and p is prime. Then* $\deg(M)$ *is odd.*

In order to construct M.S.S. over $\mathbb{Z}_p$ for a prime number p, we need to test whether a given integer is a quadratic residue or not, which is where the Legendre Symbol and the rules associated with it come into play.

Definition 1.9 *Let p be an odd prime and a be an integer not divisible by p. The Legendre Symbol $\left(\frac{a}{p}\right)$ is defined as*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \textit{if } a \textit{ is a quadratic residue of } p \\ -1 & \textit{if } a \textit{ is a quadratic nonresidue of } p. \end{cases}$$

Legendre symbols are useful in testing an integer is a perfect square modulo p or not. The following results can be found in any number theory book.

Theorem 1.10 *(Rules of Legendre Symbols) Let p and q be odd primes. Then*

$$\begin{aligned}
\left(\frac{-1}{p}\right) &= \begin{cases} 1 & \textit{if } p \equiv 1 \pmod 4 \\ -1 & \textit{if } p \equiv 3 \pmod 4, \end{cases} \\
\left(\frac{2}{p}\right) &= \begin{cases} 1 & \textit{if } p \equiv 1 \textit{ or } 7 \pmod 8 \\ -1 & \textit{if } p \equiv 3 \textit{ or } 5 \pmod 8, \end{cases} \\
\left(\frac{3}{p}\right) &= \begin{cases} 1 & \textit{if } p \equiv 1 \textit{ or } 11 \pmod{12} \\ -1 & \textit{if } p \equiv 5 \textit{ or } 7 \pmod{12}, \end{cases} \\
\left(\frac{7}{p}\right) &= \begin{cases} 1 & \textit{if } p \equiv 1, 3 \textit{ or } 9 \pmod{28} \\ -1 & \textit{if } p \equiv 5, 11 \textit{ or } 13 \pmod{28}, \end{cases} \\
\left(\frac{p}{q}\right) &= \begin{cases} \left(\frac{q}{p}\right) & \textit{if } p \equiv 1 \textit{ or } q \equiv 1 \bmod 4 \\ -\left(\frac{q}{p}\right) & \textit{if } p \equiv 3 \textit{ and } q \equiv 3 \bmod 4\ . \end{cases}
\end{aligned}$$

Obviously, for every $M \in S_p, 1 \leq \deg(M) \leq \alpha(SS_p) \leq 9$.

Dirichlet's theorem provides useful tools for us to determine the existence and the number of a special type of primes for our investigation.

Theorem 1.11 *[4] Dirichlet's theorem: Let a,b $\in \mathbb{Z}$ with a, $b > 0$ and $gcd\,(a, b) = 1$. Then, the following arithmetic progression contains infinitely many prime numbers:*

$$a, a + b, a + 2b, \cdots, a + nb, \cdots,$$

where n runs for all positive integers.

In particular, for any given positive integer $a > 1$, there are infinitely many primes of the form $am + 1$ where m is a natural number.

Consider a given form of the vector (a, b, c) such as $(a, b, b - a)$ or $(a, b, 2a - b)$ for the matrix $M(a, b, c)$. I propose the following research questions for this project:

Question 1.12 *For what number p can we construct an M.S.S. in the form of $M(a, b, c)$ with nine distinct elements* mod p*?*

Question 1.13 *If, for a prime p $\alpha(SS_p) = 9$, can it achieve degrees 3, 5, or 7? In other words, what is the maximum number of distinct elements an M.S.S.* mod *p can admit?*

Question 1.14 *In any given configuration, how many entries of a special value, such as 0, 1, or 2 can an M.S. or an M.S.S. contain?*

To answer the first question, we determine that we can construct an M.S.S. with all possible degrees with certain prime numbers p of the form $am + 1$, as described by Dirichlet's theorem. For instance, we examine cases where $p = 168m + 1$ or $p = 9240m + 1$. As for the second question, if p does not produce an M.S.S. of degree 9, some can have degrees 7, 5, or 3. This idea is evident within our configurations in subsequent sections. We look at three different configurations; but, as stated before, we can have at most three zero entries in a non-trivial M.S. or an M.S.S. over $\mathbb{Z}_p$ for $p \leq 5$. First, we give conditions under which all entries an M.S.S. are distinct.

2 Existence of Degree 9 M.S.S.

The basics are not basic, but they form a strong foundation for this section. The theorems, corollaries, and lemmas that follow all focus on M.S. as a whole with some examples in between. Let $M = [a_{ij}] \in S_p$ be an M.S. Then we can assume every entry $a_{ij} \in M$ satisfies $|a_{ij}| < p$. In order to better understand what happens, we have the following lemma:

Lemma 2.1 *Let $M = [a_{ij}]_{3\times 3}$ be a matrix in S_p where p is a prime number. If for every $i, j, s, t \in \{1, 2, 3\}$, $0 < |a_{ij} - a_{st}| \leq p - 1$ whenever $(i, j) \neq (s, t)$, then all entries of M are different in $\mathbb{Z}_p$.*

Proof. Because $0 < |a_{ij} - a_{st}| \leq p - 1$, we have that $p \nmid |a_{ij} - a_{st}|$ which also means that $p \nmid (a_{ij} - a_{st})$. The fact that p is not a divisor shows that $a_{ij} \not\equiv a_{st} \mod p$. Therefore, $a_{ij} \neq a_{st}$ in $\mathbb{Z}_p$.

Lemma 2.1 examines distinctiveness of the elements of any M.S. satisfying the above given condition, $p \nmid |a_{ij} - a_{st}|$. In fact, it is a critical lemma in the proof of one of the cases in theorem 2.4, in which we discuss the degree of an M.S.S.

Lemma 2.2 *Assume $| a_{ij} |< p$ for every i, j, $|a_{ij} - a_{st}| \neq p$, and $a_{ij} \neq a_{st}$ for all $(i, j) \neq (s, t)$. Then, $a_{ij} \neq a_{st}$ in $\mathbb{Z}_p$.*

This lemma is similar to the previous lemma in that we are arriving at the same conclusion. However, there are different conditions in play.

Proof. By the triangle inequality, $|a_{ij} - a_{st}| \leq |a_{ij}| + |a_{st}| < 2p$. From there, $-2p < a_{ij} - a_{st} < 2p$. Within these two boundaries, there are only three multiples of p: 0 and $\pm p$. Thus, $a_{ij} \not\equiv a_{st} \mod p$ because $|a_{ij} - a_{st}| \neq p$ or 0.

Definition 2.3 *(Configuration 1) Fix any prime p. Let $a = k^2, k \in \mathbb{Z}_p$, be a nonzero quadratic residue* mod *p. Consider the matrix $M(a, b, c)$ defined in lemma 1.5. Set $b = ar$ and $c = a(r-1)$*

where $r \in \mathbb{Z}_p$, then $M(a,b,c)$ becomes

$$M\left(a, ar, a\left(r-1\right)\right) = a \begin{bmatrix} r-1 & 2\left(2-r\right) & r \\ 2 & 1 & 0 \\ 2-r & 2\left(r-1\right) & 3-r \end{bmatrix}.$$

Theorem 2.4 *There are infinitely many primes p such that $\alpha(SS_p) = 9$.*

Here, we use the Rules of Legendre Symbols, Dirichlet's theorem, and, of utmost importance, the previous analysis about M in SS_p. Dirichlet's theorem and the Rules of Legendre Symbols also hold important information that will shed light on each result. Dirichlet's theorem will be used to make these certain prime numbers p. The Rules of Legendre Symbols will also be used to determine which elements are quadratic residues and see if we have an M.S.S.

Proof.

First, there are infinitely many primes of the form $p = 168m + 1, m \in \mathbb{Z}$ by Dirichlet's theorem because 168 and 1 are relatively prime to each other.

To construct a degree 9 M.S.S., we select $r = 9$ and any nonzero quadratic residue $a \in \mathbb{Z}_p$.

$$M\left(a, 9a, 8a\right) = aM\left(1, 9, 8\right) = a \begin{bmatrix} 8 & -14 & 9 \\ 2 & 1 & 0 \\ -7 & 16 & -6 \end{bmatrix}.$$

We claim that $M(a, 9a, 8a)$ or $aM(1,9,8)$ is an M.S.S. of degree 9 in SS_p. The number $168 = 8 \cdot 3 \cdot 7$. Because $p \equiv 1 \bmod 8$, by theorem 1.10

$$\left(\frac{2}{p}\right) = 1, \quad \left(\frac{-1}{p}\right) = 1, \left(\frac{3}{p}\right) = 1, \left(\frac{8}{p}\right) = \left(\frac{2}{p}\right) = 1.$$

Thus, $2, -1, 3, 8$ are quadratic residues. Furthermore, $p \equiv 1 \bmod 7 \Longrightarrow$

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1.$$

$$\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) = 1 \quad \text{and} \quad \left(\frac{-14}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{7}{p}\right) = 1.$$

So, $-6, -7, -14$ are quadratic residues.

By the analysis, all elements of $M(a, 9a, 8a)$ are quadratic residues mod p. So, M is an M.S.S.

Now, we show that M has at least nine distinct elements. Obviously $max\,|a_{ij} - a_{st}| = 30 < p$ for $i, j \in \{1, 2, 3\}$ because $p > 169$. Thus, for every $i, j, s, t \in \{1, 2, 3\}$, $0 < |a_{ij} - a_{st}| \leq p - 1$ and $p \nmid |a_{ij} - a_{st}|$ with $(i, j) \neq (s, t)$; then, by theorem 2.1 all entries of M are different. Therefore, $\deg(aM(1, 9, 8)) = 9 \Rightarrow \alpha\,(SS_p) = 9$. Since there are infinitely many primes in the form of $168m + 1$, we have an M.S.S. of degree 9 over infinitely many primes p.

Therefore, there are infinitely many primes p such that $\alpha(SS_p) = 9$.

Remark 2.5 *With regard to $M(a, 9a, -8a)$, we have a magic sum of 3a. However, we do not necessarily have to let $r = 9$. Other values for r may produce an M.S.S., but it may have different degrees. In addition, the two magic squares mentioned in the proof are of the form $M(a, ar, a(r - 1))$, in the general form of $M(a, b, c)$. As we go further, we will find such occurrences where we modify a, b, and c.*

Next; recall from the proof of theorem 2.4 that there are infinitely many primes p such that $p = 168m + 1$. This section examines all the possibilities that come from the particular form. Throughout this section, a is a quadratic residue modulo the indicated prime p.

Example 2.6 *Let $p = 168m + 1$ be a prime. We examine $M(a, 0, -a)$ or $aM(1, 0, -1)$, where a is a quadratic residue* mod p. *Notice that below, we have a matrix M resulted from $r = 0$.*

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

where $r = 0$. This M is an M.S.S. of degree 7 and the magic sum is 3a. Note that $p \equiv 1$ mod 4 which means that -1 is a quadratic residue. Additionally, $p \equiv 1$ mod 8 which implies that 2 and -2 are quadratic residues, which ultimately means that M is an M.S.S.

The next example is of degree 3 for $r = 1$.

Example 2.7 *For $M(a, a, 0) = aM(1, 1, 0)$, we have the following:*

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

where $r = 1$. For the same reasons, the above M is an M.S.S., but of degree 3.

Lemma 2.8 *Let $p = 168m + 1$ be a prime. Then, the matrix $M(a, ar, a(r-1))$ is an M.S.S. if and only if the elements $r-3$, $r-2$, $r-1$, and r are consecutive quadratic residues* mod p.

Proof. Obviously, $p \equiv 1 \bmod 4$, and $p \equiv 1 \bmod 8$; so, -1, 0, 1, and 2 are quadratic residues mod p, so $M(a, ar, a(r-1))$ in the configuration in definition 2.3 is an M.S.S. if and only if $r-3$, $r-2$, $r-1$, and r are all quadratic residues.

From the two examples above, we obtained M.S.S. of degrees 3 and 9.

Theorem 2.9 *Assume $p = 168m+1$ is a prime number, where $m \in \mathbb{Z}$, a is a quadratic residue* mod p. *Then, the M.S.S. given by $M(a, ar, a(r-1))$ achieves the degrees 3, 5, 7, and 9, which covers all possible degrees an M.S.S may admit. That is, we can use $M(a, ar, a(r-1))$ to construct an M.S.S. of all possible degrees ≥ 3.*

Proof.

From definition 2.3, $\deg(M) \geq 3$. We start off with $r = 0, 1, 2^{-1}(3)$. We construct M.S.S. by $M = (a, ar, a(r-1))$ with the indicated degrees by taking various values for r.

When $r = 0$,

$$M(a, 0, -a) = a \begin{bmatrix} -1 & 4 & 0 \\ 2 & 1 & 0 \\ 2 & -2 & 3 \end{bmatrix} \text{ which is an M.S.S. of degree 7.}$$

For $r = 1$,

$$M(a, a, 0) = a \begin{bmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix}, \text{ an M.S.S. of degree 3.}$$

For $r = 4$,

$$M(a, 4a, 3a) = a \begin{bmatrix} 3 & -4 & 4 \\ 2 & 1 & 0 \\ -2 & 6 & -1 \end{bmatrix}, \text{ degree 9.}$$

For $r = 2^{-1}(3)$,

$$M(a, 2^{-1}(3)a, 2^{-1}a) = a \begin{bmatrix} 2^{-1} & 1 & 2^{-1}(3) \\ 2 & 1 & 0 \\ 2^{-1} & 1 & 2^{-1} \end{bmatrix}, \quad \text{which is of degree 5.}$$

Because $p = 168m+1$, we know from before that $2, -1, 2^{-1}$ are all quadratic residues mod p. Also, 3 and $2^{-1}(3)$ are both quadratic residues. Thus, all of the entries of the above matrices are perfect squares mod p. Hence, all the resulting M.S. are M.S.S.

We observed that $M(a, ar, a(r-1))$ has degree 3 when $r = 1$ and that r has degree 5 when $r = 2^{-1}(3)$. The maximal degree of 9 occurs when $r \geq 4$. Other degree 3 and 7 M.S.S. are given below.

When $r = 2$, then $\deg(M) = 3$. When $r = 3$, then $\deg(M) = 7$.

Example 2.10 *For $r = 2$ or $r = 3$,*

$$M(a, 2a, a) = a \begin{bmatrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix} \quad or \quad M(a, 3a, 2a) = a \begin{bmatrix} 2 & -2 & 3 \\ 2 & 1 & 0 \\ -1 & 4 & 0 \end{bmatrix},$$

which is of degree 3 or 7.

3 M.S.S. of Type $M(a, ar, a(r-1))$

In the previous section, we introduced the first configuration as

$$M(a, ar, a(r-1)) = a \begin{bmatrix} r-1 & 2(2-r) & r \\ 2 & 1 & 0 \\ 2-r & 2(r-1) & 3-r \end{bmatrix}.$$

Throughout this section, we will let $p = 168m+1$ be a prime number. In the next subsection, we examine how many zero entries we may potentially have in the configuration $M(a, ar, a(r-1))$.

3.1 Number of Zero as Entries

From the M.S. constructed from $M(a, ar, a(r-1))$ as before a is a quadratic residue. We see that the entry at the (2,3) position must be zero. Also, all of the examples we have so far show that no M.S.S. of the form $M(a, ar, a(r-1))$ have more than three zeros. We claim in the next proposition that this is the true case.

Proposition 3.1 *Consider any M.S. $M = M(a, ar, a(r-1))$. Then, when $r = 0$ or $r = 3$, M contains exactly two zeros. When $r = 1$ or $r = 2$, M contains exactly 3 zeros. For $r \notin \{0, 1, 2, 3\}$, M has exactly one zero.*

Proof. From

$$M(a, ar, a(r-1)) = a \begin{bmatrix} r-1 & 2(2-r) & r \\ 2 & 1 & 0 \\ 2-r & 2(r-1) & 3-r \end{bmatrix},$$

if M has another zero, then $r = 0, 1, 2$, or 3. Refer to the proof of theorem 2.9. $r = 0 \Rightarrow M(a, 0, -a)$ has 2 zeros and $r = 3 \Rightarrow M(a, 3a, 2a)$ which has two zeros by example 2.10. $M(a, ar, a(r-1))$ has exactly three zeros for $r = 1$ or $r = 2$.

We can check whether or not an integer is a quadratic residue by using the Rules of Legendre Symbols. For instance, when $r = 3$,

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

We previously showed that the elements $-2, -1, 0, 1, 2$, and 3 are all quadratic residues mod $168m + 1$.

To this point, we looked at how many entries of zero any M.S.S. admits. It is true that we can have exactly one entry of zero in this configuration. In the next subsection we examine how many entries of one M can admit. Tt

3.2 Number of Ones as Entries

For this section, we answer the question of how many entries of the number 1 the configuration $M(a, ar, a(r-1))$ may have. We show that we can either have exactly one entry of 1 fixed in the (2,2) position or three entries of 1 as demonstrated in the next proposition. Without loss of generality, we assume $a = 1$.

Proposition 3.2 *All M.S.S. in the form of $M(1, r, (r-1))$ must admit exactly three entries of 1, or a single entry of 1. It has 3 entries of 1 if and only if $r \in \{1, 2, 2^{-1}(3)\}$.*

Proof. By the setting $M(1, r, (r-1))$ has 1 as the middle entry. If more than one entry of 1 is achieved, then one of the elements $r-1, 2-r, r, 2(r-1)$, or $3-r$ is equal to 1. The resulting values for r are $1, 2$, or $2^{-1}(3)$. For $r = 1$,

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

For $r = 2$,

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

For $r = 2^{-1}(3)$,

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

Each of the three M.S.S. have exactly three entries of 1. Thus, all M.S.S. in the form of $M(1, r, (r-1))$ must contain three entries of 1, or a single entry of 1.

3.3 Number of Twos as Entries

In the configuration, we have a single 2 fixed in the (2,1) position. In addition to this single entry of 2, we can have two or three entries of 2 depending on what r is. The next proposition examines these possibilities.

Proposition 3.3 *Consider any M.S. in the configuration of $M(1, r, r-1)$. Then, M contains no more than three 2's as entries. In particular, M has exactly one entry of 2 if and only if $r \notin \{0, 1, 2, 3\}$. M has two entries of 2 when $r = 0$ or $r = 3$. M has three entries of 2 when $r = 1$ or $r = 2$.*

The proof for this proposition follows the same steps from proposition 3.1 and we attain the same r-values that differentiate the number of 2's.

Proof. From the proof of theorem 2.9, we see $M(1, 0, -1)$ and $M(1, 3, 2)$ have exactly two entries of 2 ($r = 0$ or $r = 3$). $M(1, 1, 0)$ and $M(1, 2, 1)$ have exactly three 2's ($r = 1$ and $r = 2$). If M has another entry of 2, then one of the following elements must equal 2: $r - 1$, $2(2 - r)$, r, $2 - r$, $2(r - 1)$ or $3 - r$. Ultimately, it implies $r \in \{0, 1, 2, 3\}$.

3.4 M.S.S. of Degrees < 9

A full degree M.S.S. is a degree 9 M.S.S. By theorem 1.8, when p is a prime ≥ 5, the degree of an M.S. (or M.S.S.) must be 3, 5, 7, or 9. In section 2, we showed that a full degree M.S.S. exists mod some prime numbers. Next, we show that for any prime number in the form of $p = 840m + 1, m \in \mathbb{Z}$, there are M.S.S. achieving the degrees of 3, 5 or 7.

Theorem 3.4 *Define* $S_0 = \{0, 1, 2, 3, 2^{-1}(3), 3^{-1}(4), 3^{-1}(5)\}$. *If M is an M.S.S. of degree 9, then $r \notin S_0$.*

Proof. Assume that $r \in S_0$. Then, by proposition 3.1, $M = M(a, ar, a(r - 1))$ produces two zeros if $r = 0$ or $r = 3$, three zeros if $r = 1$ or $r = 2$. It implies that $\deg(M) < 9$. Also, by proposition 3.2, if $r = 2^{-1}(3)$, then $\deg(M) < 9$ because M has three ones. When $r = 3^{-1}(4)$ or $r = 3^{-1}(5)$, M has two 2's shown in proposition 3.6. Therefore, if M is of degree 9, then $r \notin S_0$.

Remark 3.5 *For $M(a, ar, a(r-1))$ to be an M.S.S., we need all entries to be quadratic residues. In the previous proposition, we assumed that $r, r - 1, r - 2, r - 3$ are all quadratic residues. A natural question to ask is "For what values of r are the four consecutive numbers $r, r-1, r-2, r-3$ all quadratic residues modulo a given prime number?" We will answer this question in a later section.*

Theorem 3.6 *Let $p = 840m+1, m \in \mathbb{Z}$, be a prime. Let $S_0 = \{0, 1, 2, 3, 2^{-1}(3), 3^{-1}(4), 3^{-1}(5)\}$. If $r \in S_0$, then $M(a, ar, a(r - 1)) \in SS(\mathbb{Z}_p)$ and has degree 3, 5, or 7.*

Proof.

Let $r = 1$. Then,

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

Similarly, for $r = 2$. Then,

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

Note that the above two M.S. are isomorphic. Obviously, each M is an M.S. of degree 3.

Furthermore,

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

This is the only occurrence of a degree 5 M.S. given the values at hand. When $r = 0$ or $r = 3$, we obtain two isomorphic M.S. of degree 7. Note that this result can also be obtained by proposition 3.2:

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

For $r = 3^{-1}(4)$ or $r = 3^{-1}(5)$, M achieves degree 7.

$$M(1,3^{-1}(4),3^{-1}) = 3^{-1} \begin{bmatrix} 1 & 4 & 4 \\ 6 & 3 & 0 \\ 2 & 2 & 5 \end{bmatrix} \cong M(1,3^{-1}(5),3^{-1}(2)) = 3^{-1} \begin{bmatrix} 2 & 2 & 5 \\ 6 & 3 & 0 \\ 1 & 4 & 4 \end{bmatrix}.$$

In the last two M.S., two of the elements after factoring out 3^{-1} are 5 and 6. Since $6 = (2)(3)$ and $2, 3$ are quadratic residues, 6 is a quadratic residue. The element 5 is also a quadratic residue because $840 = 168 \cdot 5$; and after applying Legendre Symbols,

$$\left(\frac{5}{p}\right) = \left(\frac{5}{168 \cdot 5m + 1}\right) = \left(\frac{168 \cdot 5m + 1}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Therefore, if $r \in S_0$, M is an M.S.S. with a degree 3, 5, or 7.

If $M(a, ar, a(r-1))$ is of degree 9, then $r \notin S_0$. If $r \in \{0, 3, 3^{-1}(4), 3^{-1}(5)\}$, then we obtain an M.S.S. of degree 7 M.S.S. If $r \in \{1, 2\}$, then M.S.S. of degree 3 are produced. If $r = 2^{-1}(3)$, then we have a degree 5 M.S.S. In these constructions, we see that $r, r-1, r-2, r-3$ must be quadratic residues.

3.5 Quadruplets of Quadratic Residues

Previously, we showed that $M(a, ar, a(r-1))$ is an M.S.S for infinitely many primes p and certain integers r. Some of the construction of M.S.S. require the existence of four consecutive integers which are all quadratic residues mod a prime p. A natural question is: "For what values of r are the four consecutive numbers $r, r-1, r-2, r-3$ all quadratic residues?" We attempt to obtain some values of r which can do it.

Definition 3.7 *For a prime number p, say $B(r) = (r-3, r-2, r-1, r)$ is a quadruplet of quadratic residues if all $r-3, r-2, r-1, r$ are quadratic residues* mod p.

With this definition and all of the previously tested values for r, we give a set of quadruplets of quadratic residues mod primes of the form $168m+1$.

Proposition 3.8 *Let $S_1 = \{-7, -6, -1, 0, 1, 2, 3, 4, 9, 2^{-1}(3)\}$. Consider a prime number $p = 168m+1, m \in \mathbb{Z}$. Then $B(r)$ is a quadruplet of quadratic residues* mod p *whenever $r \in S_1$. Consequently, $M(a, ar, a(r-1))$ is an M.S.S. over $\mathbb{Z}_p$ for $r \in S_1$.*

Proof. It is obvious that 0, 1, 4 are quadratic residues mod p. In the proof of theorem 2.4, it is shown that $-1, 2, 3, 7$ are all quadratic residues mod p. Assume $r \in S_1$. We prove $B(r)$ is a quadruplet of quadratic residues.

For $r = 2^{-1}(3)$, we examine $r-1, r-2, r-3$ by the definition of $B(r)$: $2^{-1}(3) - 3 = 2^{-1}(3) - 2^{-1}(6) = -2^{-1}(3)$. Similarly, $2^{-1}(3) - 2 = -2^{-1}$ and $2^{-1}(3) - 1 = 2^{-1}$. So, $B(2^{-1}(3)) = 2^{-1}(-3, -1, 1, 3)$. For $M(a, ar, a(r-1))$ to be an M.S.S. over $\mathbb{Z}_p$, $-1, r, r-1, r-2, r-3$ all have to be quadratic residues in $\mathbb{Z}_p$.

For any $r \in S_1$ and $i = 0, 1, 2, 3$, $r - i \in \{-6, -1, 0, 1, 2, 3, 4, 5, 9, 2^{-1}(3)\}$ (see table 1). Thus, $B(r)$ is a quadruplet of quadratic residues. Previously, we gave the degree of $M(a, ar, a(r-1))$ for all $r \in S_1$.

Remark 3.9 *In table 1, there are only three cases of isomorphic M.S.: $M(1, 1, 0)$ with $M(1, 2, 1)$, $M(1, 0, -1)$ with $M(1, 3, 2)$, $M(1, -1, -2)$, and $M(1, -6, -7)$ with $M(1, 9, 8)$. Some pairs of M.S. with the same degree are not isomorphc. Table 1 shows that $M(1, r, r-1)$ can achieve all possible degrees 3, 5, 7, 9 taking $r \in S_0$. For instance; $B(-6)$, $B(4)$ and $B(9)$ yield degree 9*

M.S.S.; $B(-1)$, $B(0)$, and $B(3)$ yield degree 7 M.S.S.; and $B(1)$ and $B(2)$ both yield degree 3 M.S.S., and $B(2^{-1}(3))$ yields a degree 5 M.S.S.

Now, we consider a different prime $p = 840m + 1$, $m \in \mathbb{Z}$. Since $p \equiv 1 \bmod 4$, $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, and $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)$. But 3, 5, and 7 are divisors of 840. Then, $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$, $\left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1$, and $\left(\frac{p}{7}\right) = \left(\frac{1}{7}\right) = 1$. Therefore, 3, 5, and 7 are all quadratic residues mod p.

Let $S_2 = \{-7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 2^{-1}(3), 3^{-1}(4), 3^{-1}(5)\}$.

Proposition 3.10 *For any prime in the form of $p = 840m + 1$, $m \in \mathbb{Z}$, $B(r)$ is a quadruplet of quadratic residues whenever $r \in S_2$.*

Proof. We consider the elements $3^{-1}(4)$ and $3^{-1}(5)$ from the set S_2.

For $r = 3^{-1}(4)$; $r - 1 = 3^{-1}(4) - 1 = 3^{-1}(4) - 3^{-1}(3) = 3^{-1}$; $r - 2 = 3^{-1}(4) - 2 = -3^{-1}(2)$, and $r - 3 = 3^{-1}(4) - 3 = -3^{-1}(5)$. Hence, $B(3^{-1}(4)) = 3^{-1}(-5, -2, 1, 4)$.

For $r = 3^{-1}(5)$; $r - 1 = 3^{-1}(5) - 1 = 3^{-1}(5) - 3^{-1}(3) = 3^{-1}(2)$, $r - 2 = 3^{-1}(5) - 2 = -3^{-1}$, and $r - 3 = 3^{-1}(5) - 3 = -3^{-1}(4)$. It is obvious that $B(3^{-1}(5))$ is a quadruplet of quadratic residues mod p. For table 2, we list $B(r)$ with $r \in S_2$ and attain some additional pairs of M.S.S. that are isomorphic to each other in addition to the four aforementioned M.S.S.: $M(1, 3^{-1}(4), 3^{-1})$ with $M(1, 3^{-1}(5), 3^{-1}(2))$. In this case, we have six non-isomorphic M.S.S. mod $840m + 1$. Please note that $M(1, 2^{-1}(3), 2^{-1})$ is not isomorphic to any of the other $M(1, r, r - 1)$ in either Table 1 or 2. Consider the example below:

Example 3.11 *When $r = 1$ or $r = 2$,*

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

The above two M.S.S. are isomorphic to each other.

Example 3.12 *Degree 9 M.S.S. when $r = -7$ or $r = 10$.*

$$M(1,-7,-8) = \begin{bmatrix} -8 & 18 & -7 \\ 2 & 1 & 0 \\ 9 & -16 & 10 \end{bmatrix} \quad \text{is isomorphic to} \quad M(1,10,9) = \begin{bmatrix} 9 & -16 & 10 \\ 2 & 1 & 0 \\ -8 & 18 & -7 \end{bmatrix}.$$

Examples of M.S.S. of different degrees derived from $B(r)$ for $r \in S_2$ are summarized in Table 2. Here are the M.S.S. in detail.

Example 3.13 *$M(1,1,0)$ is a degree 3 M.S.S. built from elements of $B(1)$.*

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

Example 3.14 *An M.S.S. of degree 5 using elements from $B(2^{-1}(3))$:*

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

In spite of factoring out 2^{-1}, $B(2^{-1}(3)) = 2^{-1}(-3,-1,1,3)$. It produces an M.S.S. of degree 5.

Example 3.15 *When $r = 3^{-1}(4)$,*

$$M(1, 3^{-1}(4), 3^{-1}) = 3^{-1} \begin{bmatrix} 1 & 4 & 4 \\ 6 & 3 & 0 \\ 2 & 2 & 5 \end{bmatrix}.$$

Here, $B(3^{-1}(4)) = 3^{-1}(-5,-2,1,4)$ and $M(1, 3^{-1}(4), 3^{-1})$ is an M.S.S. of degree 7.

Example 3.16 *When $r = 4$,*

$$M(1,4,3) = \begin{bmatrix} 3 & -4 & 4 \\ 2 & 1 & 0 \\ -2 & 6 & -1 \end{bmatrix}$$

is a degree 9 M.S.S. where $B(4) = (1,2,3,4)$.

Throughout this section, we investigated different features of $M(a, ar, a(r-1))$. We learned that an M.S.S. over $\mathbb{Z}_p, p = 840m + 1$ can have a maximum of three entries of zero, either one or three entries of the number 1, and can achieve degrees 3, 5, 7, and 9 depending on different values of r. Furthermore, we discussed how certain values of r can yield a quadruplet of quadratic residues and which results in an isomorphic M.S.S. In the next section, we examine another configuration with another prime number and construct M.S.S. by this configuration.

4 M.S.S. of Type $L(r)$

For further sections, we will look at other configurations which are based on the basic definition of a magic square:

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

where $a, b, c \in \mathbb{Z}_p$ for some prime p. The matrix $M(a,b,c)$ as demonstrated above is the basic form of a magic square, we examine special configurations with specific numbers of a, b, c. This entire section over $\mathbb{Z}_p$ is based on this new configuration, called $L(r)$.

Definition 4.1 *Let $a = 1, b = r$, and $c = 3 + r$. Then, $M(a,b,c)$ becomes*

$$M(1,r,3+r) = L(r) = \begin{bmatrix} 3+r & -2r & r \\ -2 & 1 & 4 \\ 2-r & 2(r+1) & -(r+1) \end{bmatrix}.$$

We discuss for what values of r, $L(r)$ is an M.S.S. We show that $L(r)$ can achieve M.S.S. of degrees 3, 5, 7, and 9 among other similar ideas discussed in the previous section. Throughout this section, we let $p = 840m + 1$ be a prime number, $m \in \mathbb{Z}$. We are also interested in the appearance of the numbers 0, 1, -2, and 4 in any M.S.S. over $\mathbb{Z}_p$.

4.1 Number of Ones as Entries

In this configuration, the middle number is 1 (in the (2,2) position); but how many 1's can we have? The next proposition will answer this question.

Proposition 4.2 *$L(r)$ can only have three entries of 1 or one entry of 1. It contains three 1's if and only if $r \in \{1, -2, -2^{-1}\}$.*

Proof. If there is another entry of 1 in $L(r)$, then it must be $r, 3+r, -2r, 2-r, -(r+1)$, or $2(r+1)$. Each case gives $r = 1, r = -2$, or $r = -2^{-1}$. As shown below, $L(1), L(2)$ and $L(2^{-1})$ all contain three entries of one.

First, let $r = -2$. Then,

$$L(-2) = \begin{bmatrix} 1 & 4 & -2 \\ -2 & 1 & 4 \\ 4 & -2 & 1 \end{bmatrix}.$$

Similarly,

$$L(-2^{-1}) = \begin{bmatrix} 2^{-1}(5) & 1 & -2^{-1} \\ -2 & 1 & 4 \\ 2^{-1}(5) & 1 & -2^{-1} \end{bmatrix}, \quad L(1) = \begin{bmatrix} 4 & -2 & 1 \\ -2 & 1 & 4 \\ 1 & 4 & -2 \end{bmatrix}.$$

Thus, $L(r)$ has only three 1's if and only if $r \in \{1, -2, -2^{-1}\}$ mod $p = 840m + 1$.

Note that here, by example 2.10, $1, 2, 4, -2, 2^{-1}5, 2^{-1}$ are all quadratic residues, so $L(-2)$, $L(-2^{-1})$, and $L(1)$ are all M.S.S. In particular, $L(-2)$ is of degree 3 and is isomorphic to $L(1)$. $L(-2^{-1})$ is of degree 5.

4.2 Number of Zeros As Entries

In the previous section, all M.S.S. mod $p = 840m + 1$ constructed have either one zero or three zeros. In the next proposition, we show that $L(r)$ can not have more than two zero entries. depending on what r is.

Proposition 4.3 *Modulo any prime $p = 840m + 1$, $L(-3)$, isomorphic to $L(2)$, are M.S.S. and have one zero. $L(0)$, isomorphic to $L(1)$, are M.S.S. and have two zeros. Otherwise, if $r \notin \{2, 0, -1, -3\}$, then $L(r)$ has no zero entries.*

Proof. By the structure of $L(r)$, if zero is an element, then we must have $3 + r, r + 1, 2 - r$ or $r = 0$ which implies $r = 0, -1, 2$ or -3.

$$L(-3) = \begin{bmatrix} 0 & 6 & -3 \\ -2 & 1 & 4 \\ 5 & -4 & 2 \end{bmatrix} \cong L(2) = \begin{bmatrix} 5 & -4 & 2 \\ -2 & 1 & 4 \\ 0 & 6 & -3 \end{bmatrix}.$$

Hence, $L(-3)$ and $L(2)$ has a single entry of zero and both M.S. are of degree 9.

$$L(0) = \begin{bmatrix} 3 & 0 & 0 \\ -2 & 1 & 4 \\ 2 & 2 & -1 \end{bmatrix} \cong L(-1) = \begin{bmatrix} 2 & 2 & -1 \\ -2 & 1 & 4 \\ 3 & 0 & 0 \end{bmatrix}$$

Thus, $L(0)$ and $L(-1)$ have two entries of zero. Additionally, both M.S. above are of degree 7.

If $r \notin \{2, 0, -1, -3\}$, then $L(r)$ will not have any zero entries.

4.3 Number of Fours as Entries

Notice that in $L(r)$, there is a number 4 fixed in the (2,3) position. That is why we examine different possibilities of resulting fours in other places.

Proposition 4.4 *$L(r)$ has more than one 4 as entries if and only if $r \in \{-5, -2, 1, 4\}$.*

Proof. Obviously, $L(1)$ and $L(2)$ has three entries of 4.

$$L(1) = \begin{bmatrix} 4 & -2 & 1 \\ -2 & 1 & 4 \\ 1 & 4 & -2 \end{bmatrix} \cong L(-2) = \begin{bmatrix} 1 & 4 & -2 \\ -2 & 1 & 4 \\ 4 & -2 & 1 \end{bmatrix}.$$

Also, $L(4)$ and $L(-5)$ have two entries of 4 and are isomorphic to each other .

$$L(4) = \begin{bmatrix} 7 & -8 & 4 \\ -2 & 1 & 4 \\ -2 & 10 & -5 \end{bmatrix} \cong L(-5) = \begin{bmatrix} -2 & 10 & -5 \\ -2 & 1 & 4 \\ 7 & -8 & 4 \end{bmatrix}.$$

For any r, if $L(r)$ has more than one entry of 4, then one of the following is true: $r = 4, 3 + r = 4, -2r = 4, 2 - r = 4, 2(r + 1) = 4$, or $-(r + 1) = 4$. It implies that $r \in \{-5, -2, 1, 4\}$.

4.4 Number of -2 as Entries

In this configuration, $L(r)$ has an entry of -2 at the (2,1) position. However, another -2 may appear in other places. The next proposition answers the question of how many entries of -2 we can have for certain r-values.

Proposition 4.5 *$L(r)$ has more than one entry of -2 if and only if $r \in \{-5, 4, -2, 1\}$. Furthermore, $L(-5)$, isomorphic to $L(4)$, has two entries of -2 and $L(-2)$, isomorphic to $L(1)$, has three entries of -2.*

Proof. If there is another entry of -2 in $L(r)$, then it must be one of the following: $r, -2r, 3+r, 2-r, 2(r-1)$, or $-(r+1)$. Each case gives $r = -5, r = 1, r = -2$, or $r = 4$. It is obvious that if $r \notin \{-5, 4, -2, 1\}$, then $L(r)$ has only one entry of -2. As shown in the next matrices, $L(-5)$ has two entries of -2 and $L(1)$ has three entries of -2.

$$L(-5) = \begin{bmatrix} -2 & 10 & -5 \\ -2 & 1 & 4 \\ 7 & -8 & 4 \end{bmatrix} \cong \quad L(4) = \begin{bmatrix} 7 & -8 & 4 \\ -2 & 1 & 4 \\ -2 & 10 & -5 \end{bmatrix}.$$

$$L(1) = \begin{bmatrix} 4 & -2 & 1 \\ -2 & 1 & 4 \\ 1 & 4 & -2 \end{bmatrix} \cong \quad L(-2) = \begin{bmatrix} 1 & 4 & -2 \\ -2 & 1 & 4 \\ 4 & -2 & 1 \end{bmatrix}.$$

4.5 M.S.S. of Degree 9 Derived From $L(r)$

In this section, we construct M.S.S. of degree 9. In order to construct these M.S.S., we define a new set $S_3 = \{-1, -5, -2, 1, -2^{-1}, 0, 4\}$.

Theorem 4.6

- *Let $p = 840m + 1$ be a prime number and $r \in S_3$. Then, $L(r)$ is an M.S.S. of degree < 9 over $\mathbb{Z}_p$. Furthermore,* $\deg(L(1)) = \deg(L(-2)) = 3$, $\deg(L(-2^{-1})) = 5$ *and* $\deg(L(0)) = \deg(L(-5)) = \deg(L(4)) = \deg(L(-1)) = \deg(L(0)) = 7$.
- *There exists $r \notin S_3$ such that $L(r)$ is an M.S.S. of degree 9.*

The proof for this theorem follows a similar process as that of theorem 3.4.

Proof. Suppose $r \in S_3$. We will show that $L(r)$ is an M.S.S. of degree less than 9 shown before.

For example, $L(0), L(1)$ have degree 7. It remains to check $r = -5$ and $r = 4$.

$$L(4) = \begin{bmatrix} 7 & -8 & 4 \\ -2 & 1 & 4 \\ -2 & 10 & -5 \end{bmatrix}, \quad L(-5) = \begin{bmatrix} -2 & 10 & -5 \\ -2 & 1 & 4 \\ 7 & -8 & 4 \end{bmatrix}.$$

Both of these M.S. are degree 7. In fact, $L(4)$ and $L(-5)$ are M.S.S. as each element including 5 and 7 are quadratic residues mod $840m + 1$. Hence, if $r \in S_3$, then $L(r)$ is an M.S.S. of degree less than 9; or, if $L(r)$ is an M.S.S. of degree 9, then $r \notin S_3$.

Now, let $r = 2$ or $r = -3$; $2, -3 \notin S_3$. Then,

$$L(2) = \begin{bmatrix} 5 & -4 & 2 \\ -2 & 1 & 4 \\ 0 & 6 & -3 \end{bmatrix}, \quad L(-3) = \begin{bmatrix} 0 & 6 & 3 \\ -2 & 1 & 4 \\ 5 & -4 & 2 \end{bmatrix}.$$

$L(2)$ and $L(-3)$ are both M.S,S, of degree 9.

Though the results are different than those in the previous section, the idea is the same. The degrees for this configuration are 3, 5, 7, and 9.

5 M.S.S. of Type $U(r)$

Let $p = 9240m + 1$ be a prime number. From the general form of a magic square, that is,

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

we derive our last configuration.

Definition 5.1 *Let $a = 1, b = 2$, and $c = r$. Then, $M(a, b, c)$ becomes the following magic square:*

$$U(r) = \begin{bmatrix} r & 1 - r & 2 \\ 3 - r & 1 & r - 1 \\ 0 & 1 + r & 2 - r \end{bmatrix}.$$

Similar to the other two configurations, we show that $U(r)$ can achieve M.S.S. of 3, 5, 7, and 9.

5.1 Number of Zeros as Entries

The entries of 0, 1, and 2 sit on the minor diagonal of the magic square represented by $U(r)$. In this configuration, we can have at most three zero entries. The proposition below best explains what values can gives us these entries.

Proposition 5.2 *Modulo any prime $p = 9240m + 1$, $U(0), U(2), U(3)$, and $U(-1)$ all contain two entries of 0 and $U(1)$ contains three entries of zero. When $r \notin \{-1, 0, 1, 2, 3\}$, $U(r)$ has only one entry of zero.*

Proof. By the structure of $U(r)$, if there are more than one zero as an entry, then we must have $r = -1, 0, 1, 2$, or 3. $U(1)$ contains 3 zeros:

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

$U(0), U(2), U(3)$, and $U(-1)$ all contain two entries of 0:

$$U(0) = \begin{bmatrix} 0 & 1 & 2 \\ 3 & 1 & -1 \\ 0 & 1 & 2 \end{bmatrix}, \quad U(2) = \begin{bmatrix} 2 & -1 & 2 \\ 1 & 1 & 1 \\ 0 & 3 & 0 \end{bmatrix},$$

$$U(3) = \begin{bmatrix} 3 & -2 & 2 \\ 0 & 1 & 2 \\ 0 & 4 & -1 \end{bmatrix}, \quad U(-1) = \begin{bmatrix} -1 & 2 & 2 \\ 4 & 1 & -2 \\ 0 & 0 & 3 \end{bmatrix}.$$

5.2 Number of Ones as Entries

In this configuration, the middle number (in the $(2,2)$ position) is 1. So $U(r)$ has at least one entry of 1. The proposition determines the number of entries of 1.

Proposition 5.3 *$U(r)$ can either have exactly three entries of 1 or a single entry of 1. It contains exactly three entries of 1 if and only if $r \in \{0, 1, 2\}$.*

Proof. If there is another entry of 1 in $U(r)$, then it must be $r, 1-r, 3-r, r-1, 1+r$, or $2-r$. Each case gives us the following results: $r = 0, r = 2, r = 1$. As shown below, $U(0), U(1)$ and $U(2)$ all contain three entries of 1:

$$U(0) = \begin{bmatrix} 0 & 1 & 2 \\ 3 & 1 & -1 \\ 0 & 1 & 2 \end{bmatrix}, \quad U(1) = \begin{bmatrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix}, \quad U(2) = \begin{bmatrix} 2 & -1 & 2 \\ 1 & 1 & 1 \\ 0 & 3 & 0 \end{bmatrix}.$$

$U(r)$ either contains exactly one entry of 1 or three entries of 1. Additionally, $U(r)$ contains three entries of 1 if and only if $r \in \{0, 1, 2\}$.

5.3 Number of Twos as Entries

Recall that $p = 9240m + 1$. Note that the entry 2 is fixed in the $(1, 3)$ position of $U(r)$. However we can have other entries of 2 as with 0 or 1.

Proposition 5.4 *For every $r \in \mathbb{Z}_p$, $U(r)$ can have a maximum of three entries of 2. Furthermore, $U(r)$ has exactly one 2 if and only if $r \notin \{-1, 0, 1, 2, 3\}$.*

Proof. If there are additional entries of 2, then 2 is equal to one of the following elements: $r, 1-r, 3-r, r-1, 1+r$, or $2-r$ which implies $r \in \{-1, 0, 1, 2, 3\}$. Thus, when $r \notin \{-1, 0, 1, 2, 3\}$, we are guaranteed to have only one entry of 2. For $r \in \{-1, 0, 2, 3\}$, $U(r)$ has exactly two entries of 2.

$$U(-1) = \begin{bmatrix} -1 & 2 & 2 \\ 4 & 1 & -2 \\ 0 & 0 & 3 \end{bmatrix}, \quad U(0) = \begin{bmatrix} 0 & 1 & 2 \\ 3 & 1 & -1 \\ 0 & 1 & 2 \end{bmatrix},$$

$$U(2) = \begin{bmatrix} 2 & -1 & 2 \\ 1 & 1 & 1 \\ 0 & 3 & 0 \end{bmatrix}, \quad U(3) = \begin{bmatrix} 3 & -2 & 2 \\ 0 & 1 & 2 \\ 0 & 4 & -1 \end{bmatrix}.$$

When $r = 1$,

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

gives three entries of 2.

Therefore, we are guaranteed at most three entries of 2. The values $r = -1, 0, 2, 3$ give two entries of 2 and the value $r = 1$ gives three entries of 2. For $r \notin \{-1, 0, 1, 2, 3\}$, $U(r)$ contains exactly one 2.

5.4 M.S.S. of Degree 9 derived from $U(r)$

Let S_4=$\{0, 1, 2, 3, 2^{-1}, 2^{-1}(3), -1\}$. Recall throughout this section that some r-values make $U(r)$ a magic square of squares. In this section, we examine what r-values can produce an M.S.S. of a given degree.

Theorem 5.5

- *Let $p = 9240m + 1$ be a prime number and $r \in S_4$. Then, $U(r)$ is an M.S.S. of degree < 9 over $\mathbb{Z}_p$. Furthermore $\deg(U(r)) = 3$ if $r = 1$, $\deg(U(r)) = 5$ if $r = 0$ and $r = 2$, and $\deg(U(r)) = 7$ if $r = 3, r = -1, r = 2^{-1}$, and $r = 2^{-1}(3)$. If $U(r)$ is of degree 9, then $r \notin S_4$.*
- *There exists an M.S.S. of degree 9* mod p.

Proof. Suppose $r \in S_4$. We will show that $U(r)$ is an M.S.S. of degree less than 9. By the proofs of propositions 5.2, 5.3 and 5.4, $U(0)$ and $U(2)$ have degree 5. Additionally, $U(1)$ is the only M.S.S. of degree 3. Finally, $U(3)$ and $U(-1)$ are both of degree 7. Subsequently, $U(2^{-1})$ and $U(2^{-1}(3))$ both remain to be checked.

$$U(2^{-1}) = 2^{-1}\begin{bmatrix} 1 & 1 & 4 \\ 5 & 2 & -1 \\ 0 & 3 & 3 \end{bmatrix} \cong U(2^{-1}(3)) = 2^{-1}\begin{bmatrix} 3 & -1 & 4 \\ 3 & 2 & 1 \\ 0 & 5 & 1 \end{bmatrix}.$$

Both of these M.S. are degree 7. Also $U(2^{-1})$ and $U(2^{-1}(3))$ are both M.S.S. as each element is a quadratic residue mod $9240m + 1$ as well as a multiple of 9240. From the above, if $U(r)$ is an M.S.S. of degree 9, then $r \notin S_4$. Now, we choose $r \notin S_4$, say, $r \in \{-3, 4\}$. Then, we have the following:

$$U(-3) = \begin{bmatrix} -3 & 4 & 2 \\ 6 & 1 & -4 \\ 0 & -2 & 5 \end{bmatrix}, \quad U(4) = \begin{bmatrix} 4 & -3 & 2 \\ -1 & 1 & 3 \\ 0 & 5 & -2 \end{bmatrix}.$$

Hence, $U(-3)$ and $U(4)$ are M.S.S. of degree 9 over $\mathbb{Z}_p$ as each entry are all quadratic residues.

Similar to $L(r)$, $U(r)$ achieves the degrees of 3, 5, 7, and 9 and when $r \in S_4$ or $r = 3$ or $r = 4$, $U(r)$ are M.S.S. over $\mathbb{Z}_p$.

5.5 Quadruplets of Quadratic Residues $\bmod 9240m + 1$

Recall from section 3 that $B(r) = (r-3, r-2, r-1, r)$ denotes a quadruplet of quadratic residues. We have the following proposition:

Proposition 5.6 *Let $S_5 = \{0, 1, 2, 3, 2^{-1}, 2^{-1}(3), -1\}$. Consider the prime number $p = 9240m+1, m \in \mathbb{Z}$. Then, $B(r)$ is a quadruplet of quadratic residues* mod *p whenever $r \in S_5$.*

Proof. Assume $r \in S_5$.

For $r = 2^{-1}(3)$, we examine $r-1, r-2, r-3$ by the definition of $B(r)$: $2^{-1}(3) - 1 = 2^{-1}(3) - 2^{-1}(2) = 2^{-1}$. Similarly, $2^{-1}(3) - 2 = -2^{-1}$ and $2^{-1}(3) - 3 = -2^{-1}(3)$. Shown in table 4, the values of $B(r)$ when $r \in S_5$ are as follows: $-4, -3, -2, -1$, 0, 1, 2, 3, $-2^{-1}(5), -2^{-1}(3), -2^{-1}, 2^{-1}$, and $2^{-1}(3)$. Obviously, the values $0, \pm 1, \pm 2, \pm 3$, and ± 4 are quadratic residues mod p. We need to check whether the element 5 is a quadratic residue using Legendre Symbols.

$$\left(\frac{5}{9240m+1}\right) = \left(\frac{9240m+1}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Thus, $B(r)$ is a quadruplet of quadratic residues mod p whenever $r \in S_5$. Note that in $U(r)$, we need $r + 1$ to be a quadratic residue mod $p = 9240m + 1$. The quadruplet of quadratic residues in table 4 produce M.S.S. because $r + 1$ is a quadratic residue in $\mathbb{Z}_p$. For $L(r)$, the quadruplet of quadratic residues in table 3 produce M.S.S. in the similar way.

6 Conclusions

Throughout this thesis, we construct several types of M.S.S. using different positive integers modulo certain prime numbers p of the form $am + 1, a \in \mathbb{N}, m \in \mathbb{Z}$ by Dirichlet's theorem such that there are infinitely many primes. We show that modulo these selected prime numbers, there exist M.S.S. of all possible degrees, i.e. 1, 2, 3, 5, 7, and 9. In each considered configuration, we investigate the number of appearances of special values in an M.S.S. For example, in one configuration, we show that a maximum of three entries of 0, 1, and 2 can appear. Similarly, $L(r)$ has a maximum of 3 entries of -2 and 4. In addition to examining degrees of M.S.S. and special values in each configuration, we study what values of $r, r-1, r-2$ and $r-3$ give us a quadruplet of quadratic residues and how we can apply them to construct M.S.S. of a desired degree. This research answers the question of whether a 3×3 magic square can be constructed using nine distinct perfect squares in a different, but similar setting. Many questions remain to be answered. For example, how many non-isomorphic M.S.S. are there modulo a fixed prime number? Two thousand years later, the magic squares problem will remain to be "more than magic." They will continue to serve as a foundation to other games, puzzles, and other concepts in the field of applied mathematics.

References

[1] Hengveld, Stewart, "Magic Square of Squares over Certain Finite Fields", Master Thesis, Montclair State University, 2012.

[2] Drew O'Neill, "Magic Squares of Squares of Order 4 Over Certain Finite Fields", Master Thesis, Montclair State University, 2013.

[3] Cox, David A. and Little, John and O'Shea, Donald, *Using Algebraic Geometry*, Berlin-Heidelberg-New York, 2nd Edition, 2005.

[4] Strayer, James K., *Elementary Number Theory*, Waveland Press, Illinois, 2002.

[5] Small, Charles, *Magic Squares over Fields*, The American Mathematical Monthly, Vol. 95, No 7, 1988, 621-625.

[6] Boyer, Christian, *Some Notes on the Magic Squares of Squares Problem*, The Mathematical Intelligencer, Vol 27, No 2, 2005, 52-64.

[7] Andrew Bremner, *On squares of squares*, Acta Arithmetica, 88(1999) 289-297

[8] Andrew Bremner, *On squares of squares II*, Acta Arithmetica, 99(2001) 289-308

[9] Cleve Moler, *Experiments with MATLAB* October 2, 2011 *Chapter 10: Magic Squares*

[10] Boyer, Christian, Multimagic Squares
http://www.multimagie.com/English/SquaresOfSquaresSearch.htm

[11] NCTM Illuminations: Magic Squares
http://illuminations.nctm.org/LessonDetail.aspx?id=L263

[12] *http://www.pballew.net/magsquar.html*

[13] *http://en.wikipedia.org/wiki/Magic_square*

r	$B(r)$	$\deg(M(1, r, r-1))$
-7	$(-10, -9, -8, -7)$	10
-6	$(-9, -8, -7, -6)$	9
-1	$(-4, -3, -2, -1)$	7
0	$(-3, -2, -1, 0)$	7
1	$(-2, -1, 0, 1)$	3
2	$(-1, 0, 1, 2)$	3
$2^{-1}(3)$	$2^{-1}(-3, -1, 1, 3)$	5
3	$(0, 1, 2, 3)$	7
4	$(1, 2, 3, 4)$	9
5	$(2, 3, 4, 5)$	9
6	$(3, 4, 5, 6)$	9
7	$(4, 5, 6, 7)$	9
8	$(5, 6, 7, 8)$	9
9	$(6, 7, 8, 9)$	9

Table 1: Quadruplet Table for $M(r)$ mod $p = 168m + 1$

r	$B(r)$	$\deg(M(1,r,r-1))$
-7	$(-10,-9,-8,-7)$	9
-6	$(-9,-8,-7,-6)$	9
-5	$(-8,-7,-6,-5)$	9
-4	$(-7,-6,-5,-4)$	9
-3	$(-6,-5,-4,-3)$	9
-2	$(-5,-4,-3,-2)$	9
-1	$(-4,-3,-2,-1)$	7
0	$(-3,-2,-1,0)$	7
1	$(-2,-1,0,1)$	3
2	$(-1,0,1,2)$	3
3	$(0,1,2,3)$	7
4	$(1,2,3,4)$	9
5	$(2,3,4,5)$	9
6	$(3,4,5,6)$	9
7	$(4,5,6,7)$	9
8	$(5,6,7,8)$	9
9	$(6,7,8,9)$	9
$2^{-1}(3)$	$2^{-1}(-3,-1,1,3)$	5
$3^{-1}(4)$	$3^{-1}(-5,-2,1,4)$	7
$3^{-1}(5)$	$3^{-1}(-4,-1,2,5)$	7

Table 2: Quadruplet Table for $M(r)$ mod $p = 840m + 1$

r	$B(r)$	$\deg(L(r))$
-3	$(-6,-5,-4,-3)$	9
-1	$(-4,-3,-2,-1)$	7
-5	$(-8,-7,-6,-5)$	7
-2	$(-5,-4,-3,-2)$	3
1	$(-2,-1,0,1)$	3
-2^{-1}	$-2^{-1}(7,5,3,1)$	5
0	$(-3,-2,-1,0)$	7
4	$(1,2,3,4)$	7
7	$(4,5,6,7)$	9
2	$(-1,0,1,2)$	9

Table 3: Quadruplets of Quadratic Residues in $L(r)$ mod $p = 840m + 1$

r	$B(r)$	$\deg(U(r))$
-3	$(-6,-5,-4,-3)$	9
-1	$(-4,-3,-2,-1)$	7
0	$(-3,-2,-1,0)$	5
1	$(-4,-3,-2,-1)$	3
2	$(-1,0,1,2)$	5
3	$(0,1,2,3)$	7
2^{-1}	$2^{-1}(-5,-3,-1,1)$	7
$2^{-1}(3)$	$2^{-1}(-3,-1,1,3)$	7
4	$(1,2,3,4)$	9

Table 4: Quadruplets in $U(r)$ mod $p = 9240m + 1$