Montclair State University

Montclair State University Digital Commons

Theses, Dissertations and Culminating Projects

5-2012

Construction and Analysis of Magic Squares of Squares over Certain Finite Fields

Stewart Hengeveld

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

Part of the Mathematics Commons

MONTCLAIR STATE UNIVERSITY

/ Construction and Analysis of Magic Squares of Squares over Certain Finite Fields /

by

Stewart Hengeveld

A Master's Thesis Submitted to the Faculty of

Montclair State University

In Partial Fulfillment of the Requirements

For the Degree of

Master of Mathematics

May 2012

College of Science and Mathematics

Department of Mathematics

Certified by:

[redacted]

Dr. Robert Prezant
Dean of College

May 3, 2012

Date

Thesis Committee:

[redacted]

Dr. Aihua Li
Thesis Sponsor

[redacted]

Dr. Jonathan Cutler
Committee Member

[redacted]

Dr. William Parzynski
Committee Member

[redacted]

Dr. Helen M. Roberts
Department Chair

Abstract

This thesis presents results of the research on the study of Magic Squares of Squares over certain finite fields. The research is motivated by an open question, which is still not answered: "Does there exist a 3×3 magic square with all nine entries being distinct perfect squares of integers?" Instead of directly trying to answer this challenging question, this research attempts to answer a parallel question: "Does there exist a 3×3 magic square with all nine entries being distinct perfect squares modulo a prime number p?" Equivalently, the question can be restated as, "Does there exist a 3×3 magic square with all nine entries being distinct quadratic residues of a prime number p?" It is shown in this thesis that the answer is "Yes" for some primes such as 29 and 59, but "No" for many other primes like 17 and 19.

Consider a prime number p and the finite field $\mathbb{Z}_p$. The focus of this research is on the existence, analysis, and construction of the magic squares of squares made of quadratic residues of p from $\mathbb{Z}_p$. The main results show that such a magic square of squares can only use an odd number of distinct quadratic residues of p when $p > 2$. Furthermore, when $p > 3$, there exist magic squares of squares over $\mathbb{Z}_p$ with 3 distinct entries. When $p \equiv 1 \mod 8$, there exist magic squares of squares over $\mathbb{Z}_p$ made of five distinct quadratic residues of p. Existence of magic squares of squares over $\mathbb{Z}_p$ made of seven or nine distinct numbers is also discussed. Investigation has been done toward answering the question: "What is the maximum number of distinct quadratic residues of p that a magic square of squares over $\mathbb{Z}_p$ can admit?"

Chapter 6 of the thesis contains results from a related educational project. Through an MSU GK-12 program funded by NSF (*Award #0638708*), the author introduced magic squares and the mathematics involved in finding them to middle school students as a part of the project "Integrating Graduate Research into Middle School Classrooms". The findings are given in this chapter.

CONSTRUCTION AND ANALYSIS OF MAGIC SQUARES OF SQUARES OVER CERTAIN FINITE FIELDS

A THESIS

Submitted in partial fulfillment of the requirements
for the degree of Masters in Mathematics

by

Stewart Hengeveld
Montclair State University
Montclair, NJ
2012

Acknowledgments

Most importantly, I would like to thank my entire family for their continued support and advice in pursuing my academic goals.

I offer special thanks to my advisor, Dr. Aihua Li, for her many hours of patience on my unique writing habits, proof and public speaking skills. She has guided me to become a better all around mathematician. Her guidance through my undergraduate and graduate studies at Montclair State University is greatly appreciated.

I would also like to thank Dr. William Parzynski, whose door has always been open for students to stop in and chat. I have found his support, encouragement and advice, both inside and outside the classroom invaluable. I thank him for serving on my thesis committee and reviewing my thesis.

Also, I would like to thank Dr. Jonathan Cutler, who has been always helpful and available to answer any question. I thank him for reviewing my thesis and being on my thesis committee.

Special thanks to all my classmates and professors at Montclair State University. Their support and help through the years of classes and projects are greatly appreciated.

I want to extend thanks to the National Science Foundation and the GK-12 program, run by Dr. Mika Munakata, Dr. Ken Wolf, and Dr. Mary Lou West, for partially funding this research.

Furthermore, I would like to thank the other GK-12 graduate fellows and the teachers associated with the program, especially Miguel Marques and Elaine McCarthy from Schuyler Middle School in Kearny, New Jersey, and my GK-12 partner Diana Sanchez.

Finally, I would like to specifically thank Emel Demirel for her continued help, support, and love through all the years.

Contents

1 History and Introduction of the Magic Square Problem

The topic of Magic Squares presents an intriguing problem in recreational mathematics. These mathematical puzzles have been part of the history of many civilizations. Cultural influences can be seen in China, India, Arabia, Persia, and Europe. In these civilizations, Magic Squares were thought to have magical, mystical, or religious properties.

The first recorded historical instance of a Magic Square was found in China from around 2,200 B.C., the time of the Chinese Emperor Yu. A simple 3×3 Magic Square was constructed, which used the numbers 1 through 9, such that all rows, columns, and diagonals sum to 15. This magic square, known as the Lo Shu square, had many connections to Chinese mythology and numerology. For example, the patterns of the Lo Shu square were thought to reflect the flooding pattern of the Lo river. Magic Squares were also believed to have had mystical powers. In early modern Europe, a magic square is found on the exterior of the Sagrada Familia church in Barcelona. This magic square has the Magic Sum 33, the age of Jesus Christ at the time of his crucification, The Magic Square puzzle has attracted

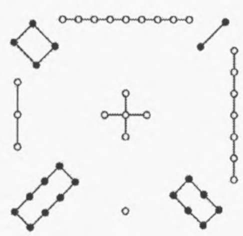

Figure 1: Lo Shu Magic Square

individuals such as Benjamin Franklin, Leonhard Euler, Arthur Cayley, Edouard Lucas, John Conway, and Martin LaBar. They have all contributed towards the construction and properties of Magic Square puzzles. Among many existing results about the solutions of Magic Squares, it is the modern work and questions posed by Martin LaBar [7] and the work of Lucas from the middle 1800's that this paper will focuses on.

The Magic Square Problem

Magic Squares of size n can be represented by $n \times n$ matrices of numbers from a ring, where all rows, columns and diagonals sum to the same number, known as the Magic Constant (Magic Sum). If all the entries are chosen from 1 to n^2 (n is a positive integer), then the Magic Square is considered to be Normal.

Constructing Magic Squares of different dimensions has been an interesting topic that has attracted many mathematicians. While it is easy to guess and check small ones, generating higher dimensional Magic Squares is time consuming. The Siamese method has been used to simplify the construction into a step by step process. (See Appendix C)

The following are two examples of Magic Squares, the first of which is normal.

Example 1.1. *A three dimensional Magic Square with Magic Constant* $C = 15$ *is as below:*

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

The second example was created in a seventh grade classroom using methods discussed later.

Example 1.2. *A three dimensional Magic Square with Magic Constant* $C = 127,026$*:*

$$\begin{bmatrix} 38,097 & 46,929 & 42,000 \\ 46,245 & 42,342 & 38,439 \\ 42,684 & 37,755 & 46,587 \end{bmatrix}.$$

Both examples show an interesting relationship between the center entry and the Magic Constant. In Example 1.1, $3(5) = 15 = C$. And in Example 1.2, $3(42,342) = 127,026 = C$. It is suggesting that all 3×3 magic squares may follow the same rule: the center entry times three is the Magic Sum. This relationship between the center entry and the magic sum in a 3×3 magic square is a known result and a simple proof by using a different algebraic method will be shown later.

The main focus of this paper lies in the following open question, as stated in 1984 by Martin LaBar. The question was restated in 1996 by Martin Gardner, offered \$100 for a solution to the problem. As we will see, it is a very interesting and difficult problem to solve and analyze.

The question was restated below.

Question 1.3 (Still Open)**.** *Can a* 3×3 *Magic Square be constructed using 9 distinct perfect squares?*

Instead of trying to answer this question directly, I shift my attention to a similar, yet mostly neglected question:

Question 1.4. *Can a* 3×3 *Magic Square be constructed using 9 distinct perfect squares from a finite field?*

In this paper, I focus on the finite field $\mathbb{Z}_p$, where p is a prime number, and $n = 3$. The existence and structures of Magic Square of Squares with nine distinct numbers from $\mathbb{Z}_p$ is discussed. The main results provide full or partial answers to the following questions:

1. For what prime numbers p, there exists a Magic Square of Squares of order 3 which uses nine distinct perfect squares from $\mathbb{Z}_p$?

2. For a positive integer r, $1 < r \leq 9$, are there Magic Square of Squares of order 3 using exactly r perfect squares from $\mathbb{Z}_p$? If such a Magic Square of Squares exists, how many of them are there ?

3. How do we construct a Magic Square of Squares of order 3 over $\mathbb{Z}_p$ which has the desired number of distinct perfect squares in $\mathbb{Z}_p$?

4. What is the general structure of a Magic Square of Square of order 3 in $\mathbb{Z}_p$ for a specific prime number p?

2 Computational and Analytical Methods

The following definitions are the basis for the rest of the thesis. From now on the Magic Square of Squares problem will be refered as the "M.S.S. problem" and an M.S.S. is refered as a "solution".

Definition 2.1. *Let k be positive integers, p be a prime number, and R be a ring. We define*

1. $S_0 = \{$*All M.S.S. of order 3 over* $\mathbb{Z}\}$ *and*
   $S_p = \left\{\text{All M.S.S. of order 3 over } \mathbb{Z}_p\right\}$
2. $M_3(R)$ *to be the set of all* $n \times n$ *matrices over R.*
3. *the* k^{th} *symbolic power of A by* $A^{(k)} = \left[a_{ij}^k\right]$*, where* $A = \left[a_{ij}\right] \in M_3(R)$.
4. $\vec{C} = [C, \ldots, C]^T$ *is an 8 dimensional vector where* $C \in R$ *and T is the matrix transpose.*

$\vec{C}$ has 8 dimensions because a degree 3 magic square has 3 row sums, 3 column sums and 2 diagonal sums.

One way to analyze the M.S.S. problem is to use its matrix form. The following definition is for Magic Squares of size 3.

Definition 2.2. *(Matrix form of a Magic Square) Let* $A = \left[a_{ij}\right] \in M_3(R)$. *Say A is a magic square over R of order 3 with magic constant C if the following are satisfied.*

$$\sum_{i=1}^{3} a_{ij} = C = \sum_{j=1}^{3} a_{ij} \qquad \text{and} \qquad \sum_{i=1}^{3} a_{ii} = C = \sum_{i=1}^{3} a_{i(4-i)}.$$

The following is a summary of the main characteristics of order 3 M.S.S. These characteristics help in classifying the solutions in S_p, predicting existence of non trivial M.S.S. in S_p, and finding the structural properties of them. The ring in consideration is be $R = Z_p$, where p is prime.

Definition 2.3. *Let* $M \in S_p$. *Define the degree of M to be the number of distinct entries in M, denoted by* $\deg(M)$. *The maximal degree of all M.S.S. solutions over* S_p *is called the M.S.S. number of* S_p, *denoted by* $\alpha(S_p)$. *That is*

$$\alpha(S_p) = max\left\{\deg(M) \mid M \in S_p\right\}.$$

Using the above notions, the original problem can be expressed in the following equivalent forms.

Remark 2.4. *Consider* 3×3 *M.S.S. and let* S_p *be as above (order 3). The following questions are equivalent.*

1. *Can one construct a* 3×3 *Magic Square, where all entries are distinct perfect squares over the finite field* $\mathbb{Z}_p$?

2. *Does there exist an M.S.S. solution M in S_p such that* $\deg(M) = 9$?

3. *Is* $\alpha(S_p) = 9$?

A related questions can be asked: "What values can $\alpha(S_p)$ take?"

Analyzing the Matrix form of M.S.S.

Now, viewing the problem as a matrix problem, a "sum" vector is defined to reflect the magic constant. This is useful for analyzing and producing M.S.S. solutions.

Definition 2.5. *Let $X = \left[x_{ij}\right] \in M_3(R)$. Define $F(X)$ as*

$$F(X) = \begin{bmatrix} f_1(X) \\ f_2(X) \\ f_3(X) \\ f_4(X) \\ f_5(X) \\ f_6(X) \\ f_7(X) \\ f_8(X) \end{bmatrix} = \begin{bmatrix} x_{11}^2 + x_{12}^2 + x_{13}^2 \\ x_{21}^2 + x_{22}^2 + x_{23}^2 \\ x_{31}^2 + x_{32}^2 + x_{33}^2 \\ x_{11}^2 + x_{21}^2 + x_{31}^2 \\ x_{12}^2 + x_{22}^2 + x_{32}^2 \\ x_{13}^2 + x_{23}^2 + x_{33}^2 \\ x_{11}^2 + x_{22}^2 + x_{33}^2 \\ x_{13}^2 + x_{22}^2 + x_{31}^2 \end{bmatrix}.$$

The elements of $F(X)$ represent the sums of the rows, columns, and diagonals of the matrix $X^{(2)}$. For a constant C, the matrix X is a solution to $F(X) = \vec{C}$ if and only if X^2 is a magic square of squares with the magic constant C.

Remark 2.6. *Let R be a ring, $M \in M_3(R)$, and $C \in R$. Then M is an M.S.S. with magic constant C if and only if there exists $A \in M_3(R)$ such that $M = A^{(2)}$ and $F(A) = \vec{C}$.*

The following function is used to generate M.S.S. solutions.

Definition 2.7. *Let $X = \left[x_{ij}\right] \in M_3(R)$. Define $\Gamma(X)$ as*

$$\Gamma(X) = \begin{bmatrix} x_{11} & 3x_{22} - x_{11} - x_{13} & x_{13} \\ x_{22} + x_{13} - x_{11} & x_{22} & x_{22} + x_{11} - x_{13} \\ 2x_{22} - x_{13} & x_{13} + x_{11} - x_{22} & 2x_{22} - x_{11} \end{bmatrix}.$$

Note that for any matrix $X \in M_3(R)$, $\Gamma(X)$ defines a magic square with constant $C = 3x_{22}$. Now we focus on the situation where R is a field. Let $\mathbf{F}$ be any field. We show that a matrix $M \in M_3(\mathbf{F})$ is an M.S.S. if and only if $M = A^{(2)} = \Gamma(A^{(2)})$ for some $A \in M_3(\mathbf{F})$. Such a matrix A acts as a "fixed point" for the operator Γ.

Lemma 2.8. *Let $\mathbf{F}$ be any field and $M = \left[m_{ij}\right] \in M_3(\mathbf{F})$. Then M is an M.S.S. with magic constant C if and only if there exists $A \in M_3(\mathbf{F})$ such that $\Gamma(M) = A^{(2)}$.*

Proof. The proof uses Gröbner Basis Theory. Please refer to a brief introduction to Gröbner Basis in the Appendix.

We treat the constant C as an indeterminate as the other variables x_{ij} in the ring $R = \mathbf{F}[x_{11}, x_{12}, x_{13}, x_{21}, x_{22}, x_{23}, x_{31}, x_{32}, x_{33}, C]$. Let $f_1, \ldots, f_8$ be as defined in Definition 2.5 and $I = \langle f_1 - C, \ldots, f_8 - C\rangle$ the ideal of R generated by $f_1 - C, \ldots, f_8 - C$. Select the lexicographic monomial ordering among the monomials in R with respect to the variable ordering of

$$1 < x_{22} < x_{11} < x_{13} < x_{31} < x_{33} < x_{12} < x_{21} < x_{23} < x_{32} < C.$$

With this ordering, we find the reduced Gröbner Basis, $\{g_1, \ldots, g_7\}$, of the ideal I, which is represented by the function vector $G(X)$:

$$G(X) = \begin{bmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \\ g_5 \\ g_6 \\ g_7 \end{bmatrix} = \begin{bmatrix} -2x_{22}^2 + x_{13}^2 + x_{31}^2 \\ -2x_{22}^2 + x_{11}^2 + x_{33}^2 \\ -3x_{22}^2 + x_{11}^2 + x_{13}^2 + x_{12}^2 \\ -x_{22}^2 + x_{11}^2 - x_{13}^2 + x_{21}^2 \\ -x_{22}^2 - x_{11}^2 + x_{13}^2 + x_{23}^2 \\ x_{22}^2 - x_{11}^2 - x_{13}^2 + x_{32}^2 \\ -3x_{22}^2 + C. \end{bmatrix}.$$

That is,

$$I = \langle f_1 - C, \ldots, f_8 - C\rangle = \langle g_1, \ldots, g_7\rangle.$$

Thus $G(X) = \vec{0} \Longleftrightarrow F(X) = \vec{C}$. In addition, the transition between the two generating sets is given by $U\left(F(X) - \vec{C}\right) = G(X)$ and $VG(X) = F(X) - \vec{C}$, where U and V are the matrices shown below.

$$U = \begin{bmatrix} 1 & 0 & 1 & 0 & -1 & 0 & -1 & 0 \\ 1 & 0 & 1 & 0 & -1 & 0 & 0 & -1 \\ 2 & 0 & 1 & 0 & -1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 1 & 1 & 1 & -1 & -1 & 0 & -1 & 0 \\ -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & -1 & 0 & -1 & -1 \end{bmatrix} \quad \text{and} \quad V = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 1 & 0 & -1 \\ 1 & 1 & 0 & 0 & 0 & 1 & -1 \\ 1 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & 1 & -1 \\ 0 & 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}.$$

By definition, M is an M.S.S. with magic constant C if and only if there is $A \in M_3(\mathbf{F})$ such that $M = A^{(2)}$ and $F(A) = \vec{C}$. However $F(A) = \vec{C} \Longleftrightarrow G(A) = 0 \Longleftrightarrow \Gamma(M) = A^{(2)}$. Thus the lemma is true.

□

Corollary 2.9. *Assume M, A be as above and they satisfy $\Gamma(M) = A^{(2)}$. From $g_7(A) = 0$, $C = 3a_{22}^2 = 3m_{22}$.*

Note that from this corollary, the magic sum is three times the center entry, which confirms the known result. Also, if the monomial ordering is changed, then other generating sets of I may be constructed.

Computational Tools

Every M.S.S. M is a solution to the equation $F(X) = \vec{C}$. By Gröbner Basis analysis from above, this equation is equivalent to $G(X) = 0$. Thus the problem is reduced to finding M and A such that $\Gamma(M) = A^{(2)}$. It can be seen that $\Gamma(X)$ is only dependent upon 3 variables.

Based upon this idea, a *Maple* code, given in Appendix D, was developed to generate all solutions over a finite field $\mathbb{Z}_p$, where p is a prime number. Since $\Gamma(X)$ is only dependent upon, x_{11}, x_{13}, x_{22}, values are first assigned to these variables. Next, calculate $\Gamma(X)$ as a potential M.S.S. Then every entry in this matrix is checked if it is a pefect square mod p. If all entries are perfect squares, then the matrix is an M.S.S. and stored. The algorithm produces all the solutions, together with their degrees, over $\mathbb{Z}_p$, regardless of permutations and reflections.

The algorithm was applied to build a solution bank for values of p from 2 to 251. The limitations of Maple began to become apparent as the run time for 251 is close to 4 hours. Further investigation for higher values of p requires a different programming language and more advanced techniques. The solution bank was frequently used to help in identifying patterns, guiding theoretical construction of solutions, and verifying the results presented in this thesis.

3 Magic Squares of Squares over Finite Fields

The focus of this section is to analyze and construct M.S.S. over $\mathbb{Z}_p$. I started by building a collection of M.S.S over small finite fields, such as S_2, S_3, S_5. It is important to identify perfect squares in the considered fields. These perfect squares are also known as quadratic residues. The following definitions and results are useful and well known in Number Theory and can be found in most number theory books, such as [3]. The first one introduces the concept of quadratic residue.

Definition 3.1. *[3] Let m be a positive integer and a be an integer relatively prime with m. We say a is a quadratic residue of m if* $x^2 \equiv a \pmod{m}$ *has a solution. Otherwise, a is called a quadratic nonresidue of m.*

Definition 3.2. *[3] 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*

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

The next theorem states some of the basic properties of the Legendre Symbol.

Theorem 3.3. *[3] Let p be an odd prime and a and b be integers not divisible by p. Then*

1. *if* $a \equiv b \pmod{p}$, *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
3. $\left(\frac{a^2}{p}\right) = 1$.

Identifying perfect squares in $\mathbb{Z}_p$ is a key task in constructing magic squares of squares, because only perfect squares are allowed as entries of an M.S.S. Thus a tool to test or check whether a member in $\mathbb{Z}_p$ is a quadratic residue is crucial. The following two theorems give the number of quadratic residues in $\mathbb{Z}_p$ and several useful formulas for the Legendre symbol, which can be used to identify quadratic residues (perfect squares).

Theorem 3.4. *[3] For any odd prime number p, there are exactly* $(p+1)/2$ *distinct quadratic residues in* $\mathbb{Z}_p$*, including* 0.

Note that since $-a \equiv p-a \pmod{p}$ and $\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)$, it is sufficient to check whether $1, 2, \ldots, \frac{p+1}{2}$ are quadratic residues or not.

Theorem 3.5. *[3] Let p be an odd prime, then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4}, \end{cases} \qquad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod{8} \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod{8}, \end{cases}$$

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1 \textit{ or } 11 \pmod{12} \\ -1 & \textit{if } p \equiv 5 \textit{ or } 7 \pmod{12}, \end{cases} \quad \textit{and}$$

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1 \textit{ or } 4 \pmod{5} \\ -1 & \textit{if } p \equiv 2 \textit{ or } 3 \pmod{5}. \end{cases}$$

Theorem 3.5 is useful in testing whether $-1, 2, 3$ or 5 are quadratic residues of p. To test if other numbers are quadratic residues of p, Theorem's 3.3 and 3.5 are applied together. Theorem 3.4 tells us how many quadratic residues of p are available.

Elements of S_2, S_3 and S_5

When $p = 2, 3, 5$ all the M.S.S. in S_p are given below, regardless of rotation and reflection:

Example 3.6 (All elements of S_2). *The set of quadratic residues for* 2 *is* $\{0, 1\}$

$$M_1 = \begin{array}{|c|c|c|}\hline 0&0&0\\\hline 0&0&0\\\hline 0&0&0\\\hline\end{array} \quad M_2 = \begin{array}{|c|c|c|}\hline 0&1&1\\\hline 1&0&1\\\hline 1&1&0\\\hline\end{array} \quad M_3 = \begin{array}{|c|c|c|}\hline 1&0&1\\\hline 0&0&0\\\hline 1&0&1\\\hline\end{array}$$

$$M_4 = \begin{array}{|c|c|c|}\hline 1&1&1\\\hline 1&1&1\\\hline 1&1&1\\\hline\end{array} \quad M_5 = \begin{array}{|c|c|c|}\hline 0&1&0\\\hline 1&1&1\\\hline 0&1&0\\\hline\end{array} \quad M_6 = \begin{array}{|c|c|c|}\hline 1&0&0\\\hline 0&1&0\\\hline 0&0&1\\\hline\end{array}.$$

Since 0 and 1 are the only two quadratic residues for $p = 2$, then there are only two choices for the center entry. If the center entry is 0, the top left entry can be 0 or 1. Since the magic sum is 0 from Corollary 2.9, the only possible forms are M_1, M_2 and M_3. Similarly, if the middle entry is 1, the magic sum is 1 ($3(1) \equiv 1 \pmod{2}$). Then the only possible forms are M_4, M_5, M_6.

Example 3.7 (All elements of S_3). *The set of quadratic residues for* 3 *is* $\{0, 1\}$

$$\begin{array}{|c|c|c|}\hline 0&0&0\\\hline 0&0&0\\\hline 0&0&0\\\hline\end{array} \quad \begin{array}{|c|c|c|}\hline 1&1&1\\\hline 1&1&1\\\hline 1&1&1\\\hline\end{array}.$$

Example 3.8 (All elements of S_5). *The set of quadratic residues for* 5 *is* $\{0, 1, 4\}$

$$\begin{array}{|c|c|c|}\hline 0&0&0\\\hline 0&0&0\\\hline 0&0&0\\\hline\end{array} \quad \begin{array}{|c|c|c|}\hline 0&4&1\\\hline 1&0&4\\\hline 4&1&0\\\hline\end{array} \quad \begin{array}{|c|c|c|}\hline 1&1&1\\\hline 1&1&1\\\hline 1&1&1\\\hline\end{array} \quad \begin{array}{|c|c|c|}\hline 4&4&4\\\hline 4&4&4\\\hline 4&4&4\\\hline\end{array}.$$

Thus $\alpha(S_2) = 2$, $\alpha(S_3) = 1$, and $\alpha(S_5) = 3$. Note that S_2 has four M.S.S. of degree 2, S_3 has only trivial solutions, and S_5 has both solutions of degree 1 and of degree 3. Furthermore, $|S_2| = 6$, $|S_3| = 2$ and $|S_5| = 4$. Later it will be shown that $p = 2$ is the only prime number such that S_p has an element of even degree, which must be of degree 2. Next it will be shown that $\alpha(S_p) \geq 3$ for all prime $p \geq 5$.

The best lower bound for $\alpha(S_p)$

It has been shown for $p = 2,3,5$, that $\alpha(S_p) = 2,1,3$ respectively. From the solution bank, for all $p \geq 5$, there exist elements of degree 3. One can ask, "is it true that $\alpha(S_p) \geq 3$ for all $p \geq 5$?" The answer is "Yes." We prove it by constructing elements in S_p with exactly three distinct quadratic residues of p. The first case is to construct such a solution with the appearance of 0. If $M = [m_{ij}]$ is a nontrivial M.S.S. solution in S_p, where $\deg(M) = 3$ and M has a zero entry, then M must be in one of the following forms, regardless of rotation and reflection:

(0_1)

a	$-a$	0
$-a$	0	a
0	a	$-a$

or (0_2)

a	$2a$	0
0	a	$2a$
$2a$	0	a

,

where $a \neq 0$, a is a quadratic residue of p. The following theorem shows that the above forms (0_1) and (0_2) are the only possible forms for M.S.S. with zero entries. These forms are from $\Gamma(M)$ when $m_{22} = 0$ or $m_{22} = a$, respectively.

Theorem 3.9. *Let p be a prime number greater than* 3. *Then S_p has M.S.S. of degree 3 with zero entries if and only $p \equiv 1,5,$ or $7 \pmod 8$. In particular,*

1. *S_p has an M.S.S. of the form (0_1) if and only if $p \equiv 1 \pmod 4$.*
2. *S_p has an M.S.S. of the form (0_2) if and only if $p \equiv 1$ or $7 \pmod 8$*

Proof.

Form (0_1): S_p has an element M of the form (0_1) if and only if there exists a nonzero quadratic residue a of p such that $-a$ is also a quadratic residue of p. By Theorem 3.5, for any quadratic residue $a \pmod p$, $-a$ is also a quadratic residue if and only if $p \equiv 1 \pmod 4$ because

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right).$$

Form (0_2): An element M of S_p exists (in the form (0_2)) if and only if there exists a nonzero quadratic residue a of p such that $2a$ is also a quadratic residue. By Theorem 3.5 again, it is equivalent to $p \equiv 1$ or $7 \pmod 8$ because

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

Thus for every non-zero quadratic residue a, form (0_1) or form (0_2) produces M.S.S. of degree 3 with zero entries. Thus S_p has M.S.S. of degree 3 when $p \equiv 1,5,$ or $7 \pmod 8$. □

Note that $p \equiv 1 \pmod 4$, if and only if $p \equiv 1$ or $5 \pmod 8$. Thus, theorem 3.9 covers the three cases: $p \equiv 1,5,$ or $7 \pmod 8$. The remaining case is when $p \equiv 3 \pmod 8$.

Corollary 3.10. *S_p has no element of degree 3 containing zero entries if and only if $p \equiv 3$ $\pmod 8$.*

Immediately, from theorem 3.9 and corollary 3.10, the following is claimed:

Theorem 3.11. *If p is prime and $p \geq 5$ then $\alpha(S_p) \geq 3$.*

Proof. If $p \equiv 1,5,7 \pmod 8$, there exists an $M \in S_p$, where $\deg(M) = 3$ and M has zero entries by Theorem 3.9.
Let $p \equiv 3 \pmod 8$. Assume a is a quadratic residue of p and $a \neq 0$. Such a exists since there are $\frac{p+1}{2} \geq 3$ quadratic residues. Then let

$$M = \begin{array}{|c|c|c|}\hline a & -2a & 4a \\ \hline 4a & a & -2a \\ \hline -2a & 4a & a \\ \hline\end{array}.$$

By Theorem 3.3, $4a$ is a quadratic residue of p since $4a = 2^2 a$. By Theorem 3.5, $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = -1$. Since $\left(\frac{a}{p}\right) = 1$, then

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

Thus $-2a$ is a quadratic residue mod p. Since $p \geq 5$, $a \neq -2a$, $a \neq 4a$, and $-2a \neq 4a$. Thus $M \in S_p$ with the magic sum $3a$ and $\deg(M) = 3$.

□

In general, all degree 3 elements $M \in S_p$ must have certain forms:

Theorem 3.12. *Let $M \in S_p$. If $\deg(M) = 3$ then M has the following form:*

$$M = \begin{array}{|c|c|c|}\hline b & 2a-b & a \\ \hline 2a-b & a & b \\ \hline a & b & 2a-b \\ \hline\end{array},$$

where a, b and $2a-b$ are distinct quadratic residues of p.

Proof. By Lemma 2.8, M has the form

$$M = \begin{bmatrix} m_{11} & 3m_{22} - m_{11} - m_{13} & m_{13} \\ m_{22} + m_{13} - m_{11} & m_{22} & m_{22} + m_{11} - m_{13} \\ 2m_{22} - m_{13} & m_{13} + m_{11} - m_{22} & 2m_{22} - m_{11} \end{bmatrix}. \quad (*)$$

Then let $m_{22} = a$ and $\deg(M) = 3$.

Case 1 Assume one of the corner entries of M is equal to a, say $m_{13} = a$. If $m_{11} = a$ then M is trivial. Thus $m_{11} \neq a$. Set $m_{11} = b$ which is $b \neq a$. Then M must have the form stated in theorem and M has a degree of 3.

Next, it will be shown that no other forms of M admit degree 3.

Case 2 Assume two corner entries are equal to each other, but not equal to a, say $m_{11} = m_{13} = b \neq a$. The form of M in $(*)$ is reduced to:

$$M = \begin{array}{|c|c|c|}\hline b & 3a-2b & b \\ \hline a & a & a \\ \hline 2a-b & 2b-a & 2a-b \\ \hline\end{array}.$$

Since $a \neq b$, the five entries $3a-2b, 2b-a, 2a-b, a, b$ are all distinct. For example, $3a-2b = 2b-a$ implies $b = a$. Thus $\deg(M) = 5 > 3$, a contradiction.

Case 3 The last possible case is when both corners are distinct and different from a. Let $m_{11} = b$ and $m_{13} = c$, where $b \neq c$. Then M is as follows:

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

Since $\deg(M) = 3$, then $m_{12} = a, b$, or c. If $m_{12} = a$, then $a = 3a-b-c$ implies $c = 2a-b$ and $m_{21} = a+c-b = 3a-2b$. But, the degree of M is 3, therefore $3a-2b \in \{a, b, 2a-b\}$, which implies $a = b$, a contradiction. Thus $m_{12} = b$ or c.

Without loss of generality, let $m_{12} = c$. Therefore M is in the following form:

$$M = \begin{array}{|c|c|c|}\hline b & c & c \\ \hline a-b+c & a & a+b-c \\ \hline 2a-c & 2a-c & 2a-b \\ \hline\end{array},$$

where a, b, c are distinct. Since $a \neq c$, then $2a-c \neq a$ and $2a-c \neq c$. Thus, $2a-c = b$, then M is in the following form:

$$M = \begin{array}{|c|c|c|}\hline 2a-c & c & c \\ \hline 2c-a & a & 3a-2c \\ \hline 2a-c & 2a-c & c \\ \hline\end{array}.$$

Applying Corollary 2.9 to the first row, $2a-c+c+c = 3a$ which implies $a = c$, a contradiction. Therefore, $2a-c \neq a, b$, or c. This case does not produce a M.S.S. of degree 3.

In summary, a degree 3 M.S.S. must have the form given in case 1, which is stated in the above theorem.

□

Existence and properties of degree 3 solutions can be used as a foundation to build up higher degree solutions. A few questions are raised: "Can the lower bound of $\alpha(S_p)$ be improved?" and "Does S_p have an element of even degree for $p \geq 5$?" First I consider the parity of $\deg(M)$, where $M \in S_p$ and $p \geq 5$.

No Magic Square of Squares of Even Degree for $p \geq 5$

Theorem 3.13. *Let $M \in S_p$, where $p \geq 5$ and p is prime. Then* $\deg(M)$ *is odd.*

Proof. Let $M = [m_{ij}] \in S_p$ and $m_{22} = a$. Consider the different cases where the other entries are equal to a or not. Then the remaining entries are filled using Corollary 2.9.

Case 1: A corner entry is equal to a. Then the opposite corner entry must be equal to a as well. Denote $m_{12} = b$. Then M must have the following form:

$$M = \begin{array}{|c|c|c|}\hline a & b & 2a-b \\ \hline 2a-b & a & b \\ \hline b & 2a-b & a \\ \hline \end{array},$$

where b, $2a-b$ are quadratic residues of p. It is easy to see that $a = b$ if and only if $2a-b = a$ and $2a-b = b$. This implies that $\deg(M) = 1$ when $a = b$ and $\deg(M) = 3$ when $a \neq b$. Thus, $\deg(M) = 1$ or 3.

Next, consider the cases where none of the four corner entries are equal to a. Then those 4 elements must be two pairs of identical elements or all distinct. Assume that b, c, d and e are not all distinct. It is sufficient to consider the following 2 subcases:

Case 2: Let $m_{11} = m_{33} = b \neq a$. Then $2b + a = 3a$ which implies $b = a$. It is a contradiction.

Case 3: Let $m_{11} = m_{13} = b \neq a$. Then $m_{31} = m_{33} = 2a - b$ and $m_{21} = m_{23} = a$, which implies that $m_{12} = 3a - 2b$ and $m_{32} = 2b - a$. Then M is in the following form:

$$M = \begin{array}{|c|c|c|}\hline b & 3a-2b & b \\ \hline a & a & a \\ \hline 2a-b & 2b-a & 2a-b \\ \hline \end{array}.$$

It is easy to check that $a, b, 3a-2b, 2a-b, 2b-a$ are all distinct because $a \neq b$. Therefore $\deg(M) = 5$.

Next assume that a, b, c, d and e are all distinct. Then M is in the form:

$$M = \begin{array}{|c|c|c|}\hline b & x_1 & c \\ \hline x_2 & a & x_3 \\ \hline d & x_4 & e \\ \hline \end{array}.$$

Case 4: Let $a \in \{x_1, x_2, x_3, x_4\}$. Without loss of generality, $a = x_1$. Using Corollary 2.9, $b + a + c = 3a$, which implies $b + c = 2a$. Also, $b + a + e = 3a$, which implies $b + e = 2a$. Then $b + c = 2a = b + e$ which implies $c = e$, a contradiction. So $a \notin \{x_1, x_2, x_3, x_4\}$.

Case 5: Let $\{x_1, x_2, x_3, x_4\} \cap \{b, c, d, e\} \neq \emptyset$ and $a \notin \{x_1, x_2, x_3, x_4\}$. It is sufficient to consider the two cases when $b = x_1$ or $b = x_3$.

If $x_1 = b$, then M must have the following form:

$$M = \begin{array}{|c|c|c|} \hline b & x_1 = b & 3a-2b \\ \hline x_2 = 4a-3b & a & x_3 = 3b-2a \\ \hline 2b-a & x_4 = 2a-b & 2a-b \\ \hline \end{array}.$$

It was already proven in theorem 3.12 case 3, that $a, b, 4a-3b, 2b-a, 2a-b, 3b-2a$, and $3a-2b$ are all distinct because a and b are distinct and $p \geq 5$. Thus $\deg(M) = 7$.

If $x_3 = b$, then $x_2 = e$ which implies that $d = c$, a contradiction.

Case 5 produces M.S.S. of degree 7 with x_1, x_2, x_3, x_4 all distinct. It must have the above form ($x_1 = b$) or a rotation or reflection of it.

Case 6: Let $\{x_1, x_2, x_3, x_4\} \cap \{a, b, c, d, e\} = \phi$. Assume $x_1 = x_4$, then $x_1 = a = x_4$, this is a contradiction, since $a \notin \{x_1, x_2, x_3 x_4\}$. If $x_1 = x_2$, then $c = d$, again a contradiction. Thus all x_i are distinct. In this case, $\deg(M) = 9$.

□

In summary, for $p \geq 5$, the only possible degrees of M.S.S. of order 3 are $1, 3, 5, 7, 9$.

4 Construction of Magic Squares of Squares of Various Degrees

By now we know that $\alpha(S_p)$ is odd and $\alpha(S_p) \geq 3$ for $p \geq 5$. A natural question can be asked, "For which values of p do M.S.S. exist of degrees 5, 7, or 9?" The solution bank provides a guide to follow. (See Section A)

Degree 5 solutions first appear in S_{17}, then again in S_{23}. From the solution bank, all examined S_p have degree 5 solutions for $p \geq 41$ and degree 9 solutions for $p \geq 71$. But some S_p does not have M.S.S. of degree 7 for large primes p. In this section, the construction of M.S.S. of degrees 5, 7, and 9 are provided in some S_p.

Existence of Magic Squares of Squares of degree 5

Two cases are investigated: when M has zero entries or when M has no zero entries.

Theorem 4.1. *Let p be a prime number and $p \equiv 1 \pmod 8$. Then S_p has an M.S.S. of degree 5, that is, $\alpha(S_p) \geq 5$.*

Proof. Given the above conditions, $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1$. Therefore $-1, 2$ are quadratic residues of p. Let

$M =$

1	−2	1
0	0	0
−1	2	−1

From here it is easy to check the magic sum is 0 and that M is an M.S.S. of degree 5. □

Example 4.2. *An M.S.S. of degree 5 in S_{17}:*

$M =$

1	15	1
0	0	0
16	2	16

Where $15 \equiv 7^2 \pmod{17}$, $16 \equiv 4^2 \pmod{17}$, *and* $2 \equiv 6^2 \pmod{17}$.

Theorem 4.3. *Let p be a prime number and $p \equiv 23 \pmod{24}$. Then there exists an M.S.S. of degree 5, and so $\alpha(S_p) \geq 5$.*

Proof. Given the conditions shown above, $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1$ because $p \equiv 23 \pmod{24}$ implies that $p \equiv 7 \pmod 8$ and $p \equiv 11 \pmod{12}$. Thus 2 and 3 are quadratic residues of p by theorem 3.3. Then M can be constructed as follows:

$M =$

3	0	3
2	2	2
1	4	1

It is easy to check that the row, column and diagonal sums are 6 and that M is an M.S.S. □

Example 4.4. *An M.S.S. of degree 5 in S_{23}:*

$$M = \begin{array}{|c|c|c|}\hline 3 & 0 & 3 \\ \hline 2 & 2 & 2 \\ \hline 1 & 4 & 1 \\ \hline \end{array},$$

where $3 \equiv 7^2 \pmod{23}$ *and* $2 \equiv 5^2 \pmod{23}$.

Existence of Magic Squares of Squares of degree 7

In this section, certain M.S.S of degree 7 containing zero entries are constructed.

Theorem 4.5. *Let p be a prime greater then 13. If -1, 2, 3, 5 are quadratic residues of p, then there exists $M \in S_p$ such that $\deg(M) = 7$ and M has at least one zero entry. A zero entry can occur in any position of M. An M.S.S. with a pair of zero entries can also be constructed.*

Proof. We construct 4 matrices as follows, where the magic sums of M_1, M_2, M_3, and M_4 are 0, 3, 3, and 3 respectively:

$$M_1 = \begin{array}{|c|c|c|}\hline 1 & 1 & -2 \\ \hline -3 & 0 & 3 \\ \hline 2 & -1 & -1 \\ \hline \end{array}, \quad M_2 = \begin{array}{|c|c|c|}\hline 0 & 0 & 3 \\ \hline 4 & 1 & -2 \\ \hline -1 & 2 & 2 \\ \hline \end{array},$$

$$M_3 = \begin{array}{|c|c|c|}\hline 2^{-1}\cdot 3 & 2^{-1}\cdot 3 & 0 \\ \hline 4-2^{-1}\cdot 9 & 1 & 2^{-1}\cdot 9-2 \\ \hline 2 & 2-2^{-1}\cdot 3 & 2-2^{-1}\cdot 3 \\ \hline \end{array},$$

$$M_4 = \begin{array}{|c|c|c|}\hline 3^{-1}\cdot 4 & 3^{-1}\cdot 4 & 1-3^{-1}\cdot 2 \\ \hline 0 & 1 & 2 \\ \hline 1+3^{-1}\cdot 2 & 3^{-1}\cdot 2 & 3^{-1}\cdot 2 \\ \hline \end{array}.$$

Then applying theorems 3.5 and 3.3, M_1 and M_2 are M.S.S. of p because $-1,2,3$ are quadratic residues of p.

For M_3, $4-2^{-1}\cdot 9$ is a quadratic residue of p because

$$\left(\frac{4-2^{-1}\cdot 9}{p}\right) = \left(\frac{4-2^{-1}\cdot 9}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{8-9}{p}\right) = \left(\frac{-1}{p}\right) = 1.$$

Similarly, $2-2^{-1}\cdot 3$ is a quadratic residue of p. However, for $2^{-1}\cdot 9-2$ to be a quadratic residue of p, it needs 5 to be so as well because:

$$\left(\frac{2^{-1}\cdot 9-2}{p}\right) = \left(\frac{2^{-1}\cdot 9-2}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{5}{p}\right).$$

For M_4, note that 3 and 5 are quadratic residues of p implies 3^{-1} and $3^{-1}\cdot 2$ are so. Furthermore,

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

and

$$\left(\frac{1+3^{-1}\cdot 2}{p}\right)=\left(\frac{3}{p}\right)\left(\frac{1+3^{-1}\cdot 2}{p}\right)=\left(\frac{5}{p}\right)=1.$$

It is straightforward to check each M_i has 7 distinct entries, for $i=1,2,3,4$. So $\deg(M_i)=7$ for each i. □

Example 4.6. *M.S.S. of degree 7 in S_{241} that satisfy Theorem 4.5:*

$$M_1=\begin{array}{|c|c|c|}\hline 1 & 1 & 239\\ \hline 238 & 0 & 3\\ \hline 2 & 240 & 240\\ \hline\end{array},\quad M_2=\begin{array}{|c|c|c|}\hline 0 & 0 & 3\\ \hline 4 & 1 & 239\\ \hline 240 & 2 & 2\\ \hline\end{array},$$

$$M_3=\begin{array}{|c|c|c|}\hline 122 & 122 & 0\\ \hline 120 & 1 & 123\\ \hline 2 & 121 & 121\\ \hline\end{array},\quad M_4=\begin{array}{|c|c|c|}\hline 162 & 162 & 161\\ \hline 0 & 1 & 2\\ \hline 82 & 81 & 81\\ \hline\end{array}.$$

Where $2^{-1}\equiv 121 \pmod{241}$ *and* $3^{-1}\equiv 161 \pmod{241}$. *Also* $2\equiv 219^2$, $3\equiv 56^2$, $8\equiv 197^2$, $81\equiv 9^2$, $82\equiv 75^2$, $120\equiv 222^2$, $121\equiv 11^2$, $122\equiv 107^2$, $123\equiv 169^2$, $161\equiv 142^2$, $162\equiv 43^2$, $238\equiv 210^2$,$239\equiv 203^2$, *and* $240\equiv 177^2 \pmod{241}$.

Corollary 4.7. *Let p be a prime number and $p\equiv 1$ or $-1 \pmod{24}$. Then there exists an M.S.S. of degree 7, that is, $\alpha(S_p)\geq 7$.*

Proof. Since $p\equiv 1$ or $-1 \pmod{24}$, $-1,2,3$ are all quadratic residues of p. Thus the matrices M_1 or M_2 in Theorem (4.5) are M.S.S. of degree 7 because the construction of these two matrices only requires $-1,2,3$ being quadratic residues of p. □

Example 4.8. *An M.S.S. of degree 7 in S_{71}:*

$$M=\begin{array}{|c|c|c|}\hline 4 & 4 & 1\\ \hline 0 & 3 & 6\\ \hline 5 & 2 & 2\\ \hline\end{array},$$

where $3\equiv 28^2 \pmod{71}$, $6\equiv 19^2 \pmod{71}$, $5\equiv 17^2 \pmod{71}$, *and* $2\equiv 12^2 \pmod{71}$.

Summary of structures and degrees of Magic Squares of Squares

Theorem 4.9. *Let $M\in S_p$. Then M must be in one of the following forms:*

$$M_1=\begin{array}{|c|c|c|}\hline a & a & a\\ \hline a & a & a\\ \hline a & a & a\\ \hline\end{array}\qquad M_2=\begin{array}{|c|c|c|}\hline a & b & 2a-b\\ \hline 2a-b & a & b\\ \hline b & 2a-b & a\\ \hline\end{array}$$

$$M_3=\begin{array}{|c|c|c|}\hline b & 3a-2b & b\\ \hline a & a & a\\ \hline 2a-b & 2b-a & 2a-b\\ \hline\end{array}\qquad M_4=\begin{array}{|c|c|c|}\hline b & b & 3a-2b\\ \hline 4a-3b & a & 3b-2a\\ \hline 2b-a & 2a-b & 2a-b\\ \hline\end{array}$$

$$M_5 = \begin{array}{|c|c|c|}\hline a & 3c-a-b & b \\ \hline c+b-a & c & c+a-b \\ \hline 2c-b & a+b-c & 2c-a \\ \hline \end{array}.$$

The above a, b, c are distinct quadratic residues of p. The corresponding degrees are: $\deg(M_1) = 1$ *(so M_1 is trivial),* $\deg(M_2) = 3$, $\deg(M_3) = 5$, $\deg(M_4) = 7$, *and* $\deg(M_5) = 9$.

Proof. Let $M = [m_{ij}] \in S_p$, $m_2 = 1, m_{12} = b$, and $m_{13} = c$. Then the (*) form of M given in the proof of Theorem 3.12 is

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

We discuss all the cases about the three independent variables a, b, c.

Case 1. $a = b = c$. In this case, M is a trivial one, that is, M is of the form M_1.

Case 2. $a = b$ but $b \neq c$. This is Case 1 in the proof of Theorem 3.12 where M is of degree 3 and has the form of M_2.

Case 3. $a \neq b$ but $b = c$. It is discussed in Case 3 of the proof of Theorem 3.12 that no M.S.S. has this form.

Case 4. a, b, c are all distinct. Since we consider M.S.S. regardless of reflection and rotation, it is sufficient to assume that all the corner entries of M are distinct. This case is discussed in the proof of Theorem 3.13 (Cases 4-6). These cases may produce M.S.S. of Degree 5, 7, or 9, with the forms of M_3, M_4, or M_5 respectively.

□

The following example shows that S_{241} has all the five forms shown above. That is, there are Magic Squares of Squares of degrees $1, 3, 5, 7$, and 9 in S_{241}. Thus $\alpha(S_{241}) = 9$.

Example 4.10. *From* S_{241}

$$M_1 = \begin{array}{|c|c|c|}\hline 1 & 1 & 1 \\ \hline 1 & 1 & 1 \\ \hline 1 & 1 & 1 \\ \hline \end{array} \quad M_2 = \begin{array}{|c|c|c|}\hline 0 & 240 & 1 \\ \hline 1 & 0 & 240 \\ \hline 240 & 1 & 0 \\ \hline \end{array} \quad M_3 = \begin{array}{|c|c|c|}\hline 0 & 25 & 0 \\ \hline 169 & 169 & 169 \\ \hline 97 & 72 & 97 \\ \hline \end{array}$$

$$M_4 = \begin{array}{|c|c|c|}\hline 0 & 0 & 36 \\ \hline 48 & 12 & 217 \\ \hline 229 & 24 & 24 \\ \hline \end{array} \quad M_5 = \begin{array}{|c|c|c|}\hline 144 & 174 & 134 \\ \hline 221 & 231 & 0 \\ \hline 87 & 47 & 77 \\ \hline \end{array}.$$

Observations

From the solution bank, the number of solutions of degree m for a prime is observed and recorded. These results are found in Appendix A. For each value of m a distinct pattern over various p is apparent. A function is defined that describes these patterns.

Definition 4.11. *Let $m \in \{1,3,5,7,9\}$ and p is a prime number. Define*

$$f(m, p) = \textit{number of degree } m \textit{ solutions in } S_p.$$

Using the table from Appendix A, the graph for $f(3, p)$ and $f(5, p)$ is seen below.

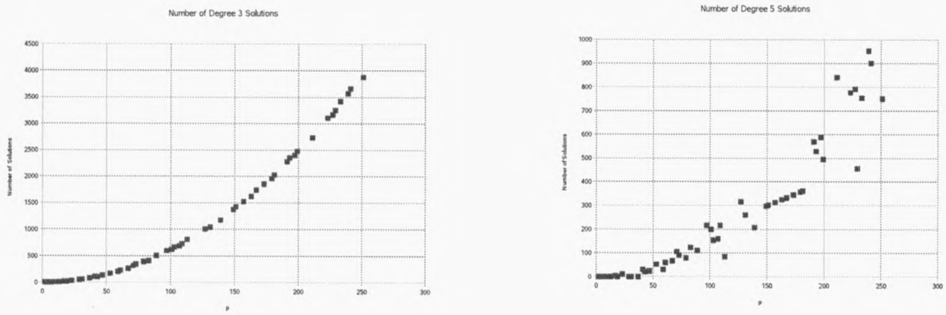

Figure 2: Graphs for $f(3, p)$ and $f(5, p)$

Furthermore, the graphs for $f(7, p)$ and $f(9, p)$ are also given. The only function that

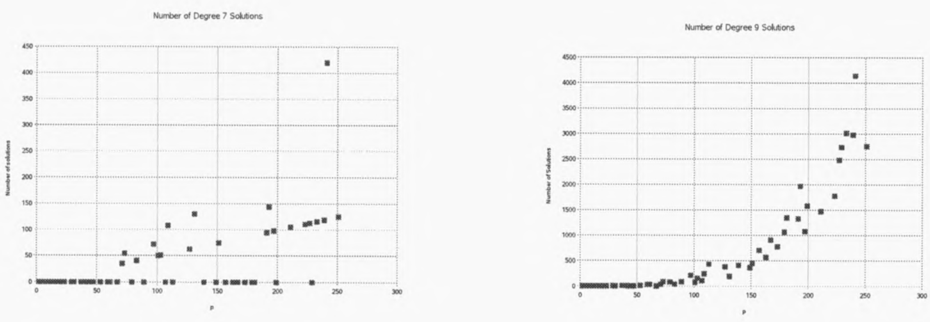

Figure 3: Graphs for $f(7, p)$ and $f(9, p)$

appears to have a 'nice' closed form is for $f(7, p)$, which appears to have linear characteristics.

5 Conclusion and Future Work

In this thesis, the structure of M.S.S. over the finite field $\mathbb{Z}_p$ was developed. For $p \geq 5$, there exists M.S.S. degree 3 over $\mathbb{Z}_p$, that is, $\alpha(S_p) \geq 3$. It is also shown that $\alpha(S_p) \geq 5$ when $p \geq 13$ and $p \equiv 1 \pmod 8$. The existence of degree 7 M.S.S. over certain $\mathbb{Z}_p$ is also discussed. When $p \geq 13$ and $p \equiv 1$ or $7 \pmod 8$, S_p has elements of degree 7.

Based upon the data from Appendix A, we conjecture that $\alpha(S_p) = 9$ for $p \geq 71$ and that S_p always has elements of degree 5 for $p \geq 41$. Future work includes trying to prove or disprove these conjectures. Furthermore, finding a prime p for which all p after have degree 7 solutions is also a question of interest.

The behavior of the function $f(m, p)$, which is the number of M.S.S. of degree m in S_p, will be another topic to investigate (p is prime, $m = 3, 5, 7$ or 9). From Appendix A, $f(m, p)$ demonstrates interesting pattern. For example, $f(7, p)$ seems linear. Future research is planned to study and prove the properties of this function.

6 Integrated Lesson: Introducing Magic Squares of Squares to Middle School Students

This research is supported by the GK-12 program at Montclair State University funded by the National Science Foundation. The program pairs graduate students (GK-12 fellows) in mathematics and science and places them in a team of middle school teachers in mathematics and science and thesis advisors from MSU. It provides the graduate fellows opportunities to experience teaching and research in the middle school classrooms. The goals of the program are to equip fellows with skills necessary to excel in STEM careers, enable teachers to inspire students in science and mathematics, increase middle grades students' interest and achievement in science and mathematics, and institutionalize project activities at Montclair State University.

The author and Diana Sanchez were paired up together with Elaine McCarthy, Science Teacher, and Miguel Marques, Math Teacher, from the Schuyler School in Kearny, New Jersey. Prior to entering the classroom, the fellows created lesson plans for the entire year based upon the years' theme of Chemical Interactions. One lesson plan and relevant classroom activities were carefully designed to introduce a mathematics topic involving graduate research to middle school students.

The topic of magic squares is one that can easily get attention from middle grade students. It is also a good topic that shows the entertaining and the power of mathematics. The instructors can use it as an informal assessment of students' skills and cognitive abilities. For this purpose, a lesson was designed and entitled "Investigating Magic Squares".

The Lesson

A goal of the GK-12 program, to introduce middle school students to graduate level research, is the primary driving force behind the lesson design. In order to make the lesson more entertaining and to achieve high level of students' involvement, the lesson starts with guided hands-on activities which give students opportunities to try to construct magic squares on their own. Several construction methods and the mathematics ideas behind them are introduced to students, with each easier and faster than the previous one. Students experienced how mathematics can simplify a complicated problem. The lesson consists of steps and procedures to construct magic squares, a brief illustration of the related graduate level research, and a follow up survey on students' learning from the lesson.

It is evident that the lesson helped increasing students' interest in mathematics. Some students showed excitement when exploring the mathematics problem. The lesson brought students to a different level in view of mathematics that they were accustomed to. On the other hand, it was a great opportunity for the graduate fellows to improve their teaching and communications skills. The planning and teaching components of the lesson provided the fellows an excellent opportunity to show their own graduate level research to a general audience. It is no doubt that these skills are valuable for the fellows' future careers.

A survey of students' preliminary knowledge was given prior to the lesson to assess the knowledge and background mathematics levels before the experiment. As is known, many cultural and societal biases and misconceptions are held by general society when it comes to mathematics. The cultural acceptance of mathematical illiteracy is evident in nearly every cultural aspect. The following is a list of questions and some of the most common or most interesting responses students gave to each of the questions posed.

1. In your own words, describe "what is mathematics?"

   Sample Students' responses

   - I don't know.
   - I am learning it so it must be important.
   - Solving problems with numbers.
   - Help you get a good job.

2. What can a mathematician do?

   - Help you in life.
   - Compute numbers very well.
   - Nothing. They can only teach you math.

These responses gave a snapshot of students' views and attitudes towards mathematics. The most interesting responses came from the second question. The last response listed above shows a genuine misconception about mathematics and mathematicians.

The lesson began with the concept of a magic square and some of the basic properties associated with it. The students were given a few minutes to try to construct a 3×3 magic square using the numbers 1 to 9 by merely guessing and checking. They were encouraged to identify patterns and bring up ideas that would make constructing a magic square easier. After comparing all the magic squares produced in class, the students were led to make conjectures on the center number and its relationship with the magic constant. Students were led to observe that the magic constant is the center number times 3.

8	1	6
3	5	7
4	9	2

Figure 4: A simple magic square of order 3 with magic constant 15

After this hands-on activity, the Siamese method (See Appendix C) was introduced to students and they were instructed to apply the method to construct new magic squares. The algorithm for the Siamese method was repeatedly applied, both at the class level and individually, in order for all students to understand the procedure and be able to produce their own magic squares. Students performed very differently in this step. Honors' students quickly mastered the method and were able to synthesize it to construct higher dimensional magic squares with little instruction. It was interesting to see the performance of the regular class made of students with a wider range of abilities. Some students had difficulties following the procedure of the Siamese Method. This was further observed in the third class, which was an inclusion class where students' abilities varied greatly.

The differences between honors students, regular students, and inclusion students were further displayed when the rotation and reflection operation were considered. From an existing magic square, 7 equivalent magic squares can be obtained by rotations and reflections. Honors students accomplished this with little to no assistance. Though the regular and inclusion classes required the use of various tools to help them understand the concepts.

At the very end of the lesson, students were shown how a mathematician approaches the problem. A magic square represented by variables, as seen in Figure 2, and algebraic equations for all the sums were shown to the students. All three group of students agreed that this was a messy and difficulty problem to solve. Then the simplified equations obtained by algebraic manipulations and other advanced techniques used in my research where shown to the students. They were amazed by the fact that mathematics can make hard problem easier to solve. Students were especially pleased when seeing the simple equation: the magic constant is three times the center number. They were then directed to construct their own magic squares using the simplified method, which depends only on three variables.

x_{11}	x_{12}	x_{13}
x_{21}	x_{22}	x_{23}
x_{31}	x_{32}	x_{33}

$$\begin{aligned}
x_{11}+x_{12}+x_{13}-C&=0\\
x_{21}+x_{22}+x_{23}-C&=0\\
x_{31}+x_{32}+x_{33}-C&=0\\
x_{11}+x_{21}+x_{31}-C&=0\\
x_{12}+x_{22}+x_{32}-C&=0\\
x_{13}+x_{23}+x_{33}-C&=0\\
x_{11}+x_{22}+x_{33}-C&=0\\
x_{13}+x_{22}+x_{31}-C&=0
\end{aligned}$$

Figure 5: A magic square with magic constant of C and the corresponding equations

x_{11}	$3x_{22}-x_{11}-x_{13}$	x_{13}
$x_{22}-x_{11}+x_{13}$	x_{22}	$x_{22}+x_{11}-x_{13}$
$2x_{22}-x_{13}$	$x_{11}+x_{13}-x_{22}$	$2x_{22}-x_{11}$

Figure 6: Simplified structure with magic constant $C=3x_{22}$

A demonstration was made using an excel spread sheet. Students were allowed to pick 3 numbers as the start entries and use them to create their own magic squares. Such one is show in Figure 4 below, which was created in class by the students.

38097	46929	42000
46245	42342	38439
42684	37755	46587

Figure 7: Student Created Magic Square with Magic Constant 127,026

The preliminary goal of the project was set forth in the GK-12 program, to increase students' enthusiasm, desire to learn, and appreciation of mathematics. The result from the lesson is positive. After the lesson was given, students from all 3 sections were posing questions outside the classroom about certain properties of magic squares. Students approached the graduate fellows and their math teacher asking specific questions about the properties of magic squares. A quick survey at the end of the lesson concluded that students changed their views about mathematics and the roles of mathematicians. Some stated that mathematicians take complex problems and make them simpler. From an observational standpoint, students seemed to enjoy the lesson and found it a fun subject in mathematics. It is also evident that this teaching module can be used at the beginning of the school year for teachers to unofficially measure their students abilities and understanding of mathematics.

7 References

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

[2] Cox, David A. and Little, John and O'Shea, Donal, *Ideals, Varieties, and Algorithms*, Springer, New York, 3rd Edition, 2007.

[3] Rosen, Kenneth H., *Elementary Number Theory*, Addison-Wesley, New York, 5th Edition, 2005.

[4] Gallian, Joseph A., *Contemporary Abstract Algebra*, Houghton Mifflin Company, Boston, Massachusetts, 2006.

[5] LaBar, Martin, *Problem 270*, College Mathematics Journal , Vol. 15, No 1, 1984, pp. 66-74.

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

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

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

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

[10] Magic Squares *http://www.pballew.net/magsquar.html*

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

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

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

A Table: Number of M.S.S. Solutions v.s. Degrees

p	$\|S_p\|$	# of deg(M) = 9	# of deg(M) = 7	# of deg(M) = 5	# of deg(M) = 3	# of deg(M) = 2	Trivial	$\alpha(S_p)$
2	6	0	0	0	4	2	2	2
3	2	0	0	0	0	0	2	1
5	4	0	0	0	1	0	3	3
7	7	0	0	0	3	0	4	3
11	11	0	0	0	5	0	6	3
13	16	0	0	0	9	0	7	3
17	33	0	0	4	20	0	9	5
19	28	0	0	0	18	0	10	3
23	56	0	0	11	33	0	12	5
29	71	7	0	0	49	0	15	9
31	76	0	0	0	60	0	16	3
37	109	9	0	0	81	0	19	9
41	166	5	0	30	110	0	21	9
43	148	0	0	21	105	0	22	5
47	185	0	0	23	138	0	24	5
53	261	13	0	52	169	0	27	9
59	291	29	0	29	203	0	30	9
61	346	30	0	60	225	0	31	9
67	364	0	0	66	264	0	34	5
71	526	35	35	105	315	0	36	9
73	613	90	54	90	342	0	37	9
79	586	78	0	78	390	0	40	9
83	657	41	41	123	410	0	42	9
89	749	88	0	110	506	0	45	9
97	1153	216	72	216	600	0	49	9
101	1001	75	50	200	625	0	51	9
103	1072	153	51	153	663	0	52	9
107	1008	106	0	159	689	0	54	9
109	1351	243	108	216	729	0	55	9
113	1387	434	0	84	812	0	57	9
127	1828	378	63	315	1008	0	64	9
131	1691	195	130	260	1040	0	66	9
139	1864	414	0	207	1173	0	70	9
149	2110	370	0	296	1369	0	75	9
151	2326	450	75	300	1425	0	76	9
157	2614	702	0	312	1521	0	79	9
163	2593	567	0	324	1620	0	82	9
167	3072	913	0	332	1743	0	84	9
173	3054	774	0	344	1849	0	87	9
179	3472	1068	0	356	1958	0	90	9
181	3826	1350	0	360	2025	0	91	9
191	4371	1330	95	570	2280	0	96	9
193	5089	1968	144	528	2352	0	97	9
197	4264	1078	98	588	2401	0	99	9
199	4654	1584	0	495	2475	0	100	9
211	5251	1470	105	840	2730	0	106	9
223	5884	1776	111	777	3108	0	112	9
227	6668	2486	113	791	3164	0	114	9
229	6556	2736	0	456	3249	0	115	9
233	7425	3016	116	754	3422	0	117	9
239	7736	2975	119	952	3570	0	120	9
241	9241	4140	420	900	3660	0	121	9
251	7626	2750	125	750	3875	0	126	9

B Gröbner Basis

Gröbner Basis was defined and developed by Bruno Buchberger in his Ph. D. thesis in 1965. It is named in honor of Buchberger's thesis advisor Wolfgang Gröbner. In recent years, Gröbner basis theory has been frequently used in algebraic geometry to study polynomial rings. The primary algorithm used to calculate Gröbner basis, Buchberger's Algorithm, has many implementations commonly found today in various computer programs such as Maple, CoCoA and Singular. An implementation of this algorithm found in Maple was used in this thesis. The advanced computational feature of Gröbner basis techniques have helped many researchers to solve or simplify complex and difficult problems found in robotics, combinatorics, graph theory, and geometry.

Affine Variety

Affine varieties and their relationship with ideals allow us to connect polynomials with Gröbner bases .

Definition B.1 (Affine Variety). *Let k be a field, and $f_1, \cdots, f_s \in k[x_1, \cdots, x_n]$. Then*

$$\mathbf{V}(f_1, \cdots, f_s) = \{(a_1 \cdots a_n) \in k^n : f_i(a_1 \cdots a_n) = 0, \forall 1 \leq i \leq s\}.$$

We say that $\mathbf{V}(f_1 \cdots f_s)$ is the Affine Variety defined by $f_1 \cdots f_s$. [2]

The above affine variety is the set of all solutions that satisfy the system of polynomial equations $f_1(x_1 \cdots x_n) = 0, \cdots, f_s(x_1 \cdots x_n) = 0$.

An example from elementary algebra is the line $y = 3x+2$. The affine variety for this line is notated by $\mathbf{V}(y-3x-2)$. All the points (x, y) on this line form the variety. This idea is expanded to systems polynomial of equations.

Polynomials and Monomial Orderings

In an intermediate algebra course, polynomial long division is usually covered and the ordering of monomials in a polynomial is easily defined. The ordering is defined from highest degree to lowest degree monomials. It is simple because there is only one variable to worry about. What happens when polynomials are multivariate?

Definition B.2 (Monomial Ordering). *A monomial ordering on $k[x_1, \cdots, x_n]$ is a relation $>$ on the set of monomials x^α in $k[x_1, \cdots, x_n]$ satisfying:*

- *$>$ is a total ordering relation*
- *$>$ is compatible with multiplication in $k[x_1, \cdots, x_n]$, in the sense that if $x^\alpha > x^\beta$ and x^γ is any monomial, then $x^\alpha x^\gamma = x^{\alpha+\gamma} > x^{\beta+\gamma} = x^\beta x^\gamma$*
- *$>$ is a well-ordering. That is, every nonempty collection of monomials has a smallest element under $>$.*

There are infinitely many monomial orderings available. The following are the two most commonly used orderings of monomials.

Definition B.3 (Lexicographic Order). *Let x^α and x^β be monomials in $k[x_1, \cdots, x_n]$. We say $x^\alpha >_{lex} x^\beta$ if in the difference of $\alpha - \beta \in \mathbb{Z}^n$, the left most nonzero entry is positive. [2]*

Lexicographic ordering is similar to ordering words in a dictionary.

Example B.4. *Set a lexicographic monomial ordering of $x >_{lex} y >_{lex} z$. We want to order the 3 monomials, x^3y^2z , x^2yz^5 , and x^4yz. Ordering them by $>_{lex}$ ordering, we find that $x^4yz >_{lex} x^3y^2z >_{lex} x^2yz^5$. Using the definition of lex ordering, x^4yz can be written as $\mathbf{x}^\alpha$, where $\alpha = (4,1,1)$. Doing the same for the other two monomials, $x^3y^2z = \mathbf{x}^\beta$ with $\beta = (3,2,1)$ and $x^2yz^5 = \mathbf{x}^{(2,1,5)}$. Comparing x^4yz to x^3y^2z, we get that $(4,1,1)-(3,2,1) = (1,1,0)$. The left most entry is 1 and positive so $x^4yz >_{lex} x^3y^2z$.*

Definition B.5 (Graded Lexicographic Order). *Let x^α and x^β be monomials in $k[x_1, \cdots, x_n]$. We say $x^\alpha >_{grlex} x^\beta$ if $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i$, or if $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ and $x^\alpha >_{lex} x^\beta$.*

Graded Lexicographic ordering, or Graded Lex ordering, is similar to univariate ordering in that it orders monomials by their total order. The tie breaker for monomials with the same total order is ordered by lex ordering.

Ideals

Definition B.6 (Ideal). *Let R be a commutative ring and $I \subseteq R$. Then I is an Ideal of R if the following are true:*

- $0 \in I$
- *If $a, b \in I$, then $a + b \in I$.*
- *If $a \in I$ and $r \in R$, then $ar \in I$.*

Gröbner Basis

Theorem B.7 (Hilbert Basis Theorem). *Every ideal $I \subset k[x_1, \cdots, x_n]$ has a finite generating set. That is, $I = \langle g_1, \cdots, g_t \rangle$ for some $g_1, \cdots, g_t \in I$.*

Definition B.8. *[2] [Gröbner Basis] Given a fixed a monomial order and a finite generating set $G = \{g_1, ..., g_t\}$ of an ideal I. G is called a Gröbner Basis of I if*

$$\langle LT(g_1), ..., LT(g_t) \rangle = \langle LT(I) \rangle.$$

Properties of Gröbner Basis

Definition B.9. *Given $I = \langle f_1, \cdots, f_s \rangle \subset k[x_1, \cdots, x_n]$, the l-th elimination ideal I_l is the ideal of $k[x_{l+1}, \cdots, x_n]$ defined by*

$$I_l = I \bigcap k[x_{l+1}, \cdots, x_n].$$

Theorem B.10 (The Elimination Theorem). *Let $I \subset k[x_1, \cdots, x_n]$ be an ideal and let G be a Gröbner bases of I with respect to lex order where $x_1 > x_2 > \cdots > x_n$. Then for every $0 \le l \le n$, the set*

$$G_l = G \bigcap k[x_{l+1}, \cdots, x_n].$$

Theorem B.11 (The Extension Theorem). *Let $I = \langle f_1, \cdots, f_s \rangle \subset \mathbb{C}[x_1, \cdots, x_n]$ and let I_l be the first elimination ideal of I. For each $1 \le i \le s$, write f_i in the form*

$$f_i = g_i(x_2, \cdots, x_n) x_1^{N_i} + \text{terms in which } x_1 \text{ has degree} < N_i,$$

where $N_i \ge 0$ and $g_i \in \mathbb{C}[x_1, \cdots, x_n]$ is nonzero. Suppose that we have a partial solution $(a_2, \cdots, a_n) \in \mathbf{V}(I_l)$. If $(a_1, \cdots, a_n) \notin \mathbf{V}(g_1, \cdots, g_s)$, then there exists $a_1 \in \mathbb{C}$ such that $(a_1, a_2, \cdots, a_n) \in \mathbf{V}(I)$.

C A Popular Method of Constructing Magic Squares: Siamese Method

The Siamese Method of Constructing Magic Squares of Order 3

1. Start with an empty magic square of order 3 and pick a sequence, i.e. $1,2,3,4,5,6,7,8,9$
2. Place 1 in the $(1,2)$-entry.
3. Go up 1 row and right 1 column. When on the edge of the magic square, the next step will wrap around to the opposite side. For example, from the $(1,2)$-entry, the next square is the $(3,3)$-entry. Then write down the next number in the sequence.
4. Repeat Step 3. If the next square is already filled in, move down one box instead of up and to the right.
5. Continue until the entire magic square is full.

Example of building a magic square of order 3 using Siamese Method

Step 1

	1	

Step 2

	1	
		2

Step 3

	1	
3		
		2

Step 4

	1	
3		
4		2

Step 5

	1	
3	5	
4		2

Step 6

	1	6
3	5	
4		2

Step 7

	1	6
3	5	7
4		2

Step 8

8	1	6
3	5	7
4		2

Step 9

8	1	6
3	5	7
4	9	2

The Siamese method, also known as the pyramid method, applies an arithmetic progression to build a magic square. While using this method, the entries of the magic square are rearranged into a 'pyramid' matrix. Referring to the magic square constructed above, the rearrangement is shown below,

		9		
	8		6	
7		5		3
	4		2	
		1		

.

It is easy to see that the above construction process uses an arithmetic progression of $1,2,3,4,5,6,7,8,9$. Generalizing this idea, any 3×3 magic square can be constructed using a specific sequence of numbers. Such a sequence is given by the following,

$$a, a+d, a+2d, a+f, a+d+f, a+2d+f, a+2f, a+d+2f, a+2d+2f.$$

The next step is to place the sequence into a 'pyramid' matrix. This is accomplished by inserting the first element of the sequence to the bottom position of the matrix. The filling the rest of the matrix by following the up and to the right direction along the diagonals.

		$a+2f+2d$		
	$a+2f+d$		$a+f+2d$	
$a+2f$		$a+f+d$		$a+2d$
	$a+f$		$a+d$	
		a		

.

Finally, the 4 empty positions are filled with the 4 outside entries. The process creates a magic square with magic sum $a+f+d$.

$a+2f+d$	a	$a+f+2d$
$a+2d$	$a+f+d$	$a+2f$
$a+f$	$a+2f+2d$	$a+d$

This process is not limited to only to 3×3 magic squares. It can be applied to construct magic squares of higher orders.

D The Maple Code

The following program can generate all solutions for a given finite field $\mathbb{Z}_p$. It takes into account rotations and permutations of a square and outputs a list of solutions. At the end of the file, it outputs the number of solutions with a certain degree.

```
> with(numtheory):
> with(ListTools):
> g7:=(a,b,k)->2*k^2-b^2:
> g9:=(a,b,k)->2*k^2-a^2:
> g2:=(a,b,k)->3*k^2-a^2-b^2:
> g4:=(a,b,k)->k^2-a^2+b^2:
> g6:=(a,b,k)->k^2+a^2-b^2:
> g8:=(a,b,k)->a^2+b^2-k^2:
> lp1:=[257, 263]:
> for p in lp1 do
> print(p):
> maxd:=(p+1)/2:
> L:=[]:
> fn:=cat("datafile",p,".mss"):
> fd:=fopen(fn,WRITE):
> cone:=0:
> ctwo:=0:
> cthree:=0:
> cfour:=0:
> cfive:=0:
> csix:=0:
> cseven:=0:
> ceight:=0:
> cnine:=0:
> for a1 from 0 to maxd do
> for b1 from 0 to maxd do
> for k1 from 0 to maxd do
> t7:=msqrt(g7(a1,b1,k1),p):
> t9:=msqrt(g9(a1,b1,k1),p):
> t2:=msqrt(g2(a1,b1,k1),p):
> t4:=msqrt(g4(a1,b1,k1),p):
> t6:=msqrt(g6(a1,b1,k1),p):
> t8:=msqrt(g8(a1,b1,k1),p):
> if not(t7='FAIL' or t9='FAIL' or t2='FAIL' or t4='FAIL' or t6='FAIL'
or t8='FAIL') then
> b:=[a1^2 mod p,g2(a1,b1,k1) mod p, b1^2 mod p,g4(a1,b1,k1) mod p,
k1^2 mod p, g6(a1,b1,k1) mod p, g7(a1,b1,k1) mod p, g8(a1,b1,k1) mod
p, g9(a1,b1,k1) mod p]:
```

```
> count:=nops(convert(b,set));
> b:=[op(b),count]:
> if Occurrences(b,L)=0 then
> L:=[op(L),[ b[1] , b[2] , b[3] , b[4],  b[5] , b[6] , b[7] , b[8]
, b[9] , b[10]],
> [ b[7] , b[4] , b[1] , b[8] , b[5] , b[2] , b[9] , b[6] , b[3] ,
b[10]],
> [ b[9] , b[8] , b[7] , b[6] , b[5] , b[4] , b[3] , b[2] , b[1] ,
b[10]],
> [ b[3] , b[6] , b[9] , b[2] , b[5] , b[8] , b[1] , b[4] , b[7] ,
b[10]],
> [ b[3] , b[2] , b[1] , b[6] , b[5] , b[4] , b[9] , b[8] , b[7] ,
b[10]],
> [ b[7] , b[8] , b[9] , b[4] , b[5] , b[6] , b[1] , b[2] , b[3] ,
b[10]],
> [ b[1] , b[4] , b[7] , b[2] , b[5] , b[8] , b[3] , b[6] , b[9] ,
b[10]],
> [ b[9] , b[6] , b[3] , b[8] , b[5] , b[2] , b[7] , b[4] , b[1] ,
b[10]]];
> L:=MakeUnique(L):
> fprintf(fd,"%5a %5a %5a %5a %5a %5a %5a %5a %5a %5a\n", b[1] , b[2]
, b[3] , b[4],  b[5] , b[6] , b[7] , b[8] , b[9], b[10]):
> if count=1 then
> cone:=cone+1:
> elif count=2 then
> ctwo:=ctwo+1:
> elif count=3 then
> cthree:=cthree+1:
> elif count=4 then
> cfour:=cfour+1:
> elif count=5 then
> cfive:=cfive+1:
> elif count=6 then
> csix:=csix+1:
> elif count=7 then
> cseven:=cseven+1:
> elif count=8 then
> ceight:=ceight+1:
> elif count=9 then
> cnine:=cnine+1:
> fi:
> fi:
> fi:
> od:
> od:
> od:
> ctotal:=cone+ctwo+cthree+cfour+cfive+csix+cseven+ceight+cnine:
> fprintf(fd,"\n\nCount results:\n"):
> fprintf(fd,"Total Solutions:  %10a \n",ctotal):
> fprintf(fd,"\n \n%5a %5a %5a %5a %5a %5a %5a %5a %5a\n",
cone,ctwo,cthree,cfour,cfive,csix,cseven,ceight,cnine):
> fclose(fd):
> od:
```

E Lesson Plan

Time Alloted: 2 Class Periods

Teachers: Stewart Hengeveld and Diana Sanchez

Goals: For students to understand how magic squares work and how to construct 3×3, 4×4, and possibly higher degree magic squares.

Objectives: Use Operations with Integers to solve problems. Analyze and Represent Patterns with Symbolic Rules.

NJCCS: 4.1.7B Numerical Operations, 4.2.7B Transforming Shapes, 4.3.7A Patterns

Materials:
Magic Square Worksheet
Magic Square Power Point

Procedure:

- Assess students' prior knowledge
  - What is mathematics? What does it do? What is its purpose?
  - What is the job of a mathematician?
  - What is a variable?
  - What is a conjecture?
  - Do they know what magic squares are?
- Introduce students to Magic squares.
- Discuss the history of magic squares and how it relates to the history of mathematics
  - Chinese History
  - Indian/Arab History
  - European/Japanese History
  - Modern
- Talk about impact of Mathematics of Magic Squares
  - Why is the study of Magic Squares important to mathematicians?
  - Math for mathematics sake or recreational mathematics. Why is this important? (Mention Fermats Last Theorem)
- Some Terminology

  - Order of a Magic Square
  - Magic Constant
  - Middle Entry
- Some Terminology
- Methods for constructing 3×3 Magic Squares
  - Guess and Check
  - Siamese Method
  - Pheru's Method
- Construct a Magic Square together with the entire class using a method listed with a magic constant of 15 and the integers 1 to 9. Then have the students pair up to construct more magic squares using the same rules.
  - Do they notice any patterns?
  - What conjectures can they make?
  - Possibly mention Rotations/permutations of a square
- Construct a magic square by the class as a whole: select s Magic Constant that is a multiple of 3.
- Depending on time, assign homework for the next class: let students construct at least 1 5×5 magic square with middle number 13 and magic sum of 65.
- At the beginning of the next class ask 3 volunteers provide the class with their 5×5 magic squares.
- Discuss even ordered Magic Squares.
  - Show how to build a 4×4 magic squares.
  - Work one out in class.
  - Have the class create their own Magic Square of order 4.
- Assess students' knowledge of Magic Squares as follows
  - Working in pairs to construct 3×3, 4×4 and 5×5 magic squares using given numbers.
  - After the lesson is finished, the students are asked the following questions.
    * What have you learned about magic squares?
    * How do mathematicians approach the problem?
    * Do you have a new view or new thoughts about mathematics?