5-2018

Magic Squares of Cubes Modulo a Prime Number

Yevgeniy Sokolovskiy
Montclair State University

Abstract

This work is dedicated to the properties of the 3×3 magic squares of cubes modulo a prime number. Its central concept is the number of distinct entries of these squares and the properties associated with this number. We call this number the degree of a magic square. The necessary conditions for the magic square of cubes with degrees 3, 5, 7, and 9 are examined. It was established that there are infinitely many primes for which magic squares of cubes with degrees 3, 5, 7, and 9 exist. I apply n-tuples of consecutive cubic residues to prove that there are infinitely many Magic Squares of Cubes with degree 9. Furthermore I use Brauer's theorem, that guarantees the existence of a sequence of consecutive integers of any length, to construct Magic Squares of Cubes whose entries are all cubic residues. Such analytic tools as Modular Arithmetic, Legendre symbol, Fermat's Little Theorem, notions of quadratic and cubic residues were employed in the process of research.

MONTCLAIR STATE UNIVERSITY

Magic Squares of Cubes Modulo a Prime Number

by

Yevgeniy Sokolovskiy

A Master's Thesis Submitted to the Faculty of

Montclair State University

In Partial Fulfillment of the Requirements

For the Degree of Master's in Mathematics May 2018

College of Science and Mathematics

Department of Mathematical Sciences

Thesis Committee:

[redacted]

Dr. Aihua Li

Thesis Sponsor

[redacted]

Dr. Baojun Song

Committee Member

[redacted]

Dr. Bogdan G. Nita

Committee Member

MAGIC SQUARES OF CUBES MODULO A PRIME NUMBER

A THESIS

Submitted in partial fulfillment of the requirements

for the degree of Master's in Mathematics

by

Yevgeniy Sokolovskiy

Montclair State University

Montclair, NJ

May 2018

Acknowledgments

I am immensely grateful to Dr. Aihua Li for giving me the opportunity to write this thesis under her supervision. I am indebted to her for providing a topic for my thesis, identifying the relevant literature for my research, and helping me in the areas where my knowledge was not sufficient. I also want to thank my parents for their unflagging moral support and advice concerning this work. The fact that my father is a mathematics teacher and mother a physics teacher greatly inspired me in my research. Gratefully, I dedicate my thesis to them.

Contents

Acknowledgments **ii**

1 Introduction **1**

1.1 History and Background 1

1.2 Basics about Quadratic and Cubic Residues 2

1.3 Magic Squares of Integers 3

1.4 Magic Squares of Cubes Mod a Prime p 4

1.5 Definitions and Notations 5

1.6 Existing Results 7

1.7 Research Questions, Goals, and Methodology 10

1.8 Main Results 10

2 Cubic Residues in $\mathbb{Z}_p$ **11**

3 Construction of Magic Squares of Cubes **14**

3.1 What Degrees are Possible for a Magic Square? 14

3.2 Magic Squares of Cubes Modulo 2, 3, 5, or 7 17

3.3 Possible Degrees of Magic Squares of Cubes over $\mathbb{Z}_p$ for $p > 7$ 19

3.4 Construction of MSC Using Consecutive Cubic Residues 24

4 Concluding Remarks and Future Direction **28**

5 References 30

Chapter 1

Introduction

1.1 History and Background

A Magic Square (MS) of order n is an $n \times n$ matrix that contains integers whose sum along any row, column or diagonal is the same. This sum is called the magic constant or magic sum. The history of magic squares goes back to 6BC China. The so called Lo Shu Square is associated with the flood that took place during the Yu Dynasty. According to the legend the people of China were able to use the pattern in the Lo Shu Square to defend themselves against the floods. The 8th century Arabian mathematician Jabir ibn Hayyan treated a magic square of order 3 as a child-bearing chasm. The 13th century Egyptian mathematician Ahmad al-Buni attributed mystical qualities to magic squares. The concept of magic square intrigued the Islamic mathematicians of Persia as well. One of them, the 10th century Persian mathematician Buzjani, performed a study of various magic squares. In India 3×3 magic squares have ritualistic significance. The magic square of order three, Kubera-Kolam (see the matrix below), is often seen on floors in India. It is in fact the result by adding 19 to each number of the Lo Shu Square:

$$L = \begin{bmatrix} 4 & 9 & 2 \\ 3 & 5 & 7 \\ 8 & 1 & 6 \end{bmatrix} \Longrightarrow M = \begin{bmatrix} 23 & 28 & 21 \\ 22 & 24 & 26 \\ 27 & 20 & 25 \end{bmatrix}.$$

In Europe magic squares are immortalized through art. A. Durer pictured a 4×4 square in his engraving Melencolia 1. The Sagrada Familia church in Barcelona features a 4×4 magic square with a magic sum $= 33$, the age of Christ at the time of his crucifixion. Overall, the concept and image of magic square belong to many civilizations never ceasing to challenge and delight their inhabitants.

1.2 Basics about Quadratic and Cubic Residues

Let p be a prime number. An integer a satisfying $x^n \equiv a \pmod p$ is called the *nth* power residue mod p. In particular when $n = 2$, a is a quadratic residue while when $n = 3$, a is a cubic residue.

Legendre symbol has been a major tool for dealing with quadratic residues. When a is a quadratic residue mod p the Legendre symbol $\left(\frac{a}{p}\right) = 1$, but when a is a quadratic non-residue mod p the Legendre symbol $\left(\frac{a}{p}\right) = -1$. The following lemma states some basic properties about Legendre symbol for quadratic residues.

Lemma 1.2.1. *Let p be a prime number and $a, b \in \mathbb{Z}$. Then*

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

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

3. $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ *if* $p \equiv 1 \pmod 4$ *or* $q \equiv 1 \pmod 4$

4. $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ *if* $p \equiv 3 \equiv q \pmod 4$.

I use the above law of quadratic reciprocity associated with Legendre symbol to establish that -3 is a quadratic residue mod any prime in the form of $3m + 1$ where m is an integer.

1.3 Magic Squares of Integers

The earliest known 3×3 magic square of integers is the Lo Shu Square whose magic sum is 15. It has been established that in a 3×3 magic square its magic sum is equal to 3 times its middle element. In the Lo Shu Square the middle element 5 multiplied by 3 yields 15. Also the Lo Shu square has 9 distinct entries thus being of degree 9. In general the number of distinct entries in an MS is called its degree. Thus the maximal degree of a 3×3 magic square is 9 while the minimum is 1. As for MS viewed modulo p it has been established that their degree can be 1, 2, 3, 5, 7, or 9. A 3×3 magic square in which every entry is a perfect square of an integer is called a Magic Squares of Squares. It has the following form:

$$M = \begin{bmatrix} a^2 & b^2 & c^2 \\ d^2 & e^2 & f^2 \\ g^2 & h^2 & i^2 \end{bmatrix},$$

where $a, b, c, d, e, f, g, h, i \in \mathbb{Z}$ and

$$\begin{aligned} a^2 + b^2 + c^2 &= d^2 + e^2 + f^2 = g^2 + h^2 + i^2 = a^2 + d^2 + g^2 \\ &= b^2 + e^2 + h^2 = c^2 + h^2 + i^2 = a^2 + e^2 + i^2 \\ &= c^2 + e^2 + g^2 = 3e^2. \end{aligned}$$

One example of an MSS of degree 3 is

$$M = \begin{bmatrix} 1 & 49 & 25 \\ 49 & 25 & 1 \\ 25 & 1 & 49 \end{bmatrix}.$$

An open question was raised by by M. LaBar in 1984 and reposed by Martin Gardner in 1996:

Open question (Labar, 1984)

Can a Magic Square possess nine distinct integer squares?

So far this conjecture remains unresolved. Motivated by this question, I try to establish for what primes Magic Squares of Cubes with 9 distinct cubes exist.

1.4 Magic Squares of Cubes Mod a Prime p

In this Master Thesis I focus on magic squares whose entries are cubes of integers modulo a prime number p. This type of MS is called Magic Squares of Cubes (MSC). It has the following form:

$$M = \begin{bmatrix} a^3 & b^3 & c^3 \\ d^3 & e^3 & f^3 \\ g^3 & h^3 & i^3 \end{bmatrix},$$

where $a, b, c, d, e, f, g, h, i \in \mathbb{Z}_p$ and mod p

$$\begin{aligned} a^3+b^3+c^3 &= d^3+e^3+f^3 = g^3+h^3+i^3 = a^3+d^3+g^3 \\ &= b^3+e^3+h^3 = c^3+h^3+i^3 \\ &= a^3+e^3+i^3 = c^3+e^3+g^3 = 3e^3. \end{aligned}$$

One example of a MSC with degree 3 over $\mathbb{Z}_3$ is

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

1.5 Definitions and Notations

Below I give formal definitions for magic squares and related concepts.

Definition 1.5.1. Let p be a prime. A magic square (MS) over $\mathbb{Z}_p$ is a 3×3 matrix $M = [a_{ij}]$ where $a_{ij} \in \mathbb{Z}_p$ such that

$$S = \sum_{j=1}^{3} a_{ij} = \sum_{i=1}^{3} a_{ij} = \sum_{i=1}^{3} a_{ii} = \sum_{j=1}^{3} a_{i(3-j)}.$$

This sum S is called the magic sum. The magic square M is trivial if all of its entries are the same. The degree of M is the number of its distinct entries in $\mathbb{Z}_p$. An MS is called a magic square of squares (MSS) over $\mathbb{Z}_p$ if all $a_{ij}s$ are squares in $\mathbb{Z}_p$. Similarly, An MS is called a magic square of cubes (MSC) over $\mathbb{Z}_p$ if all $a_{ij}s$ are cubes in $\mathbb{Z}_p$.

Definition 1.5.2. Two MSs are called isomorphic if they can be transformed into each other by rotations or reflections.

Example 1.5.3. over $\mathbb{Z}_{71}$,

$$M = \begin{bmatrix} 2^2 & 2^2 & 1^2 \\ 0^2 & 28^2 & 19^2 \\ 17^2 & 12^2 & 12^2 \end{bmatrix} = \begin{bmatrix} 4 & 4 & 1 \\ 0 & 3 & 6 \\ 5 & 2 & 2 \end{bmatrix},$$

is an MSS of degree 7.

If all $a_{ij}s$ are cubes in $\mathbb{Z}_p$ we obtain an MSC:

Example 1.5.4. Over $\mathbb{Z}_{11}$, the following matrix M is a magic square of cubes of degree 9 .

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

Note that, for some prime numbers p, all numbers in $\mathbb{Z}_p$ are cubes. For example, it is the case for $p = 11$:

Example 1.5.5. Consider the prime number $p = 11 \equiv 2 \pmod 3$. The following table shows that all numbers in $\mathbb{Z} + 11$ are cubes mod 11.

x	0	1	2	3	4	5	6	7	8	9	10
x^3	0	1	8	5	9	4	7	2	6	3	10

Thus every magic square in $\mathbb{Z}_{11}$ is also a magic square of cubes. It confirms Example 1.5.4.

In general for primes $p = 3m+2$ all the integers in $\mathbb{Z}_p$ are cubic residues while for primes $p = 3m + 1$, $m + 1$ of them are cubic residues.

1.6 Existing Results

A well-known result about magic squares of integers is given below:

Theorem 1.6.1. *Let $M = [a_{ij}]$ be a magic square of integers. Then the magic sum $S = 3a_{22}$.*

This theorem is trivial yet extremely important for 3×3 magic squares. It is also true for MS over $\mathbb{Z}_p$. In particular, the next theorem is its direct consequence.

Theorem 1.6.2. *Any 3×3 magic square $M = [a_{ij}]$ is determined by its 3 elements: in the top corners and the central one. Let $a_{11} = a$, $a_{13} = b$, $a_{22} = c$. Then*

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

characterizes all the magic squares [7].

Proposition 1.6.3 (Hengeveld and Li [8])**.** *For any prime $p > 5$, the degree of every 3×3 magic square over $\mathbb{Z}_p$ must be odd (1, 3, 5, 7, or 9).*

I use this theorem as a guideline for the project. I would like to find over which $\mathbb{Z}_p$ there exist MSCs with degree 3, 5, 7, or 9. It is a critical issue to find how many solutions the congruence $x^3 \equiv a \pmod{p}$ has for a fixed a.

The following result is known, but I would like to provide a short and simple proof.

Proposition 1.6.4. *For a given prime number $p = 3m + 2$, where m is an integer, every integer is a perfect cube mod p.*

Proof. Let x be any integer. If $p \mid x$ then $x \equiv 0^3 \pmod{p}$, done. If $p \nmid x$, by Fermat's Little Theorem we have $x^{p-1} \equiv 1 \pmod{p}$ and $x^p \equiv x \pmod{p}$. Thus

$x \equiv x^{2p-1} \equiv x^{2(3m+2)-1} \equiv (x^{2m+1})^3 \pmod p$. Therefore x is a cubic residue and all MSs are MSCs mod $p = 3m + 2$.

$\square$

To build magic squares of cubes we need a method to identify what numbers are cubes. The following theorem is a tool for finding cubes mod prime p. It was proven by R. Sharifi.

Theorem 1.6.5. *Sharifi [3]*

Let $p = 1 + 3x + 9x^2$ be a prime, where x is an integer. Then any divisor of x is a cubic residue (mod p).

Example 1.6.6. The integer $2971 = 1 + 3 \cdot 18 + 9 \cdot 18^2$ is a prime number. Since 2 and 3 are divisors of 18, they are cubic residues in $\mathbb{Z}_{2971}$.

I use Shariffi's theorem to construct prime numbers p such that over $\mathbb{Z}_p$, a desired set of numbers are cubic residues mod p.

Lemma 1.6.7. *Let p be a prime number in the form of $1 + 3x + 9x^2$ as stated in the Shariffi's theorem, where x is an integer. Consider the primary decomposition $x = p_1^{a_1} p_2^{a_2} ... p_n^{a_n}$, where $p_1, \ldots, p_n$ are distinct primes with $a_i > 0$ for all i. Then there are at least $(a_1 + 1)(a_2 + 1)...(a_n + 1)$ many nonzero cubic residues mod p. In particular, all the primes $p_1, p_2, \ldots, p_n$ are cubic residues mod p.*

Proof. The number of positive factors of x other than 1 is $(a_1+1)(a_2+1)...(a_n+1)-1$. By Sharifi's theorem, all of them are cubic residues $\pmod p$. These include the prime divisors $p_1, p_2, \ldots, p_n$.

□

The following theorem was proven by D. Lehmer, E. Lehmer, W. Mills, and J. Selfridge [5]. It enables us to construct MSCs with consecutive cubic residues.

Definition 1.6.8. [5]

For a prime p and $a \in \mathbb{Z}$, the n-tuple $(a, a+1, \ldots, a+r-1)$ is called a *Consecutive Cubic Residue (CCR)* of length r if $a, a+1, \ldots, a+r-1$ are all cubic residues mod p.

A natural question is. "For a fixed integer $r \geq 3$, how many prime numbers admit a CCR tuple of length r?" The following theorem answers the question:

Theorem 1.6.9. *(Selfridge [5])*

a) There are infinitely many primes whose smallest triplet of consecutive cubic residues is 23532, 23533, 23534.

b) Every prime, except for 2, 3, 7, 13, 19, 31, 37, 43, 61, 67, 79, 127, 283, has a triplet of consecutive cubic residues that does not exceed (23532, 23533, 23534).

The following theorem was proven by A. Brauer [6]. It proves invaluable for constructing MSCs with consecutive integers.

Theorem 1.6.10. *(Brauer [6])*

For every sufficiently large prime p there exist m consecutive positive integers r, $r+1, \ldots, r+m-1$, each of which is a k^{th} power residue of p, where $1 < k \in \mathbb{Z}$.

Proposition 1.6.11. *(Euler's Conjecture) A prime number p can be written as $p = A^2 + 27B^2$, where A and $B \in \mathbb{Z}$, if and only if 2 is a cubic residue $\pmod{p}$.*

1.7 Research Questions, Goals, and Methodology

I focus on magic squares of cubes modulo a prime p. In other words, every entry of an MS is the remainder when it is divided by a fixed prime number p. This approach grants me additional opportunities and freedom. The central question I want to address is paralell to La Bar's open question.

Research Questions

Let p be a prime number.

1. Over $\mathbb{Z}_p$, does a magic square of cubes of degree 9 exist?
2. What is the maximal degree of an MSC over $\mathbb{Z}_p$?
3. How many prime numbers admit MSCs of degree 3, 5, 7, or 9?
4. How can we construct an MSC with a given degree and/or magic sum?

Applying the theorems by Sharifi and Brauer, I attempt to obtain MSCs of degree 3, 5, 7, or 9 and claim that each type of the MSCs exist for infinitely many primes. Concrete examples were provided to illustrate my conclusions.

1.8 Main Results

In this research I established that there are infinitely many primes admitting MSCs of degree 3, 5, 7, or 9. It is proved that MSCs of degree 3 exist for any prime $p > 2$. Sharifi's theorem enables me to obtain MSCs of degree 3, 5, 7, or 9 for primes p in the form of $p = 1 + 3x + 9x^2$. I applied Brauer's theorem to prove that there are MSCs of any possible degree for infinitely many prime numbers. The proof is constructive by using consecutive cubic residues modulo appropriate primes.

Chapter 2

Cubic Residues in $\mathbb{Z}_p$

Throughout this section p denotes a prime number. By Proposition 1.6.4 if a prime is in the form $p \equiv 2 \pmod 3$ then every element in $\mathbb{Z}_p$ is a cubic residue. We are more interested in the other case where $p = 3m+1$, $m \in \mathbb{Z}$. Note that if $p = 3m+1$ is prime, then $p = 12k+1$ or $p = 12k+7$ for some integer k. A useful fact is that -3 is always a quadratic residue of p which may be used to help constructing MSCs mod p.

Lemma 2.0.1. *The number -3 is always a quadratic residue (perfect square) mod p where $p = 3m+1$ is a prime with $m \in \mathbb{Z}$.*

Proof. Let $p = 3m+1$. If $p = 12k+1$, then $p \equiv 1 \pmod 4 \implies \left(\frac{-1}{p}\right) = 1$. Also $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1$ for $p \equiv 1 \pmod 4$ by the law of quadratic reciprocity. Then we obtain $\left(\frac{-3}{p}\right)=\left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = (1)(1) = 1$.

If $p = 12k+7$ then because $p \equiv 3 \pmod 4$ we obtain $\left(\frac{-1}{p}\right) = -1$. By the law of quadratic reciprocity again, $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -1$ for $p \equiv 3 \pmod 4$. Then we obtain $\left(\frac{-3}{p}\right)=\left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = (-1)(-1) = 1$.

In either case, $-3 = p-3$ is a quadratic residue. $\square$

For the rest of this chapter, we assume $p = 3m+1$ for some $m \in \mathbb{Z}$ and p is a prime. Furthermore, assume $-3 \equiv c^2 \pmod p$ where c is an integer. Note that, $\forall a \in \mathbb{Z}$ $x^3 \equiv a \pmod p$ has exactly 3 distinct solutions.

Lemma 2.0.2. *The equation* $x^3 \equiv 1 \pmod p$, $p \geq 7$, *has exactly three distinct solutions:* $x_1 = 1$, $x_2 = 2^{-1}(c-1)$, *and* $x_3 = -2^{-1}(c+1)$.

Proof. Obviously, 1 is a solution. By checking,

$$\begin{aligned} (x_2)^3 &\equiv (2^{-1}(c-1))^3 \equiv 2^{-3}(c^3 - 3c^2 + 3c - 1) \\ &\equiv 2^{-3}(c(c^2+3) + 9 - 1) \equiv 2^{-3}(8) \equiv 1 \pmod p, \end{aligned}$$

thus $x_2 = 2^{-1}(c-1)$ is a cube root of 1. Similarly,

$$\begin{aligned} (x_3)^3 &\equiv (-2^{-1}(c+1))^3 \equiv -2^{-3}(c^3 + 3c^2 + 3c + 1) \\ &\equiv -2^{-3}(c(c^2+3) - 9 + 1) \equiv -2^{-3}(-8) \equiv 1 \pmod p. \end{aligned}$$

So $x_3 = -2^{-1}(c+1)$ is a root of 1. Next I show that x_1, x_2, x_3 are distinct. If any two numbers among these 3 are equal, there is a contradiction:

1. If $1 \equiv 2^{-1}(c-1) \pmod p$, then $3 \equiv c \pmod p \implies 9 \equiv -3 \pmod p \Rightarrow 12 \equiv 0 \pmod p$. It implies $p = 2$ or $p = 3$ which is a contradiction since $p \geq 7$.

2. If $1 \equiv -2^{-1}(c+1) \pmod p$ then $c \equiv -3 \pmod p \implies -3 \equiv 9 \pmod p \Rightarrow 12 \equiv 0 \pmod p$. Again it is a contradiction.

3. Suppose $x_2 \equiv x_3 \pmod p$ then $2^{-1}(c-1) \equiv -2^{-1}(c+1) \Rightarrow c - 1 \equiv -(c-1) \Rightarrow c \equiv 1 \pmod p$ and $-3 \equiv 1^2 \pmod p \Rightarrow 4 \equiv 0 \pmod p$, therefore $p = 2$, a contradiction.

$\square$

Next I show that these are the only solutions. Suppose, $x \in \mathbb{Z}$ and $x \neq 1$ but $x^3 \equiv 1 \pmod{p}$. Then $(x-1)(x^2+x+1) \equiv 0 \pmod{p} \implies x^2+x+1 \equiv 0 \pmod{p}$. By multiplying both sides of the congruence by 4 we obtain $4x^2+4x+4 \equiv 0 \pmod{p} \implies (2x+1)^2 \equiv -3 \pmod{p}$. By Lemma 2.0.2, $-3 \equiv c^2 \pmod{p}$. Thus $(2x+1)^2 \equiv c^2 \pmod{p} \implies (2x+1+c)(2x+1-c) \equiv 0 \pmod{p}$. Thus, $2x+1+c \equiv 0 \pmod{p}$ or $2x+1-c \equiv 0 \pmod{p} \implies x = 2^{-1}(c+1)$ or $x = 2^{-1}(c-1)$ which are x_2, x_3.

The next proposition generalizes the above result to the congruence equation $x^3 \equiv a$. It implies an important result concerning primes in the form of $p = 3m+1$.

Proposition 2.0.3. *For every $a \neq 0$ and $a \in \mathbb{Z}_p$, the equation $x^3 \equiv a^3 \pmod{p}$ has three distinct solutions: $y_1 = a$, $y_2 = ax_2$, and $y_3 = ax_3$ where $x_2 = 2^{-1}(c-1)$, $x = 2^{-1}(c+1)$.*

Obviously, $y_i^3 = (ax_i)^3 \equiv a^3x_i^3 \equiv a^3 \pmod{p}$, $i = 1, 2, 3$. So y_i is a solution. If $y_i \equiv y_j \Rightarrow ax_i \equiv ax_j \Rightarrow x_i \equiv x_j$ $(a \neq 0)$. Therefore y_1, y_2 and y_3 are distinct.

Proposition 2.0.4. *For every prime number $p = 3m+1$, there exist $m+1 = (p+2)/3$ distinct cubes, including 0.*

Proof. By Proposition 2.0.3 for every $0 \neq a \in \mathbb{Z}_p$ the equation $x^3 \equiv a^3 \pmod{p}$ has three distinct solutions x_1,x_2,x_3. Hence Z_p has $m = (p-1)/3$ distinct cubes in $\mathbb{Z}_p$. With the trivial 0 there are $m+1 = (p+2)/3$ perfect cubes in $\mathbb{Z}_p$. □

Example 2.0.5. For $p = 19$, there are 7 cubic residues 0, 1, 7, 8, 11, 12, 18:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
x^3	0	1	8	8	7	11	7	1	18	7	12	1	18

x	13	14	15	16	17	18
x^3	12	8	12	11	11	18

.

Chapter 3

Construction of Magic Squares of Cubes

The concept of degree of an MS is central to this research. In this chapter we establish what degrees are possible and later explore for what primes each degree can occur.

3.1 What Degrees are Possible for a Magic Square?

For a prime number $p > 7$ the following theorem states that every MS is of degree 1, 3, 5, 7, or 9. Therefore in this research I try to establish the existence of MSCs with odd degrees. The following theorem let us exclude degrees 4, 6, 8 and focus on degrees 3, 5, 7, and 9.

Theorem 3.1.1. *Let p be a prime number > 7. Consider the magic square M(a,b,c) configured in 1.6.2, where $a, b, c \in \mathbb{Z}_p$:*

1. $\deg(M(c,c,c)) = 1$*;*

2. $\deg(M(a,b,a)) = \deg(M(a,b,b)) = 3,$ *where* $a \neq b$*;*

3. $\deg(M(a,a,c)) = 5$ *when* $a \neq c$*;*

4. $\deg(M(a,b,c)) = 5$ *when* a*,*b*,*c *are all distinct and* $2c = a+b$*;*

5. $\deg(M(a,b,c)) = 7$ *when* a*,* b*,* c *are distinct and either* $a+c = 2b$ *or* $b+c = 2a$;

6. $\deg(M(a,b,c)) = 7$ *when* a, b, c *are all distinct,* $a+c \neq 2b$*,* $b+c \neq 2a$*, and* $a+b \neq 2c$*, plus one of the following holds: (1)* $2b+a \neq 3c$ *and* $2a+b = 3c$*; or (2)* $2a+b \neq 3c$ *and* $2b+a = 3c$*.*

7. $\deg M((a,b,c)) = 9$ *when* a, b, c *are all distinct,* $a+c \neq 2b$*,* $b+c \neq 2a$*,* $a+b \neq 2c$ $2a+b \neq 3c$*, and* $2b+a \neq 3c$*.*

Proof. Let $M(a,b,c)$ be the considered magic square over $\mathbb{Z}_p$:

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

1. It is obvious that $\deg M(c,c,c)) = 1$.

2. In case $a \neq b$, but $a = c$.

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

It is straightforward to check that all of $a, b, 2a-b$ are distinct in $\mathbb{Z}_p$. For example, if $2a-b = b$ implies $2a = 2b$. Since $p > 7$, $a = b$, a contradiction. Thus $\deg((M(a,b,a)) = 3$.

3. If $a = b \neq c$.
$$M(a,a,c) = \begin{bmatrix} a & 3c-2a & a \\ c & c & c \\ 2c-a & 2a-c & 2c-a \end{bmatrix}.$$
We can check that all $a, c, 2c-a, 2a-c, 3c-2a$ are distinct in $\mathbb{Z}_p$. For instance, if $3c-2a = a$, we obtain $3c = 3a$. But $p > 7$, so $a = c$, a contradiction. Thus $\deg(M(a,a,c)) = 5$.

In the following items, a, b, c are all distinct.

4. Assume $a + b = 2c$:
$$M(a,b,c) = \begin{bmatrix} 2c-b & c & b \\ 2b-c & c & 3c-2b \\ 2c-b & c & b \end{bmatrix}.$$
It is easy to check that $c, 2c-b, 2b-c, 3c-2b, b$ are distinct in $\mathbb{Z}_p$. For instance $2c-b = 2b-c$ implies $3c = 3b$. Since $p > 7$, $a = b$, a contradiction. Thus $\deg(M) = 5$.

5. In case of $a+c = 2b$ or $b+c = 2a$, without loss of generality, assume $a+c = 2b$, then
$$M(a,b,c) = \begin{bmatrix} 2b-c & 4c-3b & b \\ 2c-b & c & b \\ 2c-b & 3b-2c & 3c-2b \end{bmatrix}.$$
It is easy to establish that $b, c, 2b-c, 2c-b, 3b-2c, 4c-3b$, and $3c-2b$ are all distinct in $\mathbb{Z}_p$. For instance if $3b-2c = 4c-3b$ then $6b = 6c$. Since $p > 7$, $b = c$, a contradiction. Thus $\deg M(a,b,c) = 7$. The case $b+c = 2a$ is analogous.

6. If $a + b \neq 2c$, $a + c \neq 2b$, and $b + c \neq 2a$. There are two sub-cases.

Case 1. $3c - a \neq 2b$ and $3c - b = 2a$ (it is impossible to have both $2a + b = 3c$, $2b + a = 3c$ since then $a = b$, a contradiction).

Obviously, $a, b, c, c + b - a, c + a - b, 2c - b, 2c - a$ are all distinct in $\mathbb{Z}_p$. For instance $c + b - a = 2c - b$ implies $c + a = 2b$, a contradiction. Since $3c - b = 2a$ $a = 3c - a - b$ and $a + b - c = 2c - a$. Thus $\deg(M) = 7$.

Case 2. $3c - b \neq 2a$ and $3c - a = 2b$. This case is analogous to the previous one which gives $\deg(M) = 7$.

7. $a + b \neq 2c$, $a + c \neq 2b$, $b + c \neq 2a$, $2a + b \neq 3c$, and $2b + a \neq 3c$.

   Obviously, $a, b, c, c + b - a, c + a - b, 2c - b, 2c - a, a + b - c, 3c - a - b$ are all distinct in $\mathbb{Z}_p$. For instance, $3c - a - b = a$ implies $3c = 2a + b$, a contradiction. Thus $\deg(M) = 9$.

We covered all possible structures of $M(a, b, c)$ over $\mathbb{Z}_p$, $p > 7$. Thus the degrees of any MS must be 1, 3, 5, 7, or 9. □

3.2 Magic Squares of Cubes Modulo 2, 3, 5, or 7

In this section we explore MSCs of what degrees are possible for $p = 2, 3, 5$, or 7. Also all possible MSCs of degree 2 in $\mathbb{Z}_2$ and of degree 3 in $\mathbb{Z}_3$ are listed.

Proposition 3.2.1. *Consider $\mathbb{Z}_p$, $p = 2, 3, 5,$ or 7.*

1. *If $p = 2$ then there are four non-isomorphic MSCs.*
2. *If $p = 3$ then there are six non-isomorphic MSCs.*
3. *If $p = 5$ then there exist MSCs of degree 5 (maximal degree).*
4. *If $p = 7$ then there exist MSCs of degree 3 (maximal degree).*

Proof. 1. For $p = 2$, the maximal degree for a magic square over $\mathbb{Z}_2$ is 2 because there are only two elements in $\mathbb{Z}_2$. A fact is that the opposite corner elements must be the same. All the four non-isomorphic MSCs are presented here:

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

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

2. All six non-isomorphic MSCs over $\mathbb{Z}_3$ are given below:

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

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

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

□

By proposition 1.6.4 there are 5 cubic residues in $\mathbb{Z}_5$ since $5 = 3m + 2$. It can also be shown in the table below:

x	0	1	2	3	4
x^3	0	1	3	2	4

.

The maximal degree of MSCs over $\mathbb{Z}_5$ is 5, confirmed by the MSC below:

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

3. By proposition 2.0.4 there are 3 cubic residues in $\mathbb{Z}_7$ (0, 1, and 6). See the table below:

x	0	1	2	3	4	5	6
x^3	0	1	1	6	1	6	6

.

An MSC of degree 3 (maximal degree) over $\mathbb{Z}_7$ is:

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

3.3 Possible Degrees of Magic Squares of Cubes over $\mathbb{Z}_p$ for $p > 7$

One of the central questions I discuss in this work is what maximal degree an MSC may achieve mod a given prime p. MSCs of degrees 2, 3, 5, 7, and 9 are explored knowing that no MSCs of degrees 4, 6, or 8 exist. In this chapter we focus on methods of constructing MSCs of degrees 3, 5, 7, or 9.

Proposition 3.3.1. *Given a prime number $p = 3m+1$ where m is a positive integer, there exist at least m many non-isomorphic MSCs of degree 3 in $\mathbb{Z}_p$.*

Proof. By proposition 2.0.4, $\exists$ m cubic residues mod p. Assume x is such a residue. Then the matrix $M(0, x, 0)$ is an MSC of degree 3:

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

Obviously all entries are cubes. As was previously established in Proposition 2.0.4, the number of non-zero cubes of $p = 3m + 1$ is m. Thus we can construct m of such MSCs. □

Theorem 3.3.2. *For any prime $p = A^2 + 27B^2$ where A, $B \in \mathbb{Z}$, $\exists$ an MSC of degree 5 over $\mathbb{Z}_p$.*

Proof. If $p = A^2 + 27B^2$ is a prime, by Proposition 1.6.11, the number 2 is a cubic residue mod p. Thus the following matrix gives an MSC of degree 5:

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

□

<u>Remark.</u> The prime numbers 31, 43, 127, and many others are in the form stated in the above theorem. The result of the theorem guarantees that MSCs of degree 5 exist, one of which $M(-1, 1, 0)$, modulo these primes.

Applying Sharifi's Theorem, we construct MSCs of degree 5, 7, or 9 over $\mathbb{Z}_p$ for certain prime numbers p.

Proposition 3.3.3. *Assume p is a prime in the form of $p = 1 + 3x + 9x^2$, where x is a positive integer divisible by 6. Then over $\mathbb{Z}_p$, $M(-1, 1, 0)$ is an MSC of degree 5; Similarly, $M(3, 1, 2)$ and $M(2, 1, -1)$ are MSCs of degree 7 or 9 respectively.*

Proof. Since $2 \mid x$ and $3 \mid x$, by Sharifi's theorem 2, 3 are cubic residues mod p. Then the three mentioned matrices are MSCs of the indicated degree. $\square$

Consider the prime number $2971 = 1 + 3(18) + 3(18^2)$. Over $\mathbb{Z}_p$, the MSCs of degree 5, 7, or 9 are constructed in the following examples.

Example 3.3.4. $M(-1, 1, 0)$ is an MSC over $\mathbb{Z}_{2971}$:

$$M(-1,1,0) = \begin{bmatrix} -1 & 0 & 1 \\ 2 & 0 & -2 \\ -1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2970^3 & 0^3 & 1^3 \\ 286^3 & 0^3 & 2685^3 \\ 2970^3 & 0^3 & 1^3 \end{bmatrix}$$

with $\deg(M(-1, 1, 0)) = 5$.

Example 3.3.5. Two degree 7 MSCs over $\mathbb{Z}_{2971}$:

$$M(3,1,2) = \begin{bmatrix} 3 & -2 & 2 \\ 0 & 1 & 2 \\ 0 & 4 & -1 \end{bmatrix} = \begin{bmatrix} 422^3 & 2,685^3 & 286^3 \\ 0^3 & 1^3 & 286^3 \\ 0^3 & 1,579^3 & 2,970^3 \end{bmatrix},$$

$$M(2,1,0) = \begin{bmatrix} 2 & -3 & 1 \\ -1 & 0 & 1 \\ -1 & 3 & -2 \end{bmatrix} = \begin{bmatrix} 286^3 & 2,549^3 & 1^3 \\ (-1)^3 & 0^3 & 1^3 \\ (-1)^3 & 422^3 & 2,685^3 \end{bmatrix}.$$

Example 3.3.6. The matrix $M(2,1,-1)$ is an MSC of degree 9 in $\mathbb{Z}_{2971}$:

$$M(2,1,-1) = \begin{bmatrix} 2 & -6 & 1 \\ -2 & -1 & 0 \\ -3 & 4 & -4 \end{bmatrix} = \begin{bmatrix} 286^3 & 1119^3 & 1^3 \\ 2685^3 & 2970^3 & 0^3 \\ 2549^3 & 1579^3 & 1392^3 \end{bmatrix}.$$

Also, $1154^3 \equiv 7 \pmod{2971}$. Thus we have another instance of MSC of degree 9:

$$M(a,b,c) = \begin{bmatrix} 7 & -2 & 1 \\ -4 & 2 & 8 \\ 3 & 6 & -3 \end{bmatrix}.$$

Another interesting prime useful for constructing MSCs is, for instance, $p = 8191 = 1 + 3 \times 30 + 9 \times 30^2$.

Example 3.3.7. Let $p = 8191$. Over $\mathbb{Z}_p$, $M(2,1,-1)$, $M(4,2,1)$, and $M(3,2,0)$ are all MSC of degree 9. Since 2, 3, and 5 are divisors of 30, by Sharifi's theorem they are all cubic residues mod 8191. Precisely, $512^3 \equiv 2$, $1807^3 \equiv 3$, and $1938^3 \equiv 5$. Thus the following MSCs are all degree 9:

$$M(4,2,1) = \begin{bmatrix} 4 & -3 & 2 \\ -1 & 1 & 3 \\ 0 & 5 & -2 \end{bmatrix} = \begin{bmatrix} 32^3 & 6384^3 & 512^3 \\ (-1)^3 & 1^3 & 1807^3 \\ 0^3 & 1938^3 & 7679^3 \end{bmatrix}$$

and

$$M(3,2,0)=\begin{bmatrix}3 & -5 & 2\\ -1 & 0 & 1\\ -2 & 5 & -3\end{bmatrix}=\begin{bmatrix}1807^3 & 6253^3 & 512^3\\ (-1)^3 & 0^3 & 1^3\\ 7679^3 & 1938^3 & 6384^3\end{bmatrix}.$$

Example 3.3.8. The prime number 11,311 can be expressed as $11,131 = 1 + 3 \times 35 + 9 \times 35^2$, thus by Sharifi's theorem 5 and 7 are cubic residues mod 11,131. An MSC of degree 3 with magic sum 3 is constructed:

$$M(7,1,1)=\begin{bmatrix}7 & -5 & 1\\ -5 & 1 & 7\\ 1 & 7 & -5\end{bmatrix}.$$

Proposition 3.3.9. *For the prime $p = 1,922,383 = 1 + 3 \times 462 + 9 \times 462^2$, There exist MSCs of* deg $= 9$ *whose central elements are 2, 3, 4, 6, 7, 8, 9, or 11.*

Note that $462 = 2 \times 3 \times 7 \times 11$. By Sharifi's theorem 2, 3, 7, and 11 are cubes mod 1,922,383. The following constructions give the desired MSCs of degree 9:

Example 3.3.10. Over $\mathbb{Z}_{1922383}$, the following MSCs are all of degree 9 with central element 2, 3, 4, 6, 7, 9, or 11 respectively:

$$M(7,11,2)=\begin{bmatrix}7 & -12 & 11\\ 6 & 2 & -2\\ -7 & 16 & -3\end{bmatrix},\quad M(2,7,3)=\begin{bmatrix}2 & 0 & 7\\ 8 & 3 & -2\\ -1 & 6 & 4\end{bmatrix},$$

$$M(7,11,4) = \begin{bmatrix} 7 & -6 & 11 \\ 8 & 4 & 0 \\ -3 & 14 & 1 \end{bmatrix}, \qquad M(11,3,6) = \begin{bmatrix} 11 & 4 & 3 \\ -2 & 6 & 14 \\ 9 & 8 & 1 \end{bmatrix},$$

$$M(11,2,7) = \begin{bmatrix} 11 & 8 & 2 \\ -2 & 7 & 16 \\ 12 & 6 & 3 \end{bmatrix}, \qquad M(12,18,8) = \begin{bmatrix} 12 & -6 & 18 \\ 14 & 8 & 2 \\ -2 & 22 & 4 \end{bmatrix},$$

$$M(11,4,9) = \begin{bmatrix} 11 & 12 & 4 \\ 2 & 9 & 16 \\ 14 & 6 & 7 \end{bmatrix}, \qquad M(1,14,11) = \begin{bmatrix} 1 & 18 & 14 \\ 24 & 11 & -2 \\ 8 & 4 & 21 \end{bmatrix}.$$

Apparently, the number of MSC with degree 9 becomes larger as the number of prime factors of x in Sharifi's theorem grows.

3.4 Construction of MSC Using Consecutive Cubic Residues

In this section we will use the idea of consecutive cubic residues to construct MSCs of degrees 3, 5, 7, and 9. Using the theorems that guarantee the existence of consecutive cubic residues we are able to obtain fine results.

Theorem 3.4.1. *There are infinitely many primes p such that MSC of degree 3,5,7, or 9 exist over $\mathbb{Z}_p$.*

Proof. By Brauer's theorem [6], there are infinitely many primes p such that there are 9 consecutive cubic residues $r, r+1, \ldots, r+8 \bmod p$. We then construct the following magic squares of cubes using these consecutive cubic residues. The following are MSCs of various degrees over $\mathbb{Z}_p$.

MSC of degree 3:

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

MSC of degree 5:

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

MSC of degree 7:

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

Finally, we obtain the most important result of this research: there exist MSCs of degree 9 over $\mathbb{Z}_p$ for infinitely many primes p.

MSC of degree 9:

$$M(r+3, r+1, r+4) = \begin{bmatrix} r+3 & r+8 & r+1 \\ r+2 & r+4 & r+6 \\ r+7 & r & r+5 \end{bmatrix}.$$

$\square$

By a similar approach, we claim the main result which answers a similar question as the open question raised by La Bar.

Theorem 3.4.2. *There exist infinitely many primes p in the form of $3m+1$ such that MSC of degree 9 exist over $\mathbb{Z}_p$.*

Proof. By Brauer's theorem [6], there are infinitely many primes whose smallest triplet of consecutive cubic residues is (23532, 23533, 23534). All of these primes are of the form $3m+1$, because primes of the form $3m+2$ have (0,1,2) as the smallest triplet of consecutive cubic residues. Let p be such a prime. We can construct the following MSC over $\mathbb{Z}_p$:

$$M(23533,1,0) = \begin{bmatrix} 23533 & -23534 & 1 \\ -23532 & 0 & 23532 \\ -1 & 23534 & -23533 \end{bmatrix}.$$

By choosing a prime $p > 23534 + 23533 = 47,077$ we guarantee that all the entries of this MSC are distinct. Obviously, infinitely many primes mentioned above are greater than 47,077 which have (23532, 23533, 23534) as a triplet of consecutive cubic residue. $\square$

We already established that 2971 is a prime such that 2 and 3 are cubic residues in $\mathbb{Z}_{2971}$. Thus we can construct a 9-tuple of consecutive cube residues, $(-4,-3,-2,-1,0,1,2,3,4)$, and use it to obtain MSCs of degree 3, 5, 7, or 9. These are all possible degrees for MSCs over $\mathbb{Z}_{2971}$.

Example 3.4.3. Over $\mathbb{Z}_{2971}$,

An MSC of degree 3:

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

Degree 5:

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

Degree 7:

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

Degree 9:

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

Chapter 4

Concluding Remarks and Future Direction

In this research I answered questions concerning the existence of Magic Squares of Cubes of degrees 3, 5, 7, or 9 over $\mathbb{Z}_p$ where p is a prime. I proved that there are infinitely many primes in the form $3m+1$ with integer m for which MSCs of degree 3, 5, 7, or 9 exist over $\mathbb{Z}_p$. Along with theoretical results, concrete examples of such MSCs were demonstrated. However some questions remain unanswered and can be of interest to an inquisitive mathematician.

Further Questions

1. What primes do not admit MSC of degree 5 or 7 or 9?

2. For what prime p, the maximum degree of any MSC over $\mathbb{Z}_p$ is 3?

3. What prime numbers admit MSCs of degree r for a given $r = 5, 7$ or 9?

4. What prime numbers in the form of $p = 3m + 1$ have 9 consecutive cubic residues?

5. How many primes in the form of $p = 27A^2 + B^2$ with A, B being integers admit the cubic residue of 2 and thus an MSC of degree 5 exist?

6. Given $b \in \mathbb{Z}_p$, does there exist MSC over $\mathbb{Z}_p$ with the magic sum b?

Chapter 5

References

[1] K. Rosen, *Elementary Number Theory and its applications*. Addison-Wesley Publishing Company, 1984.

[2] N.A. Carella, *Primes In Cubic Arithmetic Progressions*. https://arxiv.org/ftp/arxiv/papers/1302/1302.0772.pdf.

[3] R. Sharifi, *On Cyclotomic Polynomials, Power Residues, and Reciprocity Laws*. http://math.ucla.edu/ sharifi/cycl.pdf.

[4] W. Adams, L. Goldstein, *Introduction to Number Theory*. Prentice-Hall, 1976.

[5] D.H. Lehmer, E. Lehmer, W.H. Mills, and J.L. Selfridge, *Machine Proof of a Theorem on Cubic Residues Mathematics of Computation* Vol. 16, No. 80 (Oct., 1962), pp. 407-415.

[6] D.H. Lehmer, E. Lehmer, W.H. Mills, *Pairs of consecutive power residues* Canad.J. Math.

[7] L. Sallows, *The Lost Theorem* The Mathematical Intelligence, 1997.

[8] S. Hengeveld, *Construction and Analysis of Magic Squares of Squares over Certain Finite Fields*. Master Thesis, Montclair State University, 2012.