LABORATORY REPORT: CYCLIC DIFFERENCE SETS

KHANH DINH

ABSTRACT. In this laboratory, we examine a special class of CDS derived from the non-zero squares modulo a given integer m. The study begins with an introduction to modular arithmetic, establishing foundational concepts. Utilizing theoretical proofs and MATLAB-based computations, we formulate and test conjectures to determine conditions under which these sets exhibit cyclic difference properties. The analysis reveals critical relationships between the parameters of CDS and their underlying modular structures.

1. INTRODUCTION

Cyclic difference sets (CDS) are an intriguing mathematical concept rooted in modular arithmetic, with applications spanning cryptography, coding theory, and design theory. This laboratory report integrates theoretical proofs with MATLAB-based experimentation to investigate cyclic difference sets, providing a comprehensive framework for understanding their behavior. The findings hold potential relevance in advancing mathematical theory and practical applications alike.

Before defining a cyclic difference set, we need to understand modular arithmetic. To explain the setup of modular arithmetic, we first define division in the integers:

Definition 1.1. An integer a divides an integer b if there exists an integer c such that $b = ac$. This relationship is denoted as $a \mid b$. [1]

Example 1.2. Some examples of whole number division are as follows:

(1) When $a = 6$ and $b = 18$: There exists an integer $c = 3$ such that $18 = 6 \cdot 3$. Hence, $6 \mid 18$.

(2) When $a = 5$ and $b = 14$: There is no integer c such that $14 = 5 \cdot c$. Thus, $5 \nmid 14$.

Considering special cases:

Date: December 31, 2024.

I would like to express my sincere gratitude to Professor Robinson for her meticulous proofreading and invaluable feedback on this document.

(1) When $a = 0$ and $b = 5$: 0 does not divide 5. For 0 to divide 5, there would need to exist an integer c such that $5 = 0 \cdot c$, but this is impossible as any number multiplied by 0 is 0.

(2) When $a = 5$ and $b = 0$: There exists an integer $c = 0$ such that $0 = 5 \cdot 0$. Hence, $5 \mid 0$.

(3) When $a = -7$ and $b = 35$:: There exists an integer $c = -5$ such that $35 = -7 \cdot (-5)$. Thus, $-7 \mid 35$.

Hence this definition works consistently for both positive and negative integers. Next, we need to generalize the definition of division to quotient and remainder division. For this step, we have the following Division Algorithm:

Theorem 1.3. *For any integers a and m with $m > 0$, there exist unique integers q (the quotient) and r (the remainder) such that $a = mq + r \quad$ where $\quad 0 \leq r < m$.*

We will not prove this Theorem here.

Example 1.4. Some examples of division with a quotient and remainder are as follows:

(1) When $a = 23$ and $m = 5$, we can write: $23 = 5 \cdot 4 + 3$, where the quotient $q = 4$ and the remainder $r = 3$. Note that $0 \leq 3 < 5$ and $\lfloor \frac{23}{5} \rfloor = 4$.

(2) When $a = -17$ and $m = 4$, we can write: $-17 = 4 \cdot (-5) + 3$, where the quotient $q = -5$ and the remainder $r = 3$. Note that $0 \leq 3 < 4$ $\lfloor \frac{-17}{4} \rfloor = -5$.

The Division Algorithm allows us to set up congruence classes in the integers. For example, if $m = 7$, we can write the integers in rows and columns so that we can see that each integer a will lie in exactly one row, the value of its quotient q, and exactly in one column, the value of its remainder r.

.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
$q = -1$	-7	-6	-5	-4	-3	-2	-1
$q = 0$	0	1	2	3	4	5	6
$q = 1$	7	8	9	10	11	12	13
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.

This way we see that upon division by 7 the remainder classes $\{[0],[1],[2],[3],[4],[5],[6]\}$ each stand for the integers that are congruent to one another. So for example $[5] = \{...., -9, -2, 5, 12, 19, ...\} = \{7q+5 | \text{for any } q \in \mathbb{Z}\}$.

Definition 1.5. If a is congruent to b modulo m we write that $a \equiv b \bmod m$. There are 4 different equivalent definitions for what we mean when we say that a is congruent to b modulo m. A number a is congruent to b modulo m if and only if one of the following holds:

(1) m divides the difference $a-b$.

(2) $a = b + mk$ for some integer k.

(3) $a - b = mk$ for some k in the integers.

(4) a and b have the same least positive remainder upon division by m guaranteed by the Division Algorithm.

Example 1.6. Let us look at some examples of congruence modulo m:

(1) Let $a = -23$, $b = 1$, and $m = 8$. From the multiple definitions for congruence, we see that:

- The difference $-23 - 1 = -24$, and 8 divides -24.
- We can write $-23 = 1 + 8 \cdot (-3)$, where $k = -3$ is an integer.
- The difference $-23 - 1 = -24$ can be written as $-24 = 8 \cdot (-3)$, where $k = -3$ is an integer.
- The least positive remainder when dividing -23 by 8 is 1 since $-23 = 8(-3) + 1$, and the least positive remainder when dividing 1 by 8 is also 1 since $1 = 8(0) + 1$.

Thus, $-23 \equiv 1 \pmod 8$.

(2) Consider $a = 17$, $b = 5$, and $m = 6$.

- Using Definition 1: $17 - 5 = 12$, and 6 divides 12.
- Using Definition 2: $17 = 5 + 6 \cdot 2$, with $k = 2$.
- Using Definition 3: $17 - 5 = 6 \cdot 2$, with $k = 2$.
- Using Definition 4: Both 17 and 5 have a remainder of 5 when divided by 6 since $17 = 6(2) + 5$ and $5 = 6(0) + 5$.

Thus, $17 \equiv 5 \bmod 6$.

(3) Consider $a = -11$, $b = 1$, and $m = 6$.

- Using Definition 1: $-11 - 1 = -12$, and 6 divides -12.
- Using Definition 2: $-11 = 1 + 6 \cdot (-2)$, with $k = -2$.
- Using Definition 3: $-11 - 1 = 6 \cdot (-2)$, with $k = -2$.
- Using Definition 4: Both -11 and 1 have a remainder of 1 when divided by 6 since $-11 = 6(-2) + 1$ and $1 = 6(0) + 1$.

Thus, $-11 \equiv 1 \bmod 6$.

The following proposition is very important when we compute with modular arithmetic.

Proposition 1.7. *If $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then $a \pm c \equiv b \pm d \bmod m$ and $ac \equiv bd \bmod m$.*

Proof. We are given that $a \equiv b \bmod m$ and $c \equiv d \bmod m$. By the definition of congruence, this means $a = b + mk_1 \quad \text{and} \quad c = d + mk_2$ for some integers k_1 and k_2. Consider the expression:

$$(a \pm c) = (b + mk_1) \pm (d + mk_2) = b \pm d + m(k_1 \pm k_2).$$

Thus, by definition of congruence since $k_1 \pm k_2$ is an integer, $a \pm c \equiv b \pm d \bmod m$.

Consider the expression ac:

$$ac = (b + mk_1)(d + mk_2) = bd + bmk_2 + mk_1 d + m^2 k_1 k_2 = bd + m(bk_2 + dk_1 + mk_1 k_2)$$

Thus, by definition of congruence, $ac \equiv bd \bmod m$. Hence, we proved that if $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then $a \pm c \equiv b \pm d \bmod m$ and $ac \equiv bd \bmod m$. □

This proposition means that if two numbers are congruent modulo m, then adding, subtracting, or multiplying them with other numbers that are also congruent modulo m will get results that are still congruent modulo m. Therefore, it allows us to simplify the computation by working with smaller, equivalent numbers instead of directly calculating a large number. Let us see an example:

Example 1.8. Suppose we need to compute what day it is 60^{345} days from today. Then we need to compute $60^{345} \equiv$ ____ mod 7. To begin, we can reduce 60 modulo 7. This gives us $60 \equiv 4 \bmod 7$. Thus, using our proposition 345 times, we can rewrite our original expression as $60^{345} \equiv$

$4^{345} \bmod 7$. Next, we observe the pattern in powers of 4 modulo 7:

$$\begin{aligned} 4^1 &\equiv 4 \pmod 7, & \text{so} \quad 4^{3k+1} &\equiv 4 \pmod 7, \\ 4^2 &\equiv 2 \pmod 7, & \text{so} \quad 4^{3k+2} &\equiv 2 \pmod 7, \\ 4^3 &\equiv 1 \pmod 7, & \text{so} \quad 4^{3k} &\equiv 1 \pmod 7. \end{aligned}$$

This shows that powers of 4 cycle every 3 steps: $4, 2, 1$. Since $345 = 3k$ (where $k = 115$), we find $4^{345} = 4^{3k} \equiv 1 \pmod 7$. Therefore, we conclude that $60^{345} \equiv 4^{345} \equiv 4^3 \equiv 1 \bmod 7$.

In this example, the proposition allowed us to replace 60 with 4 modulo 7 and leverage the cycle in powers of 4 to quickly find the answer without directly calculating 4^{345}. We know even when m is not prime remainders, mod m will repeat since there are only m of them.

Definition 1.9. The notation $\mathbb{Z}/m\mathbb{Z}$ denotes the **set of congruence classes modulo** m. This set consists of the elements $\{[0], [1], [2], \ldots, [m-1]\}$, where each class $[a]$ represents all integers congruent to a modulo m. For example, the class $[1]$ includes all integers n such that $[1] = \{1 + m\varepsilon \mid \varepsilon \in \mathbb{Z}\}$.

Addition and multiplication are defined on these congruence classes by performing the operations on the representatives of the classes and then taking the result modulo m. For convenience, we often simplify the notation by representing the set as $\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, \ldots, m-1\}$, where $0 = [0], 1 = [1]$, and so forth.

Let's examine addition and multiplication modulo $m = 5$ by using tables. The addition table modulo 5 shows the results of adding elements of $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ and reducing each sum modulo 5.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Each cell in the table represents the result of adding the row and column headers, reduced modulo 5. For example, $3+4=7\equiv 2 \pmod 5$, so in the row for 3 and column for 4, we find 2.

The multiplication table modulo 5 shows the results of multiplying elements of $\mathbb{Z}/5\mathbb{Z}$ and reducing each product modulo 5. For example, $3\times 4=12\equiv 2 \pmod 5$, which we find in the row for 3 and column for 4 as 2.

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Squares modulo m refers to the set of possible values that can be achieved by squaring each element in $\mathbb{Z}/m\mathbb{Z}$ (the set of integers modulo m) and then taking the result modulo m. The set of distinct values obtained in this way is known as the set of squares modulo m. For example, if $m=5$, the elements of $\mathbb{Z}/5\mathbb{Z}$ are $\{0,1,2,3,4\}$, and we calculate the squares of each element modulo 5:

$$0^2\equiv 0 \pmod 5,$$

$$1^2\equiv 1 \pmod 5,$$

$$2^2\equiv 4 \pmod 5,$$

$$3^2\equiv 4 \pmod 5,$$

$$4^2\equiv 1 \pmod 5.$$

Thus, the set of squares modulo 5 is $\{0,1,4\}$. Notice that not all elements of $\mathbb{Z}/5\mathbb{Z}$ appear as squares; in this case, 2 and 3 are not squares modulo 5.

Now we are ready to define a general Cyclic Difference Set.

Definition 1.10. A Cyclic Difference Set (CDS) is a subset D of $\mathbb{Z}/m\mathbb{Z}$ such that:

(1) The distinct differences of elements in D represent all $m-1$ non-zero elements in $\mathbb{Z}/m\mathbb{Z}$.

(2) Each non-zero element in $\mathbb{Z}/m\mathbb{Z}$ is represented the same number of times as the distinct difference of elements in D.

There are three important parameters for a CDS: m, k, and λ. m is the order of the cyclic group $\mathbb{Z}/m\mathbb{Z}$, k is the number of elements in D, and λ is the number of times each non-zero element in $\mathbb{Z}/m\mathbb{Z}$ is a difference between two elements in D. The symbol D denotes the **set of non-zero squares** in $\mathbb{Z}/m\mathbb{Z}$. In this laboratory, we will study special cyclic difference sets that come from sets D that are comprised of the non-zero squares modulo m in $\mathbb{Z}/m\mathbb{Z}$.

The **non-zero squares modulo** m are defined as the elements of the form $a^2 \pmod{m}$ where a is a non-zero element in $\mathbb{Z}/m\mathbb{Z}$ and the result is distinct modulo m.

For our purposes, we will examine the set of non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ and investigate under which conditions this set forms a cyclic difference set (CDS) in $\mathbb{Z}/m\mathbb{Z}$. Specifically, we will determine the values of k and λ for which these squares create a CDS. We will prove theorems and make conjectures about these questions.

To illustrate these concepts, let's look at some examples to see how the set of non-zero squares can form a CDS under certain conditions.

Example 1.11. Consider $m = 7$. The elements of $\mathbb{Z}/7\mathbb{Z}$ are $\{0,1,2,3,4,5,6\}$.

The non-zero squares modulo 7 are:

$$1^2 \equiv 1 \pmod{7}, \quad 2^2 \equiv 4 \pmod{7}, \quad 3^2 \equiv 2 \pmod{7},$$

$$4^2 \equiv 2 \pmod{7}, \quad 5^2 \equiv 4 \pmod{7}, \quad 6^2 \equiv 1 \pmod{7}.$$

Thus, the set of non-zero squares D is $\{1,2,4\}$, and we have $k = 3$. Now, let's compute the differences between elements in D:

$$1-2 \equiv 6 \pmod{7}, \quad 1-4 \equiv 4 \pmod{7}, \quad 2-1 \equiv 1 \pmod{7},$$

$$2-4 \equiv 5 \pmod{7}, \quad 4-1 \equiv 3 \pmod{7}, \quad 4-2 \equiv 2 \pmod{7}.$$

The differences $\{1,2,3,4,5,6\}$ cover all non-zero elements in $\mathbb{Z}/7\mathbb{Z}$, and each appears exactly once. Thus, $\lambda = 1$, and $D = \{1,2,4\}$ forms a CDS in $\mathbb{Z}/7\mathbb{Z}$.

Example 1.12. Consider $m = 8$. The elements of $\mathbb{Z}/8\mathbb{Z}$ are $\{0,1,2,3,4,5,6,7\}$.

The non-zero squares modulo 8 are:

$$1^2 \equiv 1 \pmod 8, \quad 2^2 \equiv 4 \pmod 8, \quad 3^2 \equiv 1 \pmod 8,$$

$$4^2 \equiv 0 \pmod 8, \quad 5^2 \equiv 1 \pmod 8, \quad 6^2 \equiv 4 \pmod 8,$$

$$7^2 \equiv 1 \pmod 8.$$

Thus, the set of non-zero squares D is $\{1,4\}$, and we have $k = 2$. Now, let's compute the distinct differences between elements in D: $1-4 \equiv 5 \pmod 8$, $4-1 \equiv 3 \pmod 8$. The differences $\{3,5\}$ do not cover all non-zero elements in $\mathbb{Z}/8\mathbb{Z}$, so $D = \{1,4\}$ does not form a CDS in $\mathbb{Z}/8\mathbb{Z}$.

As these examples show, whether the set of non-zero squares forms a CDS depends on the structure of $\mathbb{Z}/m\mathbb{Z}$ and the values of m, k, and λ. Our goal is to identify when the set of non-zero squares modulo m satisfies these properties to form a CDS and to determine the corresponding parameters k and λ in $\mathbb{Z}/m\mathbb{Z}$.

2. Proofs

The following section builds upon the foundational concepts introduced earlier, applying modular arithmetic properties to develop results about differences, squares, and their distinctness in modular arithmetic. Each proof is followed by examples to illustrate the meaning and application of the result.

Theorem 2.1. *Given k numbers, there are $k(k-1)$ distinct differences that can be made with those k numbers where $k \geq 2$.*

Proof. We will prove this by induction on k. For our base case, we take $k = 2$.

With two numbers a_1 and a_2, there are two distinct differences: $a_1 - a_2$ and $a_2 - a_1$. Substituting $k = 2$ into the formula, we get: $2(2-1) = 2$. Thus, the formula holds for $k = 2$.

For our inductive hypothesis, we assume that for some integer $k = n \geq 2$, the number of distinct differences that can be formed with n numbers is $n(n-1)$.

Inductive Step: We need to prove that for $n+1$ numbers, there are $(n+1)n$ distinct differences.

Consider adjoining an $(n+1)^{\text{th}}$ number, a_{n+1}, to the set of n numbers. The new number a_{n+1} can form a difference with each of the n existing numbers in two ways: $a_{n+1} - a_i$ and $a_i - a_{n+1}$ for $i = 1, 2, \ldots, n$, giving $2n$ additional differences.

According to our inductive hypothesis, the first n numbers already have $n(n-1)$ distinct differences. Adding the $2n$ new differences involving a_{n+1} gives a total of:

$$n(n-1) + 2n = n^2 - n + 2n = n^2 + n = n(n+1).$$

Thus, by mathematical induction, we have shown that for any integer k, there are $k(k-1)$ distinct differences that can be made with those k numbers. □

Example 2.2. Let $k = 3$ and consider the numbers $\{1, 2, 3\}$. The distinct differences are:

$$1-2, 2-1, 1-3, 3-1, 2-3, 3-2.$$

This gives $3(3-1) = 6$ differences, matching the formula. Similarly, for $k = 4$, the set $\{1, 2, 3, 4\}$ generates $4(4-1) = 12$ differences.

Corollary 2.3. *If the set of non-zero squares forms a cyclic difference set in $\mathbb{Z}/m\mathbb{Z}$ and k is the number of non-zero squares then $k(k-1) = \lambda(m-1)$.*

Proof. Let $D \subset \mathbb{Z}/m\mathbb{Z}$ be a CDS with k elements. By definition, each non-zero element in $\mathbb{Z}/m\mathbb{Z}$ must be represented exactly λ times among the differences between elements in D.

Since D has k elements, there are $k(k-1)$ distinct differences that can be made, as shown in Theorem 2.1. Each of these differences corresponds to a non-zero element in $\mathbb{Z}/m\mathbb{Z}$, with each such element appearing exactly λ times.

Thus, the total number of distinct differences can also be expressed as the product of the number of non-zero elements in $\mathbb{Z}/m\mathbb{Z}$, which is $m-1$, and the number of times each appears, λ. Therefore, we have proved that $k(k-1) = \lambda(m-1)$. □

Example 2.4. Let $m = 7$ and $D = \{1,2,4\}$, the set of non-zero squares modulo 7. Then $k = 3$, $m-1 = 6$, and $\lambda = 1$. The distinct differences are: $1-2$, $2-1$, $1-4$, $4-1$, $2-4$, $4-2$. Thus, $k(k-1) = 3 \cdot 2 = 6$, which equals $\lambda(m-1) = 1 \cdot 6$.

Proposition 2.5. *For x in $\mathbb{Z}/m\mathbb{Z}$, $-x$ is congruent to $m-x$ modulo m.*

Proof. Consider $-x-(m-x) = -x-m+x = -m$. Since m divides $-m$, we have $m \mid -x-(m-x)$. Therefore, $-x \equiv (m-x) \pmod{m}$. □

Example 2.6. Let $m = 5$ and $x = 3$. Then $-x = -3 \equiv 2 \pmod{5}$ and $m-x = 5-3 = 2$. Thus, $-x \equiv m-x$.

Proposition 2.7. *For $0 \leq x \leq m-1$, we have that $x^2 \equiv (m-x)^2 \pmod{m}$.*

Proof. Consider $x^2-(m-x)^2 = -m^2+2mx = m(-m+2x)$. Since m divides $m(-m+2x)$, it follows that m divides $x^2-(m-x)^2$. Therefore, by definition, we have $x^2 \equiv (m-x)^2 \pmod{m}$. □

Example 2.8. Let $m = 7$ and $x = 2$. Then $x^2 = 4$ and $(m-x)^2 = (7-2)^2 = 5^2 = 25 \equiv 4 \pmod{7}$. This calculation verifies $x^2 \equiv (m-x)^2$.

Corollary 2.9. *For any odd number m, the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is less than or equal to $\frac{m-1}{2}$.*

Proof. Let m be an odd integer. From Proposition 2.7, In $\mathbb{Z}/m\mathbb{Z}$, each element $x \in \{1,2,\ldots,m-1\}$ has $x^2 \equiv (m-x)^2 \pmod{m}$. Thus, the square of x and the square of $m-x$ are congruent and, hence, not distinct. This pairing halves the number of distinct non-zero squares.

Since m is odd, there are $m-1$ non-zero elements in $\mathbb{Z}/m\mathbb{Z}$. Dividing this set of non-zero elements into pairs, we find that the number of distinct non-zero squares is at most $\frac{m-1}{2}$. □

Example 2.10. For $m = 7$, the non-zero elements of $\mathbb{Z}/7\mathbb{Z}$ are $1,2,3,4,5,6$. The squares are $1^2 = 1, 2^2 = 4, 3^2 = 9 \equiv 2, 4^2 = 16 \equiv 2, 5^2 = 25 \equiv 4, 6^2 = 36 \equiv 1$, so there are 3 distinct squares: 1, 2, and 4, which is less than or equal to $\frac{7-1}{2} = 3$.

Corollary 2.11. *For any even number m, the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is less than or equal to $\frac{m}{2}$.*

Proof. Let m be an even integer. In this case, m has $m-1$ non-zero elements. Similarly to the odd case, we apply Proposition 2.7, where $x^2 \equiv (m-x)^2 \pmod{m}$, so each non-zero element x pairs with $m-x$, getting the same square modulo m.

However, for even m, the element $\frac{m}{2}$ pairs with itself, as $m - \frac{m}{2} = \frac{m}{2}$. Thus, $\frac{m}{2}$ squared remains distinct by itself, while other elements pair with their opposites. Therefore we have $\frac{m}{2}$ distinct non-zero squares modulo m. □

Example 2.12. For $m = 8$, the non-zero elements of $\mathbb{Z}/8\mathbb{Z}$ are $1,2,3,4,5,6,7$. The squares are $1^2 = 1, 2^2 = 4, 3^2 = 9 \equiv 1, 4^2 = 16 \equiv 0, 5^2 = 25 \equiv 1, 6^2 = 36 \equiv 4, 7^2 = 49 \equiv 1$, so there are 3 distinct squares: 1, 4, and 0, which is less than or equal to $\frac{8}{2} = 4$.

Theorem 2.13. *If $m = a^2$ for some $a > 1$, then the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is less than $\frac{m-1}{2}$ if m is odd.*

Proof. Since $m = a^2$ is odd, we know that $m-1$ is even. We have the table of modular congruence with $m = a^2$ as follows:

x	0	1	$\cdots$	$\frac{m-1}{2}$	$\frac{m+1}{2}$	$\cdots$	$m-1$
x^2	0	1	$\cdots$	$\left(\frac{m-1}{2}\right)^2$	$\left(\frac{m+1}{2}\right)^2$	$\cdots$	$(m-1)^2$

Since $m = a^2$ is odd, a must also be odd. We know that $m = a^2$, so a is an integer, and $a \geq 3$ (since $a > 1$ and odd). This setup implies that $a^2 > 2a \Rightarrow a^2 - 1 \geq 2a$. Dividing both sides by 2, we get $\frac{a^2-1}{2} \geq a$. Thus, a serves as a lower bound, and we have $3 \leq a \leq \frac{m-1}{2}$. Consequently, there is at least one value $x = a$ where $x^2 \equiv 0 \pmod{m}$ for $0 < x < \frac{m-1}{2}$. This redundancy in values where x^2 is congruent to zero modulo m indicates that not all values within the range contribute distinct non-zero squares. Therefore the theorem holds. □

Example 2.14. For $m = 9$, the non-zero elements of $\mathbb{Z}/9\mathbb{Z}$ are $1,2,3,4,5,6,7,8$. The squares are $1^2 = 1, 2^2 = 4, 3^2 = 9 \equiv 0, 4^2 = 16 \equiv 7, 5^2 = 25 \equiv 7, 6^2 = 36 \equiv 0, 7^2 = 49 \equiv 4, 8^2 = 64 \equiv 1$, so there are 3 distinct squares: 1, 4, and 7, which is less than $\frac{9-1}{2} = 4$.

Theorem 2.15. *If $m = ab$ where $1 < a < b < m$ and a and b are both odd, then the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is strictly less than $\frac{m-1}{2}$.*

Proof. Since m is the product of two odd numbers a and b, m is odd. By Corollary 2.9, the maximum number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is $\frac{m-1}{2}$. We will show that this maximum is not reached.

Let $m = ab$ with $1 < a < b < m$. Consider the squares of $a+b$ and $a-b$ modulo m:

$$(a+b)^2 \equiv a^2 + b^2 + 2ab \pmod{m},$$

$$(a-b)^2 \equiv a^2 + b^2 - 2ab \pmod{m}.$$

Simplifying these modulo $m = ab$, we observe that:

$$(a+b)^2 \equiv a^2 + b^2 \pmod{m}, \quad (a-b)^2 \equiv a^2 + b^2 \pmod{m}.$$

Thus, $(a+b)^2$ and $(a-b)^2$ are congruent modulo m.

Using Proposition 2.7, the additive inverses of these values also share the same squares. Hence, we have four potentially distinct elements: $(a+b)^2$, $(a-b)^2$, $(m-(a+b))^2$, $(m-(a-b))^2$. We argue these values are distinct:

(1) $a+b \neq m-(a+b)$ and $a-b \neq m-(a-b)$, since no number equals its additive inverse modulo m.

(2) $a+b \neq a-b$, as $a \neq b$.

(3) $a+b \neq m-(a-b)$. Simplifying $a+b \neq m-a+b$, we get $a \neq m-a$, which is true since $1 < a < m$.

Since $m = ab$ and $1 < a < b < m$, at least four of these squares must map to the same equivalence class modulo m, and two of these four repeats must be in range $1 \leq x \leq \frac{m-1}{2}$. Thus $P(n)$ holds. □

Example 2.16. For $m = 15$, the non-zero elements of $\mathbb{Z}/15\mathbb{Z}$ are $1,2,3,4,5,6,7,8,9,10,11,12,13,14$. The squares are $1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 16 \equiv 1, 5^2 = 25 \equiv 10, 6^2 = 36 \equiv 6, 7^2 = 49 \equiv 4, 8^2 = 64 \equiv 4, 9^2 = 81 \equiv 6, 10^2 = 100 \equiv 10, 11^2 = 121 \equiv 1, 12^2 = 144 \equiv 9, 13^2 = 169 \equiv 4, 14^2 = 196 \equiv 1$, so there are 5 distinct squares: 1, 4, 6, 9, and 10, which is strictly less than $\frac{15-1}{2} = 7$.

Theorem 2.17. *If m is an odd prime, then the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is exactly $\frac{m-1}{2}$.*

Proof. Assume $0 \leq x < y \leq \frac{m-1}{2}$. We want to show that $x^2 \not\equiv y^2 \pmod{m}$ so that all the $\frac{m-1}{2}$ possible values from 1 to $\frac{m-1}{2}$ have distinct squares. We assume for the sake of contradiction that $x^2 \equiv y^2 \pmod{m}$. Then we can express this as $x^2 = y^2 + mk \quad$ for some integer k. This equation can be rearranged to $x^2 - y^2 = mk$. Factoring the difference of squares, we get $(x+y)(x-y) = mk$.

Since m is prime, it must divide either $x+y$ or $x-y$. Therefore, we have two cases:

1. $x+y \equiv 0 \pmod{m}$: This result implies $x+y = m\ell$ for some integer ℓ. However, this result means that $x \equiv -y \pmod{m}$ and so $x \equiv m-y \pmod{m}$ but since $y \leq \frac{m-1}{2}, \quad m-y > \frac{m-1}{2}$ and that is impossible since $x \leq \frac{m-1}{2}$. 2. $x-y \equiv 0 \pmod{m}$: This result implies $x = y \pmod{m}$, which contradicts our assumption that $x < y$.

Thus, it is impossible for $x^2 \equiv y^2 \pmod{m}$ under the given conditions. This result shows that the non-zero squares are distinct modulo m. Furthermore, the additive inverses are only values for which the squares repeat and then occur for values after $\frac{m-1}{2}$, which means that the distinct squares are precisely the values x^2 for x in $0 \leq x \leq \frac{m-1}{2}$. □

Example 2.18. For $m = 7$, the non-zero elements of $\mathbb{Z}/7\mathbb{Z}$ are $1,2,3,4,5,6$. The squares are $1^2 = 1, 2^2 = 4, 3^2 = 9 \equiv 2, 4^2 = 16 \equiv 2, 5^2 = 25 \equiv 4, 6^2 = 36 \equiv 1$, so there are exactly 3 distinct non-zero squares: 1, 2, and 4, which is $\frac{7-1}{2} = 3$.

Theorem 2.19. *If the number of non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is $\frac{m-1}{2}$, then m is an odd prime.*

Proof. Clearly, m is odd if the number of non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is $\frac{m-1}{2}$. It is also clear that m cannot be expressed as $a \cdot b$ where $1 < a < b < m$ and $m \neq a^2$ where a is odd.

Thus, if $\frac{m-1}{2}$ equals the number of squares, then m is odd prime. □

Example 2.20. For $m = 5$, the non-zero elements of $\mathbb{Z}/5\mathbb{Z}$ are $1,2,3,4$. The squares are $1^2 = 1, 2^2 = 4, 3^2 = 9 \equiv 4, 4^2 = 16 \equiv 1$, so there are 2 distinct squares: 1 and 4, which is $\frac{5-1}{2} = 2$. Hence, $m = 5$ is an odd prime.

Theorem 2.21. *If D (the non-zero squares in $\mathbb{Z}/m\mathbb{Z}$) is a cyclic difference set and $k = \frac{m-1}{2}$, then m is prime and $m = 4\lambda + 3$.*

Proof. We begin with Corollary 2.3, which states that if the set of non-zero squares forms a cyclic difference set in $\mathbb{Z}/m\mathbb{Z}$ and k is the number of non-zero squares, then $k(k-1) = \lambda(m-1)$, where $k = \frac{m-1}{2}$. Substituting $k = \frac{m-1}{2}$ into this equation, we get $\left(\frac{m-1}{2}\right)\left(\frac{m-1}{2} - 1\right) = \lambda(m-1)$. Simplifying the left-hand side: $\left(\frac{m-1}{2}\right)\left(\frac{m-3}{2}\right) = \lambda(m-1)$. Multiplying both sides by 4 to eliminate the fractions: $(m-1)(m-3) = 4\lambda(m-1)$. Dividing both sides by $m-1$ (since $m \neq 1$): $m-3 = 4\lambda$. Thus, we have $m = 4\lambda + 3$.

Since the number of non-zero squares is $\frac{m-1}{2}$, and by Theorem 2.19, m must be prime. Therefore, m must satisfy $m = 4\lambda + 3$ for some integer λ, and m must be an odd prime. □

Example 2.22. For $m = 7$, the non-zero elements of $\mathbb{Z}/7\mathbb{Z}$ are $1,2,3,4,5,6$. The squares are $1^2 = 1, 2^2 = 4, 3^2 = 9 \equiv 2, 4^2 = 16 \equiv 2, 5^2 = 25 \equiv 4, 6^2 = 36 \equiv 1$. The set of squares $\{1,2,4\}$ forms a cyclic difference set in $\mathbb{Z}/7\mathbb{Z}$, and $m = 7 = 4(1) + 3$, which is of the form $4\lambda + 3$.

3. Conjectures

In this section, we present conjectures derived from observed patterns. Each conjecture is supported by examples and computational evidence (using MATLAB) to illustrate where these sets form CDS or exhibit other notable properties.

3.1. **Big Conjecture:** The set of nonzero squares D in $\mathbb{Z}/m\mathbb{Z}$ forms a Cyclic Difference set if and only if m is an odd prime of the form $m = 4\lambda + 3$, where λ is the number of times each nonzero element in $\mathbb{Z}/m\mathbb{Z}$ is represented as a difference of squares in D.

- **Example where D forms a CDS:** Let $m = 7$, an odd prime of the form $4\lambda + 3$ with $\lambda = 1$. The squares modulo 7 are $\{1,2,4\}$. For each pair $x, y \in D$, the differences $x - y \pmod 7$ yield all nonzero elements of $\mathbb{Z}/7\mathbb{Z}$ exactly once. Thus, D satisfies the CDS condition.
- **Example where D does not form a CDS:** Consider $m = 13$, a prime of the form $4n + 1$. The squares modulo 13 are $\{1,3,4,9,10,12\}$. Checking all pairwise differences reveals that some elements are repeated while others are omitted.

3.2. **Second Conjecture:** If m is a prime of the form $m = 4n+1$, then the non-zero squares do not form a CDS, but they do represent every nonzero element in $\mathbb{Z}/m\mathbb{Z}$ as a difference. In this case, the nonzero squares in $\mathbb{Z}/m\mathbb{Z}$ are represented in $n-1$ ways and the non-squares are represented in n ways.

- **Example:** Let $m = 17$, a prime of the form $4n+1$ with $n = 4$. The nonzero squares modulo 17 are $\{1,4,9,16,2,8,13,15\}$. Computing the differences modulo 17 shows that every element of $\mathbb{Z}/17\mathbb{Z}$ is represented, with squares appearing $n-1 = 3$ times and non-squares $n = 4$ times.

3.3. **Third Conjecture:** If $m = 2p$ where p is an odd prime, then the non-zero squares do not form a CDS, but they do represent every nonzero element in $\mathbb{Z}/m\mathbb{Z}$ as a difference. However, in this case, the nonzero elements in $\mathbb{Z}/m\mathbb{Z}$ are all represented in $\frac{p-1}{2}$ ways, except the element p in $\mathbb{Z}/m\mathbb{Z}$, which is represented in twice as many ways so that it is represented in $p-1$ ways as a difference. Also, the number of distinct non-zero squares modulo $2p$ is exactly p, and the element p is always a square modulo $2p$. In fact, $p^2 \equiv p \pmod{2p}$.

- **Example:** Let $m = 14$ ($p = 7$). The nonzero squares modulo 14 are $\{1,4,9,11,13,6,8\}$. Pairwise differences among these squares cover all elements of $\mathbb{Z}/14\mathbb{Z}$, with every nonzero element represented. The element $p = 7$ appears $p-1 = 6$ times, while other elements appear $\frac{p-1}{2} = 3$ times.
- **Example:** For $m = 10$ ($p = 5$), the nonzero squares modulo 10 are $\{1,4,9,6,5\}$. As predicted, $p = 5$ appears $p-1 = 4$ times, while other elements appear $\frac{p-1}{2} = 2$ times.

4. Conclusion

In this laboratory, we learned about the properties of modular arithmetic, cyclic difference sets, and the behavior of squares in modular systems. Through proving theorems and constructing conjectures, I developed a deeper understanding of how distinct differences and squares interact in $\mathbb{Z}/m\mathbb{Z}$ under various conditions. Additionally, I gained experience determining when a statement should be classified as a theorem, conjecture, proposition, or corollary, as well as using MATLAB for the first time.

One of the most surprising and rewarding aspects of this lab was discovering its connections to another course I am currently taking: Discrete Mathematics. It was fascinating to see how concepts learned in one class could be applied in another, often just a day apart.

I believe the most critical theorem in this investigation was the relationship between the number of elements in a cyclic difference set, k, and the total number of distinct differences, $k(k-1)$. This result is directly connected to the constraints imposed by cyclic difference sets, providing a common thread throughout the investigation.

Understanding the concept of a cyclic difference set (CDS) was initially challenging. The abstract definition and the process of proving properties related to CDS required me to put in considerable effort and focus. Proving results, in general, was also difficult.

Before this lab, I had limited experience in formulating and clearly stating conjectures. This investigation showed me how conjectures can arise naturally from patterns and examples and how they lead to formal proofs. The process of refining and testing conjectures felt like an exercise in creativity and logic.

If I were to continue this investigation, I would create more tables instead of lists of numbers and include MATLAB results to better support and illustrate my conjectures. Additionally, I would try to make the evidence for my conjectures clearer and provide more detailed reasoning to explain why I believe they hold true.

While this lab was not my favorite topic in the course, it has been a rewarding experience overall. It challenged me to think critically, make connections across subjects, and explore new tools like MATLAB, all of which contributed to my growth as a student of mathematics.

REFERENCES

[1] Mustafa Jarrar. Number theory. *Discrete Mathematics with Ducks*, 2018.

Email address: dinh224k@mtholyoke.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, MOUNT HOLYOKE COLLEGE, SOUTH HADLEY, MA 01075