CYCLIC DIFFERENCE SETS

BHARGAVI PATIL

Abstract. In this laboratory we will investigate and analyze a special class of cyclic difference sets that come from the non-zero squares modulo a number m. First we will introduce modular arithmetic and then we will use a MATLAB program to formulate conjectures, present examples, and prove some of our conjectures.

1. Introduction

In mathematics, patterns often emerge when we examine the relationships between numbers under specific operations. One interesting example of such a pattern appears in cyclic difference sets, which are formed by studying the differences between numbers in a carefully chosen set. These structures have significant applications in various fields such as coding theory, cryptography, and digital signal processing.

To understand and work with cyclic difference sets, we need to first establish a solid foundation in modular arithmetic. Since modular arithmetic deals with integers and their remainders upon division by the modulus, let us begin with the definition of division.

Definition 1.1. An integer b divides and integer a if there exists an integer c such that:

$$a = b \times c.$$

I would like to thank Professor Robinson and my classmates for helping me learn and understand the concepts presented in this paper.

Let us look at some examples to better understand the concept of integer division:

Example 1.2. The integer 4 divides 20 because there exists an integer $c = 5$, such that:

$$20 = 4 \times 5.$$

Example 1.3. The integer 0 does not divide 20 because there is no integer c, such that:

$$20 = 0 \times c.$$

Example 1.4. The integer -5 divides 25 because there exists an integer $c = -5$, such that:

$$25 = (-5) \times (-5).$$

Having understood integer division, let us now look at the Division Algorithm. This theorem helps us understand how any integer can be divided by another, resulting in a unique quotient and remainder.

Theorem 1.5. *Given two integers a and m where $m > 0$ there must exist unique q and r in the integers such that $a = mq+r$ and $0 \leq r < m$.*

Example 1.6. Given the integers $a = 78$ and $m = 5$, the Division Algorithm says that:

$$78 = 5 \times 15 + 3.$$

In this example, $q = 15$ and $r = 3$.

Example 1.7. Given the integers $a = -78$ and $m = 5$ the Division Algorithm says that:

$$-78 = 5 \times (-16) + 2.$$

In this example, $q = -16$ and $r = 2$.

The Division Algorithm allows us to set up congruence classes within the integers. For example, when $m = 7$ we can write the integers in rows and columns based on their quotients and remainders on division by 7. When we arrange it like that, we can see that each integer a lies in exactly one row, determined by the value of its quotient q and exactly one column, determined by 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
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.

Using the division algorithm, we can categorize all integers into distinct congruence classes based on their remainders when divided by a fixed modulus. In our example, where we use modulus $m = 7$, the integers are partitioned into seven remainder classes: $\{[0], [1], [2], [3], [4], [5], [6]\}$. Each class $[r]$ contains all the integers that are congruent to r mod 7.

Formally, this means:

$$[r] = \{7q + r \mid q \in \mathbb{Z}\}$$

For example, $[5] = \{...., -9, -2, 5, 12, 19, ...\} = \{7q + 5 | q \in \mathbb{Z}\}$. Building upon the concept of congruence classes, we now formally define what it means for two integers to be congruent modulo m.

Definition 1.8. We say that an integer a is congruent to an integer b modulo m, written as $a \equiv b \bmod m$, if both integers have the same remainder when divided by m.

There are 4 equivalent definitions for this relationship and they are as follows:

(1) **Same Least Positive Remainder:**
Integers a and b have the same least positive remainder when divided by m.

(2) **Linear Relationship:**
a can be expressed as $b + mk$, where $k \in \mathbb{Z}$.

(3) **Difference Divisible by m:**
The difference $a - b$ is equal to mk, where $k \in \mathbb{Z}$.

(4) **Divisibility of Differences:**
The modulus m divides the difference $(a-b)$, denoted as $m|(a-b)$.

Example 1.9. Consider an integer $a = 17$ and modulus $m = 5$, applying the Division Algorithm we get:

$$17 = 5 \times 3 + 2$$

Therefore, $17 \equiv 2 \bmod 5$

Example 1.10. Similarly, consider an integer $a = -18$ and modulus $m = 5$, applying the Division Algorithm we get:

$$-18 = 5 \times (-4) + 2$$

Therefore, $-18 \equiv 2 \bmod 5$

From the above two examples, we can see that 17 and -18 belong to the same congruence class [2] modulo 5. These examples demonstrate how congruence is consistent for both, positive and negative integers, given they have the same remainder upon division by the modulus. To better understand and use these properties in modular arithmetic, we need to first understand how congruence behaves under various arithmetic operations. This leads us to the following proposition:

Proposition 1.11. *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. Since $a \equiv b \bmod m$, there exists an integer k such that:

$$a = b + mk.$$

Similarly, because $c \equiv d \bmod m$, there exists an integer l such that:

$$c = d + ml.$$

To understand how congruence behaves under addition and subtraction, we add the expressions for a and c and get:

$$a \pm c = (b + mk) \pm (d + ml).$$

By distributing the addition/subtraction, the expression simplifies to:

$$a \pm c = b \pm d + m(k \pm l).$$

Since k and l are integers, $k \pm l$ is also an integer. Using the definition of modulus, we get:

$$a \pm c \equiv b \pm d \text{ mod } m.$$

Next, we understand how congruences behaves under multiplication by multiplying the expressions for a and c:

$$ac = (b + mk)(d + ml).$$

By expanding the products, we get:

$$ac = bd + bml + mkd + m^2kl.$$

Grouping the terms with m yields:

$$ac = bd + m(bl + kd + mkl).$$

Since b, l, k, d, m are all integers, $(bl + kd + mkl)$ is also an integer. Using the definition of modulus, we get:

$$ac \equiv bd \text{ mod } m.$$

□

The above proposition is important as it ensures that the congruence relationship is preserved under addition, subtraction and multiplication. This proposition allows us to break down large numbers into smaller numbers, perform calculations on these parts, and then combine the results while maintaining their congruence properties. Let us look at an example to better understand how this proposition helps us simplify complex modular arithmetic operations.

Example 1.12. Consider the following expression which we want to evaluate:

$$60^{345} \equiv \underline{\quad\quad} \bmod 7.$$

We being by simplifying the base 60 modulo 7:

$$60 \div 7 = 8 \times 7 + 4.$$

This division gives us:

$$60 \equiv 4 \bmod 7.$$

Using the properties of congruence and Proposition 1.11, we can simplify the original expression to:

$$60^{345} = 4^{345} \bmod 7.$$

Next, we look at the powers of 4 modulo 7 and observe the following pattern:

$$\begin{aligned}
&4^1 \equiv 4 \equiv 4 \bmod 7,\\
&4^2 \equiv 16 \equiv 2 \bmod 7,\\
&4^3 \equiv 64 \equiv 1 \bmod 7,\\
&4^4 \equiv 256 \equiv 4 \bmod 7,\\
&\vdots
\end{aligned}$$

From these calculations, we observe that the powers of 4 modulo 7 cycle every 3 exponents. Proposition 1.11 confirms that this cyclical pattern will continue. This cyclical pattern allows us to simplify larger exponents by expressing them in terms of the cycle length. Since our cycle length is 3, we express the exponent 345 as:

$$4^{345} \bmod 7 \equiv (4^3)^{115} \bmod 7 \equiv 1 \bmod 7.$$

Combining the above steps, we conclude:

$$60^{345} \equiv 1 \bmod 7.$$

The above example demonstrate how congruence relationships can simplify complex calculations. To effectively work with these congruence relationships, we introduce the following definition:

Definition 1.13. With the notation $\mathbb{Z}/m\mathbb{Z}$ we mean the set of congruence classes $\{[0], [1], [2], ..., [m-1]\}$. For example, the class [1] for example consists of all integers congruent to 1 modulo m. Addition and multiplication are defined on the congruence classes by adding and multiplying the representatives of the classes modulo m. To simplify the notation, we often write:

$$\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, 3, ..., m-1\}$$

where $0 = [0], 1 = [1]$, and so on.

To perform operations within modular arithmetic, we define addition and multiplication in a way that the results stay within the set of possible remainders for a given modulus. These operations are essential for understanding how cyclic difference sets behave.

Addition modulo m involves adding two integers and taking the remainder when divided by m. This ensures that the result is always within the range of 0 to $m-1$. To understand this better, let us look at the addition table in 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

Similarly, multiplication modulo m involves multiplying two integers and then taking the remainder divided by m. To understand this better, let us look at the multiplication table in modulo 5 :

×	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

These tables are important for visualizing how addition and multiplication behave in modular arithmetic. In modular arithmetic, the square of an integer is simply the result of multiplying the integer by itself modulo m. Understanding squares modulo m is really important for understanding the cyclic difference sets we are going to be investigating.

With the notation $\mathbb{Z}/m\mathbb{Z}$ defined as the set of congruence classes $[0], [1], [2], ..., [m-1]$, we can now explore a more specialized concept within modular arithmetic: Cyclic Difference Sets. These sets have important applications in fields such as combinatorics and cryptography. Let us begin with the definition of a cyclic difference set:

Definition 1.14. A cyclic difference set is a subset D of $\mathbb{Z}/m\mathbb{Z}$ such that each non-zero element in $\mathbb{Z}/m\mathbb{Z}$ is represented as a difference of elements in D the same number of times. Specifically:

- The number of elements in D is denoted by k,
- The number of times each non-zero element is represented by a difference is denoted by λ.

Understanding cyclic difference sets requires a strong understanding of modular arithmetic, where we only consider the remainder after dividing by a certain number (called the modulus). For example, when working in modulo 5, we represent numbers by their remainder after division by 5:

(i) $7 \equiv 2 \bmod 5$ because $7 = 1 \times 5 + 2$,

(ii) $13 \equiv 3 \bmod 5$ because $13 = 2 \times 5 + 3$,

(iii) $-3 \equiv 2 \bmod 5$ because $-3 = (-1) \times 5 + 2$.

We use the symbol "≡" to indicate that two numbers are equivalent (or congruent) modulo 5, meaning they have the same remainder when divided by 5. With this understanding, let's look at cyclic difference sets. Consider the numbers 1, 2, and 4 when working in modulo 7. On calculating all possible differences between these numbers, we get:

$$\begin{aligned}
2 - 1 &\equiv 1 \bmod 7,\\
4 - 1 &\equiv 3 \bmod 7,\\
4 - 2 &\equiv 2 \bmod 7,\\
1 - 2 &\equiv 6 \bmod 7,\\
1 - 4 &\equiv 4 \bmod 7,\\
2 - 4 &\equiv 5 \bmod 7.
\end{aligned}$$

In the above calculations, we see that when calculating differences that give us negative results, we transform these negative values by adding the modulus. Consider our calculation in $\bmod 7$: if we subtract 2 from 1 and get -1, we add 7 to obtain 6. In our modulo system, -1 and 6 are in the same congruence class. By adding the modulus, we can map negative values to their positive representation between 0 and $m - 1$, where m is our modulus.

The set $\{1, 2, 4\}$ forms a cyclic difference set. To understand why, observe that when we take all possible differences between its elements, each non-zero number modulo 7 (i.e. $1, 2, 3, 4, 5, 6$) appears exactly once in our list of differences. This uniform distribution of differences is a key characteristic of cyclic difference sets. This example introduces us to three important parameters that define a cyclic difference set:

(1) Modulus (m): This is the number we use for modular arithmetic. In our example, $m = 7$ as all calculations are done modulo 7,
(2) Size (k): This represents the number of elements in the set. In our example, $k = 3$ as $\{1, 2, 4\}$ contains three numbers,
(3) Parameter (λ): This tells us how many times each non-zero number appears as a difference. In our example, $\lambda = 1$ as each non-zero number (1 through 6) appears once when we take all possible differences.

These three parameters, m, k, and λ, help us in understanding and defining cyclic difference sets. This simple example also illustrates several key ideas that we will explore later in this paper:

(1) Working with numbers modulo m,
(2) The concept of differences between numbers in a set,
(3) The special properties that make certain sets cyclic difference sets,
(4) The relationships between the parameters m, k, and λ.

In this laboratory, we will study the special cyclic difference sets that come from sets D consisting of non zero squares in $\mathbb{Z}/m\mathbb{Z}$. We will look at the conditions under which these sets form a cyclic difference set in $\mathbb{Z}/m\mathbb{Z}$, and determine the corresponding values of k and λ when the squares form a cyclic difference set.

2. Theorems, Propositions and Corollaries

In this section, we present and prove several theorems, propositions, and corollaries related to cyclic difference sets formed by non-zero squares in $\mathbb{Z}/m\mathbb{Z}$. Let us start with a theorem on the number of distinct differences in a set:

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

Proof. We will prove this theorem by induction on k. For our base case, we let $k = 2$. Using our theorem, the number of distinct differences is:

$$2(2-1) = 2.$$

Consider a set $A = \{a_1, a_2\}$ where $a_1 \neq a_2$. The possible differences are:

$$a_2 - a_1 \text{ and } a_1 - a_2.$$

Since $a_1 \neq a_2$, we have two distinct differences. Thus, our base case holds.

Now, we consider the inductive hypothesis for k and assume that for some $k \geq 1$, any set of k numbers yields exactly $k(k-1)$ distinct differences. That is, if we have a set:

$$A = \{a_1, a_2, ..., a_k\},$$

then the number of distinct differences $a_i - a_j$ (for $i \neq j$) is $k(k-1)$. Our goal is to show thar a set of $k+1$ numbers will yield exactly $(k+1)k$ distinct differences. Consider a set:

$$A' = \{a_1, a_2, ..., a_k, a_{k+1}\},$$

containing $k+1$ numbers. By our inductive hypothesis, we know that there are exactly $k(k-1)$ distinct differences among the first k numbers:

$$a_i - a_j \text{ for } 1 \leq i, j \leq k \text{ and } i \neq j$$

Now, let us look at the differences involving the $(k+1)$th number. These are the differences:

$$a_{k+1} - a_j \text{ and } a_j - a_{k+1} \text{ for } 1 \leq j \leq k$$

Since a_{k+1} is distinct from the other k numbers, each of these differences is distinct and does not overlap with the existing differences from our first k numbers. Therefore, we have:

- k differences of the form $a_{k+1} - a_j$,
- k differences of the form $a_j - a_{k+1}$.

Adding the $k+1$th number to our set gives us $2k$ new distinct differences. We then add these new distinct differences to the existing ones from our the first k numbers to get:

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

Thus, we have shown that our inductive hypothesis holds and our theorem is true by induction for all integers $k \geq 2$. Therefore for any set of k numbers there are exactly $k(k-1)$ distinct differences. □

The preceding theorem establishes a fundamental property of distinct differences in a set. Building upon this result, we now explore a more specific application of this difference to non-zero squares in $\mathbb{Z}/m\mathbb{Z}$.

Theorem 2.2. *If the set of non-zero squares D 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. We know that in cyclic difference sets, each non zero element of $\mathbb{Z}/m\mathbb{Z}$ is represented exactly λ times as a difference of elements from D. Since there are $(m-1)$ non-zero elements in $\mathbb{Z}/m\mathbb{Z}$, the total number of differences is:

$$\lambda(m-1).$$

From Theorem 3.1, we know that for a set D containing k elements, the number of distinct differences that can be formed is:

$$k(k-1).$$

Since both expressions represent the total number of distinct differences in the set D, we equate them to get:

$$k(k-1)=\lambda(m-1).$$

□

This theorem helps us establish the relationship between parameters k, λ, and m for a cyclic difference set formed by non-zero squares in $\mathbb{Z}/m\mathbb{Z}$. We now work on a fundamental property of additive inverses in modular systems.

Proposition 2.3. *For any $x \in \mathbb{Z}/m\mathbb{Z}$, the additive inverse $-x$ is congruent to $(m-x)$ modulo m. That is:*

$$-x \equiv (m-x) \bmod m.$$

Proof. To prove that $-x \equiv (m-x) \bmod m$, we will use the definition of congruence in modular arithmetic which states that two integers a and b are congruent modulo m if and only if their difference is divisible by m. Formally,

$$a \equiv b \bmod m \Longleftrightarrow m|(a-b).$$

By this defintion, to prove our theorem, we need to show that:

$$m|-x-(m-x).$$

We compute the difference and get:

$$-x-(m-x)=-x-m+x=-m.$$

Since, $-m = m \times (-1)$, we can say that:

$$m | -m.$$

Therefore,

$$m | -x - (m - x).$$

Thus, we have proved that $-x \equiv (m - x) \bmod m$. □

Having established the symmetry of additive inverses in modular arithmetic, we now work on a similar property involving squares.

Proposition 2.4. *For any integer x with $0 \leq x \leq m - 1$, the square of x is congruent to the square of $(m - x)$ modulo m. That is:*

$$x^2 \equiv (m - x)^2 \bmod m.$$

Proof. To prove that $x^2 \equiv (m - x)^2 \bmod m$, we will use the definition of congruence in modular arithmetic which states that two integers a and b are congruent modulo m if and only if their difference is divisible by m. Formally,

$$a \equiv b \bmod m \Longleftrightarrow m|(a - b).$$

By this definition, to prove our theorem, we need to show that:

$$m|x^2 - (m - x)^2.$$

We compute the difference and get:

$$x^2 - (m - x)^2 = x^2 - (m^2 - 2mx + x^2) = 2mx - m^2.$$

Factoring the above expression, we get:

$$m(2x - m).$$

Since, $2x - m$ is an integer, it follows that:

$$m|m(2x - m).$$

Therefore,

$$m|x^2 - (m - x)^2.$$

Thus, we have proved that $x^2 \equiv (m - x)^2 \bmod m$. □

To better understand Proposition 2.3 and Proposition 2.4, let us look at an example where $m = 7$.

Example 2.5. Consider the elements x in $\mathbb{Z}/7\mathbb{Z}$. For each x, the additive inverse $-x$ mod 7 is equal to $(7-x)$ mod 7 as illustrated below:

$$-1 \equiv 6 \bmod 7,$$

$$-2 \equiv 5 \bmod 7,$$

$$-3 \equiv 4 \bmod 7,$$

$$-4 \equiv 3 \bmod 7,$$

$$-5 \equiv 2 \bmod 7,$$

$$-6 \equiv 1 \bmod 7.$$

Next, let us consider the elements x in $\mathbb{Z}/7\mathbb{Z}$ and their corresponding squares x^2 modulo 7:

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

The square of x is congruent to the square of $(7 - x)$ modulo 7 as illustrated below:

$$1^2 \equiv 6^2 \bmod 7 \text{ as } 6^2 = 36 \equiv 1 \bmod 7,$$

$$2^2 \equiv 5^2 \bmod 7 \text{ as } 5^2 = 25 \equiv 4 \bmod 7,$$

Proposition 2.4 reveals a symmetrical property of squares in modular arithmetic. Theorem 2.6 uses this insight to show a fundamental constraint on the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ for odd moduli.

Theorem 2.6. *For an odd integer 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. From Proposition 2.4, we know that the square of x is congruent to the square of $(m - x)$ modulo m. Formally,

$$x^2 \equiv (m - x)^2 \bmod m.$$

This result implies that x and $m - x$ yield the same remainder when squared and divided by m. Therefore, each pair $\{x, m - x\}$ produce identical squares in $\mathbb{Z}/m\mathbb{Z}$. The pairs $(1, m-1), (2, m-2), ..., (\frac{m-1}{2}, \frac{m+1}{2})$ all pair up when m is odd and this set of pairs covers all non-zero elements in $\mathbb{Z}/m\mathbb{Z}$. As a result, the set of squares in $\mathbb{Z}/m\mathbb{Z}$ exhibits symmetry, limiting the number of distinct non-zero squares. Since there are $m - 1$ non zero elements in $\mathbb{Z}/m\mathbb{Z}$, and each distinct square is produced by a pair of elements $\{x, m-x\}$, the maximum number of distinct non-zero squares is:

$$\frac{m-1}{2}.$$

However, it is important to note that some squares may yield the same remainder even within these pairs which could lead to the actual number of distinct non-zero squares k being less than $\frac{m-1}{2.}$ Therefore, we conclude that:

$$k \leq \frac{m-1}{2}.$$

This argument establishes that for an odd integer m, the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ does not exceed $\frac{m-1}{2}$. □

From Example 2.5, we can see that for odd $m = 7$, the distinct non-zero squares are $\{1, 2, 4\}$, which gives us 3 distinct non-zero squares. This satisfies $k \leq \frac{7-1}{2} = 3$, confirming Theorem 2.6. This theorem derives the bounds of distinct non-zero squares for modulus which are odd integers. Theorem 2.7 extends this investigation to even integers.

Theorem 2.7. *For an even integer m, the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is less than or equal to $\frac{m}{2}$.*

Proof. From Proposition 2.4, we know that the square of x is congruent to the square of $(m-x)$ modulo m. Formally,

$$x^2 \equiv (m-x)^2 \bmod m.$$

This implies that x and $m-x$ yield the same remainder when squared and divided by m. Therefore, each pair $\{x, m-x\}$ produce identical squares in $\mathbb{Z}/m\mathbb{Z}$. Since m is even, x and $m - x$ are distinct for all x in the range $1 \leq x \leq \frac{m}{2} - 1$. When $x = \frac{m}{2}$, x pairs with itself as $m - \frac{m}{2} = \frac{m}{2}$ and $\frac{m}{2}$ is its own additive inverse.

As there are $m - 1$ non zero elements in $\mathbb{Z}/m\mathbb{Z}$, and each distinct square is produced by a pair of elements $\{x, m - x\}$, which includes $\{\frac{m}{2}\}$, the maximum number of distinct non-zero squares is:

$$\frac{m}{2.}$$

However, it is important to note that some squares may yield the same remainder even within these pairs which leads to the actual number of distinct non-zero squares k to be less than $\frac{m}{2.}$ Therefore, we conclude that:

$$k \leq \frac{m}{2}.$$

This argument establishes that for an even integer m, the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ does not exceed $\frac{m}{2}$. □

Let us look at an example with even modulus $m = 4$ to understand this better:

Example 2.8. Consider the elements x in $\mathbb{Z}/4\mathbb{Z}$ and their corresponding squares x^2 modulo 4:

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

We can see that for even $m = 4$, the distinct non-zero squares is $\{1\}$, which gives us 1 distinct non-zero square. This satisfies $k \leq \frac{4}{2} = 2$, consistent with Theorem 2.7. The symmetry occurs with $\{1, 3\}$

producing the same square value mod 4, and $\{2\}$ pairing with itself to produce 0.

Having established an upper bound on the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ for odd and even m, we now extend our investigation to a more specific case. Theorem 2.9 explores what happens when the modulus m is a perfect square, adding additional constraints on the number of distinct non-zero squares.

Theorem 2.9. *If $m = a^2$ for some integer $a > 1$, then:*

- *If m is odd, the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is strictly less than $\frac{m-1}{2}$,*
- *If m is even, the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is strictly less than $\frac{m}{2}$.*

Proof. With $m = a^2$ and $a > 1$, let us look at the multiples of a within $\mathbb{Z}/m\mathbb{Z}$. These multiples consist of $a, 2a..., (a-1)a$. There are exactly $a-1$ such non-zero multiples because to yield distinct results less than m, we need to multiply a by integers k where $1 \leq k \leq a-1$ as $ka < a^2$ for $k < a$. Each of these multiple satisfies:

$$(ka)^2 = k^2a^2 = k^2m \equiv 0 \bmod m.$$

Thus, these $a-1$ elements have squares congruent to zero modulo m and do not contribute to the count of distinct non-zero squares. Excluding these $a-1$ elements, there remains $m-1-(a-1) = m-a$ non-zero elements in $\mathbb{Z}/m\mathbb{Z}$ that are not multiples of a. Using Proposition 2.4, these remaining elements can be paired as $\{x, m-x\}$, where each pair yields the same square modulo m. Now, on the basis of m, we have two cases.

For our first case, we consider m is odd. Since $m = a^2$ and the square of an odd integer is odd, we conclude that a is odd. Using Theorem 2.6, we can establish that for an odd integer m, the number of pairs with the same square modulo m cannot exceed $\frac{m-1}{2}$. After subtracting the $a-1$ elements that are congruent to zero modulo m, the total number of distinct non-zero squares k formed by the remaining $m-a$ non-zero elements is bounded by:

$$k \leq \frac{m-a}{2}.$$

Given that $a > 1$ and a is odd, $a \geq 3$. Therefore, it follows that:

$$\frac{m-a}{2} \leq \frac{m-3}{2} < \frac{m-1}{2}.$$

This inequality shows that when m is odd, k is strictly less than $\frac{m-1}{2}$.

For our second case, we consider m is even. Since $m = a^2$ and the square of an even integer is even, we conclude that a is even. Using Theorem 2.7, we can establish that for an even integer m, the number of pairs with the same square modulo m cannot exceed $\frac{m}{2}$. After subtracting the $a-1$ elements that are congruent to zero modulo m, the total number of distinct non-zero squares k formed by the remaining $m-a$ non-zero elements is bounded by:

$$k \leq \frac{m}{2}.$$

Given that $a > 1$ and a is even, $a \geq 2$. Therefore, it follows that:

$$\frac{m-a}{2} \leq \frac{m-2}{2} < \frac{m}{2}.$$

This inequality shows that k is strictly less than $\frac{m}{2}$.
In both cases, the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is strictly less than the upper bounds of $\frac{m-1}{2}$ for odd m and $\frac{m}{2}$ for even m. This decrease is caused by the presence of $a-1$ non-zero elements that are multiples of a whose squares are zero modulo m. □

To understand this better, consider Example 2.8, where $m = 4 = 2^2$. We have only one distinct non-zero square,$\{1\}$. This is consistent with our theorem which states that for an even $m = a^2$, the number of distinct non-zero squares is strictly less than $\frac{m}{2} = 2$.

The previous theorem examined the case where m is a perfect square. Theorem 2.10 explores this further by considering a more general case of composite moduli, specifically when m is a product of two distinct odd integers.

Theorem 2.10. *If $m = ab$ where $1 < a < b < m$ and both a and b are odd integers, then the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is strictly less than $\frac{m-1}{2}$.*

Proof. We begin by looking at specific elements in $\mathbb{Z}/m\mathbb{Z}$. Consider the elements, $a+b$ and $a-b$. Calculating the difference of squares of these elements, we find:

$$(a+b)^2 - (a-b)^2 = (a^2 + 2ab + b^2) - (a^2 - 2ab + b^2) = 4ab = 4m.$$

By definition of congruence, $4m \equiv 0 \bmod m$ and since the difference is divisible by m:

$$(a+b)^2 \equiv (a-b)^2 \bmod m.$$

This congruence indicates that the squares of $a+b$ and $a-b$ are equivalent modulo m. However, for this proof to hold, $a+b$ and $a-b$ must be distinct elements in $\mathbb{Z}/m\mathbb{Z}$. Suppose for contradiction, $a+b \equiv a-b \bmod m$. This expression can be rearranged to yield:

$$2b \equiv 0 \bmod m.$$

Given that $m = ab$ and both, a and b are greater than 1, this implies:

$$2b \equiv 0 \bmod ab \implies 2 \equiv 0 \bmod a$$

Since a is an odd integer greater than 1, it cannot divide 2. This contradiction shows us that $a+b$ and $a-b$ are indeed distinct modulo m.

Next, we must verify that $a+b$ does not coincide with the additive inverse of $a-b$ in $\mathbb{Z}/m\mathbb{Z}$. Assume for contradiction that:

$$a+b \equiv (m-(a-b)) \bmod m.$$

Simplifying the right hand side and subtracting b from both sides yields:

$$a \equiv (m-a) \bmod m.$$

Adding a to both sides results in:

$$2a \equiv m \bmod m \implies 2a \equiv 0 \bmod m.$$

Substituting $m = ab$, we have:

$$2a \equiv 0 \bmod ab \implies 2a = abk \text{ for some integer } k.$$

Dividing both sides by a (which is valid as $a > 1$) leads to:

$$2 = bk.$$

However, since b is an odd integer greater than 1, there exists no integer k that satisfies this equation. This contradiction confirms that $a + b$ does not equal $m - (a - b)$ modulo m.

According to Theorem 2.6, for an odd integer m, the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ cannot exceed $\frac{m-1}{2}$.The modulus m is an odd integer as the product of two odd integers is odd. Using Proposition 2.4, we know that $m - (a + b)$ must have the same square as $(a + b)$ modulo m and $m - (a - b)$ must have the same square as $(a - b)$ modulo m. This pairing ensures that the actual number of distinct non-zero squares is strictly less than $\frac{m-1}{2}$. □

Let us look at an example with $m = 15$, where $a = 3$ and $b = 5$:

Example 2.11. Consider $\mathbb{Z}/15\mathbb{Z}$. The elements we are specially interested in are:

$$a + b = 3 + 5 = 8 \equiv 8 \bmod 15,$$

$$a - b = 3 - 5 = -2 \equiv 13 \bmod 15,$$

$$m - (a + b) = 15 - 8 = 7 \equiv 7 \bmod 15,$$

$$m - (a - b) = 15 - 13 = 2 \equiv 2 \bmod 15.$$

Computing their squares modulo 15 we get:

$$8^2 = 64 \equiv 4 \bmod 15,$$

$$13^2 = 169 \equiv 4 \bmod 15,$$

$$7^2 = 49 \equiv 4 \bmod 15,$$

$$2^2 = 4 \equiv 4 \bmod 15.$$

To verify Theorem 2.10, when we compute the distinct non-zero squares in $\mathbb{Z}/15\mathbb{Z}$, we find 5 distinct non-zero squares, which is strictly less than the upper bound $\frac{15-1}{2} = 7$. This reduction occurs due to the symmetrical pairing of squares created by the odd factors 3 and 5.

Having explored the case of composite moduli, we now look at the case when the modulus is an odd prime.

Theorem 2.12. *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. According to Theorem 2.6, for an odd integer m, the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ cannot exceed $\frac{m-1}{2}$. Thus we consider the set of integers x such that $0 < x \leq \frac{m-1}{2}$. Our goal is to show that the squares x^2 modulo m are all distinct for these values of x. For the sake of contradiction, suppose there exist distinct integers x and y with $0 < x < y \leq \frac{m-1}{2}$ such that:

$$x^2 \equiv y^2 \bmod m.$$

This congruence implies that:

$$x^2 - y^2 \equiv 0 \bmod m.$$

Factoring the left hand side, we get:

$$(x+y)(x-y) \equiv 0 \bmod m.$$

Using Definition 1.8, we can say that m divides the product $(x+y)(x-y)$:

$$m|(x+y)(x-y).$$

Since m is a prime number, it must divide at least one of the factors $(x+y)$ or $(x-y)$. Let us look at both cases:

For the first case, let us consider $m|(x+y)$. This means that $x+y \equiv 0 \bmod m$, or $x \equiv -y \bmod m$. By Proposition 2.3, we know that:

$$-y \equiv (m-y) \bmod m.$$

Now let us look at the ranges of x and y. Since $1 \leq y \leq \frac{m-1}{2}$, it follows that $\frac{m-1}{2} \leq m-y \leq m-1$. Since $1 \leq x \leq \frac{m-1}{2}$, $x \not\equiv m-y \bmod m$ and therefore $x+y \equiv 0 \bmod m$ is not possible.

For the second case, let us consider $m|x-y$. Since $x < y$, x is not equivalent to $y \bmod m$. That is:

$$x \not\equiv y \bmod m.$$

By Definition 1.8, we can say that $x - y \not\equiv 0 \bmod m$.

Since m does not divide $x - y$ or $x + y$, we reach a contradiction. There are no distinct values of x and y in the range $0 < x < y \leq \frac{m-1}{2}$ such that $x^2 \equiv y^2 \bmod m$. Thus we conclude that all squares x^2 are distinct for $0 < x \leq \frac{m-1}{2}$ and there are exactly $\frac{m-1}{2}$ squares when m is an odd prime. □

Let us look at an example where the modulus is an odd prime to better understand this theorem.

Example 2.13. Let us consider the elements x in $\mathbb{Z}/7\mathbb{Z}$ and their corresponding squares x^2 modulo 7:

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

We find that there are 3 distinct non-zero squares, which is exactly $\frac{(7-1)}{2} = 3$, confirming Theorem 2.12.

Having established that an odd prime has exactly $\frac{m-1}{2}$ distinct non-zero squares, we now prove the reverse: if a modulus has exactly $\frac{m-1}{2}$ distinct non-zero squares, then it must be an odd prime.

Theorem 2.14. *If the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is exactly $\frac{m-1}{2}$, then m is an odd prime.*

Proof. Firstly, the number of distinct non-zero squares being $\frac{m-1}{2}$ implies that m is odd. If m were even, then $\frac{m-1}{2}$ would not be an integer since $m - 1$ would be odd.

Assume for contradiction that m is composite and therefore not prime. When m is composite, it can either be a perfect square or a product of two distinct odd integers. Therefore, the way m is be expressed can be split into two cases.

In the first case, $m = a^2$ for some integer $a > 1$. Since m is odd, by Theorem 2.9, the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is strictly less than $\frac{m-1}{2}$. This directly contradicts our initial assumption that there are exactly $\frac{m-1}{2}$ distinct non-zero squares.

In the second case, $m = ab$ where $1 < a < b < m$ and both a and b are odd integers. By Theorem 2.10, if $m = ab$ with $1 < a < b < m$ and both, a and b are odd, then the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is strictly less than $\frac{m-1}{2}$. Again, this contradicts our initial assumption that there are exactly $\frac{m-1}{2}$ distinct non-zero squares.

In both cases where m is composite, the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is not equal to $\frac{m-1}{2}$. Our initial assumption that m is composite is false, making m prime. Therefore, we conclude that if the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is exactly $\frac{m-1}{2}$, then m must be odd and prime. □

We have established that a modulus with exactly $\frac{m-1}{2}$ distinct non-zero squares must be an odd prime. We now take this further by specifying a more precise condition: not only must the modulus be an odd prime, but it must be of the specific form $m = 4\lambda + 3$ to form a cyclic difference set.

Theorem 2.15. *If D (the non-zero squares in $\mathbb{Z}/m\mathbb{Z}$) is a cyclic difference set with $k = \frac{m-1}{2}$, then m an odd prime of the form $m = 4\lambda+3$.*

Proof. By Theorem 2.14, we can establish that if k, the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is $\frac{m-1}{2}$, then m is an odd prime. Next, we establish the specific form of m. Since D is a cyclic difference set with parameters (m, k, λ), using Theorem 2.2, we can establish that:

$$k(k-1) = \lambda(m-1).$$

Since $k = \frac{m-1}{2}$, we substitute k to get:

$$\frac{m-1}{2} \times \frac{m-3}{2} = \lambda(m-1).$$

Simplifying this further, we get:

$$\frac{(m-1)(m-3)}{4} = \lambda(m-1).$$

We then divide both sides by $(m-1)$:

$$\frac{m-3}{4} = \lambda.$$

Rearranging this expression gives us:

$$m = 4\lambda + 3.$$

Therefore, we have established that m is an odd prime of the form $m = 4\lambda + 3$. □

Building upon our proofs, we now transition to computational exploration of cyclic difference sets.

3. Data and Conjectures

In this section, we will explore conjectures related to cyclic difference sets (CDS) formed by the set of non-zero squares in $\mathbb{Z}/m\mathbb{Z}$. We will use computational methods to generate data, identify patterns, and propose mathematical conjectures that extend our current understanding. Each conjecture represents a hypothesis. We begin with our first conjecture, which describes the conditions under which the set of non-zero squares constitutes a CDS and examines its relationship with the modulus m.

Conjecture 3.1. The set of non-zero 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 non-zero element in $\mathbb{Z}/m\mathbb{Z}$ is expressed as a difference of squares in D.

Evidence. To support this conjecture, we will provide cases where m is in the form of $4\lambda + 3$ as well as other forms and examine if D satisfies the conditions needed to form a cyclic difference set.

First, let us consider the case where $m = 7$, which is an odd prime of the form $m = 4(1)+3$. The non-zero elements in $\mathbb{Z}/7\mathbb{Z}$ are $\{1, 2, 3, 4, 5, 6\}$. Squaring these elements modulo 7 gives us $\{1, 4, 2, 2, 4, 1\}$. The distinct non-zero squares form $D = \{1, 2, 4\}$. Using Theorem 2.2 to verify if D forms a cyclic difference set, we find that $k(k-1) = \lambda(m-1)$ holds true as $3 \times 2 = 1 \times 6$. Therefore, D forms a cyclic difference set in $\mathbb{Z}/7\mathbb{Z}$.

For our second case, let us take $m = 5$, which is an odd prime but of the form $m = 4(1) + 1$. The non-zero elements in $\mathbb{Z}/5\mathbb{Z}$ are $\{1, 2, 3, 4\}$. Squaring these elements modulo 5 gives us $\{1, 4, 4, 1\}$. The distinct non-zero squares form $D = \{1, 4\}$. Using our computational analysis, we observe that not all elements in $\mathbb{Z}/5\mathbb{Z}$ are represented the same number of times by all distinct differences. Therefore, D does not form a cyclic difference set in $\mathbb{Z}/5\mathbb{Z}$.

Lastly, let us look at a case where $m = 6$, an even composite number of the form $m = 4(1) + 2$. The non-zero elements in $\mathbb{Z}/6\mathbb{Z}$ are $\{1, 2, 3, 4, 5\}$. Squaring these elements modulo 6 gives us $\{1, 4, 3, 4, 1\}$. The distinct non-zero squares form $D = \{1, 3, 4\}$. Using our computational analysis, we observe that not all elements in $\mathbb{Z}/6\mathbb{Z}$ are represented the same number of times by all distinct differences. Therefore, D does not form a cyclic difference set in $\mathbb{Z}/6\mathbb{Z}$.

Using computational analysis, we found that this conjecture holds for all primes p where $p = 4\lambda + 3$ and $p \leq 43$ and the set of distinct non-zero squares consistently forms a cyclic difference set.

These examples support our conjecture by showing that when m is an odd prime of the form $4\lambda + 3$, the set D of distinct non-zero squares forms a cyclic difference set in $\mathbb{Z}/m\mathbb{Z}$. On the other hand, when m is an even number or odd prime of a different form, D does not seem to form a cyclic difference set. □

After exploring the behavior of non-zero squares in moduli of the form $4\lambda+3$, our computational investigations turn to primes of the form $4n+1$. Conjecture 3.2 reveals a distinct pattern that while these primes do not form cyclic difference sets, they exhibit a unique characteristic of representing every non-zero element as a difference, albeit with unequal representation.

Conjecture 3.2. If m is a prime of the form $4n+1$, then the set of non-zero squares do not form a cyclic difference set. However, they do represent every non-zero element in $\mathbb{Z}/m\mathbb{Z}$ as a difference. If $p > 5$, the non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ are represented in $n-1$ ways, while the non-squares are represented in n ways.

Evidence. To support this conjecture, we will provide cases where m is a prime in the form of $4n+1$ and observe how they represent non-zero elements in $\mathbb{Z}/m\mathbb{Z}$ as a difference.

For our first case, let us take $m = 13$, which is a prime of the form $m = 4(3)+1$. The non-zero elements in $\mathbb{Z}/13\mathbb{Z}$ are $\{1, 2, 3, ...12\}$. Squaring these elements modulo 13 gives us $\{1, 4, 9, 3, 12, 10, 10, 12, 3, 9, 4, 1\}$. The distinct non-zero squares form $D = \{1, 3, 4, 9, 10, 12\}$. Using our computational analysis, we observe that not all elements in $\mathbb{Z}/13\mathbb{Z}$ are represented the same number of times by all distinct differences. Therefore, D does not form a cyclic difference set in $\mathbb{Z}/13\mathbb{Z}$. However, every non-zero element in $\mathbb{Z}/13\mathbb{Z}$ can be expressed as a difference of elements in D. Specifically, non-squares are represented in $n = 3$ ways, while squares are represented in $n - 1 = 2$ ways.

For our next case, let us take $m = 17$, which is a prime of the form $m = 4(4) + 1$. The non-zero elements in $\mathbb{Z}/17\mathbb{Z}$ are $\{1, 2, 3, ...16\}$ and squaring these elements modulo 17 gives us $D = \{1, 4, 9, 16, 8, 2, 15, 13, 13, 15, 2, 8, 16, 9, 4, 1\}$. The distinct non-zero squares form $\{1, 2, 4, 8, 9,$

$13, 15, 16\}$. Utilizing our computational analysis, we observe that not all elements in $\mathbb{Z}/17\mathbb{Z}$ are represented the same number of times. Therefore, D does not form a cyclic difference set in $\mathbb{Z}/17\mathbb{Z}$. However, every non-zero element in $\mathbb{Z}/17\mathbb{Z}$ can be expressed as a difference of elements in D. Specifically, non-squares are represented in $n = 4$ ways, while squares are represented in $n - 1 = 3$ ways.

These examples support that for primes of the form $m = 4n + 1$, the set D of non-zero squares does not satisfy the conditions required to form a cyclic difference set. However, the structure of these primes ensures that every non-zero element is expressed as a difference of squares, but with unequal occurrences between squares and non-squares. □

Building upon this insight, we extend our exploration to moduli of the form $2p$, where p is an odd prime.

Conjecture 3.3. If $m = 2p$, where p is an odd prime, then the non-zero squares do not form a cyclic difference set. However, they do represent every non-zero element in $\mathbb{Z}/m\mathbb{Z}$ as a difference. In this case, the non zero elements in $\mathbb{Z}/m\mathbb{Z}$ are all represented in $\frac{p-1}{2}$ ways, except for the element p, which is represented in twice as many ways as the others, specifically in $p - 1$ ways. Additionally, the number of distinct non-zero squares modulo $2p$ is exactly p, and the element p is always a square modulo $2p$ as $p^2 \equiv p \bmod 2p$.

Evidence. To provide evidence for this conjecture, let us look at cases where $m = 2p$.

For the first case, let us consider $m = 10$, where $p = 5$. The non-zero elements in $\mathbb{Z}/10\mathbb{Z}$ are $\{1, 2....10\}$. The distinct non-zero squares form $\{1, 4, 5, 6, 9\}$. Utilizing our computational analysis, we observe that not all elements in $\mathbb{Z}/10\mathbb{Z}$ are represented the same number of times. Therefore, D does not form a cyclic difference set in $\mathbb{Z}/10\mathbb{Z}$. However, every non-zero element in $\mathbb{Z}/10\mathbb{Z}$ is represented as a difference in 2 (i.e.$\frac{5-1}{2}$) ways, except for the element $p = 5$, which is represented in twice as many ways as the others, specifically in 4 ways.

For the second case, let us consider $m = 14$, where $p = 7$. The non-zero elements in $\mathbb{Z}/14\mathbb{Z}$ are $\{1, 2....14\}$. The distinct non-zero squares form $\{1, 2, 4, 7, 8, 9, 11\}$. Utilizing our computational analysis, we observe that not all elements in $\mathbb{Z}/14\mathbb{Z}$ are represented the same number of times. Therefore, D does not form a cyclic difference set in $\mathbb{Z}/14\mathbb{Z}$. However, every non-zero element in $\mathbb{Z}/14\mathbb{Z}$ is represented as a difference in 3 (i.e.$\frac{7-1}{2}$) ways, except for the element $p = 7$, which is represented in twice as many ways as the others, specifically in 6 ways.

These examples support that for primes of the form $m = 2p$, where p is an odd prime, the set D of non-zero squares does not satisfy the conditions required to form a cyclic difference set. However, the structure of these primes ensures that every non-zero element is expressed as a difference of squares, with the element p represented twice as many times as the other elements.

□

4. Conclusion

This study of cyclic difference sets provides insights into modular arithmetic, prime number properties, and the application of computational tools in mathematical research.

Initially, it was difficult to completely understand the concept of a cyclic difference set. The abstract nature of the mathematical concepts like modular arithmetic and congruence classes was the reason for this initial difficulty.

Central to understanding the concept of a CDS is the critical role of the modulus m, which determines whether the set D of non-zero squares forms a cyclic difference set. A CDS emerges exclusively when m is an odd prime of the form $m = 4\lambda+3$, demonstrating how primality and numerical structure influence mathematical sets.

Theorem 2.15 proved a fundamental relationship: if D is a cyclic difference set with $k = \frac{m-1}{2}$, then m is an odd prime of the form $4\lambda+3$. The proof of this theorem leveraged essentially all of our theorems. The set of non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ for moduli not meeting this condition, such as primes where $m = 4n + 1$ and even m of form $m = 2p$ where p is prime, also showed interesting properties. These sets of squares did not form a complete CDS but could still represent every non-zero element as a difference of squares, displaying consistent patterns in the numbers of difference representations.

To understand cyclic difference sets, it is important to understand the term, "all distinct differences." This term means that we calculate the differences between every possible pair of non-zero square elements within the modular arithmetic system. Clarifying the term helped understand the fundamental properties of cyclic difference sets.

This research laboratory was my first substantive engagement with making mathematical conjectures. Using computational tools to observe patterns, generalize them, and potentially prove them was exciting. I realized that the ability to see patterns and develop conjectures is an important skill not just in mathematics, but across various fields of research and problem-solving. The process of moving from raw data to meaningful mathematical insights was one of my main takeaways from this laboratory.

Looking forward, future research directions include a deeper exploration of non-zero square behaviors under alternative modular conditions and investigating real-world applications of cyclic difference sets in fields like cryptography and coding theory.

References

[1] Department of Mathematics and Statistics at Mount Holyoke College, *Laboratories in Mathematical Exploration: A Bridge to Higher Mathematics*, Springer-Verlag, New York, 1997.

Email address: `patil22b@mtholyoke.edu`

Department of Mathematics and Statistics, Mount Holyoke College, South Hadley, MA 01075