CYCLIC DIFFERENCE SETS

ABY SOUMARE

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

Before giving definition of a cyclic difference set, we need to understand modular arithmetic.

Definition 1.1. An integer a divides and integer b if there exists some integer m such that $b = am$.

Example 1.2. An example of whole number division is $15 = 3 * 5$. Another example can be $15 = -5 * -3$. Also note that any number cannot divide zero, but zero divides all numbers. See: $0 = 5 * 0$, but $5 \neq 0 * m$ because m does not exist.

Next we have a way to generalize division using the Division Algorithm, which can be stated as follows:

Theorem 1.3. *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 $0 \leq r < m$.*

I thank Professor Robinson for helping me with this report.

Example 1.4. Given the integers $a = 78$ and $m = 5$, the division algorithm says that $78 = 5 * 15 + 3$. Given the integers $a = -78$ and $m = 5$, the division algorithm says that $-78 = 5 * -16 + 2$. Given the integers $a = 25$ and $m = 5$, the division algorithm says that $25 = 5 * 5 + 0$. Given the integers $a = 25$ and $m = 0$, the division algorithm says that this cannot exist since there is no $q \in \mathbb{Z}$ such that $25 = 0 * m$.

The Division Algorithm allows us to create a table of congruence classes. A congruence class is a set of numbers in which every number is equivalent upon division by m. To understand this visually, each integer a will be in the same column as its equivalent numbers, but in a different quotient, q, row. See this diagram of $\mathbb{Z}/7\mathbb{Z}$:

.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
$q = -1$	-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. We say that an integer a is congruent to an integer b modulo m if they have the same remainder in the Division Algorithm.

Another way to understand it is if they are in the same equivalence class. 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 and they are as follows:

(1) a and b are in the same equivalence class.
(2) a and b have the same, least positive, remainder promised by the Division Algorithm.
(3) or $a = b + mk$ for k an integer.
(4) m divides $(a - b)$.

Example 1.6. Given $m = 10$ and $a = 15$, $15 \equiv -5 \bmod 10$ because $15 = 10 * 1 + 5$ and $-5 = 10 * -2 + 5$.
Given $m = 10$ and $a = 15$, $15 \equiv 5$ because $15 = 10 * 1 + 5$ and $5 = 10 * 0 + 5$.
Given $m = 10$ and $a = 5$, $b = 15$ $10|(5 - 15)$ because $10 = (5 - 15) = -10 = 10(-1)$.

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 will begin this proof by making a few things clear. Since we know that $a \equiv b \bmod m$, then we know by definition that $a = mq_1 + r_1$, and $b = mq_2 + r_1$. We also know that $c = mq_3 + r_2$ and $d = mq_4 + r_2$ by definition as well since $c \equiv d$. Since we know these facts, consider:

$$a + c = mq_1 + r_1 + mq_3 + r_2.$$

Combine all factors of m,

$$a + c = m(q_1 + q_3) + r_1 + r_3.$$

Now consider $b + d$:

$$b + d = mq_2 + r_1 + mq_4 + r_2.$$

Combine all factors of m,

$$b + d = m(q_2 + q_4) + r_1 + r_3.$$

Since $a + c$ and $b + d$ have the same remainder, then we know they are congruent to each other mod$m$ by definition. A similar argument can be made for $(a - c) \equiv (b - d)$. Now, in order to prove that $ac \equiv bd$, consider:

$$ac = (mq_1 + r_1)(mq_3 + r_2).$$

Multiply the two factors out:

$$ac = m^2q_1q_3 + mq_1r_2 + r_1mq_3 + r_1r_2.$$

Factor out the m:

$$ac = m(mq_1q_3 + q_1r_2 + r_1q_3) + r_1r_3.$$

Now, we will do the same thing for bd, consider:

$$bd = (mq_2 + r_1)(mq_4 + r_2).$$

Multiply the two factors out:

$$bd = m^2q_2q_4 + mq_2r_2 + r_1mq_4 + r_1r_2.$$

Factor out the m:

$$bd = m(mq_2q_4 + q_2r_2 + r_1q_4) + r_1r_3.$$

Since ac and bd have the same remainder mod$m$, then by definition these are equivalent to each other. Therefore, we have proven our proposition. □

Because of our Proposition 1.7, we will be able to do some form of substitution when computing numbers with large squares modulo m. Since multiplication and subtraction holds when we are computing the congruences of numbers, we are allowed to use Proposition 1.7 to compute smaller numbers. See this example:

Example 1.8.

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

Because $60 = (7 * 8) + 4$, so we are able to substitute the 4 for 60 345 times. So we now have $60^{345} \equiv 4^{345} \equiv x \bmod 7$. After that, we can go further and investigate the powers of 4 modulo 7. We need to observe how the powers of 4 act modulo 7:

$$4^1 \equiv 4 \bmod 7,$$
$$4^{2*1} \equiv 2 \bmod 7,$$
$$4^{3*1} \equiv 1 \bmod 7.$$

Once we get to 4^4, our exponents modulo 7 will cycle back to 4. Now, we have to simplify the exponent 345. We can compute that $345 = 3 * 115$, and we know that an exponent of 4^{3*n} where $n \in \mathbb{Z}$ will become 1 mod 7. What this idea is saying to us is that $4^{345} = 4^3 * 4^3 * ... * 4^3 \equiv (1)^{115} \equiv 1$ modulo 7.

Definition 1.9. With the notation $\mathbb{Z}/m\mathbb{Z}$ we mean the set of congruence classes, $\{[0],[1],[2],...,[m-1]\}$ where the set $[1]$ for example stands for all the numbers in the integers that are congruent to 1 modulo m and addition and multiplication is defined on the congruence classes by adding and multiplying the representatives of the classes modulo m. Often to simplify the notation, we just let $\mathbb{Z}/m\mathbb{Z} = \{0,1,2,3,...,m-1\}$ where $0 = [0]$ etc.

Example 1.10. Given $\mathbb{Z}/7\mathbb{Z}$,

$5 + 6 = 11 \equiv 4 \bmod 7$.

$5 - 6 = -1 \equiv 6 \bmod 7$.

$5 * 6 = 30 \equiv 2 \bmod 7$.

Definition 1.11. A Cyclic Difference Set 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.

We will be studying the cyclic difference sets that come from the squares modulo m. What it means for there to be squares modulo m can best be described with an example. So, see this example and the explanation after to understand this topic:

Example 1.12. For $m = 7$:

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

Since the numbers $D = \{1, 2, 4\}$ are the only non-zero numbers that are appearing when we square our x's modulo 7, then this is the list of non-zero squares in $\mathbb{Z}/7\mathbb{Z}$. Now we are to subtract all the squares with each other. See this play out in the table below:

$1 - 2 = \mathbf{6} \bmod 7$	$1 - 4 = \mathbf{4} \bmod 7$	$2 - 4 = \mathbf{5} \bmod 7$
$2 - 1 = \mathbf{1} \bmod 7$	$4 - 1 = \mathbf{3} \bmod 7$	$4 - 2 = \mathbf{2} \bmod 7$

Since all numbers 1 through 6 are represented one time as a difference between two of the non-zero squares, then D is a cyclic difference set in $\mathbb{Z}/m\mathbb{Z}$.

Definition 1.13. We define $k = |D|$ in a cyclic difference set.

Example 1.14. Given the cyclic difference set $\mathbb{Z}/7\mathbb{Z}$ and its set $D = \{1, 2, 4\}$, $k = 3$.

Definition 1.15. The λ of a cyclic difference set is the number of times the elements in $\mathbb{Z}/m\mathbb{Z}$ are represented as a difference from the distinct squares.

Example 1.16. Let us continue with $\mathbb{Z}/7\mathbb{Z}$ where we know $D = \{1, 2, 4\}$. Recall the table from example 1.11. See how all elements of $\mathbb{Z}/7\mathbb{Z}$ is represented as a difference from the set $D = \{1, 2, 4\}$ one

time. Therefore, we would say that $\lambda = 1$. Furthermore, we always know that λ must always be 1 for the set to be a cyclic difference set.

In this laboratory, we will study the special cyclic difference sets that come from sets D that are made from the non-zero squares modulo m. What we mean by the set of squares modulo m is what was shown in example 1.11.

2. Analysis

The topic of cyclic difference sets is a vast area of study, and there are many elements within the topic that we do not yet have the skill set to prove. To see into the ideas of cyclic difference sets, see these 3 conjectures:

Conjecture 2.1. The set of non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ forms a cyclic difference set if and only if m is a prime of the form $m = 4\lambda + 3$ for an integer k.

Example 2.2. Some primes that follow this structure are thus:

(1) 3, $\lambda = 0$,
(2) 7, $\lambda = 1$,
(3) 11, $\lambda = 2$,
(4) 19, $\lambda = 4$.

We already saw how $\mathbb{Z}/m\mathbb{Z}$ forms a cyclic difference set, so reference that for this conjecture. We see that in these numbers, we will have a cyclic difference set because they are prime, and they cannot be expressed as a sum of two squares. We would assume based on future findings in our lab that any prime will take the form of a cyclic difference set, but since numbers like 5 and 13 can be expressed as a sum of two squares ($2^2 + 1^2 = 5$ and $3^2 + 2^2 = 13$), and hence don't follow the desired form of our Conjecture, then we know they will not form a cyclic difference set. In our laboratory, we saw this pattern arise as we tested different m. So, try your own $m = 4\lambda + 3$ to check the pattern.

Conjecture 2.3. If m is odd and prime and $m = 4\ell + 1$, and $m > 5$, then all non-zero elements in $\mathbb{Z}/m\mathbb{Z}$ can be represented as a difference of squares,

$$\lambda_a = \begin{cases} \ell & \text{for } a \not\equiv x^2 \bmod m \\ \\ \ell - 1 & \text{for } a \equiv x^2 \bmod m. \end{cases}$$

Example 2.4. Given $m = 13$, then we have:

$$D = \{1, 3, 4, 9, 10, 12\}$$

$4 - 1 = \mathbf{3} \bmod 13$	$9 - 12 = \mathbf{10} \bmod 13$	$4 - 3 = \mathbf{1} \bmod 13$
$1 - 10 = \mathbf{4} \bmod 13$	$12 - 10 = \mathbf{2} \bmod 13$	$3 - 4 = \mathbf{12} \bmod 13$
$10 - 1 = \mathbf{9} \bmod 13$	$3 - 10 = \mathbf{6} \bmod 13$	$10 - 12 = \mathbf{11} \bmod 13$
$4 - 9 = \mathbf{8} \bmod 13$	$4 - 10 = \mathbf{7} \bmod 13$	$4 - 12 = \mathbf{5} \bmod 13$
$9 - 10 = \mathbf{12} \bmod 13$		

Other numbers such as $m = 17$ and $m = 29$ were tested in order to derive this pattern.

Conjecture 2.5. If $m = 2p$ where p is odd, then all non-zero elements in $\mathbb{Z}/m\mathbb{Z}$ are represented as a difference of squares,

$$\lambda_a = \begin{cases} \frac{p-1}{2} & \text{for } a \neq p \\ \\ p - 1 & \text{for } a = p. \end{cases}$$

Example 2.6. Given $m = 6$, then we have:

$$D = \{1, 3, 4\}.$$

So we can made the table:

$1-3=\mathbf{4} \bmod 6$	$1-4=\mathbf{3} \bmod 6$	$3-4=\mathbf{5} \bmod 6$
$3-1=\mathbf{2} \bmod 6$	$4-1=\mathbf{3} \bmod 6$	$4-3=\mathbf{1} \bmod 6$

Notice how 3 shows up multiple times. We tested other numbers such as $m = 10$, $m = 14$, and $m = 26$ to derive this pattern.

As stated before, we know broadly what a cyclic difference set is, but to begin to understand the topic in more detail, we come up with this theorem:

Theorem 2.7. *Given $k = |D|$, there are $k(k-1)$ distinct differences that can be made with those k numbers.*

Proof. We want to prove that there are $k(k-1)$ distinct differences where $k \geq 2$. We will continue via proof by induction. Consider the base case $k = 2$:

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

distinct differences. Since we have $s = \{a, b\}$ with two different $a - b, b - a$ then our base case holds, and we will continue by assuming that if we have a set $s = \{a_1, ...a_k\}$, then there are $k(k-1)$ differences. Now suppose we have a set $s = \{a_1, ..., a_k, a_{k+1}\}$. We still make all the $k(k-1)$ differences between all $a_1, ...a_k$, but now we have $2k$ new

differences by doing:

$$a_1 - a_{k+1}, a_{k+1} - a_1,$$

$$.$$

$$.$$

$$.$$

$$a_k - a_{k+1}, a_{k+1} - a_k.$$

Thus, there are $k(k-1)+2k$ differences. Our value $k(k-1)+2k$ can be reduced to $k(k+1)$ between the numbers. Therefore, our inductive step holds and we have proven our statement via induction. □

Remember example 1.11, where we made a table of all the differences of squares for $m = 7$; this is the theorem that explains to us why we have $3(3-1) = 6$ differences. If you are feeling confused as to how many differences you should have when figuring out if you're working with a cyclic difference set, then theorem 2.1 is how you can reassure yourself.

Theorem 2.8. *If D forms a cyclic difference set and there are k elements within D, and λ is a value within D, then $k(k-1) = \lambda(m-1)$.*

Proof. We know that there are $m-1$ elements in $\mathbb{Z}/m\mathbb{Z}$, and $k(k-1)$ represents the number of distinct differences in D.
Since we know $k(k-1)$ is the number of distinct differences in a cyclic difference set, and we also know that all elements of $\mathbb{Z}/m\mathbb{Z}$ must be represented as a difference, then we know that,

$k(k-1)$ must equal the number of differences in D.

We also know that if a set is a cyclic difference set, there are $m-1$ non-zero elements and they must be repeated λ times. So, the number of differences must be $\lambda(m-1)$. Thus, $k(k-1) = \lambda(m-1)$ and we have proven our Theorem. □

Now we want to understand the squares themselves. There might be a pattern within the squares that we don't yet understand, so we must first explore the topic of modular arithmetic in more detail. See this theorem:

Theorem 2.9. *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 for $x \in \mathbb{Z}/m\mathbb{Z}$, $-x \equiv m - x \bmod m$.*

Proof. To show $a \equiv b \bmod m$ we need to show $m|(a-b)$. In order to do this, consider $-x$:

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

Multiply out the negative:

$$-x-m+x.$$

Cancel out the x's:

$$-m.$$

Therefore, $m|-x-(m-x)$ and that therefore shows that $-x \equiv (m-x) \bmod m$. □

What this is pointing us to is to more deeply understand congruence within the elements $\bmod m$. Now, based off this theorem, we now know that large elements within the set $\bmod m$ will be congruent to its negative element.

Now we will explore the behavior of those same elements when squared. See this theorem:

Theorem 2.10. *For $x \in \mathbb{Z}/m\mathbb{Z}$, we have that $x^2 \equiv (m-x)^2 \bmod m$.*

Proof. To show that $x^2 \equiv (m-x)^2 \bmod m$, we need to show that $m|x^2 - (m-x)^2$. Consider:

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

Expand $(m-x)^2$ to be:

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

Multiply out the two factors $(m-x)(m-x)$:

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

Multiply out the negative to $(m^2 - 2mx + x^2)$:

$$x^2 - m^2 + 2mx - x^2.$$

Cancel out the x^2s:

$$-m^2 + 2mx.$$

Factor out the m:

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

Therefore $x^2 - (m-x)^2 = m(-m+2x)$ and hence by our definition of congruence, we have proven the statement. □

Example 2.11. See how this works for $m = 7$ and $x = 4$:

$$4^2 \equiv (7-4)^2 \bmod 7.$$

This is the same as:

$$16 \equiv 3^2 \bmod 7.$$

Since $3^2 = 9$, and $9 \equiv 2 \bmod 7$, then we can write this as:

$$16 \equiv 2 \bmod 7.$$

And this is true. You can see this happening with other m and x.

Now we know that this same behavior holds when the elements are being squared. So now we know that large elements within the set modulo m will be congruent to it's negative element when squared.

The next step in understanding the topic of Cyclic Difference Sets completely is to understand the number of elements within the squares mod$m$. Since the squares of a set being able to derive all elements in the original set via a difference is what defines a Cyclic Difference Set, we want to know how many elements will be in the set of squares. First, we will find the pattern for odd m. See this theorem:

Theorem 2.12. *In $\mathbb{Z}/m\mathbb{Z}$ when m is odd, the number of distinct non-zero squares in is less than or equal to $\frac{(m-1)}{2}$.*

Proof. To prove this theorem, consider the theorem previous: Theorem 2.3 states that $x^s \equiv (m-x)^2 \bmod m$. So, given this theorem, consider $(m-1)^2$ which is the largest element in $\mathbb{Z}/m\mathbb{Z}$:

$$(m-1)^2 \equiv 1^2 \bmod m.$$

Since we know this is true, we then can continue with every other element within $\mathbb{Z}/m\mathbb{Z}$,

$$(m-2)^2 \equiv 2^2 \bmod m,$$

$$(m-3)^2 \equiv 3^2 \bmod m,$$

$$\vdots$$

$$(\frac{m-1}{2})^2 \equiv (m - \frac{m-1}{2})^2 \bmod m = (\frac{m+1}{2})^2 \bmod m$$

As one may notice, this will produce a reflective pattern within the squares. Where the largest elements have the same squares as it's opposite, smallest element. Because of this pattern, there will be, at most, half as many non-zero squares as there are non-zero elements within $\mathbb{Z}/m\mathbb{Z}$. At the most central point in the set, we can then imagine how the two middle elements will have the square of $\frac{m-1}{2}$ and then, $\frac{m+1}{2}$ since our m is an odd number. Since $(\frac{m+1}{2})^2 \bmod m$ would be the same as $(\frac{m-2}{2})^2 \bmod m$, then we know that the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is less than or equal to $\frac{m-1}{2}$. □

Now we have an upper bound on the number of non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ when m is odd.

We will now continue to understand the pattern for different types of m. See this theorem for even m:

Theorem 2.13. *In $\mathbb{Z}/m\mathbb{Z}$, if m is even, then the number of distinct non-zero squares in $\mathbb{Z}/m\mathbb{Z}$ is less than or equal to $\frac{m}{2}$.*

Proof. For this proof, we can look to the proof for the theorem 2.4 to serve as a base for this, as they are largely the same. The only difference between these two theorems, however, is the behavior we observe in the middle of the set. If we were to take the squares of all elements, we would not see the pattern of $\frac{m-1}{2}$ and $\frac{m+1}{2}$ as the most

central elements in the set. See this idea visualized here:

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

Because our m is an even number, we are able to divide the set of squares into an even $\frac{m}{2}$ by definition. So, we would see the middle-most element in the set of distinct squares of $\mathbb{Z}/m\mathbb{Z}$ where m is an even number as $\frac{m}{2}$ because of its evenness. Therefore, we know that the number of distinct non-zero squares would be less than or equal to $\frac{m}{2}$. □

We may see a pattern with how m is being manipulated in the numerator when the m is odd versus when m is even. This has more to

do with the fact that m can be divided by a number, and not with the fact that it is odd or even.

To continue our discovery of this topic, we will look at the pattern of m when it is the product of a squared number. See this theorem:

Theorem 2.14. *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 and less than $\frac{m}{2}$ if m is even*

Proof. For this proof, we have two cases:

- Where m is odd.
- Where m is even.

Because of this, we will continue with proof by cases. Case 1 is where m is even. First off, we need to establish that $a^2 \equiv 0 \bmod m$. Now, because m is even, we then can consider:

$$2 \leq a.$$

Since 2 is our first even number within $\mathbb{Z}$. Now, we can consider:

$$2a \leq a^2.$$

Now divide the 2 to get:

$$a \leq \frac{a^2}{2}.$$

Since we know $a^2 = m$, we can write this equality as:

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

Since we know $a^2 \equiv 0 \bmod m$, and that $a \leq \frac{m}{2}$, then we will not be counting a number of distinct non-zero squares, we will in fact have less than $\frac{m}{2}$. Therefore, we have proven our case where m is even.
Now, consider the case where m is odd. We need to show $1 < a < \frac{m-1}{2}$. Consider a:

$$1 < a.$$

We know from our statement. Now consider 2:

$$2 < a.$$

We know this because a has to be an odd integer. Now we can multiply both sides by a:

$$2a < a^2.$$

We know this to be true. Now, if we were to consider $a^2 - 1$:

$$2a \leq a^2 - 1.$$

Since we do not know that $2a$ is strictly less than $a^2 - 1$, we have to change the inequality. Now, we divide both sides by 2:

$$a \leq \frac{a^2 - 1}{2}.$$

Now we can consider $m = a^2$:

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

Now since $a^2 \equiv 0 \bmod m$ and $a \leq \frac{m-1}{2}$, then there can't be $\frac{m-1}{2}$ distinct non-zero squares. Therefore, we have proven our case where m is odd. Since we have proven both cases where m is odd and m is even, then we have therefore proven our Theorem by proof by cases. □

This result is a similar idea to the previous theorems we were looking over. However, we now know that the same idea holds for odd m that is divisible by something. In other words, we know the pattern for non-prime odd m.

We will continue with this exploration for non-prime m and see if the pattern changes for $m = ab$ where a, b are odd numbers. Think of numbers like $15 = 3 * 5$ when looking over this theorem:

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

Proof. To prove this Theorem, we need to find two numbers less than $\frac{m-1}{2}$ that have the same square in order to show that we have strictly less than $\frac{m-1}{2}$ distinct squares. We will continue with this proof via contradiction.

Consider $a, b \in \mathbb{Z}/m\mathbb{Z}$. Consider $(a+b)^2 - (a-b)^2$:

$$(a+b)^2 - (a-b)^2 =,$$

$$a^2 + 2ab + b^2 - a^2 - 2ab - b^2 =,$$

$$4ab =,$$

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

By definition of congruence, $(a+b)^2 \equiv (a-b)^2 \bmod m$. We know $m - (a+b) \equiv (a+b)^2 \bmod m$ and $m - (a-b) \equiv (a-b)^2 \bmod m$. So, we know that these two numbers, when subtracted by the modulus, are equal to their squares. Let us summarize the information we have accumulated thus far:

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

$$(a+b)^2 = mk + (m - (a+b)),$$

$$(a+b)^2 = mk + m - a - b,$$

$$(a+b)^2 = m(k+1) - a - b.$$

We also know:

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

$$(a-b)^2 = mk + (m - (a-b)),$$

$$(a-b)^2 = mk + m - a + b,$$

$$(a-b)^2 = m(k+1) - a + b.$$

So, from this, we know that $(a+b)^2 \not\equiv (a-b)^2$ since the remainders are different. Therefore, we have a contradiction. Since we have a contradiction, we therefore know that our original statement is true. Therefore, we have proven our Theorem via contradiction. $\square$

Now we know a very specific pattern for odd m that is the result of a product. To continue with this idea, we can see that the end of the proof holds by looking at $m = 15$, since the number of distinct squares within $m = 15$ is 5.

Now we want to specify our pattern for when m is prime, as we have only been looking at odd m where it is divisible by something. See this theorem:

Theorem 2.16. *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. Because we know m is an odd prime, then we know by theorem 2.4 the largest number of non-zero distinct squares a set can have is $\frac{m-1}{2}$. Therefore, we have to prove that $\frac{m-1}{2}$ is the exact number of non-zero squares. We take $1 \leq x < y \leq \frac{m-1}{2}$, and we want to show that $x^2 \not\equiv y^2 \bmod m$. Let us continue to prove this by contradiction. We suppose $x^2 \equiv y^2 \bmod m$, so consider:

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

Via the definition of congruence, $x^2 - y^2 \equiv 0 \bmod m$ is equal to:

$$x^2 - y^2 = mk.$$

Therefore, we know $m|(x^2 - y^2)$. We can expand this to being $m|(x + y)(x - y)$. However, m is prime, so $m|(x - y)$ or $m|(x + y)$. So, $x \equiv y \bmod m$ or $x \equiv -y \bmod m$. Since $1 \leq x < y \leq \frac{m-1}{2}$, neither of the above equalities hold since x, y cannot be equal to each other

and m is defined as prime. So, $x^2 \not\equiv y^2 \bmod m$. Therefore, there are $\frac{m-1}{2}$ distinct non-zero squares mod a prime m and we have proven our Theorem via proof by contradiction. □

Now we know the strict pattern where m is prime.

Example 2.17. The result for when $m = 5$ is the squares being: $\{1, 4\}$, and the difference count being: $\{1 = 0, 2 = 1, 3 = 1, 4 = 0\}$. See how $\frac{5-1}{2} = 2$ and our example shows this to be true.

To continue with prime m see this theorem:

Theorem 2.18. *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. Since we have $\frac{m-1}{2}$ squares, we then know m is odd since $\frac{m-1}{2}$ for an even $m \notin \mathbb{Z}$. So, now we know m is odd. We can continue to say that $m \neq ab$ for a, b odd integers because then we would have $< \frac{m-1}{2}$ non-zero distinct squares. Additionally, we know that $m \neq a^2$ since there would be $< \frac{m-1}{2}$ non-zero distinct squares. Therefore, m cannot be composite and must be prime. Thus, we have proven our Theorem. □

Now we know that if m is prime, then $\frac{m-1}{2}$ is the number of distinct squares, **and** that if $\frac{m-1}{2}$ is the number of distinct squares then m is prime.

Theorem 2.19. *Suppose D is the set of squares in $\mathbb{Z}/m\mathbb{Z}$ and forms and cyclic difference set, and $|D| = \frac{m-1}{2}$, then m is prime and $m = 4\lambda + 3$.*

Proof. By Theorem 2.9, since the number of non-zero squares is $\frac{m-1}{2}$, we know that m must be an odd prime since there are the maximum number of squares. Now, by Theorem 2.2, which states $k(k-1) = \lambda(m-1)$, and the fact that we know $k = \frac{m-1}{2}$, then we can consider: Substitute all ks with $\frac{m-1}{2}$:

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

Give the inside of the parentheses a common divisor:

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

Multiply out the $\frac{m-1}{2}$ to get rid of the parentheses:

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

Cancel out the $(m-1)$ from both sides of the equation:

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

Multiply both sides by 4:

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

Add three to both sides:

$$m = 4\lambda + 3$$

Since our $m = 4\lambda + 3$, we have therefore proven our theorem. □

3. Conclusion

In this report, we thoroughly investigated the behavior of cyclic difference sets. Make sure to try searching for other cyclic difference sets as examples, since in this report we mostly used the example of $\mathbb{Z}/m\mathbb{Z}$ to illustrate our points. There are some unanswered questions that arise within this report. One of them being, what is the connection with the Gaussian integers, $\mathbb{Z}[i]$, and cyclic difference sets? If you are familiar with the topic of Gaussian integers, then you would be able to recognize that Theorem 2.14 points to the fact that primes in the integers that remain prime in the Gaussian integers have the property that when you look at $\mathbb{Z}/m\mathbb{Z}$ for those primes, their set of non-zero squares form cyclic difference sets. This topic is not explored within this report, and we do not yet have the skill set to prove this conjecture. In conclusion, we are now able to understand the fundamentals of cyclic difference sets, how different kinds of m affect the set, and what can and cannot be a cyclic difference set.

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: souma23a@mtholyoke.edu

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