An Introduction to Equation Solving in Finite Systems
UCI Math Circle

1 Introduction

Tonight we will be learning about the finite systems (rings) $\mathbb{Z}_n$, where n is a natural number greater than or equal to 2. When we solve linear or quadratic equations over the real numbers, we have a set of techniques that after time become second nature to us. For instance, suppose we try to solve the linear equation $y = mx + b$ for x. We subtract b from both sides and multiply by $\frac{1}{m}$, so long as m is not zero. Or suppose we want to factor $x^2 - 4$ as $(x-2)(x+2)$. If you were asked to find where this product is zero, you would set $(x-2) = 0$ and $(x+2) = 0$ and have your solution. As you will see tonight, however, these techniques we take for granted may have strange behavior in finite systems. In fact, some of these finite systems will even have non-zero elements that together multiply to zero (these are called zero divisors) and fail to have multiplicative inverses!

1.1 Acknowledgments

This lesson was heavily influenced by the Teachers' Circle Workshop paper on finite systems. The challenge problem found later in this lesson was influenced by Chapter 19, Exercise 12 in Fraleigh's "A First Course in Abstract Algebra."

2 Directions for the Instructor

Begin by defining $\mathbb{Z}_n$ as the set $\{0, 1 \ldots, n-1\}$ together with multiplication and addition modulo n. Introduce the notation $+_n$ and $\times_n$ for addition and multiplication modulo n, respectively, and define the modulo operation. To help the students understand these concepts, fill out addition and multiplication tables together as a class for $\mathbb{Z}_3$ and $\mathbb{Z}_4$, given below.

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Addition and multiplication tables for $\mathbb{Z}_3$.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Addition and multiplication tables for $\mathbb{Z}_4$.

To check the understanding of the class, ask whether $\mathbb{Z}_3$ and $\mathbb{Z}_4$ have multiplicative and additive inverses and to identify them. Ask students to find a non-zero element of $\mathbb{Z}_4$ which does not have a multiplicative inverse and ask students if such an element exists in $\mathbb{Z}_3$. Ask the students to find an example of a zero divisor. To demonstrate the usefulness of the tables, help students solve $3x + 3 = 2$ in $\mathbb{Z}_4$. Ask them for the additive inverse of 3 (what added to 3 makes 0 in $\mathbb{Z}_4$) and for

the multiplicative inverse of 3 (what times 3 makes 1 in $\mathbb{Z}_4$.) Demonstrate the following.

$$\begin{aligned} 3x+3 \equiv_4 2 &\iff 3x+3+1 \equiv_4 2+1 \\ &\iff 3x \equiv_4 3 \\ &\iff (3)3x \equiv_4 (3)3 \\ &\iff x \equiv_4 1. \end{aligned}$$

Explain that when we are working modulo n the solutions we find to equations are not single values. Using the example above, explain that $x \equiv_4 1$ means that any integer of the form $4m+1$ will be a solution to our equation.

3 Worksheet for Students

3.1 Introduction and Background Information

Here is a copy of the introduction and examples done together as a class. If you are comfortable with the material so far feel free to move on to the problems!

Tonight we will be learning about the finite systems (rings) $\mathbb{Z}_n$, where n is a natural number greater than or equal to 2. When we solve linear or quadratic equations over the real numbers, we have a set of techniques that after time become second nature to us. For instance, suppose we try to solve the linear equation $y = mx + b$ for x. We subtract b from both sides and multiply by $\frac{1}{m}$, so long as m is not zero. Or suppose we want to factor $x^2 - 4$ as $(x-2)(x+2)$. If you were asked to find where this product is zero, you would set $(x-2) = 0$ and $(x+2) = 0$ and have your solution. As you will see tonight, however, these techniques we take for granted may have strange behavior in finite systems. In fact, some of these finite systems will even have non-zero elements that together multiply to zero (these are called zero divisors) and fail to have multiplicative inverses!

Let's start by defining what we mean by $\mathbb{Z}_n$. Let n be an integer greater than or equal to 2. Then $\mathbb{Z}_n$ is the set of numbers $\{0, 1, 2, \ldots, n-1\}$. Using this set of numbers, instead of adding and multiplying how we normally would, we do these operations *modulo n*. This is just a fancy way of saying that we record the remainder when we divide by n and take that as our answer. Let's look at an example to see what this means. The set $\mathbb{Z}_3$ is equal to $\{0, 1, 2\}$. To add in $\mathbb{Z}_3$ we add numbers like we normally would but divide by 3 and take the remainder as our answer. For example, $1 + 2 = 3$ and 3 divide by 3 is 1, which has 0 remainder. We say that $1 +_3 2 \equiv_3 0$; $+_3$ just tells us that we are doing addition modulo 3 and $\equiv_3$ tells us that our solution is an element of $\mathbb{Z}_3$ (there is one more important thing to note about this symbol, but we will talk about it a little later.) Notice that the elements of $\mathbb{Z}_3$ are all the possible remainders we can get when we divide by 3.

Let's do one more example with multiplication this time: $2 \times 2 = 4$ and 4 divided by 3 has remainder 1. We say that $2 \times_3 2 \equiv_3 1$. Notice that similar to addition, $\times_3$ just tells us that we are doing multiplication modulo 3. Below you will find the addition and multiplication tables for $\mathbb{Z}_3$ and $\mathbb{Z}_4$. You read them by taking a number in a row and a number in a column. Then the sum (or product) of the numbers is equal to the number you find where the row and column intersect. Suppose we wanted to find what $2 \times_4 2$ is in $\mathbb{Z}_4$. The highlighted cell in the multiplication table for $\mathbb{Z}_4$ shows where we could find the answer to $2 \times_4 2$.

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Addition and multiplication tables for $\mathbb{Z}_3$.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Addition and multiplication tables for $\mathbb{Z}_4$.

Looking at the multiplication table for $\mathbb{Z}_4$, do you notice anything strange? We see that 2 is a non-zero number, but it has no multiplicative inverse. If we look along the row for 2 we see that there is no 1. This means that there is no other element in $\mathbb{Z}_4$ that we could multiply 2 with to get 1. The number 2 in $\mathbb{Z}_4$ is what we call a zero divisor. Notice that 2 is not equal to 0 but $2 \times_4 2 \equiv_4 0$. Are there any elements in $\mathbb{Z}_3$ with this property? We will now try to solve the equation $3x +_4 3 \equiv_4 2$. Looking at the table for $\mathbb{Z}_4$, we see that the additive inverse of 3 is 1 ($3 +_4 1 \equiv_4 0$) and the multiplicative inverse of 3 is 3 ($3 \times_4 3 \equiv_4 1$.) Then, to solve the equation we first add 1 to both sides and then multiply both sides by 3.

$$\begin{aligned} 3x +_4 3 +_4 1 &\equiv_4 2 +_4 1 \text{ (Add 1 to both sides.)} \\ 3x &\equiv_4 3 \ (2 +_4 1 \equiv_4 3) \\ 3 \times_4 3x &\equiv_4 3 \times_4 3 \text{ (Multiply both sides by 3.)} \\ x &\equiv_4 1 \end{aligned}$$

So we see that $x \equiv_4 1$ is our solution. The other important thing to note about the $\equiv_4$ notation is that it means our equation does not just have one solution, but a family of them. Notice that $x \equiv_4 1$ means that any x that has a remainder of 1 when divided by 4 will be a solution to our equation.

3.2 Problem Set

1. Similar to how we filled out addition and multiplication tables for $\mathbb{Z}_3$ and $\mathbb{Z}_4$ as a class, fill out the corresponding tables for $\mathbb{Z}_6$.

$+_6$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

$\times_6$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

2. Fill out the addition and multiplication tables for $\mathbb{Z}_7$.

$+_7$	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

$\times_7$	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

3. Using your tables for addition and multiplication in $\mathbb{Z}_7$, answer the following questions.

(a) What is the additive inverse of 2 in $\mathbb{Z}_7$? (what number added to 2 is 0?)

(b) What is the multiplicative inverse of 2 in $\mathbb{Z}_7$? (what number multiplied with 2 is 1?)

(c) Using parts (a) and (b), solve $2x + 2 = 4$ in $\mathbb{Z}_7$.

(d) Since $\mathbb{Z}_7$ only has 7 elements, it is easy to check for solutions to linear equations. We just have to try all possible values of x. Show that you can also find solutions to $2x + 2 = 4$ in $\mathbb{Z}_7$ by filling out the table below.

x	$2x + 2$
0	
1	
2	
3	
4	
5	
6	

(e) What is the range of $f(x) = 2x + 2$ in $\mathbb{Z}_7$? (Range is the set of values the function outputs. What are the possible values of $2x + 2$ in $\mathbb{Z}_7$?) Do you notice anything special about it? How does it compare to the range of $f(x) = 2x + 2$ in the real numbers?

4. We now try to solve $3x + 2 = 4$ in $\mathbb{Z}_6$. Fill out the table below (remember that all addition and multiplication should be done modulo 6.) Do you see any solutions?

x	$3x + 2$
0	
1	
2	
3	
4	
5	

5. Why doesn't $3x + 2 = 4$ have a solution in $\mathbb{Z}_6$? (Hint: think about multiplicative inverses. What elements in $\mathbb{Z}_6$ don't have multiplicative inverses?)

6. (MC4-HReiter) We now move to solving quadratic equations. When we think of solving quadratic equations over the real numbers, we have two main techniques at our disposal: factoring and the quadratic formula. The following problems are meant to highlight why these techniques work in $\mathbb{R}$ and help us figure out when they might work in finite systems. Tonight we will be focusing on factoring.

   (a) How would you try to solve $x^2 - 4x + 3 = 0$ over the real numbers using the factoring technique?

   (b) Try multiplying $(x - 3)(x - 1)$ together in $\mathbb{Z}_7$. $\mathbb{Z}_7$ is a commutative ring, which means multiplication has the commutative property ($a \times b = b \times a$ for any a, b in $\mathbb{Z}_7$) and you may expand the product using normal techniques. Remember that multiplication and addition are done modulo 7 and that -3 means the additive inverse of 3, which is 4.

(c) In the previous question you should have found that $(x-3)(x-1)$ is equal to x^2-4x+3. Look at the multiplication table for $\mathbb{Z}_7$. Do you see any non-zero elements that do not have a multiplicative inverse? Remember that if a non-zero number does not have a multiplicative inverse it is called a zero divisor. If $\mathbb{Z}_7$ has no zero divisors, then $a \times b = 0$ if and only if a or b is 0. Using this, how many solutions does $(x-3)(x-1) = 0$ have in $\mathbb{Z}_7$? What are they?

7. How many solutions does $x^2 - x = 0$ have in the real numbers? What are the solutions? How would you factor $x^2 - x$?

8. Fill out the table below to find the solutions to $x^2 - x = 0$ in $\mathbb{Z}_6$. Remember that all multiplication and addition is done modulo 6.

x	$x^2 - x$
0	
1	
2	
3	
4	
5	

9. Using the table above, how many solutions to $x^2 - x = 0$ are there in $\mathbb{Z}_6$? Is this more or less than the number of solutions over the real numbers?

10. If we try to solve $x(x-1)$ by setting $x = 0$ and $x - 1 = 0$ in $\mathbb{Z}_6$ do we get all the solutions? Why or why not?

4 Challenge Problem/Take-Home Problem

(Fraleigh-19,12) For this problem, we will be looking at $\mathbb{Z}_3 = \{0, 1, 2\}$. $\mathbb{Z}_3$ is said to have characteristic 3. This means that if we take any element of $\mathbb{Z}_3$ and multiply by 3, it will be equal to 0 modulo 3. To see that this is true, try it out for yourself in the table below. Remember that multiplication is done modulo 3.

x	$3x$
0	
1	
2	

Show that because $\mathbb{Z}_3$ has characteristic 3 for any a, b in $\mathbb{Z}_3$ it is true that $(a+b)^9 = a^9 + b^9$. Hint: write $(a+b)^9 = ((a+b)^3)^3$. First figure out what $(a+b)^3$ is in $\mathbb{Z}_3$ and figure out what the cube of that is in $\mathbb{Z}_3$.

5 Solutions to Worksheet

1. Here are the addition and multiplication tables for $\mathbb{Z}_6$. Remember that when working in $\mathbb{Z}_6$ we divide by 6 and record the remainder when doing addition and multiplication. For example, $5 +_6 1 \equiv_6 0$ since the remainder of 6 divided by 6 is 0.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

2. Here are the addition and multiplication tables for $\mathbb{Z}_7$. We fill them out similarly to how we did for $\mathbb{Z}_6$, but now record the remainder after division by 7.

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\times_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

3. Using your tables for addition and multiplication in $\mathbb{Z}_7$, answer the following questions.

   (a) What is the additive inverse of 2 in $\mathbb{Z}_7$? (what number added to 2 is 0?)

   We look at the row for 2 in our addition table and see that $2 + 5 \equiv_7 0$. We see that 5 is the additive inverse of 2 in $\mathbb{Z}_7$.

   (b) What is the multiplicative inverse of 2 in $\mathbb{Z}_7$? (what number multiplied with 2 is 1?)

   We look in our multiplication table for $\mathbb{Z}_7$ and look for something that multiplies with 2 to make 1. We see that $2 \times 4 \equiv_7 1$, so 4 is the multiplicative inverse of 2 in $\mathbb{Z}_7$.

   (c) Using parts (a) and (b), solve $2x + 2 = 4$ in $\mathbb{Z}_7$.

We can solve the equation as follows.

$$\begin{aligned} 2x + 2 + 5 &\equiv_7 4 + 5 \\ 2x &\equiv_7 2 \\ (4)2x &\equiv_7 (4)2 \\ x &\equiv_7 1 \end{aligned}$$

We see that $x \equiv_7 1$, so any integer of that form $7n + 1$ will be a solution to this equation since the remainder of $7n + 1$ is always 1 if n is an interger.

(d) We will now show that we can find the solution to the equation by simply trying every value of x and seeing if we get that $2x + 2 = 4$.

x	$2x + 2$
0	2
1	4
2	6
3	1
4	3
5	5
6	0

(e) What is the range of $f(x) = 2x + 2$ in $\mathbb{Z}_7$? Do you notice anything special about it? How does it compare to the range of $f(x) = 2x + 2$ in the real numbers?

To find the range of $f(x)$ we look at the right-most column of our table. We see that $\{0, 1, 2, 3, 4, 5, 6\}$ are the elements of the range. Notice that they are the same as the elements in $\mathbb{Z}_7$. When a function has this property we say that it is surjective (or onto); the equation $f(x) = 2x + 2$ in the real numbers is also surjective. This means that for any number y we pick, we can always solve $y = 2x + 2$.

4. We now try to solve $3x + 2 = 4$ in $\mathbb{Z}_6$. Fill out the table below (remember that all addition and multiplication should be done modulo 6.) Do you see any solutions?

x	$3x + 2$
0	2
1	5
2	2
3	5
4	2
5	5

Looking in the right column, we never see the number 4 appear. We see that there are no solutions to this equation in $\mathbb{Z}_6$.

5. Why doesn't $3x + 2 = 4$ have a solution in $\mathbb{Z}_6$? (Hint: think about multiplicative inverses. What elements in $\mathbb{Z}_6$ don't have multiplicative inverses?)

   Let's try to solve $3x + 2 = 4$ in $\mathbb{Z}_6$. Looking at our addition table we see that the inverse of 2 is 4, but what happens when we try to find a multiplicative inverse for 3? We see that there is no element in $\mathbb{Z}_6$ that multiplies with 3 to make 1.The reason for this is that 3 is a zero divisor. Notice that 2 times 3 is 0 in $\mathbb{Z}_6$. Just like how we can't divide by zero, we can't divide by 3 in $\mathbb{Z}_6$. For those who are interested, the "deeper" reason that there is no solution to this equation is that the greater common divisor of 3 and 6 does not divide 2; to learn more, try searching for "solving linear equations in a ring."

   $\star$ From this point on we will drop the "$\equiv$" notation when solving equations, but please keep in mind that when we get solutions in our finite systems, they are not single solutions but a family of solutions that all have the same remainder.

6. (MC4-HReiter)

   (a) How would you try to solve $x^2 - 4x + 3 = 0$ over the real numbers using the factoring technique?

   We factor this equation as $x^2 - 4x + 3 = (x - 3)(x - 1)$ and set it equal to zero. Since every non-zero real number has a multiplicative inverse, we know that there are no zero divisors in the real numbers. Because of this, $(x-3)(x-1) = 0$ means the only solutions are given by $x - 3 = 0$ and $x - 1 = 0$, so $x = 3$ and $x = 1$ are our solutions.

   (b) Try multiplying $(x - 3)(x - 1)$ together in $\mathbb{Z}_7$. $\mathbb{Z}_7$ is a commutative ring, which means multiplication has the commutative property ($a \times b = b \times a$ for any a, b in $\mathbb{Z}_7$) and you may expand the product using normal techniques. Remember that multiplication and addition are done modulo 7 and that -3 means the additive inverse of 3, which is 4.

   Because $\mathbb{Z}_7$ has many nice properties (it is a field!) we can just FOIL this as $(x-3)(x-1) = x^2 - x - 3x + 3 = x^2 - 4x + 3$. What if we didn't know $\mathbb{Z}_7$ had these nice properties? Any ring must satisfy the distributive law, so we could alternatively solve the problem like this,

$$\begin{aligned}(x - 3)(x - 1) &= (x - 3)(x) + (x - 3)(-1) \\ &= x^2 - 3x - x + 3 \\ &= x^2 - 4x + 3.\end{aligned}$$

   (c) In the previous question you should have found that $(x-3)(x-1)$ is equal to x^2-4x+3. Look at the multiplication table for $\mathbb{Z}_7$. Do you see any non-zero elements that do not have a multiplicative inverse? Remember that if a non-zero number does not have a

multiplicative inverse it is called a zero divisor. If $\mathbb{Z}_7$ has no zero divisors, then $a \times b = 0$ if and only if a or b is 0. Using this, how many solutions does $(x-3)(x-1) = 0$ have in $\mathbb{Z}_7$? What are they?

We see that $\mathbb{Z}_7$ has no zero divisors. Because of this, $(x-3)(x-1)$ is equal to 0 if and only if $(x-3) = 0$ or $(x-1) = 0$. This shows that there are only two solutions: $x = 3$ and $x = 1$.

7. How many solutions does $x^2 - x = 0$ have in the real numbers? What are the solutions? How would you factor $x^2 - x$?

   We can factor $x^2 - x = 0$ into $x(x-1) = 0$. Because $\mathbb{R}$ has no zero divisors, we know that $x(x-1) = 0$ if and only if $x = 0$ or $x = 1$. We see that there are exactly 2 solutions: $x = 0$ and $x = 1$.

8. Here is the table for $x^2 - x = 0$ in $\mathbb{Z}_6$. Remember that all multiplication and addition is done modulo 6.

x	$x^2 - x$
0	0
1	0
2	2
3	0
4	0
5	2

9. Using the table above, how many solutions to $x^2 - x = 0$ are there in $\mathbb{Z}_6$? Is this more or less than the number of solutions over the real numbers?

   We see from the table about that there are 4 solutions: $x = 0$, $x = 1$, $x = 3$, and $x = 4$. Recall that there were only 2 solutions over the real numbers.

10. If we try to solve $x(x-1)$ by setting $x = 0$ and $x - 1 = 0$ in $\mathbb{Z}_6$ do we get all the solutions? Why or why not?

    Notice that we get some of the solutions, but not all of them. This is again because $\mathbb{Z}_6$ has zero divisors, and it is possible for two non-zero numbers to still multiply to zero.

6 Solution to Challenge/Take-Home Problem

We first expand $(a+b)^3$. We can do this using normal techniques because $\mathbb{Z}_3$ is a field and has many of the nice properties we associate with the real numbers. Recall that 3 times anything in $\mathbb{Z}_3$ is 0

(the table you filled out should have all zeros in the right column.)

$$\begin{aligned}(a+b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3 \\ &= a^3 + b^3 \\ ((a+b)^3)^3 &= (a^3 + b^3)^3 \\ &= a^9 + 3a^6b^3 + 3a^3b^6 + b^9 \\ &= a^9 + b^9.\end{aligned}$$

You may be wondering if a^6b^3 and other powers of a and b are contained in $\mathbb{Z}_3$. The answer is yes because $\mathbb{Z}_3$ is closed under both addition and multiplication. This means that no matter what we add and multiply in $\mathbb{Z}_3$, the sum or product will stay in $\mathbb{Z}_3$. For those who are interested, you may look up the definitions of groups and rings to learn more about the properties of $\mathbb{Z}_3$ and other similar structures.