Quadratics: Put a Ring On It

by Tyler Erb, 2016 CTI Fellow
Community House Middle School

This curriculum unit is recommended for:
Math 2, grade 8 or 9

Keywords: modular arithmetic, additive inverse, multiplicative inverse, linear equation, quadratic equation, quadratic formula,

Teaching Standards: See Appendix 1 for teaching standards addressed in this unit.

Synopsis: This curriculum unit will focus on having students get back to basics of using the language of multiplicative inverse and additive inverse while extending students understanding of solving linear and quadratic equations. Students will investigate how to solve both linear and quadratic equations by using modular arithmetic to solve. Using field Z_5 and ring Z_6, students will have to first start by solving linear equations by finding additive inverses that add the constant to either 5 or 6 respectively. When solving linear equations with a variable other than one, students will discover that the multiplicative inverse for a number is not the reciprocal which is what they are accustom to in their normal solution set of all real numbers. By taking them outside the normal way they solve linear and quadratic equations, they go back to remembering the basics of additive and multiplicative inverse. Students finish the unit by proving that the quadratic formula in Z_5 and move on to solving quadratic equations.

I plan to teach this unit during the coming year to 28 students in Math 2 to 8th Graders.

Quadratics: Put a Ring On It

Tyler Erb

Introduction

Every year, over thirty of Charlotte's brightest math students walk down the halls of Community House Middle School. These students are great problem solvers and conceptually understand math better than any other students in the school. They are enrolled in the highest level math class one can take at the middle school level, Math 2. As eighth graders, they are taking a class meant for sophomores; therefore they are able to grasp almost any topic with relative ease. 11 out of the 38 students that I taught Math 2 to last year were able to get a perfect score on the end of year assessment from the state, and all finished with an "A" average. With that in mind, I sometimes find it hard to challenge my students in some content areas in which I teach. Differentiating can be difficult as I need to teach to meet the needs of all students, those working to grasp Math 2 concepts and those capable of taking Math 3.

An interesting part about my students' accelerated path is that all of them had to take honors sixth grade math and Math 1 in seventh grade. This means that at the sixth grade, they were able to solve equations with variables on both sides and solving basic one variable equations. In seventh grade, they were capable of solving quadratic equations for their roots. These students have been introduced and mastered some of the basics of algebra for a few years now. They have mastered solving problems with the basic operations for some time. This means that some of the mystery of math and algebra has vanished for them. They know once they get to a certain step in solving an algebraic problem, it is the same routine that they have done since they were in elementary school or the beginning of middle school. In turn, I want to challenge my students by having solve linear and quadratic equations over other rings and fields.

With rings, specifically Z_6, and the field of Z_5, students will see an entirely new way to look at solving linear and quadratic equations. [1] I hope to instill in my students a sense of lost enthusiasm and sense of discovery when it comes to solving these types of problems. They will have to refer to their tables, and have some prior knowledge of modular arithmetic. By introducing the topic of solving linear and quadratic equations, my goal is for students to return to their rudimentary understanding of how to solve these types of problems. Therefore, allowing students to break away from routine procedures when solving equations. Students will gain a deeper understanding by having to go back to the basics of subtracting a number to isolate the variable, adding the additive inverse. They will have more of a conceptual knowledge conveying the reasoning for dividing. Division is the same as multiplying by the multiplicative inverse. This will hopefully carry into the classroom where we can use proper math terminology in class. Having learned these operations at such a young age, many students are relying on rote memorization without truly understanding the reasoning behind the mathematics.

Lastly, my final is to further encourage the sense of discovery and exploration when it comes to mathematics topics outside the boundary of the school curriculum. I want students interested in fields beyond what they are "told to learn". When students propel their own learning goals and topics of interest they begin to truly value learning becoming further engaged and responsible in the learning process. By teaching students topics outside of what they need to know for the curriculum, they get excited to do research on their own and discover math they potentially would not have been exposed to.

School/Student Demographic

My school is 57% white, 12% black, 5% Native American, 17% Asian, 11 % Hispanic while 5% is race unknown. 42% are male and 58% are female. 23% are academically gifted while 5% are students with disabilities. Overall only 17% are economically disadvantaged. In total, there were 1753 students enrolled at Community House last year.

Unit Goals

The major unit goals are to challenge students in a topic branching off of their normal curriculum, for students to better understand why we can subtract and divide, and lastly to introduce intriguing topics outside of their day to day math. This unit will extend after our quadratic unit where students have just discovered imaginary solutions. Once students have done that, this lesson will seem easy until they understand that operations such as division and subtraction no longer exist in the conventional sense. Students will have to discover what it truly means to divide and subtract. This means they will have to add the additive inverse and use the multiplicative inverse to reduce quantities to zero, or one respectively. Lastly, students will be intrigued by this new branch of math that they have not been exposed to before. Having that sense of wonder and secrecy about math makes students engaged in their learning. The students will be excited to learn mathematics that no other group of students in the school will be learning not to mention that many high school students won't learn. They will instantly want to devour all of the information given to them!

Although this lesson does not align to any of the North Caroline State Standards it does go into solving linear equations and even quadratic equations. Furthermore the lesson does not deal with anything pertaining to complex numbers. My goal is by stretching the standards a little, I will be able to teach concepts from NC.M2.A-REI.1 where students will have to justify a method of solving their quadratic equations. It also utilizes NC.M2.F-IF.8 where students have to complete the square to solve quadratic functions and interpret the solutions in context. Lastly, the unit will go into all 8 standard practices in depth as students will have to reason through the field Z_5 and ring Z_6.

Content Research

The first thing to understand about this entire unit is modular arithmetic. Modular arithmetic is a special type of arithmetic where all other values wrap around a set number. Modular arithmetic happens in a modulus, which is a modular arithmetic system. For example, if we were to count in modulus "5" we would count "0, 1, 2, 3, 4, 0, 1, 2, 3, 4..." and so on and so forth. You can also count backwards at "4, 3, 2, 1, 0, 4, 3, 2, 1, 0, 4..." When a number is put into the schema of a modulus, that number is divided and the remainder, or residue, is what you is left over. These residues makes up congruence classes. In mod 5 they are "0, 1, 2, 3, 4". For modulus "9" it would be "0, 1, 2, 3, 4, 5, 6, 7, 8". Notice how in both cases the value of the modulus is never included. The reason for this is because "5" modulus, or "mod 5", would just be "5" divided by "5" has no remainder or no residue. The same is true for mod "9". "9 mod 9" has no remainder, or no residue. The mathematical way to site this is that $n \equiv a\ (mod\ m), and\ 0 \leq a < m.$ [2]

With that definition we can see when integers in a given modulus are equivalent. For example $7 \equiv 2\ (mod\ 5)$ because when dividing 7 by 5, it has a remainder of 2. This also means that $10 \equiv 5 \equiv 0\ (mod\ 5)$ because 20 can be perfectly divided into 5 with no remainder. This property works with any integer that we can put into Z_5. When we have a negative integer, say -18, we first start by adding positive multiples of the modulus until the number becomes a positive integer. In that problem, we would add 20 to -18 which gives us 2. Therefore $-18 \equiv 2\ (mod\ 5)$. [1] If we had added a larger multiple, for example 25, we would still get the same residue. -18+24=6 and $6 \equiv 1\ (mod\ 5)$. Stated by the Art of Problem Solving, "In general, two integers a and b are congruent modulo n when $a - b$ is a multiple of n. In other words, $a \equiv b \pmod{n}$ when $\dfrac{a-b}{n}$ is an integer. Otherwise, $a \not\equiv b \pmod{n}$, which means that a and b are **not congruent** modulo n. " [3]

Another important property to note is that every element in a modulus has an additive inverse. 0 is its own inverse. The important aspect of having an additive inverse is that when adding a number and its additive inverse in the set of all real numbers, they give us the additive identity. In the solution set of all real numbers, the additive inverse of a number is just the opposite of the number. Negative four is the additive inverse of four, because together they make the additive identity of zero. The reason we can add a number to both sides of an equation is because we are technically adding the additive identity to the whole problem. This is different for equations in Z_5 and Z_6. If we look at the addition table for modulus 6, we find that each element has a number that when added to it will have an additive inverse of 0 in modulus 6. However, because no negative numbers exist in either Z_5 or Z_6, we have to find the number that adds up to the modular base number. In Z_6, the additive inverse of 1 is 5 while 3 has an additive inverse of itself. Below are the tables for addition in Z_5 on the left and Z_6 on the right to illustrate that property.

+	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

+	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

Another important part of solving equations is having a multiplicative identity. The multiplicative identity is one because any number multiplied by one is itself. The truly interesting part when we try and find the multiplicative inverse. The multiplicative inverse of a number is a number that multiplies another number to get the multiplicative identity. This is very easy when dealing with numbers in the set of all real number because we can always multiply a non-zero element in that set by its reciprocal. That is the not the case when dealing with numbers in a particular modulus. Modulus 6's element's do not all have a multiplicative inverse. 5 has a multiplicative inverse of itself as $5 * 5 = 25 \equiv 1 \ (mod\ 6)$, but 2 does not. When we multiply 2 by either 1, 2, 3, 4, or 5 we find that its product will be congruent to either 2, 4 or 0 mod 6.

Looking at different modulo, we find that the same problem arises when we look at modulus 4, 8, 9, 10, and 12. Each of these have at least one element, if not more, that have no multiplicative inverses. This is due to the fact that they are all composite numbers. By being composite, there is always some number, or multiple numbers, that have like factors. Having those like factors leads to the multiples of the number to never have a remainder of 1. In fact, many times these numbers will have some numbers to have another element of the residue that will multiply it to have a product of zero. For example, in mod six, two multiplied by three will have a product of zero mod six. Having that pair of numbers breaks the zero product property. In short, any composite modulo will be what is called a ring because it cannot satisfy the zero product property. A field is simply a ring with some extra properties and holding the zero product property is true is one of them.

If we were to look at prime modulus' such as 3, 5, or 7 we find that each element in the field has a multiplicative inverse. [4] The main reason that this is important is that when students are exposed to the topic for the first time, they need to be able to be exposed to fields that will yield solutions for any values given and to have rings where they cannot. Doing so will hopefully let the students make their own connections that non-prime numbers will be rings and will have some linear or quadratic equations with no solution. However, whether a problem is solved in a ring or a field, solving a quadratic can lead to no solutions. This is due to the fact that not all congruence sets will perfect square. In linear equations, students will find that they will not be able to solve every problem if they are in a ring. If they are solving in a field, they will be able to produce a solution to linear equations every time. [5]

While solving linear equations is a great entry point, solving quadratics yields to even more intriguing questions. One of those is whether or not we can use the quadratic formula. The answer here again is that it depends on the modulo. If the modulo is a field, then the answer is no due to the fact the mod does not satisfy the zero product property. However, even in mod 7, we find that the only perfect squares are 1, 2, and 4. If we try to take the square root of a number other than those three, we cannot. This leads to half the field having no solutions in a quadratic equation. [6]

When looking at both rings and fields, it is important to discuss with the students why they can and cannot work. The discussion will build a deeper understanding of why quadratics work in the first place and help to build stronger foundations of why and how students can solve quadratic equations. Students will be able to make connections between solving linear equations in both fields and rings to solving more complex quadratics. When first introduced, proving the quadratic formula can be used at all is very important. From there students can recognize where the perfect squares exist.

Applications

One of the more interesting applications for modular arithmetic is that of divisibility. Students are taught some of the tricks in 7th grade or earlier without understanding how they work. For example the sum of the digits are divisible by 3, the number must be divisible by 3. Once students are introduced to modular arithmetic, it is not too difficult to prove to them that this works is that $10^k \equiv 1 \pmod 3$where k ∈ $\mathbb{Z}$. Any digit is just that value multiplied by a power of 10 so when the sum of the digits is congruent to 0, the number must be divisible. Students are able to explore the rule for dividing by 11 once they understand modular arithmetic as well.

Modular arithmetic can also be used in matrices, which can lead to encrypted messages. [7] This is very important in today's world where encryption of personal information is key. Cryptology in general is a growing field in computers as programmers want an easier and more efficient way of storing information. According to R. Chaves and L. Sousa "the asymmetrical encryption algorithm RSA that intensively uses modular multiplications with operands up to 2048 bits, and the international data encryption algorithm (IDEA) symmetrical algorithm, which applies the $2^{16} + 1$ modular multiplication." [8]. These programs are increasing modulus size to become more efficient. Binary uses simple modulus 2 or can be converted to process as such. However, programmers are moving into sets of modulus 3 and modulus 4 for more efficient encryption. Encryption can also extend to images. Taking an image and cropping it into very tiny pixels lets computer programmers assign those colors numerical values. From there, they can use a random generator to change the color of each individual pixel so that the image appears as static to anyone without the ability to decrypt the image. [9]

Teaching Strategies

Students must first have the basics of adding and subtracting in Z_5 or Z_6. To start this off, they will play the game of "Sticks". "Sticks" is a game played with two students where each hand has one finger up. Students will have hit the other students' fingers until they get to five fingers up on one hand. When a student gets five fingers on one hand, that hand is out. If a students would have over 5 fingers up, then the number of fingers over five is put up on their hand. For example, if a student had four fingers up on one hand while their opponent has two fingers up, their opponent would only put up one finger because six is one more than five. The first student to knock out both their opponent's hands, wins. [10] This is a great way for students to be introduced to modular arithmetic considering this is a common game some students are familiar with. Therefore, students can easily understand modulus five here making a transition into mod five and six easier.

Students will need to practice rewriting numbers in ring Z_6 and field Z_5. Starting simple, they will build up their understanding of the solutions that are possible in the set and build into converting negative integers into their main congruence set. Addition tables must also be made so that students can easily reference sums of integers until they get familiar with whatever modular set we are using to solve linear and quadratic equations. Having them create addition tables for both sets by themselves will help prepare them to understand how numbers in certain modulo will mirror those of base ten. They can compare the tables to that of a base ten addition table and see how the pairs of the numbers that add up to the modular number will be zero, which is similar to the pairs that in base ten add up to ten. The biggest hurtle that students will struggle with in terms of addition is converting negative numbers into their positive counterpart in the congruence class. By grasping that concept, they can start to solve simple linear equations with variable coefficients of one.

Multiplication tables have to be mastered before students can begin to solve any more complex linear equations. Students will need to make multiplication tables, preferably on their own so that they get practice with multiplying the numbers. By doing both the addition table and the multiplication table on their own, the tables will be more meaningful as well as more memorable. At this point, students will be looking for patterns in the both mod six and mod five. They will be pleased to see that the four in mod five and the five in mod six will act similar to nine in base ten as they are one less than the base. The most interesting aspect here is some students may find that when multiplying in the ring of mod six there will be more products of zero. This is not the case in mod five due to the fact that five is prime. In mod six, similar to base ten, we can get products that are multiples of six which leads to a value of zero in the congruence set. An example of this is the product of three and four equals twelve or zero in mod six. On the next page is the multiplication table for Z_5 and Z_6 to illustrate.

x	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

x	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Extending this into solving linear equations allows students to better understand division. In division, students have to discover that this is done by multiplying by the multiplicative inverse to get the multiplicative identity. For example, if we were to get to the equation 4x=5 in mod six, we are unable to solve the problem due to the fact that there is no number in mod six that multiplies four to have a product of one. In mod six, no numbers have a multiplicative inverse other than one or five. This is a great time to point out to students the reasoning behind this is due to the fact that all other numbers other than one and five share a common factor with six. Doing so can lead to students hypothesizing that any modular base that is not prime will run into the same issue with at least some of the coefficients. Mod five does not run into this problem and students can solve any linear equation in it. [11]

Once students start to solve quadratic equations, it is important for them to remember the entire basis that we solve quadratic equations on. The Zero Product Property makes it so that we can factor and have solutions in the first place. Students need to have the problem worked out for them in mod five because instead of the dividing by a number, we are multiplying by the multiplicative inverse yet again. Doing so is a little more complicated because you have to lead students into having the multiplicative inverse of two being three. When referencing their charts, students will be able to identify why the Zero Product Property does not apply to mod six but the property holds in mod five. This is a great time to introduce the vocabulary of rings versus fields.

Students can now start to solve quadratics. As students go further into solving quadratics, they will find that unlike solving quadratics in the set of all real numbers, there are many cases of which there will be no solution. In modular six, they cannot even solve quadratic equations because the zero product property does not work as seen in the table on the page before. With this is mind, it makes sense to first review why we can solve quadratics and why we can even use the quadratic formula in the first place. Once completing the square is brought up as why we can use the quadratic formula, students must figure out that not all quadratic equations will even have solutions, even in fields. This is mostly because in the field Z_5, when using the quadratic formula, you have to take the square root of a number. However, the only perfect squares that are in mod five are one and four. This can be difficult for students to grasp as they are used to calling a solution simplified if the solution is a radical. However, in modular five or any integer set, you cannot have any irrational numbers because they do not exist and are not a part of any congruence set. Students may connect here that in the solution set of all real numbers, a quadratic can have a no real solutions as well. This simply means that there were a pair of complex solutions instead. As we have only the numbers zero through four as solutions, there is no room for complex solutions in mod five.

The biggest part in all of this is practice. Students need some of the initial problems worked out with them as this will be entirely foreign concept to most. By working out the problems with them, a rich discussion can occur to let the students know the reasons behind what you are doing. Over time, they will discover the patterns that lie beneath the numbers, but that will only come when they have more practice with the material and getting to see the patterns on their own. There are plenty of places to go from here and students should be encouraged to look at other rings and fields.

Teaching Implementation

Day 1

My curriculum unit will last four days, with two of them being half days due to the school schedule. On day one, students start off by being exposed to the addition of integers in Z_5 and Z_6. The lesson will start by dividing numbers by 5 and 6 and to figure out the remainder. This will give them a general way or how we think about a number mod 5 or 6. Doing so also shows them the equivalence that numbers will have in both mods by showing them the congruence class. We know that {…-9, -4, 1, 6, 11, 16…} are all going to be congruent in Z_5.

After students have seen this, they will start by playing a game called “Sticks” which is where students try and get each other’s hands to hold up five fingers making their hand go out. For example, when a student with two fingers taps a student with three fingers, their opponents hand goes out because 5 mod 5 is congruent to 0. However, if a student had two fingers on one hand and tapped their opponent's hand holding up four fingers, the opponent's hand would have one finger held up because 6 mod 5 is 1. Students are also allowed to take the fingers they have on their hands and split them up differently. If a student were to have one finger on one hand, and three fingers on the other, they can spend their turn making their hand either two on each hand or four on one hand and one on another. Once students have had a chance to play this game for a few minutes, they are shown new moves that they can do. Being focused on having their hands go over, leads students forget that they can also go backwards. Using congruence classes, we know that 1 is congruent to 6 in Z_5, we can also take one finger and break it up on our two hands into either three and three or four and two. With this new rule in mind, students are able to go back and play the game again for another two to three minutes to try out the new rule.

Students will recall where they have seen modular arithmetic before which is dealing with the powers of imaginary numbers. Having simplified imaginary numbers before by knowing that i^3 is congruent to i^7 because $i^7=i^4*i^3$ and $i^4=1$. They then have a chance to work out a problem set where they are simply changing numbers into the congruent number in mod 5 or 6. A choice that I had to make when dealing with problems in Z_5 and Z_6 was to go outside of the actual set of numbers that exist in the set. Throughout my lessons I used negatives and numbers larger than the modular base such as 11 in Z_6 or Z_5 and converting that to 5 and 1 respectively. Without going past the numbers in Z_5 and Z_6, students will find the unit too simplistic and will also shut them off from thinking of numbers as their congruence class as well.

Another way for students to think about numbers in Z_5 and Z_6 is by rewriting them as an addition problem. This can help students easily convert a number into its congruent number in the mod. For example, we can convert 11 into 6+5 in Z_6 which becomes 0+5 or just 5. They also practice adding numbers in Z_5 and Z_6. Students will add 8+4 mod 6. Students can either first convert the 8 to 2 and then add 2 and four to make six which is equivalent to 0 mod 6 or they can add them together to make 12 before rewriting 12 as 0 mod 6. Once students have had the chance to see what it means to be a number in the integer set of mod 5, they are exposed to a few more examples of basic addition before they are tasked with creating an addition table for both Z_5 and Z_6. It is important for students to work out these addition tables on their own so that they can work out any patterns that they may see. This also provides more ownership of the understanding of the material.

The last part of day one is having students solve simple linear equations with a variable coefficient of one. For examples students need to able to understand how to solve $x + 4 \equiv 1 \ (mod\ 5)$. Students are first asked to solve it where their given set of solutions can be all real numbers. Students will subtract 4 from both sides and see that the answer would be x= -3. However, when we change this to the solution set of Z_5, they are not allowed to subtract four because negative four does not exist. Instead, they have to add one to both sides because one is the additive inverse of four in Z_5. Students are then asked why we can subtract in the first place and have to make sure we are using the language of additive identity. Our goal in getting rid of a constant is by adding a number to it to make the additive identity. In the solution set of all real numbers the number is always just the opposite of the constant, but in Z_5 and Z_6 we have to add a number to get make the constant go to the mod number. This really brings students back to why we can solve linear equations in the first place and sets them up into tomorrow where they will be looking at the multiplicative inverse.

After students are walked through a few, they are given a set of problems to work on in small group to make sure they understand the process. These problems can be found on panel 15 in Appendix 2. Students then are given a challenge problem. They are tasked with finding what the remainder of the 2000th term of the Fibonacci sequence divided by four. Students first need to convert all the numbers in the Fibonacci sequence into their equivalent mod 4. Once they see the pattern of 0, 1, 1, 2, 3, 1 repeats, they divide the number 2000 by six because the pattern is six numbers long. Finding the remainder is 2, they know that the remainder of the 2000th term of the Fibonacci sequence is 1. Lastly, they are given an exit ticket where they are asked to rewrite numbers in Z_5 in Z_6, and have to solve linear equations with a coefficient of one.

Day 2

With this being a half day, students really get to the heart of solving linear equations with coefficients other than one. Students are first asked to multiply two numbers together and rewrite it in mod 6. Once students are reminded that they must be simplified to the lowest equivalent number in the mod, they make a multiplication table for both Z_5 and Z_6. Once they have made their multiplication tables and checked with their small group and whole class, we look at the patterns to compare and contrast. They find that there is a symmetry when looking at the diagonals of the table in both cases. Also, when two numbers are equidistant from the mod number and are multiplied, they are in the reverse order. For example, looking at the multiplication row of 2 in Mod 5, it goes 2, 4, 1, 3. The multiplication row of 3 in Mod 5 is 3, 1, 4, 2. This same patterns happens whether we look at any row in Z_6 as well.

The main difference between the multiplication tables are that in Z_6 there are four instances where the number is zero. These happen at 2*3, 3*2, 3*4, and 4*3. Students will find that in Z_5 this never happens due to the fact that it is a field. With five being prime, you find that no pair of numbers can multiply together and get zero in Z_5 without the number being a multiple of five. Students see that because six is a composite number, they will have multiple zeros and can relate this to multiplying five and two in base ten. Here students may even hypothesize that any prime number mod will have no way to get zero unless multiplying zeroes and that any composite number will be able to get zeroes by other means. This will be utilized later when they realize that in Z_6 there will be a few linear equations you cannot solve.

Students next do a white board race where they practice their multiplication skills and go past numbers in just Z_5 and Z_6. This can be found on slide 7 of Appendix 3. Going into larger numbers, students could multiply 24562 by 73843 in Z_5 by just looking at the units digit. They only need to multiply by units digit to get six and then simplify that to one mod five. Students find this to be an interesting feature of modular arithmetic and can even extend it into multiplying by negative numbers in Z_5 and Z_6 as well.

Finishing off day two, students start to solve linear equations with coefficients other than one. We start off by solving 3x+4=1 in R where students have to justify why we are solving the way we are. They first subtract 4 because -4 is the additive inverse of 4 in R and then lastly remember that the reason we divide by 3 is that the multiplicative inverse of 3 is 1/3. As a whole class, we then look at solving the equation in Z_5. Students now have to add 1 to both sides because the additive inverse of 4 is 1 in Z_5. This gives us $3x \equiv 2\ (mod\ 5)$. Now instead of dividing by 3, students have to multiply by 2 because 2 is the multiplicative inverse of 3. This leaves us with $x \equiv 4\ (mod\ 5)$. Students try one more because they are given a chance to solve their own in small group. The first two problems are in Z_5 while the third is in $Z_{6.}$ However, with the coefficient being 5, it is one of the two coefficients of x that can be solved in Z_6 because the multiplicative inverse of 5 in Z_6 is 5. The fourth problem, $2x + 3 \equiv 4\ (mod\ 6)$ cannot be solved because there is no multiplicative inverse of 2 in Z_6. From there, students discover that when 2, 3, and 4 are coefficients of x in Z_6, there is no solution. Students finish the day by being given the following exit ticket.

Exit Ticket:

1.) 5x+5=1 (mod 6)

2.) 3x+4=2 (mod 5)

3.) 2x+3=4 (mod 5)

Students are also given a homework on solving linear equations which can be found in Appendix 4. In the worksheet, they solve linear equations in Z_5 and even extend to solving linear equations in Z_7.

Day 3

Starting off the half day, students start by solving $2x + 4 \equiv 1 \ (mod\ 5)$ and $5x + 5 \equiv 3 \ (mod\ 6)$ with solutions of $x \equiv 1 \ (mod\ 5)\ and\ x \equiv 2 \ (mod\ 6)$. Once students have started to master solving linear equations in Z_5 and Z_6, students are introduced to solving quadratic equations. We start by looking at the equation $x^2+2x+2=0$ in the set of all real numbers and imaginary numbers. Students know that they cannot solve this equation by simple factoring and by using the quadratic formula, they find that the equation has no real solutions but 2 imaginary solutions of $-1 \pm i$. Students are then tasked to try and solve this equation in Z_5. They are still not comfortable with trying to figure out what factors could multiply to make 2 and add up to be 2 in Z_5. This means that students need to use the quadratic formula, but they are not yet sure if they quadratic formula works in Z_5 so we have to prove it. Below is the proof for the quadratic formula in Z_5.

$$ax^2+bx+c=0$$

$$x^2+a^{-1}bx+a^{-1}c=0$$

$$x^2+a^{-1}bx=-(a^{-1}c)$$

$$\begin{aligned}
x^2+a^{-1}bx+(a^{-1}b/2)^2 &= -(a^{-1}c)+(a^{-1}b/2)^2 \\
&= -(a^{-1}c)+(a^{-1}b/2)a^{-1}b/2 \\
&= -(a^{-1}c)+(3a^{-1}b)(3a^{-1}b) \\
&= -(a^{-1}c)+4a^{-1}a^{-1}bb \\
&= -(a^{-1}c)a^{-1}a+4a^{-1}a^{-1}bb \\
&= (4b^2-ac)(a^{-2}) \\
&= 4(4b^2-ac)(a^{-2})(4^{-1})
\end{aligned}$$

$$x^2+a^{-1}bx+(a^{-1}b/2)^2= (b^2-4ac)(2a)^{-2}$$

$$x^2+a^{-1}bx+(a^{-1}b/2)^2= (b^2-4ac)(2a)^{-2}$$

$$(x+a^{-1}b/2)^2= (b^2-4ac)(2a)^{-2}$$

$$(x+3a^{-1}b)^2= (b^2-4ac)(2a)^{-2}$$

$$x+3a^{-1}b= \pm \frac{\sqrt{(b^2-4ac)}}{2a}$$

$$x= -3a^{-1}b \pm \frac{\sqrt{(b^2-4ac)}}{2a}$$

$$x = \frac{-b \pm \sqrt{(b^2-4ac)}}{2a}$$

The big differences in this proof compared to the normal proof of the quadratic formula is in line 6 and 7 where we see dividing by 2 is the same as multiplying by 3. In the next line, we multiply the 3's to get 4 mod 5. The second to last line in the proof is also confusing because we go from -3, which is 3 mod 5. We turn multiplying by 3 to dividing by 2 to get quadratic formula.

Students are next asked to look at the multiplication table for Z_6 to see if they would be able to use the quadratic formula. By looking at the table, they will discover that this is not the case because the Zero Product Property does not hold. They may even theorize that this will happen in any ring because every ring is a composite numbers therefore there will always be a pair of numbers that will multiply to get a multiple of the mod number. After we discuss why we cannot solve quadratics in Z_6, students look at solving $2x^2+4x+4=0$ (mod 5). They are shown how to solve it by completing the square so that they see another method. After we solve it by completing the square, we run through using the quadratic formula as well to find that our solutions are 1 and 2. This example can be seen on slide 9 in Appendix. Students then try one more with their table in the form of $2x^2+3x+1=0$ (mod 5) where they can either factor, complete the square, or use the quadratic formula. On slide 10 of Appendix 4, this problem is worked out using the quadratic formula. Doing so will give them solutions of 2 and 4.

Students are given one last problem to try with their table which is $3x^2+x+4=0$ (mod 5). In this problem, students find that they are not able to have a solution. Using the quadratic formula, they find that they end up with a square root of three. However, looking in the multiplication table of Z_5, there is no number that multiplies itself to become three. Students will be perplexed by this because they are used to having solutions that can have a square root of three. The last question students are asked is to figure out when they will have a solution for quadratic problems in Z_5. Looking at their multiplication table, they can find that they are only able to find a solution if they are taking a square root of 1 and 4.

Day 4

In day 4, students are given a warm up to solve quadratics in Z_5 before they are given the chance to practice the skill of solving quadratic equations. Students will have three stations to go through with the final one being an assessment given via Google forms. The first station is having students apply what they have learned about solving quadratics with a worksheet. The answer key is attached to the worksheet so that students can check themselves as they go. This independent practice time also allows me to work with any students who may be struggling with the concept. Students are also given the chance to solve some problems in Z_7 as an extension piece. The worksheet can be found in Appendix 5. The next worksheet is more real life applications where students can figure out what day of the week their birthday. They also work with grouping numbers based on different mods as well as converting days from Earth to days on Venus. This worksheet can be found in Appendix 6. The final assessment of the unit is a google form quiz where students have to solve both linear and quadratic equations in Z_5 as well as a linear equation in Z_6. Students finally have to write a short response on why we are not able to use the quadratic formula in Z_6. My final resource is in Appendix 7.

Appendix 1: Implementing Teaching Standards

NC.M2.A-REI.1: Explain each step in solving a simple equation as following from the equality of numbers asserted at the previous step, starting from the assumption that the original equation has a solution. Construct a viable argument to justify a solution method. *For example, students have to justify why they can solve linear and quadratic equations in Z_5 and Z_6.*

NC.M2.F-IF.8: Write a function defined by an expression in different but equivalent forms to reveal and explain different properties of the function.

For example, students solve quadratic equations by completing the square to solve for the variable.

Appendix 2

Warm up!!!

What is the remainder of 17/5?

What is the remainder of 20/5 ?

What is the remainder of 20/6 ?

What is the remainder of 31/5?

Today we will start off by playing the game of Sticks. Does anyone want to explain the game to the class?

Take 2-3 minutes and play a game with people at your table.

I'm going to show you a new rule with splitting up fingers. I need a volunteer...

With the new rule, try again with your partner implementing this strategy.

What you just did was called modular arithmetic.

By adding fingers after they are tapped, you are taking numbers and putting them into mod 5.

For example, when 3 fingers hits 3 fingers what do you get?

This is because 6/5 has a remainder of 1

Have we used rewriting numbers similar to modular arithmetic before?

Let's rewrite some numbers in Mod 5 and Mod 6. Try and write equivalent numbers for each one given.

$\equiv$ 6 mod 5

$\equiv$ 13 mod 5

$\equiv$ 17 mod 5

$\equiv$ -5 mod 5

$\equiv$ -11 mod 5

$\equiv$ 8 mod 6

$\equiv$ 13 mod 6

$\equiv$ 24 mod 6

$\equiv$ -7 mod 6

$\equiv$ -3 mod 6

$\equiv$ -10 mod 6

How could I rewrite 6 mod 5 into an addition problem?

Rewrite 11 mod 6 into an addition problem

Simplify:

4+5 (mod 6)

8+4 (mod 6)

9 - 11 (mod 6)

By yourself create a modular arithmetic for Mod 5 and Mod 6

+	0	1	2	3	4
0					
1					
2					
3					
4					

+	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

If you were given the equation x+4= 5 how would you solve it? Why would you solve it that way?

If you were given the equation x+4= 3 (mod 5), how would you solve it?

x+4=3 (mod 6)?

So what does it mean to subtract? Why are we able to do this operation in mod 5 and mod 6?

Try some out with your table group! (Reference your addition charts for 5 and 6

x+4 =2 mod 5	x+3 =1 mod 6
x+3= 2 mod 5	x+4= 1 mod 6
x+4=4 mod 5	x+5=4 mod 6
x-4=2 mod 5	x-2=5 mod 6
x-4= 3 mod 5	x-4= 4 mod 6

Challenge problem...

With what you just learned, what would be the remainder of the 2000th term fibonacci sequence divided by 4?

Exit Ticket

1.) Simplify 27 (mod 5)

2.) Rewrite -4 in (mod 5) and (mod 6)

3.) What does it mean to subtract?

4.) Solve for x:

a.) x+4= 2 mod 6 b.) x+3 = 1 mod 5

Appendix 3:

Warm up!!

Solve for x:

x+5= 3 mod 6	x+9=5 mod 6
x-3= 4 mod 5	x+6= -3 mod 5

Let's Multiply!

2*5 mod 6

4*2 mod 5

3*2 mod 6

By yourself, create a table for Multiplication in Mod 5 and Mod 6

X	1	2	3	4
1				
2				
3				
4				

X	1	2	3	4	5
1					
2					
3					
4					
5					

Compare and Contrast the 2 tables. How are they the same? How are they different? How are they similar to the normal multiplication table you are used to?

How could we go about multiplying numbers such as 13 and 9 in mod 5?

White Board Race!

4(5) (mod 6)

3(2) (mod 5)

3*4 (mod 6)

3*4 (mod 5)

11*4 (mod 5)

-2*4 (mod 6)

9(-3) (mod 6)

(4)(2) (mod 5)

24562*73843 (mod 5)

Let's solve a linear equation as we normally do. Justify each step as we go:

$$3x+4=1$$

Let's solve some Linear Equations in Mod 5. How is it different?

$3x+4=1$ (mod 5)

Another one...

$4x+3=4$ (mod 5)

You try!!

1.) $2x+3=4$ (mod 5)

2.) $4x+4=2$ (mod 5)

3.) $5x+2=3$ (mod 6)

4.) $2x+3=4$ (mod 6)

Why does $2x+3=4$ (mod 6) have no solutions? Where else does it have no solutions?

Do linear equations in Mod 5 have no solutions? Why or why not?

Exit Ticket:

1.) $5x+5=1$ (mod 6)

2.) $3x+4=2$ (mod 5)

3.) $2x+3=4$ (mod 5)

Appendix 4: Solving Linear Equations in Z_5 and Z_6

1.) $3x + 4 \equiv 2\ (mod\ 5)$ — $x \equiv 1$

2.) $5x + 4 \equiv 1\ (mod\ 6)$ — $x \equiv 3$

3.) $4x + 3 \equiv 1\ (mod\ 5)$ — $x \equiv 2$

4.) $2x + 5 \equiv 3\ (mod\ 6)$ — No Solutions

5.) $3x + 4 \equiv\ 1\ (mod\ 5)$ — $x \equiv 4$

<u>Try it out!</u>

6.) $5x + 6 \equiv 2\ (mod\ 7)$ — $x \equiv 2$

7.) $4x + 5 \equiv 3\ (mod\ 7)$ — $x \equiv 3$

Appendix 5:

Warm up!!

Solve.

1.) $2x+4=1$ (mod 5)

2.) $5x+5=3$ (mod 6)

What would happen if we were to solve....

$x^2+2x+2=0$

What would happen if we were to solve....

$x^2+2x+2=0$ (mod 5)

Let's prove the Quadratic Formula in Mod 5

$$ax^2+bx+c=0$$

Step 1: $x^2+a^{-1}bx+a^{-1}c=0$

$x^2+a^{-1}bx= -(a^{-1}c)$

What do I do from here? (Complete the Square)

$$\begin{aligned}
x^2+a^{-1}bx +(a^{-1}b/2)^2 &= -(a^{-1}c) +(a^{-1}b/2)^2\\
&= -(a^{-1}c) +(a^{-1}b/2)a^{-1}b/2\\
&= -(a^{-1}c) +(3a^{-1}b)(3a^{-1}b)\\
&= -(a^{-1}c) +4a^{-1}a^{-1}bb\\
&= -(a^{-1}c)a^{-1}a +4a^{-1}a^{-1}bb\\
&= (4b^2-ac)(a^{-2})\\
&= 4(4b^2-ac)(a^{-2})(4^{-1})\\
x^2+a^{-1}bx +(a^{-1}b/2)^2 &= (b^2-4ac)(2a)^{-2}
\end{aligned}$$

So if

$$x^2+a^{-1}bx+(a^{-1}b/2)^2= (b^2-4ac)(2a)^{-2}$$

Then....

$$(x+a^{-1}b/2)^2= (b^2-4ac)(2a)^{-2}$$

$$(x+3a^{-1}b)^2= (b^2-4ac)(2a)^{-2}$$

$$x+3a^{-1}b=\frac{\pm\sqrt{(b^2-4ac)}}{2a}$$

$$x= -3a^{-1}b \pm \frac{\sqrt{(b^2-4ac)}}{2a}$$

$$x = \frac{-b}{2a} \pm \frac{\sqrt{(b^2-4ac)}}{2a}$$

$$x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$$

Therefore we can use the quadratic formula in mod 5! Look at your multiplication tables.

- Why can we not use the quadratic formula in (mod 6)?
- What property does not hold to make it impossible to solve quadratics?

Let's go back to:

$2x^2+4x+4=0$ (mod 5)

Step One: Factor out a 2

$2(x^2+2x)+4=0$ Mod 5

Step Two: Complete the Square

$2(x^2+2x+1 -1)+4=0$ Mod 5

$2(x+1)^2+2=0$ Mod 5

$2(x+1)^2=3$ Mod 5

Change 3 to an 8

How Do we divide 3 by 2 in Mod 5?

$(x+1)^2=4$ Mod 5

$x+1= 2$ or $x+1=3$

$x=1$ or $x=2$

What if it were? Do we know how to?

$2x^2+3x+1=0$ (mod 5)

$$X=\frac{-3\pm\sqrt{3^2-4(2)(1)}}{2(2)}$$

$$X=\frac{2\pm\sqrt{1}}{4}$$

$X=4(2\pm1)$ so $4(2+1)$ or $4(2-1)$

$4(3)$ $\quad 4(2+4)$

12 $\quad 4(6)$

$X=2$ or $x=4$

Let's try one More...

$3x^2+x+4=0$ Mod 5

With your table, try and figure out when can we have solutions in Mod 5.

Appendix 6:

1.) $x^2 + 4 \equiv 0\ (mod\ 5)$

$$x \equiv 4\ or\ x \equiv 1$$

2.) $x^2 + 2x + 3 \equiv 1\ (mod\ 5)$

$$x \equiv 1\ or\ x \equiv 2$$

3.) $2x^2 + 3x \equiv 4\ (mod\ 5)$

$$x \equiv 4\ or\ x \equiv 2$$

4.) $5x^2 + 2x + 4 \equiv 1\ (mod\ 6)$

No solutions

5.) $3x^2 + 4x + 3 \equiv 2\ (mod\ 5)$

$$x \equiv 3\ or\ x \equiv 4$$

6.) $3x^2 + 2x + 4 \equiv 1\ (mod\ 5)$

No solution

<u>Try it out!</u>

7.) $3x^2 + 3x \equiv 6\ (mod\ 7)$

$$x \equiv 1$$

Appendix 7: A leap year occurs every four years. A leap year occurs on any year that is divisible by 4 (ex: 4, 8, 12 ... 1996, 2000, 2004, 2008, 2012)

1. Solve the following: (a) What is 73 (mod 9)? (b) What is 51 (mod 5)? (c) What is -7 (mod 10)?

2. My 25st birthday on October 14th, 2016. On what day of the week was I born? (Don't forget about leap years!)

3. One year on Moon lasts 27 Earth days. Hajarah is 14 years and 85 days old. How many days until her next Moonian birthday? How old will she be turning (in Moonian years)? Omit leap years.

4. It is 8:00 PM. What time is it in a 3 hour world?

5. Aakash is facing East, he rotates 1170◦ counter-clockwise. What direction is he now facing? (Note: A circle has 360 degrees)

6. After a big battle, a general wanted to get an idea of the number of soldiers he had remaining. When they are in squads of 5, there were 2 leftovers. When the general put them in squads of 7, there were 3 leftovers. When he put them in squads of 11, there were 6 leftovers. The general knows that at least 2000 soldiers survived. What is the smallest possible number of soldiers he could have?

7. What is the remainder when $777^{333} + 333^{777}$ is divided by 7?

Appendix 8: Quiz

1.) Solve for x: $3x + 4 \equiv 1 \ (mod\ 5)$ ___________________

2.) Solve for x: $5x + 2 \equiv 2 \ (mod\ 6)$ ___________________

3.) Solve for x: $4x + 5 \equiv 3 \ (mod\ 6)$ ___________________

4.) Find the sum of solutions for the quadratic in Z_5: $2x^2 + 3x + 2 \equiv 0$

a.) No Solution b.) 1 c.) 2 d.) 3 e.)4

5.) Find the sum of the solutions for the quadratic in Z_5: $2x^2 + x \equiv 1$

a.) No Solution b.) 1 c.) 2 d.) 3 e.)4

6.) Why can we not solve quadratic equations in Z_6? ___________________

Resources

List of Materials for Classroom Use

- Pencil and Paper
- Calculator if needed by students
- Access to a computer for final quiz
- Appendix 4, 6, and 7 for worksheets

Resources for Students

- The Art of Problem Solving has a very good site for students to read that helps them understand the properties of modular arithmetic.
- Khan Academy has a great intro to modular arithmetic and its applications with an intro to cryptography.

- Chris Christensen wrote a short article on Introduction to Finite Fields that students could easily grasp.
- For students who need more of a challenge, this article by Dr. Reiter is a terrific read with challenge questions at the end

Resources for Teachers

- The above two articles in the student section are also great teacher reads along with the following article by Keith Conrad. It has some ways you can introduce cryptography to your students as well.
- This paper contains information to extend the lesson into using modular arithmetic with UPC, ISBN, and the USPS Zip Code.
- Dr. Reiter's website for our seminar is a vast expanse of resources to extend both students and

Notes

1. Harold Reiter. "Introduction to Modular Arithmetic, the rings Z_6 and Z_7."

2. Keith Conrad. "Modular Arithmetic."

3. Art of Problem Solving "Modular Arithmetic Introduction"

4. Chris Christensen "Introduction to Finite Fields"

5. Harold Reiter. "Introduction to Modular Arithmetic, the rings Z_6 and Z_7."

6. See Above

7. R. Chaves and L. Sousa "Improving Residue Number System Multiplication with More Balanced Moduli Sets and Enhanced Modular Arithmetic Structures."

8. See Above

9. Shen, Jianbing, and Xiaogang Jin. "A Color Image Encryption Algorithm Based on Magic Cube ..."

10. Sarah Dees "How to Play Sticks"

11. Victor Adamchik. "Modular Arithmetic."

Annotated Bibliography

Adamchik, Victor. "Modular Arithmetic." Cs.cmu.edu/. October 2005. Accessed September 24, 2016. https://www.cs.cmu.edu/~adamchik/21-127/lectures/congruences_print.pdf.
This paper focuses mostly on applications of modular arithmetic and assumes the reader has a basic understanding of modular arithmetic. It includes a crash course of theorems for modular arithmetic that help the reader follow these applications.

Chaves, R., and L. Sousa. "Improving Residue Number System Multiplication with More Balanced Moduli Sets and Enhanced Modular Arithmetic Structures." *IET Comput. Digit Tech* 1, no. 5 (September 2007): 474-80. Accessed September 24, 2016. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.117.8354&rep=rep1&type=pdf
While the article can be dense at times, for a novice such as myself in commuter programming and cryptography, it was a very interesting read. When students ask when you can use this in real life, send them to this article.

Christensen, Chris. "Introduction to Finite Fields." Nku.edu/~christensen/. March 2011. Accessed September 24, 2016. http://www.nku.edu/~christensen/Introduction to finite fields I.pdf.
Great explanation to what it means to be a field while introducing readers to Z_2, Z_3, and Z_5. There is also a brief explanation about additive and multiplicative inverses in Z_5.

Conrad, Keith. "Modular Arithmetic." Math.uconn.edu. July 2015. Accessed September 24, 2016. http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/modarith.pdf.
A more intense look at modular arithmetic while providing a very thorough groundwork for many theorems that are used in modular arithmetic. There are also tons of examples worked out in this paper that help the reader apply what each theorem means.

Dees, Sarah. "How to Play Sticks (A Finger Counting Game for Kids!) - Frugal Fun For Boys." Frugal Fun For Boys. March 07, 2015. Accessed September 24, 2016. http://frugalfun4boys.com/2015/03/07/play-sticks-finger-game-kids/.
Sarah Dees explains the rules to play sticks with visuals that make it easy for the reader. It does not however delve into more complex rules of sticks.

"Modular Arithmetic Introduction." Artofproblemsolving.com. 2016. Accessed September 24, 2016. http://www.artofproblemsolving.com/wiki/index.php/Modular_arithmetic/Introduction
Fantastic introduction piece to both students and educators alike with helpful facts at the end. It shows an easy way to think of modular arithmetic, which is that of time.

Shen, Jianbing, and Xiaogang Jin. "A Color Image Encryption Algorithm Based on Magic Cube ..." Research Gate. November 2005. Accessed November 18, 2016.

https://www.researchgate.net/publication/220763802_A_Color_Image_Encryption_Algorithm_Based_on_Magic_Cube_Transformation_and_Modular_Arithmetic_Operation.
Another great piece of application that shows how images can be encrypted by using modular arithmetic operations.

Reiter, Harold. "Introduction to Modular Arithmetic, the Rings Z6 and Z7." Saylor.org Academy. June 2012. Accessed September 24, 2016. http://www.saylor.org/site/wp-content/uploads/2012/06/MA111_Z6and-Z7so.pdf.
One of the cornerstones that this paper is built around. This paper really digs into how quadratics can be solved in modular arithmetic while also doing a proof of the quadratic formula in Z_7. If you are looking to solve quadratics in any modular set, this is a must read.