Dido Salazar-Torres
12/16/09
Math 728
Lesson Plan

Modulo Arithmetic

Introduction:

Many people grow up with the idea that 1 + 1 = 2. Since math is commonly perceived as having everything right or wrong, people will immediately reject the idea of 1+1 = 0. They misunderstand the meaning of this equation. Most people would never accept the idea that 3*2 = 0. In fact, they should not accept 1+1 = 0 or even 3*2 = 0 if 1, 2, and 3 are actually natural numbers and + and * are the usual addition and multiplication operations on natural numbers. What most people do not realize is their familiarity with "clock arithmetic." They subconsciously accept that 9 + 4 = 1, and 12 + 12 = 12 in 12hr and that 12 + 12 = 0 in 24hr. They also accept 30 + 2 = 1 or 30 + 1 =1, and even 28 + 1 =1 when they think about days in a month. They never take the time to notice that a more general idea is behind all of these "strange" results when adding times together. These ideas are used in computer science, and have other applications. Without an understanding of modulo arithmetic, people won't appreciate the many things that come as a result of it, such as programs, calendars, time, and the many tricks and theorems found in Number Theory.

The modulo arithmetic lesson aims to teach students addition and multiplication modulo n. They will see strange ideas like, "1 + 1 = 0" and "3 * 2 = 0." The lesson will give them a lot of practice with order of operations, associative property of addition and multiplication, commutative property of addition and multiplication, FOIL, and division. The lesson will help them see that it is ok to think about what happens if they change some conditions or ideas. They will see that they can find a totally new and interesting theory or find interesting questions and ideas that are worth exploring. They will also be introduced to the idea of operation tables and a new way to look at addition and multiplication, and they will also see relationships between addition, multiplication and division.

There are many potential difficulties with this lesson plan. In particular, the students may have a difficult time with thinking about things that contradict the memorized "additon facts" and "multiplication facts." Some will need help in accepting the ideas because they may be well beyond their comfort zone. Other difficulties may arise in the solving of the problems. Many of the problems have a step that if it is overlooked, then the students will not see how the remainders add or multiply together, which is important to understanding modulo arithmetic. There are many places where a minor trick is required, but the students may not always think of doing that for solving their problems. The students should get an opportunity to present solutions often if possible and be guided as they present, so that the important ideas are highlighted to the class. Skipping the tricks or the steps indicated in the plan may affect the students' understanding. In many cases, the students may need hints in order to do the tricks or the extra step so they get the answers that are consistent with the remainder of the number when it is divided by the modulus.

This lesson will also help them see that they do not always have to see things the way they were taught to see them; they can actually take what they know or learned and tinker with it and see what it leads to. In many cases, they could run into a new way of understanding something, or they run into something totally new and interesting to them.

The activity should have helped the students realize that modulo arithmetic can help them understand numbers better. They get to see what happens if 1 + 1 = 0, and if 2 * 2 = 0. The students are also shown there is nothing wrong with changing the current assumptions or thinking about something that is absurd at first glance.

In the next session, the students can use this to explore exponentiation modulo n and Fermat's Little Theorem. They can start by making a multiplication table and using it to help them raise a number to a given power. They should do this enough to see the pattern that occurs when a number is raised to a certain power and to see more strange results. After they got the patterns they can be led to investigating the patterns they found and eventually finding Fermat's Little Theorem.

Lesson Plan: Modulo Arithmetic

This lesson teaches addition modulo n for a natural number n. It is aimed toward students with an understanding of integers, division of integers, the concepts of even/odd, FOIL or distributive property, and knowledge of how to read time on an analog clock. The activities will give them a lot of practice with order of operations and using the associative property. The activity is best for high school students who have completed a first year algebra course. It can be used in Math Circle or the classroom.

Introduction

What is an even number? (The students should respond or "a number of the form 2n" or "with "a number divisible by 2," and in that case, they should be helped in noticing "divisible by 2" means that the number is of the form 2n. If they only give examples, then help them find the pattern and conclude that even numbers are of the form 2n.)

What is an odd number? (The students should come up with a response along the lines of: "a number that is of the form 2n-1" or " a number of the form 2n+1" If they have trouble with it or only give examples, then help them find the pattern and conclude that odd numbers are of the form 2n+1. If they respond with a number that is not even, then get them to look for the pattern odd numbers form and conclude they are of the form 2n + 1.)

Now look at the possible remainders when dividing a number by 2. They are 0 and 1. Write 2n and 2n+1 on the board. Put a bar above the 1 as a marker. Now point out that 2n is actually 2n + 0, and put a bar above the 0.

Activity 1:

Hand out the Activity 1 worksheet. Then, help the students understand the instructions in parts A-D, and lead them into discussions about their results.

A. Have four groups or students present their solutions to the problems.

Determine whether the following are even or odd:

a. 16 + 12 even
b. 14 + 5 odd
c. 13+15 even

Now use your results from A to figure out the following:

a. Even+ Even = Even
b. Even+ Odd = Odd
c. Odd + Odd = Even

Do the following arithmetic problems marking the remainders by putting bars above them. For example, If your answer is 2x3, write 2x3 + $\overline{0}$ instead and if your answer is of the form 2x4 + 1, write 2x4 + $\overline{1}$.

a. $6 + 8 = 14 = 2 \times 7 + \overline{0}$
b. $2 + 5 = 7 = 2 \times 3 + \overline{1}$
c. $7 + 4 = 11 = 2 \times 10 + \overline{1}$
d. $13 + 15 = 28 = 2 \times 14 + \overline{0}$

They should proceed with their solutions to D as follows. If they do not have these steps in the presentation, then make them add in the steps, because they are critical in helping the students see what happens when we add the marked remainders.

1. $$\begin{aligned}(2n+\overline{0})+(2n+\overline{0}) &= (2n+2n)+(\overline{0}+\overline{0}) \\ &= 2(2n)+\overline{0}\end{aligned}$$

2. $$\begin{aligned}(2n+\overline{0})+(2n+\overline{1}) &= (2n+2n)+(\overline{0}+\overline{1}) \\ &= 2(2n)+\overline{1}\end{aligned}$$

3. $$\begin{aligned}(2n+\overline{1})+(2n+\overline{0}) &= (2n+2n)+(\overline{1}+\overline{0}) \\ &= 2(2n)+\overline{1}\end{aligned}$$

4.
$$\begin{aligned}(2n+\overline{1})+(2n+\overline{1}) &= (2n+2n)+(\overline{1}+\overline{1})\\ &= 2(2n)+2\\ &= 2(2n+1)+\overline{0}\end{aligned}$$

The students may have difficulty with the last problem. They might get the answer as 4n + 2, and might not have any bars. They need to factor out the 2 and rewrite the answer as $2(2n+1)+\overline{0}$. Explain to them that 2(2n + 1) is in the same form as 2n, and the 1 is not at the end of the solution, so it does not get marked.

E. The next exercise helps the students understand the idea of a number modulo 2. They are to find what the number is modulo 2. Introduce the notation a $\equiv$ b mod n to mean that b is the remainder when a is divided by n. To find b mod n, the students should divide b by n and take the remainder as the answer. In the following problems, they are to find what number mod 2 is congruent to the given number.

1. 24 mod 2 $\equiv$ 0 mod 2

2. 13 mod 2 $\equiv$ 1 mod 2

3. 6 mod 2 $\equiv$ 0 mod 2

4. 29 mod 2 $\equiv$ 1 mod 2

They should find the by division or making a small clock and winding around it b times: The clock looks like this:

For example 3 mod 2 means to wind the hand around 3 times starting at 0

C. Talk about the results.

Notice that math with barred numbers is different. The barred numbers in the parentheses have unusual equalities in the sense of remainders:

1. $\overline{0}+\overline{0}=\overline{0}$

2. $\overline{0}+\overline{1}=\overline{1}$

3. $\overline{1}+\overline{0}=\overline{1}$

4. $\overline{1}+\overline{1}=\overline{0}$

Help the students notice that when we add remainders we either get 0 or 1 and when we add two numbers with a remainder of 1, we get a remainder of 0 again. They should also notice that these results show that the sum of two even numbers is even, the sum of two odd numbers is even, and that the sum of an odd number with an even number is odd, and that the barred numbers are consistent with these facts. They can think of $\overline{0}$ representing an even number and $\overline{1}$ representing an odd number. This allows for the translation:

1. $\overline{0}+\overline{0}=\overline{0}$ means even + even = even
2. $\overline{0}+\overline{1}=\overline{1}$ means even + odd = odd
3. $\overline{1}+\overline{0}=\overline{1}$ means odd + even = odd
4. $\overline{1}+\overline{1}=\overline{0}$ means odd + odd = even

The biggest surprise they might have is that they have an equation where "1 + 1 = 0." This part may disturb some because they might feel that it is wrong and that it is impossible. Extra time may be necessary to revisit the arithmetic done in part A. The fact 1 + 1 = 0 in this case means that 2 ~ 0 in the sense of remainders because if we divide the number by 2, and if its remainder is 2, then we can also divide the remainder by 2 so we don't really have a remainder.

When the found the numbers mod 2 they found the following solutions either by using their clocks or by division:

1. 0 mod 2
2. 1 mod 2
3. 0 mod 2
4. 1 mod 2

The students should start to notice that all multiples of 2 are always 0 mod 2 and if they have a number that is not a multiple of 2, then it will be 1 mod 2.

Activity 2

A. Have a clock and if possible give each group a clock. Given a time, people can add hours to it to get another time. When hours are added to a time on a clock, the small hand passes above the numbers starting at the one it was pointing at, and stops after passing the number of hours added. Give them the following exercises, and tell them that AM and PM are not important here (alternatively, 24-hr time can be done, just multiply the numbers in 1, 2, 3, and 5 by 2):

1. 1:00 + 3 hours
2. 5:00 + 7 hours
3. 7:00 + 8 hours
4. 12:00 + 12 hours
5. 6:00 + 6 hours

Make one column on the board and have the groups write their answers on the board. Leave the next column for the answers to the next set of problems. The students should be encouraged to obtain the answers using the clocks. They should demonstrate how they counted the hand moving around the clock in order to get the answer. They should get the following answers:

1. 1:00 + 3 hours = 4:00
2. 5:00 + 7 hours = 12:00
3. 7:00 + 8 hours = 3:00
4. 12:00 + 12 hours = 12:00
5. 6:00 + 6 hours = 12:00

B. They should do the next set of problems. Using the bar notation from before, putting bars over the remainders:

There might be difficulty with 3, they need to expand 15 as 12 + 3, so they might need a hint telling them to do that. The other possible difficulties may arise in 2 and 5, however it is similar to 4 in Activity 1A, except that now they get that "6 + 6 = 0" and "5 + 7 = 0."

Afterwards, they should write their answers in the next column. Make sure to note that the barred numbers correspond to the times they added in part A. They should present the following steps in their solutions to the class. As in Activity 1A, they should show the steps that bring out the bar addition: (If the students seem more inclined toward putting a bar over the 12 in some of the problems, then if a majority feels the same way, explain that 12 is the same as 0 as remainders and replace 0 with 12 in the final answers. This will shorten the solutions in some problems.)

1. $$\left(12n+\overline{1}\right)+\left(12n+\overline{3}\right)=\left(12n+12n\right)+\left(\overline{1}+\overline{3}\right)$$
$$=12\left(2n\right)+\overline{4}$$

2. $$\left(12n+\overline{5}\right)+\left(12n+\overline{7}\right)=\left(12n+12n\right)+\left(\overline{5}+\overline{7}\right)$$
$$=12\left(2n\right)+\overline{12}$$
$$=12\left(2n+1\right)+\overline{0}$$

point out that we have "$\overline{12}$" here and that it is the same as $\overline{0}$ here because of the step where 12 is factored out of the parentheses.

3. $$\left(12n+\overline{7}\right)+\left(12n+\overline{8}\right)=\left(12n+12n\right)+\left(\overline{7}+\overline{8}\right)$$
$$=\left(12n+12n\right)+15$$
$$=12\left(2n\right)+12+3$$
$$=12\left(2n+1\right)+\overline{3}$$

They need to write 15 as 12 + 3

4. $$\left(12n+\overline{0}\right)+\left(12n+\overline{0}\right)=\left(12n+12n\right)+\left(\overline{0}+\overline{0}\right)$$
$$=12\left(2n\right)+\overline{0}$$

5. $$\left(12n+\overline{6}\right)+\left(12n+\overline{6}\right)=\left(12n+12n\right)+\left(\overline{6}+\overline{6}\right)$$
$$=12\left(2n\right)+12$$
$$=12\left(2n+1\right)+\overline{0}$$

C. Now as a group, compare the answers from A and B. The students should notice that adding the barred remainders is the same as adding the times on a clock, so addition of remainders is the same as addition on a clock. They should realize that the barred numbers correspond to the times they have. They should try to find the correspondence for a few minutes. They should realize that:

$$\overline{0} = 12:00$$
$$\overline{1} = 1:00$$
$$\overline{2} = 2:00$$
$$\overline{3} = 3:00$$
$$\overline{4} = 4:00$$
$$\overline{5} = 5:00$$
$$\overline{6} = 6:00$$
$$\overline{7} = 7:00$$
$$\overline{8} = 8:00$$
$$\overline{9} = 9:00$$
$$\overline{10} = 10:00$$
$$\overline{11} = 11:00$$

This means that in particular, whenever two times on a clock add up to 12, their corresponding barred numbers add up to 0.

D. The group should notice that when the hours added up to 12, they get 0 in the remainder addition column. The group should be led into observing that the arithmetic is working the same way, but the only difference is that 12 plays the role of 0 when adding on a clock. Now it is not that 1 + 1 =0, instead it is the case that 6 + 6 = 0, 5 + 7 = 0, 7 + 8 = 0, and that in fact, when any two summands add to 12, they actually add up to 0 as remainders.

E. The next exercise helps the students understand the idea of a number modulo 12. They are to find what the number is modulo 12. Introduce the notation a = b mod n to mean that b is the remainder when a is divided by n. To find b mod n, the students should divide b by n and take the remainder as the answer. In the following problems, they are to find what number mod 12 is congruent to the given number.

1. 24 mod 12

2. 13 mod 12

3. 6 mod 12

4. 29 mod 12

A great solution for b mod n that students could present is where they find the number by winding around the clock b times and seeing where they stop. Difficulties may arise in problem 3 because 6 is smaller than 12, so in the worst case, they need help in realizing 6 = 12(0) + 6 is a valid solution, or have them do it on the clock. They should find the following solutions either by using their clocks or by division:

5. 0 mod 12

6. 1 mod 12

7. 6 mod 12

8. 5 mod 12

The students should start to notice that all multiples of 12 are always 0 mod 12 and if they have a number that is not a multiple of 12, then it will be a nonzero number in mod 12.

Activity 3

A. Now that the students have learned how to add modulo n and "convert" numbers to modulo n. This activity will teach them to multiply modulo n. Now the students will work with the integers mod 3, so there are only 0, 1, and 2. The first activity is to make an addition table for addition modulo 3.

1. Do the following problems, put answers in the form (3n + 1):

    1. 15 + 6
    2. 4 + 7
    3. 5 + 3
    4. 2 + 7
    5. 4 + 3
    6. 5 + 8

2. Now make a table

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

B. Once they have the addition table modulo 3, they should do the following problem set. This set is similar to previous ones except that multiplication is being done except addition. They should remember that the bar is just marking the remainders in these exercises.

    1. 4 x 7
    2. 3 x 5

3. 8 x 17

4. 4 x 4

Now do the next set:

1. $(3n+\overline{1})\cdot(3n+\overline{2})$

2. $(3n+\overline{0})\cdot(3n+\overline{2})$

3. $(3n+\overline{2})\cdot(3n+\overline{2})$

4. $(3n+\overline{1})\cdot(3n+\overline{1})$

The solutions can be obtained quickly for these problems if the multiplication is only focused on the last parts of the expressions in the (3n + b) set. However, it may not be obvious that the answer will be of the form 3n + b. The problems will also illustrate what happens when remainders are multiplied together. The students might have difficulty with problem 3, and the solution to this problem is a similar trick to the one done in problem 3 in Activity 2B. The solutions should have the following steps:

1. $$\begin{aligned}(3n+\overline{1})\cdot(3n+\overline{2}) &= 3\cdot(3n^2+3n)+\overline{1}\cdot\overline{2}\\ &= 3\cdot(3n^2+3n)+\overline{2}\end{aligned}$$

2. $$\begin{aligned}(3n+\overline{0})\cdot(3n+\overline{2}) &= 3(3n^2+2n)+\overline{0}\cdot\overline{2}\\ &= 3(3n^2+2n)+\overline{0}\end{aligned}$$

3. $$\begin{aligned}(3n+\overline{2})\cdot(3n+\overline{2}) &= 3(3n^2+4n)+\overline{2}\cdot\overline{2}\\ &= 3(3n^2+4n)+4\\ &= 3(3n^2+4n)+3+1\\ &= 3(3n^2+4n+1)+\overline{1}\end{aligned}$$

4. $$\begin{aligned}(3n+\overline{1})\cdot(3n+\overline{1}) &= 3(3n^2+2n)+\overline{1}\cdot\overline{1}\\ &= 3(3n^2+2n)+\overline{1}\end{aligned}$$

The multiplication of the barred numbers leads to the barred number at the end of the result. In particular, the exercise exposes the strange idea that 2 * 2 = 1. The students should be led into noticing that multiplying barred numbers is the same as multiplying them and then finding the number modulo 3. Note that problem 3 shows this process.

C. Now the students should make a multiplication table for multiplication modulo 3.

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

In particular, $2^2 = 1$ in this case, which is another surprise about working modulo n. Note that multiplication by 0 and by 1 still works the same way as it does with ordinary multiplication. The students should compare this table with the one they made in part A. The addition table has each number appear exactly 3 times, while the multiplication table has a zero row and zero column and 1 and 2 appear two times each.

D. The next activity requires the students to do more multiplication modulo n. They should use the observation from before that $\overline{a} \cdot \overline{b} = \overline{ab}$, and division or clocks to get the remainder that corresponds to $\overline{ab}$. The first part of this activity is to construct an addition table for the integers modulo 4.

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Now that they see addition modulo 4, it can be brought to their attention that $2 + 2 = 0$ and that this is the same as doing $2 * 2$, so $2 * 2 = 0$.

E. Now the students should construct a multiplication table for the integers modulo 4.

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

The table should show the students some really peculiar results. For example, $2 * 2 = 0$, $3 * 2 = 2$ but $3 \neq 1$ mod 4, and $3 * 3 = 1$. When compared to the addition table, both tables have a 0 where the 2's are operated on each other, which is consistent with the fact that 2 * 2 = 2 + 2 = 0. Furthermore, each number shows up four times in the addition table, while 0 shows up 8 times in the multiplication table, and 2 shows up 4 times, and 1 and 3 only appear twice in the multiplication table.

Activity 1 Worksheet

A. Determine whether the following are even or odd:

a. 16 + 12

b. 14 + 5

c. 13+15

B. Now use your results from A to figure out the following:

a. Even+ Even

b. Even+ Odd

c. Odd + Odd

C. Do the following arithmetic problems marking the remainders by putting bars above them. For example, If your answer is 2x3, write 2x3 + $\overline{0}$ instead and if your answer is of the form 2x4 + 1, write 2x4 + $\overline{1}$.

a. 6 + 8 =

b. 2 + 5 =

c. 7 + 4 =

d. 13 + 15 =

D. Do the following problems marking the remainders by putting bars above them. For example, If your answer is of the form 2n, write 2n + $\overline{0}$ instead and if your answer is of the form 2n + 1, write 2n + $\overline{1}$.

1. $(2n+\overline{0})+(2n+\overline{0})$

2. $(2n+\overline{0})+(2n+\overline{1})$

3. $(2n+\overline{1})+(2n+\overline{0})$

4. $(2n+\overline{1})+(2n+\overline{1})$

E. a $\equiv$ b mod n means that b is the remainder when a is divided by n. To find b mod n, divide b by n and take the remainder as the answer. In the following problems, find what number mod 2 is congruent to the given number.

1. 24 mod 2

2. 13 mod 2

3. 6 mod 2

4. 29 mod 2

Activity 2 Worksheet

A. Given a time, people can add hours to it to get another time. When hours are added to a time on a clock, the small hand passes above the numbers starting at the one it was pointing at, and stops after passing the number of hours added. Figure out the following times. AM and PM are not important here

6. 1:00 + 3 hours
7. 5:00 + 7 hours
8. 7:00 + 8 hours
9. 12:00 + 12 hours
10. 6:00 + 6 hours

B. Do the following problems. Use the bar notation from before, putting bars over the remainders:

1. $(12n + \overline{1}) + (12n + \overline{3})$
2. $(12n + \overline{5}) + (12n + \overline{7})$
3. $(12n + \overline{7}) + (12n + \overline{8})$
4. $(12n + \overline{0}) + (12n + \overline{0})$
5. $(12n + \overline{6}) + (12n + \overline{6})$

C. Find what the number is modulo 12. In other words, find what number mod 12 is congruent to the given number.

1. 24 mod 12
2. 13 mod 12
3. 6 mod 12
4. 29 mod 12

Activity 3 Worksheet

A. Do the following problems, put answers in the form (3n + 1):

1. 15 + 6
2. 4 + 7
3. 5 + 3
4. 2 + 7
5. 4 + 3
6. 5 + 8
7. Now make a table for addition

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$			
$\overline{1}$			
$\overline{2}$			

B. Do the following problem set putting bars over the remainders.

1. 4 x 7
2. 3 x 5
3. 8 x 17
4. 4 x 4

Now do the next set:

1. $(3n+\overline{1})\cdot(3n+\overline{2})$
2. $(3n+\overline{0})\cdot(3n+\overline{2})$
3. $(3n+\overline{2})\cdot(3n+\overline{2})$
4. $(3n+\overline{1})\cdot(3n+\overline{1})$

D. Now make a multiplication table for multiplication modulo 3.

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$			
$\overline{1}$			
$\overline{2}$			

E. Now make an addition table and multiplication table for addition and multiplication modulo 4.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$				
$\overline{1}$				
$\overline{2}$				
$\overline{3}$				

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$				
$\overline{1}$				
$\overline{2}$				
$\overline{3}$				