1 Modular Arithmetic

Students will explore a type of arithmetic that results from arranging numbers in circles instead of on a number line. Students make and prove conjectures about patterns relating to factors and remainders.

Grade Level/Prerequisites: This activity is suitable for students in grades 3 through 6.

Time: This will fit in one 60 to 90-minute session.

Materials: An outdoor space, sidewalk chalk, a poster chart, markers, handouts, and pencils. Alternatively, number disks (such as a roll of shelf liner rubber) can be used indoors, or dry erase boards or paper can be used to draw the number rings.

Preparation: Prepare handouts and materials, if necessary.

Objectives: Students will gain a deeper understanding of factors and multiples. Modular arithmetic can be related to other topics involving factors and divisibility, or to Nim games.

Navajo Nation Math Circle Connection This was one of the topics explored at the Tsehootsooi Intermediate Learning Center Math Circle during the 2015-2016 academic year. Devon Lynch, one of the students in that group said that this was one of his favorite activities. A year later, he still enjoys "tricking people" by asking them whether there are any other reasonable answers to $2 + 1$ besides 3. He then teaches them modular arithmetic and shows them that when working modulo 3, $2 + 1$ is equivalent to 0.

Modular Arithmetic

We will explore a type of arithmetic that results from arranging numbers in circles instead of on a number line. On some of our circles, $4+5$ is not equal to 9! Modular arithmetic is useful in situations where some quantity cycles. Time on a clock is one example of this. You use modular arithmetic when you try to figure out what time is 5 hours after 9 AM. In computer programming the "mod" operation is used for programs that need to assign values cyclically.

Modular arithmetic is one of the first example systems that undergraduate math majors encounter in abstract algebra. Algebraists study underlying patterns to determine when two systems that look different on the surface really have the same structure. Examples of systems that algebraists study are arithmetic of real numbers, modular arithmetic, arithmetic of string braids, composition of motions, and operations based on symmetries of physical objects.

Emmy Noether was a mathematician who made important contributions to abstract algebra and modern physics. Instead of thinking in terms of long and complicated computations, Emmy looked for simple underlying patterns. This enabled her to create new and more powerful ways of thinking about difficult problems in mathematics and physics.

Moduli and Stepping Numbers

- Make a circle with whole numbers zero up to some number.
- How many numbers are in your circle? (Remember to count the zero.) This number is called the "modulus". The plural of "modulus" is "moduli".
- Choose a stepping number – the number of steps you will take each time.
- Find the space in the chart on the back of this page corresponding to the modulus and the stepping number you chose. Put a big circle in that box so you remember which spot you are working on.
- Start on the zero.
- Start stepping in the direction of the 1 on the circle. Go as many steps as are in your magic stepping number. Call out the final number you land on (but not the numbers in between).
- Keep going until you see a pattern in the numbers you are calling out.
- Did you call out all the numbers? If the answer is "yes" then write that word in the chart where your circle is. If you did not land on all the numbers, then write the word "no".

Modulus

Stepping Number	1	2	3	4	5	6	7	8	9	10
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

Modular Counting

Use a circle with modulus 5 (0 through 4).

(1) Start on the 0. If you take 5 steps, where do you land?

(2) Start on the 0. If you take 6 steps, where do you land?

(3) Start on the 0. If you take 9 steps, where do you land?

(4) Start on the 0. If you take 13 steps, where do you land?

(5) Start on the 0. If you take 15 steps, where will you land?

(6) Start on the 0. If you take 100 steps, where will you land? Why?

(7) Start on the 0. If you take 147 steps, where will you land? Why?

(8) Start on the 0. If you take 284 steps, where will you land? Why?

Now use a circle with a modulus of 7.

(9) Start on the 0. If you take 15 steps, where will you land?

(10) Start on the 0. If you take 482 steps, where will you land? Why?

Suppose you use a circle with modulus m and you take k steps starting from zero. What procedure can you use to figure out where you will land?

Arithmetic on a Number Line

(1) How could you use a number line to find the answer to $6 + 2$?

(2) How could you use a number line to find the answer to $6 - 2$?

(3) How could you use a number line to find the answer to $2 - 6$?

(4) How could you use a number line to find the answer to 6×2?

(5) How could you use a number line to find the answer to $6 \div 2$?

Modular Arithmetic

Addition

Use a circle with modulus 5.

$2 + 2 \equiv_5$ _____

$3 + 4 \equiv_5$ _____

Subtraction

Use a circle with modulus 7.

$6 - 4 \equiv_7$ _____

$3 - 6 \equiv_7$ _____

Multiplication

Use a circle with modulus 10.

$2 \times 4 \equiv_{10}$ _____

$5 \times 3 \equiv_{10}$ _____

Division

Use a circle with modulus 8.

$6 \div 2 \equiv_8$ _____

$5 \div 3 \equiv_8$ _____

Modular division is not as straightforward as the other arithmetic operations. Sometimes there is no answer to a modular division problem. Find an example of a modular division problem with no solution.

Teacher Guide/Solutions

Moduli and Stepping Numbers

Modulus

Stepping Number	1	2	3	4	5	6	7	8	9	10
1	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**
2	**Y**	**N**	**Y**	**N**	**Y**	**N**	**Y**	**N**	**Y**	**N**
3	**Y**	**Y**	**N**	**Y**	**Y**	**N**	**Y**	**Y**	**N**	**Y**
4	**Y**	**N**	**Y**	**N**	**Y**	**N**	**Y**	**N**	**Y**	**N**
5	**Y**	**Y**	**Y**	**Y**	**N**	**Y**	**Y**	**Y**	**Y**	**N**
6	**Y**	**N**	**N**	**N**	**Y**	**N**	**Y**	**N**	**N**	**N**
7	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**N**	**Y**	**Y**	**Y**
8	**Y**	**N**	**Y**	**N**	**Y**	**N**	**Y**	**N**	**Y**	**N**
9	**Y**	**Y**	**N**	**Y**	**Y**	**N**	**Y**	**Y**	**N**	**Y**
10	**Y**	**N**	**Y**	**N**	**N**	**N**	**Y**	**N**	**Y**	**N**

Ask students to formulate and write down some *conjectures* as they work. Conjectures are the mathematical equivalent of a hypothesis. In this case the students' conjectures will be guesses about patterns that they see in the chart, which they think will continue for numbers larger than 10. There are many patterns they may notice. Some of their conjectures will likely be correct, while others may turn out to be incorrect. A conjecture can be turned into a theorem if the student gives a reason why they know for sure that the pattern will continue. The reason needs to be logically complete and convincing to others to be a proof. Some potential conjectures and the overarching theorem for this activity are given below.

At some point, it is important to get students to double check the answers in the chart and to double check each other's conjectures. I usually have a group chart which teams are invited to fill in. I ask some teams to double check results from other teams and put a circle around the answer if they agree.

Refining conjectures sometimes needs to occur during a separate session, depending on how quickly the group is moving. A conjecture should be written where everyone can see it, and students should be encouraged to read the conjecture like a lawyer. They should nitpick holes in the way it is written. Is it written using good grammar and spelling? Is it clear and complete? Can they come up with a counter-example – an example that shows that it is wrong? On the other hand, they may agree with the conjecture as it is written and may think that the writing cannot be improved. I often have pairs of teams exchange conjectures first, then write the surviving conjectures on the board for the whole group to consider together. The next task is to write proofs that are clear, complete and exhibit good grammar.

Here is one example of a conjecture that students might find. "If the stepping number is 2 and the modulus is even, then you will not land on all of the numbers." That is clear and complete. When moving on to the proof, some students might say something like "This is true because 2 is a factor of any even number." That is true, and it even gets to the heart of the matter, but it does not really spell out the connection with stepping on the numbers. Push them to write proofs that really explain what is going on and which refer to the numbers in the circles and the stepping process.

Here are a few of the smaller conjectures/theorems that students might find. The overarching theorem that determines the answer to this question in general is farther down because students usually do not find that one until later.

> Theorem: If the modulus is 1, then you will land on all of the numbers.
>
> Proof: The only number in the circle is a zero, and you start on that number, so clearly we land on all of the numbers in the circle. Also, when you apply a stepping number, you are basically jumping up and down in place and so you will always land on the zero.
>
> Theorem: If the stepping number is 1, then you will land on all of the numbers.
>
> Proof: When you use a stepping number of 1, you start at the 0 and then take one step to the next number, which is 1 (unless the modulus is only 1). As you apply the stepping number, you never

skip any numbers, but instead land on each of them in turn until you return to 0. Thus, you will land on all of the numbers.

Theorem: If the stepping number is 2 and the modulus is even, then you will not land on all of the numbers. On the other hand, if the stepping number is 2 and the modulus is odd, then you will land on all of the numbers.

Proof: When stepping by 2s the first time around, you will land on all of the even numbers and skip the odd numbers, just as you do when counting by 2s with natural numbers on the number line. If the modulus is even, then the number right before the 0 will be an odd number, and so you will not land on it the first time around. Instead, you will land on 0 again and the pattern will start over. Thus, if the modulus is even, you will never land on any of the odd numbers with a stepping number of 2. On the other hand, if the modulus is odd, then the number right before the 0 will be an even number. When continue around the circle by stepping 2 from there, you will skip the 0 and land on the 1. When stepping by 2s the second time around, you will land on all of the odd numbers in turn. Since we land on all of the even numbers the first time around and all of the odd numbers the second time around, we will step on all of the numbers in that case.

Theorem: If the modulus is 2 and the stepping number is even, then you will not land on all of the numbers. On the other hand, if the modulus is 2 and the stepping number is odd, then you will land on all of the numbers.

Proof: When the modulus is 2 there is only a 0 and a 1 in the circle. Every time you step 2, it takes you back to 0. Any even stepping number can be thought of as adding 2 a certain number of times (because any even number e is equal to $2 \times n$ for some whole number n, which can be interpreted as making 2 steps n times). Since each 2-step takes you back to 0 without landing on 1 it is clear that stepping the entire even number also takes you back to 0 without landing on 1. On the other hand, any odd number can be thought of as adding 2 a certain number of times followed by adding 1. After stepping all of the 2s you will be at 0, but adding one more step takes you to 1. Thus, you land on both 0 and 1, and so you do step on all of the numbers.

Theorem: If the modulus is a multiple of the stepping number, and

the stepping number is not 1, then you will not land on all of the numbers.

Proof: If the modulus is a multiple of the stepping number (which is not 1), then on the first time around you will skip all of the numbers which are not multiples of the stepping number and land back at 0 again. This is true because if we applied the stepping number starting at 0 on the number line, we would land on the number representing the modulus (because it is a multiple of the stepping number). If we coil the number line around the circle, the number representing the modulus would land in the same position as the 0. Since we landed back at 0 without landing on all of the numbers, it is not possible to land on all of the numbers in this case.

Students may come up with other conjectures and/or proofs for specific cases.

The big theorem that determines the answer for every modulus and every stepping number is as follows. The proof is a bit involved for students to come up with on their own. However, they will probably have grappled with most of these ideas in proving the simpler cases, and may be able to prove this in general. When I work on this with middle school students, they usually discover this conjecture after making less general conjectures, but we may or may not go through the complete proof depending on their stamina and the amount of time we have.

Modular Arithmetic Stepping Number Theorem: When the modulus and the stepping number are relatively prime, you will land on all of the numbers. Otherwise, you will not land on all of the numbers.

Proof: Suppose that the modulus and the stepping number are not relatively prime. That means that they have some factor f, which is not equal to 1, in common. Because f is a factor of the modulus which is greater than 1, if f was the stepping number, then on the first time around we would land on all of the multiples of f and then back at 0. We would not land on any of the other numbers. Since the stepping number is a multiple of f, we must land on one of the numbers which is a multiple of f or 0 itself (since we make the stepping number by stringing together some number of f-steps). No matter how many times we step by the stepping number, we can never leave the multiples of f, and so we will never land on the other numbers.

Now we need to prove that if the modulus m and the stepping number s are relatively prime, then you will land on all the numbers. One way to think about this is to picture the number line being wrapped around the circle over and over

again. When the number line is wrapped around the number circle of modulus m, we can see that if we take any multiple of m steps, then we land on 0 in the circle.

Claim: the smallest number which is a multiple of both m and s is their product, ms. This is true because of the Fundamental Theorem of Arithmetic, which tells us that each number has a unique prime factorization. This theorem means that each number is built from its prime factors. If m and s have no prime factors in common, then the only way to build a number which can be divided by all of the prime factors in m and by all of the factors in s is to multiply m by s.

Because ms is the smallest number which is a multiple of both m and s, if we start at 0 on the number line and make s steps each time, we will not arrive back at 0 until we have made m jumps, which is the number of numbers in the circle. Now we need to show that we could not have landed at the same number more than once during those m jumps. If we had landed on the same number during those m jumps, then there would be a way to travel a distance equal to a multiple of m by using fewer than m jumps of size s. Since there is no multiple of m and s that is smaller than ms, this is not possible. Thus, we must have landed on all of the numbers.

Modular Counting

Use a circle with modulus 5 (0 through 4).

(1) Start on the 0. If you take 5 steps, where do you land? **0**

(2) Start on the 0. If you take 6 steps, where do you land? **1**

(3) Start on the 0. If you take 9 steps, where do you land? **4**

(4) Start on the 0. If you take 13 steps, where do you land? **3**

(5) Start on the 0. If you take 15 steps, where will you land? **0**

(6) Start on the 0. If you take 100 steps, where will you land? Why? **0. Because 100 is a multiple of 5 and every time we go 5 steps we return to 0.**

(7) Start on the 0. If you take 147 steps, where will you land? Why? **2. After 145 steps we will be back at 0 because 145 is a multiple of 5. Two more steps will take us to 2.**

(8) Start on the 0. If you take 284 steps, where will you land? Why? **4. After 280 steps we will return to 0 because 280 is a multiple of 5. Four more steps will take us to 4.**

Now use a circle with a modulus of 7.

(9) Start on the 0. If you take 15 steps, where will you land? **1**

(10) Start on the 0. If you take 482 steps, where will you land? Why? **6. If we went 490 steps, we would land back at 0 because 490 is a multiple of 7. That is 8 steps too many, so if we go backwards around the circle 7 steps and then one more, we would land at 6. We could also divide 482 by 7 and then find the remainder.**

Suppose you use a circle with modulus m and you take k steps starting from zero. What procedure can you use to figure out where you will land?

You can divide k by m and find the remainder. The remainder tells you which number you will land on. This works because every m steps bring you back to 0, so any multiple of m takes you to 0 also. The remainder tells us the steps that are left over out of k steps after we go a multiple of m steps.

Arithmetic on a Number Line

(1) How could you use a number line to find the answer to $6 + 2$?

You could start at 0, go 6 in the positive direction, and then go 2 more (landing at 8). Alternatively, start on the 6 and then go 2 in the positive direction on the number line.

(2) How could you use a number line to find the answer to $6 - 2$?

You could start at 6 and then go 2 on the number line in the negative direction (landing at 4). Alternatively, you could start at the 2 (the second number) and count the number of steps that you need to walk in the positive direction to reach the 6 (the first number).

(3) How could you use a number line to find the answer to $2 - 6$?

You could start at 2 and then go 6 on the number line in the negative direction to land at -4. Alternatively, you could start at the 6 (the second number) and count the number of steps that you need to walk in the positive direction to reach the 2 (the first number). You actually need to walk backwards and so you need negative four of these steps.

(4) How could you use a number line to find the answer to 6×2? **You could interpret this as starting at the 0 and going 6 two times in the positive direction (to land at 12). Alternatively, you could start at 0 and go 2 six times in the positive direction.**

(5) How could you use a number line to find the answer to $6 \div 2$? **You could interpret this as starting at the 6 and going by jumps of 2 in the negative direction until you land at 0. Since you need to make 3 jumps, this is the answer. Alternatively, you could start at the 0 and make jumps of 2 in the positive direction until you land at the 6, keeping track of the number of jumps needed. You will still make 3 jumps.**

Modular Arithmetic

Adding on a circle is a lot like adding on a number line. You can start at the first number and step off the second number, making sure that you go in the direction the numbers are increasing (except for the jump back to 0).

Notice that $3 + 4 = 7$ on a number line, and that if you make a total of 7 steps on the circle of modulus 5, then you will land on the 2 since the remainder from $7 \div 5$ is 2. This is another way to obtain the answer to $3 + 4 \equiv_5$ which some students may choose to use for the second problem below.

Subtracting on a number line is also like subtracting on a number line. You can start at the first number and walk backwards the number of steps shown in the second number. Alternatively, you can start at the second number and count the number of steps that you need to take in the forwards direction to reach the first number.

Multiplication is just repeated addition, and so the multiplication problems can be interpreted in that way.

Division can be interpreted as repeated subtraction. Starting at the first number, go backwards using a jump size indicated by the second number. Count how many jumps of that size are needed to return to 0. You may need to pass zero several times before ultimately landing on it.

We can also interpret division as the inverse of multiplication. To use this approach, we could start at 0 and make jumps in the positive direction of the size indicated by the second number. Count the number of jumps of this size needed to reach the first number.

Addition

Use a circle with modulus 5.

$2 + 2 \equiv_5$ **4**

$3 + 4 \equiv_5$ **2**

Subtraction

Use a circle with modulus 7.

$6 - 4 \equiv_7$ **2**

$3 - 6 \equiv_7$ **4**

Multiplication

Use a circle with modulus 10.

$2 \times 4 \equiv_{10}$ **8**

$5 \times 3 \equiv_{10}$ **5**

Division

Use a circle with modulus 8.

$6 \div 2 \equiv_8$ **3**

$5 \div 3 \equiv_8$ **7**

Modular division is not as straightforward as the other arithmetic operations. Sometimes there is no answer to a modular division problem. Find an example of a modular division problem with no solution.

A modular division problem will have no solution if it is impossible to reach 0 by repeated subtraction of the second number starting from the first number. If the second number is a factor of the modulus and the first one is not, this will happen. For example, $5 \div 4 \equiv_8$ **has no solution because if you start at 5 and make jumps of 4 in the negative direction, then after one jump you will land at 1 and after two jumps you will land back at 5 again. This pattern will continue forever and it is not possible to land at 0.**