Modular Arithmetic

Math 12, Veritas Prep.

We're interested in the algebraic properties of mathematical structures—the formal, symbolic, structural properties of those systems. So far, we have at least three examples of mathematical structures—arithmetic, logic, and set theory. But there's another useful structure we should talk about—the **integers mod n**.

The idea is this: what if you want to count and add and multiply, but rather than having an infinite number of numbers, you have a finite number of numbers? Suppose, for instance, you only know how to use numbers that you can represent with your fingers. You start counting "one, two, three..." and when you hit "ten," you run out of numbers, so you just repeat: "nine, ten, one, two, three..." Your world is repetitive, rather then continuous. You walk in circles rather than straight lines.

Here's another example: with clocks, we only have twelve (or sometimes 24) numbers to count with. If it's 8 o'clock right now, the time in seven hours won't be "15 o'clock"—it'll be 3 o'clock. The hours start over as soon as we reach 12. The fancy name for this is that when we're counting times, we counting **modulo 12**, or **mod 12** for short. In mod 12 arithmetic, 15 is the same as 3. Or, put differently, 15 is equal to 3 (mod 12). (Or sometimes the word "congruent" is used: 15 is **congruent mod 12** to 3.)

Yet another example. Normally when we count, we do something like this:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \cdots$$

But what if we don't have all $\aleph_0$ of $\mathbb{N}$ to count with? What if, say, we only have three numbers? Then we'd have to count like this:

$$0, 1, 2, 0, 1, 2, 0, 1, 2, 0, 1, 2, 0, 1, 2 \cdots$$

What if we are adding, rather than just counting? If we have ordinary addition with the natural numbers, we can summarize the results in a table, like below. (We usually denote this as $(\mathbb{N}, +)$.) It's an infinitely-large table, since there are infinitely-many natural numbers. This is not exciting, but it may dredge up buried memories from elementary school:

$\mathbb{N}, +$	0	1	2	3	$\cdots$
0	0	1	2	3	$\cdots$
1	1	2	3	4	$\cdots$
2	2	3	4	5	$\cdots$
3	3	4	5	6	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

But what if we want to add, and we only have three numbers (i.e., we can only count "$0, 1, 2$")? What if, for example, we want to add $2 + 1$? Usually $2 + 1 = 3$, but there's no 3 in our new system of numbers. Instead of 3, we have a 0 again.

$$\begin{array}{rccccccc} \mathbb{N}: & 0 & 1 & 2 & 3 & 4 & 5 & 6\cdots \\ \mathbb{Z}_3: & 0 & 1 & 2 & 0 & 1 & 2 & 0\cdots \end{array}$$

Note that here I'm denoting this "world of only three numbers" as $\mathbb{Z}_3$. Why I'm using that as notation, and not, say, $\mathbb{N}_3$, will become clear later. Anyway, we want to know what $2 + 1$ is in $\mathbb{Z}_3$, and since in $\mathbb{Z}_3$ 3 is the same as 0 in $\mathbb{N}$, we must have that in this world, $2 + 1 = 0$.

The usual name for this stuff is **modular arithmetic**; in this case, **arithmetic mod three** or **addition mod three**. Sometimes, to be clear that we're not talking about "normal" arithmetic, we might put in a little subscript next to our + sign:

$$2 +_3 1 = 0$$

We could summarize our results about how to add these numbers:

$\mathbb{Z}_3, +_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Compare and contrast this to our addition table for ($\mathbb{N}$,+).

Problems

1. What is 12 mod 3? That is, if you're counting with only three numbers (in $\mathbb{Z}_3$), what is the number 12 the same as?

2. What about 13 mod 3? 11 mod 3? 15 mod 3? 900 mod 3? 901 mod 3?

3. Do the following arithmetic problems in mod 3:

(a) $1 +_3 0$
(b) $2 +_3 2$
(c) $0 +_3 0$
(d) $1 +_3 1$
(e) $4 +_3 0$
(f) $5 +_3 1$
(g) $5 +_3 4$
(h) $300 +_3 604$

4. Mod 3 gets kind of boring. Write out what counting in, say, mod 5 looks like. Then write out the addition table for addition mod five.

5. And then do the following arithmetic problems in mod 5:

(a) $1 +_5 0$
(b) $2 +_5 2$
(c) $0 +_5 0$
(d) $1 +_5 1$
(e) $4 +_5 0$
(f) $5 +_5 1$
(g) $5 +_5 4$
(h) $300 +_5 604$

6. Likewise, write out the addition table for addition mod seven, and then do the following arithmetic problems in mod 7:

(a) $1 +_7 0$
(b) $2 +_7 2$
(c) $0 +_7 0$
(d) $5 +_7 6$
(e) $4 +_7 10$
(f) $3 +_7 9$
(g) $5 +_7 4$
(h) $300 +_7 604$

7. Addition gets kind of boring. Write out the multiplication table for mod 3.

8. And then do these multiplication problems in mod 3:

(a) $1 \bullet_3 0$
(b) $2 \bullet_3 2$
(c) $0 \bullet_3 0$
(d) $1 \bullet_3 1$
(e) $4 \bullet_3 0$
(f) $5 \bullet_3 1$
(g) $5 \bullet_3 4$
(h) $300 \bullet_3 604$

9. Write out the multiplication table for $\mathbb{Z}_7$, too (i.e., the integers mod 7).

10. Write out the multiplication table for $\mathbb{Z}_6$.

11. Write out the multiplication table for $\mathbb{Z}_8$.

12. Here's a question: if we're adding natural numbers, we can add zero to any natural number, and just get the original natural number. Same thing with integers—we can add zero to any integer, and get the original integer. (Remember that integers include the negatives.) So the fancy name for zero then is that it's the **additive identity**, or the **identity element** with respect to addition.

But integers have an additional arithmetical property that the naturals don't—namely, if I have any integer, there's some other integer such that when I add it to the first integer, I get zero. For all $x \in \mathbb{Z}$, $\exists y \in \mathbb{Z}$ such that $x + y = 0$. I.e., integers have negatives. Every element of the integers has an **inverse** (or an **additive inverse**), i.e., some element that when I add an element and its inverse together, I get the identity element (zero).

The natural numbers don't have this property. I can't add two natural numbers together and get zero (unless, maybe, I define $\mathbb{N}$ to include zero and I have $0 + 0$. But in general, I can't.)

But what if you have $\mathbb{Z}_3$? Can you add two (non-zero) elements of $\mathbb{Z}_3$ together and get 0? Is there, for example, an inverse of 1 in $\mathbb{Z}_3$? It can't be -1, because there's no -1 in $\mathbb{Z}_3$. But is there some element of $\mathbb{Z}_3$ that, when added to 1, begets 0? What is it?

Likewise, does 2 have an inverse? What about 0?

13. Now consider $(\mathbb{Z}_5, +)$. $\mathbb{Z}_5$ has five elements: $0, 1, 2, 3$, and 4. What are the additive inverses of each of these elements?

14. Likewise, write out each element of $\mathbb{Z}_7$ and its corresponding additive inverse.

15. These interrelated ideas of "identities" and "inverses" come up when we talk about multiplication, too. We can multiply any number by 1, and just get the same number back. So 1 is the **multiplicative identity**. And, if I have fractions (i.e., if we are working with rational numbers), we can multiply any number by its reciprocal to get back to 1. For example, $5 \cdot \frac{1}{5} = 1$. So $\frac{1}{5}$ is the **multiplicative inverse** of 5. (And vice-versa: 5 is the multiplicative inverse of 1/5.)

But if we're not working with the rational numbers, we lose that. If we are discussing multiplication of natural numbers (i.e., $(\mathbb{N}, \cdot)$), we don't have inverses. There's no natural number than I can multiply, say, 5 by, and get back to 1. In fact (other than 1 and itself), there's no natural number that I can multiply some other natural number by and get 1. If we're talking about multiplication with natural numbers, we don't have inverses! Maybe this makes sense—after all, we've already seen that the natural numbers don't have additive inverses.

But we've also seen that the $\mathbb{Z}_n$, i.e., the integers mod n, *do* have additive inverses. (Which is so weird—like, we have *fewer* elements, and we get *more* structure.) So if we start talking about multiplication rather than addition, the natural question to ask is: does $\mathbb{Z}_n$ have multiplicative inverses? do the integers mod n, together with the operation of multiplication, have inverses? always? never? sometimes? when?

To investigate this question, take a look at your multiplication table for $\mathbb{Z}_3$. Do the elements $0, 1, 2$ have inverses? what are they?

Now take a look at the multiplication tables for $\mathbb{Z}_7$, $\mathbb{Z}_6$, and $\mathbb{Z}_8$. Does each element in each of these systems have a multiplicative inverse?

$\mathbb{N}, +$	0	1	2	3	4	5 $\cdots$
0	0	1	2	3	$\cdots$	
1	1	2	3	4	$\cdots$	
2	2	3	4	5	$\cdots$	
3	3	4	5	6	$\cdots$	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	

equality mod n (or, more often, **congruence mod** *n*) is an equivalence relationship.

$\mathbb{Z}_4, +$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2