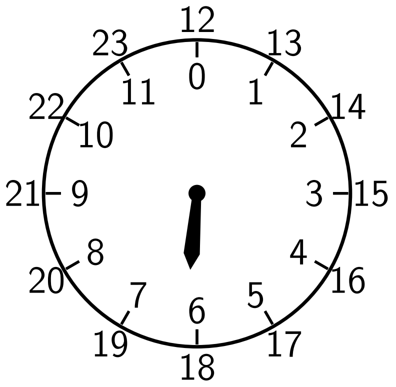
Modular Arithmetic

We've studied examples of objects that you can "add": the symmetry groups of planar shapes. These groups satisfy all axioms of addition except possibly commutativity. Yet, we would still be hard-pressed to call the objects in these groups "numbers" or "number-like" since we can't add *and* multiply them together. So, we turn our attention to sets that have addition and multiplication that follow the algebraic axioms of the real line. These sets are called *fields*. The most important examples of a field for our goal to mathematically model *SET* are the modular arithmetic fields.

Reviewing arithmetic modulo 12

We have previously worked through a modular arithmetic handout in which we focused much of our efforts on constructing the modular numbers from the integers. In this handout, we simply review how to do computations with these numbers. Recall that we can turn a circle into a number line by dividing it into twelve equal parts, just like a clock.



This new circular number line leads to modular arithmetic, namely *arithmetic modulo 12*. The hour hand moves from 0 to 1, from 1 to 2, ... , and from 11 to 12 just as it would have on the straight number line. However, we consider 12 to equal 0 on this circle, so there the hour hand goes again, from 1 to 2, and so on. We say that 12 is *congruent to 0 modulo 12*, 13 is *congruent to 1 modulo 12*, 14 is *congruent to 1 modulo 12*, and so on. We write down these observations as

$$(12 \mod 12) = 0, \quad (13 \mod 12) = 1, \quad (14 \mod 12) = 2, \ \dots$$

Overall, we recall the following definition and algebraic properties.

Definition 1. *For any integer x, we let $(x \mod 12)$ equal the unique integer in $0, 1, 2, \ldots, 11$ that is congruent to x modulo 12. In other words, if you divide x by 12, then we define $(x \mod 12)$ to be the integer remainder. So, "$\mod 12$" is the way mathematicians write "`% 12`" when doing math computations instead of programming.*

Proposition 1. *It holds true for any two integers x, y that*

$$(x + y \mod 12) = \big((x \mod 12) + (y \mod 12) \mod 12\big)$$

and that

$$(x \cdot y \mod 12) = \big((x \mod 12) \cdot (y \mod 12) \mod 12\big) .$$

Problem 1. *Answer the following computations.*

$(1155 \mod 12) =$ _________

$(-1152 \mod 12) =$ ________

$(-1 + 20 \mod 12) =$ _______

$(-10 \cdot 10 \mod 12) =$ _______

$(31 + 47 \mod 12) =$ ________

$(7 \cdot 119 \mod 12) =$ _________

$(-1 \mod 12) + (20 \mod 12) =$ ________

$(-10 \mod 12) \cdot (10 \mod 12) =$ ________

$\big((31 \mod 12) + (47 \mod 12) \mod 12\big) =$ _________

$\big((7 \mod 12) \cdot (119 \mod 12) \mod 12\big) =$ __________

Altogether, we can define arithmetic modulo 12 to be its own number system!

Definition 2. *Let* $\mathbb{Z}_{12}$ *be the set of numbers* $0, 1, \ldots, 11$. *We define addition* $+_{12}$ *on* $\mathbb{Z}_{12}$ *as* $x +_{12} y = (x + y \mod 12)$ *for integers* $x, y \in \mathbb{Z}_{12}$. *We can similarly define multiplication* $\cdot_{12}$ *on* $\mathbb{Z}_{12}$ *as* $x \cdot_{12} y = (x \cdot y \mod 12)$ *for integers* $x, y \in \mathbb{Z}_{12}$.

$\mathbb{Z}_{12}$ is one of our new number systems! Moreover, we know from the prior modular arithmetic packet that $\mathbb{Z}_{12}$ with $+_{12}$ and $\cdot_{12}$ actually satisfies all twelve of the algebraic axioms from the real line except for one! Answer the following problems to jog your memory.

Problem 2. *Why is* $\mathbb{Z}_{12}$ *closed under* $+_{12}$*? Why is* $\mathbb{Z}_{12}$ *closed under* $\cdot_{12}$*?*

Problem 3. *What is the additive identity of* $\mathbb{Z}_{12}$ *under* $+_{12}$*? What is the multiplicative identity of* $\mathbb{Z}_{12}$ *under* $\cdot_{12}$*?*

Problem 4. *What are the additive inverses of* $0, 2, 5, 9$ *in* $\mathbb{Z}_{12}$ *under* $+_{12}$*?*

Problem 5. *Which of the twelve algebraic axioms does* $\mathbb{Z}_{12}$ *with* $+_{12}$ *and* $\cdot_{12}$ *not satisfy? Can you explain why by giving a counterexample to this axiom? Remember there are five axioms for addition, five analogous axioms for multiplication, and two axioms for distributivity.*

General Modular Arithmetic

So far, we've worked with the familiar case of clock face arithmetic, meaning arithmetic modulo 12. This begs the question, what is special about 12? Well, nothing! We can define a new number system for any integer $n \geq 2$.

Definition 3. *Fix an integer $n \geq 2$, which we call the modulus. For any integer x, we let $(x \mod n)$ equal the unique integer in $0, 1, 2, \ldots, n-1$ that is congruent to x modulo n. In other words, if you divide x by n, then we define $(x \mod n)$ to be the integer remainder.*

Proposition 2. *It holds true for any two integers x, y that*

$$(x + y \mod n) = \big((x \mod n) + (y \mod n) \mod n\big)$$

and that

$$(x \cdot y \mod n) = \big((x \mod n) \cdot (y \mod n) \mod n\big) .$$

Definition 4. *For modulus $n \geq 2$, let $\mathbb{Z}_n$ be the set of numbers $0, 1, \ldots, n-1$. We define addition $+_n$ on $\mathbb{Z}_n$ as $x +_n y = (x + y \mod n)$ for integers $x, y \in \mathbb{Z}_n$. We can similarly define multiplication $\cdot_n$ on $\mathbb{Z}_n$ as $x \cdot_n y = (x \cdot y \mod n)$ for integers $x, y \in \mathbb{Z}_n$.*

Problem 6. *Fill out the following tables for addition and multiplication in $\mathbb{Z}_2$. For each cell, you compute the row label plus or times the column label.*

$+_2$	0	1
0		
1		

$\cdot_2$	0	1
0		
1		

Problem 7. *What are the additive and multiplicative identities of $\mathbb{Z}_2$? If they exist, what are the additive and multiplicative inverses of 1 in $\mathbb{Z}_2$?*

Problem 8. *Fill out the following tables for addition and multiplication in $\mathbb{Z}_3$. For each cell, you compute the row label plus or times the column label.*

$+_3$	0	1	2
0			
1			
2			

$\cdot_3$	0	1	2
0			
1			
2			

Problem 9. *What are the additive and multiplicative identities of $\mathbb{Z}_3$? If they exist, what are the additive and multiplicative inverses of 2 in $\mathbb{Z}_3$?*

Problem 10. *Fill out the following tables for addition and multiplication in $\mathbb{Z}_4$. For each cell, you compute the row label plus or times the column label.*

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

$\cdot_4$	0	1	2	3
0				
1				
2				
3				

Problem 11. *What are the additive and multiplicative identities of $\mathbb{Z}_4$? If they exist, what are the additive and multiplicative inverses of 2 and 3 in $\mathbb{Z}_4$?*

Problem 12. *Fill out the following tables for addition and multiplication in $\mathbb{Z}_5$. For each cell, you compute the row label plus or times the column label.*

$+_5$	0	1	2	3	4
0					
1					
2					
3					
4					

$\cdot_5$	0	1	2	3	4
0					
1					
2					
3					
4					

Problem 13. *What are the additive and multiplicative identities of $\mathbb{Z}_5$? If they exist, what are the additive and multiplicative inverses of 2 and 3 in $\mathbb{Z}_5$?*

Problem 14. *Fill out the following tables for addition and multiplication in $\mathbb{Z}_6$. For each cell, you compute the row label plus or times the column label.*

$+_5$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

$\cdot_5$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

Problem 15. *What are the additive and multiplicative identities of* $\mathbb{Z}_6$*? If they exist, what are the additive and multiplicative inverses of 2 and 3 in* $\mathbb{Z}_6$*?*

Problem 16. *Let* $n \geq 2$ *be an integer. What are the additive and multiplicative identities of* $\mathbb{Z}_n$*?*

Problem 17. *Let* $n \geq 2$ *be an integer. Does every non-zero number in* $\mathbb{Z}_n$ *have to have a multiplicative inverse?*

Problem 18. *Are there some values of* $n \geq 2$ *such that* $\mathbb{Z}_n$ *with* $+_n$ *and* $\cdot_n$ *satisfies all twelve algebraic axioms? Which such values of* n *can you name off the top of your head?*

Problem 19. *Do you notice any patterns in the values of* $n \geq 2$ *for which* $\mathbb{Z}_n$ *with* $+_n$ *and* $\cdot_n$ *satisfies all twelve algebraic axioms?*