

Modular Arithmetic, Continued

- Comprehension Question:

- Closes at 9am on day of class
 - Press "check", then "Finish attempt", then "Submit all and finish"
 - Any attempt gets full credit
 - Do/re-do today's if you need to!
-

- Video: Given any two elements of the set $\{0, 1, 2, 3\}$,

we can add them mod 4 to get a new element of that set.

E.g.

$$1+2 \equiv 3 \pmod{4}$$

$$2+3 \equiv 5 \equiv 1 \pmod{4}$$

↑
"modulo 4"

Worksheet 2: Modular Arithmetic, continued

Math 335


Get to know each other: Go around the group, and have each member introduce themselves with their name and answer the following question:

- What's one skill (a real-life skill or superpower) that you wish you had?

1. Fill in the following table for addition modulo 4, using **only** the numbers 0, 1, 2, and 3. For example, I've filled in one entry to show that $3 + 1 \equiv 0 \pmod{4}$.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

2. What features do you notice in the table from Problem 1? Do you think these features would still hold in an addition table modulo some number other than 4?

- Commutative ($a+b=b+a$)
(Graphically, table is symmetric across )
- Associative ($(a+b)+c=a+(b+c)$)
(Not obvious from table!)
- Every entry appears exactly one in each row & column
(Means $a+x \equiv b \pmod{4}$ can always be solved for x)

3. Now try making a table for **multiplication** modulo 4, again using only the numbers 0, 1, 2, and 3. For example, I've filled in one entry to show that $3 \cdot 2 \equiv 2 \pmod{4}$.

\times	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

4. What features do you notice in the table from Problem 3? In what ways is it similar to the addition table from Problem 1, and in what ways is it different?

- Still commutative
- Still associative
- Not true that each number appears exactly once in each row & column!

Vague thought question: Some people talk describe modular arithmetic as “arithmetic on a clock.” Does this analogy make sense to you? Discuss it as a group.

Some Notation

$$\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$$

Coming attractions: The fact that you can add two elements of \mathbb{Z}_n to get a new element of \mathbb{Z}_n (& some properties are satisfied....) makes it an example of a "group."