

NOTATION FOR OUR SMALL, SIMPLE NUMBER SYSTEMS

We looked at a small, simple number system with five elements, which we denoted 0, 1, 2, 3, and 4. The addition and multiplication tables were

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Of course, here 0, 1, 2, 3, and 4 are definitely *not* the usual integers. But there was a reasoning behind these tables: we did the usual addition and multiplication, then “reduced” the answer modulo 5.

What we would like to do is treat things here in a manner similar to the integers and polynomials. In order to do that with less confusion, we need to be clear exactly what we’re dealing with.

Suppose we have a given modulus m . We lump all the integers with the same remainder together and call this subset of integers a *congruence class modulo m* . Since there are m possible remainders when you divide by m using the division algorithm, there are m congruence classes modulo m .

Examples: If we use modulus 4, there are 4 congruence classes:

$$\begin{aligned} \dots - 12, -8, -4, 0, 4, 8, 12, \dots & \quad (\text{remainder } 0) \\ \dots - 11, -7, -3, 1, 5, 9, 13, \dots & \quad (\text{remainder } 1) \\ \dots - 10, -6, -2, 2, 6, 10, 14, \dots & \quad (\text{remainder } 2) \\ \dots - 9, -5, -1, 3, 7, 11, 15, \dots & \quad (\text{remainder } 3) \end{aligned}$$

We denote congruence classes with an integer in the congruence class surrounded by brackets, $[]$, and (unless the modulus is clear from the context) the modulus as a subscript. For example,

$$\begin{aligned} \dots - 12, -8, -4, 0, 4, 8, 12, \dots & = [12]_4, \\ \dots - 11, -7, -3, 1, 5, 9, 13, \dots & = [-7]_4 \end{aligned}$$

Note that the integer inside the brackets is *not unique!* In other words, $[a]_n$ and $[b]_n$ can be different representations of the exact same congruence class even when $a \neq b$. For example, $[0]_4 = [16]_4 = [-28]_4$ since 0, 16 and -28 all have the same remainder when divided by 4. This isn't a new new thing for you; think of the different fractions that all equal one half, or different decimal representations of the same real number.

Definition: Suppose m is a positive integer. Then the *integers modulo m* , written $\mathbb{Z}/m\mathbb{Z}$ or \mathbb{Z}_m , is the number system consisting of the different congruence classes $[0]_m, \dots, [m-1]_m$. These are added and multiplied as follows. Given $[a]_m, [b]_m \in \mathbb{Z}_m$, we define $[a]_m + [b]_m = [a + b]_m$ and $[a]_m \cdot [b]_m = [a \cdot b]_m$.

Example: Let's write out addition and multiplication tables for \mathbb{Z}_7 .

We saw how \mathbb{Z}_5 and \mathbb{Z}_2 (the two such number systems we looked at before) satisfied the usual addition and multiplication axioms. We can see via our tables that \mathbb{Z}_7 does, too. We'd like to show the same is true in general for any \mathbb{Z}_m . But first, does our addition and multiplication even make good sense? After all, our definition of addition and multiplication seems to use the particular representatives of the congruence class. Hmmm.....