Congruences as a number system: Zn

Reading

- Section 8.1, 8.2

Practice Problems

8.2 ~

Challenge 8.2 (Optional)

Notes

We saw that if we consider the congruence classes modulo n, there are exactly n of them, represented by the remainders when dividing by n. We will denote them thusly:

$$\mathbb{Z}_n = \bar{0}, \bar{1}, \ldots, \overline{n-1}$$

This idea takes some getting used to: Each of these "barred numbers" represents a whole set of numbers, namely all elements in that congruence class. Yet we want to think of that entire set as "one number".

The interesting thing is that we can now define arithmetic operations on this set:

> We define the "sum" and "product" of two congruence classes, as the congruence class of the sum/product of representatives of those classes. In other words:
>
> $$\bar{a} + \bar{b} = \overline{a+b}$$
> $$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

We must show that this is actually *well-defined*: What if we choose a different a to present the class $\bar{a}$? Could that possibly change the result?

The fact that these operations are well-defined follows from our previous result for how congruences behave under addition and multiplication. Recall:

> If $a \equiv c \bmod n$ and $b \equiv d \bmod n$, then $a + b \equiv c + d \bmod n$ and $a \cdot b \equiv c \cdot d \bmod n$.

This says exactly what we need: Congruent input values give us congruent results. So changing the representative does not change the congruence class of the result.

As a quick example, suppose we work modulo 5. Then $\bar{2} + \bar{4} = \bar{6} = \bar{1}$. If we choose different representatives, we would get the same result: $\bar{7} + \bar{4} = \bar{1}1 = \bar{1}$.

This is an important general idea to keep in mind, when we want to define operations like this:

1. We want to define something that should make sense as an operation on an entire set (like a congruence class in this example).
2. To do that, we pick an arbitrary representative from the set, and use that specific element to define the operation.
3. We then show that the result does not depend on the choice of representative.
4. We then can say that the operation is *well-defined*.

We will denote this system of congruence classes modulo n with $\mathbb{Z}_n$, and call it a **finite number system**. There is one such system for every n.

These finite number systems retain many of the familiar properties. Consider each of the following questions.

1. Is addition commutative?
2. Is addition associative?
3. Is there an identity for addition? (similar to the "zero")
4. Does every element have an additive inverse?
5. Is multiplication commutative?
6. Is multiplication associative?
7. Is there an identity for multiplication? (similar to the "one")
8. Does multiplication distribute over addition?
9. Does every element have a multiplicative inverse?
10. Can I cancel out the same number if present on both sides of an equation?

Properties 1-8 together are the definition of what we would call a **ring**. So we can say that $\mathbb{Z}_n$ has a ring structure.