NUMBER THEORY
FALL 2023

ASSIGNMENT 5.1
DUE SEPTEMBER 27

Fix a modulus $n \in \mathbb{N}$. Recall that for $a \in \mathbb{Z}$ the congruence class of $a \pmod{n}$ is

$$a + n\mathbb{Z} = \{a + kn \mid k \in \mathbb{Z}\},$$

which is simply the equivalence class of a under congruence mod n. By definition we have

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad a + n\mathbb{Z} = b + n\mathbb{Z}.$$

Because every congruence class contains exactly one of the integers $0, 1, 2, \ldots, n-1$, the set of all equivalence classes (quotient space) is

$$\mathbb{Z}/n\mathbb{Z} := \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + a\mathbb{Z}\}.$$

In the following exercises you will prove that $\mathbb{Z}/n\mathbb{Z}$ has the algebraic structure of a *ring*, so that modular arithmetic in $\mathbb{Z}$ is equivalent to ordinary arithmetic in $\mathbb{Z}/n\mathbb{Z}$. We will take advantage of this ring structure to prove several important results in the theory of congruences.

Exercise 1. For $a + n\mathbb{Z}, b + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$, define their *sum* to be the congruence class of $a+b$, that is

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) := (a + b) + n\mathbb{Z},$$

and define their *product* to be the congruence class of ab, or

$$(a + n\mathbb{Z})(b + n\mathbb{Z}) := ab + n\mathbb{Z}.$$

Use established properties of congruences to prove that these operations are *well-defined*. In other words, prove that if $a + n\mathbb{Z} = c + n\mathbb{Z}$ and $b + n\mathbb{Z} = d + n\mathbb{Z}$, then

$$(a + b) + n\mathbb{Z} = (c + d) + n\mathbb{Z} \quad \text{and} \quad ab + n\mathbb{Z} = cd + n\mathbb{Z}.$$

Exercise 2. Show that $\mathbb{Z}/n\mathbb{Z}$ with the addition operation defined above is an abelian group.

Exercise 3. Show that $\mathbb{Z}/n\mathbb{Z}$ with the multiplication operation defined above is a commutative monoid.

Exercise 4. Show that multiplication of congruence classes in $\mathbb{Z}/n\mathbb{Z}$ distributes over addition of congruence classes.