13. \( \mathbb{Z}_n \), the integers modulo \( n \)

**Definition 1.** Let \( S \) be a set and \( \sim \) an equivalence relation on \( S \). For \( a \in S \), we define the equivalence class \( \text{cl}(a) \) by

\[
\text{cl}(a) = \{ b \in S \mid b \sim a \}.
\]

So for example, if \( S \) is the set of all people and \( \sim \) is the relation defined by \( P \sim Q \) if \( P \) and \( Q \) have the same birthday, then there are 366 distinct equivalence classes, and that everyone is in one and only one equivalence class. In general, the equivalence classes of a set form a partition of the set \( S \), which means that every element is in one and only one equivalence class.

**Exercise:** Let \( S \) be a set and \( \sim \) an equivalence relation on \( S \). For \( a, b \in S \), prove that \( \text{cl}(a) = \text{cl}(b) \) if and only if \( a \sim b \).

Now, let’s return to the equivalence on the integers defined by congruence modulo \( n \). For \( n \geq 1 \) and \( a \in \mathbb{Z} \), let \( \text{cl}(a) \) denote the equivalence class of \( a \) under this equivalence relation. Instead of \( \text{cl}(a) \), more commonly this equivalence class is denoted \([a]_n\) and is called the **congruence class** of \( a \) modulo \( n \). Following the definition, we have

\[
[a]_n = \{ b \in \mathbb{Z} \mid b \equiv a \pmod{n} \}
= \{ b \in \mathbb{Z} \mid n \mid b - a \}
= \{ b \in \mathbb{Z} \mid b - a = qn \text{ for some } q \in \mathbb{Z} \}
= \{ b \in \mathbb{Z} \mid b = a + qn \text{ for some } q \in \mathbb{Z} \}
= \{ a + qn \mid q \in \mathbb{Z} \}
\]

So for instance, \([4]_9 = \{4 + 9q \mid q \in \mathbb{Z} \}\) and \([-100]_{15} = \{-100 + 15q \mid q \in \mathbb{Z} \}\).

Note by the Exercise above, \([a]_n = [b]_n\) if and only if \( a \equiv b \pmod{n} \). In particular, for any integer \( a \), \([a]_n = [r]_n\) where \( r = \text{ln}(a, n) \), since \( a \equiv r \pmod{n} \). Hence, every congruence class modulo \( n \) is equal to one (and only one) of \([0]_n, [1]_n, \ldots, [n-1]_n\). Since no two numbers between 0 and \( n - 1 \) are congruent modulo \( n \), we can also see that none of these equivalence classes are equal.

We now define the \( \mathbb{Z}_n \), the integers modulo \( n \), to be the set of all congruence classes modulo \( n \):

\[
\mathbb{Z}_n = \{ [a]_n \mid a \in \mathbb{Z} \}
= \{ [0]_n, [1]_n, \ldots, [n-1]_n \}.
\]

Notice that \( \mathbb{Z}_n \) is **not** a set of integers, but rather a **set of subsets of the integers**. For example, \( \mathbb{Z}_3 = \{ [0]_3, [1]_3, [2]_3 \} \) has exactly 3 elements. On the other hand, every integer is in one of the three classes, \([0]_3, [1]_3, \text{ or } [2]_3\), depending on its remainder upon dividing by 3.

Now we wish to define arithmetic operations on \( \mathbb{Z}_n \).

Let \([a]_n\) and \([b]_n\) be congruence classes modulo \( n \). We define addition of congruence classes as follows:

\[
[a]_n + [b]_n = [a + b]_n.
\]

We define multiplication of congruence classes similarly:

\[
[a]_n \cdot [b]_n = [ab]_n.
\]
Now, we have to be careful in making these definitions. To illustrate, let’s suppose \( n = 8 \). Consider the sum of \([10]_8\) and \([−17]_8\). According to the definition, our answer is \([10 + (−17)]_8 = [−7]_8\). However, there are many ways to write the same congruence class. For instance, \([10]_8 = [−6]_8\) and \([−17]_8 = [7]_8\). If we use these other ways of writing the same congruence classes, we get the sum to be \([−6 + 7] = [1]_8\). However, we want only one answer! So, we ask, is \([−7]_8 = [1]_8\)? The answer is yes, since \(−7 \equiv 1 \mod 8\). We want to make sure this happens every time. Similarly with multiplication.

**Proposition 2.** Let \( n \geq 1 \) and \( a, b, c, d \) be integers. Suppose \([a]_n = [b]_n\) and \([c]_n = [d]_n\). Then

1. \([a]_n + [c]_n = [b]_n + [d]_n\).
2. \([a]_n \cdot [c]_n = [b]_n \cdot [d]_n\).

**Proof.** For the first part, we have by assumption that \([a]_n = [b]_n\) and \([c]_n = [d]_n\). By the exercise above, we have that \(a \equiv b \mod n\) and \(c \equiv d \mod n\). By Proposition 3 on Worksheet #7, we have that \(a + c \equiv b + d \mod n\). Thus, \([a + c]_n = [b + d]_n\). By definition of addition of congruence classes, we have \([a]_n + [c]_n = [b]_n + [d]_n\). The second part is left as an exercise.

**Exercise:** Prove the second part of Proposition 2.

Next, we want to be sure that the rules for this ‘arithmetic’ satisfy certain basic properties:

**Theorem 3.** Let \( n \geq 1 \) be an integer and \( a, b, c \in \mathbb{Z} \). Then

1. \([a]_n + [b]_n = [b]_n + [a]_n\) (The commutative property of addition).
2. \(([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)\) (The associative property of addition).
3. \([a]_n + [0]_n = [a]_n\) (The existence of an additive identity).
4. \([a]_n + [−a]_n = [0]_n\) (The existence of additive inverses).
5. \([a]_n \cdot [b]_n = [b]_n \cdot [a]_n\) (The commutative property of multiplication).
6. \(([a]_n \cdot [b]_n) \cdot [c]_n = [a]_n \cdot ([b]_n \cdot [c]_n)\) (The associative property of multiplication).
7. \([a]_n \cdot ([b]_n + [c]_n) = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n\) (The distributive property of multiplication over addition).
8. \([a]_n \cdot [1]_n = [a]_n\) (The existence of a multiplicative identity).

**Proof.** All of these follow by the definition of the arithmetic operations on congruence classes, along with the axioms for arithmetic on the integers. For example, let’s prove the distributive axiom:

\[
[a]_n \cdot ([b]_n + [c]_n) = [a]_n \cdot [b + c]_n = [a(b + c)]_n = [ab + ac]_n = [ab]_n + [ac]_n = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n
\]

The other properties are proved similarly.
**Exercise:** Prove the associative property of addition (part (2) of Theorem 3).

**Homework:**

1. Write down the addition and multiplication tables for \( \mathbb{Z}_9 \).

2. Give an example of an integer \( n \geq 1 \) and \( a, b \in \mathbb{Z} \) such that \([a]_n \cdot [b]_n = [0]_n\) but \([a]_n \neq [0]_n\) and \([b]_n \neq [0]_n\).

3. Let \( p \) be a prime integer and \( a, b \in \mathbb{Z} \). Prove that if \([a]_p \cdot [b]_p = [0]_p\) then \([a]_p = [0]_p\) or \([b]_p = [0]_p\).

4. Let \( n \geq 1 \) and \( a \in \mathbb{Z} \). Prove that there exists an element \([b]_n \in \mathbb{Z}_n\) such that \([a]_n \cdot [b]_n = [1]_n\) if and only if \( \gcd(a, n) = 1 \).