11 Arithmetic Modulo \( n \)

For a positive integer \( n \), the congruence modulo \( n \) relation induces a partition on the set of integers by means of the elements of \( \mathbb{Z}_n \) given by

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

Also, recall from Theorem 9.2, that if \( a \equiv b (mod \ n) \) then \([a] = [b]\). Thus, for example, if \( n = 6 \) then all of the following congruence classes are equal:

\[
[3] = [9] = [-3] = \{ \cdots, -9, -3, 3, 9, \cdots \}
\]

A word of caution must me made regarding the notation \([a]\). In later sections we will consider mappings from \( \mathbb{Z}_m \) to \( \mathbb{Z}_n \). So in order to distinguish between the elements of these sets we will adopt the notation \([a]_m\) to be an element of \( \mathbb{Z}_m \) and that of \([a]_n\) to be an element of \( \mathbb{Z}_n \). In a context where only the elements of \( \mathbb{Z}_n \) are involved then we will keep the using the notation \([a]\).

Next, we consider two operations on \( \mathbb{Z}_n \): Addition and multiplication.

**Definition 11.1**

For \([a] \in \mathbb{Z}_n\) and \([b] \in \mathbb{Z}_n\) we define addition by the rule

\[
[a] \oplus [b] = [a + b]
\]

**Example 11.1**

For \( n = 6 \), we have \([-2] \oplus [7] = [-2+7] = [5] \) and \([3] \oplus [9] = [3+9] = [12] = [0] \).

The operation of addition turns \( \mathbb{Z}_n \) into a finite Abelian group as shown next.

**Theorem 11.1**

(a) \( \oplus \) defines a binary operation on \( \mathbb{Z}_n \). That is, \( \mathbb{Z}_n \) is closed under \( \oplus \).

(b) \( \oplus \) is commutative.

(c) \( \oplus \) is associative.

(d) \([0]\) is the additive identity.

(e) Each \([a] \in \mathbb{Z}_n\) has an additive inverse \([-a] \in \mathbb{Z}_n\).

(f) \( |\mathbb{Z}_n| = n \).
Proof.
(a) We need to show that if \((a, b) \in \mathbb{Z}_n \times \mathbb{Z}_n\) and \((c, d) \in \mathbb{Z}_n \times \mathbb{Z}_n\) are such that \((a, b) = (c, d)\) then \([a] \oplus [b] = [c] \oplus [d]\). That is, \([a + b] = [c + d]\). Equivalently, according to Theorem 9.2, we need to show that \(a + b \equiv c + d (\text{mod } n)\). Since \([a] = [c]\) then \(a \equiv c (\text{mod } n)\). Similarly, since \([b] = [d]\) then \(b \equiv d (\text{mod } n)\). By Theorem 10.4, \(a - c = nq\) and \(b - d = nq'\) for some integers \(q, q'\). Thus, \((a + b) - (c + d) = n(q + q')\) and by Theorem 10.4, \(a + b \equiv c + d (\text{mod } n)\). Applying Theorem 9.2, we have \([a + b] = [c + d]\).

(b) The commutative property follows from the fact that addition in \(\mathbb{Z}\) is commutative
\[
[a] \oplus [b] = [a + b] = [b + a] = [b] \oplus [a]
\]

(c) The associative property follows from the fact that addition in \(\mathbb{Z}\) is associative
\[
([a] \oplus [b]) \oplus [c] = [a + b] \oplus [c] = [(a + b) + c] = [a + (b + c)] = [a] \oplus [b + c] = [a] \oplus ([b] \oplus [c])
\]

(d) Since 0 is the identity of the group \((\mathbb{Z}, +)\) then \([a] \oplus [0] = [a + 0] = [a]\) and \([0] \oplus [a] = [0 + a] = [a]\).

(e) Since for each \(a \in \mathbb{Z}\) we have \(a + (-a) = (-a) + a = 0\) then
\[
[a] \oplus [-a] = [a + (-a)] = [0]
\]

and
\[
[-a] \oplus [a] = [(-a) + a] = [0]
\]

(f) This follows from the definition of \(\mathbb{Z}_n\).

Remark 11.1
With the above theorem, we have a tool now to construct finite abelian groups of any order.

Example 11.2
Let us construct the Cayley table for \((\mathbb{Z}_4, \oplus)\).
Definition 11.2
The group \((\mathbb{Z}_n, \oplus)\) is called the **group of integers modulo** \(n\).

Multiplication in \(\mathbb{Z}_n\) is defined as follows:

\[
[a] \odot [b] = [ab]
\]

Example 11.3
For \(n = 6\), we have \([3] \odot [5] = [15] = [3]\).

We next state the basic properties for this operation.

**Theorem 11.2**
(a) \(\mathbb{Z}_n\) is closed under \(\odot\).
(b) \(\odot\) is commutative.
(c) \(\odot\) is associative.
(d) \([1]\) is the identity element.

**Proof.**
The proofs of (a) - (d) are quite similar to those for the corresponding parts of Theorem (11.1), and are left as an exercise for the reader.

When we compare the properties listed in Theorems 11.1 and 11.2, we see that the existence of multiplicative inverses is missing. So, in contrast to \(\mathbb{Z}_n\) with \(\oplus\), \(\mathbb{Z}_n\) with \(\odot\) needs not be a group. The following example illustrates this situation.

**Example 11.4**
Writing Cayley table for \(\mathbb{Z}_4\) we find

\[
\begin{array}{c|cccc}
\oplus & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2 \\
\end{array}
\]
Note that no element in \( \mathbb{Z}_4 \) satisfy the equation \( [x] \odot [0] = [1] \). That is, \([0]\) has no multiplicative inverse.

You might suspect that by removing the zero elements, the set \( \mathbb{Z}_n^* = \{[1], [2], \cdots, [n-1]\} \) with \( \odot \) might be a group. Unfortunately, this is true for some values of \( n \) but not for all \( n \) as shown in the following two examples.

**Example 11.5**
\( \mathbb{Z}_6^* \) is not a group with respect to \( \odot \) since \( \mathbb{Z}_6^* \) is not closed under \( \odot \). Indeed, \([2] \odot [3] = [0] \not\in \mathbb{Z}_6^* \).

**Example 11.6**
Constructing the Cayley table of \( \mathbb{Z}_5^* \) with respect to \( \odot \) we find

\[
\begin{array}{cccc}
\end{array}
\]


In the next section, we will characterize those elements in \( \mathbb{Z}_n^* \) that have multiplicative inverses in \( \mathbb{Z}_n^* \) and establish a condition on \( n \) for which \( \mathbb{Z}_n^* = \{[1], [2], \cdots, [n-1]\} \) is a group under the operation \( \odot \).