Section 8.6: The Integers Modulo n

Juan Patricio Carrizales Torres

July 4, 2022

We know that for any positive integer $n \in \mathbb{N}$, the relation R defined on $\mathbb{Z}$ by $a\ R\ b$ if $a \equiv b \pmod{n}$ is an equivalence relation that results in the distinct equivalence classes $[0], [1], \ldots, [n-1]$. Then, we can define some class that contains these equivalences classes, namely, $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$, where $\mathbb{Z}_n$ is known as **integers modulo n**. Although, some may refer to it as the set of **residue classes**. Furthermore, one can define some type of addition and multiplication on $\mathbb{Z}_n$ as follows:

$$[a] + [b] = [a+b] \quad [a] \cdot [b] = [ab],$$

for any $[a], [b] \in \mathbb{Z}_n$. Since the elements of $\mathbb{Z}_n$ are equivalence classes (partitions of $\mathbb{Z}$), it follows that both $a+b \in [c]$ and $ab \in [d]$ for some $[c], [d] \in \mathbb{Z}_n$, which implies that $[a+b] = [c]$ and $[ab] = [d]$. Hence, this addition and multiplication are *operations* in $\mathbb{Z}_n$, which means that both the sum and product of two equivalence classes are also equivalence classes. In fact, these operations are *well-defined* and so the sum and product of two equivalence classes do not depend on the representative integers. More precisely, if $[a] = [b]$ and $[c] = [d]$, then $[a+c] = [b+d]$ and $[ac] = [bd]$. This operations have the familiar properties of addition and product on $\mathbb{Z}$, namely,

(a) Commutative Property
$[a] + [b] = [b] + [a]$ and $[a] \cdot [b] = [b] \cdot [a]$ for all $a, b \in \mathbb{Z}$

(b) Associative Property
$([a] + [b]) + [c] = [a] + ([b] + [c])$ and $([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c])$ for all $a, b, c \in \mathbb{Z}$

(c) Distributive Property
$[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$ for all $a, b, c \in \mathbb{Z}$.