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 $[0], [1], \dots, [n-1]$. Then, we can define some class that contains these equivalences classes, namely, $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$, 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 $a, b, c \in \mathbb{Z}$.

Problem 57. Let $S = \mathbb{Z}$ and $T = \{4k : k \in \mathbb{Z}\}$. Thus T is a nonempty subset of S.

(a) Prove that T is closed under addition and multiplication.

Proof. Let $a, b \in T$. Then, $a = 4m$ and $b = 4n$ for some $n, m \in \mathbb{Z}$. Then, $a + b = 4m+4n = 4(n+m)$ and $ab = 16nm = 4(4nm)$. Since both $n+m$ and $4nm$ are integers, it follows that $a+b, ab \in T$. Hence, T is closed under addition and multiplication. □

(b) If $a \in S - T$ and $b \in T$, is $ab \in T$?

Solution (b). Yes. Since multiplying the integer divisible by four $b = 4m$ by the integer a, one gets the integer divisible by four $ab = 4(ma)$ which is an element of T.

(c) If $a \in S - T$ and $b \in T$, is $a + b \in T$?

Solution (c). No. Since $a \in S - T$, it follows that $a = 4k + m$ where $k \in \mathbb{Z}$ and $m \in 1, 2, 3$. Hence, $a + b = 4l + m$, where $l \in \mathbb{Z}$, is not divisible by 4 and so it is not an element of T.

(d) If $a, b \in S - T$, is it possible that $ab \in T$?

Solution (d). Yes. Let $a = 4n + 2$ and $b = 4m + 2$ for integers n, m. Hence, $a, b \in S - T$. However, $ab = 16mn + 8n + 8m + 4 = 4(4mn + 2m + 2n + 1)$ which is divisible by 4. Thus, $ab \in T$.

(e) If $a, b \in S - T$, is it possible that $a + b \in T$?

Solution (e). Yes. Let $a = 4n + 2$ and $b = 4m + 2$ for integers n, m. Hence, $a, b \in S - T$. However, $a + b = 4n + 4m + 4 = 4(m + n + 1)$ which is divisible by 4. Thus, $a + b \in T$.

We can conclude that $S - T$ is not closed under addition and multiplication.

Problem 58. Prove that the multiplication in $\mathbb{Z}_n$, $n \geq 2$, defined by $[a][b] = [ab]$ is well-defined.

Proof. Consider the equivalence classes $[a] = [b]$ and $[c] = [d]$ in $\mathbb{Z}_n$ where $a, b, c, d \in \mathbb{Z}$. Then, $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. By **theorem 4.11**, $ac \equiv bd \pmod{n}$ and so $[ac] = [bd]$. $\square$

Problem 59. (a) Let $[a], [b] \in \mathbb{Z}_8$. If $[a] \cdot [b] = [0]$, does it follows that $[a] = [0]$ or $[b] = [0]$?

Solution (a). Let $a = [2]$ and $b = [4]$. Then, $[a] \cdot [b] = [2] \cdot [4] = [8] = [0]$. However, $[2], [4] \neq [0]$.

(b) How is the question in (a) answered if $\mathbb{Z}_8$ is replaced by $\mathbb{Z}_9$? by $\mathbb{Z}_{10}$? by $\mathbb{Z}_{11}$?

Solution (b). For $\mathbb{Z}_9$, note that $[3] \cdot [3] = [0]$, for $\mathbb{Z}_{10}$, note that $[2] \cdots [5] = [0]$. However, for $\mathbb{Z}_{11}$,$[ab] = [0] = [11k]$ for some $k \in \mathbb{Z}$ if and only if either a or b are multiples of 11 since 11 is a prime integer. This suggests that the question in (a) follows only for prime numbers.

(c) For which integers $n \geq 2$ is the following statement true? (You are only asked to make a conjecture, not to provide a proof.) Let $[a], [b] \in \mathbb{Z}_n$, $n \geq 2$. If $[a] \cdot [b] = [0]$, then $[a] = [0]$ or $[b] = [0]$.

Solution (c). This seems to be true for all **prime** integers $n \geq 2$. Namely, if $[a] \cdot [b] = [0] = [nk]$ for some integer k, then $[a] = [0] = [nm]$ or $[b] = [0] = [nl]$ for integers l, m.

Problem 60. For integers $m, n \geq 2$ consider Z_m and Z_n. Let $[a] \in \mathbb{Z}_m$ where $0 \leq a \leq m-1$. Then, $a, a+m \in [a]$ in $\mathbb{Z}_m$. If $a, a+m \in [b]$ for some $[b] \in \mathbb{Z}_n$, then what can be said of m and n?

Solution 60. If $a, a+m \in [b]$ for some $[b] \in \mathbb{Z}_n$, then $a - b = kn$ and $(a+m) - b = ln$ for integers l, k. Thus, $kn + m = ln$ and so $m = n(l-k)$, where $l - k \in \mathbb{Z}$ and $l - k \neq 0$. This implies that $n \mid m$.