# FUNCTIONS OF MODULO N

Link to: physicspages home page.

To leave a comment or report an error, please use the auxiliary blog and include the title or URL of this post in your comment.

Post date: 10 September 2025.

The $\mod n$ relation is an equivalence relation. The set $\mathbb{Z}_n$ is defined as the set of equivalence classes for the integer $n$:

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

We can define mappings from one such set to another, as in $\mathbb{Z}_n \to \mathbb{Z}_m$, but if we want these mappings to qualify as functions, we must ensure that the conditions for a function are satisfied. These conditions are

(1) The relation must exist for every element $a \in \mathbb{Z}_n$. This is the completeness condition.
(2) If two elements $a, b \in \mathbb{Z}_n$ are equal, then $f(a) = f(b)$. That is, the equal elements in $\mathbb{Z}_n$ cannot map to more than one element in $\mathbb{Z}_m$. This is the uniqueness condition.

**Example 1.** Define the mapping $f$ by

$$f : \mathbb{Z}_5 \to \mathbb{Z}_{10}, \text{ where } f([a]_5) = [6a]_{10} \tag{2}$$

From the definition of the modulus, members $a$ and $b$ of the class $[a]_5$ must satisfy $5|(b-a)$. That is

$$b - a = 5q \tag{3}$$

for $q \in \mathbb{Z}$. Also, members of $[6a]_{10}$ must satisfy

$$6b - 6a = 10s \tag{4}$$

for $s \in \mathbb{Z}$. Multiplying 3 through by 6 we get

$$6b - 6a = 30q \tag{5}$$

Since $10|30q$, this is a well-defined function.

---

We can generalize this example to deal with the case $f([a]_n) = [ka]_m$ where $n, m, k \in \mathbb{N}$. That is, we map $\mathbb{Z}_n \to \mathbb{Z}_m$ where the class in $\mathbb{Z}_m$ is a multiple of the class in $\mathbb{Z}_n$.

**Theorem 1.** *With these conditions, $f$ is a well-defined map (that is, a function) if and only if $m|kn$.*

*Proof.* An 'if and only if' proof requires that we argue in both directions. First, assume that $f$ is a function. Then, since $[0]_n = [n]_n$, both these classes map to the same class in $\mathbb{Z}_m$. That is, $f([0]_n) = [k \times 0]_m = [0]_m$ and $f([n]_n) = [kn]_m$. In order for $[0]_m$ to equal $[kn]_m$, we must have $m|kn$.

Conversely, suppose that $m|kn$. Then there exists $\ell \in \mathbb{Z}$ such that $kn = m\ell$. We now wish to show that for two elements $[a]_n$ and $[b]_n$ with $[a]_n = [b]_n$, that $f([a]_n) = f([b]_n)$. That is, we start with $[a]_n = [b]_n$ which implies that $n|(b-a)$. Then

$$\begin{aligned}
n|(b-a) &\Rightarrow b-a = nq \text{ for } q \in \mathbb{Z} && (6)\\
&\Rightarrow kb-ka = knq && (7)\\
&\Rightarrow kb-ka = m\ell q = m(\ell q) && (8)\\
&\Rightarrow m|(kb-ka) && (9)\\
&\Rightarrow [ka]_m = [kb]_m && (10)\\
&\Rightarrow f([a]_n) = f([b]_n) && (11)
\end{aligned}$$

□

---

In particular, we can use the mapping of the element $[0]_n$ to prove that the map is not a function if $m \nmid kn$.

**Example 2.** Define

$$f : \mathbb{Z}_7 \to \mathbb{Z}_{12} \text{ where } f([a]_7) = [a]_{12} \tag{12}$$

In this case, $n = 7$, $m = 12$ and $k = 1$, and $m \nmid kn$ since 12 does not divide 7. Thus this is not a function. Looking at the class $[0]_7$, we have $[0]_7 = [7]_7$ but $f([0]_7) = [0]_{12}$ and $f([7]_7) = [7]_{12} \neq [0]_{12}$.

---

**Example 3.** Define

$$f : \mathbb{Z}_4 \to \mathbb{Z}_6 \text{ where } f([a]_4) = [3a]_6 \tag{13}$$

Here, $n = 4$, $m = 6$ and $k = 3$, and $6|(3 \times 4)$, so this is a well-defined function.

---

**Example 4.** Define

$$f : \mathbb{Z}_8 \to \mathbb{Z}_4 \text{ where } f([a]_8) = [ka]_4 \tag{14}$$

where $k \in \mathbb{Z}$. In this case $n = 8$ and $m = 4$. Since $4|8k$ for any $k$, this is a function.

---

**Example 5.** Define

$$f : \mathbb{Z}_4 \to \mathbb{Z}_8 \text{ where } f\left([a]_4\right) = [ka]_8 \tag{15}$$

Here, $n = 4$ and $m = 8$. In order for this to be a function, we must have $8|4k$, which is true if $k$ is an even integer.

---

**Example 6.** Suppose that $m, n \in \mathbb{Z}$such that $m > n$, and define

$$f : \mathbb{Z}_n \to \mathbb{Z}_m \text{ where } f\left([a]_n\right) = [a]_m \tag{16}$$

Since $m > n$ and $k = 1$, $m$ can never divide $kn$, so this is not a function for any such values of $m$ and $n$.