

MODULO N AS AN EQUIVALENCE RELATION

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: 7 September 2025.

The $\text{mod } n$ relation is defined as $a \cong_n b$ if $n \mid (b - a)$. An alternative notation is $a \equiv b \pmod{n}$. The $\text{mod } n$ relation is an equivalence relation. We can see this as follows.

- (1) $\text{mod } n$ is reflexive, since $a \cong_n a$ if $n \mid (a - a)$ or $n \mid 0$. Since every integer divides 0, this is true.
- (2) The relation is symmetric, since if $n \mid (b - a)$ then $n \mid (a - b)$ (the quotient just has the opposite sign).
- (3) The relation is transitive. If $a \cong_n b$ and $b \cong_n c$, this means that $n \mid (b - a)$ and $n \mid (c - b)$. Therefore $n \mid (c - b + b - a)$ so $n \mid (c - a)$.

The equivalence class of an integer a in the $\text{mod } n$ relation is the set of all elements that are related to a . We denote this by $[a]_n$. If $a \cong_n b$ then $n \mid (b - a)$ so $b - a = qn$ for any integer $q \in \mathbb{Z}$. This gives the condition

$$[a]_n = a + n\mathbb{Z} \quad (1)$$

For a given n , there are exactly n distinct equivalence classes, since each of $a = 0, 1, 2, \dots, n - 1$ gives a separate equivalence class. We denote the set of equivalence classes for the integers modulo n by $\mathbb{Z}_n$, so we have

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n - 1]_n\} \quad (2)$$

If there is no ambiguity, we can drop the subscript n on $[a]_n$, so we can refer to just $[a]$.

Example 1. For $n = 7$ we have

$$\mathbb{Z}_7 = \{[0], [1], \dots, [6]\} \quad (3)$$

Some examples of classes in $\mathbb{Z}_7$ are

- (1) $[0] = 0 + 7\mathbb{Z} = \{0 + 7q : q \in \mathbb{Z}\} = \{\dots, -14, -7, 0, 7, 14, \dots\}$
- (2) $[6] = 6 + 7\mathbb{Z} = \{6 + 7q : q \in \mathbb{Z}\} = \{\dots, -8, -1, 6, 13, 20, \dots\}$
- (3) $[25] = [3 \times 7 + 4] = [4] = \{4 + 7q : q \in \mathbb{Z}\} = \{\dots, -10, -3, 4, 11, 18, \dots\}$
- (4) $[-20] = [-3 \times 7 + 1] = [1] = \{1 + 7q : q \in \mathbb{Z}\} = \{\dots, -13, -6, 1, 8, 15, \dots\}$
- (5) $[100] = [14 \times 7 + 2] = [2] = \{2 + 7q : q \in \mathbb{Z}\} = \{\dots, -12, -5, 2, 9, 16, \dots\}$

Note that in the case of $[-20]$ we need to write -20 in proper quotient-remainder form, that is

$$-20 = 7q + r \tag{4}$$

where $0 \leq r < 7$. It is not correct to write $-20 = -2 \times 7 - 6$ and then to say that $[-20] = [6]$. It is true that $[-20] = [-6]$ but it's traditional to write the classes so that they match one of the elements of $\mathbb{Z}_7$ as given in 3.

PINGBACKS

Pingback: Functions of modulo n

Pingback: Addition and multiplication modulo n

Pingback: Linear equations with modulo n

Pingback: Cayley tables for finite groups