ADDITION AND MULTIPLICATION 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: 13 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:

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

Addition and multiplication can be defined on $\mathbb{Z}_n$. These create new relations defined as follows.

$$\oplus_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \text{ (addition)} \tag{2}$$

$$\otimes_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \text{ (multiplication)} \tag{3}$$

Addition is defined as

$$[a] \oplus_n [b] = [a+b] \tag{4}$$

where the square brackets indicate equivalence classes.

Example 1. We have

$$[5] \oplus_{10} [4] = [9] \tag{5}$$

$$[6] \oplus_{10} [5] = [11] = [1] \tag{6}$$

$$[-3] \oplus_{10} [-13] = [-16] = [4] \tag{7}$$

In the last example, we must express -16 in quotient-remainder form, where the remainder is always positive, which is $-16 = -2 \times 10 + 4$.

Multiplication is defined as

$$[a] \otimes_n [b] = [ab] \tag{8}$$

Example 2. We have

$$[5] \otimes_{10} [4] = [20] = [0] \tag{9}$$

$$[6] \otimes_{10} [7] = [42] = [2] \tag{10}$$

$$[-3] \otimes_{10} [13] = [-39] = [1] \tag{11}$$

We can also define multiples and powers of classes. For $k>0$ we have

$$k[a] = \underbrace{[a]\oplus_n [a]\oplus_n \ldots \oplus_n [a]}_{k \text{ times}} \tag{12}$$

$$[a]^k = \underbrace{[a]\otimes_n [a]\otimes_n \ldots \otimes_n [a]}_{k \text{ times}} \tag{13}$$

Example 3. We have

$$3[4]_8 = [4]\oplus_8 [4]\oplus_8 [4] = [12]_8 = [4]_8 \tag{14}$$

$$[4]_8^4 = [4]\otimes_8 [4]\otimes_8 [4]\otimes_8 [4] = [256]_8 = [0] \tag{15}$$

The *multiplicative inverse* of a class $[a]$, denoted as $[a]^{-1}$, is a class $[b]$ such that $[a]\otimes_n [b] = [1]$. Not all classes have multiplicative inverses.

Example 4. We have, for $\mathbb{Z}_{10}$:

$$[3]\otimes_{10} [7] = [21] = [1] \tag{16}$$

so $[3]^{-1} = [7]$ and $[7]^{-1} = [3]$.

The class $[2]$ has no inverse in $\mathbb{Z}_{10}$ since multiplying 2 by any integer always gives an even integer, so the associated equivalence class can never be $[1]$. Besides $[3]$ and $[7]$, the only other inverses in $\mathbb{Z}_{10}$ are $[9]$, and $[1]$, which are their own inverses, since $[9]\otimes_{10}[9] = [81] = [1]$ and $[1]\otimes_{10}[1] = [1]$. Thus, for example, $[2]^{-1}$ is not defined for $\mathbb{Z}_{10}$.

In general, the multiplicative inverse of a class $[a]$ modulo n exists if and only if $\gcd(a,n) = 1$. That is, a and n are relatively prime.

For $\mathbb{Z}_7$, we have an inverse for all a such that $1 \le a \le 6$, since all these numbers are relatively prime with 7:

$$[1]^{-1} = [1] \tag{17}$$

$$[2]^{-1} = [4] \tag{18}$$

$$[3]^{-1} = [5] \tag{19}$$

$$[6]^{-1} = [6] \tag{20}$$

For a class that has an inverse, we may define a negative power. That is, for $k>0$ we have, if $[a]$ has an inverse:

$$[a]^{-k} = \underbrace{[a]^{-1}\otimes_n [a]^{-1}\otimes_n \ldots \otimes_n [a]^{-1}}_{k \text{ times}} \tag{21}$$

Example 5. We have, for $\mathbb{Z}_{10}$:

$$[3]^{-3} = [7]^3 = [343] = [3] \tag{22}$$

PINGBACKS

Pingback: Cayley tables for finite groups