ARITMÉTICA MODULAR

En 1801, Gauss introdujo el concepto de congruencia. Adoptando el símbolo para la congruencia dada la analogía que existe entre ella y la igualdad algebraica.
Se dice que dos enteros cualesquiera a, b son congruentes módulo n si su diferencia es divisible por n, siendo n un número natural.Es decir

a, b Z a b(n) n (a – b), n N

Se demostró que se trata de una relación de equivalencia cuyo conjunto cociente se simboliza $\mathbf{Z_n}$ **.** Esta formado por clases de equivalencia cuyos indicadores corresponden a los restos de dividir por n. Dado un número entero cualquiera a, su clase de equivalencia es el conjunto formado por todos los enteros que dan el mismo resto que a al dividirlos entre n.
Si n es un número natural tal que n 2**,**

$$\mathbf{Z_n} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3},..., \overline{n-1}\}$$

En $\mathbf{Z_n}$ se definen dos operaciones binarias suma y producto de enteros módulo n;

Suma de clases de equivalencia: $\overline{+}_n : Z_n \times Z_n \rightarrow Z_n$ /

$\overline{a}, \overline{b}$ Z_n $\overline{a} \overline{+}_n \overline{b} = \overline{a + b}$

$\overline{+}_n$ Asigna a la suma de clases de equivalencia la clase de la suma en Z

Ejemplo

Para n = 3 $Z_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ la tabla de la operación binaria $\overline{+}_3$ es:

$\overline{+}_3$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Cálculo

$\overline{0} +_3 \overline{0} = \overline{0+0} = \overline{0}$

$\overline{1} +_3 \overline{0} = \overline{1+0} = \overline{1}$

$\overline{1} +_3 \overline{1} = \overline{1+1} = \overline{2}$

$\overline{1} +_3 \overline{2} = \overline{1+2} = \overline{3} = \overline{0}$

Si $\overline{h}$ y $\overline{k}$ pertenecen a $\mathbf{Z_n}$, entonces $\overline{h+k}$ es igual al resto de la división de h + k por n.

Producto de clases de equivalencia: $\overline{\ }_n : Z_n \times Z_n \rightarrow Z_n$ /

$\overline{a}, \overline{b} \quad Z_n \qquad \overline{a} \ \overline{\ }_n \overline{b} = \overline{a \quad b}$

$\overline{\ }_n$ Asigna al producto de clases de equivalencia la clase del producto.

Ejemplo

Para n = 3 $Z_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ la tabla de la operación binaria $\overline{\ }_3$ es:

$\overline{\ }_3$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Cálculo

$\overline{0} \ \overline{\ }_3 \overline{0} = \overline{0 \quad 0} = \overline{0}$

$\overline{1} \ \overline{\ }_3 \overline{0} = \overline{1 \quad 0} = \overline{0}$

$\overline{1} \ \overline{\ }_3 \overline{1} = \overline{1 \quad 1} = \overline{1}$

$\bar{2} \;\bar{\cdot}_3\; \bar{2} = \overline{1 \cdot 2} = \bar{4} = \bar{1}$

Si $\bar{h}$ y $\bar{k}$ pertenecen a $\mathbf{Z_n}$, entonces $\overline{h \cdot k}$ es igual al resto de la división de $h \cdot k$ por n.

Cabe señalar que tanto la suma de clases $\bar{+}_n$ y el producto de clases $\bar{\cdot}_n$ están bien definidas, es decir no dependen del representante escogido en cada clase.

Para n = 4 $Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ las tablas de las operaciones binarias son:

Para la suma

$\bar{+}_4$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Para el producto

$\bar{\cdot}_4$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Grupo aditivo de los enteros módulo n

La suma de clases de equivalencia cumple con las siguientes propiedades en Z_n:

Ley de composición interna

$\bar{a}, \bar{b} \in Z_n \qquad \bar{a} +_n \bar{b} = \overline{a + b} \in Z_n$

1.

1.+ es cerrada en Z

Asociatividad

$\bar{a}, \bar{b}, \bar{c} \in Z_n \qquad (\bar{a} +_n \bar{b}) +_n \bar{c} = \bar{a} +_n (\bar{b} +_n \bar{c})$

Demostración

$(\bar{a} +_n \bar{b}) +_n \bar{c} = \overline{(a + b)} +_n \bar{c} = \overline{(a+b) + c} = \overline{a + (b+c)} = \bar{a} +_n \overline{(b + c)} = \bar{a} +_n (\bar{b} +_n \bar{c})$

1.

1. + es asociativa en Z

Existencia de elemento neutro

$\bar{e} \in Z_n \ / \ \bar{a} \in Z_n: \ \bar{a} +_n \bar{e} = \bar{e} +_n \bar{a} = \bar{a}$ de donde $\bar{a} +_n \bar{e} = \overline{a + e} = \bar{a} \rightarrow a + e = a$

$\rightarrow$ e =0 es el elemento neutro de la + en Z por lo tanto $\bar{e} = \bar{0}$;

$\bar{e} +_n \bar{a} = \overline{e + a} = \bar{a} \rightarrow e + a = a \rightarrow$ e =0 es el elemento neutro de la + en Z por lo tanto $\bar{e} = \bar{0}$

Existencia de simétricos

$\bar{a} \in Z_n \quad \bar{(a)}' \in Z_n / \ \bar{a} +_n \bar{(a)}' = \bar{(a)}' +_n \bar{a} = \bar{0}$ de donde $\bar{(a)}' +_n \bar{a} = \overline{(a)' + a} = \bar{0} \rightarrow (a)' + a = 0$

$\rightarrow (a)' = -a$ es el elemento simétrico de a respecto a la + en Z por lo tanto $\bar{(a)}' = \overline{(a')}$;

$\bar{a} +_n \bar{(a)}' = \overline{a + (a)'} = \bar{0} \rightarrow a + (a)' = 0 \rightarrow (a)' = -a$ es el elemento simétrico de a respecto a la + en Z por lo tanto **(a)´ = (a´)**

Como la $+_n$ en Z_n es ley de composición interna; asociativa; con neutro y todos los elementos de Z_n tienen simétricos, el par $(Z_{n;}\ +_{n)}$ tiene estructura de grupo

Además

Conmutatividad

$\overline{a}, \overline{b} \in Z_n \qquad \overline{a} +_n \overline{b} = \overline{a + b} = \overline{b + a} = \overline{b} +_n \overline{a}$
1.

1.+ es conmutativa en Z

Por lo tanto $(Z_{n;}\ \overline{+}_n)$ *es grupo abeliano*

Semigrupo multiplicativo de los enteros módulo n

El producto de clases de equivalencia cumple con las siguientes propiedades en $Z_{n:}$

Ley de composición interna

$\overline{a}, \overline{b} \in Z_n \qquad \overline{a} \ _n \overline{b} = \overline{a \ b} \in Z_n$
1.

1. es cerrada en Z

Asociatividad

$\overline{a}, \overline{b}, \overline{c} \in Z_n \qquad (\overline{a} \ _n \overline{b}) \ _n \overline{c} = \overline{a} \ _n (\overline{b} \ _n \overline{c})$

Demostración

$(\overline{A} \ _n \overline{b}) \ _n \overline{c} = \overline{(a \ b)} \ _n \overline{c} = \overline{(a \ b) \ c} = \overline{a \ (b \ c)} = \overline{a} \ _n \overline{(b \ c)} = \overline{a} \ _n (\overline{b} \ _n \overline{c})$
1.

1. es asociativo en Z

Existencia de elemento neutro

$\bar{e} \in Z_n$ / $\forall \bar{a} \in Z_n$: $\bar{a} \odot_n \bar{e} = \bar{e} \odot_n \bar{a} = \bar{a}$ de donde $\overline{a \cdot e} = \overline{a}$ $\overline{a \cdot e} = \overline{a} \rightarrow a \cdot e = a$

$\rightarrow e = 1$ es el elemento neutro de la en Z por lo tanto $\bar{e} = \bar{1}$;

$\bar{e} \odot_n \bar{a} = \overline{e \cdot a} = \bar{a} \rightarrow e \cdot a = a \rightarrow e = 1$ es el elemento neutro de la en Z por lo tanto $\bar{e} = \bar{1}$

Existencia de simétricos

No todos los elementos de Z_n tienen simétrico respecto al $\odot_n$ (inverso multiplicativo).

Por ejemplo $\bar{0}$ no tiene inverso multiplicativo ya que $\forall \bar{a} \in Z_n : \bar{0} \odot_n \bar{a} = \overline{0 \cdot a} = \bar{0}$

Como el $\odot_n$ en Z_n es ley de composición interna; asociativo; con neutro, el par $(Z_n; \odot_n)$ tiene estructura de semigrupo con neutro

Además

Conmutatividad

$\forall \bar{a}, \bar{b} \in Z_n \quad \bar{a} \odot_n \bar{b} = \overline{a \cdot b} = \overline{b \cdot a} = \bar{b} \odot_n \bar{a}$

1.

1. es conmutativo en Z

Por lo tanto $(Z_n; \odot_n)$ es semigrupo con neutro conmutativo

Inversibles de un semigrupo con neutro e (A,*)

El conjunto de todos los elementos que tienen simétrico en el conjunto A respecto de la operación binaria ***** se denomina **conjunto de los inversibles de un semigrupo**

$$INV(A) = A' = \{ a \in A / a' \in A \}$$

Ejemplos:

1) En (Z;), los inversibles son solamente el 1 y el -1, pues los demás enteros no tienen inverso entero.Es decir Z´= {1,-1}

2) En (R;), los inversibles son todos excepto el cero.Por lo tanto R´= R – {0}

3) En el conjunto de matrices cuadradas de nxn con elementos reales y la multiplicación (R^{nxn};), los elementos inversibles son las llamadas matrices inversibles o regulares, es decir aquellas cuyo determinante es distinto de cero.

4) En (Z_4; $\bar{}_4$), los elementos que tienen inverso multiplicativo son $\bar{1}$ y $\bar{3}$ .O sea Z'_4= {$\bar{1}$,$\bar{3}$}

5) Para (Z_5; $\bar{}_5$) los inversibles son $\bar{1}$, $\bar{2}$, $\bar{3}$, $\bar{4}$.

En general para el semigrupo con neutro ($Z_{n;}$ $\bar{}_n$) el conjunto de los inversibles se obtiene de la siguiente manera:

$$Z'_n = \{\bar{k} \ / \ m.c.d\ \{k, n\} = 1 \quad 1 \quad k \quad n-1\}$$

Es decir n y k deben ser coprimos

Propiedad:

Sea (A; *) un semigrupo con neutro e. Entonces (INV (A); *) o bien (A´;*) es grupo y se lo llama Grupo de Inversibles de A.

Ejemplos

1) (Z_4; $\bar{}_4$) semigrupo conmutativo con neutro e =$\bar{1}$

Para encontrar los inversibles de Z_4: mcd {4,0}= 4; **mcd {4,1}= 1**; mcd {4,2}= 2; **mcd {4,3}= 1**

Por lo tanto Z'_4= {$\bar{1}$,$\bar{3}$}

La tabla de la operación binaria $\bar{}_4$ es la siguiente:

$\bar{}_4$	$\bar{1}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$

De la tabla

$\bar{\cdot}_4$ es ley de composición interna en Z'_4

El elemento neutro es $\bar{1}$

Los simétricos son $(\bar{1})' = \bar{1}$; $(\bar{3})' = \bar{3}$

$\bar{\cdot}_4$ es asociativo y conmutativo en Z_4 ;como $Z'_4 \subset Z_4$ entonces $\bar{\cdot}_4$ es asociativo y conmutativo en Z'_4

Por lo tanto $(Z'_4 ; \bar{\cdot}_4)$ es grupo abeliano

2) $(Z_5; \bar{\cdot}_5)$ semigrupo conmutativo con neutro $e=\bar{1}$
Los inversibles de Z_5: mcd {5,0}= 5; **mcd {5,1}= 1**; **mcd {5,2}= 1**; **mcd {5,3}= 1; mcd {5,4}= 1**

Por lo tanto,

$Z'_5 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

La tabla de la operación binaria $\bar{\cdot}_5$ es la siguiente:

$\bar{\cdot}_5$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

De la tabla

$\bar{\cdot}_5$ es ley de composición interna en Z'_5

El elemento neutro es $\bar{1}$

Los simétricos son $(\bar{1})' = \bar{1}$; $(\bar{2})' = \bar{3}$; $(\bar{3})' = \bar{2}$; $(\bar{4})' = \bar{4}$

$\bar{}_5$ es asociativo y conmutativo en Z_5 ;como $Z'_5 \subset Z_5$ entonces $\bar{}_5$ es asociativo y conmutativo en Z'_5

Por lo tanto (Z'_5 ; $\bar{}_5$) es grupo abeliano