

Matemática Discreta

Vaira, Stella - Fedonczuk, Miguel
Colliard, David - Cottonaro, Mariana

Lic en Sistemas de Información - FCyT - UADER

2022

Anillos.

El anillo de los enteros módulo n .

Definición

Sea $n \in \mathbb{Z}^+$, $n > 1$. Para $a, b \in \mathbb{Z}$, decimos que a es congruente con b módulo n , y escribimos:

$$a \equiv b \pmod{n}$$

si $n|(a - b)$ o equivalentemente $a = b + kn$ para algún $k \in \mathbb{Z}$

Ejemplos:

a) $10 \equiv 1 \pmod{3}$ porque $3|(10 - 1)$, es decir $10 = 3(3) + 1$.

También serán equivalentes con $1 \pmod{3}$ todo entero que al ser dividido por 3 da como resto 1.

b) $30 \equiv 5 \pmod{25}$ porque $25|(30 - 5)$, es decir $30 = 25(1) + 5$.

También serán equivalentes con $5 \pmod{25}$ todo entero que al ser dividido por 25 da como resto 5.

c) $29 \equiv -1 \pmod{5}$ porque $5|(29 - (-1))$, es decir $29 = 5(6) + (-1)$.

¿Puedes concluir en términos del resto, de la misma forma que en los puntos anteriores?

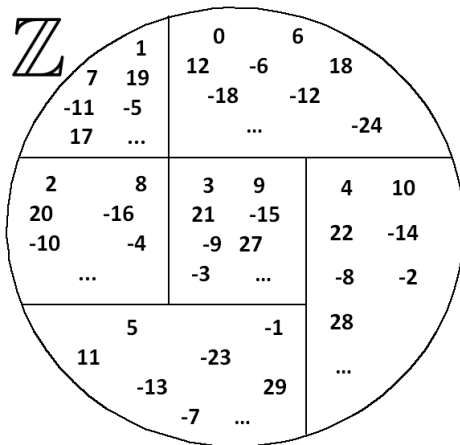
Teorema

La congruencia módulo n es una relación de equivalencia sobre \mathbb{Z}

Para $n \geq 2$ esta relación de equivalencia induce una partición sobre \mathbb{Z} .

La congruencia módulo n divide a \mathbb{Z} en n clases de equivalencias.

Por ejemplo, si $n = 6$:



Teorema

La congruencia módulo n es una relación de equivalencia sobre \mathbb{Z}

Para $n \geq 2$ esta relación de equivalencia induce una partición sobre \mathbb{Z} .
La congruencia módulo n divide a \mathbb{Z} en n clases de equivalencias:

$$[0] = \{\dots, -2n, -n, 0, n, 2n, \dots\} = \{nx + 0/x \in \mathbb{Z}\}$$

$$[1] = \{\dots, -2n + 1, -n + 1, 1, n + 1, 2n + 1, \dots\} = \{nx + 1/x \in \mathbb{Z}\}$$

$$[2] = \{\dots, -2n + 2, -n + 2, 2, n + 2, 2n + 2, \dots\} = \{nx + 2/x \in \mathbb{Z}\}$$

$$\vdots \quad \vdots$$

$$[n-1] = \{\dots, -2n + (n-1), -n + (n-1), n-1, n + (n-1), 2n + (n-1), \dots\}$$

$$[n-1] = \{nx + (n-1)/x \in \mathbb{Z}\}$$

Por el algoritmo de la división: $\forall t \in \mathbb{Z} \ t = qn + r$ con $0 \leq r < n$

Por lo que t pertenece a la clase $[r]$ o la clase de t es la misma que la clase de r ($[t] = [r]$)

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

si consideramos que a es un elemento de \mathbb{Z}_n , y no hay ambigüedad en la notación, podemos escribir:

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

En este conjunto se definen las operaciones binarias cerradas, adición y multiplicación:

$\forall [a], [b] \in \mathbb{Z}$:

$$[a] + [b] = [a + b] \quad [a] \cdot [b] = [a][b] = [ab]$$

$$[a] + [b] = [a + b] \quad [a] \cdot [b] = [a][b] = [ab]$$

Por ejemplo, en \mathbb{Z}_7 :

$$[2] + [6] = [2 + 6] = [8] = [1] \text{ y } [2][6] = [2(6)] = [12] = [5]$$

En términos de módulo diremos que:

Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, entonces

$$a + c \equiv b + d \pmod{n} \quad \text{y} \quad ac \equiv bd \pmod{n}$$

Teorema

Para $n \in \mathbb{Z}^+$, $n > 1$:

\mathbb{Z}_n es un anillo conmutativo con elemento unidad igual a $[1]$ en las operaciones binarias cerradas definidas antes.

Al ser \mathbb{Z}_n un anillo finito, podemos expresar las operaciones entre los elementos por medio de dos tablas. Por ejemplo:

\mathbf{Z}_5	+	0	1	2	3	4
	0	0	1	2	3	4
	1	1	2	3	4	0
	2	2	3	4	0	1
	3	3	4	0	1	2
	4	4	0	1	2	3

	.	0	1	2	3	4
0	0	0	0	0	0	0
1	0	1	2	3	4	0
2	0	2	4	1	3	0
3	0	3	1	4	2	0
4	0	4	3	2	1	0

Para \mathbb{Z}_5 :

Identificar las unidades, sus respectivos inversos multiplicativos. ¿Tiene divisores propios de cero? ¿Cuáles son?

\mathbf{Z}_5	+	0	1	2	3	4
	0	0	1	2	3	4
	1	1	2	3	4	0
	2	2	3	4	0	1
	3	3	4	0	1	2
	4	4	0	1	2	3

.	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Para \mathbb{Z}_6 :

Identificar las unidades, sus respectivos inversos multiplicativos. ¿Tiene divisores propios de cero? ¿Cuáles son?

$\mathbf{Z_6}$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

.	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Teorema

\mathbb{Z}_n es un cuerpo si y sólo si n es primo.

$\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7, \dots$ son cuerpo; y $\mathbb{Z}_6, \mathbb{Z}_9, \mathbb{Z}_{200}$, por ejemplo, no lo son.

Teorema

En \mathbb{Z}_n , $[a]$ es una unidad si y sólo si $\text{mcd}(a, n) = 1$

En \mathbb{Z}_{15} :

$[1], [2], [4], [7], [8], [11], [13], [14]$ son unidades.

$[3], [5]$ son divisores propios de cero porque $[3][5] = [15] = [0]$

$[6], [10]$ son divisores propios de cero porque $[6][10] = [60] = [0]$

$[9], [10]$ son divisores propios de cero porque $[9][10] = [90] = [0]$

$[12], [5]$ son divisores propios de cero porque $[12][5] = [60] = [0]$

Hallar el inverso multiplicativo de $[25]$ en \mathbb{Z}_{72}

$[25]^{-1}$ es tal que $[25]^{-1}[25] \equiv 1 \pmod{72}$

Si $[25]^{-1} = x$, buscamos que $25x = 72y + 1$, con $y \in \mathbb{Z}$

De esta manera debemos resolver la ecuación diofántica: $25x - 72y = 1$.

Resolvermos aplicando el algoritmo de Euclides:

$$\begin{array}{r|l} 72 & 25 \\ 22 & 2 \end{array} \quad 22 = 72 + (-2)25$$

$$\begin{array}{r|l} 25 & 22 \\ 3 & 1 \end{array} \quad 3 = 25 + (-1)22$$

$$\begin{array}{r|l} 22 & 3 \\ 1 & 7 \end{array} \quad 1 = 22 + (-7)3$$

Mediante una sustitución hacia atrás se obtiene que

$$1 = (-23)25 + (8)72 \quad \text{entonces} \quad 1 \equiv (-23)25 \pmod{72}$$

Como $[-23] = [-23 + 72] = [49]$

$$[25]^{-1} = [49] \text{ en } \mathbb{Z}_{72}$$

Ya sabemos cómo identificar si un elemento es, o no, una unidad.
Ahora nos preguntamos:

¿Cuántas unidades tiene el anillo \mathbb{Z}_n ?

Para calcular dicho número utilizamos la función $\varphi(n)$
Sea la factorización de n como producto de primos distintos:

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$$

$$\varphi(n) = n \left(\frac{p_1 - 1}{p_1} \right) \left(\frac{p_2 - 1}{p_2} \right) \dots \left(\frac{p_r - 1}{p_r} \right)$$

En \mathbb{Z}_n , existen $\varphi(n)$ unidades y $n - 1 - \varphi(n)$ divisores propios de cero.

Por ejemplo para $n = 7875 = 3^2 5^3 7$, \mathbb{Z}_{7875} tiene:

$\varphi(7875) = 7875 \frac{2}{3} \frac{4}{5} \frac{6}{7} = 3600$ unidades, y 4274 divisores propios de cero.

C.Aux: $7875 - 1 - 3600 = 4274$