

Definición

Sea \equiv la relación de congruencia módulo n . El conjunto de **enteros módulo n** se denota con \mathbb{Z}_n o $\mathbb{Z}/n\mathbb{Z}$ y este es el cociente \mathbb{Z}/\equiv ,

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

Resulta que el conjunto cociente \mathbb{Z}_n tiene una estructura aritmética definida por las siguientes operaciones:

$$[a] + [b] = [a + b], \quad [a][b] = [ab].$$

Por ejemplo, en \mathbb{Z}_3

$$[2][2] = [2 * 2] = [4] = [1]$$

pues 4 y 1 están relacionados: $4 \equiv 1 \pmod{3}$. Y similarmente

$$[2] + [3] = [5] = [2]$$

pues $5 \equiv 2 \pmod{3}$.

De esta forma tenemos las siguientes tablas de suma y producto en \mathbb{Z}_3 .

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

*	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

La aritmética de \mathbb{Z}_n tiene uso en criptografía.

Definición

Una partición de un conjunto B es una familia $A_i, i \in I$ de subconjuntos de B tales que

1. $B = \bigcup_{i \in I} A_i$
2. $(\forall i \in I)(\forall j \in I)(B_i \cap B_j \neq \emptyset \Rightarrow B_i = B_j)$

Sabemos que una relación de equivalencia induce una partición, siendo la familia de tal partición las clases de equivalencia.

Recíprocamente: una partición induce una relación de equivalencia.

Propiedad

Si $A_i, i \in I$, forman una partición de un conjunto B entonces esta induce una relación de equivalencia:

$$aRb \Leftrightarrow \exists i \in I \text{ tal que } a \in A_i \wedge b \in A_i$$

Dem.

Probaremos que R es relación de equivalencia:

1. Reflexiva: si $a \in B$ entonces $a \in \bigcup_{i \in I} A_i$, luego existe $j \in I$ tal que $a \in A_j$. Así $a \in A_j$ y $a \in A_j$, luego aRa .
2. Simétrica: si aRb entonces existe $i \in I$ tal que $a \in A_i$ y $b \in A_i$; luego $b \in A_i$ y $a \in A_i$ entonces bRa .
3. Transitiva: si aRb y bRc entonces existe $i \in I$ tal que $a, b \in A_i$ y existe $j \in I$ tal que $b, c \in A_j$. Luego $b \in A_i \cap A_j$, esto es $A_i \cap A_j \neq \emptyset$ lo que implica $A_i = A_j$. Entonces $a \in A_i$ y también $c \in A_i$. Por lo tanto aRc .



Ejemplo

La población de la ciudad de Puebla está dividida por colonias; luego la siguiente es una relación de equivalencia entre la población de Puebla:

$$aRb \Leftrightarrow a \text{ y } b \text{ viven en la misma colonia}$$

y la ciudad queda dividida en clases:

$$P = \underbrace{[\text{José Doger}]}_{\text{Bosques de la Calera}} \cup \underbrace{[\text{yo}]}_{\text{La Vista}} \cup \underbrace{[\text{E. Aguera}]}_{\text{Valsequillo}} \cup \dots$$

Ejemplo

Sea $B = \{a, b, c, d, e\}$. Una partición de B viene dada por

$$B = \underbrace{\{a\}}_{A_1} \cup \underbrace{\{b, c\}}_{A_2} \cup \underbrace{\{d, e\}}_{A_3}$$

Luego una relación de equivalencia en A es

$$xSy \Leftrightarrow \text{existe } i \text{ con } 1 \leq i \leq 3 \text{ tal que } x \in A_i \text{ y } y \in A_i$$

luego $[a] = \{a\}$, $[b] = \{b, c\}$ y $[d] = \{d, e\}$ y el conjunto cociente es

$$A/S = \{ \underbrace{[a]}_{A_1}, \underbrace{[b]}_{A_2}, \underbrace{[d]}_{A_3} \}$$

Ejemplo

En \mathbb{Z}_6 (la relación es $x \equiv y \pmod{6} \Leftrightarrow x - y$ es múltiplo de 6 con $x, y \in \mathbb{Z}$) tenemos que

$$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$$

y las clases forman una partición de \mathbb{Z} :

$$\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4] \cup [5]$$

Tarea

Sea A un conjunto no vacío con conjunto universal E . En 2^X se define la relación R como

$$XRY \Leftrightarrow X \cap A \subseteq Y \cap A$$

¿Qué propiedades verifica R ? ¿Es relación de equivalencia? ¿Y si en la definición se cambia \subseteq por $=$? En éste último caso calcular $[\emptyset]$ y $[E]$.

Tarea

1. Considere el conjunto de enteros módulo 5 \mathbb{Z}_5 y la clase $[3]$. Encontrar una clase $[x]$ tal que $[3x] = [1]$.
2. ¿Es posible repetir el ejercicio anterior con \mathbb{Z}_6 ?

Tarea

Describir $[4] \in \mathbb{Z}_n$ si

1. $n = 2$
2. $n = 3$
3. $n = 6$
4. $n = 8$.

Tarea

Sea R la relación de equivalencia en $\mathbb{Z} \times \mathbb{Z}$ definida por

$$(a, b)R(c, d) \Leftrightarrow ad = bc.$$

Describir $[(1, 2)]$.

Tarea

¿Cuáles de estas colecciones de subconjuntos son particiones de $\{1, 2, 3, 4, 5, 6\}$?

1. $\{\{1, 2\}, \{2, 3, 4\}, \{4, 5, 6\}\}$
2. $\{\{1\}, \{2, 3, 6\}, \{4\}, \{5\}\}$
3. $\{\{2, 4, 6\}, \{1, 3, 5\}\}$
4. $\{\{1, 4, 5\}, \{2, 6\}\}$

Tarea

¿Cuáles de estas colecciones de subconjuntos son particiones del conjunto de cadenas de bits de longitud 8?

- 1. El conjunto de cadenas de bits que empiezan por 1, el conjunto de cadenas de bits que empiezan por 00 y el conjunto de cadenas de bits que empiezan por 01.*
- 2. El conjunto de cadenas de bits que contienen la cadena 00, el conjunto de cadenas de bits que contienen la cadena 10 y el conjunto de cadenas de bits que contienen a la cadena 11.*
- 3. El conjunto de cadenas de bits que terminan en 00, el conjunto de cadenas de bits que terminan en 01, el conjunto de cadenas de bits que terminan en 10 y el conjunto de cadenas de bits que terminan en 11.*
- 4. El conjunto de cadenas de bits que terminan en 111, el conjunto de cadenas de bits que terminan en 011 y el conjunto de cadenas de bits que terminan en 00.*

Tarea

Enumerar los pares ordenados de las relaciones de equivalencia producidas por las siguientes particiones de $\{0, 1, 2, 3, 4, 5\}$:

1. $\{0\}, \{1, 2\}, \{3, 4, 5\}$
2. $\{0, 1\}, \{2, 3\}, \{4, 5\}$
3. $\{0, 1, 2\}, \{3, 4, 5\}$
4. $\{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}$