Aritmética modular

Recordemos la relación de equivalencia sobre $\mathbb{Z}$ definida de la siguiente manera:

$$R = \{(a,b) : n \mid (a - b), n \in \mathbb{Z}^+\}$$

Esta relación (llamada **congruencia módulo *n***), como toda relación de equivalencia, induce una partición del conjunto $\mathbb{Z}$.

Notación: Usamos la notación $a \equiv b \pmod{n}$ o bien $a \equiv_n b$ para indicar que $(a,b) \in R$ (se lee «a es congruente con b módulo n».

Al conjunto de todas las clases de equivalencia (el conjunto cociente) se le llama **conjunto de enteros módulo *n*** y se le representa mediante $\mathbb{Z}_n$ (se lee «zeta ene»).

Ejemplo 1. Conjunto de enteros módulo 2.

Dado que los posibles residuos al dividir por 2 son 0 y 1, entonces el conjunto $\mathbb{Z}_2$ es:

$$\mathbb{Z}_2 = \{[0], [1]\}$$

en donde, $[0] = \{2k, k \in \mathbb{Z}\}$ & $[1] = \{2k + 1, k \in \mathbb{Z}\}$.

Ejemplo 2. Conjunto de enteros módulo 3.

Dado que los posibles residuos al dividir por 3 son 0, 1 y 2, entonces el conjunto $\mathbb{Z}_3$ es:

$$\mathbb{Z}_3 = \{[0], [1], [2]\}$$

en donde, $[0] = \{3k, k \in \mathbb{Z}\}$, $[1] = \{3k + 1, k \in \mathbb{Z}\}$ & $[2] = \{3k + 2, k \in \mathbb{Z}\}$.

Listamos algunos miembros del conjunto [2]:

$$[2] = \{..., -7, -4, -1, 2, 5, 8, 11, 14, ...\}$$

Ejemplo 3. Conjunto de enteros módulo 5.

Dados que los posibles residuos al dividir por 5 son 0, 1, 2, 3 y 4, entonces el conjunto $\mathbb{Z}_5$ es:

$$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$$

en donde, $[0] = \{5k, k \in \mathbb{Z}\}$, $[1] = \{5k + 1, k \in \mathbb{Z}\}$, $[2] = \{5k + 2, k \in \mathbb{Z}\}$, $[3] = \{5k + 3, k \in \mathbb{Z}\}$ & $[4] = \{5k + 4, k \in \mathbb{Z}\}$.

Listamos algunos miembros del conjunto [3]:

$$[3] = \{..., -12, -7, -2, 3, 8, 13, 18, ...\}$$

⚠️ En general, el conjunto $\mathbb{Z}_n$ con $n > 1$ es:

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

en donde $[0] = \{kn, k \in \mathbb{Z}\}$, $[1] = \{kn + 1, k \in \mathbb{Z}\}$, ..., $[n - 1] = \{kn + (n - 1), k \in \mathbb{Z}\}$

Aritmética modular

La **aritmética modular** es un sistema aritmético (conjunto de operaciones bien definidas) para las clases de equivalencia de la relación congruencia módulo n, es decir, para el conjunto $\mathbb{Z}_n$.

🔍 La aritmética modular fue introducida por Carl Friedrich Gauss (siglo XIX).

Suma de clases de equivalencia

$[a]_n + [b]_n = [a + b]_n$

Por ejemplo, en $\mathbb{Z}_7$ $[4]_7 + [6]_7 = [4 + 6]_7 = [10]_7 = [3]_7$

👨‍🏫 Por simplicidad, ya no vamos a escribir $[k]_n$ para representar a la clase de equivalencia de k módulo n, sino que vamos a usar una *notación simplificada* y escribir solamente k.

Usando la *notación simplificada*, el ejemplo anterior se escribe como:

$$4 + 6 = 10 \equiv 3 \pmod 7$$

Multiplicación de clases de equivalencia

$[a]_n \cdot [b]_n = [a \cdot b]_n$

Usando la *notación simplificada*, tenemos, por ejemplo:

$$9 \cdot 4 = 36 \equiv 3 \pmod{11}$$

👨‍🏫 La *resta de clases de equivalencia*, se define igual que la suma. Ahora bien, la *división de clases de equivalencia* es una operación que **no está definida**. En su lugar, vamos a estudiar la *multiplicación por inversos*.

Congruencias módulo n

Si a y b son enteros y n es un entero tal que $n \geq 2$, entonces la ecuación $ax \equiv b \pmod n$ se llama **congruencia lineal**. Buscamos el valor o valores de x en $\mathbb{Z}_n$ tales que se satisfaga la congruencia lineal.

❓ ¿Cuándo tiene una congruencia lineal $ax \equiv b \pmod n$ solución?

De la definición de congruencia módulo n, $ax \equiv b \pmod n$ significa que:

$n \mid (ax - b) \rightarrow ax - b = kn \rightarrow ax + n(-k) = b$, una ecuación diofántica con variables x & k

MAC

⚠️ Entonces, podemos concluir que la congruencia lineal $ax \equiv b \pmod{n}$ tiene solución, si y solo si, ***b* es un múltiplo de mcd(*a, n*)**.

Ejemplo 4. Encuentre, si existe, la solución de la congruencia lineal $11x \equiv 4 \pmod{23}$.

Primero verificamos si el problema tiene solución. Calculamos mcd(23, 11) usando el algoritmo de Euclides:

$$23 = 2 \cdot 11 + 1$$
$$11 = 11 \cdot 1$$

$\therefore$ mcd(23, 11) = 1 $\rightarrow$ como $b = 4$ es un múltiplo de mcd(23, 11), entonces la congruencia lineal sí tiene solución.

⚠️ Si mcd(a,n) = 1, entonces la congruencia lineal $ax \equiv b \pmod{n}$ tiene solución **para cualquier valor de *b***.

Luego, por la identidad de Bézout sabemos que:

$$1 = 23 - 2 \cdot 11 \rightarrow 1 = 23 + 11(-2)$$

Recordemos que $11x \equiv 4 \pmod{23}$ *significa* que $11x + 23(-k) = 4$

Entonces, usando el resultado de la identidad de Bézout podemos multiplicar por 4 toda la ecuación:

$$1 = 23 + 11(-2) \rightarrow 4 = 23(4) + 11(-8) \rightarrow x = -8 \overset{+23}{\equiv} 15 \pmod{23}$$

En conclusión, la solución de la congruencia lineal $11x \equiv 4 \pmod{23}$ es $x \equiv 15 \pmod{23}$.

⚠️ La congruencia lineal $ax \equiv b \pmod{n}$ tiene solución única en $\mathbb{Z}_n$, si y solo si, mcd(a,n) = 1.

Ejemplo 5. Encuentre, si existe, la solución de la congruencia lineal $7x \equiv 8 \pmod{15}$.

Calculamos mcd(15,7) usando el algoritmo de Euclides:

$$15 = 2 \cdot 7 + 1$$
$$7 = 7 \cdot 1$$

$\therefore$ mcd(15,7) = 1 $\rightarrow$ la congruencia lineal tiene solución única.

Luego por la identidad de Bézout sabemos: $1 = 15 + 7(-2)$

Finalmente multiplicamos por 8 la ecuación: $8 = 15(8) + 7(-16) \rightarrow x = -16 \overset{+15}{=} -1 \overset{+15}{\equiv} 14 \pmod{15}$

En conclusión, la única solución de la congruencia lineal $7x \equiv 8 \pmod{15}$ es $x \equiv 14 \pmod{15}$

Ejemplo 6. La congruencia lineal $3x \equiv 4 \pmod{9}$ no tiene solución.

El mcd(9,3) = 3, pero $b = 4$ no es un múltiplo de mcd(9,3) = 3 $\rightarrow$ la congruencia lineal no tiene solución.